

**T.C. KOCAELİ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI**

**TÜRK CEZA HUKUKUNDA KİŞİSEL VERİLERİN
KORUNMASI**

DOKTORA TEZİ

Metin ÇOKMUTLU

KOCAELİ 2014

**T.C. KOCAELİ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI**

**TÜRK CEZA HUKUKUNDA KİŞİSEL VERİLERİN
KORUNMASI**

DOKTORA TEZİ

Metin ÇOKMUTLU

Danışman: Doç. Dr. İsa DÖNER

KOCAELİ 2014

**T.C. KOCAELİ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI**

TÜRK CEZA HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASI

DOKTORA TEZİ

Tezi Hazırlayan: Metin ÇOKMUTLU

Tezin Kabul Edildiği Enstitü Yönetim Kurulu Karar ve No:

Jüri Başkanı:

Jüri Üyesi:

Jüri Üyesi:

Jüri Üyesi:

Jüri Üyesi:

KOCAELİ 2014

İÇİNDEKİLER

İÇİNDEKİLER.....	3
ÖZET	11
ABSTRACT	12
KISALTMALAR	13
GİRİŞ	15

BİRİNCİ BÖLÜM

KİŞİSEL VERİ, KİŞİSEL VERİLERİN İŞLENMESİ VE KORUNMASI KAVRAMLARI İLE KİŞİSEL VERİLERİN KORUNMASI HAKKININ SINIRLARI

1. GENEL OLARAK	19
2. KİŞİSEL VERİ.....	22
2.1. Kişisel Verinin Tanımı.....	22
2.2. Kişisel Verinin Unsurları.....	24
2.2.1. Kişisel Verinin Unsuru Olarak Bilgi.....	24
2.2.2. Kişisel Verinin Unsuru Olarak Kimliği Belirli veya Belirlenebilir Bir Kişi.....	27
2.2.3. Kişisel Verinin Unsuru Olarak Bilginin Kişiye İlişkin Olması.....	28
2.3. Hassas Kişisel Veriler	30
3. KİŞİSEL VERİLERİN İŞLENMESİ.....	35
4. KİŞİSEL VERİLERİN KORUNMASI.....	38
4.1. Kişisel Verilerin Korunmasındaki Amaç	38
4.2. Kişisel Verilerin Korunmasının Tarihsel Gelişimi.....	39
4.3. Kişisel Verilerin Korunması Hakkının Hukuki Niteliği.....	45
4.3.1. Genel Olarak	45
4.3.2. Mülkiyet Hakkı Görüşü	48
4.3.3. Fikri Mülkiyet Hakkı Görüşü.....	50

4.3.4. İnsan Onuru, Bireysel Özerklik ve Bilgilerin Geleceğini Belirleme Hakkı Görüşü	53
4.3.5. Özel Hayatın Gizliliği Hakkı Görüşü.....	55
4.4. Kişisel Verilerin Korunması Hakkının Diğer Hak ve Özgürlüklerle İlişkisi	61
4.4.1. Bilgi Edinme Hakkı ile İlişkisi.....	62
4.4.2. İfade Özgürlüğü ile İlişkisi	64
4.4.3. Haberleşme Özgürlüğü ile İlişkisi.....	66
5. KİŞİSEL VERİLERİN KORUNMASI HAKKININ SINIRLARI.....	66

İKİNCİ BÖLÜM

ULUSLARARASI ÖRGÜTLERİN HUKUKİ DÜZENLEMELERİNDE KİŞİSEL VERİLERİN KORUNMASI VE MUKAYESELİ HUKUKTA KİŞİSEL VERİLERİN KORUNMASI HAKKININ İHLALİNE İLİŞKİN YAPTIRIMLAR

1. GENEL OLARAK	71
2. ULUSLARASI ÖRGÜTLERİN KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN HUKUKİ DÜZENLEMELERİ	72
2.1. Kişisel Verilerin Korunmasına İlişkin Birleşmiş Milletler Düzenlemeleri	72
2.2. Kişisel Verilerin Korunmasına İlişkin Ekonomik İşbirliği ve Kalkınma Teşkilatı Düzenlemeleri.....	75
2.3. Kişisel Verilerin Korunmasına İlişkin Avrupa Konseyi Düzenlemeleri	78
2.3.1. Genel Olarak	78
2.3.2. Kişisel Verilerin Otomatik İşlenmesi Sırasında Bireylerin Korunmasına İlişkin Sözleşme	80
2.3.3. Avrupa İnsan Hakları Sözleşmesi	83
2.3.3.1. Genel Olarak	83
2.3.3.2. Kişisel Verilerin Korunmasına İlişkin AİHM Kararları	85
2.3.3.2.1. Klass ve Diğerleri v. Almanya Kararı.....	85
2.3.3.2.2. Leander-İsveç Kararı.....	86
2.3.3.2.3. Rotaru-Romanya Kararı	88
2.3.3.2.4. Amann-İsviçre Kararı	90
2.3.3.2.5. P.G. ve J.H. - Birleşik Krallık Kararı	91

2.3.3.2.6. Z.-Finlandiya Kararı.....	93
2.3.3.2.7. M. S. - İsveç Kararı.....	97
2.3.3.2.8. Friedl - Avusturya Kararı.....	97
2.3.3.2.9. I v. Finlandiya Kararı.....	98
2.3.3.2.10. S. and Marper Kararı.....	99
2.3.3.2.11. Kişisel Verilerin Korunmasına Dolaylı Yönden Temas Eden Kararları.....	99
2.4. Kişisel Verilerin Korunmasına İlişkin Avrupa Birliği Düzenlemeleri.....	100
2.4.1. Genel Olarak.....	100
2.4.2. 95/46/EC sayılı Kişisel Verilerin İşlenmesi Sırasında Gerçek Kişilerin Korunması ve Bu Türdeki Verilerin Serbest Dolaşımına İlişkin Avrupa Konseyi ve Parlamentosu Direktifi.....	102
2.4.2.1. Veri Kalitesine İlişkin İlkeler.....	103
2.4.2.2. Kişisel Verilerin İşlenmesinde Hukuka Uygunluk Nedenleri.....	103
2.4.2.3. Hassas Verilerin İşlenmesi.....	104
2.4.2.4. Verileri İşlenen Kişinin Hakları.....	105
2.4.3. Avrupa Birliği Temel Haklar Şartı.....	106
2.4.4. Elektronik İletişim Alanında Özel Yaşamın Gizliliğinin Korunması ve Kişisel Verilerin İşlenmesine İlişkin Yönerge	108
2.4.5. İletişim Trafik Verilerinin Saklanması Yönergesi	108
2.4.6. Avrupa Birliği Adalet Divanının Kişisel Verilerin Korunması Hakkındaki Kararı	109
2.4.6.1. Genel Olarak	109
2.4.6.2. Unutulma Hakkı Kararı.....	110
3. MUKAYESELİ HUKUKTA KİŞİSEL VERİLERİN KORUNMASI HAKKININ İHLALİNE İLİŞKİN YAPTIRIMLAR.....	113
3.1. Genel Olarak	113
3.2. Almanya.....	113
3.3. İngiltere.....	114
3.4. Fransa.....	114
3.5. İsviçre.....	116
3.6. Amerika Birleşik Devletleri.....	116

ÜÇÜNCÜ BÖLÜM

TÜRK HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASI

1. GENEL OLARAK.....	118
2. 1982 ANAYASASINDA KİŞİSEL VERİLERİN KORUNMASI.....	119
3. KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN YASAL DÜZENLEMELER.....	125
3.1. 4721 sayılı Türk Medeni Kanun	125
3.2. 4857 sayılı İş Kanunu.....	128
3.3. 5490 sayılı Nüfus Hizmetleri Kanunu	129
3.4. 213 sayılı Vergi Usul Kanunu	131
3.5. 2559 sayılı Polis Vazife ve Salahiyet Kanunu	132
3.6. 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu.....	133
3.7. 5809 sayılı Elektronik Haberleşme Kanunu	139
3.8. 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun.....	142
3.9. 5237 sayılı Türk Ceza Kanunu	144
3.9.1. Genel Olarak	144
3.9.2. Kişisel Verilere Dolaylı Yönden Koruma Sağlayan Suç Tipleri	145
3.9.2.1. Haberleşmenin Gizliliğini İhlal Suçu.....	145
3.9.2.2. Kişiler Arasındaki Konuşmaların Dinlenmesi ve Kayda Alınması Suçu	147
3.9.2.3. Özel Hayatın Gizliliğini İhlal Suçu.....	150
3.9.2.4. Ticari Sır, Bankacılık Sırrı veya Müşteri Sırrı Niteliğindeki Bilgi ve Belgelerin Açıklanması Suçu	153
3.9.2.5. Göreve İlişkin Sırrın Açıklanması Suçu	155
3.9.2.6. Sistemi Engelleme, Bozma, Verileri Yok etme veya Değiştirme Suçu	156
3.10. 5271 sayılı Ceza Muhakemesi Kanunu	157
3.10.1. Genel Olarak	157
3.10.2. Ceza Muhakemesi Kanunda Kişisel Verilerin Korunmasına İlişkin Hükümler ..	157
3.10.2.1. Vücut Muayenesi ve Vücuttan Örnek Alınması	157

3.10.2.2. Parmak İzi Alınması ve DNA Analiz Kaydı.....	158
3.10.2.3. İletişimin Tespiti	159
3.10.2.4. Teknik Araçlarla izleme.....	162
3.10.2.5. Duruşmanın Kapalı Yapılması.....	165
3.11. 6100 sayılı Hukuk Usulü Muhakemeleri Kanunu.....	165
4. DİĞER DÜZENLEMELER.....	166
4.1. Kişisel Verilerin Korunmasına İlişkin Kanun Tasarısı	166
4.2. Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik	169

DÖRDÜNCÜ BÖLÜM

5237 SAYILI TÜRK CEZA KANUNUNDA KİŞİSEL VERİLERİN HUKUKA AYKIRI OLARAK KAYDEDİLMESİ, VERİLERİ HUKUKA AYKIRI OLARAK VERME VEYA ELE GEÇİRME, VERİLERİ YOK ETMEME SUÇLARI

1. GENEL OLARAK.....	170
2. KİŞİSEL VERİLERİN HUKUKA AYKIRI OLARAK KAYDEDİLMESİ SUÇU .	173
2.1. Genel Olarak	173
2.1. Korunan Hukuki Değer.....	174
2.3. Suçun Unsurları	176
2.3.1. Tipiklik.....	176
2.3.2. Maddi Unsurlar	177
2.3.2.1. Suçun Konusu	177
2.3.2.2. Fail ve Mağdur.....	183
2.3.2.3. Hareket ve Netice.....	185
2.3.3. Manevi Unsur.....	191
2.3.4. Hukuka Aykırılık Unsuru.....	192
2.3.4.1. Genel Olarak	192
2.3.4.2. Hukuka Uygunluk Sebepleri.....	199

2.3.4.2.1. İlgili Kişinin Rızası	200
2.3.4.2.2. Kanun Hükmünün Yerine Getirilmesi	205
2.3.4.2.3. Bir Sözleşmenin İfası İçin Gerekli Olma	208
2.3.4.2.4. Bir Hakkın Tesisi ve Kullanılması İçin Zorunlu olma.....	209
2.3.4.2.5. Hukuki Yükümlüğün Yerine Getirilmesi.....	210
2.3.4.2.6. Zorunluluk Hali.....	210
2.4. Suçun Özel Görünüş Halleri	211
2.4.1. Teşebbüs	211
2.4.2. İştirak	212
2.4.3. İçtima	212
3. VERİLERİ HUKUKA AYKIRI OLARAK VERME VEYA ELE GEÇİRME SUÇU	213
3.1. Genel Olarak	213
3.2. Korunan Hukuki Yarar	215
3.3. Suçun Unsurları	215
3.3.1. Tipiklik.....	215
3.3.2. Maddi Unsurlar	216
3.3.2.1. Suçun Konusu	216
3.3.2.2. Fail ve Mağdur	216
3.3.2.3. Hareket ve Netice.....	217
3.3.3. Manevi Unsur.....	221
3.3.4. Hukuka Aykırılık Unsuru.....	222
3.3.4.1. Genel olarak	222
3.3.4.2. Hukuka Uygunluk Sebepleri.....	222
3.3.4.2.1. İlgili Kişinin Rızası	223
3.3.4.2.2. Kanun Hükmünün Yerine Getirilmesi	224
3.3.4.2.3. Zorunluluk Hali.....	225
3.3.4.2.4. Bir Sözleşmenin İfası İçin Gerekli Olma	227
3.3.4.2.5. Bir Hakkın Tesisi ve İcrası İçin Zorunlu olma.....	227

3.3.4.2.6. Hukuki Yükümlülüğün Yerine Getirilmesi.....	228
3.4. Suçun Özel Görünüş Halleri	228
3.4.1. Teşebbüs	228
3.4.2. İştirak	229
3.4.3. İçtima	229
3.5. Suçun Nitelikli Halleri	230
3.5.1. Suçun Kamu Görevlisi Tarafından ve Görevinin Verdiği Yetki Kötüye Kullanılmak Suretiyle İşlenmesi Hali	230
3.5.2. Suçun Belli Bir Meslek ve Sanatın Sağladığı Kolaylıktan Yararlanmak Suretiyle İşlenmesi	234
4. VERİLERİ YOK ETMEME SUÇU.....	236
4.1. Genel Olarak	236
4.2. Korunan Hukuki Yarar	238
4.3. Suçun Unsurları	239
4.3.1. Tipiklik.....	240
4.3.2. Maddi Unsurlar	240
4.3.2.1. Suçun Konusu	240
4.3.2.2. Fail ve Mağdur	241
4.3.2.3. Hareket ve Netice.....	242
4.3.3. Manevi Unsur.....	246
4.3.4. Hukuka Aykırılık Unsuru.....	247
4.4. Suçun Özel Görünüş Halleri	250
4.4.1. Teşebbüs	250
4.4.2. İştirak	251
4.4.3. İçtima	251
4.5. SUÇUN NİTELİKLİ HALİ	251
4.5.1. Genel Olarak	251
4.5.2. Ceza Muhakemesi Kanununa Göre Ortadan Kaldırılması veya Yok Edilmesi Gereken Veriler.....	252

4.5.2.1. Moleküler Genetik İncelemeler Sonucu Elde Edilen Kişisel Veriler	252
4.5.2.2. Kimlik Teşhisi İçin Elde Edilen Kişisel Veriler	253
4.5.2.3. Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi Sonucu Elde Edilen Kişisel Veriler	253
4.5.2.4. Gizli Soruşturmacı Görevlendirilmesi Sonucu Elde Edilen Kişisel Veriler	254
4.5.2.5. Teknik Araçlarla İzleme Sonucu Elde Edilen Kişisel Veriler.....	254
5. YARGILAMA USULLERİ.....	255
5.1. Genel Olarak	255
5.2. Soruşturma Usulü	255
5.3. Görevli Mahkeme.....	256
5.4. Yetkili Mahkeme	257
5.5. Yaptırım.....	258
SONUÇ	260
KAYNAKÇA	271
Kitaplar	271
Makaleler	276
Yararlanılan İnternet Siteleri.....	281
ÖZGEÇMİŞ.....	282

ÖZET

Kişisel veri, kimliği belirli veya belirlenebilir bir kişiye ilişkin her türlü bilgidir. Kişinin adı soyadı, adresi gibi kimlik bilgileri; hastalıkları, tedavileri, kan grubu ve DNA bilgileri gibi sağlık kayıtları ile finansal bilgileri ve mahkûmiyetleri, kişisel veri olarak sayılabilir.

Kişisel verilerin korunması, özel hayatın gizliliği hakkı ve kişinin maddi ve manevi varlığını geliştirme hakkıyla yakından ilişkilidir. Nitekim 2010 yılında yapılan anayasa değişikliğiyle kişisel verilerin korunmasını isteme hakkı anayasal güvenceye kavuşturulmuş ve temel bir hak haline gelmiştir. Bu hakkın ihlali durumu ise 5237 sayılı Türk Ceza Kanununda suç olarak tanımlanmış ve yaptırıma bağlanmıştır.

İşte bu çalışmada kişisel verilerin korunmasını isteme hakkının ihlali halinde ortaya çıkan suçlar incelenmiştir. Bu kapsamda kişisel verilerin kaydedilmesi suçu, kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçu ve verileri yok etmeme suçu açıklanmış, uygulamada karşılaşılan sorunlar tespit edilmeye çalışılmıştır.

Çalışma tamamlandığında, gerek Anayasadaki düzenlemenin gerek TCK'daki düzenlemelerin kişisel verilerin korunmasında tek başlarına fayda sağlamadığı, uygulamadaki sorunların giderilebilmesi için bu alanı bütüncül bir şekilde düzenleyen müstakil bir kanuna ihtiyaç olduğu, bu nedenle çalışmaları halen devam eden “Kişisel Verilerin Korunması Kanunu Tasarısı”nın bir an evvel kanunlaşması gerektiği sonucuna varılmıştır.

ABSTRACT

Personal data means any information concerning an identified or identifiable person. Personal identifying information such as his or her name, surname, address; health records like illnesses, treatments, blood type and DNA information can be deemed as personal data.

Protection of personal data is closely linked to the right to respect for private and family life. The right to protection of personal data has been covered a constitutional safeguard and become a fundamental right by constitutional amendments in 2010. In case of infringement, it is considered a criminal offence in Criminal Law numbered 5237.

In this study, it has been examined some relevant crimes in the event of infringement for the right to protection of personal data. In this context, Recording of Personal Data, Illegally Obtaining or Giving Data and Destruction of Data has been clarified, has attempted to identify problems encountered in practice.

It is realized at the end of this study that, both arrangement in the Constitution and regulations in Turkish Criminal Code are not sufficient alone in the area of protection for personal data. Therefore, it needs a specific law regarding personal data to determine a holistic approach to this field and to remove problems encountered in practice. This is due to the necessity to adopt law on protection of personal data as soon as possible.

KISALTMALAR

A.B.	Avrupa Birliđi
ABAD	Avrupa Birliđi Adalet Divanı
ABD	Amerika Birleşik Devletleri
AEPD	Agencia Española de Protección de Datos
A.İ.H.M.	Avrupa İnsan Hakları Mahkemesi
A.İ.H.S.	Avrupa İnsan Hakları Sözleşmesi
A.Ü.H.F.D	Ankara Üniversitesi Hukuk Fakültesi Dergisi
A.K.	Avrupa Konseyi
A.Y.	1982 Anayasası
A.Y.M	Anayasa Mahkemesi
BDSG	Bundesdatenschutzgesetz
CGTİK	Ceza ve Güvenlik Tedbirlerinin İnfazı Hakkında Kanun
CMK	5271 sayılı Ceza Muhakemesi Kanunu
DNA	Deoksiribonükleik Asit
E.	Esas
EC	European Commission
G.Ü. H.F.D	Gazi Üniversitesi Hukuk Fakültesi Dergisi
H.U.K.A.B	Hukuk Adamları Birliđi
İ.H.E.B	İnsan Hakları Evrensel Beyannamesi
İ.Ü.H.F.D	İstanbul Üniversitesi Hukuk Fakültesi Dergisi

K.	Karar
m.	Madde
O.E.C.D	The Organisation for Economic Co-operation and Development
P.V.S.K.	2559 sayılı Polis Vazife ve Salahiyet Kanunu
R.G.	Resmi Gazete
S.	Sayı
s.	Sayfa
sk.	Sayılı Kanun
T.B.B.D	Türkiye Barolar Birliği Dergisi
T.B.M.M.	Türkiye Büyük Millet Meclisi
TCK	5237 sayılı Türk Ceza Kanunu

GİRİŞ

Kişisel veri, doğrudan doğruya ya da dolaylı olarak bir gerçek kişi ile ilintili olabilecek her türlü bilgiyi ifade etmektedir. Başka bir anlatımla, kişisel veri, bir gerçek kişi hakkında ve onu belirlenebilir kılacak her türlü bilgi olarak tanımlanmaktadır. Buna göre isim, yaş, adres, medenî durum, telefon numarası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, ses ve parmak izleri gibi bilgiler kişisel veri olarak kabul edilmektedir.

Bilgi çağı olarak nitelendirilen çağımızda, kişisel verilerin, geleneksel yöntemlerin yanı sıra bilgisayar gibi elektronik ortamlarda da işlenerek veri bankalarında depo edilmesi yaygınlaşmış, özellikle verilerin elektronik olarak işlenmesi sayesinde mal ve hizmetlerin üretilmesi ile bunların bireylere daha ucuz ve hızlı bir şekilde sunulmasına imkân sağlanmıştır. Binlerce veriyi aynı anda kaydedip depolayabilen elektronik veri işleme sistemleri, sağlık, sosyal güvenlik, eğitim, vergi, kamu düzeni ve güvenliği gibi alanlarda da yaygın olarak kullanılmaya başlanmıştır.

Kişisel verilerin bu şekilde toplanması, kaydedilmesi ve paylaşılmasının kolaylaşması bir taraftan kişilerin menfaatine uygun olsa da bir taraftan da kişisel verilerin, hukuka aykırı olarak elde edilmesi, paylaşılması, açıklanması ve yetkisiz kişilerin eline geçmesi halinde kötüye kullanılarak kişilik haklarının ihlal edilmesi ihtimallerini doğurduğundan veriler işlenirken kişinin dokunulmazlığı, maddi ve manevi varlığı ile özel hayatın gizliliği gibi temel hak ve özgürlüklerinin korunmasına da dikkat edilmelidir.

Özel hayata, aile hayatına, konuta ve haberleşmeye saygı hakkını düzenleyen Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesi kapsamında olduğu kabul edilen kişisel verilerin korunması hakkı, Anayasamızın “Özel Hayatın Gizliliği ve Korunması” üst başlığı altında düzenlenen 20. maddesine 2010 yılında yapılan Anayasa değişikliği ile üçüncü fıkra olarak eklenmiştir. Buna göre, herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Kişisel veriler ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilecektir. Kişisel verilerin korunmasına ilişkin esas ve usuller ise kanunla düzenlenecektir.

Bu maddeyle kişisel verilerin korunmasını hakkı anayasal düzeyde koruma altına alınmış, bir başka deyişle anayasal güvenceye kavuşturulmuştur. Böylece, bireylerin kendileriyle ilgili kişisel veriler üzerinde hangi hak ve yetkilere sahip olduğu ve kişisel verilerin hangi hallerde işlenebileceği hükme bağlanmıştır. Konuyla ilgili ayrıntılı düzenlemenin ise kanunla yapılması hüküm altına alınmıştır.

Anayasadaki bu amir hükme rağmen kişisel verilerin korunmasına ilişkin müstakil bir kanun henüz çıkarılabilmiş değildir. Adalet Bakanlığı tarafından hazırlanan “Kişisel Verilerin Korunması Kanunu Tasarısı” halen Başbakanlıkta TBMM’ye sevk edilmek üzere bekletilmektedir.

Kişisel verilerin bütüncül bir şekilde korunmasına ilişkin bir kanun çıkarılamasa da, 12 Ekim 2004 tarihinde yürürlüğe giren 5237 sayılı Türk Ceza Kanununda kişisel verilerin korunması hakkının ihlal edilmesi halleri suç olarak yaptırıma bağlanmıştır. Türk Ceza Kanunun 135. maddesinde “kişisel verilerin kaydedilmesi, 136. maddesinde “verileri hukuka aykırı olarak verme ve ele geçirme”, 138. maddesinde ise “verileri yok etmeme” suçları düzenlenmiştir.

Avrupa ülkelerinin 1970’li yıllardan itibaren kafa yordukları bir mesele olan kişisel verilerin korunması, ülkemizde bilgisayar teknolojilerinin ilerlemesi, özellikle internet kullanımının yaygınlaşması neticesinde, verilerin kaydının ve transferinin kolaylaşması ve bununla birlikte kötüye kullanmaların artmasıyla birlikte gündeme gelebilmiş bir konudur. Halen de kişisel verilerin gerek kamu sektörü gerekse özel sektör tarafından nasıl hukuka uygun şekilde işlenebileceği net olarak ortaya konulabilmiş değildir.

Bu husus açıklığa kavuşturulmadan kişisel verilerin hukuka aykırı şekilde işlenme hallerin suç olarak düzenlenmesi ve yaptırım altına alınması karşısında uygulamada bu suçların soruşturulması ve kovuşturulması aşamalarında birçok sorunla karşılaşmak mümkündür. Nitekim konuya ilişkin Yargıtay kararlarının çok az nitelikte olması uygulayıcıların işini zorlaştırmakta, özellikle verilerin internet üzerinde depolanması ve paylaşılması hallerinde suçların analizi ve unsurlarının tespiti kolay olmamaktadır.

2010 yılında yapılan anayasa değişikliğinden sonrada bu alanda yazılan eser sayısının yeterli olmaması da ayrı bir zorluk olarak karşımıza çıkmıştır.

İşte bu konuda yazılan eser sayısının az olması, konunun temel hak ve özgürlükleri yakından ilgilendirmesi, yaklaşık dokuz yıldır ceza kanununda yer almasına rağmen uygulamadaki tereddütlerin halen giderilememiş olması, aynı zamanda konunun Avrupa Birliği İlerleme Raporlarında ülkemizin halen yasal gereğini yerine getiremediği taahhütleri arasında yer alması nedeniyle güncel nitelik arz etmesi sebepleri, bu konuyu tez çalışması olarak seçmemizde bize fikir vermiştir.

Bu kapsamda hazırladığımız tezimiz, dört bölümden oluşmaktadır: Birinci bölümde; kişisel veri, kişisel verilerin işlenmesi ve korunması kavramları açıklanmış, bu kavramın tarihsel gelişimi, hukuki niteliği ve sınırları üzerinde durulmuştur.

İkinci bölümde, kişisel verilerin korunmasının uluslararası belgelerde ve düzenlemelerde nasıl olduğu, kişisel verilerin işlenmesinde esas alınan temel ilkelerin neler olduğu, Avrupa İnsan Hakları Mahkemesinin konuya nasıl yaklaştığı ve mukayeseli hukukta bu hakkın ihlalinin yaptırımlarının neler olduğu incelenmiştir.

Üçüncü bölümde, kişisel verilerin korunması konusunda ülkemizdeki mevcut düzenlemelerin neler olduğu açıklanmış; bu kapsamda mevcut Anayasal ve yasal düzenlemelerde kişisel verilerin korunmasına ilişkin hükümler kısaca açıklanmaya çalışılmış, bu düzenlemelerin yeterli olup olmadığına ilişkin eleştiri ve önerilere de yer verilmiş ayrıca bu konuda önemli bir kanun haline gelmesi beklenen Kişisel Verilerin Korunması Kanunu Tasarısının neler getirdiğinden de bahsedilmiştir.

Dördüncü bölümde ise, Türk Ceza Kanunun 135. maddesinde düzenlenen “kişisel verilerin kaydedilmesi”, 136. maddesinde düzenlenen “verileri hukuka aykırı olarak verme ve ele geçirme” ve 138. maddesinde düzenlenen “verileri yok etmeme” suçları ile 137. Maddede düzenlenen suçların “nitelikli halleri” doktrinin görüşleri çerçevesinde, Avrupa İnsan Hakları Mahkemesi kararları ile Yargıtay içtihatları da dikkate alınarak incelenmiş, uygulamada ortaya çıkan sorunlar tespit edilip, çözüm yolları gösterilmeye çalışılmıştır. Söz konusu suçların konusunun net bir şekilde

tespit edilebilmesi için birinci bölümdeki bilgilerden, hukuka aykırılık unsurunun açıklanabilmesi için ise ikinci bölümdeki bilgilerden faydalanılmıştır.

Maddelerin yazımından kaynaklanan ve tezimizde ortaya konan sorunların bir kısmının yasal değişiklikle çözülebileceği, maddelerin yorumundan doğan bir kısım sorunların ise kişisel verilerin korunması hukukunun bütüncül bir şekilde değerlendirilerek yorum yapılması yoluyla çözülebileceği vurgulanmıştır.

BİRİNCİ BÖLÜM

KİŞİSEL VERİ, KİŞİSEL VERİLERİN İŞLENMESİ VE KORUNMASI KAVRAMLARI İLE KİŞİSEL VERİLERİN KORUNMASI HAKKININ SINIRLARI

1. GENEL OLARAK

İçinde yaşadığımız ve “bilgi çağı” olarak adlandırılan bu çağda, bilgi ve iletişim teknolojilerinde inanılmaz bir gelişme yaşanmakta ve bu teknolojiler hızla sosyal hayatı kuşatmaktadır. Bilişim teknolojilerinin gelişimine paralel olarak, yazılı bilgi, ses, fotoğraf ve video ve benzeri kişisel bilgiler içeren objelerin sanal ortamlarda paylaşımı giderek yaygınlaşmaktadır. İnternet de, bilgi ve iletişim teknolojilerinin yaygınlaşmasında lokomotif bir rol oynamaktadır (Cate, 1998: s. 877; Aktaran: Kılınç, 2012: s. 1091).

Bilgi ve iletişim teknolojilerindeki bu ilerleme sayesinde, kişisel verilerin derleme, sınıflandırma, saklama işlemlerine tabi tutulması ve istendiğinde kolayca sunulabilmesi kolaylaşmış ve bunun sonucunda özel yaşamla ilgili bu bilgilerin haksız olarak kullanılması riski ortaya çıkmıştır. Bu teknolojiler, kişisel verilerin kişinin rızası alınmadan başkalarına açıklanmasına ve bilginin bulunduğu yerden başka yerlere aktarılmasına imkân sağlamıştır (Ersoy, a.g.m; Cate, 1998: s. 877; Aktaran: Kılınç, 2012: s. 1091).

Bilgiayarların yeni yeni kullanılmaya başlanıldığı 1960’lı yıllarda kamu kurum ve kuruluşları ve özel şirketler, kendilerine gerekli olan kişisel verileri toplamak, işlemek ve ilişkilendirmek ve saklamak yolunda büyük ilerlemeler kaydetmişlerdir. Bu başarılı uygulamalar etkinlik ve verimlilik açısından büyük avantajlar sağlarken, bir yandan da bireylerle ilgili çok kapsamlı verilerin depolanmakta olduğu görülmüştür. Böylece bir taraftan gerek kamu ve gerek özel sektör kuruluşlarını kişiler karşısında çok güçlü kılacak bilgilerin toplanması

şeklinde bir gelişme vuku bulmuş, diğer taraftan da kişi hak ve özgürlükleri yönünden bazı endişeler doğuracak olumsuzluklara yol açılmıştır¹.

1980'li yıllardan itibaren ise özellikle internet'in yaygınlaşmasıyla artık verileri toplayan ve işleyenlerin yalnızca devletler olmadığı, veri işlemenin pek çok alanda günlük hayatın bir parçası olduğu, bu kapsamda gerçek kişiler ve özel hukuk tüzel kişilerinin de yoğun bir şekilde veri işlemeye başladıkları görülmüştür. Örneğin iş alanında işçilere ait bilgilerin elektronik ortamda ya da işyerine giriş çıkışlarının elektronik olarak denetlenmesi sistemleri kullanılmaya başlanmıştır. 1990'lı yıllarda ise bankacılık ve telekomünikasyon alanlarında yapılan veri işlemler gündeme gelmiştir (Küzeci, 2010: s. 47; Ersoy, a.g.m.).

Bankacılık ve telekomünikasyon alanların yanı sıra diğer hizmet sektörlerinde de müşterilere daha iyi hizmet sunmak için onların telefon görüşmeleri de dahil olmak üzere neredeyse tüm bilgilerini kayıt altına alan şirketlerin sayısı her geçen gün biraz daha artmıştır. Bazı oteller, müşterilerine sundukları hizmetin kalitesini artırmak için onların tercihlerini uluslararası veri tabanlarından takip etmekte, internet üzerinden satış yapan şirketler kişilerin satın alma davranışlarını izlemektedirler. Bunun yanında, bankalar müşterilerine ait ayrıntılı kayıtlar tutarken, pek çok şirket, çalışanlarının iş verimliliğini denetlemek için kameralar aracılığıyla onları gözetlemekte, çeşitli havayolları şirketleri güvenlik için park eden bütün araçların plakalarını kaydetmektedirler (Küzeci, 2010: s. 47; Ersoy, a.g.m.).

Diğer yandan bireylerin kişisel verilerinin anlatıldığı kadar çok toplanabilmesi çoğu zaman kişilerin bu durumu gönüllü olarak kabul etmelerinden de kaynaklanmaktadır. Zira kişiler, verilerini paylaşıırken kendi menfaatleri gereğince de hareket edebilmektedirler. Kişiler, pek çok şirketin sunduğu çeşitli hizmetleri almak ve sunulan fırsatlardan yararlanabilmek için verilerini gönüllü bir şekilde paylaşmakta, evinde bilgisayarı üzerinden sanal alışveriş sitelerinden alışveriş yapabilmek amacıyla kimlik ve adresi bilgileri ile ödeme bilgilerini rızasıyla vermekte, bilişim teknolojilerinin gelişmesiyle ortaya çıkan internet üzerinde oluşturulan sosyal paylaşım sitelerinde, sosyal ilişkilerin içine girebilmek amacıyla,

¹ <http://www.scribd.com/doc/19952426/1-Bilisim-Surasi-Hukuk-Raporu?query=ki%C5%9Fisel+verilerin+korunmas%C4%B1>. s. 31, Erişim Tarihi:20.03.2012

bu site üzerindeki tanıdıkları ya da tanımadıkları pek çok başka kullanıcıya ve kuruluşa da verilerini paylaşabilmektedirler (Küzeci, 2010: s. 49)².

Diğer yandan günümüzde gerek devlet gerekse özel sektör elektronik ortamda çeşitli hizmetler vermektedir. E-devlet uygulamaları, internet bankacılığı ve internet üzerinden sanal alışveriş yapılabilmesi bu duruma verilebilecek en iyi örneklerdir. Bu hizmetlerin verilebilmesi için kişisel verilerin toplanması ve işlenmesi gerekmektedir. Hatta kişisel verilerin işlenmesi günümüzde zorunluluk haline geldiği de söylenebilir.

Türkiye’de, en çok veri toplayıcısı teknik tabiri ile veri işleyicisi devlettir. Devlet denen yapı içerisinde vatandaşların kimlik bilgilerini tutan nüfus ve tapu müdürlükleri, vergi daireleri, Sosyal Güvenlik Kurumu ve Adli Sicil ve İstatistik Genel Müdürlüğü gibi birçok kurum vardır. Elektronik ortamda tutulan bu kayıtların üçüncü kişilerin eline geçmesi durumu, ticarete ve şantaja konu olabileceği gibi, oy kullanma süreçlerinde ve nüfus kaydı işlemlerinde sahteciliklere veya ölmüş birinin yerine geçme gibi birçok kanun dışı işlem ve uygulamalara neden olabilmektedir.

Kişilerin devlet eliyle tutulan en önemli kayıtlarının kimlik bilgileri ve adres bilgileri olduğu kabul edilmekle birlikte özel kurumlarca tutulduğu kabul edilen en önemli kayıtlar ise kredi kartı bilgileri ve telefon kayıtlarıdır. Kredi kartı ile yapılan alışverişlerden kişinin tüketim alışkanlıkları, yaşam biçimi, yaşadığı, bulunduğu yerler belirlenebilmekle birlikte yasal bir soruşturma kararı olmadan bireyin bu yolla izlenmesi bireysel haklara tecavüz olarak nitelendirilmektedir (E. Kurt, a.g.m.).

Kişisel bilgilerin korunması konusunda telefon kayıtları da önemli bilgiler içermekte özellikle bağlı olduğu sistemle sürekli etkileşim halinde olan cep telefonu vasıtasıyla kişilerin yerleri tespit edilebilmektedir. Diğer taraftan internette harcanan her saniyenin bırakacağı izlerin birleştirilmesi suretiyle toplanan verilerden hareketle kullanıcının hangi sayfalara bağlandığı, kimlerle internetten haberleştiği gibi hususlarla ilgili birçok başka bilgi edinilebilmekte ve bu bilgilerin tümü bir kişisel

² Sosyal paylaşım siteleri, kullanıcıların sosyal ağda yer alan profillerinden indirilen tüm bilgi ve resimlere erişilebilmeye ve bunların internet kullanan herkes tarafından görülebilmesine imkân sağlamaktadır. Sosyal Paylaşım siteleri hakkında ayrıntılı bilgi için bkz. **Evcı, Özge**, “Facebook ve Kişisel Bilgi Güvenliği”,

<http://hukukcu.com/modules/smartsection/item.php?itemid=205> et:21.02.2012

veri olup kullanıcı hakkında bir kullanım profilinin oluşturulmasına imkân sağlamaktadır (E. Kurt, a.g.m.; Dinç, a.g.m.).

Kişisel verilerin bu şekilde işlenmesi, çeşitli sorunları da ortaya çıkarmıştır. Örneğin, öncelikle hangi veriler kişisel veri olarak kabul edilecektir? Bu verileri kimler toplayacaktır? Bu veriler nerelerde kullanılacaktır? Bu veriler ne kadar süre saklanacaktır? Bu verilere kimler ulaşabilecektir? Bu veriler nasıl korunacaktır? Şeklindeki soru ve sorunlar ile karşı karşıya kalınmıştır (Kılınç, 2012: s. 1092).

İşte bu sorunlara çözüm bulabilmek için öncelikle bu kavramların etraflıca açıklanmasında fayda bulunmaktadır.

2. KİŞİSEL VERİ

2.1. Kişisel Verinin Tanımı

Kişisel veri, doğrudan doğruya ya da dolaylı olarak bir gerçek kişi ile ilintili olabilecek her türlü bilgiyi ifade etmektedir (Başalp, 2004: s. 33). Buna göre isim, yaş, adres, medenî durum, telefon numarası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim ve ses, parmak izleri gibi bilgiler kişisel veri olarak kabul edilmektedir.

Ulusal ve uluslar arası pek çok belge ve sözleşmede kişisel veri, açık bir şekilde tanımlanmıştır³.

Avrupa Konseyi tarafından hazırlanan “Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme” nin 2. maddesinde kişisel veri; “Kimliği belirtilen veya belirtilebilen gerçek kişiyle ilgili tüm bilgiler” olarak tanımlanmıştır⁴.

Kişisel verilerle ilgili önemli bir düzenleme olan Avrupa Birliği’nin “95/46/EC sayılı Kişisel Verilerin İşlenmesi ve Bu Türdeki Verilerin Serbest Dolaşımı Bağlamında Bireylerin Korunmasına İlişkin Avrupa Konseyi ve

³ Avrupa Birliği Veri Koruma Direktifi m.2/1-a, Avrupa Konseyinin 108 Nolu Sözleşmesi, m. 2/1-a, Kişisel Verilerin Korunması Kanun Tasarısı m.3, **Küzeci**, s. 9

⁴ Sözleşmenin orijinal metni için bkz. <http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm>
Erişim Tarihi: 28.01.2014;

Parlamentosu Direktifi” nin 2. maddesinde kişisel veri; “Kimliği belirli veya belirlenebilen bir kişiyle ilgili her türlü bilgi” olarak tanımlanmıştır⁵.

Maddenin devamında “bir gerçek kişinin belirlenebilir olması, özellikle şifre numarasına göre ya da psişik, psikolojik, fiziksel, ekonomik, kültürel veya sosyal benliği ifade eden bir veya birden fazla unsura aidiyeti aracılığı ile doğrudan veya dolaylı olarak teşhis edilebilmesi anlamına gelmektedir” şeklinde ifade edilmiştir. Buna göre; bir kişinin doğrudan veya dolaylı olarak tanımlanabilmesine imkân sağlayan kişinin kimlik numarası, fiziksel, psikolojik, duygusal, ekonomik ve kültürel kimliği veya sosyal kimliği kişisel veri olarak değerlendirilebilir. Yine, isim, telefon numarası, elektronik posta adresi, doğum tarihi, parmak izi, DNA, adres, sosyal güvenlik numarası, hesap numarası da bu kapsamdadır (Civelek, 2011: s. 16; Kılınç, 2012: s. 1094; Şimşek, a.g.m.).

Federal Almanya Verilerin Korunması Kanunu'nda kişisel veri; “Belirli ya da belirlenebilen bir gerçek kişinin kişisel ya da maddi ilişkilerine ait münferit veriler” olarak tanımlanmıştır (Şimşek, a.g.m.).

Avusturya Verilerin Korunması Kanunu'nda kişisel veri, kişisel nitelikli veri olarak ifade edilmiş ve “Kimliği belirli ya da belirlenebilen ilgili hakkındaki bilgiler” şeklinde tanımlanmıştır (Şimşek, a.g.m.).

Kişisel Verilerin Korunması Kanunu Tasarısının 3. maddesinde kişisel veri; “Belirli veya kimliği belirlenebilir gerçek kişilere ilişkin bütün bilgiler” şeklinde ifade edilmiştir⁶.

Doktrinde de; kişisel veri, uluslar arası sözleşme ve belgelerdeki tanımlamayla benzer şekilde, “belirli veya belirlenebilir nitelikteki bir kişiye ilişkin her türlü bilgi” olarak tanımlanmıştır (Şimşek, 2008: s. 43; Arslan, 2011: s. 33; Kaymaz, 2011: s. 79)⁷.

⁵ Direktifin orijinal metni için bkz. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML> Erişim Tarihi: 28.01.2014

⁶ Tasarının ilk halinde tüzel kişilerin de verileri kapsam dâhilinde iken yenilenen Tasarıda sadece gerçek kişilerin verileri korunma kapsamına alınmıştır. Bkz.

<http://www.kgm.adalet.gov.tr/Tasariasamaları/Basbakanlik/Basbakanlik.html> Erişim T: 10.04.2014

⁷ Kılınç ise kişisel verinin gerçek kişilere ait olabileceği gibi tüzel kişilerin verilerinin de kişisel veri olabileceğini savunmuştur. Bkz. **Kılınç**, s. 1094. Ancak biz bu görüşe katılmıyoruz.

O halde, kişisel veriyi, belirli veya belirlenebilir bir gerçek kişi hakkında her türlü bilgi olarak tanımlanmak mümkündür.

Görüldüğü üzere kişisel veriler, kişiyi hangi yönden ilgilendirirse ilgilendirsin, kişi hakkındaki tüm bilgilerdir. Bu kapsamda kişi hakkında önemsiz veriler ve yayımlanmış veriler de bu kavrama dâhildir (Şimşek, 2008: s. 43; Özdemir, 2009, s. 124).

İleride kişisel verilere karşı işlenen suçların konusunun sınırlarının net bir şekilde çizilebilmesi için kişisel veri kavramının kapsamının ayrıntılı bir şekilde açıklanmasında fayda bulunmaktadır.

Nitekim Avrupa Birliğinin 1995 yılında kabul ettiği AB Veri Koruma Yönergesinin 29. maddesi çerçevesinde kurulan ve veri koruması ile mahremiyet konularında faaliyet gösteren bağımsız bir tavsiye organı niteliğindeki çalışma grubu (Working Party), üye ülkelerde kişisel veri kavramına yaklaşım farklılığını önlemek için kişisel veri kavramının tanım ve unsurlarına ilişkin olarak bir rapor hazırlamıştır⁸.

2.2. Kişisel Verinin Unsurları

Yukarıda bahsedilen kişisel veri tanımından yola çıkarak, ulusal ve uluslararası düzenlemelerde dikkate alınmak suretiyle, kişisel veri kavramının üç temel unsurdan oluştuğunu söylemek mümkündür. Bu çerçevede, kişisel veri kavramının unsurları; “bilgi”, “kimliği belirli veya belirlenebilir bir kişi” ve “bilginin kişiye ilişkin olması”dır⁹.

2.2.1. Kişisel Verinin Unsuru Olarak Bilgi

Kişisel veri kavramının unsurlarından ilki bilgidir. Yukarıda belirtildiği üzere hem AB Direktifi hem de Tasarı da, kişisel veri, belirli veya kimliği belirlenebilir olmak şartıyla bir kişiye ilişkin “bütün bilgiler” olarak tanımlanmıştır. Bu tanımlara

⁸ Rapor için bkz. **Article 29 Data Protection Working Party**: Opinion 4/2007 on the Concept of Personal Data, <ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf, s. 3. (Aktaran; **Aksoy, Hüseyin Can**, Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması, Çakmak Yayınevi, Ankara, 2010, s. 13)

⁹ Benzer tasnif için bkz. **Aksoy**, 2010, s. 13

göre, içeriğinden bağımsız olarak, bir kişiye ilişkin her türlü bilgi kişisel veri niteliği taşımaktadır. Nitekim kişisel veri kavramının tanımında yer alan “bütün bilgiler” ifadesinin oldukça geniş kapsamlı bir ifade olması, kanun koyucunun bu konudaki iradesini yansıttığından söz konusu ifadeyi geniş şekilde yorumlamak uygun olacaktır (Aksoy, 2010: s. 13). Bu bağlamda, bir kimsenin özel hayatı ve aile yaşamına ilişkin bilgiler kişisel veri niteliği taşıdığı gibi, aynı kişinin iş ilişkileri ve ekonomik ve sosyal yaşamına ilişkin bilgiler de kişisel veri olarak kabul edilmelidir. Ancak, belirli veya kimliği belirlenebilir olmak şartıyla, bir kişiye ilişkin bilginin kişisel veri olarak kabul edilmesi, söz konusu bilginin gizli olmasını gerekli kılmamaktadır. Örneğin, kişinin cinsel tercihi ve kredi kartı şifresi gibi gizli bilgiler kişisel veri olduğu gibi, kişinin fiziksel özellikleri, arabasının markası ve kamuya açık bir toplantıda giymiş olduğu kıyafetin rengi gibi herkesçe rahatlıkla ulaşılabilecek şekilde aleni bilgiler de kişisel veri kapsamına girmektedir¹⁰.

Bir bilginin nesnel veya öznel nitelik taşıması, o bilginin kişisel veri olarak kabul edilip edilmemesi bakımından herhangi bir önem taşımamaktadır. Bu bağlamda, bir kimsenin geçirdiği hastalıklara, malvarlığına veya mesleğine ilişkin nesnel bilgi bir tür kişisel veri kabul edilecekken, benzer şekilde bir kimsenin zengin veya fakir olduğu ya da karakter itibarıyla güvenilir veya güvenilmez olduğu gibi öznel bilgiler, görüşler ve değerlendirmeler de kişisel veri kapsamında değerlendirilecektir. Nitekim, bu ikinci grup bilgiler, istihdam ve sigorta sektörleri ile bankacılık sektöründe önemli ölçüde kullanılmaktadır. Örneğin, bir bankadan kredi başvurusunda bulunan bir kimsenin güvenilirliğinin değerlendirilmesinde, söz konusu öznel nitelikli bilgiler büyük önem taşımaktadır (Aksoy, 2010: s. 14).

Ayrıca, aranan diğer şartları taşıdığı sürece, herhangi bir bilginin kişisel veri olarak kabul edilebilmesi için, gerçek veya doğruluğu kanıtlanmış olması koşulu da aranmamaktadır. Örneğin, bir kimsenin iflas etmiş olduğuna dair bir bilgi, aslen yanlış dahi olsa, o kişiye ilişkin kişisel bir veri olarak kabul edilecektir. Nitekim bu bilgiyi elde eden bir bankanın, o kişinin yapmış olduğu kredi başvurusunu geri çevirmesi ihtimali büyük ölçüde artmaktadır. Benzer şekilde, asılsız haber olmakla birlikte, bir kimsenin eşini aldattığına veya bir suç islediğine dair yayınlanan bir

¹⁰ **Article 29 Data Protection Working Party**, s. 6 (Aktaran: Aksoy, 2010: s. 14)

gazete haberi de, doğru olup olmadığına bakılmaksızın, kimliği belirli bir kimseye ilişkin bilgi olduğundan, kişisel veri niteliği taşımaktadır¹¹.

Diğer taraftan bir bilginin kişisel veri olup olmadığı meselesi, o bilginin biçiminden ve saklandığı ortamdan bağımsız olarak ele alınmalıdır. Nitekim AB Direktifi ve Tasarıda kişisel verilerin işlenmesi tanımlanırken verilerin “otomatik olan veya otomatik olmayan yollarla elde edilmesi...” şeklinde bir tanımlama metodu kullanılarak, aranan diğer şartları taşıdığı sürece, bir verinin niteliği itibarıyla alfabetik, sayısal, çizgesel, fotografik veya akustik olması ile kâğıt üzerinde veya bilgisayar ortamında saklanması önemli olmadığı vurgulanmıştır. Buna göre, ses ve görüntü verilerinin de kişisel veri olarak kabul edilmesi gerekmektedir. Örneğin, güvenlik kameraları ile kaydedilen görüntüler ile telefon bankacılığı işlemleri sırasında müşterinin kaydedilen sesi kişisel veri olarak kabul edilmelidir¹².

Yukarıda yapılan açıklamalara bakıldığında hangi verilerin kişisel olduğunu saptamakta bir sorun bulunmamaktadır. Bu noktada, verinin ne olduğuna da kısaca değinmek gerekir. Zira doktrinde “veri”, “enformasyon” ve “bilgi” kavramlarının birbirlerinin yerine kullanıldığı ve aralarında fark olup olmadığı hususlarında görüş birliği olmadığı görülmektedir (Küzeci, 2010: s. 9-10).

Türk Dil Kurumu tarafından veri; bir araştırmanın, bir tartışmanın, bir muhakemenin temeli olan ana öge, muta, done; bir sanat eserine veya bir edebî esere temel olan ana ilkeler; bir problemde bilinen, belirtilmiş anlatımlardan bilinmeyeni bulmaya yarayan şey; olgu, kavram veya komutların, iletişim, yorum ve işlem için elverişli biçimli gösterimi olarak tanımlanmıştır (Türkçe Sözlük, 2009. S. 2087). Görüldüğü üzere veri, matematik, bilişim ve edebiyat, gibi çeşitli alanlarda farklı şekillerde tanımlanmıştır.

Bilgi ise, yine birden fazla anlamda; insan aklının erebileceği olgu, gerçek ve olguların bütünü, malumat; öğrenme, araştırma veya gözlem yoluyla elde edilen gerçek, malumat, vukuf; insan zekâsının çalışması sonucu ortaya çıkan düşünce ürünü; genel olarak zihnin kavradığı temel düşünceler, malumat; bilim; kurallardan

¹¹ **Article 29 Data Protection Working Party**, s. 6 (Aktaran: Aksoy, s. 14)

¹² **Article 29 Data Protection Working Party**, s. 7-8 (Akran: Aksoy, s. 15-16); Benzer şekilde ses ve görüntü verilerinin de kişisel veri olarak kabul edileceğine ilişkin bkz. Küzeci, 2010: s. 12- 30; Başalp, 2004: s. 34; Şimşek, 2008: s. 42

yararlanarak kişinin veriye yönelttiği anlam olmak üzere birden çok şekilde tanımlanmıştır (Türkçe Sözlük, 2009. S. 267).

Doktrinde de bilgi, anlamlı bir biçime sokularak, kullanıcısına güncel ve olası kararların alınmasında yardımcı olan veri olarak tanımlanmıştır (Çubukçu, 1987: s. 24). Bu görüşten bilginin, verinin işlenmesi sonucu ortaya çıkan bir kavram olduğu anlaşılmaktadır. Diğer yandan, bilgi ve verinin birbirinden farklı kavramlar olduğu, bilginin temel ve her türlü malumat olduğu, bu malumatın bilgisayarın anlayıp işleyebileceği haline de veri denildiği doktrinde ileri sürülmüştür (L. Kurt, 2005: s. 38).

Türk Dil Kurumu Türkçe Sözlükte yapılan tanımlara bakıldığında ise, bilgi ve verinin hemen hemen eş anlamlarda kullanıldığı görülmektedir. Her iki kavramın karışık ve belirsiz yapısı, yukarıda da belirtildiği üzere birden çok tanımlama yapılması dikkate alındığında, her iki kavram arasında farklılıklar olduğu kabul edilse de, kişisel verilerin korunması konusunda birbirlerinin yerine kullanılmalarında herhangi bir sorun olmayacağı ifade edilmiştir (Küzeci, 2010: s. 12).

Bizde tezimizde kişisel verilerin korunması konusunda veri ve bilgi kavramlarını eşdeğer kabul ederek açıklamalarda bulunacağız.

2.2.2. Kişisel Verinin Unsuru Olarak Kimliği Belirli veya Belirlenebilir Bir Kişi

Kişinin belirli olması, kişinin adı, soyadı, kimlik numarası gibi verilerle kişinin kimliğinin doğrudan ortaya çıkarılması demektir. Yani karışık birtakım işlemlere gerek duymadan doğrudan bir kişiyle bağlantı kurmayı mümkün kılan veriler belirli kişilere ilişkindir (Şimşek, 2008: s. 122). Örneğin, “A şahsına ait doğum tarihi” şeklinde kaydedilmiş bir veri, belli bir kişiye ait kişisel veri olarak kabul edilmelidir.

Kişinin belirlenebilir olması hususu ise, verilerin doğrudan veya dolaylı olarak bir gerçek kişiyle ilişkilendirilmesi suretiyle kişiyi tanımlayabilme özelliğini ifade eder. Örneğin verilerin bir kimlik numarasıyla ilişkilendirilmesi, yada kişinin psişik, psikolojik, fiziksel, ekonomik, kültürel, veya sosyal kimliğini, ifade eden spesifik bir içerik taşıması sonucunda kişinin belirlenmesini sağlayan tüm halleri

kapsar. Başka bir ifade ile isim, telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim ve ses, parmak izleri gibi bilgilerin kombinasyonu sonucu o kişiye ulaşılabilmesini ifade eder (Başalp, 2004: s. 33-34). Örneğin, bir kişinin ismi kaydedilmese bile, 50 yaşında olduğu, iki çocuk sahibi olduğu, muhasebeci olduğu, şurada çalıştığı gibi veriler kaydedilirse bu kişinin özellikleri vasıtasıyla belirlenebilir kılınması söz konusudur (Şimşek, 2008: s. 43). Diğer yandan, Anayasa Mahkemesinin şu anki Başkanına, geçen seneki Adalet Bakanına ilişkin bir veri söz konusu olduğunda da bu verileri belirlenebilir kişilere ait kişisel veri olarak nitelendirebiliriz.

Ancak istatistiksel bilgiler, yani herhangi bir kişiyle ilişkili olmayan, herhangi bir kişi ile ilişkilendirilemeyen veriler, kişisel veri olarak kabul edilemez¹³.

2.2.3. Kişisel Verinin Unsuru Olarak Bilginin Kişiye İlişkin Olması

Her şeyden önce belirtmek gerekir ki, kişisel verilerin korunması hakkı öncelikle gerçek kişiler için söz konusudur. Yani verilerin korunması hukuku bakımından verilerin, belirli veya belirlenebilir bir gerçek kişiye ilişkin olması gerekmektedir (Şimşek, 2008: s. 121-122).

Kişisel verilerin korunmasına ilişkin uluslararası düzenlemelerin verilerin işlenmesi sırasında esas olarak gerçek kişileri korumayı hedef aldıkları görülmektedir. Bu çerçevede Avrupa Konseyinin Verilerin Korunmasına İlişkin Sözleşmesi geçerlilik alanını gerçek kişilerle ve gerçek kişilere ait (kişisel) verilerle sınırlamıştır¹⁴. Buna karşılık Sözleşmeye taraf Devletler, dolaylı veya doğrudan gerçek kişilerden oluşan kişi grupları, dernekler, vakıflar, topluluklar, kurumlar ve öteki organlar bakımından da Sözleşmenin uygulanabileceğini belirtebileceklerdir¹⁵. Aynı şekilde OECD'nin Verilerin Korunmasına ilişkin Rehber İlkeleri de geçerlilik alanını belirli veya belirlenebilir gerçek kişiler ile sınırlamış (m. 1), tüzel kişilerin ve kişi gruplarının uygulama alanına dâhil edilmesi üye Devletlerin takdirine bırakılmıştır (m. 6).

Avrupa Birliğinin Kişisel Verilerin Korunması Direktifi de (95/46/EC) gerçek kişilerin korunmasına yöneliktir. Direktifin uygulama alanının düzenlendiği 3.

¹³ Bu tür verilere anonim veriler de denmektedir. Bkz. **Arslan**, 2011: s. 33-34.

¹⁴ Bkz. AK 108 nolu Sözleşme md. 2/ a

¹⁵ Bkz. AK 108 nolu Sözleşme md. 3/ 2-b).

maddesinde, Direktifin gerçek kişilere ilişkin veri işleme faaliyetlerinde uygulanacağı belirtilmektedir. Buna karşılık Avusturya, Danimarka, İtalya ve Lüksemburg ile AB üyesi olmayan İzlanda, Norveç ve İsviçre gibi bazı Devletlerin verilerin korunmasına ilişkin kanuni düzenlemelerinde tüzel kişileri de koruma kapsamına aldıkları görülmektedir (Aksoy, 2010: s. 19; Şimşek, 2008: s. 122).

O halde kişisel verilerin korunması temel hakkının sahibi gerçek kişilerdir. Diğer bir deyişle kişisel verilerin korunması hakkının sahibi "herkes"tir. Dolayısıyla bu hak bir insan hakkıdır. Kişisel verilerin korunması hakkı esas olarak bireyin kişisel verilerinin geleceğini belirleme hakkını koruduğundan hak sahibinin yaşayan bir gerçek kişi olması gerekir. Bu nedenle insan öldükten sonra kişisel verilerin korunması hakkının doğrudan sahibi olamamaktadır (Şimşek, 2008: s. 123).

Kişisel verilerin korunması hakkının temel hak bağlamında esasında insan kişiliğini ve onun özel alanını koruduğu noktasından hareket edilirse, kişisel verilerin korunması hakkının tüzel kişilere uygulanamayacağı sonucuna varılmaktadır. Buna karşılık şüphesiz ki tüzel kişiler nezdinde doğrudan veya dolaylı olarak bireyler hakkındaki kişisel verilerin bulunması (örneğin, bir işletmenin ticari ilişkilerinde işletmecinin kişisel verilerin bulunması gibi) da mümkündür. Örneğin bir Limited Şirkete ilişkin bazı veriler içerisinde şirket ortaklarına veya müdürüne ilişkin bilgiler de bulunabilir. Dolayısıyla tüzel kişilere ilişkin veriler, aynı zamanda gerçek kişiye ilişkin kişisel verileri de içeriyorsa, bu verilerde kişisel verilerinin korunması hakkı kapsamında korunmalıdır (Başalp, 2004: s. 35; Şimşek, 2008: s. 123).

Kanaatimizce de, temel bir insan hakkı olan kişisel verilerin korunmasının gerçek kişilere yönelik olması daha uygun olacaktır. Zira bu hak bir insan hakkıdır. Bu hak bireyin kişisel verileri üzerindeki belirleme hakkını koruduğundan hak sahibinin yaşayan, gerçek kişi olması gerekmektedir. Nitekim yukarıda da açıklandığı üzere uluslararası düzenlemeler ve Anayasal düzenlememiz de bu yöndedir¹⁶.

¹⁶ Ayrıca Kişisel Verilerin Korunması Kanun Tasarısı, 08/06/2012 tarihinde Adalet Bakanlığı tarafından yenilenerek Başbakanlığa gönderilmiş olup, yenilenen Tasarıda da tüzel kişilerin verileri kapsam dışına çıkarılarak sadece gerçek kişilerin verileri koruma altına alınmıştır.

2.3. Hassas Kişisel Veriler

Kişisel verilerin korunması alanında karşımıza çıkan diğer önemli bir kavram da “hassas veriler”, diğer bir ifadeyle “özel nitelikli veriler” dir. Veri koruma kanunları bulunan hemen hemen bütün ülkeler hassasiyet gösteren bazı veri türleri olduğunu kabul etmişler ve bu yönde düzenlemeler yapmışlardır¹⁷.

Kişisel verilerin korunmasına ilişkin uluslararası belgelerde ve veri koruma kanunlarında genellikle kişilerin ırksal kökenine, dini ve felsefi inançlarına, sağlık durumlarına ve siyasi görüşlerine ilişkin veriler hassas veri olarak kabul edilmektedir. Bu bağlamda hassas veriler, kişisel verilerin daha fazla koruma uygulanan küçük bir grubu olarak ifade edilmektedirler. Ayrıca, 95/46 sayılı Veri Koruma Direktifinin giriş kısmında hassas veriler, temel hakları ve özel yaşamın gizliliğini ihlal edici nitelikte bulunan veriler olarak tanımlanmıştır¹⁸.

Kişisel verilerin korunmasıyla ilgili uluslararası belgelere bakıldığında, belirli konularla ilgili kişisel verilerin diğerlerine göre daha sıkı bir koruma altına alındığı görülmektedir.

Avrupa Konseyi’nin 108 sayılı Sözleşmesinin “Özel Veri Kategorileri” başlıklı 6. maddesinde hassas veriler açısından daha kapsamlı bir koruma öngörülmüştür. Sözleşme’nin 6. Maddesine göre; *ırksal kökeni, siyasi görüşleri, dinsel ya da diğer inançları açığa çıkaran kişisel veriler ile kişinin sağlığı ya da cinsel yaşamı ile ilgili olan verilerin ve cezai mahkûmiyetlere ilişkin veriler*, özel nitelikli veri olarak kabul edilmiş ve bu verilerin otomatik yollarla işlenmesini yasaklanmıştır¹⁹.

Avrupa Birliği’nin 95/46 sayılı Direktifinin “Özel Kategorideki Verilerin İşlenmesi” başlıklı 8. maddesinin 1. fıkrasında ise; *“Devletler ırksal veya etnik kökeni, politik düşünceleri, dini veya felsefi inançları, sendika üyeliklerini açığa çıkaran kişisel veriler ile sağlık veya cinsel yaşamla ilgili kişisel verilerin işlenmesini*

¹⁷ **Lloyd, Ian J.**, Information Technology Law, Fifth Edition, Oxford University Press, Oxford, 2008, s. 42 (Aktaran: **Kaya, Cemil**, “Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi”, İÜHFİM, C. LXIX, S. 1, 2011, s. 317)

¹⁸ **Carey Peter**, Data Protection: A Practical Guide to UK and EU Law, Third Edition, Oxford University Press, Oxford, 2009, s. 81 (Aktaran: Kaya, s. 318)

¹⁹ Ancak bu yasak mutlak değildir. İç hukukun yeterli güvenceyi sağlaması durumunda buna izin verilebileceği yine Sözleşmede belirtilmiştir. Bkz. **Atak, Songül**, “Avrupa Konseyinin Kişisel Veriler İçin Sağladığı Temel Güvenceler” TBB Dergisi, S. 87, 2010, s. 96

yasaklayacaktır.” şeklinde düzenlemeye yer verilmiştir. Direktife göre, kişilerin ırksal veya etnik kökenine, politik düşüncelerine, dini veya felsefi inançlarına, sendika üyeliklerine ilişkin veriler ile sağlık veya cinsel yaşamla ilgili verileri, özel katogorideki veriler, diğer bir ifadeyle hassas veri olarak kabul edilmiştir.

Görüldüğü üzere her iki metinde de, belli tür verilerin işlenmesiyle ilgili katı düzenlemelere gidilerek bu tür veriler için işlem yasağı getirilmiştir. Ancak bu yasak mutlak olarak öngörülmemiş, birtakım istisnalar getirilerek hassas verilerin hangi durumlarda işlenebilecekleri belirtilmiştir.

Hassas veriler, esas itibariyle birer kişisel veridirler. Ancak, söz konusu verilere kanun koyucunun bazı toplumsal ve siyasi kaygılar sonucu farklılık tanınmış ve daha sıkı korunması gerektiği belirtilmiştir. Bu bakımdan hassas veriler; daha çok, ırk ve etnik unsurlara, düşünce özgürlüğüne, cinsel yaşama ve geniş anlamda sağlık durumuna ilişkin verilerdir. Söz konusu verilerin işlenmeleri kural olarak yasaktır. Bu verilerin ortak paydası yüksek risk faktörü taşımalarıdır. Bu risk faktörü ise, ayrımcılık tehlikesidir. Öyle ki, üçüncü kişilerin öğrenmeleri halinde, bu veriler ilgili kişinin mağduriyetine sebep olabilirler. Son dönemlerde dünyada yaşanan ırkçılığın bir sonucu olarak belli bir gruba karşı olan kin ve nefretin sebep olacağı ayrımcılık tehlikesinin artması ihtimali bulunmaktadır. Zira politik görüşler, dini ve felsefi inanç gibi veriler kişinin eylemleri, eğilimleri ve alışkanlıkları hakkında bilgi edinilmesine imkân vermekte ve kişiler sırf farklı düşünceleri, farklı inanmaları veya farklı etnik kökenden gelmeleri nedeniyle ayrımcılığa uğrayarak kişilik hakları ağır bir şekilde ihlal edilebilmektedir (Özdemir, 2009: s. 126; Şimşek, 2008: s. 86).

Hassas verilere dolaylı olarak ulaşım imkânı veren veriler de, koruma altındadır. Meselâ siyasî partilerin yayınlarına abone olanların listesi de politik görüşler hakkında dolaylı bir erişim imkânı verdiği için AB Direktifi kapsamında korunmaktadır. Dolaylı hassas veri ayrımının sebebi ise, adı geçen verilerin net bir şekilde hassas olmayan verilerden ayrılamaması, bununla birlikte yüksek ve kapsamlı bir koruma sağlama ihtiyacıdır (Özdemir, 2009: s. 127).

Avrupa İnsan Hakları Mahkemesi de “S. ve Marper Birleşik Krallık” davasında, kişinin hücre örnekleri ve DNA profili gibi bazı veri gruplarının, kişinin etnik kökeni ve genetik bağlarını ortaya çıkarabilme imkânı vermesi nedeniyle,

parmak izi gibi diğer verilere göre daha kapsamlı korunması gerektiğine işaret etmiştir (Kaya, 2011: s. 323).

Naomi Campbell v MGN davasında ise AİHM, Bayan Campbell'in fotoğrafları onun ten rengini ortaya çıkarttığı için bunların hassas veri olarak nitelenip nitelenmeyeceğini değerlendirmiştir. Mahkeme, fotoğrafların Bayan Campbell'in ırksal kökeni ile ilgili bilgileri açıkladığına, ancak bu durumun fotoğrafların yayınlanma amacı karşısında önemsiz kaldığına, veri sahibinin, tanınmış siyah bir manken olmaktan gurur duyduğu ve siyah bir kadın olarak fotoğraflarının çekilmesinin onun yaşam tarzının ve mesleğinin bir parçası olduğu hallerde durumun değişeceğine ve bu olayda fotoğrafların hassas veri olarak kabul edilemeyeceğine karar vermiştir. Bununla birlikte aynı davada mahkeme Bayan Campbell'in the Narcotics Anonymous'de aldığı tedavinin niteliği ve detayları ile ilgili bilgileri, fiziksel ve zihinsel sağlık durumuyla ilgili bilgiler olarak görmüş ve bu nedenle de açıkca bu bilgileri hassas veri tanımı içinde mütalaa etmiştir (Kaya, 2011: s. 323).

1982 Anayasasında herkesin kişisel verilerinin korunmasının isteme hakkına sahip olduğu belirtilmesine rağmen kişisel verinin ne olduğu tanımlanmamış, ayrıca hassas kişisel verilerin özel olarak daha sıkı koşullarda korunması gerektiğine ilişkin bir düzenleme de yapılmamıştır²⁰.

Henüz kanunlaşamayan Kişisel Verilerin Korunması Kanunu Tasarısı'nın 7. maddesinin 1. fıkrasında(yeni Tasarı 6. madde) ise AB'nin 95/46 sayılı Direktifine paralel şekilde özel nitelikli veriler düzenlenmiştir²¹.

Hassas verilere, 5237 sayılı Türk Ceza Kanununun (TCK) 135. maddesinin ikinci fıkrasında şu şekilde yer verilmiştir:

“Kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimse, yukarıdaki fıkra hükmüne göre cezalandırılır”.

²⁰ Bkz. 1982 Anayasası m. 20/3.

²¹ **Özel nitelikli kişisel verilerin işlenme şartları-** “Madde 6 - (1) Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, dernek, vakıf ya da sendika üyeliği, sağlığı veya cinsel hayatıyla ilgili verileri, özel nitelikli kişisel veriler olup bunların işlenmesi yasaktır.”

TCK'nunda da yer verilmiş olan hassas veri kategorilerini, ileride kişisel verilere karşı işlenen suçların özellikle suç konusunun analizinde fayda sağlayacağından kısaca açıklamakta fayda vardır:

Siyasi Görüş: Kişilerin, devletin etkinliklerinin amaç, yöntem ve içerik açısından hangi esaslara göre düzenlenmesi ve gerçekleştirilmesi gerektiğine ilişkin kendi özel düşüncelerini ifade eder²².

Felsefi ve Dini Görüş: Dini görüş kişinin Tanrı'ya, doğaüstü güçlere, çeşitli kutsal varlıklara inanma ve tapınma istemidir²³. Felsefi görüş ise kişinin düşünce etkinliği sonucu ulaştığı tüm görüşler şeklinde tanımlanabilir. Diğer bir anlatımla felsefi görüşlere ilişkin kişisel veriler, kişinin yaşam biçimini ortaya çıkaran verilerdir. Bu nedenle mevzuatımız açısından bu kavramlar bir arada düşünülmelidir²⁴.

Felsefi ve dini görüş, hassas verileri tanımlayan ve TCK'ndaki düzenlemelere kaynaklık eden AK'nin 108 sayılı Sözleşmesinde “dini ya da diğer inanç”, AB'nin 95/46 sayılı Direktifinde ise “dini veya felsefi inanç” şeklinde ifade edilmiştir. Anayasamızın kanun önünde eşitliği düzenleyen 10. maddesinde de “felsefi inanç” kavramının kullanıldığı görülmektedir. Bu nedenle burada bahsedilen “felsefi görüş” kavramının, inanç niteliği taşıyan felsefi görüşleri kapsadığı savunulmuştur. Ateizm, deizm gibi, dinle bağlantılı ve inanç ya da inançsızlık niteliği taşıyan görüşler felsefi görüşe örnek olarak verilebilir (Akdağ, 2013: s. 23).

Nitekim Avrupa İnsan Hakları Mahkemesi de “Campbell ve Cosans – İngiltere” davasında verdiği kararın 36. paragrafında felsefi inancı, demokratik bir toplumda saygı görmeye değer olan ve insan onuru ile bağdaşmaz bir nitelik taşımayan fikirler olarak tanımlamıştır²⁵.

²² <http://tdkterim.gov.tr/bts/?kategori=verilst&kelime=politika&ayn=tam> . Erişim Tarihi: 18.04.2013; Benzer şekilde **Parlar, Ali/Hatipoğlu, Muzaffer**, Türk Ceza Kanunu Yorumu, 2. Baskı, C. 2, Seçkin Yayınevi, Ankara, 2008, s. 2044

²³ <http://tdkterim.gov.tr/bts/?kategori=verilst&kelime=din&ayn=tam> . Erişim Tarihi: 18.04.2013

²⁴ **Singleton, Susan**, Data Protection – The New Law, Jordans, Bristol 1998, s.10. (Aktaran: **Akdağ, Hale**, Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması, Adalet Yayınevi, Ankara, 2013, s. 23); Aynı yönde bkz. **Parlar/Hatipoğlu**, 2008, s. 2045;

²⁵ Mahkemenin 25.02.1982 tarihi ve B.n. 7611/76; 7743/76 sayılı Kararı. bkz. **Akdağ**, s. 23

Irki Köken: Kişilerin, kalıtsal olarak, ortak fiziksel ve fizyolojik özellikler taşıyan insan topluluklarından hangisine dâhil olduğu bilgisidir²⁶. Bu veri kategorisi etnik kökeni de kapsamaktadır (Akdağ, 2013: s. 33).

Ahlaki Eğilim: Kişilerin toplum içinde yaşamaları dolayısıyla uymaları gereken kurallara yaklaşımları olarak tanımlanabilir²⁷. Bu veri kategorisine uluslararası mevzuatta hassas veri olarak yer verilmemiştir. Bu yaklaşım bizim mevzuatımıza özgüdür²⁸. Kişinin ahlaki eğiliminden kastın, TCK'nun “Genel Ahlaka Karşı Suçlar” bölümünde yer alan suçlar da göz önüne alınarak, toplumun genelince hoş görülme ve özellikle cinsellikle bağlantılı davranışlara ilişkin eğilim olduğu doktrinde ifade edilmiştir (Akdağ, 2013: s. 33).

Cinsel Yaşam: Kişinin cinsel eğilimlerini ve seks hayatını kapsayan bir kavramdır. Özellikle toplumun geneli tarafından normalin dışında kabul edilen eşcinsellik, biseksüellik, sadizm, mazoşizm gibi eğilimlere sahip bireyler açısından, bu tür bilgiler gerçekten ayrımcılığa maruz kalınma riski yaratan ve hassas bir nitelik taşır (Akdağ, 2013: s. 34).

Sağlık Durumu: Kişinin sağlığı ile ilgili sadece mevcut durumu değil, sağlık geçmişiyse de ilgili her türlü bilgiyi kapsayan, çok geniş bir kategoridir²⁹. Kişinin

²⁶ **Türk Dil Kurumu Türkçe Sözlük**, Türk Dil Kurumu Yayınları, Ankara 2009, s. 913; **Parlar/Hatipoğlu**, 2008, s. 2045

²⁷ **Türk Dil Kurumu Türkçe Sözlük**, Türk Dil Kurumu Yayınları, Ankara 2009, s. 43

²⁸ **Küzeci**, s. 373

²⁹ **Akdağ**, s. 34; Bu kategori o kadar geniş bir alanı kapsamaktadır ki, bir kişinin bir meslektaşının ayağını incittigine ve bu nedenle de kısmi statüde çalıştığına ilişkin bilgiyi internet sitesine koyması durumunda bile bu bilgi hassas nitelikte kabul edimiştir. Avrupa Toplulukları Adalet Divanı'nın (European Court of Justice – ECJ) (ATAD) Bodil Lindqvist kararı buna örnektir. Bodil Lindqvist davasında İsveç Mahkemeleri tarafından sorulan bazı sorulara karşılık ATAD'dan “ön karar” (preliminary ruling) vermesi istenmiştir. Bu davaya konu olayda Bayan Lindqvist, kendi internet sitesinde meslektaşları hakkında kişisel bilgileri yayımladığı gerekçesiyle İsveç Veri Koruma Kanunu'nu ihlal etmekle suçlanmıştır. Bayan Lindqvist, meslektaşlarının ad ve soyadlarını ya da sadece adlarını kendi internet sitesine koymuştur. Ayrıca Bayan Lindqvist, meslektaşlarının yaptıkları işleri, onların hobilerini, aile durumlarını, telefon numaralarını da bu siteye koymuştur. Aynı zamanda bir meslektaşının ayağını incittiğini ve bu nedenle de kısmi statüde çalıştığına ilişkin bilgiye de sitesinde yer vermiştir. İsveç Makamları, diğerleriyle birlikte, Bayan Lindqvist'i, meslektaşları ile ilgili hassas verileri onların muvafakatını almadan ve İsveç Ulusal Veri Koruma Otoritesinden izin almadan işlemekle suçlamıştır. ATAD'ın kararında: “Direktifin amaçları ışıığında, 8. maddenin 1. fıkrasında kullanılan sağlıkla ilgili veri ifadesi, bir kişinin fiziksel ve zihinsel sağlığının bütün yönleriyle ilgili bilgileri kapsayacak şekilde geniş yorumlanmalıdır”. Görüldüğü üzere ATAD, Bayan Lindqvist'in ismi belli bir meslektaşının ayağını incittigine ve bu nedenle de kısmi statüde çalıştığına

gerek kamu gerek özel sađlık kuruluřlarınca tutulan tedavi bilgileri, hangi ilaları kullandıđına iliřkin kayıtlar bu kapsamda deđerlendirilebilir.

Sendikal Bađlantı: Kiřilerin, iři veya iřverenlerin iř, kazanç, toplumsal ve kltrel konular bakımından ıkarlarını korumak ve daha da geliřtirmek iin kendi aralarında kurdukları birliklerden hangisine ye olduđunu veya hangisi ile beraber alıřtıđını gsterir bilgidir (Trke Szlk, 2009, s. 1729).

Hassas veri/Hassas olmayan veri kategorilerinin yaratılması, bunların sınırlı řekilde sayılması ve bu ayrımın toplumdan topluma deđiřebileceđi gerekleriyle eleřtirilmiřtir³⁰.

Kanaatimizce bazı veri kategorilerinin, diđerlerine kıyasen daha sıkı korunmaları gerektiđi dřncesiyle ayrıca dzenlenmesi ve ulusal ve uluslararası mevzuatta bu tr verilerin iřlenebilecekleri durumların daha sınırlı řekilde belirlenmesinin temel hak ve zgrlklerin korunması zellikle de ayrımcılıđın nne geilebilmesi aısından faydalı olmuřtur.

3. KİřİSEL VERİLERİN İřLENMESİ

Kiřisel verilerin iřlenmesi kavramı nitelik olarak geniř bir ieriđe sahiptir. Bu konuda Anayasamızda ve Trk Ceza Kanunu'nda bir tanım yapılmamıř ise de, AK'nin 108 sayılı Szleřmesinde, AB'nin 95/46 sayılı Direktifinde, Kiřisel Verilerin Korunması Kanunu Tasarısında ve Elektronik Haberleřme Sektrnde Kiřisel Verilerin Korunması Ynetmeliđinde tanım yapılmıřtır.

AK'nin 108 sayılı Szleřmesinin 2. maddesinin (c) bendinde kiřisel verilerin iřlenmesi "otomatik iřleme" olarak adlandırılmıř ve "Kısmen ya da tamamen otomatik yollarla gerekleřtirilen veri kaydını, bu verilere mantıksal ve/veya aritmetik iřlemlerin uygulanması, bu verilerin deđiřtirilmesi, silinmesi, dzeltilmesi ya da aıklanması" řeklinde ifade edilmiřtir (Atak, 2010: s. 95; řimřek, 2008: s. 22).

AB'nin 95/46 sayılı Direktifinin 2. Maddesinin (b) bendinde kiřisel verilerin iřlenmesi, otomatik bir sre yardımıyla olsun veya olmasın toplama, kaydetme,

iliskin bilgileri internet sitesine koymasını Veri Koruma Direktifinin 8. maddesinin 1. fıkrası kapsamında saymıřtır. Bkz. **Kaya**, "Hassas Veriler", 2013, s. 322

³⁰ Eleřtiriler iin bkz. **Kzeci**, s. 373

organizasyon, muhafaza etme, intibak etme, deęiřtirme, ayıklama, soruřturma, yayma, kombinasyon veya baęlantılandırma, engelleme, silme veya imha etme gibi kiřisel verilerle baęlantılı bütn iřlem veya iřlem izinlerini ifade ettięi belirtilmiřtir (řimřek, 2008: s. 44).

Kiřisel Verilerin Korunması Kanunu Tasarısının 3. maddesinde kiřisel verilerin iřlenmesi; kiřisel verilerin otomatik olan veya olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, deęiřtirilmesi, silinmesi veya yok edilmesi, yeniden dzenlenmesi, aıklanması veya bařka bir řekilde elde edilebilir hale getirilmesi, nc kiřilere aktarılması, kullanılmasının sınırlanması amacıyla iřaretlenmesi veya tasniflenmesi veya kullanılmasının engellenmesi gibi bu veriler zerinde gerekleřtirilen bir iřlem ya da iřlemler btn řeklinde tanımlanmıřtır.

24.07.2012 tarihli ve 28363 sayılı Resmi Gazetede yayımlanarak yrrlęe giren Elektronik Haberleřme Sektrnde Kiřisel Verilerin İřlenmesi ve Gizlilięinin Korunması Hakkında Ynetmelięin 3. Maddesinin birinci fıkrasının (i) bendinde de Tasarıdaki tanımın benzeri bir tanım yapılmıřtır.

AB'nin 95/46 sayılı Direktifinde verilerin otomatik olan veya olmayan yollarla iřlenmesi arasında fark grlmezken, AK'nin 108 sayılı Szleřmesinde verilerin iřlenmesinin sadece otomatik yollarla iřlenmeye hasredilmesi eleřtirilmiřtir. Zira gnmzde veri iřleme sadece otomatik veya elektronik yollarla yapılmamakta, fiziki olarak kâğıt ve benzeri řeyler zerine yazılarak ta yapılabilmektedir³¹.

O halde yukarıdaki tanımlar nazara alınarak, kiřisel verilerin iřlenmesini; kiřisel verilerin otomatik olan veya olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, deęiřtirilmesi, silinmesi veya yok edilmesi, yeniden dzenlenmesi, aıklanması veya bařka bir řekilde elde edilebilir hale getirilmesi, nc kiřilere aktarılması, kullanılmasının sınırlanması amacıyla iřaretlenmesi veya tasniflenmesi veya kullanılmasının engellenmesi gibi bu veriler zerinde gerekleřtirilen her trl iřlem veya iřlemler btn olarak tanımlayabiliriz.

Grldę zere kiřisel verilerin iřlenmesi, verilerin elde edilmesinden silinmesine kadar geen srete veriler zerinde yapılan her trl iřlemi

³¹ Eleřtiri iin bkz. **Atak**, 2010: s. 95

kapsamaktadır (Kaya, 2011: s. 317). İşleme içerisinde sayılan elde etme, kaydetme, depolama, değiştirme ve silme gibi işlemler, bu süreçte birbirini takip eden ayrı safhalardır. Ancak verilerin işlenmesi için hepsinin gerçekleşmesine gerek yoktur. Bunlardan birinin yapılması, örneğin verinin kaydedilmesi, tek başına bir veri işleme sayılmaktadır.

Diğer yandan tanımdan da anlaşılacağı üzere, bu işlemler sınırlı şekilde sayılmamıştır. Tanımda sayılan eylemlere benzer şekilde veriler üzerinde yapılan her türlü işlemlerde kişisel verilerin işlenmesi sayılacaktır.

Burada önem arz ettiği için TCK'da ki düzenlemeleri de belirtmekte yarar vardır. Zira TCK'da kişisel verilerin işlenmesi diye bir suç tanımı yapılmamış, “kişisel verilerin hukuka aykırı olarak kaydedilmesi, ele geçirilmesi, verilmesi, yayılması ve yok edilmemesi” eylemleri suç olarak 135, 136 ve 138. maddelerde sayılmıştır. Kanunilik ilkesi gereği TCK'nunda bu eylemlerden başka bir işleme fiili suç olarak sayılamayacaktır³². Bu konu üçüncü bölümde ayrıntılı olarak inceleneceğinden burada bu kadar açıklama ile yetinilmiştir.

Yine kişisel verilerin işlenmesi eyleminin otomatik olan veya olmayan yani manuel yollarla yapılması arasında bir fark yoktur. Veriler ister bilgisayar ve benzeri cihazlarda kaydedilsin ister kâğıt, dosya ve benzeri fiziki evraklara kaydedilsin, burada depolansın, her iki yöntem de veri işleme sayılacak ve veri koruma hukuku kurallarına tabi olacaktır. Nitekim AB'nin 95/46 sayılı Direktifi dolayısıyla AB uygulaması da bu yöndedir. Türk Ceza Kanunun 135. maddesinde de kişisel verilerin hukuka aykırı olarak kaydedilmesi suçu açısından verilerin bilgisayar ortamında veya kâğıt üzerinde kayda alınması arasında bir ayırım gözetilmemiştir³³.

Ayrıca, ülkemizde kişisel verilerin korunması gündeme geldiğinde, genellikle sadece kişisel verilerin kaydedilmesi fiili ele alınmakta, veri koruma hukukunun sadece kişisel verilerin hukuka aykırı olarak kaydedilmesini engellemeye çalıştığı şeklinde bir algı bulunmaktadır. Fakat hem Avrupa Birliği Direktifinde hem de

³² Kanunilik ilkesi için bkz. **Artuk, M. Emin/Gökçen, Ahmet/Yenidünya, A. Caner**, Türk Ceza Hukuku Genel Hükümler, 7. Baskı, Adalet Yayınevi, Ankara, 2013, s. 98-100; **Özgenç, İzzet**, Türk Ceza Hukuku Genel Hükümler, 7. Bası, Seçkin Yayınevi, Ankara, 2012, s. 103-106

³³ Bkz. TCK 135 madde gerekçesi.

Avrupa Konseyi'nin 108 sayılı Sözleşmesinde kişisel verilerin “işlenmesi” fiiline atıf yapılmakta ve bu tanım içerisinde kişisel verilerin elde edilmesi ve kaydedilmesinden başlayarak bu verilerin yabancı ülkelere transferine kadar birçok işlem dâhil edilmektedir. Başka bir ifadeyle veri koruma hukuku ile amaçlanan sadece kişisel verilerin hukuka aykırı olarak kaydedilmesini önlemek değil, aynı zamanda bu veriler üzerinde gerçekleştirilen tüm işlemlerin hukuka uygun olmasını temin etmektir (Uygun, 2010: s. 48).

Konuya bu açıdan bakıldığında, kişisel verilerin işlenmesi fiiline birçok örnek vermek mümkündür. Kişinin sağlık durumuna ilişkin bilgilerin sağlık dosyalarına kaydedilmesi, bir kişinin nüfus ve adres bilgilerinin kişinin kendisinden veya başka bir kaynaktan elde edilmesi, bir otomatik sisteme veya fiziki bir dosyaya elle kaydedilmesi, bu bilgilerin saklanması veya başkalarına aktarılması, kişinin fotoğraf veya parmak izinin elde edilmesi ve saklanması, sesinin veya görüntüsünün kaydedilmesi veya bu kayıtların başkalarına aktarılması veya yayınlanması, kişinin telefon numarasının, e posta adresinin veya IP adresinin elde edilmesi, bunların başkalarına verilmesi veya doğrudan pazarlama amacıyla kullanılması, kişinin kredibilitesini gösteren banka hesaplarına ilişkin bilgilerin incelenmesi, üzerinde çalışılması, başka kurumlara aktarılması veya yeni hizmet sunumu için kullanılması gibi fiiller sayısız veri işleme faaliyetlerinden sadece birkaçıdır³⁴.

4. KİŞİSEL VERİLERİN KORUNMASI

4.1. Kişisel Verilerin Korunmasındaki Amaç

Günümüzde, bilgi, güç ile eş değer tutulmakta, bu nedenle de kişisel veriler, hem kamu, hem de özel sektör tarafından toplanmakta ve çeşitli şekillerde kullanılmaktadır. Devletler, vatandaşlarının hak ve özgürlüklerini güvence altına almak amacıyla, kamu güvenliğini sağlamak ve sosyal düzeni korumak zorundadır. Bu nedenle, kamu kurumları, daha sağlıklı kamu hizmeti sunmak, suçlularla mücadele etmek ve vergi toplamak gibi amaçlarla, bireyler hakkında çeşitli bilgiler

³⁴ ATAD, Lindqvist Davasında; Yönergenin 2(b) maddesiyle verilerin işlenmesinin; verilerin toplanması, kaydedilmesi, yayılması gibi veriler üzerinde yapılan her türlü işlem olarak tarif edildiğini bu nedenle, verilerin bir web sayfasına yüklenmesinin de bu tür bir işleme fiili olarak kabul edilmesi gerektiğini ileri sürmüştür. ATAD'a göre; verilerin isteyen herkesin ulaşabileceği bir şekilde bir web sayfasına yerleştirilmesi, en azından kısmen otomatik yollarla işleme sayılmalıdır. Bkz. Uygun, 2010: s. 48

toplamaktadırlar. Benzer şekilde özel hukuk tüzel kişileride, hedef kitleleri olan tüketicilerden toplayabildikleri her türlü bilgiyi depolama eğilimi göstermektedirler. Toplanan bilgilerin, yalnızca tüketicilerin kimlik bilgileri ile pazarlanan ürün hakkındaki görüşlerinden ibaret olmayıp, aynı zamanda, tüketicinin yaşam biçimi ve hatta psikolojik özellikleri dâhil olmak üzere bizzat kendisine ilişkin çeşitli bilgileri de içerdiği görülmektedir. Nitekim bu tür bilgileri toplayan teşebbüsler sundukları hizmetin kalitesini arttırmak ve iç pazarlama stratejilerini geliştirmenin yanında bu bilgileri üçüncü kişilere devrederek ayrıca ticari kazanç da sağlamaktadırlar (Arslan, 2011: s. 32; Aksoy, 2010: s. 75-76).

Daha önce de değinildiği gibi, kişilerin de daha hızlı ve ucuz mal ve hizmet satın alabilmek amacıyla kişisel verilerini kendi rızalarıyla paylaşmaları durumu da kurum ve kuruluşların veri işleme eğilimini artırmaktadır.

Diğer yandan özellikle bilgisayar ve internete yönelik teknolojiadaki gelişmeler nedeniyle, gerek kamu kurumları gerekse özel sektör tarafından toplanan kişisel veriler, bilişim sistemleri üzerinde depolanmaya başlamış, bu durum, verilerin hukuka aykırı olarak paylaşılması, ifşa olması gibi riskleri de beraberinde getirmiştir.

İşte kişisel verilerin önemi ve bu bilgilerin yoğun bir şekilde işlenmesi eğilimi karşısında, ortaya çıkan veri koruma hukukunun amacı, bireyin temel kişilik haklarının korunması ile verilerin serbest dolaşımı arasındaki dengenin sağlanmasıdır (Aksoy, 2010: s. 75; Arslan, 2011: s. 32).

Bu amaç, aşağıda kişisel verilerin korunmasının tarihsel gelişimi altında neden sonuç ilişkisi içerisinde izah edildiğinde daha net anlaşılacaktır.

4.2. Kişisel Verilerin Korunmasının Tarihsel Gelişimi

Kişisel verilerin korunmasına ve üçüncü kişilerle paylaşılmamasına yönelik bazı ilkelerin ilk zamanlarda özellikle sır saklama yükümlüğüne tabi doktor, avukat, din adamı gibi bazı meslek sahiplerine yönelik olduğu bilinmektedir (Şimşek, 2008: s. 6).

Günümüzde anladığımız şekliyle kişisel verilerin korunması, yeni bir alan olarak karşımıza çıkmasına rağmen kısa sürede hızla yayıldığı ve geliştiği görülmüştür (Küzeci, 2010: s. 105).

1950'li ve 1960'lı yıllar bilgisayarların ortaya çıktığı, hızla geliştiği ve yaygınlaşmaya başladığı bir dönem olmuştur. Bu dönemde çeşitli devlet organları ve işletmeler ellerindeki bilgileri merkezi bir veri tabanında birleştirmeye yönelik ciddi hazırlıklar yapmışlardır. İşte veri korumaya ilişkin ilk düzenlemelerin ortaya çıkışında, bu düşünceye karşı oluşan tepki etkili olmuştur. Verilerin insan eliyle işlenmesinden otomatik işlemeye geçişin yeni ve ciddi riskler ortaya çıkaracağı düşünülmüştür. Devletin, çeşitli kaynaklardan elde ettiği bilgileri ilişkilendirerek bireylerin karşısında aşırı güçlenmesi tehlikesi fark edilmiş ve kanun yapanların, yeni teknolojilerin getirdiği bu olanakların kullanımını denetlenebilir ve şeffaf kılmaya özel bir dikkat göstermeleri gerektiği düşüncesi ön plana çıkmaya başlamıştır³⁵.

Bu düşüncelerden hareketle 1970'li yıllarda, kişisel verilerle ilgili kişisel mahremiyet hukuku veya kişisel verilerin korunması hukuku olarak adlandırılan ayrı bir hukuk alanı ortaya çıkmış ve daha sonra Avrupa kıtasında gündeme gelmeye başlamış ve hukuki düzenlemelerin konusu olmuştur (Tanrıkulu, 2007: s. 46).

Özellikle o yıllarda teknolojinin hızla ilerlemeye başlaması, kitle iletişim araçlarının yaygınlaşması ve yaygınlaşan bu araçlar sayesinde kişilerle ilgili bilgilerin paylaşılmaya başlanması ve erişiminin çok kolaylaşması, bu verilerin hukuka aykırı olarak yetkisiz ve çoğu zaman kötü niyetli kişilerin eline geçmesine neden olmaya başlamıştır. Kişisel verilerin üzerindeki hâkimiyet konusunda o kadar çok hassasiyet ve korku ortaya çıkmıştır ki, bu korku romanlara konu olmuştur. Nitekim George Orwell'in 1949 yılında yayınlanan "1984" isimli romanında³⁶ gelişen bilgi teknolojileri sayesinde Büyük Abi'nin (Big Brother'ın) herkesi gözetlediği ve kişiler hakkında her türlü bilgileri toplayarak bu kişiler üzerinde hâkimiyet kurduğu teması işlenmiş ve özel hayatın gizliliği gibi temel hakların ihlali karşısında toplumu bilinçlendirme yolunda yayınlar yapılmaya başlanmıştır (Başalp, 2004: s. 21; Tanrıkulu, 2007: s. 46).

Bu endişeye paralel olarak kişisel verilerin korunması bağlamında gerek teknik, gerekse hukuksal gelişmeler yaşanmıştır.

³⁵ **Jori, Andreas**, "dataprotection.eu", <http://www.dataprotection.eu/>. Erişim T: 25.07.2012 (Aktaran, Küzeci, s. 106)

³⁶ **Orwell, George**, Bin Dokuz Yüz Seksen Dört, 34. Baskı, Çeviri: Celal Üster, Can Yayınları, 2011

Kişisel verilerin korunmasına ilişkin ilk yasal düzenleme, 1970 yılında Almanya'nın Hessen eyaletinde yapılmıştır. Bu yasanın kabulüne neden olan en önemli dinamiğin, "*Hessen Planı*" olarak adlandırılan bir program içerisinde 1960'lı yılların sonunda, özel yaşamın gizliliği hakkı üzerindeki olası olumsuz sonuçlar doğurabilecek olan federe düzeyde merkezi bir veri bankasının kurulmasına ilişkin kanun tasarısı olduğu söylenmiştir³⁷.

Hessen eyaletinin verilerin korunmasına ilişkin yaptığı düzenleme ve sonrasında konuyla ilgili ortaya çıkan tartışmalar, Almanya'da federal düzeyde bir koruma öngörülmesini de sağlamıştır. Bu doğrultuda 1977 yılında Federal Almanya Veri Koruma Kanunu kabul edilmiştir. Ancak bu Kanun, kişisel verilerin korunması görevini, aynı zamanda milli istihbarat ve polis teşkilatından da sorumlu olan İçişleri Bakanlığına bırakması nedeniyle oldukça eleştirilmiştir (Küzeci, 2010: s. 108).

Kişisel verilerin korunmasına ilişkin Almanya'nın Hessen eyaletinde kabul edilen yasanın ardından, 1973 yılında İsveç'te verilerin korunmasına ilişkin kanun çıkarılmıştır. Bu dönemde hızla ilerleyen teknolojinin bir parçası olan otomatik veri işleme sistemlerinin, özellikle Batı Avrupa'da yaygınlaşması ve bu sistemin beraberinde getirdiği riskler, Almanya'dakine benzer şekilde İsveç'te veri koruması yasasının kabul edilmesine neden olmuştur (Küzeci, 2010: s. 108; Civelek, 2011: s. 10).

Aynı dönemde, kişisel verilerin korunması, başka Avrupa ülkelerinde de tartışma konusu olmuş; Hessen ve İsveç veri koruma yasalarından kısa bir süre sonra, kişisel verilerin korunmasına ilişkin yasal düzenlemeler Avrupa'da pek çok ülkede kabul edilmiştir. 1980 yılına gelindiğinde İrlanda, İtalya ve İngiltere dışında, Avrupa Ekonomik Topluluğu'nun bütün üyelerinin ya bu konuda düzenleme yaptıkları, ya da ciddi hazırlıklar içinde bulundukları görülmüştür (Küzeci, 2010: s. 108).

Ancak 1970'li yıllarda yalnızca Avrupa'da değil, ABD'de de kişisel verilerin korunması yönünde bazı girişimlerde bulunmuştur. Bu tarihlerden itibaren

³⁷ **Kuner, Christopher**, European Data Protection Law: Corporate Compliance and Regulation, Oxford University Press, Second Edition, 2007, s. 13 (Aktaran: **Civelek, Dilek Yüksel**, Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi (Uzmanlık Tezi), Bilgi Toplumu Dairesi Başkanlığı Yayınları, Nisan 2011, s. 9; **Küzeci**, s. 107)

Amerika'da kişisel mahremiyet konusunda artan bir hassasiyet ortaya çıkmaya başlamış ve 1974 yılında kabul edilen Özel Yaşamın Gizliliği Yasası (Privacy Act) ile kişilerin yalnız kalma hakları olduğu ve bu haklarından dolayı kişilerin özel hayatının hukuk düzenince daha sıkı bir şekilde korunması gerektiği kabul edilmiştir (Tanrıkulu, 2007: s. 46).

Avrupa Birliği konuya temel haklar boyutuyla yaklaşırken Amerika Birleşik Devletlerinin konuya ticari açıdan yaklaştığı görülmüştür. Bu kapsamda, Özel Yaşamın Gizliliği Yasasının uygulama alanını kısıtlayan ekonomi ve ticaret hayatında verilerin paylaşımına yönelik konularda çıkarılan kanunlar nedeniyle, Amerika'da kurumsallaşmış bir veri koruma düşüncesi uygulamaya geçememiştir (Küzeci, 2010: s. 109).

Kişisel verilerin korunmasına yönelik olarak kabul edilen ilk yasalarda öngörülemeyen önemli bir gelişimde, bilgisayarların yaygınlaşmasıyla kamu ve özel sektörde pek çok veri bankasının kurulmuş olmasıdır. Bunun sonucunda bireyin kendisiyle ilgili bilgilerin toplanması ve işlenmesinin yaratacağı tehlikeleri açıkça ve doğrudan hissetmesi, yalnızca belirli bir veri işleme sürecinin düzenleme kapsamına alınmasının ötesinde verilerinin korunmasının talep edilmesine neden olmuştur. Bu talep, kişisel verilerin korunmasında yeni bir dönemin de habercisi olmuş ve konu özel yaşamın gizliliği ve geniş olarak insan hakları ekseninde tartışılmaya başlanmıştır. Ayrıca kişisel verilerin korunmasının vatandaşların hakları arasındaki yeri de belirginleşmeye başlamıştır. Nitekim Portekiz, İspanya, Avusturya gibi ülkelerde kişisel verilerin korunması bu dönemde anayasal bir hak olarak tanınmıştır (Küzeci, 2010: s. 110-111).

2 Nisan 1976 tarihli Portekiz Anayasasının 35. maddesinde, her vatandaşın kendisiyle ilgili tutulan verilerine erişme, düzeltilmesini ve güncellenmesini isteme ve hangi amaçla toplandığı konusunda bilgilendirilme hakkının olduğu, kişisel verilerin bağımsız bir idari kuruluş vasıtasıyla korunması gerektiği hüküm altına alınmıştır (Avrupa Birliği Üyesi Bazı Ülkelerin Anayasaları, 2011: s. 455).

Benzer şekilde 31 Ekim 1978 tarihli İspanya Anayasası'nın 18. maddesinin dördüncü fıkrasında, yurttaşların onuru, kişisel ve ailevi mahremiyetleri ile haklarını tam anlamıyla kullanımlarını güvence altına almak için kişisel verilerin işlenmesi yasa

ile sınırlanacağı belirtilmiştir (Avrupa Birliği Üyesi Bazı Ülkelerin Anayasaları, 2011: s. 542).

Kişisel verilerin korunmasının anayasal düzeyde tanınması olgusunun yalnızca bu ülkelerde değil Avusturya, Macaristan ve İsveç gibi demokratik ülkelerde de görülmüştür. Bu husus, kişisel verilerin korunmasına anayasal düzeyde yer verilmesinin yanında, kaynağını özel yaşamın gizliliğinde bulduğu genel olarak ifade edilen kişisel verilerin korunmasının artık bağımsız bir hak olarak yükselmeye başladığının da işareti olarak yorumlanmıştır³⁸.

Bunda 1983 yılında Alman Anayasa Mahkemesi'nin “Nüfus Sayımı Kararı”ndaki saptamaları da etkili olmuştur. Mahkeme kararında, kamu idarelerine karşı kişilerin kişisel verilerini koruma haklarına sahip olmaları konusunda önemli ilkeler ortaya koymuştur. Bu kararı önemli kılan da kişilerin verileri bakımından kendi geleceklerini belirleme haklarına sahip olduklarının açıkça belirtilmesi ve Alman Anayasasının 2. maddesinde belirtilen bu hususun dayanak yapılarak Avrupa Hukukunda ilk kez kişisel verilerin korunması hukukunda idareye karşı birtakım kuralların ortaya konması ve kişinin devlete karşı korunması olmuştur. Bu karara göre idare gereksiz şekilde belki ilerde lazım olabilir diye verileri toplayamayacak, ancak gerekli ve yeteri kadar veri toplayabilecektir (Küzeci, 2010: s. 112).

Alman Anayasa Mahkemesi'nin bu kararından sonra kişisel verilerin korunması, bireyin veri işleme sürecinde söz sahibi olduğu “bilgilerin geleceğini belirleme hakkı” olarak anılmaya başlanmıştır (Aksoy, 2008: s. 241-242).

Kişisel Verilerin Korunması Hukukunun ortaya çıkıp hızla gelişmesinin diğer bir sebebi de özellikle Batı kültüründe bireyin toplum karşısındaki öne çıkışı ve ferdiyetçiliğin giderek etkisini arttırmasıdır (Tanrıku, 2007: s. 46).

Bu etki, kişisel verilerin korunmasının uluslararası alanda da çözüm aranan bir konu haline gelmesine neden olmuştur. Bu düşünceden hareketle Birleşmiş Milletler, Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD), Avrupa Konseyi ve Avrupa Birliği gibi etkili uluslararası kuruluşlar kişisel verilerin korunmasına ve

³⁸ **Early, Lawrence**, “Science, Technology and Human Rights: The Role of Data Protection”, Human Rights in the Twenty first Century, A Global Challenge, C. 2, haz. Katleen E. Mahoney, Paul Mahoney, Maritus Nijhoff Publishers, Hollanda, 1993, s.801-815. (Aktaran: Küzeci, s. 111)

özellikle kişisel verilerin uluslararası aktarımına ilişkin kurallar belirleme düşüncelerini ard arda yaşama geçirmişlerdir. Bu bağlamda kişisel verilerin korunması, artık ulusal sınırları aşmış ve etki düzeyleri birbirinden farklı çeşitli uluslararası metinlerin konusu olmaya başlamıştır.

Bu kapsamda, ilerde ikinci bölümde ayrıntılı olarak açıklanacağı üzere, 1980 yılında Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD) tarafından kabul edilen ve bağlayıcı olmayan kişisel verilerin korunmasına ilişkin rehber ilkeleri de burada zikretmek gerekir³⁹.

Aynı şekilde Avrupa Konseyinin “Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair 28 Ocak 1981 tarihli 108 nolu Sözleşme”si ile üye devletlerin hâkimiyet alanında kişisel alanın korunması hedeflenerek, kişisel verilerle ilgili yeknesak bir hukuk düzeni ortaya konulmaya çalışılmıştır (Tansuğ, 2005: s. 55).

AİHS’nin yorumlamak ve uygulamakla görevli Avrupa İnsan Hakları Mahkemesi de bu temelden hareketle çeşitli davalarda kişisel verilerle ilgili kararlar vererek kişisel verilerin korunması ve verilerin gizliliği gibi ilkeleri kabul ederek bu konuda, uyulama yönüyle, öncülük etmiştir⁴⁰.

1990’lı yıllarda ise kişisel verilerin korunması konusunda Avrupa Birliği’nde ilk tasarılar ortaya çıkmaya başlamış ve uzun çalışmalar sonunda 24 Ekim 1995 tarihinde Avrupa Parlamentosu ve Konseyi 95/48/EC sayılı “Kişisel Verilerin İşlenmesinde Gerçek Kişilerin Korunması Direktifi”ni kabul etmiştir. Kabul edilen bu Direktif, 1998 yılında yürürlüğe girebilmiştir (Tansuğ, 2005: s. 55).

Bu düzenlemelerle birlikte de kişisel verilerin korunması hakkı, artık özel hayatın gizliliği hakkının çatısı altında kalmaktan çıkarak birbirlerinden ayrılmaları sağlanmıştır (Tanrıkulu, 2007: s. 47).

³⁹ Rehber ilkeler hakkında ayrıntılı bilgi için bkz. **Özdemir**, 2009: s. 19

⁴⁰ AİHM’in kişisel veriler ile ilgili ilk kararı Leander-İsveç kararıdır. Kararda, kişiye ait verilerin toplanması ve iletilmesinin AİHS’nin 8. Maddesinin bir ve ikinci fıkrası kapsamında kişisel hayatı ihlal ettiği belirtilmiştir. Bkz. **Özdemir**, 2009: s. 26

Bu Direktifi desteklemek maksadıyla eksik kalan alanlarda Avrupa Parlamentosu ve Konseyi 1997 yılında “Telekomünikasyon Alanında Kişisel Verilerin İşlenmesi ve Mahremiyetin Korunması Direktifi” yürürlüğe koymuştur. Bu Direktif, 97/66/EG nolu Yönerge ismini almıştır. Daha sonra AB, bu Yönergeyi tamamlayan 2002/58/EC Sayılı "Özel Hayatın Korunması ve Elektronik İletişim Yönergesi"ni de ileri teknolojik ortamlardaki ilişkileri de kapsayan yeni bir veri saklama hukuku olarak ortaya koymuştur. Bu yönerge 2006/24/AB sayılı ve 15 Mart 2006 tarihli Direktif ile yenilenmiştir (Tansuğ, 2005: s. 55).

AB tarafından çıkarılan bu direktiflerin Türkiye’de Kişisel Verilerin Korunması Kanun Tasarısının oluşumunda önemli etkileri olmuştur.

2001 yılında ise yine Avrupa Birliği’nde kişisel verilerin korunması hakkı temel bir hak olarak Temel Haklar ve Hürriyetler Şartının 8. maddesinde yerini almıştır. 7 Aralık 2000 tarihinde Fransa’nın Nice kentinde imzalanan AB Temel Haklar Şartı, AB’nin tarihinde ilk kez Avrupa vatandaşlarının ve AB’de yaşayan bütün insanların bireysel, siyasal ve ekonomik haklarını tek bir metinde toplaması yönüyle önemlidir. AB Temel Haklar Şartının konumuz açısından diğer bir önemli hatta en önemli yönü, kişisel verilerin korunması hakkının ayrı bir hüküm altında düzenlemiş olmasıdır⁴¹.

4.3. Kişisel Verilerin Korunması Hakkının Hukuki Niteliği

4.3.1. Genel Olarak

2010 yılına kadar kişisel verilerin korunması hakkı Anayasalarımızda temel bir hak olarak yer almamıştır. 12 Eylül 2010 tarihinde yapılan halkoylaması ile yürürlüğe giren 5982 sayılı Kanunla Anayasanın özel hayatın gizliliği hakkını düzenleyen 20. maddesine bir fıkra eklenerek kişisel verilerin korunmasını isteme hakkı temel bir hak olarak Anayasada yerini almıştır.

⁴¹ AB Temel Haklar Şartı’nın "Kişisel verilerin korunması" kenar başlıklı 8. maddesi şöyledir: “Herkes, kendisini ilgilendiren kişisel verilerin korunması hakkına sahiptir.

Bu veriler, dürüst bir şekilde, belirli amaçlar için ve ilgili kişinin rızasına veya yasa ile öngörölmüş diğer meşru bir temele dayanılarak işlenir. Herkes kendisi hakkında toplanmış verilere erişme ve bunları düzelttirme hakkına sahiptir.

Bu kurallara uyulması bağımsız bir makam tarafından denetlenir”. Bkz. **Küzeci**, s. 158

Bu zamana kadar ise doktrinde, kişisel verilerin korunması hakkı Anayasada düzenlenen diğer temel hak ve özgürlükler içerisinde veya onlarla bağlantılı şekilde açıklanmaya çalışılmıştır. Ağırlıklı olarak, bireyin kişisel verilerinin hukuksal temellerini, kişinin maddi ve manevi varlığını koruma ve geliştirme hakkı yani kişiliğin serbest geliştirilmesi hakkı ve insan onuru ilkesini düzenleyen Anayasanın 17. maddesinden aldığı ifade edilmiştir (Şimşek, 2008: s. 111; Özdemir, 2009: s. 80-81; Aksoy, 2010: s. 71). Yine özel yaşamın gizliliği (Any. md 20) hakkının da kendi koruma alanları içerisinde kişisel verilerin korunması hakkına bir takım garantiler getirdiği belirtilmiştir (Aksoy, 2010: s. 47 vd.).

Kişisel verilerin korunması hakkı, demokratik ve özgür bir toplum düzeninde yaşayan ve yaşamını kendi özgür iradesiyle belirleme yeteneğine sahip olan kişinin kişisel verileri üzerindeki haklarının korunmasıdır. Bu nedenle, modern toplumlarda veri işleme faaliyetlerinin riskleri karşısında bireyin korunabilmesi için her şeyden önce bireyin kendisine ait verileri üzerindeki belirleme hakkının yani bireyin kişisel verileri üzerinde karar verme özgürlüğünün güvence altına alınması gerekmektedir⁴².

Bu hak, aynı zamanda kişisel verilerin korunması yoluyla bireyin yapacağı ve yapmayacağı bir davranış hakkında özgürce karar verme ve bu kararına uygun davranış imkânının korunmasını da içermektedir. Çünkü birey kendisini ilgilendiren hangi verilerin kimler tarafından, ne zaman, hangi kapsamda ve ne sebeple bilindiğini ve yine olası haberleşme ortağını yeterli bir güvenlik içinde olduğundan emin olamıyorsa, bu durumda bireyin kendi iradesiyle karar verme ve yaşamını düzenleyebilme özgürlüğünü gerçek anlamda kullanabilmesi zordur. Dolayısıyla kişisel verilerin korunması hakkı, kişisel verilerin toplanması, kullanımı ve devri konusunda esas olarak bireyin söz sahibi olmasını gerekli kılmaktadır. Bu nedenle bireyin iradesine aykırı olarak ve yasal temelden yoksun şekilde yürütülen veri işleme faaliyetleri, kişisel verilerin korunması hakkına bir müdahale oluşturacaktır (Şimşek, 2008: s. 112).

Teknolojinin gelişmesiyle paralel şekilde artan veri işleme faaliyetleri karşısında bireyin kişisel verilerinin kolayca elde edilmesi, sınırsız bir şekilde toplanması, kullanılması ve üçüncü kişilere aktarılması karşısında bireyin

⁴² Bkz. BVerfGE 65 1, 41. Alman Anayasa Mahkemesinin Nüfus Sayımı Hakkındaki Kararından. (Aktaran: **Özdemir**, 2009: s. 81)

korunmasını amaçlayan ve bireye verileri üzerinde belirleme hakkını garanti eden kişisel verilerin korunması hakkı, ülkemizde, öncelikli olarak insan onuru bağlantısıyla kişiliğin serbest geliştirilmesi hakkı, yani genel kişilik hakkı ile temellendirilmektedir (Any. m. 17). Sürekli gözetlenen, yaşam ilişkilerine ilişkin tüm kişisel verileri kapsamlı bir kayda tabi tutulan ve özel yaşamının gizliliği kaldırılarak şeffaf hale getirilen ve kişisel verileri üzerinde hiç bir hakka sahip olmayan kişinin, kişiliğini serbestçe geliştirebilmesi mümkün değildir. Bu şekilde bütün yaşam ilişkilerinde gözetlenip, kayıt altına alınmış, özel yaşamının gizliliği ortadan kaldırılmış birey, toplumsal yaşamda muhtemelen kendi özgür kişiliğinin gereği gibi değil, kendisinden istenilen davranış tarzıyla hareket edecektir. Bu nedenle bireyin kişisel verilerinin korunması hakkı, ona kişisel verilerinin hukuka aykırı olarak, sınırsız bir şekilde kaydedilmesi ve işlenmesi karşısında temel hak boyutuyla bir koruma getirmekte ve yine basit bir veri objesi olmaktan korumaktadır (Şimşek, 2008: s. 112).

Başka bir gerekçeyle ifade etmek gerekirse bireyin kişisel verileri hakkında karar verme özgürlüğüne yönelik ortaya çıkan tehlikeler karşısında bireyin korunması ve kamusal organların sınırsız bir şekilde veri işleme yetkisine anayasal sınırların konulması zorunluluğundan hareketle, bireyin kişisel verileri üzerindeki hakkı kabul edilmiş bulunmaktadır.

Temel bir insan hakkı olduğu sonucuna varılan kişisel verilerin korunması hakkının hukuki niteliğine ilişkin doktrinde çeşitli görüşler bulunmaktadır. Bu görüşler, esas itibarıyla, kişisel verilerin özünde hangi hukuki varlık ve menfaatin yattığı noktasında birbirinden ayrılmaktadırlar (Aksoy, 2010: s. 37). Diğer bir anlatımla, kişisel verilerin korunması ile amaçlanan çıkarın ne olduğu sorusu özellikle Kıta Avrupa'sında ve ABD'de birbirinden farklı şekilde yorumlanmakta, verinin, üzerinde tasarrufta bulunulabilen bir mal yani mülkiyet hakkının bir türü mü olduğu, yoksa bireylere doğal hukukça bahsedilmiş doğuştan gelen bir hak mı olduğu tartışılmaktadır (Küzeci, 2010: s. 60).

Bu görüşleri temel olarak; mülkiyet hakkı görüşü, fikri mülkiyet hakkı görüşü, insan onuru, bireysel özerklik ve bilgilerin geleceğini belirleme hakkı ve özel hayatın hakkı görüşü olmak üzere dört başlık altında toplamak mümkündür.

4.3.2. Mülkiyet Hakkı Görüşü

Kişisel verilerin korunmasının hukuki niteliğine görüşlerden ilki, özellikle Amerikan kaynaklarında ileri sürülen mülkiyet hakkı görüşüdür. Bu görüşe göre, kişisel veriler, yalnızca kişiliğin bir uzantısı olmayıp, aynı zamanda kişiliğin bir ürünüdür. Bu çerçevede, herkesin, kendisine ilişkin kişisel verilerin sahibi olduğu kabul edilmeli ve herkes mülkiyetindeki bu verilerin hangi şartlar altında kullanılabileceğini kontrol edebilmelidir⁴³.

Bu görüşte, kişisel verilere mülkiyet hakkı temeline dayanan bir koruma sağlanırsa, veri öznesinin kendine ilişkin bilgiler üzerinde tam bir denetim hakkına sahip olacağı ve mülkiyet sahibine tanınan geniş yasal korumalardan da yararlanacağı savunulmuştur (Akgül, 2014: s. 73).

Verilerin mülkileştirilmesini savunan yazarlar, bu yolla bireylerin uygun antlaşmalar yaparak verilerinin kullanımının maddi ve manevi karşılığını alabileceklerini, böylece kişisel veriler pazarının daha adil işleminin sağlanabileceğini ileri sürmektedirler. Bu bağlamda bireyler, istedikleri takdirde kişisel bilgilerini satabilmeli ya da açıklayabilmelidir. Bunun yanında bu yaklaşımın şirketleri kişisel verilerin toplanması ve işlenmesinden dolayı ortaya çıkan maliyetleri benimsemeye zorlayacağı ve bu yolla özel yaşamın gizliliğinin daha güçlü bir şekilde korunacağı da savunulmuştur (Küzeci, 2010: s. 62).

Bilgilerinin kötüye kullanılması durumunda ilgili kişiye doğrudan dava açma ya da zararın giderilmesi için talepte bulunma hakkını vermesinin, bu teorinin güçlü yanı olduğu söylenmiştir. Ayrıca herkese kendine ilişkin profil üzerinde bir denetim olanağı verilip, bu hakkını mahkeme önünde savunması da sağlanırsa, mülkiyet hakkı yaklaşımı ilgili kişinin izni olmaksızın bilgilerinin paylaşımını önleyebilecektir (Küzeci, 2010: s. 62).

Diğer yandan bu görüşte kişisel verilerin ticari değeri ön plana çıkmaktadır. Teşebbüsler, topladıkları kişisel verilerden faydalanarak, müşterilerine sundukları hizmetin kalitesini arttırmanın yanında, bu verileri hem iç pazarlama stratejilerinin

⁴³ **Prins, Corien**, “When Personal Data, Behavior And Virtual Identities Become A Commodity: Would A Property Rights Approach Matter? (personal data)”, Scripted, C. 3, S. 4, 2006, s. 274-275. (Aktaran: Aksoy, s. 57) benzer şekilde, **BRIN, David**, The Transparent Society(Will Technology Force Us to Choose Between Privacy and Freedom), Addison-Wesley, ABD 1998. (Aktaran: Küzeci, s. 62)

belirlenmesinde kullanılmakta hem de üçüncü kişilere devrederek ticari kazanç sağlamaktadırlar. Örneğin, bir teşebbüs, müşterilerinin beğenileri ve ilgi alanlarına ilişkin verileri, müşterilerine sunacağı ürün ve hizmetlerin cinsini belirlemekte kullanabilmekte, müşterilerinin beklentilerinden yola çıkarak pazarlama stratejilerini şekillendirebilmektedir. Hatta aynı teşebbüs, bu bilgileri, benzer amaçlarla kullanabilecek diğer teşebbüslere de satabilmektedir. Ancak, geniş çapta kişisel veri toplayan, bunları kullanan ve üçüncü kişilere satan teşebbüslerin bu uygulamalarının olumsuz sonuçları, doğrudan veri sahipleri üzerinde doğmaktadır⁴⁴.

Teşebbüslerin kişisel veriler üzerinden para kazanmaları karşısında, kişisel verileri işenenen kişilerinde verilerin kullanımları karşılığında adil bir karşılık talep etme hakları bulunmaktadır. Nitekim kişisel verilerinin üçüncü kişilerce kullanılmasının olumsuz sonuçlarına katlanacak olan veri sahipleri, bir teşebbüs ile belli bir amaç için paylaştıkları kişisel verilerinin bu amaç dışında kullanıldığını çoğu zaman bilememekte ve herhangi bir hak iddiasında bulunamamaktadırlar. Ancak, mülkiyet hakkı görüşünün kabul edilmesi halinde, kendi kişisel verileri üzerinde mülkiyet hakkına sahip olan bir kimse, sahip olduğu veri türlerinden hangilerini hangi işletmelerle paylaşacağına karar verirken, aynı zamanda bu paylaşım karşılığında talep edeceği bedel konusunda da pazarlık edebilecektir⁴⁵.

Mülkiyet hakkı görüşünü savunanlara göre, bu görüşün kabul edilmesi uygulama açısından da kolaylık sağlayacaktır. Nitekim bu görüşün kabulü halinde, kişisel verilerin korunması başka herhangi bir sistem oluşturma ihtiyacı kalmaksızın, mülkiyet hakkının korunması kapsamında, sağlanabilecektir⁴⁶.

Kişisel verilerin ticari değer kazanmış olduğu düşüncesinden yola çıkan mülkiyet hakkı görüşü, sonuçları itibariyle, birçok açıdan da eleştiriye uğramıştır.

Mülkiyet hakkı görüşüne yöneltelen ilk eleştiri, mülkiyet hakkı kavramının niteliği itibariyle kişisel veriler bakımından kabul edilemeyeceğine ilişkindir. Zira mülkiyet hakkının temel niteliklerinden biri, malın ilk sahibi malını sattıktan sonra yeni hak sahibinin bunu istediği gibi kullanabilecek ve satabilecek olmasıdır. Bu çerçevede, mülkiyet hakkının malike sağladığı yetkilerden tasarruf yetkisinin, kişisel

⁴⁴ **Prins**, Personel Data, s. 279 (Aktaran: Aksoy, 2010, s. 57)

⁴⁵ **Prins**, Personel Data, s. 279 (Aktaran: Aksoy, 2010: s. 58)

⁴⁶ **Clarke, Roger**, Internet Privacy Concerns Confirm the Case for Intervention, (Internet), Communication of the ACM, C. 42, S. 2, 1999, s. 63 (Aktaran: Aksoy, 2010, s. 60)

veriler bakımından da söz konusu olduğunu kabul etmek oldukça güçtür. Mülkiyet hakkı görüşü çerçevesinde, tasarruf yetkisinin kişisel veriler bakımından da söz konusu olduğunun kabulü halinde, bir kişiden kişisel verilerini rızası çerçevesinde satın alan kimse, bu verileri kendisine devreden veri sahibinin rızası aranmaksızın üçüncü kişilere devredebilecektir. Ancak, kişisel verilerini bir teşebbüsle paylaşan bir kimsenin aynı veriyi başka bir teşebbüsle paylaşmak istememesi de mümkündür. Bu çerçevede, mülkiyet hakkı görüşü, kişisel verilerini bir başkasına devreden veri sahiplerini, kendilerine ilişkin olan bu verilerden mutlak şekilde soyutlamakta, bu durum da kişisel verilerin niteliği ile bağdaşmamaktadır (Aksoy, 2010: s. 64-65; Küzeci, 2010: s. 63).

Mülkiyet hakkı görüşüne getirilen ikinci eleştiri, bu hakkın işlevine yöneliktir. Buna göre, mülkiyet hakkının doğuş nedeni, doğadaki sınırlı kaynakların dağılımının sağlanmasıdır. Ancak, doğada, kişisel veriler bakımından herhangi bir kıtlık söz konusu değildir. Bu açıdan bakıldığında, kişisel verilerin hukuki niteliğinin mülkiyet hakkı olduğunun kabul edilebilmesi mümkün değildir (Aksoy, 2010: s. 66; Küzeci, 2010: s. 64).

Bu görüşe yapılan diğer bir eleştiri de, görüşün pratik sonuçlarına yöneliktir. Buna göre, mülkiyet hakkı görüşünün kabulü halinde, veri sahiplerinin kendi kişisel verilerini üçüncü kişilere devri, hem masraf, hem de süre yönünden elverişsiz olacaktır. Zira kişisel veri toplayan teşebbüslerin toplayacakları her bir veri için, o verinin malikinden izin almaları gerekecektir. Bu da ekonomi üzerinde olumsuz etkiler doğuracaktır. Nitekim bireylerin kendilerine ilişkin kişisel verilerin toplanmasını, kullanılmasını ve el değiştirmesini kontrol edebileceklerinin kabulü halinde, bilginin serbest dolaşımı baltalanmış olacağından modern ticaret zarar görecektir (Aksoy, 2010: s. 65).

Bizim de katıldığımız bu eleştirilere bakıldığında kanaatimizce de, gerek kişisel verilerin niteliği, gerekse de verilerin üçüncü kişilerle paylaşılması halinde dahi kişiyle irtibatının kesilmemesi nedenlerinden dolayı kişisel verilerin hukuki niteliğinin mülkiyet hakkı olduğunu savunmak mümkün değildir.

4.3.3. Fikri Mülkiyet Hakkı Görüşü

Kişisel verilerin hukuki niteliğine ilişkin olarak ileri sürülen ikinci bir görüş ise, fikri mülkiyet hakkı görüşüdür. Bu görüşü savunanlara göre, kişisel verilerin

korunması ile fikri mülkiyet hakkı arasında amaçsal bir benzerlik bulunmaktadır. Zira her iki hakkın korunmasındaki temel amaç, bilginin korunması ve dağılımının kontrolünün sağlanmasıdır⁴⁷.

Fikri mülkiyet görüşünü savunanlar, kişisel veri sahibinin kendisine ilişkin veri üzerindeki hakları ile fikri mülkiyet hukukundaki eser sahibinin meydana getirdiği eser üzerindeki manevi hakları arasında bir benzerlik bulunduğu noktasından yola çıkmışlardır (Akgül, 2014: s. 74). Diğer bir deyişle fikri mülkiyet hakkı görüşünde, kişisel verilerin veri sahibine sağladığı haklar ile eser sahibinin manevi haklarından “eseri umuma arz yetkisi” ve “eserde değişiklik yapılmasını yasaklama yetkisi” arasında bir benzerlik bulunduğu savunulmaktadır. Umuma arz yetkisi, eser sahibinin eserini umuma arz edip etmeyeceğini ve eğer umuma arz edecekse, eserin yayınlanma zamanı ve tarzını belirleme yetkisini ifade etmektedir. Eserde değişiklik yapılmasını yasaklama yetkisi ise, eserde veya eserin adında kısaltmalar, eklemeler veya başka değiştirmeler yapılabilmesinin eser sahibinin iznine tabi olduğu anlamına gelmektedir. Bu çerçevede, fikri mülkiyet hakkı çerçevesinde karşımıza çıkan bu haklara benzer şekilde, kişisel veri sahibinin de, kendisine ait verileri kimlerle ve hangi şartlar altında paylaşacağını tespit yetkisi ve üçüncü kişilerin elinde bulunsa dahi kendisine ait verilerin bütünlüğünün ve doğruluğunun korunmasını isteme yetkisi vardır. Bu benzerlik, esas itibarıyla, fikri mülkiyet hakkı görüşünün temelini oluşturmaktadır (Aksoy, 2010: s. 61).

Bu görüşte çeşitli açılardan eleştiriye uğramıştır.

İlk eleştiri, bilgiyi temel alan mülkiyet hakkı olarak da nitelendirilen fikrî mülkiyet gibi bir hak alanı ile kişisel verileri korumanın olanaklı olmadığına yöneliktir. Her şeyden önce fikrî mülkiyet hukukunun ekonomik temeli, fikri ürünlerle ortaya çıkabilecek sorunlarının üstesinden gelmektir. Oysa kişisel veriler, fikir ürünü olarak nitelendirilemez (Küzeci, 2010: s. 64).

İkinci eleştiri, her iki hakkın korunması amacına yöneliktir. Fikri mülkiyet hakkı görüşünü savunanlara göre, hem fikri mülkiyet haklarının, hem de kişisel verilerin korunmasının amacı bilgi ekonomisine katılımı sağlamaktır. Ne var ki, fikri mülkiyet görüşüne dayanak teşkil eden bu ortak amaca karşın, iki kurum arasında

⁴⁷ **Prins**, Personel Data, s. 1146 (Aktaran, Aksoy, 2010, s. 60)

doğaları itibariyle önemli farklılıklar bulunmaktadır; Fikri mülkiyete konu olan değerler, kişinin bilinçli bir şekilde sarf ettiği emeğin ürünü olarak meydana getirilir. Bu nedenle burada asıl korunan kişinin emeğidir. Ancak, kişisel verilerin meydana gelmesi bakımından her hangi bir emek, çaba söz konusu olmamakta, kişisel veriler, kişinin belirli tercihleri çerçevesinde yaşamını sürdürmesi sonucu, kişinin tabii varlığından doğmaktadır⁴⁸.

Üçüncü eleştiri, her iki hakkın varlık amacına ilişkindir. Fikri mülkiyet hakkı, gelişimin teşvik edilmesi, fikri ve sınaî haklar alanında kalkınmanın sağlanması amacıyla geliştirilmiştir. Bu çerçevede, kişinin fikri çabası sonucu meydana getirdiği eserlerin, bir tür mülkiyet hakkı çerçevesinde korunması, kişiye çabasının ticari semerelerinden faydalanma imkânı tanımaktadır. Ancak, kişisel verilerin korunmasında bu tür bir teşvik amacı bulunmamaktadır. Kişisel verilerin yaratılmasını veya geniş çaplı şekilde dağılımını sağlamak için bunlara mülkiyet hakkı tanınması gerekli değildir. Kişisel veriler, yukarıda da belirtildiği üzere, bunların yaratılması için herhangi bir çabaya gerek olmaksızın, kişinin belirli tercihleri çerçevesinde yaşamını sürdürmesi sonucu varlık kazanmaktadır. Bu nedenle, veri sahiplerine bu veriler üzerinde bir tür mülkiyet hakkı tanıyarak, bu verilerin yaratılmasını teşvik etme ihtiyacı bulunmamaktadır. Aksine kişisel verilerin korunma amacının, bu verilerin toplanmasının, kullanılmasının ve dağılımının sınırlandırılması olduğu dahi ileri sürülebilmektedir⁴⁹.

Dördüncü ve son eleştiri her iki hakkın korunmamasının doğuracağı sonuçlara ilişkindir. Gerçekten de, kişisel verilerin korunmaması, fikri mülkiyet hakkının korunmamasına kıyasla daha büyük ve ağır zararlara yol açabilmektedir (Aksoy, 2010: s. 66; Küzeci, 2010: s. 64-65). Örneğin, hassas nitelikteki verileri korunmayan kişi ayrımcılığa maruz kalabilecek, bu nedenle mesleğinden atılma ihtimali doğabilecek, belki de toplum içinde bazı özelliklerinin bilinmesi nedeniyle aşağılanabilecek, bu şekilde ağır insan hakkı ihlallerine konu olabilecektir. Fikri mülkiyet hakkının korunmaması halinde ise uğranılan zarar genellikle maddi zarar olarak karşımıza çıkmaktadır.

⁴⁸ **Prins**, Personal Data, s. 296 (Aktaran, Aksoy, 2010, s. 66)

⁴⁹ **Prins**, Personal Data, s. 296 (Aktaran: Aksoy, s. 66)

Bizim de katıldığımız bu eleştirilere bakıldığında kanaatimizce de, kişisel verilerin niteliği, her iki hakkın ortaya çıkış nedeni, korunma amaçları ve korunmamasını sonuçlarına dikkate alındığında, her iki hakkın birbirinden farklı olduğu görülecektir. Bu nedenle kişisel verilerin özünde fikri mülkiyet hakkı olduğunun kabul etmek mümkün değildir.

4.3.4. İnsan Onuru, Bireysel Özerklik ve Bilgilerin Geleceğini Belirleme Hakkı Görüşü

Kişisel verilerin korunması, günümüz bilişim teknolojileri karşısında kişisel bilgileri sınırsız bir şekilde toplanan, kullanılan, devredilen bireyin korunmasını amaçlamaktadır. Bu bağlamda kişisel verilerin korunması hakkının ilk olarak insan onuru ve bu kapsamda kişiliğin serbestçe geliştirilmesi hakkına dayandırıldığı görülmektedir (Şimşek, 2008: s. 111; Özdemir, 2009: s. 80-81; Aksoy, 2010: s. 71). Federal Almanya Anayasa Mahkemesi de 1983 yılında verdiği “Nüfus Sayımı” kararında bu duruma işaret etmiştir⁵⁰.

Federal Almanya Anayasa Mahkemesi bu kararında parlamento tarafından oy birliği ile kabul edilen Nüfus Sayımı Yasasını Anayasaya aykırı bulmuştur⁵¹.

Mahkeme kararında “*Anayasal düzenin merkezinde toplumun özgür bir üyesi olarak kişinin onuru bulunur. Günümüzdeki teknik gelişmeler ve buna bağlı olarak ortaya çıkan tehlikeler karşısında kişiliğin korunması özel bir önem kazanmaktadır. Hakkında edinilen bilgilerin neler olduğunu ve bu bilgilerin kimin elinde bulunduğunu öğrenebilme olanağına sahip olmayan bireyin kendi kararlarını verme özgürlüğü önemli ölçüde zarar görür. Özellikle otomatik veri işleme araçları ile verilerin sınırsız bir şekilde kaydedilebilmesi, bu verilerin her zaman ulaşılabilir niteliği ve bireyin ayrıntılı kişilik profilinin oluşturulabilme olasılığı da dikkate alındığında, kişinin üzerinde psikolojik baskı yaratılması ve onun kamusal yaşama katılımını etkilemesi olanaklıdır*”. Şeklinde tespitlerde bulunarak bu yasayı iptal etmiş, ayrıca, Alman Anayasasının insan onurunun korunmasıyla ilgili 1/1 ve

⁵⁰ Aksoy, Hüseyin Can, “The Right to Personality and Its Different Manifestations As the Core of Personal Data”, Ankara Law Review, Vol. 5, No. 2, 2008, s. 241-242;

⁵¹ Söz konusu Yasa, 1983 yılında memurların kapı kapı dolaşarak yapacakları sayımda yurttaşların sayılmasından başka bilgilerin edinilmesi de öngörmüş ve vatandaşlara kapsamlı bilgileri açıklama yükümlülüğü getirmiştir. Bu yükümlülüğü yerine getirmeyenler için ise yaptırım öngörülmüştür. Küzeci, 2010: s. 68

kişiliğin korunması hakkına ilişkin 2/1. maddelerini bir arada değerlendirerek, *“bilgilerin geleceğini belirleme hakkı”*nı türetmiştir⁵².

Gerçekten de, örneğin toplantı ve gösteri yürüyüşü ya da sivil toplum örgütlerine katılmasının resmi makamlarca kayıt altına alındığını ve bundan dolayı çeşitli mağduriyetler yaşayacağını düşünen birey, bu haklarını kullanmaktan vazgeçebilir. Bu durum, yalnızca bireyin kendi kişiliğini geliştirme hakkını zedelemekle kalmaz, ayrıca kamu çıkarlarına da zarar verir, çünkü özgürlükçü bir demokrasinin işlemesi topluma katılma ve toplum içerisinde işlev görme becerisine bağlıdır. Bu nedenle, kişiliğin serbestçe gelişebilmesi ve demokratik toplum yapısının sürekliliği için devlet tarafından kişisel verilerinin toplanılması, kaydedilmesi, kullanılması ve devredilmesi karşısında bireyin korunması bir gerekliliktir. Birey, yaşam ilişkilerinin açığa çıkacağı zamana ve bunun sınırına kendisi karar vermelidir. Nitekim bilgilerin geleceğini belirleme hakkı, ilke olarak bireyin kendi kişisel verileri üzerinde tasarrufunu sağlamaktadır (Küzeci, 2010: s. 69).

Diğer taraftan sürekli izlenen, yaşamına ilişkin bilgiler kayıt altına alınan, bütün bunların sonucunda adeta şeffaflaşan, bireyin kişiliğini serbestçe geliştirebilmesi olanaklı değildir. Bu kişinin toplumsal yaşamda kişiliğini özgürce belirleyememesi, kendinden beklenen davranış tarzına göre hareket etmesi de olasıdır. Bu noktada kişisel verilerin korunması hakkı, bireye kişisel verilerinin hukuka aykırı olarak sınırsız bir şekilde kaydedilmesi, işlenmesi, paylaşılması karşısında temel bir hak vermekte ve onu basit bir veri nesnesi olmaktan korumaktadır. Kısacası verilerin geleceğini belirleme hakkı, bireye verilerinin kullanılması üzerinde karar verme hakkını tanımaktadır (Şimşek, 2008: s. 112).

Ancak kişisel verilerin korunmasının altında yatan menfaatin sadece bilgilerin geleceğini belirleme hakkı olamayacağı yönünde görüş belirten yazarlar da olmuştur (Aktaran: Küzeci, 2010: s. 70).

Kanaatimizce kişilik hakkının bir görünümü olan insan onuru, bireysel özerklik ve bilgilerin geleceğini belirleme hakkı, Alman anayasa Mahkemesinin

⁵² Alman Anayasa Mahkemesinin bu kararı doktrinde bu alanda milat olarak değerlendirilmiş ve karar ülke sınırlarını aşarak diğer ülkelerin anayasalarında kişisel verilerin korunmasının düzenlenmesi konusunda öncülük ettiği belirtilmiştir. **Akgül**, 2014: s. 87; **Küzeci**, 2010: s. 69

türettiği “bilgilerin geleceğini belirleme hakkı” na ilişkin yorumlarıyla birlikte değerlendirildiğinde kişisel verilerin korunmasının temellerinden birini, hatta en önemlisini oluşturmaktadır. Zira kişisel verilerin korunması, sadece veriler toplandığı aşamada değil, verilerin elde edilmesinden silinmesine kadar geçen bütün aşamalarda bireyin korunmasını hedeflemektedir. Bu süreç içerisinde veri sahibi olan kişiye verileri üzerinde belli hakları kullanabilme imkânı vermektedir. Bilgilerin geleceğini belirleme hakkında da, kişinin verileri üzerinde tasarruf yetkisinin devam etmesi öngörüldüğünden her iki hak birbiriyle örtüşmektedir.

4.3.5. Özel Hayatın Gizliliği Hakkı Görüşü

Kişisel verilerin korunmasının özel hayatın gizliliği hakkı ile olan bağına geçmeden önce özel hayatın gizliliği kavramını, soyut ve tanımlanamayan niteliği nedeniyle, kısaca açıklamak gerekmektedir.

Özel hayat kişilik hakları içinde özel bir öneme sahiptir ve demokratik bir hukuk devletinde vazgeçilmez nitelik taşımaktadır. Aynı zamanda özel hayat kişiliğin en temel çekirdeği olarak da kabul edilmektedir. Günümüz modern hukukunda kişi her yönüyle bir bütün olarak kabul edilmekte ve özel hayat da bu bütünün bir parçası olarak görülmektedir. Bu itibarla da bireye kişiliğini serbestçe geliştirebilmesi için kendisi ve yakınları ile baş başa kalabileceği, devletçe ya da diğer kişilerce rahatsız edilmeyeceği özerk bir alanın sağlanması zorunludur (Kazancı, 2007: s. 131).

Bu kadar önemli ve vazgeçilmez bir hak olmasına rağmen gerek ulusal gerekse uluslararası düzenlemelerde özel hayatın tanımı yapılmamıştır. Doktrin görüşleri ve yargı kararları vasıtasıyla bazı tespit ve tanımlar yapılmaya çalışılmıştır.

Avrupa İnsan Hakları Sözleşmesinin uygulayıcısı konumunda olan Avrupa İnsan Hakları Mahkemesine göre özel hayat bütün unsurlarıyla tanımlanamayacak kadar geniş bir kavramdır. Ancak bu kavram, açık bir biçimde mahremiyet hakkından daha geniştir ve herkesin özgür olarak kişiliğini oluşturmasını ve geliştirmesini sağlayan bir alan içermekte olup, diğer insanlarla ve dış dünyayla ilişki geliştirmek hakkını da kapsamaktadır (K. Özdemir, 2005: s. 1).

Örneğin AİHM, Niemietz - Almanya kararında⁵³ özel hayatla ilgili önemli tespitlerde bulunmuştur. Mahkemeye göre; “*Özel hayat kavramını, bireyin kişisel hayatını istediği gibi yaşayabileceği bir iç alanla kısıtlamak ve bu alanın dışında kalan dış dünyayı bu alandan tamamen hariç tutmak aşırı sınırlayıcı bir yaklaşımdır. Özel hayata saygı, başka insanlarla ilişki kurmak ve söz konusu ilişkileri geliştirmek hakkını da bir dereceye kadar içermelidir* (Üzeltürk, 2004: s. 168; K. Ödemir, 2005).”

AİHM’e göre, özel hayat, hayatın iç alanıyla sınırlanmamalı, dış dünya da konuya dahil edilmelidir. Bir bireyin cinsel ilişkiler dâhil çeşitli tür ilişkiler oluşturabilmesi ve cinsel kimliğini belirleme ve benimseme tercihi, yapılan telefon konuşmasının içeriği, özel haberleşmeye müdahale amaçlı gizli teknolojik aletlerin kullanılması, bir devlet tarafından bireyler hakkında rızaları alınmaksızın bilgi toplanması, zorunlu tıbbî tedaviler, başka insanlarla ilişki kurma ve bu ilişkileri geliştirme özel hayat kapsamında değerlendirilmelidir (Kılınç, 2012: s. 1100; K. Ödemir, 2005).

Özel hayat, doktrinde “*Kişinin sadece kendisi için saklı tuttuğu ve başkalarının bilgisinden uzak kalmasını istediği yaşam görünümünü*”, “*Herkes tarafından bilinmeyen, özel araştırma ve bilgi edinmeyle sağlanan kişiye ait hususlar*”, “*Kişilerin gizli hayat alanlarında yapmış oldukları faaliyetlerin başkaları tarafından bilinmemesini istedikleri taraflar*”, “*Bireyin kişiliğini geliştirmek ve manevi değerlerine güvence sağlamak için başkaları tarafından bilinmesini istemediği hususların oluşturduğu ve korunması hukuken gerekli görülen hayat üzerindeki hakkı*” şeklinde tanımlanmaktadır (Kılınç, 2012: s. 1100).

Tanımlarda ortak olan nokta, kişiye ait bir alan ve bu alanın başkaları tarafından bilinmemesidir. Başka bir ifadeyle, özel yaşamda birey bu özgün alanın kendine hasredilmesini talep etmektedir (Kılınç, 2012: s. 1100).

AİHM içtihatlarına göre; cinsiyet, medeni hal, doğum yeri, diğer kişisel veriler ile ilgili bilgileri içeren uygulamalar, parmak izi, fotoğraf ve benzeri kişisel bilgilerin kaydedilmesi; tıbbi verilerin toplanması ve tıbbi kayıtların tutulması,

⁵³ Niemietz v. Germany, 13710/88, 16.12.1992, §29. Bkz. **Salihpaşaoğlu, Yaşar**, “Özel Hayatın Kapsamı: Avrupa İnsan Hakları Mahkemesi İçtihatları Işığında Bir Değerlendirme”, GÜHFD, C. 17, S. 3, Y. 2013, s. 235

sağlık, sosyal hizmetler ve vergi gibi idari ve sivil konuları ele alan bireysel kimlik belirleme sistemi kişisel veriler kapsamında değerlendirilmiştir⁵⁴.

Özel hayatın korunmasının kapsamı konusu tartışmalı olsa da genel de özel hayatın üç alana ayrıldığı ve korunma derecelerinin birbirinden farklı olduğu görülmektedir:

Bu alanlardan ilki ortak alandır. Ortak hayat alanı, başkaları tarafından bilinmesinde herhangi bir sakınca görülmeyen ve topluma açık olan, herkes tarafından bilinip girilebilen genel alandır. Kişi bu hayat alanında yaşarken bunu gizleme gereği duymamaktadır. Örneğin, bir kimsenin kültürel faaliyetlerde bulunması, alışveriş merkezlerine gitmesi, toplu taşıma araçlarına binmesi gibi kamuya açık alanlardaki eylemlerinden oluşan alandır (Özbek, 2008: s. 916; Üzeltürk, 2004: s. 4; Kılınç, 2012: s. 1101).

Ortak alanda kişinin statüsü de belirleyici bir etkidir. Bu kapsamda kamuoyuna mal olmuş resmi kişiler ve sanatçılar gibi kişilerin ortak yaşamı ile sıradan bir kişinin ortak alanı şüphesiz farklı olacaktır. Bu tür durumlarda, bu kişilerin özel yaşamlarının sınırları normal insanlara göre daraldığı veya bazen de ortadan kalktığı söylenebilir (Kılınç, 2012: s. 1102).

İkincisi, özel alandır. İstendiğinde ancak en yakın kişilerle paylaşılabilen, esasen gizli olan ve nisbi sınırlar barındıran bir alandır. Kişinin ailesi, dostları, akrabaları, iş arkadaşları ve arkadaşlarıyla paylaştığı yaşam alanına, özel alan denmektedir. Herkesin, özel alanına giren olayların gizli kalmasını isteme hakkı vardır. Başka bir ifadeyle, kişiler özel yaşamına ilişkin konuların başkaları tarafından bilinmemesini isteyebilirler. Özel alan, gizli alana göre daha alenidir. Ancak, bu alenilik toplum nezdinde bir aleniliği ifade etmemekte, sadece olayların meydana geliş şekliyle birlikte belirli vasıf ve sayıda kişiyle paylaşımın sözkonusu olmasıdır. Örneğin, kişinin kiminle nişanlandığı veya kimlerle arkadaşlık yaptığı, ailevi sorunları sadece kendisini ve belirli kişileri ilgilendirmektedir. Kişi, özel alana ait olayları yalnızca yakınlarıyla paylaşır. Bu nedenle, bu alana giren olayların üçüncü kişilere duyurulması halinde, özel hayat alanı ihlal edilmiş olur (Özbek, 2008: s. 916; Kılınç, 2012: s. 1102). Kişinin fiziksel ve zihinsel dokunulmazlığının korunması,

⁵⁴ Ayrıntılı bilgi için bkz. Salihpaşaoğlu, s. 237

bireyin onur ve şöhretinin haksız fiillere karşı korunması, bireyin adı, kimliği, resminin haksız kullanımlara karşı korunması, bireyin izleme, gözetleme ve tacizlere karşı korunması, mesleki sır kapsamına giren bilgilerin açıklanmasına karşı korunması, hayatın özel alanı kapsamında hukuken korunmaktadır (Üzeltürk, 2004: s. 169 vd.). Bu kapsamda bireyin kişisel verilerinin hayatın özel alanına girdiği söylenebilir.

Üçüncüsü, gizli alandır. Gizli alan, sır alanı olarak da ifade edilmektedir (Küzeci, 2010: s. 71; Aksoy, 2010: s. 52). Kişi burada başkaları tarafından öğrenilmesini istemediği bir hayat yaşamakta ve bu alana giren olayları, sadece özel olarak, yakınlık hissettiği kişilerle paylaşmaktadır. Gizli hayat alanı, bir kimsenin hayatının en özel ve gizli kısmını oluşturur. Kişinin sırları, duyguları, düşünceleri, ümitleri, korkuları, tercihleri, gibi konular bu alana girer. Gizli alan dokunulmaz olduğu gibi, her türlü müdahaleye karşı da hukuki koruma altındadır. Bu alanda yer alan bilgiler basın, yayına kapalıdır. Bu nedenle, kişinin hassas nitelikteki örneğin, dini veya felsefi inançlarına, siyasi görüşlerine, cinsel hayatına ve sağlık bilgilerine ilişkin verilerin bu alana girdiği söylenebilir (Özbek, 2008: s. 917; Kılınç, 2012: s. 1102).

Hayatın gizli alanına girilmesi kişi için ağır bir hak ihlalidir. Bu nedenle bu alan her türlü müdahaleye karşı mutlak olarak korunmuştur. Buna karşılık hayatın özel alanı ise üçüncü kişiler ve devlet müdahalesine karşı kural olarak korunmuş olmakla birlikte, dokunulmaz değildir, suçla mücadele, başkalarının hak ve özgürlüklerinin korunması gibi nedenlerle bu hakka müdahale mümkün olabilmektedir. Bu nedenle bu alandaki korumanın nisbi nitelikte olduğu belirtilmiştir. En dış olan hayatın ortak (genel) alanı ise kural olarak korumasızdır. Ancak burada da istisnai olarak örneğin sıradan bir kişinin kafede arkadaşıyla otururken fotoğrafının çekilmesi, eğer kişinin rızası yoksa veya haber değeri taşıyan bir olay değilse, haksızlık teşkil edecektir (Özbek, 2008: s. 917)

Özel yaşamın gizliliği hakkında yapılan bu açıklamalardan sonra kişisel verilerin korunması hakkı, ilk aşamada özel yaşamın gizliliği hakkı içinde değerlendirilebilir. Nitekim AİHM Klass kararında, bireyin özel hayatına ilişkin verilerin kamusal organlar tarafından toplanmasına, depolanmasına ve işlenmesi konusunda; bireyin özel yaşamı kapsamındaki bilgilere ilişkin kamusal müdahaleleri,

bireyi koruyucu uygun ve etkili garantiler içeren yasal düzenlemeler bulunmadığı sürece Sözleşmenin 8. maddesinde belirtilen hakların ihlali olarak değerlendirmiştir (Kılınç, 2012: s. 1099).

Kıta Avrupası hukukundaki genel görüş de bu yönde olup, kişisel veriler kişilik hakkının parçası olarak kabul edilmektedir. Nitekim AB Direktifinin amaç başlıklı birinci maddesinde, mahremiyet hakkı başta olmak üzere, bireylerin temel hak ve özgürlüklerinin korunmasının hedeflendiği açıkça ifade edilmiştir. Bu çerçevede, mahremiyet hakkı olarak ifade edilen hak, hukukumuzda kişilik hakkının bağımsız görünüm türlerinden birisi olarak kabul edilen özel hayattır⁵⁵.

Esasında özel yaşamın gizliliği hakkının kişisel verilerin korunmasından çok daha geniş bir alanı nitelemektedir. Ancak günümüzde kazandığı önem dolayısıyla kişisel verilerin korunması hakkı, her ne kadar özel yaşamın gizliliği hakkına ilişkin temel ilkelerden kaynağını alsa da ondan büyük oranda ayrılmıştır. Bu şekilde haberleşme özgürlüğüne benzetilebilir. Nitekim haberleşme özgürlüğünde temelde özel yaşamın gizliliği hakkı kapsamındadır. Ancak özel önemi ve gereklilikleri dolayısıyla pek çok metinde ayrı olarak düzenlenmiştir. Benzer bir ilişkinin düşünceyi açıklama özgürlüğü ve basın özgürlüğü arasında bulunduğu da söylenebilir (Küzeci, 2010: s. 74).

Nitekim gelişen teknoloji, özel yaşamın gizliliği hakkına geleneksel yaklaşımlar ve bu alanda benimsenen ilkelerin verilerin korunmasında yetersiz kaldığı doktrinde bazı yazarlar tarafından da belirtilmiş ve tarihsel süreç içerisinde kendisinden daha köklü bir hak alanı olan özel yaşamın gizliliği hakkından ayrılmaya başladığı ifade edilmiştir. Bu anlamda kişisel verilerin korunmasının özel yaşamın gizliliği hakkının özellik taşıyan bir türü olduğu ve kendine özgü bazı gereklilikleri nedeniyle ayrı bir alan olarak algılanmaya başlandığı da söylenmiştir⁵⁶.

Bu kapsamda, kişisel veri kavramının özel hayat alanında yer almayan ve dolayısıyla üçüncü kişilerden gizliliğine riayet edilmesi beklenmeyen olaylara ilişkin bilgileri de kapsayabileceği öne sürülmüş; örneğin, kişinin hangi sendikanın üyesi olduğu üçüncü kişiler açısından gizliliğine riayet edilmesi gereken bir özel hayat

⁵⁵ **Ketizmen, Muammer**, “Kişisel Verilerin Korunması” Tebliğ,

http://www.tbd.org.trusr_imgcdkamubib14raporlarPDFRP2-2008.pdf Erişim Tarihi: 27.02.2014

⁵⁶ **Prins**, “Property and Privacy”, s. 227-228 (Aktaran, Küzeci, s. 70)

olayı kabul edilemeyeceği halde bu hususun, hukuka aykırı olarak kaydedilmesi durumunda TCK m. 135/2'de düzenlenen suçun oluşumuna imkân verebilecek nitelikte bir kişisel veri olduğu da gerekçe olarak gösterilmiştir (Keklik, 2012: s. 27).

Gerçekten de AİHM bu hususu, Rotaru/Romanya davasına ilişkin olarak verdiği 04.05.2000 tarihli kararında şu şekilde vurgulamıştır: “*Ayrıca kamuya açık bilgiler, düzenli olarak toplandığında ve yetkili makamlar tarafından dosyalarda saklandığında da özel hayat kapsamına girebilir. Bu durum özellikle söz konusu bilgiler kişinin geçmişine aitse daha da geçerlidir* (Keklik, 2012: s. 27).”

Bunun yanında Avrupa Birliği Temel Haklar Şartı ve çeşitli devletlerin anayasalarında kişisel verilerin korunması hakkının, özel yaşamın gizliliği hakkından bağımsız olarak temel haklar içerisinde yer aldığı görülmektedir⁵⁷.

ABTHŞ'nda özel yaşamın gizliliği ile kişisel verilerin korunması farklı maddelerde ayrı ayrı hüküm altına alınmıştır⁵⁸. Benzer bir durum anayasal düzenlemeler açısından da kendini göstermektedir. Özel yaşamın gizliliği hakkı, hemen hemen bütün devletlerin anayasalarında temel bir hak olarak belirlenmiştir. Ancak kişisel verilerin korunması hakkının bağımsız olarak anayasal temelde korunduğu örnekler de artmaktadır⁵⁹.

AB Temel Haklar Şartı'nda özel yaşamın gizliliği hakkı ile kişisel verilerin korunması hakkı arasında bir ayrımın öngörülmesi önemlidir. Zira kişisel verilerin korunması hakkı, özel yaşamın gizliliği hakkının çekirdeği içerisinde değerlendirilemeyecek bazı konuları koruma kapsamına almaktadır.

⁵⁷ Bkz. 1997 tarihli Polonya Anayasası 51. madde, 1976 tarihli Portekiz Anayasası 26. madde, 1978 tarihli İspanya Anayasası 18. Madde. Bkz. **Avrupa Birliği Üyesi Bazı Ülkelerin Anayasaları**, s. 397-451-543

⁵⁸ ABTŞ'nin “**Özel hayata ve aile hayatına saygı**” kenar başlıklı 7. maddesi: “Herkes özel hayatına, konutuna ve haberleşme özgürlüğüne saygı gösterilmesini isteme hakkına sahiptir”. “**Kişisel verilerin korunması**” kenar başlıklı 8. maddesi ise: “(1) Herkes, kendisini ilgilendiren kişisel verilerinin korunması hakkına sahiptir. (2) Bu veriler, adil bir şekilde, belirli amaçlar için ve ilgili kişinin rızasına veya yasa ile Öngörölmüş diğer meşru bir temele dayanarak tutulur. Herkes, kendisi hakkında toplanmış verilere erişme ve düzeltirme hakkına sahiptir, (3) Bu kurallara uyutması, bağımsız bir makam tarafından denetlenir”. Şeklindedir. Metnin Türkçe çevirisi için bkz. Avrupa Birliği Temel Haklar Şartı, Avrupa Birliği ile İlişkiler Genel Müdürlüğü, Kasım 2001, www.dpt.gov.tr/DocObjects/Download/2962/temelhak.pdf, (s.y. 7 Şubat 2009).

⁵⁹ 2002 tarihli Hollanda Anayasası, m. 10/2,3; 1997 tarihli Polonya Anayasası 51. madde, 1976 tarihli Portekiz Anayasası 26 ve 35. madde, 1978 tarihli İspanya Anayasası 18. madde. Bkz. **Avrupa Birliği Üyesi Bazı Ülkelerin Anayasaları**, Ankara, 2011

Bunlardan ilki, AB Temel Haklar Şartı'nın 8. maddesinde herkesin kendisi hakkında toplanmış verilere erişme ve bunları düzelttirme hakkına sahip olduğunun belirtilmesidir. Zira AİHM'de özel yaşamın gizliliği hakkına dayanarak oluşturduğu içtihatlarında bu hususu tam anlamıyla cevaplayamamaktadır.

Diğeri, gizli olmayan kişisel verilerin de kişilik hakkı olması ve kişisel verilerin korunması hukuku alanında korunmasıdır. Zira kişisel veri, uluslararası belgelerde gerçek kişiyle ilgili bütün bilgiler olarak tanımlanmış, bu konuda gizli olan gizli olmayan veya doğru bilgi yanlış bilgi gibi bir ayırım yapılmamıştır. Yegâne ölçüt, bir bilginin belirli ve ya belirlenebilir bir kişiyle ilintili olmasıdır. Özel yaşam kavramı ise, kamusal alana ilişkin verilerin özel yaşam çerçevesinde korunmasına imkân tanımamaktadır.

Ayrıca AB Temel Haklar Şartı'nda kişisel verilerin korunmasının özel yaşamın gizliliği hakkından ayrı olarak düzenlenmesi, kişisel verilerin korunmasının artık bağımsız bir hak olarak kabul edildiğinin önemli bir işaretidir (Küzeci, 2010: s. 160).

O halde kişisel verilerin korunması hakkı, özel hayatın gizliliği hakkı ile yakın bir ilişki içinde olsa ve çoğu zaman da ortak bir alana yönelik olsa da, kişilik hakkı çatısı altında artık bağımsız bir hak olarak yerini almaya başladığı söylenebilir.

Sonuç olarak, özel yaşamın gizliliği hakkı, kişilik hakkının görünüm türlerinden yalnızca bir tanesi olup, bu görünüm türleri daha önce de belirtildiği üzere sınırlı sayıda değildir. Bu nedenle kişisel verilerin korunması hakkının kaynağını kişilik hakkının görünüm türlerinden olan insan onuru, bireysel özerklik ve bilgilerin geleceğini belirleme hakkı ile özel yaşamın gizliliği hakkında bulduğunu, ancak yukarıda da açıklanmaya çalışıldığı üzere, gelişen hukuk düzeninde bağımsız bir temel hak olarak da kabul edilmeye başlandığı söyleyebiliriz.

4.4. Kişisel Verilerin Korunması Hakkının Diğer Hak ve Özgürlüklerle İlişkisi

Kişisel verilerin korunması hakkı, kendisinden daha köklü bir tarihe sahip başka hak ve özgürlüklerle yakından ilişkilidir. Bu haklarla kimi zaman karşılıklı destekleme, kimi zaman da çatışma halindedir (Küzeci, 2010: s. 60). Burada sadece,

bilgi edinme hakkı, düşünceyi açıklama özgürlüğü ve haberleşme hürriyeti ve basın hürriyeti ile olan bağlantısından söz edilecektir.

4.4.1. Bilgi Edinme Hakkı ile İlişkisi

Bilgi edinme hakkı, bireylerin devletin tuttuğu bilgilere ulaşabilme hakkı anlamına gelir⁶⁰. Bu hakla, kişilerin idarenin etkinlikleri, yetkileri ve kararları konusunda bilgi sahibi olmalarını, kamu otoritelerinin denetlenmesini ve kamu hizmetinin etkin bir şekilde güvence altına alınması hedeflenmiştir. Bilgi edinme hakkı, idarenin elindeki bilgilerin artması sonucunda, bir denge unsuru olmakta ve idarenin gücüne ve iktidarına sınırlama getirmesi yönüyle hukuk devleti için aranan unsurlar arasında yer almaktadır (Kaya, 2005: s. 44). Bu yönüyle, kişisel verilerin korunması hukuku ile amaç bakımından, benzer olduğu görülmektedir.

İdarenin elindeki bilgilerin gereksiz ve usulsüz biçimde gizlenmesi demokrasinin işlerliği açısından sorun yaratabilecek olmakla birlikte, bilgiyi tekeli altında bulunduranların, bu bilgileri imtiyazlı şekilde kullanma tehlikesi de mevcuttur⁶¹.

Bu sakıncaların giderilmesini sağlamak amacıyla kabul edilen bilgi edinme hakkı, kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarının görevleri gereği sahip olduğu ya da olmak zorunda olduğu bilgi ve belgeleri talepte bulunan kişilerle paylaşmaları yükümlülüğü getirmektedir. Bilgi edinme bir hak olarak yasal zemine kavuşturulurken, hakkın kullanılmasında öne çıkan temel düzenleme, idarenin, görevi gereği sahip olduğu ya da olmak zorunda bulunduğu bilgi ve belgeleri talepte bulunan kişilerle paylaşmasının zorunlu olmasıdır⁶².

⁶⁰ Çolak, N. İlker, “Bilgi Edinme Hakkı, Önemi ve Bilgi Verme Yükümlülüğü”, <http://www.ilkercolak.com.tr/bilgi-edinme-hakki-onemi-ve-bilgi-verme-yukumlulugu/> Erişim Tarihi: 27.5.2014; Çolak, N. İlker, “Bilgi Edinme Hakkının Sınırları ve Sınırlama Ölçütleri”, e-akademi Hukuk, Ekonomi ve Siyasal Bilimler Aylık İnternet Dergisi, S. 39. Mayıs 2005, parag. 1, <http://www.e-akademi.org/makaleler/nicolak-2.htm> Erişim T: 27.05.2014; Kaya, Cemil, İdare Hukukunda Bilgi Edinme Hakkı, Seçkin, Ankara 2005, s. 41-42

⁶¹ Tortop, Nuri "İletişim ve Bilgi Edinme Hakkının Önemi", AİD, C.37, S.1, Mart 2004, s. 36.(Aktaran, Küzeci, s. 93)

⁶² Çolak, “Bilgi Edinme Hakkının Sınırları ve Sınırlama Ölçütleri”, parag. 1

Pek çok lke, kişisel verilerin korunmasına ve bilgi edinme hakkına ilişkin hukuksal düzenlemeleri bir arada kabul etmiştir⁶³. Yani bunların hukuk düzenin bir parçası olması çeşitli yerlerde zaman açısından paralellik göstermektedir. Ayrıca çeşitli devletlerde her iki hakkın sağlanmasını denetleyen bağımsız kurulların aynı çatı altında toplandığı da görölmektedir. Burada her iki hak alanının birbirinin bütünleyicisi olduğu ve düzenlemelerin birbirleriyle uyumluluğunda yarar bulunduğu düşüncesi hâkim olmuştur⁶⁴.

Kişisel verilerin korunması hakkı ile bilgi edinme hakkı arasında farklı bir ilişki vardır. Yani iki hak bazı durumlarda birbirini sınırlamakta, bazı durumlarda ise birbirinin içine geçmiş konuları düzenlemektedir. Gerçekten de kişisel veriler bir açıdan bilgi edinme hakkı çerçevesinde erişilebilecek bir bilgi kategorisini oluşturmakta; bir başka açıdan ise kişisel verilerin korunması, bilgi edinme hakkına sınır getirmektedir (Kaya, 2005: s. 89-91).

Kişisel veriler, bilgi edinme hakkı kapsamında erişilebilecek bir bilgi kategorisini oluşturmaktadır. Kişiler kural olarak, bu kapsamda başvuruda bulunarak kendilerine veya başka kişilere ve olaylara ilişkin idarenin tuttuğu verileri öğrenebilirler. Ancak idareden istenen veriler başkalarının özel hayatına ilişkin ise bu durumda bu veriler idare tarafından, bilgi edinme hakkının kapsamına girmediği gerekçesiyle verilmeyebilecektir.

Konuya bu açılardan bakıldığında her iki hakkın birbirini bütünlediğini ve bir yandan bireylerin kendileri hakkındaki bilgilere ulaşmasını sağlarken, öte yandan özel yaşamların korunmasına hizmet ettiğini görmekteyiz.

Diğer taraftan da esasında bilgi edinme hakkı ile kişisel verilerin korunması farklı alanları düzenlemektedirler. Bu kapsamda, devletin topladığı verilerin büyük bir bölümü vatandaşların yönetime katılımını sağlamak için son derece önemlidir ve

⁶³ Demokratik ve şeffaf yönetimin gereği olan eşitlik, tarafsızlık ve açıklık ilkelerine uygun olarak kişilerin bilgi edinmelerini sağlamak amacıyla 9.10.2003 tarihinde kabul edilen 4982 sayılı Bilgi Edinme Hakkı Kanunu ile mevzuatımıza girmiş olan bilgi edinme hakkı, 2010 yılında 5982 sayılı Kanunla Anayasanın 74. maddesine eklenmek suretiyle de anayasal bir hak haline gelmiştir. Ayrıntılı bilgi için bkz. **Çolak, N. İlker**, “Bilgi Edinme Hakkı, Önemi ve Bilgi Verme Yükümlülüğü”, <http://www.ilkercolak.com.tr/bilgi-edinme-hakki-onemi-ve-bilgi-verme-yukumlulugu/> Erişim Tarihi: 27.5.2014

⁶⁴ **Küzeci**, s. 94; Ülkemizde ise Kişisel Verilerin korunmasına ilişkin henüz bir kanun çıkarılabilmiş değildir.

bilgi edinme özgürlüğü kapsamında korunmaktadır. Şehir planlamasına, çevre kirliliği ve trafik sorunlarına ilişkin tutulan veriler buna örnek gösterilebilir. Ancak bu sorunlara ilişkin bilgilerin kişisel veri niteliği taşımadığı açıktır. Burada kişisel verilerin korunması hakkı ile bilgi edinme hakkı ayrıştığı için aralarında bir çatışmadan söz etmek de olanaklı değildir (Küzeci, 2010: s. 94).

Ancak bilgi edinme hakkının, bireyin kendisine ilişkin kamusal organlarca tutulan verilere ulaşmasını sağlayabilmesi nedeniyle kişisel verilerin korunmasını destekler mahiyette olduğunu söyleyebiliriz (Küzeci, 2010: s. 94).

Konuya bilgi edinme hakkının sınırlarından biri olan özel hayatın gizliği açısından bakılacak olursa; bilgi edinme hakkının kişisel verilerin korunması açısından faydaları daha net görülecektir. Zira devlet, çok geniş bir kişisel veri arşivine sahiptir. Bu gücün sınırlandırılmaması, özel yaşamın gizliliği hakkının özüne müdahale oluşturur (Kaya, 2005: s. 89-91). Zira Devletin elinde vatandaşlara hatta ülkeye giren yabancılara ait doğum, ölüm, evlatlık edinme, sabıka, sağlık kayıtları, seçmen kütükleri kayıtları, banka, sosyal güvenlik, vergi, iflas ve malvarlığına ilişkin kayıtlar gibi binlerce kayıt bulunmaktadır. Bunların bir kısmının oldukça hassas nitelik gösterdiği ve bireyin isteği dışında, herhangi bir kamusal gereklilik olmaksızın, başkalarının eline geçmesi durumunda ortaya çıkabilecek zararlar da açıktır. Bu bilgilerin başka kişilere aktarılması bireylerin temel hak ve özgürlükleri ile özel yaşamlarına zarar verebileceği gibi, onların bağımsızlığını da zedeleyebilir (Küzeci, 2010: s. 95).

4.4.2. İfade Özgürlüğü ile İlişkisi

Düşünceyi açıklama özgürlüğü olarak ta adlandırılan ifade özgürlüğü, *“insanın serbestçe düşünce ve bilgilere ulaşabilmesi, edindiği düşünce ve kanaatlerden dolayı kınanaması ve bunları tek başına ya da başkalarıyla birlikte çeşitli yollarla serbestçe açıklayabilmesi, savunabilmesi, başkalarına aktarabilmesi ve yayabilmesi anlamına gelmektedir”⁶⁵*.

⁶⁵ **Tanör, Bülent**, Türkiye'nin İnsan Hakları Sorunu, BDS Yayınları, 3. Baskı, İstanbul 1994, s. 59 (Aktaran, **Özbey, Özcan**, “Avrupa İnsan Hakları Sözleşmesi Işığında İfade Özgürlüğü Kısıtlamaları”, TBB Dergisi, S. 106, 2013, s. 44)

Anayasa Mahkemesi de yakın zamanda verdiđi “Twitter” kararında⁶⁶, ifade özgürlüğünün, “sadece düşünce ve kanaate sahip olma özgürlüğünü deđil, aynı zamanda sahip olunan düşünce ve kanaati açıklama ve yayma, buna bađlı olarak haber veya görüş alma verme özgürlüklerini de kapsadıđı, bu çerçevede ifade özgürlüğü bireylerin serbestçe haber ve bilgilere, başkalarının fikirlerine ulaşabilmesi, edindiđi düşünce ve kanaatlerden dolayı kınanaması ve bunları tek başına veya başkaları ile birlikte çeşitli yollarla serbestçe ifade edebilmesi, anlatabilmesi, savunabilmesi, başkalarına aktarabilmesi ve yayabilmesi” anlamına geldiđini belirtmiştir (Akgül, 2014: s. 90).

Kişisel verilerin korunması hakkı, ifade özgürlüğü ile çođu zaman çatışma halindedir. Bu çatışma özellikle düşünceyi açıklama özgürlüğü içerisinde deđerlendirilen basın özgürlüğü açısından kendini gösterir. Özellikle magazin alanında yapılan yayınlarda, kamuya, başkalarına ilişkin son derece mahrem bilgiler, yazı, fotoğraf ya da görüntüler aktarılmaktadır (Küzeci, 2010: s. 86).

Bu hallerde, bir tarafta halkın ilgisini çeken konuları araştıran, deđerlendiren, yayınlayan basın kuruluşları, diđer yanda, kişisel bilgilerinin paylaşılmamasını isteyen bireyler arasında bir çekişme söz konusu olmaktadır. Buradaki sorunun çözüm kaynađı, basın özgürlüğü ile özel yaşamın gizliliđi ve kişisel verilerin korunması hakkı arasındaki ilişkide hangisine ağırlık verileceğinin belirlenmesinde yatmaktadır. Bu durumda da her bir olayda ölçme ve deđerlendirme yapılmalı ve somut olayın kendisine özgü koşulları içinde hangisine ağırlık verileceđi saptanmalıdır⁶⁷.

Bunun yanında her iki hak ve özgürlüğün birbirlerini desteklediđi alanlar da bulunmaktadır. Kimsenin düşüncelerini açıklamaya zorlanamayacađı kuralı düşünceyi açıklama özgürlüğü kapsamında deđerlendirilirken, aynı zamanda kişisel verilerin korunması açısından da kısmi bir güvence sağlamaktadır. Bu kural, bireyin gizli kalmasını istediđi verileri açıklamaya zorlanamamasına ve özellikle hassas verilerinin kendisinde saklı tutması isteđine destek verir. Bu şekilde, kural olarak bireyin kişisel verilerinin ancak kendi rızası ile toplanabilmesi ilkesi ve kişisel

⁶⁶ AYM’nin 02.04.2014 tarihli ve 2014/3986 Başvuru Numaralı 3.4.2014 tarihli ve 28961 sayılı R.G. de yayınlanan kararı.

⁶⁷ **Küzeci**, s. 87; Konuyla ilgili ayrıntılı bilgi için bkz. **Çolak, N. İlker**, Kitle İletişim Hukuku, Oniki Levha Yayıncılık, İstanbul, 2013

verilerini açıklama konusunda bireyin belirleme hakkı düşüncüyü açıklama özgürlüğü ile de desteklenmiş olmaktadır (Şimşek, 2008: s. 146-147).

4.4.3. Haberleşme Özgürlüğü ile İlişkisi

Haberleşmenin gizliliği ile kişilerin telefon, telgraf, mektup, elektronik posta gibi araçlarla gerçekleştirdikleri özel iletişimlerinin gizliliğini ve güvenilirliğini korumak amaçlanmaktadır. Bu hak, normatif temelini özel yaşamın gizliliği hakkında bulur (Gözübüyük ve Gölcüklü, 2004: s. 341). Bireyin dilediği kişiyle dilediği şekilde haberleşmesinin engellenmemesi ve bu haberleşmelerin ilgilinin onayı ya da yasal gereklilikler olmaksızın üçüncü kişilerin müdahalecinden korunması, haberleşmenin gizliliğinde ana ilkedir. Nitekim özel yaşamın korunmasına ilişkin AIHS'nin 8. ve İHEB'nin 12. maddeleri ile çoğu ülke anayasalarında haberleşmenin gizliliği hakkından da bahsedilmektedir (Küzeci, 2010: s. 97).

Haberleşme özgürlüğü ile kişisel verilerin korunması hakkı, haberleşme içeriklerinin kişisel veri niteliğinde olması halinde birlikte gündeme gelmektedirler. Zira hukuka aykırı bir şekilde iletişimin dinlenmesi ya da kayda alınması ile kişisel verilerin elde edilmesi durumunda hem özel haberleşmenin gizliliği, hem de kişisel verilerin korunması hakkı ihlal edilmektedir. Nitekim verilerin toplanması ve işlenmesinde hukuka uygunluk ve dürüstlük, kişisel verilerin korunmasına hâkim olan temel ilkelerdendir. Özel haberleşmenin gizliliği ile haberleşmenin içeriği üçüncü kişilerin müdahalesinden korunmakta, haberleşmenin içeriği ve muhatabını serbestçe belirleme özgürlüğünü desteklemektedir (Şimşek, 2008: s. 149).

Bu nedenle, özel haberleşmenin gizliliği, kişisel verilerin korunması hakkı açısından da dolaylı yönden güvence sağlamaktadır.

5. KİŞİSEL VERİLERİN KORUNMASI HAKKININ SINIRLARI

Normatif temelini esas olarak insan onuru ve kişiliğin serbest geliştirilmesi hakkı ile özel hayatın gizliliğinden alan kişisel verilerin korunması hakkı, sınırsız olarak garanti edilmemektedir. Diğer bir deyişle bireyin kişisel verileri üzerinde mutlak ve sınırsız bir hâkimiyeti bulunmamaktadır. Bir toplum düzeni içerisinde yaşayan birey, ağırlıklı kamu yararı nedeniyle kişisel verilerine yönelik olarak

anayasaya uygun ve yasal temele dayanan sınırlamalara uymak zorundadır (Şimşek, 2008: s. 149).

Aynı şekilde örneğin, devletin hukuk devleti ve sosyal devlet olması nedeniyle ödevlerini yerine getirirken duyacağı bilgi gereksinimi de kişisel verilerin korunması hakkına yapılacak sınırlamaları meşrulaştıracaktır. Gerçekten de sosyal devlet ilkesi⁶⁸, sosyal yaşamı düzenleyen, hizmet eden, koruma getiren devlet faaliyetlerini gerekli kılmaktadır. Sosyal devletin bu niteliğinden kaynaklanan ödevlerini yerine getirebilmesi için toplumdaki sosyal durumları bilmesi gerekmektedir. Toplumdaki sürekli artan ihtiyaçları karşılamak, sosyal devletin gereklerini yerine getirmek için etkili bir yönetim faaliyetine gereksinim vardır ve bu faaliyetin de bir takım kişisel veriler elde edilmeden yerine getirilmesi mümkün değildir. Ancak bu tür kişisel veriler toplanırken, verilerin toplanması devletin meşru faaliyetlerini yerine getirebilmesi için bir araç olmalı, yoksa başlı başına bir araç olmamalı ve bu hakkın anayasal garantilerine riayet edilmelidir (Şimşek, 2008: s. 124).

Kişisel verilerin korunmasına ilişkin olarak uluslararası düzenlemelerde de bir takım sınırlamalar getirildiği görülmektedir. Bu çerçevede Avrupa Konseyinin verilerin korunmasına ilişkin 108 nolu Sözleşmesi, yasal olarak öngörülmüş olma ve demokratik bir toplumda gerekli bir önlem olma koşuluyla aşağıdaki durumlarda üye Devletlere istisna getirme hakkını tanımaktadır (m. 9) (Şimşek, 2008: s. 127):

- Devlet güvenliğinin, kamu güvenliğinin, devletin ekonomik menfaatlerinin korunması ve suçlarla mücadelenin söz konusu olması.

- İlgilinin veya üçüncü kişilerin hak ve özgürlüklerinin korunması.

- Bunun yanı sıra Sözleşmede otomatik olarak toplama, verilerin istatistiki veya bilimsel amaçlarla kullanılması durumlarında da ilgilinin katılım haklarına bir takım sınırlamalar öngörülmüştür (m. 9/3).

AB'nin 95/46/EC sayılı Kişisel Verilerin Korunması Direktifi de kişisel veriler bakımından Direktifte öngörülen güvencelere, sınırlama ve istisnalar

⁶⁸ Sosyal devlet ilkesi ile ayrıntılı bilgi için bkz. **Gözler, Kemal**, Türk Anayasa Hukuku, Ekin Kitabevi Yayınları, Bursa, 2000, s.154-168

getirilebilmesine imkân vermektedir (m. 13). Buna göre, üye Devletler devlet güvenliği, ülke savunması, kamu güvenliği, suçtan korunma, suçların soruşturulması ve kovuşturulması, üye devletin önemli ekonomik ve finansal yararı, ilgili kişinin korunması, diğer kişilerin hak ve özgürlüklerinin korunması gibi nedenlerle Direktifteki düzenlemelere sınırlama ve istisnalar getirebileceklerdir (Uygun, 2010: s. 69-70; Şimşek, 2008: s. 127).

AK Sözleşmesi ve AB Direktifindeki hakkın korunma alanına ilişkin istisnalar Kişisel Verilerin Korunması Kanunu Tasarısında da benzer şekilde düzenlenmiş olmakla birlikte, Tasarı kanunlaşmadığı için henüz uygulama imkânı bulunmamaktadır.

Anayasamızda ise kişisel verilerin korunması hakkının düzenlendiği 20. maddede bu hakkın sınırlama sebepleri düzenlenmemiştir. 20. maddenin ikinci fıkrasındaki sınırlama sebepleri ise, her ne kadar doktrinde görüş birliği olmasa da, özel hayatın gizliği kapsamında arama ve elkoymaya ilişkindir⁶⁹. Ancak 20. maddenin üçüncü fıkrasında kişisel verilerin mahiyeti gereği, kişisel verilerin kişinin açık rızasıyla ve kanunda öngörülen hallerde işlenebileceği hüküm altına alınmıştır. Burada kişinin rızası olması durumunda hakkın sınırlandırılmasından söz edilemeyecektir. Kanunda öngörülmenin ise bir sınırlama sebebi değil de bir sınırlama yöntemi olduğu, bu nedenle de kişisel verilerin işlenmesine kanunla izin verilmesiyle bu işlemin otomatikmen hukuka uygun olmayacağı, bu kanununda anayasadaki temel hak ve özgürlüklerin sınırlandırılması rejimine uygun olması gerektiği ileri sürülmüştür (Akdağ, 2013: s. 84-87).

Gerçekten de Anayasada kişisel veriler için özel bir sınırlandırma sebebi öngörülmemiş ise de, Anayasanın 13. maddesinde temel hak ve hürriyetlerin nasıl sınırlandıracağı, sınırlamayı yapan kanunun hangi standartta olacağı belirlenmiştir. Ayrıca 13. maddede 2001 yılında yapılan değişiklikle, genel sınırlama rejimden vazgeçilerek her hakkın niteliğine özgü sınırlama sebepleri kabul edilmiştir (Yokuş, 2003: s. 212).

⁶⁹ Bu konudaki tartışmalar için bkz. Akdağ, s. 86

13. maddenin ikinci cümlesine göre, *“Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve laik cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz.”*

O halde kişisel verilerin korunması hakkına müdahale edilmesi halinde müdahale yöntemlerinin Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve laik cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olmaması gerekmektedir.

Ölçülülük ilkesine göre, temel hakkın sınırlanmasında başvuru araç, sınırlama amacını gerçekleştirmeye elverişli olmalı, araç amaç için elverişli olmalı ve araçla amaç arasında ölçüsüz bir oran bulunmamalıdır. Bu anlamda kişisel verilere yönelik sınırlama ve müdahalelerde başta ölçülülük ilkesi olmak üzere Anayasanın temel hakların sınırlanması rejimine uyulması gerekmektedir (Şimşek, 2008: s. 125).

Diğer yandan kişisel verilerin korunması hakkına yapılacak yasal müdahalede açıklık ilkesine de uyulmalıdır. Açıklık ilkesine göre, kişisel verilerin korunması hakkına yönelik sınırlamaya imkân tanıyan yasal düzenleme, açık ve herkes için kavranabilir olmalıdır. Bu yasal düzenlemenin, veri işlemenin kapsamını ve amaçlarını o derece açık bir şekilde ortaya koyması gerektirmektedir ki, ilgili kişi kişisel veriler üzerindeki karar verme hakkına yönelik sınırlamanın kapsamını zamanında ve net bir şekilde tahmin edebilmelidir. Bu durum aynı zamanda veri işlemenin şeffaflığı ilkesinin de mantıksal bir sonucudur (Şimşek, 2008: s. 126).

Kişisel verilerin korunması hakkına yapılan müdahalelerde amaca bağlılık ilkesine de uyulmalıdır. Bu ilke, veri toplamanın yasal olarak belirlenen amaç için söz konusu olmasını ve bu amaca bağlı kalınmasını gerektğini ifade etmektedir. Bu nedenle belirsiz veya henüz belirli olmayan amaçlarla stok yapmak üzere veri toplamak, amaca bağlılık ilkesi ve temel haklara en az müdahalede bulunulması ilkesiyle bağdaşmamaktadır. Aynı şekilde belirli bir amaç için toplanan verilerin toplandıktan sonra toplanma amacına yabancı amaçlarla kullanılması ve devrine karşı kişinin korunması ve bu konudaki gerekli önlemlerin alınması gerekmektedir (Şimşek, 2008: s. 126).

Sonu olarak, kiřisel verilerin korunması temel hakkı sınırsız olarak korunmamaktadır ve esas olarak bu hakka müdahale mümkündür. Ancak kamusal organlar tarafından kiřisel verilerin korunması hakkına yapılacak müdahale, řayet kiřinin usulüne uygun rızası bulunmuyorsa ancak bir kamu yararı varsa yapılabilmesi ve mutlaka yasal bir temele sahip olmalıdır. Bu yasanın da anayasanın temel hakların sınırlandırılmasına ilişkin temel kurallarına uygun olması gerekmektedir.

İKİNCİ BÖLÜM

ULUSLARARASI ÖRGÜTLERİN HUKUKİ DÜZENLEMERİNDE KİŞİSEL VERİLERİN KORUNMASI VE MUKAYESELİ HUKUKTA KİŞİSEL VERİLERİN KORUNMASI HAKKININ İHLALİNE İLİŞKİN YAPTIRIMLAR

1. GENEL OLARAK

Gerek kamu hizmetlerinin zamanında ve sağlıklı verilebilmesi ve devletin güvenlik sağlama ihtiyacı, gerek özel sektörün yaptığı hizmetleri yürütebilmesi için kişisel verilerin işlenmesi giderek bir zorunluluk haline gelmiştir. Veri işlemenin elektronik ortamlarda yapılmaya başlanmasıyla birlikte, işlem sayısının her geçen gün artması, kişisel verilerin korunmasında yeni önlemler alınması ve düzenlemeler yapılmasını zorunlu hale getirmiştir. Bu nedenle gerek devletler, gerekse uluslararası örgütler konuyla ilgili önlemler almaya çalışmışlardır. Bu kapsamda birçok uluslararası sözleşme ve düzenleme yapılmıştır.

Bir kısım uluslararası belgelerde kişisel verilerin korunması doğrudan düzenlenmemiş, kişisel veriler özel hayatın gizliliği hakkı kapsamında değerlendirilmişlerdir. Bu kapsamda Birleşmiş Milletler İnsan Hakları Bildirisi, Medeni ve Siyasal Haklar Sözleşmesi ve Avrupa İnsan Hakları Sözleşmesi başta olmak üzere, pek çok uluslararası belgede özel hayatın gizliliği, temel insan hakları arasında düzenlenmiştir.

Bunun yanında uluslararası alanda doğrudan kişisel verilerin korunmasına alanını yönelik metinler de hazırlanmıştır. 1970' li yıllardan itibaren ilk veri koruma kanunlarının kabul edilmesinden kısa bir süre sonra, verilerin ülkeler arasında transferinde sorun yaşanmaması için ulusal yasaların uyumlaştırılması gereksinimi ortaya çıkmıştır. Bu doğrultuda 1980'li yılların başından itibaren verilerin korunması açısından yeni bir döneme girilmiştir. OECD, BM, AK, ve AB gibi uluslararası kuruluşlar, kişisel verilerin korunmasına ilişkin temel ilkeleri ve verilerin sınırötesi aktarımını düzenleyen metinler kabul etmişlerdir. Bu metinlerde, ulusal hukuklarda genel olarak geçerli olacak veri koruma ilkeleri belirlenerek, veri koruma hukukunun gelişimine büyük katkı sağlanmıştır (Küzeci, 2010: s. 117).

Nitekim pek çok bölgeden çok çeşitli devletlerin kişisel verilerin korunmasında Avrupa modelinden etkilendiği görülmüştür. Bunda, AB'nin 95/46/EC sayılı Direktifinin kişisel verileri “yeterli” oranda korumayan devletlere veri aktarımını yasaklamasının önemli bir etken olduğu ifade edilmiştir⁷⁰.

2. ULUSLARASI ÖRGÜTLERİN KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN HUKUKİ DÜZENLEMELERİ

2.1. Kişisel Verilerin Korunmasına İlişkin Birleşmiş Milletler Düzenlemeleri

İkinci Dünya Savaşında sonra 24 Ekim 1945 tarihinde 51 devlet tarafından kurulan Birleşmiş Milletler (BM) örgütünün günümüzde 192 üyesi bulunmaktadır. Temel amaçlarından biri herkesin insan hakları ve temel özgürlüklerine saygı gösterilmesinin geliştirilip desteklenmesi olan BM, bu alanda birçok düzenleme yapmıştır (Arslan, 2011: s. 37; Özdemir, 2009: s. 17-18; Aksoy, 2010: s. 6; Kılınç, 2012: s. 1111).

BM'nin kuruluşundan kısa bir süre sonra 10 Aralık 1948 yılında kabu edilen “Birleşmiş Milletler İnsan Hakları Evrensel Bildirisi”, insan haklarının korunması alanında dünya ölçeğinde bir standart oluşturmaları nedeniyle, bu konuda önemli bir adım olmuştur. Bildirinin 12. maddesinde özel yaşamın gizliliği hakkı düzenlenmiştir. Madde hükmü şöyledir (Arslan, 2011: s. 37):

"Hiç kimse, özel yaşamına, ailesine, konutuna ya da haberleşmesini yönelik keyfi müdahalelere ya da onur ve şöhretine yönelik saldırılan maruz bırakılmayacaktır. Herkesin, bu tür müdahale ya da saldırılan karşı yasa ile korunma hakkı vardır".

16 Aralık 1966 tarihinde kabul edilen Birleşmiş Milletler Medeni ve Siyasi Haklar Sözleşmesinin 17. maddesinde de, benzer ifade ile özel hayatın gizliliğine yer verilmiştir. Ancak daha önemlisi, kişisel verilerin korunması hakkının bu Sözleşme'de yer alan özel yaşamın gizliliği hakkı kapsamında görüldüğünün BM İnsan Hakları Komitesi tarafından açıkça kabul edilmesidir (Arslan, 2011: s. 37).

⁷⁰ Küzeci, s. 118; Zira ülkemizde de Kişisel Verilerin Korunması Kanunu Tasarısı hazırlanırken, tasarının gerekçesinde de belirtildiği üzere AB Direktifindeki ilke ve kurallara dikkate alınmıştır.

Her ne kadar sözleşme metninde "Özel hayat ve kişisel verilerin korunması" kavramları tanımlanmamışsa da, sözleşmenin kurduğu denetim mekanizmasını yürütmekten sorumlu İnsan Hakları Komitesi'nin 16 nolu Genel Yorumunda 17. maddenin çerçevesi çizilmiştir (Aslan, 2010: s. 4). 16 nolu Yorumda Komite;

"...kamu otoritelerinin, özel kişi veya kurumların bilgisayarlarında, data bankalarında veya benzeri cihazlarda kişisel bilgileri toplaması veya saklaması hukuki düzenlemeye tabi tutulmalıdır. Devletler, bir kimsenin özel hayatına dair bilgilerin hukuken bu bilgilere sahip olma ve kullanma yetkisine sahip olmayanların eline geçmesini ve bu bilgilerin Sözleşme'nin amaçlarına aykırılık teşkil edecek şekilde kullanılmasını engellemek için etkili tedbirler almalıdır. Özel hayatın gizliliğinin en etkili şekilde korunabilmesi için, her birey otomatik veri dosyalarında kendisiyle ilgili bilgiler saklanmışsa bu bilgilerin ne tür bilgiler olduğunu ve ne amaçla saklandığını öğrenme hakkına sahiptir. Ayrıca her birey hangi kamu otoritelerinin veya özel kişilerin veya kurumların bu dosyaları kontrol altında tuttuğunu veya tutabileceğini öğrenebilmelidir. Söz konusu dosyaların, yanlış kişisel bilgilere yer vermesi halinde veya bu bilgilerin hukuka aykırı şekilde toplanması veya kullanılması halinde her birey düzeltme veya bilgilerin ortadan kaldırılmasını talep etme hakkına sahiptir..." şeklinde tespitlerde bulunmuştur.

İnsan Hakları Komitesi, 17. madde ekseninde geliştirdiği yorumdan şu sonuçları çıkarmak mümkündür:

- ❖ Öncelikle, kişisel verilerin korunması özel yaşamın gizliliği hakkı içerisinde değerlendirilmiştir.
- ❖ Kişisel verilerin toplanması ve depolanması işlemleri mutlaka hukuki düzenlemeye dayanmalıdır. Bu kapsamda hukuka uygun veri işlemenin nasıl yapılacağı kanuni düzenlemelerle belirlenmelidir.
- ❖ Devletlerin yükümlüğü bununla sınırlı olmayıp ayrıca verilerin yetkisiz üçüncü kişilerin eline geçmesini engellemek için gerekli tedbirleri almalıdır veya alınmasını sağlamalıdır.
- ❖ Ayrıca verileri işlenen kişilere verilerin nerede veya kimler tarafından tutulduğunu öğrenme hakkı verilmelidir. Kişiler öğrenme haklarının yanı

sırta hatalı ya da yanlış veri tutulması durumunda bunların düzeltilmesini veya silinmesini de talep edebilmelidirler.

Bu düzenlemelerin yanı sıra Birleşmiş Milletler, 1990 yılında, OECD'nin Rehber İlklerine benzer ancak daha ayrıntılı ölçütler içeren, kişisel verilerin korunması konusunda “Bilgisayarla İşlenen Kişisel Veri Dosyaları Hakkında Yönlendirici İlkeler” adını taşıyan bir belge kabul etmiştir (Şimşek, 2008: s. 16; Özdemir, 2009: s. 18-19; Kılınç, 2012: s. 1111).

Belgede kişisel verilerin korunmasına ilişkin ilkeler ayrıntılı bir şekilde açıklanmıştır. Bu ilkeler şunlardır (Kılınç, 2012: s. 1111):

“1- Yasallık ve dürüstlük: Kişisel veriler kanuna aykırı ve dürüst olmayan yollarla toplanmamalı ve toplanış amacına ve temel haklar ve özgürlüklerle ilgili ilkelere aykırı olarak kullanılmamalıdır.

2- Doğruluk: Toplanan verilerin doğruluğu kontrol edilmeli ve doğru ve eksiksiz olarak saklanmasını ve güncelliğini sağlamak için saklandığı süre zarfında düzenli olarak kontrol edilmelidir.

3- Amacın belirli ve haklı olması: Kişisel verilerin hangi haklı amaçla toplandığı başlangıçta kesin olarak belirlenmeli ve bu amaç bütün ilgililere açık olarak bildirilmelidir.

4- İlgili kişilerin erişme hakkı: Kişisel veri ile ilgili kişi kimliğini kanıtlamak koşulu ile kendisi hakkında toplanan bilgilerin ne gibi bir işleme tabi tutulduğunu öğrenebilmeli ve bunların bir anlaşılabilir biçimdeki bir örneğini aşırı bir masraf ve zaman kaybı olmadan elde edebilmelidir.

5- Ayrımcılıktan kaçınma: Kişinin etnik kökeni, ırkı, cinsel yaşamı, dini veya felsefi inançları gibi duyarlılık konularla ilgili bilgiler ancak yasanın izin verdiği haklı ve gerekli durumlarda toplanmalıdır.

6- İstisna koyma yetkisi: Görevli makamlara, milli güvenliği, kamu düzenini, halk sağlığını, genel ahlakı korumak veya diğer kişilerin hak ve özgürlüklerine zarar vermemek amacıyla yasallık ve dürüstlük, doğruluk, amacın belirli ve haklı olması, ilgili kişilerin erişme hakkı ilkeleri ile ilgili önlemlerden ayrılma yetkisi tanınabilir. Ancak bu yetkinin kapsamı ve sınırları kanunda açıkça belirlenmelidir. Ayrımcılıktan

kaçınma ilkesine getirilecek istisnanın her durumda temel hak ve özgürlüklere aykırı olmaması gerekir.

7- Güvenlik: Kişisel verilerin toplanması, saklanması ve işlenmesi ile görevli bütün kurum ve kişiler, bu verilerin doğal afetler, kazalar ve insanların işleyecekleri hata, kusur ve suçların yaratacağı tehlikelere karşı korunması için her türlü önlemi almalıdır.

8- Denetim ve yaptırım: Kişisel verilerin korunması ile ilgili düzenlemelerde öngörülen ilke ve kuralların uygulanması ve önlemlerin alınması ve gerekli denetimlerin yapılması sorumluluğu tarafsız, yetkin ve adil bir makama verilmelidir.

9- Sınır ötesi veri transferi: Kişisel verilerin saklanmakta olduğu ülkeden başka bir ülkeye aktarılması için öncelikle her iki ülkenin ulusal mevzuatlarının bu aktarmaya izin vermesi gerekir. Ayrıca, bu veriler için verinin gönderileceği ülkenin bu veri için sağladığı korumanın verinin bulunduğu ülkede sağlanan korumadan daha aşağı düzeyde olmaması da gerekir.”

2.2. Kişisel Verilerin Korunmasına İlişkin Ekonomik İşbirliği ve Kalkınma Teşkilatı Düzenlemeleri

Kişisel verilerin korunmasının konusunda uluslararası arenada ilk adımı Ekonomik İşbirliği ve Kalkınma Teşkilatı (The Organisation for Economic Co-operation and Development- OECD) atmıştır. OECD, batılı sanayileşmiş ülkelerin yanı sıra Avrupa dışındaki ABD, Kanada, Japonya, Yeni Zelanda ve Meksika gibi devletlerin de dâhil olduğu bir kuruluştur. 1961 yılında kurulan OECD'nin temel hedefleri arasında ekonomik büyümeyi desteklemek, iş alanlarını arttırmak, yaşam standardını yükseltmek, finansal dengeyi korumak, başka devletlerin ekonomik gelişimine yardımcı olmak, küresel ticaretin büyümesine katkı sağlamak ile demokrasi ve pazar ekonomisine bağlı devletleri bir araya getirmek bulunur⁷¹. OECD bu kapsamda verilerin ülkeler arasında değişimini sağlama ve ulusal düzenlemeleri uyumlaştırmak amacıyla 1980 yılında *"Özel Yaşamın Gizliliğinin ve Sınır Ötesi*

⁷¹ Ekonomik İşbirliği ve Kalkınma Teşkilatı (Organization for Economic Cooperation and Development OECD), 1961 yılında Türkiye'nin de içinde bulunduğu yirmi ülke ile kurulmuştur. Daha sonra on ülke daha OECD'ye katılmıştır. OECD'nin ürettiği tavsiyelerin bağlayıcılığı bulunmamaktadır. Bkz. **İktisadi İşbirliği ve Kalkınma Teşkilatı ve Türkiye**, <http://www.oecd.org/dataoecd/39/40/42122130.pdf>. Erişim Tarihi: 27.5.2014

Kişisel Veri Dolaşımının Korunmasına İlişkin Rehber İlkeler" i kabul etmiştir (Şimşek, 2008: s. 12; Küzeci, 2010: s. 119; Özdemir, 2009: s. 19; Aksoy, 2010: s. 4).

OECD Rehber İlkeleri, hukuksal açıdan tavsiye kararı niteliğindedir ve üye ülkeler için bağlayıcılığı yoktur. Dolayısıyla ilkelerin içeriğinin iç hukuka aktarımına konusunda üye Devletlerin serbestisi bulunmaktadır. Buna karşılık OECD'nin bu Kılavuz İlkeleri, getirdiği düzenlemelerin hayata geçirilmesi yoluyla esas olarak üye Devletlerde çoğulcu demokrasinin, insan haklarına riayet ve serbest piyasa ekonomisinin gerçekleşmesini amaçlamaktadır. Bu İlkelerde üye Devletlere iç hukuktaki yasal düzenlemeler vasıtasıyla kişilik alanının korunması, temel hak ve özgürlüklere riayet edilmesi, sınır aşan verilerin serbest trafiği için haksız engellerin kaldırılması, yeni engellerin oluşturulmaması ve Rehber İlkelerdeki hükümlerin gerçekleştirilmesi hususunda işbirliği yapılması tavsiye edilmektedir (Şimşek, 2008: s. 13; Özdemir, 2009: s. 19).

Kişisel verilerin korunmasına ilişkin asgari ölçütlerin belirlendiği OECD Rehber İlkelerini şu şekilde özetleyebiliriz (Şimşek, 2008: s. 12; Kılınç, 2012: s. 1110):

“1- Veri toplamasının sınırlı olması ilkesi: Bu ilkeye göre, kişisel verilerin toplanmasına sınır getirilmelidir. Kişisel verilerin toplanması, sadece hukuka uygun olarak, dürüst araçlarla, gerektiğinde veri öznesinin rızası veya bilgisi dâhilinde gerçekleşmelidir.

2- Veri kalitesi ilkesi: Kişisel veriler amacına uygun olmalı ve bu amaç için gerekli ölçüde, eksiksiz ve güncel olmalıdır.

3- Amacın belli olması ilkesi: Kişisel verilerin toplandığı amaç verilerin toplanma anında belirlenmiş olmalıdır. Veriler, daha sonra bu amaç dışında kullanılamamalıdır.

4- Kullanmanın sınırlı olması ilkesi: Bu ilkeye göre kişisel veriler ifşa edilemez, emre amade halde tutulamaz veya toplanma amacı dışında kullanılamaz. Ancak, veri öznesinin rızası veya kanun tarafından öngörülen durumlar bunun dışındadır.

5- Veri güvenliği ilkesi: Bu ilkeye göre kişisel veriler, kaybolma yetkisiz erişim, tahrip edilme, kullanma, değiştirilme veya ifşa edilme gibi risklere karşı uygun güvenlik önlemleri vasıtasıyla güvence altına alınmalıdır.

6- Açıklık ilkesi: Bu ilkeye göre kişisel verilere ilişkin olarak, işlemler ve önlemler genel olarak aleniyet politikası çerçevesinde gerçekleştirilmelidir.

7- Bireyin katılımı ilkesi: Bireyin katılım hakkı çerçevesinde birey, her şeyden önce esas veri sorumlusu vasıtasıyla ya da başka bir usulle kendisini ilgilendiren verilerin mevcut olup olmadığının onaylanmasını talep hakkına sahiptir. Burada, belirtilen hakların kullanımının reddedilmesi durumunda talebin neden reddedildiğinin gerekçe ile bildirilmesini isteme ve ret kararına karşı hukuk yollarına başvurabilme hakkı da düzenlenmiştir. Ayrıca veri öznesine, kendisi hakkında veri işlenmesine itirazda bulunma ve itirazın haklı bulunması halinde kendisi hakkındaki verilerin silinmesini, düzeltilmesini, eksikliklerinin tamamlanmasını veya değiştirilme yapılmasını isteme hakkı da öngörülmüştür.

8- Hesap verilebilirlik İlkesi: Veri sorumlusu yukarıdaki ilkelerin hayata geçirilebilmesi için gerekli önlemlere riayet etmesi bakımından hesap verebilir durumda olmak zorundadır.”

OECD Rehber İlkeleri konuya ilişkin uluslararası alanda yapılan ilk önemli girişimin ürünü olması nedeniyle önemli bir düzenlemedir. Başka bir deyişle kişisel verilerin korumasının ulusal hukuk sistemlerinin yanında, uluslararası alanda da tartışılan ve çözüm aranan bir konu olduğunun ilk işaretidir. Aynı zamanda kişisel bilgilerin denetiminin nasıl yapılacağı, kullanım şekillerinin nasıl saptanacağı konusunda geniş kapsamlı bir uzlaşayı da yansıtmaktadır. Diğer bir yönden ise OECD Rehber İlkeleri, her ne kadar üye ülkeler için bağlayıcı olmasa da, konuya ilişkin pek çok ulusal ve uluslararası metnin kabul edilmesini ve bunların içeriğinin belirlenmesini önemli oranda etkilemiştir (Küzeci, 2010: s. 119-121; Özdemir, 2009: s. 20).

2.3. Kişisel Verilerin Korunmasına İlişkin Avrupa Konseyi Düzenlemeleri

2.3.1. Genel Olarak

Kişisel verilerin korunması yönünde önemli çalışmalar yürüten diğer bir uluslararası örgüt, Avrupa Konseyi'dir. Avrupa Konseyi, Türkiye'den Rusya'ya, Karadağ'dan İsviçre'ye kadar Avrupa kıtasındaki hemen tüm devletlerin üyesi olduğu, sıklıkla karıştırılmasına rağmen Avrupa Birliği ile herhangi bir organik bağı bulunmayan hükümetler arası bir uluslararası teşkilattır. Bölgesel bir kuruluş olan AK'nin amaçlarından en önemlisi insan haklarının korunması ve geliştirilmesidir⁷². Konsey bünyesinde çeşitli hukuksal metinlerin kabulü ve çalışmaların yürütülmesi ile insan haklarının korunmasına katkı sağlanmaya çalışılmaktadır. 4 Kasım 1950'de Roma'da imzalanan ve Türkiye tarafından da 18 Mayıs 1954 tarihinde onaylanmış bulunan İnsan Haklarının ve Temel Özgürlüklerin Korunmasına Dair Avrupa Sözleşmesi, kısa ve yaygın adıyla Avrupa İnsan Hakları Sözleşmesi (AİHS) de bunun bir örneğidir (Berber vd 2009: s. 103).

Bilindiği gibi, AİHS'nde kişisel verilerin korunması, bağımsız bir hak olarak yer almamakta, kişisel veriler, Avrupa İnsan Hakları Mahkemesi içtihatlarında AİHS'nin özel hayatın gizliliğini düzenleyen 8. maddesi kapsamında değerlendirilmektedir. Ancak teknik ve hukuki boyutlarıyla yeni gelişen bir alan olması ve özel yaşamın gizliliğinin korunmasına yönelik geleneksel yaklaşımlarla bu hakkı yeterli düzeyde korumanın mümkün olmadığına anlaşılmaması, Avrupa Konseyi'ni bu konuda müstakil düzenlemeler yapmaya itmiştir (Arslan, 2011: s. 38-39).

Bu kapsamda çalışmalara başlayan Konsey, 1973 ve 1974 yıllarında kabul ettiği iki kararda kişisel verilerin korunması için gerek kamu ve gerek özel sektör kurum ve kuruluşlarında göz önünde bulundurulması gereken ilkeleri saptamıştır. Bu suretle konunun ulusal düzeyde çıkarılacak mevzuat ile düzenlenmesine ön ayak olunmak istenmiştir. Bununla beraber daha sözü edilen karar sureti metnlerinin hazırlanması sırasında bile bağlayıcı bir uluslararası belge çıkarılmadan ulusal

⁷² Avrupa Konseyi hakkında ayrıntılı bilgi için bkz. **Özdek, Yasemin**, Avrupa İnsan Hakları Sözleşmesi ve Türkiye, Ankara, 2004, s. 1-24

mevzuatın istenen yönde gelişmesinin sağlanamayacağı anlaşılmış ve bu konuda bağlayıcı bir belgenin kabul edilmesi kararlaştırılmıştır⁷³.

İşte Avrupa Konseyi kişisel verilerin korunması konusunda, gerek kamu gerekse özel sektör kurum ve kuruluşlarında göz önünde bulundurulması gereken ilkeleri saptamak ve konunun ulusal düzeyde çıkarılacak mevzuat ile düzenlenmesine ön ayak olmak amacıyla, 28 Ocak 1981 tarihinde, “Otomatik Olarak İşlenen Kişisel Veriler Bakımından Bireylerin Korunması Hakkında Sözleşme” yi kabul etmiştir⁷⁴.

Bu Sözleşme ile ilgili olarak bu güne kadar çeşitli tavsiye kararları alınmış, 1999 yılında da belgede bazı değişiklikler yapılmıştır. Bununla beraber Sözleşme yalnız Avrupa ülkelerinde değil bütün dünyada kabul görmüş ve ulusal mevzuatın hazırlanmasında göz önünde bulundurulmuştur⁷⁵. Ayrıca Avrupa Konseyi’nin kişisel veriler açısından sağladığı koruma 108 sayılı Sözleşme’deki düzenlemelerle sınırlı kalmamıştır. Daha sonraki yıllarda özellikle Avrupa Konseyi Bakanlar Komitesi’nin yayınladığı kararlar ile birçok alanda kişisel veriler açısından etkili bir koruma sağlama yoluna gidilmiştir (Atak, 2010, s. 90).

Ayrıca 2001 yılında Sözleşme için bir Ek Protokol imzaya açılmıştır. Protokol, Sözleşme’ye taraf devletlerde ulusal kontrol makamlarının oluşturulmasını zorunlu kılmış ve kişisel verilerin yeterli düzeyde koruma sağlamayan ülkelere ve uluslararası örgütlere transfer edilmesini yasaklamıştır. 2004 yılında yürürlüğe giren bu Protokolü, Ocak 2010 itibariyle Avrupa Konseyi üyesi 25 devlet onaylamıştır⁷⁶.

108 sayılı Sözleşme ve Bakanlar Komitesi’nin yayınladığı kararların yanı sıra Avrupa İnsan Hakları Sözleşmesi de kişisel verilerin korunması konusunda önemli bir rol oynamıştır. Avrupa İnsan Hakları Sözleşmesi’nde kişisel verilerin korunmasına ilişkin doğrudan bir hüküm yer almamasına rağmen, özel yaşamın

⁷³ <http://www.scribd.com/doc/19952426/1-Bilisim-Surasi-Hukuk-Raporu?query=ki%C5%9Fisel+verilerin+korunmas%C4%B1>. s. 31, Erişim Tarihi:20.03.2012

⁷⁴ Kılınç, s. 1112; Sözleşme, 1 Ekim 1985 tarihinde beş devletin onaylama işlemi tamamlamasıyla yürürlüğe girmiştir. 1 Mayıs 2009 tarihine kadar Sözleşme’nin onaylama sürecini 41 devlet tamamlamıştır. Rusya, Türkiye ve Ukrayna ise Sözleşme’yi imzalamış ancak onaylama işlemi henüz gerçekleştirilmemiştir. Bkz. <http://conventions.coe.int>. Erişim T: 25.5.2014

⁷⁵ <http://www.scribd.com/doc/19952426/1-Bilisim-Surasi-Hukuk-Raporu?query=ki%C5%9Fisel+verilerin+korunmas%C4%B1>. s. 31, Erişim Tarihi:20.03.2012

⁷⁶ Türkiye, Sözleşmede olduğu gibi, bu protokölü de imzalamasına rağmen henüz bu konuda bir kanun çıkaramadığı için protokolü onaylayamamıştır. Atak, 2010: s. 94

gizliliği hakkını koruyan 8. madde bu alanı da kapsamaktadır. Nitekim Sözleşme hükümlerinin üye devletlerde uygulanmasını izlemekten sorumlu olan Avrupa İnsan Hakları Mahkemesi, 8. maddenin sağladığı korumanın kişisel verileri de kapsadığı yönünde kararlar vermiştir (Atak, 2010, s. 91).

Aşağıda öncelikle AK'nin kişisel verilerin korunmasına ilişkin 1981 tarihli Sözleşmesi incelenecek, ardından Avrupa İnsan Hakları Sözleşmesi ve bu minvalde Avrupa İnsan Hakları Mahkemesinin konuya bakış açısı anlatılmaya çalışılacaktır.

2.3.2. Kişisel Verilerin Otomatik İşlenmesi Sırasında Bireylerin Korunmasına İlişkin Sözleşme

Sözleşmenin halen kişisel verilerin korunması alanında bağlayıcı olan tek uluslararası metin olması (Sevimli, 2006: s. 113; Arslan, 2011: s. 39) ve TCK'da düzenlenen kişisel verilere karşı işlenen suçların yorumunda bu sözleşme hükümlerinden yararlanılacak olması nedeniyle üzerinde ayrıntılı durmakta fayda vardır.

Sözleşmenin amacı, 1. maddesinde de belirtildiği üzere, taraf devletlerde bulunan her bir birey için uyrukluğı veya ikametgâhı ne olursa olsun, kişisel verilerin otomatik işlenmesi karşısında temel hak ve özgürlüklere ve özellikle mahremiyet hakkına saygı gösterilmesini sağlamaktır (Berber vd 2009: s. 111; Küzeci, 2010: s. 131; Atak, 2010: s. 94). Daha açık ifadeyle Sözleşmeyle, kişisel verilerinin korunması amaçlanmıştır.

Sözleşme'nin uygulama alanı ise 3. maddede belirtilmiştir. Bu düzenlemeye göre, Sözleşme kamusal ve özel sektörde kişisel verilerin otomatik yollarla işlenmesi halinde uygulanacaktır. Bu düzenleme ile Sözleşme'nin uygulama alanı dar tutulmuştur. Sözleşme yalnızca gerçek kişilere ait veriler için koruma sağlamakta ayrıca verilerin otomatik olmayan yollarla işlenmesini kapsamamaktadır (Atak, 2010: s. 95).

Sözleşmeye taraf devletler kendi ülkelerinde bulunan herkes için geçerli olacak şekilde bu metinde yer alan ilkeleri iç hukuk düzenlerinin parçası durumuna getirme yükümlülüğü altındadır. Sözleşmenin 4. Maddesi uyarınca, her taraf devlet, en geç bu Sözleşme kendisi açısından yürürlüğe girinceye kadar, burada yer alan

ilkelere etkinlik kazandırmak için kendi ulusal hukukunda gerekli düzenlemeleri yapmak zorundadır⁷⁷.

Sözleşme'nin yalnızca otomatik yollarla işlenen kişisel veriler açısından güvenceler öngörmesi Sözleşme'nin eksikliklerinden biri olduğu doktrinde ifade edilmiştir⁷⁸. Ancak Sözleşme ile kişisel verilerin korunmasma yönelik "asgari" gereklilikler belirlenmiştir. Bu nedenle taraf devletlerin daha geniş bir koruma getirmesi önünde herhangi bir engel bulunmamaktadır⁷⁹.

Sözleşmenin 5. maddesinde, kişisel verilerin tutulmasında göz önünde bulundurulması gereken ilkeler de belirlenmiştir. Buna göre veriler (Şimşek, 2008: s. 23; Kılınç, 2012:s. 1114; Özdemir, 2009: s. 21);

- 1- Hukuka ve dürüstük kurallarına uygun olarak elde edilmeli ve işlenmelidir.
- 2- Belli ve meşru amaçlar için kaydedilmeli ve bu amaca aykırı şekilde kullanılmamalıdır.
- 3- Kaydedildikleri amaca göre uygun ve elverişli olmalı ve aşırı olmamalıdır.
- 4- Doğru ve gerektiğinde güncel olarak saklanmalıdır.
- 5- İlgili kişilerin kimliklerini belirtecek bir biçim altında ve kaydedildikleri nihai amaç için gerekli görülen süreyi aşmayacak bir süre için muhafaza edilmelidir.

Sözleşmenin 6. maddesine göre, hassas nitelikte kişisel veriler özel olarak korunmalıdır; bu kapsamda, kişilerin ırkı kökenlerine, siyasi görüşlerine veya dini veya diğer inanışlarına, aynı şekilde sağlık veya cinsel hayatlarına ve ceza mahkûmiyetlerine ilişkin bilgiler, ilgili devletin ulusal hukuku uygun garantiler sağlamadığı sürece otomatik olarak işlenemeyeceklerdir (Atak, 2010: s. 96; Küzeci, 2010: s. 132).

Kişisel verilerin işlenmesinde yer alan hassaslık ilkesi, hassas verilerin işlenmesinde sıradan verilerin işlenmesine nazaran daha katı denetim kurallarının var olması anlamına gelmektedir (Kaya, 2011: s. 324). Bu nedenle Sözleşmenin 6. maddesinde, ulusal hukuka uygun güvenceler alınmadıkça hassas verilerin otomatik

⁷⁷ **Küzeci**, s. 132; Türkiye bu Sözleşmeyi 28 Ocak 1981 tarihinde imzalamış olmasına karşın, halen iç hukukta gereken düzenlemeler yapılmadığı için Sözleşmenin onaylanması işlemi tamamlanmamıştır.

⁷⁸ **Atak**, s. 95

⁷⁹ Bkz. 108 nolu Sözleşme m.11

olarak işlenemeyeceği hükme bağlanmıştır⁸⁰. Ancak Sözleşmede hassas verilerin istisnai olsada işlenebilmesi için alınması gereken güvencelerin neler olabileceği belirtilmemiştir.

Sözleşmenin 7. Maddesine göre veri güvenliğine ilişkin hükümler içermektedir. Buna göre, otomatik veri dosyalarında saklanan kişisel verilerin kazara veya yetkisiz tahribatlara veya kazara söz konusu olabilecek kayıplara karşı korunması, aynı şekilde bu verilere yetkisiz erişim, değiştirme veya yaymalara karşı da korunması için uygun güvenlik önlemleri alınmalıdır. Ülkeler, verilerin güvenliğinin sağlanması için gerekli hukuksal düzenlemeleri yapmalıdır (Atak, 2010: s. 96).

Diğer yandan Sözleşmenin 8. maddesinde bireylerin haklarında tutulan kayıtlara ulaşma hakkı düzenlenmiştir. Buna göre herkes kendisi ile ilgili kişisel nitelikteki veri bulunup bulunmadığını bilme ve erişme, bu bilgilerin anlaşılır bir biçimde kendisine bildirilmesini sağlama, gerekli olan durumlarda, bu verileri düzelttirme veya sildirtme haklarına sahip olmalıdır. Ayrıca bu maddede belirtilen güvencelerin yerine getirilmemesi durumunda ilgili kişiye hukuksal yollara başvurabilme hakkı da tanınmalıdır (Şimşek, 2008: s. 24; Atak, 2010: s. 96).

Sözleşmenin 9. Maddesinde bu hakların kullanımına bazı sınırlamalar getirildiği ancak burada sınırlamaların sınırsız olmadığı görülmektedir. Buna göre, sınırlamalar ancak yasa ile ve eğer demokratik bir toplumda gerekli ise; devletin ya da kamunun güvenliği, devletin ekonomik çıkarlarının korunması, suçlarla mücadele veya ilgili kişinin ya da başkaları hak ve özgürlüklerinin korunması amacıyla yapılabilecektir. Burada AİHS'nin özel yaşamın gizliliği hakkını düzenleyen 8. maddesinin 2. fıkrasındaki sınırlamalara koşut bir düzenleme getirildiği görülmektedir (Küzeci, 2010: s. 133; Atak, 2010: s. 97).

108 sayılı Sözleşme taraf devletlere, yukarıda açıklandığı üzere, önemli yükümlülükler getirmektedir. Her şeyden önce Sözleşme'ye taraf olacak ülke, iç hukukunda bir yasayla verilerin hukuki rejiminin tanımlanması gereklidir. Bu nedenle bu Sözleşme, doğrudan uygulamaya elverişli olmayıp, bir uygulama yasası aracılığıyla hükümlerinin ayrıntılandırılması ve ülke şartlarına uydurulması

⁸⁰ Kılınç, s. 1114; Kaya, “..Hassas Veriler”, 2011, s. 327

gerekmektedir. İç hukuklarda yürürlüğe konulan bu yasalar ile hem Sözleşme'nin etkili hale gelmesi sağlanmış olacak hem de kişisel verilerin işlenmesi konusunda ortak temel güvenceler sağlanacaktır (Atak, 2010: s. 97).

2.3.3. Avrupa İnsan Hakları Sözleşmesi

2.3.3.1. Genel Olarak

Avrupa Konseyi bünyesinde kişisel verilerin korunmasına ilişkin diğer bir önemli metin Avrupa İnsan Hakları Sözleşmesidir. 4 Kasım 1950'de Roma'da imzalanan ve Türkiye tarafından da 18 Mayıs 1954 tarihinde onaylanmış bulunan İnsan Haklarının ve Temel Özgürlüklerin Korunmasına Dair Avrupa Sözleşmesi, kısa ve yaygın adıyla Avrupa İnsan Hakları Sözleşmesi (AİHS), Avrupa Konseyi'nin faaliyetleri kapsamında hazırlanarak yürürlüğe konulmuş bir uluslararası sözleşmedir. Sözleşmenin taraf devletlerce uygulanıp uygulanmadığının denetimi, önce Avrupa İnsan Hakları Komisyonu ve Avrupa İnsan Hakları Mahkemesi (AİHM) tarafından yapılmaktayken, Komisyon'un kaldırılmasıyla, yalnızca Avrupa İnsan Hakları Mahkemesi tarafından yapılmaktadır (Berber, vd 2009: s. 103).

AİHS, uygulanmaya başlandığından bugüne, insan hakları alanında en önemli kaynaklardan biri olma özelliğini korumaktadır⁸¹. Ancak, daha öncede belirttiğimiz üzere AİHS'de kişisel verilerin korunması, bağımsız bir hak olarak yer almamıştır.

Kişisel verilerin korunması hakkı, AİHS'nde özel olarak düzenlenmese de, Sözleşmenin yorumcusu ve uygulanması takip etmekle görevli AİHM tarafından, Sözleşmenin 8. maddesinde düzenlenen “özel hayatın gizliliği hakkı” kapsamında değerlendirilmiştir (Şen, 1996: s. 73; Tezcan vd 2004: s. 385; Doğru ve Nalbant, 2013: s. 6; Akyürek, 2011: s. 47).

Avrupa İnsan Hakları Sözleşmesi'nin, “Özel Hayata ve Aile Hayatına Saygı Hakkı” kenar başlığını taşıyan 8. maddesi şöyledir:

“1) Herkes özel ve aile hayatına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahiptir.

⁸¹ AİHS hakkında ayrıntılı bilgi için bkz. **Özdek**, s. 28-73

2) *Bu hakkın kullanılmasına bir kamu otoritesinin müdahalesi, ancak millî güvenlik, kamu emniyeti, ülkenin iktisadî refahı, dirlik ve düzenin korunması, suç işlenmesinin önüne geçilmesi, sağlığın veya ahlâkın veya başkalarının hak ve hürriyetlerinin korunması amacıyla, demokratik bir toplumda gerekli görülen ölçüde ve kanunla düzenlenmesi şartıyla söz konusu olabilir."*

Maddede yer alan "saygı gösterilmesi" ifadesi, devletin yalnızca müdahalede bulunmamayı değil, aynı zamanda bu hakların fiilen ve gerçekten kullanılmasına olanak verecek önlemleri alma konusunda pozitif bir yükümlülük yüklendiğini de ifade etmektedir. Bu nedenle, maddeyle özel yaşamın korunması konusunda taraf devletlere bu hakka keyfî müdahalede bulunmayı yasaklayan negatif bir yükümlülük yüklendiği gibi aynı zamanda bu hakkın korunmasına yönelik olarak ta gerekli önlemleri alma yönünde pozitif bir yükümlülük te yüklenmiştir (Atak, 2010: s. 102).

Devletin negatif yükümlülüğü, özel yaşamın korunması amacıyla belirli eylemleri yapmaktan kaçınmasını ifade etmektedir. Kişisel verilerin korunması açısından devletin negatif yükümlülüğü, Sözleşme'ye aykırı olarak kişisel verileri toplama, saklama ve işleme gibi müdahalelerden kaçınmasını ifade ettiği söylenebilir. Devletin pozitif yükümlülüğü ise, özel yaşam hakkına saygıyı güvence altına almak için gerekli önlemleri almasını ifade etmektedir. Pozitif yükümlüğün kişisel verilerin korunması açısından anlamı ise Devletin kişisel verilerin gizliliğini güvence altına alabilmek için, kişisel verileri koruyacak kuralları yürürlüğe koyması ve gerekli güvenceleri sağlamasıdır (Atak, 2010: s. 102).

Diğer taraftan AIHS'nin 8. maddesi ile dört alanda koruma getirilmektedir: bunlar kişinin; özel yaşamı, aile yaşamı, evi ve haberleşmesidir. Özel yaşamın korunması hakkı bu dört alan içerisinde en geniş kapsamlı olanıdır. Bu kapsama kişisel verilerin korunmasına ilişkin temel ilkelerin dâhil olup olmadığını saptayabilmek için Avrupa İnsan Hakları Mahkemesinin kararlarına başvurmak gerekir (Küzeci, 2010, s. 136).

Avrupa İnsan Hakları Mahkemesinin kararlarına genel olarak bakıldığında, Mahkemenin; 8. maddenin 1. fıkrasında sayılan "aile" veya "konut" gibi unsurlara bakmadan, doğrudan özel hayat kavramı üzerinden değerlendirme yaptığını ve özel hayat kavramını geniş bir şekilde yorumlayarak kişisel verileri de bu kapsamda

değerlendirdiği görülmektedir. Mahkeme kararlarına göre, kişilerin fizikî ve sosyal kimlikleri, **kişisel bilgileri**, cinsiyetleri, şahıslarına ait özerk sahaları, adları, fizikî ve ruhsal bütünlükleri, iş ilişkileri, sosyal etkinlikleri, kişisel gelişimi, fizikî ve moral güvenliği, dış çevrede insanlarla ilişkiler geliştirmesi ve özel hayatına dair bilgilerin açıklanması, “özel hayat” kavramı içinde değerlendirilmelidir (Gözübüyük ve Gölcüklü, 2004: s. 331; Şen, 1996: s. 70).

2.3.3.2. Kişisel Verilerin Korunmasına İlişkin AİHM Kararları

Avrupa İnsan Hakları Mahkemesi, kişisel verilerin korunmasıyla bağlantılı başvurulara ilişkin verdiği kararlarda, kişisel verilerin özel yaşam alanı içinde yer aldığını belirtmekte ve kişiye ilişkin bu verilerin toplanması, saklanması ve açıklanmasıyla ilgili sorunları da Sözleşme'nin 8. maddesi içinde ele almaktadır (Atak, 2010: s. 103).

Bu minvalde yapılan başvurularda Mahkeme öncelikle, yapılan işlemin ya da alınan önlemin Sözleşme'nin 8. maddesinde güvence altına alınan özel yaşam hakkına yönelik bir müdahale oluşturup oluşturmadığını değerlendirmekte; bir müdahalenin olduğuna kanaat getirmesi durumunda ise bu müdahalenin ulusal yasalara uygunluğunu incelemektedir. Ancak Mahkeme müdahalenin ulusal yasalara uygunluğunu yeterli bulmamakta ayrıca ulusal yasanın hem Avrupa İnsan Hakları Sözleşmesi'ne hem de 108 sayılı Sözleşme'ye uygun olup olmadığını değerlendirmektedir (Atak, 2010: s. 103).

Bu kapsamda Mahkemenin konuyla ilgili önemli kararlarını incelemekte fayda bulunmaktadır. Zira bu kararlarda kişisel veri ve hassas kişisel veri kavramları ile verilerin hukuka uygun işlenip işlenmediğine ilişkin yapılan tespitler, son bölümde kişisel verilere karşı işlenen suçların incelenmesi sırasında konuya ışık tutacak niteliktedir.

2.3.3.2.1. Klass ve Diğerleri v. Almanya Kararı

Mahkeme'nin bu konuyu ele aldığı ilk dava Klass ve Diğerleri v. Almanya davası olmuştur⁸². Mahkeme kararında kişisel verilerden bahsetmese de bu davada verdiği kararla, istihbarat örgütlerinin gizli izleme yoluyla bireylerin haklarına

⁸² Klass and Others v. Germany, 5029/71, 06.09.1978.

yönelik gerçekleştirdikleri müdahalelerin etkili bir denetime tabi olması gerektiğini kabul etmiş ve ulusal güvenlikten kaynaklanan ihtiyaçlara her durumda öncelik verilemeyeceğini, Avrupa ülkelerinin casusluk ve terörizmle mücadeleyi gerekçe göstererek uygun gördükleri her türlü tedbiri alamayacaklarını belirtmiştir (Atak, 2010: s. 103-104).

Mahkeme bu davada, mektupların ve telgrafların okunmasına, telefon görüşmelerinin dinlenmesi ve kaydedilmesine olanak tanıyan bir yasanın Sözleşme'ye uygunluğunu incelemiştir. Mahkeme genel olarak gizli izleme yöntemlerine demokratik kurumların korunması için kesinlikle zorunlu olması durumunda başvurulabileceğini kabul etmiş ise de, bireyin 8. maddede güvence altına alınan hakkı kullanabilmesi ile demokratik bir toplumu koruma amacıyla gizli izlemenin yapılmasının gerekliliği arasında da bir denge kurulması gerektiğini belirtmiştir. Mahkeme'ye göre, *“bu konuda devletlerin sınırsız bir takdir yetkisi yoktur. Zira sınırsız önlemler alınmasına izin veren bir yasa demokrasi için tehdit oluşturur. Gizli izlemeye olanak tanınması durumunda bunun kötüye kullanılmasının engellenmesi için yeterli ve etkili güvencelerin sağlanması gerekir. İzleme ancak başka bir yöntemle bilgilere ulaşamıyorsa yapılmalı, yazılı izin şartı aranmalı ve belli bir süreyle sınırlı tutulmalıdır. İzlemeyi gerektiren nedenlerin ortadan kalkması durumunda izlemeye son verilmeli, elde edilen veriler başka bir amaç için kullanılmamalı, izlemenin amacının gerçekleşmesi durumunda veriler en kısa süre içinde imha edilmelidir.”* Mahkeme, mevcut yasanın bu güvenceleri sağladığını saptamış ve bu nedenle 8. maddenin ihlal edilmediğine karar vermiştir (Atak, 2010: s. 104; Şimşek, 2008: s. 32).

2.3.3.2.2. Leander-İsveç Kararı

Bu konuyla ilgili Mahkemenin ikinci kararı 26 Mart 1987 tarihli **Leander-İsveç** kararıdır⁸³. Mahkeme bu kararı kişisel verilerin korunmasının 8. maddenin 1. fıkrası kapsamında olduğu tespiti nedeniyle önemlidir. Bu bağlamda kişisel verinin kaydedilmesi, kullanılması ve ilgilinin hakkında toplanan bilginin aksini ispat isteminin reddedilmesi hallerinde özel hayat hakkı ihlal edilmiş olacaktır (Akyürek, 2011: s. 47). Bir başka deyişle AIHM, Leander-İsveç davası kararında, kişinin aleyhinde bilgi toplama faaliyetlerinin 8. maddenin 1. fıkrasının ihlali anlamına

⁸³ 26 Mart 1987, Seri A No. 116, s. 22 ve 25-27, paragraf 48, 60, 65 ve 67

geldiğine karar vermiştir. Davaya konu olay, Devlet yetkilileri tarafından Bay Leander hakkında toplanan bilgilere dayanılarak, Bay Leander'in bir deniz üssündeki göreve getirilmemesidir. Söz konusu bilgi toplama faaliyetinin, ulusal güvenliğin devam ettirilebilmesi için demokratik bir toplumda zorunlu olduğu İsveç Devleti tarafından savunulmuştur. AİHM, bu davada şu gözlemlerde bulunmuştur (Dutertre, 2007: s. 309):

“Gizli polis kayıtlarında Bay Leander'in özel hayatıyla ilgili bilgiler olduğuna karşı çıkılmamaktadır. Bu bilgilerin saklanması ve açıklanması ve bir de Bay Leander'a bu duruma karşı çıkma hakkı verilmemesi, 8. Madde 1. fıkra da teminat altına alınmış olan özel hayata saygı gösterilmesi hakkına müdahale edilmesi anlamına gelmektedir.” Ancak AİHM gerekçesini belirtirken, bu müdahalenin 2. fıkra kapsamında haklı olduğuna karar vermiştir. İsveç Devlet'i, söz konusu sicilin adayların deniz üssündeki göreve atanmasında yardımcı olmak amacıyla hazırlandığını ve bunun güvenlik nedeniyle yapıldığını savunmuştur. AİHM, Bay Leander hakkındaki bilgilerin saklanması, demokratik bir toplumda ulusal güvenliği sağlamak için gerekli olduğuna karar vererek bu görüşü kabul etmiş ancak, söz konusu sicilin varlığının ve kullanımının bazı koruyucu önlemlere tâbi olması gerektiğini belirtmiştir (Dutertre, 2007: s. 309):

“Mahkeme, ulusal güvenliği korumaya yönelik bir gizli izleme sisteminin, demokrasiyi korumak adına demokrasiye zarar vermesi, hatta demokrasiyi ortadan kaldırması riski yarattığını göz önünde bulundurarak, istismara karşı yeterli ve etkin teminatların olduğundan tatmin olmalıdır. Mahkeme, Ulusal Polis Kurulu'nda milletvekillerinin olmasına ve Adalet Bakanı'nın ve Meclis Denetçisi'nin yanı sıra Meclis Adalet Kurulu'nun bu konudaki denetimine özellikle önem vermektedir. Komisyon gibi Mahkeme de, İsveç personel izleme sistemindeki koruyucu önlemlerin, 8. Madde 2. fıkrasının şartlarına uyduğu sonucuna ulaşmıştır. Davalı Devlet'e sağlanan geniş takdir payı göz önünde bulundurulduğunda davalı Devlet'in, bu davada, ulusal güvenlik konusundaki çıkarlarının başvuru bireyin çıkarlarından daha üstün olduğu kanaatine sahip olmaya hakkı vardır. Bu nedenle, Bay Leander'in maruz kaldığı müdahalenin güdülen meşru amaca göre orantısız olduğu söylenemez.”

Mahkeme bu davada, kamusal nitelikli verilerin de sistematik olarak toplanıp kaydedilmesi halinde özel hayata dâhil olabileceğini, hele de kişinin uzak geçmişi söz konusu ise bunun daha da belirgin olduğunu söylemiş ve kişiler hakkında bilgi toplama ve bu bilgileri saklama sistemi ile ilgili önemli bazı ayrıntılara değinmiştir⁸⁵. Bu nedenle bu kararı önemine binaen ayrıntılı incelemekte fayda bulunmaktadır. Mahkeme kararında (Dutertre, 2007: s. 288-289):

“Hükümet, RIS’nin 19 Aralık 1990 tarihli mektubunun başvurusunun özel hayatıyla değil, kamu hayatıyla ilgili olduğunu iddia ederek 8. Madde’nin uygulanamaz olduğunu ileri sürmüştür. Başvurucu, siyasi faaliyetlerde bulunmaya ve broşür bastırmaya karar vererek, özel hayatın doğasında olan “gizlilik” (anonymat) hakkından zımni olarak feragat etmiştir. Polis tarafından sorguya çekilmiş olması ve sabıka kaydı ise kamuya açık bilgilerdir.

Mahkeme, bir bireyin özel hayatına ait bilgilerin gizli bir sicilde saklanması ve bu tür bilgilerin açıklanmasının 8. Madde 1. fıkranın kapsamına girdiğini tekrar beyan eder (bkz. Leander-İsveç davası kararı, 26 Mart 1987, Seri A No. 116, s. 22, paragraf 48).

Özel hayata saygı duymak, başka insanlarla ilişkiler kurmayı ve bu ilişkileri geliştirmeyi de belirli bir derecede içermelidir; ayrıca meslekle veya işle ilgili faaliyetleri “özel hayat” kavramının dışında tutmayı gerektiren bir ilkeden söz edilemez (bkz. Niemietz-Almanya davası kararı, 16 Aralık 1992, Seri A No. 251-B, s. 33-34, paragraf 29 ve Halford-Birleşik Krallık davası kararı, 25 Haziran 1997, Reports 1997-III, s. 1015-1016, paragraf 42-46.)

Mahkeme, bu kararında ayrıca Avrupa Konseyi’nin 28 Ocak 1981 tarihli ve 1 Ekim 1985’de yürürlüğe girmiş olan Şahsi Verilerin Kendiliğinden İşlenmesi Konusunda Bireylerin Korunması konulu Sözleşmeye atıfta bulunmuş; bu belgenin amacının, “bütün bireylerin haklarına ve temel özgürlüklerine ve özellikle kendisine ait şahsi verilerin kendiliğinden işlenmesi konusunda mahremiyetine saygı gösterilmesini [...] sağlamak olduğunu, kişisel verilerin ise 2. Madde’de tanımlandığı üzere “kimliği belirli veya belirlenebilecek bir bireye ait her türlü bilgi” olarak

⁸⁵ 4 Mayıs 2000 tarihli karar, Başvuru No. 28341/95, paragraf 42-44. Bkz. Akçürek, 2011: s. 47

tanımlandığını belirtmiştir (bkz. Amann-İsviçre [BD], No. 27798/95, paragraf 65, AİHM 2000-II). Kararda ayrıca;

“Mahkeme, bir bireyin özel hayatına ait bilgilerin gizli bir sicilde saklanması ve bu tür bilgilerin açıklanmasının 8. Madde 1. fıkranın kapsamına girdiğini tekrar beyan eder.

Ayrıca kamuya açık bilgiler, düzenli olarak toplandığında ve yetkili makamlar tarafında dosyalarda saklandığında da özel hayat kapsamına girebilir. Bu durum, özellikle söz konusu bilgiler kişinin geçmişine aitse daha da geçerlidir.” şeklinde tespitlerde bulunmuştur.

Bu davada Mahkeme, RIS’nin 19 Aralık 1990 tarihli mektubunda, bir kısmı elli yıldan uzun bir süre önce toplanmış olan, başvurunun hayatıyla ve özellikle eğitimi, siyasi faaliyetleri ve sabıka kaydıyla ilgili bazı bilgiler olduğuna dikkat çekmiştir. Mahkeme’nin görüşüne göre, bu tür bilgiler düzenli olarak toplandığında ve Devlet’in yetkilileri tarafından dosyada saklandığında, AİHS’nin 8. Madde 1. fıkrası açısından “özel hayat” kapsamına girmektedir. Özellikle bu davada, bilgilerin bir kısmı yanlış olduğu ve başvurunun itibarını zedeleyebileceği için, bu durum daha da geçerlidir. Bu nedenle 8. Madde ihlal edilmiştir (Dutertre, 2007: s. 289).

2.3.3.2.4. Amann-İsviçre Kararı

Kişiler hakkında hukuka aykırı olarak bilgi toplanması, başka bir deyişle kişilerin “fişlenmesi” özel hayata müdahale oluşturacaktır (Tezcan vd. 2004: s. 386). Bu nedenle 8. maddeye göre, bunun ayrıntılı bir şekilde kanunla düzenlenmesi gerekmektedir. Bu çerçevede AİHM’in 16.2.2000 tarihli **Amann-İsviçre Kararı** güzel ve önemli bir örnektir. Karara konu olan olayda; Bir iş adamı olan başvurucuyu Sovyet Büyükelçiliği’nde çalışan bir bayan, telefonla arayarak bir ürün siparişi vermiştir. Büyükelçilik telefonlarını dinleyen İsviçre Federal Savcılığı başvurucu hakkında bir fiş oluşturmuştur. Savcılıkta tutulan kayıta, başvurana ilişkin “ticaret yaptığı” ve “Rus Elçiliği nezdinde temas noktası” olduğu yazılmıştır. Söz konusu olay 1981 yılında gerçekleşmiştir. Kendisi hakkında tutulan fişin varlığını 1990 yılında öğrenen başvurucu tazminat talebinde bulunmuş ancak bu talebi İsviçre makamları tarafından reddedilmiştir. Başvuruyu inceleyen Mahkeme, telefon görüşmelerinin dinlenmesi ve kayda alınmasının ve bireyin özel yaşamına ilişkin bilgilerin kamu görevlileri tarafından saklanması özel yaşama bir müdahale

oluşturduğunu kabul etmiştir. Mahkeme, yapılan müdahalenin yasaya dayanılarak yapıldığını saptamış ancak mevcut yasal düzenlemenin yeterli korumayı sağlamadığını açıklamıştır. Mevcut yasa savcılık makamının veri toplama, kaydetme ve saklama yetkisini kullanma koşullarını ve kapsamını belirlememekte, hangi bilgilerin saklanacağı ve nasıl bir yöntem izleneceği konusunda açıklık içermemektedir. Bu nedenden dolayı 8. maddenin ihlali söz konusu olduğuna kara vermiştir (Atak, 2010: s. 108) .

Karara göre, Savcılıkta tutulan kayıta, başvurana ilişkin “ticaret yaptığı” ve “Rus Elçiliği nezdinde temas noktası” olduğunun yazılması başvuranın özel hayatına müdahale oluşturmaktadır. Mahkemeye göre bu bilgi daha sonra ister kullanılsın, ister kullanılsın 8. madde kapsamına girer. Şayet mevcut yasa hükmü bu bilgilerin toplanmasını, kaydedilmesini, saklanmasını ve gereksiz hale geldiğinde imhasını düzenlemiyorsa, 8. maddenin ihlali söz konusu olur. Bu nedenle özellikle suçların aydınlatılması ve önlenmesi ile devlet güvenliği gerekçeleriyle kişiler hakkında gizli yollarla veri elde etme eylemleri bakımından 8. maddenin özel bir garanti içerdiği belirtilmiştir (Tezcan vd. 2004: s. 387).

2.3.3.2.5. P.G. ve J.H. - Birleşik Krallık Kararı

Benzer şekilde, AİHM, P.G. ve J.H.-Birleşik Krallık kararında (25 Eylül 2001, Başvuru No. 44787/98, paragraf 56-60) önceki içtihatlarının adeta bir özetini vermiştir. Bu dava, yakalanan kişilerin hem nezarethanede, hem de polis tarafından haklarındaki suçlamalar okunurken seslerinin kaydedilmesi ile ilgilidir. Söz konusu kişilere haber verilmeden yapılan bu kayıtlar, apartman dairelerinde yapılmış olan başka kayıtlarla karşılaştırılmak amacıyla hazırlanmıştır. AİHM, bu konuda şöyle demiştir (Dutertre, 2007: s. 290):

“Özel hayat, kapsamlı bir tanım yapılamayacak kadar genel bir terimdir. Mahkeme, cinsiyet belirleme, isim ve cinsel tercih ve cinsel hayatın, 8. Madde’nin korumasına giren özel alanın önemli unsurları olduğunu daha önce belirtmiştir (bkz. örneğin B.-Fransa davası kararı, 25 Mart 1992, Seri A No. 232-C, paragraf 63; Burghartz-İsviçre davası kararı, 22 Şubat 1994, Seri A No. 280-B, paragraf 24; Dudgeon-Birleşik Krallık davası kararı, 22 Ekim 1981, Seri A No. 45, paragraf 41; ve Laskey, Jaggard ve Brown-Birleşik Krallık davası kararı, 19 Şubat 1997, Reports 1997-I, paragraf 36). 8. Madde ayrıca kimlik ve kişisel gelişim hakkını ve başka

insanlarla ve dış dünyayla ilişkiler kurma ve bu ilişkileri geliştirme hakkını da korumaktadır (bkz. örneğin Burghartz-İsviçre, 21 Ekim 1992 tarihli Komisyon raporu, a.g.e. paragraf 47; ve Friedl-Avusturya, No. 15225/89, 19 Mayıs 1994 tarihli Komisyon raporu, Seri A No. 305-B, paragraf 45). **Mesleki veya işle ilgili faaliyetleri de içerebilir** (bkz. Niemietz-Almanya davası kararı, 16 Aralık 1992, Seri A No. 251-B, paragraf 29; ve Halford-Birleşik Krallık kararı, 25 Haziran 1997, Reports, 1997-III, paragraf 44). **Bu nedenle, bir bireyin başkalarıyla girdiği etkileşimlerin bir kısmı, kamusal bir bağlamda yapılsa bile, “özel hayat” kapsamına girebilir.**

Bir kişinin evinin veya özel mülkünün dışında alınan önlemlerin, kişinin özel hayatına dahil olup olmadığının belirlenmesinde göz önünde bulundurulması gereken birkaç unsur vardır. İnsanlar bazen kamuya açık bir biçimde kaydedilebilen veya rapor edilebilen faaliyetlere bilerek veya kasten dahil olabildikleri için, kişinin mahrumiyet hakkındaki makul beklentileri, kararı belirleyen etken olmasa da, önemli olabilir. Sokakta yürüyen bir kişi, kaçınılmaz olarak orada bulunan diğer kişiler tarafından görünür olacaktır. Teknolojik yöntemlerle aynı kamusal mekânın izlenmesi de (örneğin kapalı devre televizyon ile güvenlik görevlilerinin izlemesi) benzer özelliktedir. **Ancak kamu alanındaki bu tür bilgilerin düzenli veya kalıcı olarak kaydı söz konusu olunca, özel hayatla ilgili konular ortaya çıkmaktadır. İşte bu nedenle güvenlik görevlileri tarafından belirli bir birey hakkında toplanan dosyalar, söz konusu bilgi müdahaleci veya gizli bir yöntemle toplanmamış olsa bile, 8. Madde kapsamına girer** (bkz. Rotaru-Romanya [BD], No. 28341/95, AİHM 2000-V, paragraf 43-44). Mahkeme, bu bağlamda Avrupa Konseyi’nin 28 Ocak 1981 tarihli, 1 Ekim 1985’de yürürlüğe girmiş olan Şahsi Verilerin Kendiliğinden İşlenmesi Konusunda Bireylerin Korunması konulu Sözleşmeye daha önce atıfta bulunmuştur; bu belgenin amacı, “bütün bireylerin [...] haklarına ve temel özgürlüklerine ve özellikle kendisine ait şahsi verilerin kendiliğinden işlenmesi konusunda mahremiyetine saygı gösterilmesini [...] sağlamaktır”; bu tür veriler 2. Madde’de “kimliği belirli veya belirlenebilecek bir bireye ait her türlü bilgi” olarak tanımlanmıştır (bkz. Amman-İsviçre [BD], No. 27798/95, AİHM 2000-II, paragraf 65-67).

Fotoğraflar söz konusu olduğunda, 8. Madde’nin sunduğu korumanın içeriğini yetkili makamların keyfi müdahalesine karşı korumak amacıyla Komisyon,

ister özel, ister kamusal olaylarla ilgili olsun ve ister sınırlı kullanım amaçlı, ister kamuya açık olsun, fotoğraf çekmenin bir bireyin özel hayatına müdahale olup olmadığını değerlendirmiştir (bkz. Friedl-Avusturya, No. 15225/89, 19 Mayıs 1994 tarihli Komisyon raporu, Seri A No. 305-B, s. 21, paragraf 49-52). Komisyon, başvurucunun fotoğraflarının kamuya açık bir yerde yapılan genel bir gösteride çekildiği ve polis dosyalarında saklandığı bir davada, söz konusu fotoğrafın yapılan gösterinin bir kaydı olarak çekildiğine ve saklandığına ve fotoğrafta görülen kişilerin kimliklerini belirlemek için veri işleme yöntemleri kullanılarak herhangi bir şey yapılmadığına ağırlık vererek müdahale olmadığına karar vermiştir (bkz. yukarıda belirtilen Friedl-Avusturya davası, paragraf 51-52).”

Görüldüğü gibi mahkeme, telefon konuşmalarının gizli olarak kaydedilmesinin 8. maddede güvence altına alınmış olan özel yaşama ve haberleşmeye saygı hakları kapsamına girdiği tespitini birden fazla davada yapmıştır.

Genellikle söz konusu kayıtlar, konuşmalarının içeriğinin bir şekilde kullanılması amacıyla yapılırken, Mahkeme ses örneği olarak kullanılmak amacıyla yapılan kayıtların 8. madde kapsamındaki sunulan korumanın dışında kaldığı konusunda ikna olmamıştır. Çünkü söz konusu kişinin sesinin kalıcı bir kaydı alınmıştır ve bu ses, şahsi veriler açısından ilgili kişinin kimliğinin belirlenmesi amacıyla analiz edilebilir niteliktedir. Başvurucular, kendilerine suç isnat edildiği sırada, polis memurlarının onları dinlediği bir yerde kendilerine sorulan resmi sorulara yanıt veriyor olmasına rağmen, **mahkeme tarafından, seslerinin kaydı ve analizi, başvuruçular hakkında kişisel veri olarak değerlendirilmiştir** (Dutertre, 2007: s. 290).

Sonuç olarak Mahkeme, başvuruçuların seslerinin suç isnat edilirken ve polis hücrelerinde kaydedilmesinin, AİHS 8. Madde 1. fıkra kapsamında özel hayata saygı gösterilmesi hakkına müdahale olduğu sonucuna varmıştır (Dutertre, 2007: s. 290).

2.3.3.2.6. Z.-Finlandiya Kararı

Mahkeme, 25 Şubat 1997 tarihli **Z.-Finlandiya kararında**, kişinin özel hayatına ve aile hayatına saygı hakkından yararlanabilmesi için kişisel verilerin korunmasının hayati önemi olduğuna işaret etmiştir. Hatta bu kararda başta sağlığa ilişkin gizli bilgiler olmak üzere bireye ilişkin bütün kişisel bilgilerin gizlilik hakkına

dâhil olduğunun vurgulanmış olması, Mahkemenin özel hayatın gizliliği hakkına verdiği önemi ve bunu yalnızca bazı kişisel verilerle kısıtlamadığını göstermesi açısından son derece ilgi çekicidir (Akyürek, 2011: s. 48). Söz konusu kararın bir diğer önemli yönü de kişisel verilerin özellikle tıbbi verilerin neden korunması gerektiğine işaret etmesidir. Bu nedenle kararın ayrıntılarına bakmak faydalı olacaktır (Dutertre, 2007: s. 310-312; Tezcan vd. 2004: s. 385):

“Z.-Finlandiya davasında, başvurucunun kocasıyla ilgili bir ceza davası için, başvurucudan önceden onay alınmadan hakkındaki gizli tıbbi bilgiler açıklanmıştır.

Mahkeme bu bağlamda, şahsi bilgilerin ve özellikle tıbbi verilerin saklanması, AIHS 8. Madde (madde 8) kapsamındaki özel hayata ve aile hayatına saygı gösterilmesi hakkı açısından çok önemli olduğunu göz önünde bulunduracaktır. Tıbbi verilerin gizliliğine saygı göstermek, AIHS’e taraf olan bütün Sözleşmeciler Devletler’in yasal sistemlerinin temel bir prensibidir. Sadece hastanın özel hayatına saygı göstermek değil, hastanın tıp mesleğine ve genel olarak sağlık hizmetlerine duyduğu güveni de korumak şarttır.

Böyle bir koruma olmazsa, tıbbi yardıma ihtiyacı olanlar doğru tedavi görmek için ve hatta tıbbi yardım almak için gerekli olan kişisel veya mahrem bilgileri açıklamaktan cayabilir; bu durum da hem kendi sağlıklarını, hem de bulaşıcı hastalıklar söz konusu olduğunda toplum sağlığını tehlikeye atarlar (bkz. 24 Ekim 1989’da Avrupa Konseyi Bakanlar Komitesi tarafından kabul edilen, sağlık hizmetleri ve toplumsal ortamlarda HIV enfeksiyonu ile ilgili etik meseleler konulu Tavsiye No. R (89) 14, özellikle açıklama bölümünde 165. paragraftaki tıbbi verilerin gizliliği ile ilgili genel gözlemler).

Bu nedenle ulusal kanunlar, AIHS 8. Madde’deki (madde 8) teminatlarla tutarsız olabilecek biçimde şahsi tıbbi verilerin bildirilmesini veya açıklanmasını önleyecek uygun önlemler içermelidir (bkz., gerekli değişikliklerle, Şahsi Verilerin Otomatik olarak İşlenmesi konusunda Bireylerin Korunması Amaçlı Konvansiyon, Avrupa Anlaşmaları Seri No. 108, Strasbourg, 1981, 3. Madde, paragraf 2.c, 5, 6, ve 9).

Yukarıdaki konular, bir kişinin HIV enfeksiyon durumuyla ilgili verilerin gizliliğinin korunması açısından özellikle önemlidir. Bu tür bilgilerin açıklanması,

kişinin özel ve aile hayatının yanı sıra sosyal durumunu ve iş durumunu kökten etkileyebilir, adının lekelenmesi veya toplumdan dışlanması riskini ortaya çıkartabilir. Bu nedenle söz konusu kişiye tanı konmasını veya bu kişinin tedavi edilmesini önleyebilir ve böylece toplumun bu salgını önleme çabalarına zarar verebilir (bkz. Tavsiye No. R (89) 14'un açıklama bölümü, paragraf 166-68). Bu nedenle, yapılan müdahalenin meşru amaçla orantılı olup olmadığı belirlenirken, bu tür bilgilerin gizliliğinin korunması terazide ağırlıklı olacaktır.

Bu tür müdahaleler, önemli bir kamu yararı olmadığı durumlarda, AİHS 8. Madde (madde 8) ile uyumlu olamaz. Bir bireyin HIV enfeksiyon durumunun çok mahrem ve hassas bir konu olduğu göz önünde bulundurularak, Devlet tarafından, başvurulmuş hastanın rızası olmadan söz konusu bilginin bildirilmesini veya açıklanmasını zorunlu kılan herhangi bir önlem, etkin bir koruma sağlamayı amaçlayan bütün önlemlerde olduğu gibi, Mahkeme tarafından çok ayrıntılı olarak incelenecektir (bkz., gerekli değişikliklerle, Dudgeon-Birleşik Krallık davası kararı, 22 Ekim 1981, Seri A No. 45, s. 21, paragraf 52; ve Johansen-Norveç davası kararı, 7 Ağustos 1996, Reports of Judgments and Decisions 1996-III, s. 1003-1004, paragraf 64).

Mahkeme aynı zamanda, hastanın çıkarının ve kamunun yararının bulunduğu tıbbi verilerin gizliliğine ilişkin koruma bazen suçların soruşturulması, suçluların takibi ve davaların kamuya açık olması gibi daha önemli konular önünde önem derecesini yitirebilir (bkz. gerekli değişikliklerle, 1981 tarihli veri koruma konvansiyonunda 9. Madde).

Söz konusu soruşturmadaki tedbirler bağlamında unutulmaması gereken, Mahkeme'nin, adli yargılama sırasında kullanılan delillerin yerindeliği konusundaki ulusal makamların değerlendirmelerinin yerine kendi görüşlerini koymasının uygun olmadığıdır (bkz. örneğin yukarıda bahsedilen Johansen davası kararı, s. 1006-1007, paragraf 73).

Kamunun şahsi bilgilere erişimi konusunda Mahkeme, bir yandan davaların kamuya açık olması, diğer yandan bu tür verilerin gizliliğinin korunması konusunda bir tarafın veya bir üçüncü şahsın çıkarları arasında âdil bir denge kurulması konusunda ulusal makamlara belirli bir takdir payı bırakılması gerektiğinin farkındadır. Bu takdir payının genişliği, söz konusu çıkarların doğası ve ciddilik

düzeyi, müdahalenin şiddeti gibi etkenlere göre değişir (bkz. örneğin *Leander-İsveç davası kararı*, 26 Mart 1987, Seri A No. 116, s. 25, paragraf 58; ve gerekli değişikliklerle, *Manoussakis ve Diğerleri-Yunanistan davası kararı*, 26 Eylül 1996, Reports 1996-IV, s. 1364, paragraf 44).”

Bu davada, başvurucunun tıbbi danışmanları, mahkeme emri gönderilerek tanıklığa zorlanmıştır. AIHM’nin görüşüne göre: “Başvurucunun doktorlarının ve psikiyatrlarının tanıklığa zorlanması ile ilgili emre gelince, Mahkeme bu önlemlerin Z’nin Finlandiya kanunlarına göre kocası aleyhine delil vermeme hakkını kullanması bağlamında alındığına dikkat çeker (bkz. yukarıdaki paragraf 14, 17 ve 21). Buradaki tek amaç, Z’nin tıbbi danışmanlarına danışarak X’in HIV enfeksiyonu olduğunu öğrendiğini veya bu durumdan şüphelendiğini belirlemektir. Bu delil, X’in sadece cinsel suçlar mı işlediği, yoksa HIV testinin pozitif sonucunun açıklandığı 19 Mart 1992 tarihinden önce işlenmiş iki suçla ilgili olarak, daha ciddi bir suç olan adam öldürmeye teşebbüs suçundan da mı suçlu olduğunu belirlemek için o dönemde önemliydi.

Yetkili ulusal makamların, beş suçun hepsiyle birlikte adam öldürmeye teşebbüs suçundan dolayı soruşturma yapmak ve X’i yargılamak konusundaki kamu yararının üstün olduğunu düşünmek konusunda haklı oldukları şüphe götürmez.

Mahkeme, Finlandiya kanunlarına göre, sadece çok sınırlı şartta, yani bir soruşturmaya ilgili olarak ve en az 6 yıl hapis cezası öngörülen ciddi suçların isnat edilmesi bağlamında, başvurucunun tıbbi danışmanlarının başvurucunun onayı olmadan hakkında delil vermeye zorlanabileceğine dikkat çeker (bkz. yukarıdaki paragraf 46). Tıbbi danışmanlar polise delil vermeyi reddettiği için polis, onları tanık yapabilmek için bir yargı makamı olan Şehir Mahkemesi’nden yetki almak zorundaydı (bkz. yukarıdaki paragraf 28). Soruşturma, tanık ifadelerinin dökümü dahil dava dosyasının gizli tutulmasını önceden emretmiş olan Şehir Mahkemesi’nin salonunda gizli olarak yapılmıştır (bkz. yukarıdaki paragraf 19 ve 23). Davaya dahil olan herkes, bilgileri gizli tutma yükümlülüğü altındaydı. Bu yükümlülüğü ihlal edenler, Finlandiya kanunlarına göre medeni hukuk ve/veya ceza hukuku kapsamında sorumlu tutulabilirdi (bkz. yukarıdaki paragraf 53 ve 56).”

Mahkeme ortaya koyduğu bu görüşler doğrultusunda, başvurucunun doktorlarından bilgi istenmiş olmasının ve başvurucunun tıbbi kayıtlarının

soruşturma dosyasına konulmasının izlenen meşru amaçla orantılı olduğunu açıklamış ve bu açılardan Sözleşme'ye bir aykırılık görmemiş ve söz konusu müdahalenin 8. maddenin ikinci fıkrasına göre haklı olduğu sonucuna ulaşmıştır (Dutertre, 2007: s. 312; Tezcan vd. 2004: s. 385; Atak, 2010: s. 116; Ayrıca Kilkelly, 2003: s. 41).

2.3.3.2.7. M. S. - İsveç Kararı

M.S-İsveç davasında⁸⁶ Mahkeme, bir kamu kuruluşunda saklanmakta olan başvurucuya ait tıbbî verilerin, hizmet alması amacıyla bir başka kamu kuruluşu olan sosyal sigortalar kurumuna verilmesini ihlâl addetmemiştir. Aktarılan verilerin sigorta talebiyle ilişkili olması, gizli tutulması ve herhangi bir suiistimal hâlinde yetkililere karşı ceza ve hukuk davası açabilme imkânının bulunması, Avrupa İnsan Hakları Mahkemesi tarafından yeterli ve orantılı bulunmuştur⁸⁷.

2.3.3.2.8. Friedl - Avusturya Kararı

Friedl-Avusturya davasında ise, izinsiz bir gösteri sırasında Viyana polisi tarafından fotoğrafları çekilen ve kişisel bilgileriyle beraber dosyalanan başvurucu, özel hayatına saygı gösterilmediği iddiasıyla Strazburg makamlarına müracaat etmiştir. Avrupa İnsan Hakları Komisyonu'nun kaldırılması dönemine denk gelen bu davada Komisyon, polislerin başvurucunun evine veya başka bir özel mekânına girmediğini, fotoğrafların kamuya açık ve birden fazla kişinin katıldığı bir gösteride çekildiğini, böyle bir uygulama yapılmasının sebebinin ise suçların soruşturulması olduğunu vurgulayarak, 8. maddenin ihlâl edilmediği kararına varmıştır. Ayrıca Komisyon, eski ceza davaları sebebiyle kayıt tutulması uygulamasının, özel hayata müdahale olarak değerlendirilmemesi ve söz konusu kayıtların, demokratik bir sistemde suçların önlenmesi için elzem görülmesi gerektiğini belirtmiştir⁸⁸.

Diğer bir olayda Komisyon, Birleşik Krallıkla terörle mücadele çerçevesinde gözaltına alınan kişilerin parmak izlerinin ve fotoğraflarının alınması ve bu kayıtların

⁸⁶ M. S. v. Sweden, 20837/92, 27.08.1997.

⁸⁷ Üzeltürk, 2004, s. 190; Ayrıca bkz. Yokuş, Handan Sevük, Türk Alman Tıp Hukuku Sempozyumu, "Tıp Ceza Hukukunun Güncel Sorunları- Tıp Ceza Hukukunda Kişisel Verilerin Açıklanması", Tebliğ, Ankara, 28 Şubat-1 Mart 2008; Güleç, Recep Aydın/ Sarıtaş, Hatice/Demirbaş, Sevil Neşeli, "Kişisel Sağlık Verilerinin Mahremiyeti", E-Yaklaşım Dergisi, S. 59, Haziran, 2008, s. 11-12

⁸⁸ Case of Friedl v. Avusturya, 15225/89, 31/01/1995, European Court of Human Rights Portal - Human Rights Documentation, <http://hudoc.echr.coe.int/>. Bkz. Berber/Ülgü/Er, s. 108

elde bulundurulmaya devam edilmesi konusunda, 8. maddenin ihlâl edildiğine dair bir karar vermemiştir. Benzer şekilde, cinayet şüphesiyle emniyette DNA örneği alınan ve kan testi yapılan başvurunun şikâyeti üzerine de Mahkeme, kan örneğinin alınmasının üzerinden 11 ay geçtikten sonra yok edildiğini ve bu zaman zarfında da başka amaçla kullanılmadığını göz önünde bulundurarak, bu sürenin bir cinayet soruşturması için makul olduğuna hükmetmiş ve Avrupa İnsan Hakları Sözleşmesi'nin ihlâl edilmediğine karar vermiştir (Üzeltürk, 2004: s. 193).

2.3.3.2.9. I v. Finlandiya Kararı

I v. Finlandiya kararı⁸⁹ değişik nedenlerle toplanan kişisel verilerin tutulması ve kullanılması ve bunlara kimlerin erişim sağlayabileceği konusunda önemli tespitler içeren bir karardır.

“I” rumuzlu, 1960 doğumlu başvuru, bir Finlandiya vatandaşıdır ve 1989-1994 yılları arasında bir devlet hastanesinde sözleşmeli hemşire olarak çalışmıştır. 1987 tarihinden itibaren aynı hastanenin bulaşıcı hastalıklar kliniğinde muayene olan başvurunun HIV virüsü taşıdığı ortaya çıkmış, 1992 tarihinden itibaren ise bazı meslektaşlarının hukuka aykırı bir şekilde bu bilgiye vâkıf olduğunu öğrenmiş, üç yıl sonra ise iş akdi yenilenmemiştir. Başvurunun şikâyeti, yetkili mercilerin kendi sağlık kayıtlarına haksız biçimde erişilmesini engelleyemediği yönünde olmuştur ve özel hayatın gizliliği hakkının ihlâl edildiğini ileri sürmüştür. Başvuruyu değerlendiren Mahkeme, AİHS'in 8. maddesinin ihlâl edildiğine oybirliğiyle karar vermiş, Finlandiya makamlarının başvurunun hasta kayıtlarını korumakta yetersiz kalarak hataya düştüğüne hükmetmiştir. Mahkeme karar gerekçesinde, kamu kurumlarının ve devletin, mahrem olarak saklanması gereken verileri, mahrem olarak saklamakta başarısız oldukları takdirde Avrupa İnsan Hakları Sözleşmesini ihlâl eder duruma düştüklerine hükmetmiştir. Olayda, başvuru hemşire, verilerin kasten ele geçirildiğini veya gizliliğin kasten bozulduğunu kanıtlamakla yükümlü görülmemiştir. Bu verilerin güvenli bir şekilde saklanmalarındaki başarısızlık, Sözleşme'nin ihlal için yeterli olmaktadır. Mahkeme ayrıca, sağlık kuruluşlarının, konuyla ilgisi olmayan personelin gizli bilgilere erişimine engel olacak bir sistem kuramamasını ihmâl olarak kabul etmiştir (Berber vd 2009: s. 110).

⁸⁹ I. v. Finland, 20511/03, 17.07.2008

Bu karardan sonra, sađlık kuruluřlarının elektronik hasta kayıtlarına erişim ve güvenlik mekanizmalarının, yetkisiz veri erişimleri ihtimali karşısında güvenli ve sağlam olup olmadığını kontrol etmeleri asgari bir gereklilik olduđu doktrinde ifade edilmiştir (Berber vd 2009: s. 110).

2.3.3.2.10. S. and Marper Kararı

Tıbbi verilerin gizliliđi ve tutulmasına ilişkin bir diđer örnek karar da, AİHM'in Büyük Daire'sinin 2008 yılında Birleşik Krallık aleyhine verdiği S. and Marper kararıdır⁹⁰. Her ikisi de Birleşik Krallık vatandaşı olan 1989 doğumlu S. ve 1963 doğumlu Michael Marper'in başvuruları, bir ceza yargılaması öncesinde parmak izlerinin, hücre örneklerinin ve DNA profillerinin alınması ve hukuki süreçten sonra bunların tutulmaya devam edilmesine ilişkindir. Davaya bakan ilgili dairenin konuyu doğrudan Büyük Daire'ye havale etmesi AİHM'in davaya verdiği önemin bir göstergesidir. Mahkeme, kararında konunun AİHS'in 8. maddesinde korunan özel hayatın gizliliđi hakkına dair olduğunu vurgulamıştır. Mahkûm olmamış, hükûm giymemiş kişilerin parmak izlerinin, hücre örneklerinin ve DNA profillerinin söz konusu hukukî sürecin sonrasında tutulmasının kamu ve özel menfaatler arasındaki adil dengeyi bozduğuna işaret eden Mahkeme, Birleşik Krallık'ın bu konuda kabul edilebilir takdir yetkisini aştığına hükmetmiştir⁹¹. Bu itibarla, gerekçeli karar göre, başvuruçuların özel hayatının gizliliđi, demokratik bir toplumda gerekli görülenin ötesinde, oransız bir şekilde müdahaleye uğramıştır. AİHM, başvuruçuların ve diđer kişilerin bu yöndeki mağduriyetinin sonlandırılması gerektiğine karar vermiştir⁹².

2.3.3.2.11. Kişisel Verilerin Korunmasına Dolaylı Yönden Temas Eden Kararları

Mahkeme, 18 Kasım 1982 tarihli X.-İngiltere kararında, nüfus sayımında veri toplanmasını, 28 Kasım 1994 tarihli **Murray-İngiltere** ve 18 Mart 1981 tarihli

⁹⁰ S. and Marper v. the United Kingdom, 30562/04 and 30566/04, 04.12.2008.

⁹¹ Birleşik Krallık, Avrupa Konseyi üyesi 47 ülke arasında, beraat eden ya da haklarındaki ceza davası düşen kişilere ait DNA profillerinin ve hücre örneklerinin sistematik ve süresiz bir şekilde tutulmasına izin veren tek ülkedir. Bu ülkede 5 milyondan fazla kişinin DNA profili saklanmaktadır. Bunun yaklaşık 1 milyonu herhangi bir suçtan dolayı mahkûm olmamış kişilere aittir. Yarım milyonu ise yetişkin olmayan kişilere aittir. Bkz. **Atak**, s. 119

⁹² Case of S. and Marper v. United Kingdom, 30562/04 & 30566/04, 04/12/2008, European Court of Human Rights Portal - Human Rights Documentation, <http://hudoc.echr.coe.int/> bkz. **Berber/Ülgü/Er**, s. 110-111

McVeigh-İngiltere kararlarında, kolluk güçlerinin fotoğraf çekip parmak izi almasını, 13 Aralık 1979 tarihli **X.- Avusturya kararında**, zorunlu tıbbi muayeneyi ve 9 Temmuz 1991 tarihli **Chave nee Jullien-Fransa kararında** tıbbi bilgilerin saklanmasını müdahale saymıştır. Söz konusu müdahalelerin 8. maddenin 2. fıkrası gereğince hukuka uygun hale gelebilmesi için Mahkeme'nin benzer yapıdaki diğer düzenlemeler açısından da geçerli olan yerleşik içtihatları uyarınca "yasallık, haklı neden ve orantılılık" koşullarına uyulması gerekmektedir (Akyürek, 2011: s. 47).

Mahkeme, **Lustig/Prean/İngiltere kararında** da benzer şekilde, kolluk güçlerinin kişinin parmak izinin ve benzeri kişisel bir takım bilgilerinin almasının özel hayata müdahale teşkil ettiğini, dolayısıyla bu yönde bir müdahalenin ancak yasayla ve meşru bir sebebin bulunması durumunda gerçekleştirilebileceğini ifade etmiştir⁹³.

Görüldüğü gibi kişisel verilerin büyük oranda AİHS kapsamında güvence altındadır. Genel olarak, ilgili kişinin izni ya da icazeti olmaksızın kişiliğine ilişkin verilerin işlenmesi, toplanması, verilerin sınırsız ya da gerektiğinden uzun süre tutulması, meşru amacın açık bir şekilde belirtilmemesi ve gereken güvencelerin sağlanmaması durumlarında kişisel verilerin korunmasına yönelik olarak özel hayatın gizliğinin ihlal edildiğini söyleyebiliriz (Küzeci, 2010: s. 141-142).

2.4. Kişisel Verilerin Korunmasına İlişkin Avrupa Birliği Düzenlemeleri

2.4.1. Genel Olarak

Avrupa Birliği, temel hak ve özgürlüklerin korunması, eşitlik, insan saygınlığı, demokratik kurumların varlığı, hukukun üstünlüğü ve şeffaflığın sağlanması gibi genel anlamda kabul görmüş ortak evrensel değerler üzerine kurgulanmıştır. Kişilerin, malların, hizmetlerin, sermayenin ve bilginin serbestçe dolaşabilmesi için iç hukuklarda çalışmalar yapan AB'nde, kişisel verilerin de belli güvenceler sağlanması koşuluyla serbest dolaşımı hedeflenmiştir (Kılınç, 2012: s. 1117).

Avrupa'da 2. Dünya savaşıdan sonra yürürlüğe giren hukuki metinlerde özel hayatın korunması temel insan haklarından birisi olarak düzenlenmiştir. Bu dönemde

⁹³ Lustig-Prean/İngiltere, 31417/96, 27.09.1999. bkz. **Aslan**, s. 5

yaşanan trajediler ve insanlık dışı uygulamalar bu yaklaşımda etkili olmuştur. Bu dönemde kişisel veri tabanları ırkçılık, azınlık grupları yok etmek, soykırımı kolaylaştırmak gibi amaçlarla kullanılmıştır. Burada yaşanan olaylar, insanlığa devletlerin özel alanı hangi oranda ihlal edebileceğini öğretmiştir. Bu nedenle, devletlerin kişisel verileri saklaması konusunda çok sıkı kurallar getirilmiş ve bu kuralların uygulanmasında da büyük bir dikkat gösterilmiştir (Kılınç, 2012: s. 1117).

Bu nedenle Avrupa kişisel verilerin korunmasının anavatanı olarak nitelendirilmiştir. Nitekim Avrupa'da, bu alanda hem Avrupa Birliği (AB), hem de ulusal hukuk sistemleri düzeyinde oldukça gelişkin bir mevzuat bulunmaktadır. Almanya'nın Hessen eyaletinde ilk yasal düzenlemenin yapıldığı günden bugüne bölgede kişisel verilerin korunması hukuku yayılmış ve gelişmiştir. Kişisel verilerin korunmasının ayrı bir hüküm altında düzenlendiği ABTHŞ'nin hukuksal bağlayıcılığa kavuşmasını sağlayan Lizbon Antlaşmasının 1 Aralık 2009'da onaylanması ile AB bünyesinde kişisel verilerin korunması daha da önemli hale gelmiştir (Küzeci, 2010: s. 154).

Ancak AB'de kişisel verilerin korunmasında ilk önemli belge 24 Ekim 1995 tarihli ve 95/46/EC sayılı “Kişisel Verilerin İşlenmesi ve Bu Türdeki Verilerin Serbest Dolaşımı Bağlamında Bireylerin Korunmasına İlişkin Yönerge/Direktif” dir⁹⁴.

Zira Avrupa Birliğince kişisel verilerin korunması konusunda üye ülkeler tarafından uygulanan esaslar arasındaki farklılıkların giderilmesi amaçlanmıştır. Bu amaç doğrultusunda, Avrupa Birliği Komisyonu tarafından üye ülkelerde kişisel verilerin korunmasına ilişkin mevzuatların uyumlu hale getirilmesine yönelik olarak çalışma başlatılmış ve çeşitli Direktifler kabul edilerek yürürlüğe konulmuştur (Özdemir, 2009: s. 27) . İşte 95/46/EC sayılı Direktif, konuyu ayrıntılı bir şekilde düzelediği için önemlidir. Çalışmamızın konusunun daha iyi anlaşılabilmesi ve son bölümde incelenecek suçların yorumunda bize ışık tutacak nitelikte olması nedeniyle bu Direktifi ayrıntılı incelemekte fayda bulunmaktadır.

⁹⁴ Direktifin İngilizce metni için bkz. <http://eur-ex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML> Erişim Tarihi: 10.04.2014

2.4.2. 95/46/EC sayılı Kişisel Verilerin İşlenmesi Sırasında Gerçek Kişilerin Korunması ve Bu Türdeki Verilerin Serbest Dolaşımına İlişkin Avrupa Konseyi ve Parlamentosu Direktifi

Kişisel verilerin korunması alanında en önemli hukuksal metinlerden biri olarak kabul edilen bu Direktif⁹⁵, tüm AB üyesi devletlerin iç hukuklarına uyarlanması ve bu sayede tüm üye devletlerde kişisel verilerin işlenmesine dair gerçek kişilerin hak ve özgürlüklerinin korunması konusunda bir standart belirlemek ve ulusal mevzuatları uyumlaştırmak amacıyla, 24 Ekim 1995 tarihinde kabul edilmiştir (Başalp, 2004; s. 31).

Direktifinin temel amacı; gerçek kişilerin temel hak ve özgürlüklerini korumaktır. Nitekim Yönerge'nin 1. Maddesinde; üye Devletlerin, gerçek kişilerin temel hak ve özgürlüklerini ve özellikle kişisel verilerin işlenmesi ile ilgili özel yaşamın gizliliği hakkını koruyacağı, hüküm altına almıştır. Yönerge ile güdülen bir diğer amaç ise bütün üye devletlerde geçerli olacak asgari veri koruma ölçütlerini belirlemektir (Küzeci, 2010: s. 164-165). Ancak Direktifin bunun ötesinde bir amacı daha mevcut olduğu, bununda, iç pazar bağlamında kişisel verilerin AB kapsamında serbest dolaşımına izin vermek olduğu belirtilmiştir. Bu nedenle Direktifin amacının bir yandan bireylerin mahremiyetlerini korumak iken, öte yandan iç pazarın gelişimine katkıda bulunmak amacıyla, AB çapında veri akışına özgürlük tanımak olduğu söylenebilir⁹⁶.

Direktif, koruma kapsamını 108 nolu AK Sözleşmesinden daha geniş tutarak; yalnızca otomatik veri işleme tabi olan kişisel verileri değil, klasik bir dosyada bulunan veya bulunabilecek kişisel verileri de kapsamaktadır (m. 3/1). Öte yandan Direktif, “veri işlem sorumlusu”, “veri işleyen”, “üçüncü kişi”, “alıcı”, “ilgili kişinin rızası” gibi temel kavramları tek tek tanımlamaktadır (m. 2). Verileri işleyen açısından “bilgi verme” yükümlülüğü bulunduğu gibi (m. 10, 11), ilgilinin verilerine “ulaşma hakkı” (m. 12) ve “verilerin işlenmesine itiraz hakkı” da (m. 14)

⁹⁵ <http://eur-ex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML> Erişim Tarihi: 10.04.2014; Bir kısım yazarlar tarafından “Yönerge” olarak ta adlandırılan bu metni çalışmamızda “95/46/EC sayılı Veri koruma Direktifi” adıyla kullanacağız.

⁹⁶ Legally e-Health, Putting e-Health in its European Legal Context, Legal and Regulatory Aspects of e-Health, Study Report, March 2008, s. 14. (Aktaran: **Berber/Ülgü/Er**, s.115); aynı yönde bkz. **Özdemir**, 2009, s. 29

bulunmaktadır. Öte yandan Direktif, tüm üye devletlere ulusal düzeyde bağımsız bir denetim makamı oluşturma zorunluluğu getirmekte (m. 28), bütün makam temsilcilerinin bir araya gelerek “bir veri koruma grubu” oluşturmalarını da öngörmüştür (m. 29). Ayrıca “uygun bir koruma düzeyinin” bulunmadığı üçüncü ülkelere veri aktarımı da, kural olarak yasaklanmıştır (m. 25) (Şimşek, 2008: s. 41 vd).

Direktifte yukarıda belirtilen hükümlerden; verilerin kalitesine ilişkin ilkeler ve verilerin işleme şartları, bir başka deyişle verilerin işlenmesinde hukuka uygunluk nedenleri, ilgili kişinin haklarına ilişkin kısımlar konumuz açısından önemli olduğundan bunları ayrıntılı incelemekte fayda bulunmaktadır.

2.4.2.1. Veri Kalitesine İlişkin İlkeler

Bu ilkeler, 108 sayılı AK Sözleşmesi ve OECD Rehber ilkelerine paralel olarak Direktifin 6. Maddesinde düzenlenmiş olup, maddeye göre; kişisel veriler hukuka ve dürüstlük kurallarına uygun olarak işlenmeli; belirli, açık ve meşru amaçlar için toplanmalı; toplanma amaçlarıyla ilgili, ölçülü ve yeterli olmalı; doğru ve güncel tutulmalı ve gerekli olan süre kadar saklanmalıdır (Uygun, 2010: s. 52).

2.4.2.2. Kişisel Verilerin İşlenmesinde Hukuka Uygunluk Nedenleri

108 sayılı Sözleşmede Devletlerin takdirine bırakılan bir konu olan kişisel verilerin işlenmesinde hukuka uygunluk nedenleri, bir başka deyişle verilerin işlenmesi şartları, direktifte ayrıntılı şekilde düzenlenmiştir. Direktifin 7. maddesine göre, kişisel veriler ancak ilgili kişinin açık rızasıyla veya belirli sebeplerin varlığı halinde işlenebilir. Belirli sebeplerden kasıt; ilgili kişinin taraf olduğu bir sözleşmenin veya veri işlem sorumlusunun bir hukuksal bir yükümlülüğünün yerine getirilmesi, ilgili kişinin hayati öneme sahip yararlarının korunması, kamu yararı bulunan bir görevin yerine getirilmesi, veri işlem sorumlusu tarafından korunması gerekli olan haklı bir yararın bulunması durumlarıdır (Şimşek, 2008: s. 46).

Rıza, Direktifin 2. Maddesinde, “veri öznesinin kendisiyle ilgili kişisel verilerin işlenmesine onayının işareti olan, belirli bir konuda ve aydınlatılmış özgür iradesinin belirtisi” olarak tanımlanmıştır (Küzeci, 2010: s. 221). Direktife göre rızanın hukuka uygunluk nedeni olarak kabul edilebilmesi için ayrıca rızanın şüpheye yer bırakmayacak nitelikte olması başka bir deyişle kesin olması

gerekmektedir. Ayrıca işlenecek verinin hassas veri olması halinde ise bu rızanın “açık rıza” olması aranmıştır (Küzeci, 2010: s. 221).

Kişi, herhangi bir baskıya maruz kalmaksızın özgür bir şekilde, somut olarak belirli bir veri işleme faaliyeti ile ilgili yeterli bilgiye sahip olarak yaptığı her türlü olumlu irade açıklamasıyla, verilerin işlenmesini hukuka uygun hale getirmektedir (Uygun, 2010: s. 53).

Rızanın olmadığı durumlarda ise diğer sebeplerin varlığı aranmaktadır. Örneğin bir bankanın veya alışveriş merkezinin kendi güvenliği veya müşterilerinin güvenliği için bina içinde güvenlik kamerasıyla kişilerin görüntülerini kaydetmesi, veri sorumlusunun meşru haklı çıkarlarının korunması için gerekli olduğundan hukuka uygun kabul edilmektedir.

Bir otelin müşterisiyle yaptığı konaklamaya ilişkin sözleşme gereği konaklama bilgilerini veya bankanın kredi verme sözleşmesi yapması nedeniyle müşterisinin kimlik, adres ve maaş bilgilerini kaydetmesi eylemleri sözleşmenin ifası için gerekli olması nedeniyle hukuka uygun olacaktır. İşverenin çalıştırdığı kişilerin sendika aiatını yatırabilmesi veya sosyal güvenlik primlerini yatırabilmesi için işçinin sendika üyelik bilgileri ile özlük bilgilerini kaydetmesi, hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olduğundan hukuka uygun olacaktır. Yine kamu görevlilerinin kanundan kaynaklanan görevlerini yerine getirebilmek için kişilerin verilerini kaydetmeleri de bu kapsamda hukuka uygun olacaktır. Ancak bunun için mutlaka bu yetkinin kanundan kaynaklanması gerekmekte ve işlemenin görev alanına giren konularda yapılması gerekmektedir. Örneğin adli sicil kayıtlarının 5252 sayılı Kanun gereği Adalet Bakanlığınca tutulması gibi.

2.4.2.3. Hassas Verilerin İşlenmesi

Direktife göre, hassas verilerin diğer bir deyimle özel nitelikli verilerin işlenmesi kural olarak yasaktır. Direktifte kişilerin ırksal ya da etnik kökenine, politik düşüncesine, dinsel veya felsefi kanaatlerine veya sendika üyeliğine, sağlığına ve cinsel yaşamına ilişkin veriler, hassas veri olarak belirlenmiş ve bu verilerin işlenmesi kural olarak yasaklanmıştır (m. 8) (Şimşek, 2008: s. 46).

Ancak bu kuralın sınırlı da olsa istisnaları bulunmaktadır. Direktifin 8. Maddesinin ikinci fıkrasına göre (Küzeci, 2010: s. 240-241; Başalp, 2004: s. 44-45);

- İlgili kişinin açık rızasının bulunması,
 - Veri işleme, veri koruma görevlisinin iş hukukundan kaynaklanan hak ve yükümlülüklerini yerine getirmesi için zorunlu olması,
 - Veri öznesinin ya da diğer bir kişinin yaşamsal çıkarı için gerekli olması,
 - İşlemenin ilgili kişi tarafından kamuya açıklanan verilere ilişkin olması,
 - Bir hakkın kurulması, kullanılması veya korunması için gerekli olması,
 - Kar amacı gütmeyen bir kurum tarafından yasal etkinliklerini yerine getirilmesi için işlemenin gerekli olması,
 - Veri işlemenin önleyici hekimlik, tıbbi teşhis, tıbbi yardım veya bakım veya sağlık hizmetlerinin idari olarak yürütülmesi için gerekli olması ve bu verilerin ya sağlık personeli veya sağlık personeli gibi sır saklama yükümlülüğüne tabi kişiler tarafından işlenmesi,
- Hallerinde, veri işleme hukuka uygun olacaktır. Burada bu sebeplerden herhangi birinin bulunması yeterlidir. Hepsinin aynı anda gerçekleşmesine gerek yoktur.

2.4.2.4. Verileri İşlenen Kişinin Hakları

İlgilinin kendisine ilişkin verilere ulaşma hakkı da Direktifle garanti edilmiştir. Buna göre, her ilgili kişi veri işlem sorumlusundan aşağıdaki bilgileri alma hakkına sahip olmalıdır (md. 12, Şimşek, 2008: s. 46):

- Kendisine ilişkin verilerin işlenmesine yönelik bir faaliyetin bulunup bulunmadığı, başka bir ifade ile kendisi hakkında veri işlenip işlenmediğini sorma,
- İşlenmiş ise bu veriler hakkında bilgi alma;
- Direktif hükümlerine aykırı olarak işlenen veriler var ise, özellikle eksik ya da yanlış olması durumunda bunların düzeltilmesini, silinmesini veya engellenmesini isteme hakkı ile yapılan değişikliklerden kendisine veri aktarılmış üçüncü kişilerin bilgilendirilmesini isteme,

Hakları bulunmaktadır. Ayrıca ilgili kişinin kişisel verilerinin işlenmesine itiraz hakkı da Direktifte yer alan önemli bir garantidir. Buna göre, ilgili kişinin haklı

sebeplerle kendisine ilişkin kişisel verilerin işlenmesine itiraz hakkı bulunmaktadır. (md.14, Şimşek, 2008: s. 47).

Görüldüğü gibi Direktifte ilgili kişilere tanınan bu haklar, büyük ölçüde Anayasamızın 20. Maddesinin üçüncü fıkrasında da benzer şekilde düzenlenmek suretiyle, anayasal güvence altına alınmıştır. Henüz kişisel verilerin korunmasına ilişkin kanun yürürlüğe girmemiş olsa da Anasadaki bu hüküm de uygulanabilir olduğundan ilgili kişiler, haklarında veri tutulup tutulmadığını, tutuluyor ise bu verilerin neler olduğunu bilme, yanlış veya eksik iseler düzeltilmesini veya silinmesini isteme haklarına sahiptirler.

2.4.3. Avrupa Birliği Temel Haklar Şartı

7 Aralık 2000 tarihinde Fransa'nın Nice kentinde imzalanan AB Temel Haklar Şartının amacı, AB kurumlarının insan hakları konusunda AB kurumlarının insan haklarına saygı duymasını sağlamak, temel hakları güvence altına almak suretiyle etkin bir şekilde korumaktır. Bir başka deyişle, Avrupa Birliği'nin yetkilerinin temel haklar lehine sınırlandırılması amaçlanmaktadır (Yüksel, 2002: s. 46). Bu belge ile AB'nin tarihinde ilk kez Avrupa vatandaşlarının ve AB'de yaşayan bütün insanların bireysel, siyasal ve ekonomik hakları tek bir metinde toplanmıştır⁹⁷. Lizbon Antlaşmasının 1 Aralık 2009 tarihinde yürürlüğe girmesi ile ABTHŞ hukuksal açıdan tam anlamıyla bağlayıcı hale gelmiştir (Küzeci, 2010: s. 158-159).

AB Temel Haklar Şartı'nın, konumuz açısından önemli yanı, kişisel verilerin korunması hakkını ayrı bir hüküm altında düzenlenmesidir.

AB Temel Haklar Şartı'nın "*Kişisel verilerin korunması*" kenar başlıklı 8. maddesi şöyledir (Küzeci, 2010: s. 161):

“(1) Herkes, kendisini ilgilendiren kişisel verilerin korunması hakkına sahiptir.

(2) Bu veriler, dürüst bir şekilde, belirli amaçlar için ve ilgili kişinin rızasına veya yasa ile öngörülmüş diğer meşru bir temele dayanılarak işlenir. Herkes kendisi hakkında toplanmış verilere erişme ve bunları düzelttirme hakkına sahiptir.

⁹⁷ AB Temel Haklar Şartının İngilizce metni için bkz.

<http://www.tbmm.gov.tr/komisyon/abuyum/ABTemelBelgeler.htm> Erişim Tarihi: 10.3.2014

(2) Bu kurallara uyulması bağımsız bir makam tarafından denetlenir.”

Görüldüğü gibi maddede *herkesin* kişisel verilerinin korunması hakkına sahip olduğu, verilerin ancak kişinin rızasıyla veya kanunla öngörülmüş meşru bir amaç için işlenebileceği ve kişinin verilerine erişme ve düzeltme haklarına sahip olduğu hüküm altına alınmıştır. Dikkat edilecek olursa hükmün kaynağını, 95/46/EC sayılı AB Direktifi, 108 sayılı AK Sözleşmesi ve AİHS'nin 8. maddesinin oluşturduğu görülecektir.

AB Temel Haklar Şartının da Anayasamızın 20. Maddesinin üçüncü fıkrasına kaynaklık ettiği de söylenebilir. Zira bu hüküm benzer şekilde Anayasa da yer almaktadır.

Bu belgede özel yaşamın gizliliği hakkı ile kişisel verilerin korunması hakkı arasında bir ayrımın öngörülmesi, ulusal hukuk sistemlerinde yapılacak yeni anayasal çalışmalara da örnek oluşturacak niteliktedir⁹⁸. Önceki bölümde ayrıntılı şekilde açıklandığı üzere, kişisel verilerin korunması hakkı, özel yaşamın gizliliği hakkının çekirdeği içerisinde değerlendirilemeyecek bazı konuları koruma kapsamına almaktadır. Nitekim kişinin kamuya açık olan bilgilerinin de kişisel verilerin korunması hakkı kapsamında hukuksal korumadan yararlanması buna örnektir. Yine sözkonusu Şartın 8. maddesinde herkesin kendisi hakkında toplanmış verilere erişme ve bunları düzelttirme hakkına sahip olduğunun belirtilmesi, AİHM'nin özel yaşamın gizliliği hakkına dayanarak oluşturduğu içtihatlarında tam anlamıyla cevaplayamadığı bazı hukuksal sorunları da çözmektedir (Küzeci, 2010: s. 162).

Sonuç olarak AB Temel Haklar Şartı'nda kişisel verilerin korunmasının özel yaşamın gizliliği hakkından ayrı olarak düzenlenmesi, kişisel verilerin korunmasının artık bağımsız bir hak olarak kabul edildiğinin önemli bir işaretidir⁹⁹.

⁹⁸ Anayasamızda ise kişisel verilerin korunması hakkı, özel hayatın gizliliğinin düzenlendiği, 20. maddenin son fıkrasında yer almaktadır.

⁹⁹ **Commission of the European Communities**, Report From The Commission, First Report On The Implementation Of The Data Protection Directive (95/46/EC), 15 Mayıs 2003 Brüksel, COM(2003) 265 final, s. 3-4.(Aktaran; **Küzeci**, s. 162)

2.4.4. Elektronik İletişim Alanında Özel Yaşamın Gizliliğinin Korunması ve Kişisel Verilerin İşlenmesine İlişkin Yönerge

95/46/AT sayılı Direktif, kişisel verilerin korunmasına yönelik genel ve kapsayıcı hükümler içermektedir. Ancak AB’nde bu alanda öne çıkan bazı sektörlerde özel düzenlemeler yapma gerekliliği de hissedilmiştir. Bu kapsamda 2002/58/AT sayılı Elektronik İletişim Alanında Özel Yaşamın Gizliliğinin Korunması ve Kişisel Verilerin İşlenmesine İlişkin Yönerge kabul edilmiştir (Küzeci, 2010: s. 187).

Direktif, halka açık iletişim ağları vasıtasıyla verilen elektronik iletişim hizmetleri hakkında uygulanacaktır (Şimşek, 2008: s. 57).

Bu Direktifle, üye devletlerin pek çok iletişim aracına ilişkin trafik ve yer bilgisini kaydetmelerine imkan veren yasal düzenlemeler yapma imkanı getirilmiştir. Bu kapsamda üye devletler mobil telefon, sms, sabit telefon, faks, elektronik posta, sohbet odaları, İnternet ve diğer iletişim araçları üzerinden yapılan iletişim verilerini tutabileceklerdir. Ayrıca milli güvenlik, suçun önlenmesi, suç soruşturma ve kovuşturmalarda kanunun öngördüğü şartlarda bu veriler kullanılabilir (Kılınç, 2012: s. 1128).

Diğer yandan üye devletler ulusal hukuklarında yapacakları düzenlemeler ile iletişimin gizliliğini sağlamak zorundadırlar. Bu kapsamda özellikle, kişilerin rızası olmaksızın, iletişimin ve trafik verilerinin dinlenilmesi, izlenilmesi, kaydedilmesi gibi içeriğine ulaşma ve gözetleme yöntemlerine karşı gerekli önlemlerin alınması zorunludur (Küzeci, 2010: s. 190).

2.4.5. İletişim Trafik Verilerinin Saklanması Yönergesi

2006 yılında AB Konseyi, 2006/24/AT sayılı İletişim Trafik Verilerinin Saklanması Yönergesi’ni kabul etmiştir. Direktif, özellikle suç soruşturması ve kovuşturmalarda kullanılmak üzere, elektronik haberleşme altyapı ve hizmetlerinin kullanımı ile ortaya çıkan trafik ve konum bilgilerine ilişkin esasları düzenlemek amacıyla hazırlanmıştır (Kılınç, 2012: s. 1128).

Direktif, suçun takibi ve yargıya intikali sürecinde gerekli verilerin sağlanabilmesi amacıyla elektronik haberleşme hizmet sağlayıcılarına bazı yükümlülükler getirmiş, bu kapsamda, saklanacak veri kategorileri, saklama süresi,

verileri saklama koşulları ve veri güvenliği kapsamında gözetilecek kuralları düzenlemiştir (Kılınç, 2012: s. 1128).

Direktifin 5. maddesinde düzenlenen verilerin saklanması kişisel verilerin korunması açısından önem taşımaktadır. Buna göre servis sağlayıcılar, arayan ve aranan telefon numarası, abonenin adı ve adresi, internet kullanıcıları için kullanıcı kimliği ve adresi, iletişimin veya bağlantının tarihi, saati ve süresi ve coğrafi konumu gibi bilgileri altı ay ile iki yıl arası bir süre için saklamakla yükümlüdürler. Bu trafik verileri; İnternet telefonunu da içeren telefon numaraları, elektronik posta ve bunların tarih ve sürelerini de içermelidir. Üye ülkelerdeki ulusal polis kendi hukuk sistemlerine saygı ilkesi çerçevesinde bu bilgilere ulaşabilmelidir (Kılınç, 2012: s. 1128).

Söz konusu verilere ancak, AİHS çerçevesinde gereklilik ve ölçülülük ilkelerine uygun olarak yetkili ulusal makamlarca erişim sağlanabileceği de Direktifin gerekçesinde belirtilerek devletlere tanınan bu yetki sınırlandırılmıştır (Uygun, 2010: s. 88; Şimşek, 2008: s. 67).

2.4.6. Avrupa Birliği Adalet Divanının Kişisel Verilerin Korunması Hakkındaki Kararı

2.4.6.1. Genel Olarak

Avrupa Birliği Adalet Divanı (European Court of Justice) Avrupa Birliği bünyesi içinde yer alan en yüksek mahkeme olup, Avrupa Birliği üyesi ülkeleri arasında, Avrupa Birliği hukukunu ilgilendiren konularda karar veren son mercidir. Temel amacı, Avrupa Birliği hukukunun Avrupa Birliği içerisinde her yerde aynı şekilde yorumlanmasını ve uygulanmasını sağlamaktır. Avrupa Birliği Adalet Divanı üye ülkelerle ya da Avrupa Birliği kurumlarıyla ilgili davalarla ve üye ülke mahkemelerinin bir üst kuruma sevk ettiği uyuşmazlıklara bakmakla görevlidir¹⁰⁰.

1952 yılında kurulan Avrupa Birliği Adalet Divanı (ABAD), Adalet Divanı, Genel Mahkeme ve Uzmanlık Mahkemeleri olmak üzere üçlü bir yapıdan oluşur. Divan, Birlik hukukunun yorumlanmasında ve uygulanmasında hukuka saygıyı sağlama, ulusal hukuk düzenleri ile AB hukuk düzeni arasındaki ilişkilerin

¹⁰⁰ Divanın resmi internet sitesine http://curia.europa.eu/jcms/jcms/j_6/ adresinden ulaşılabilir.

düzenlenmesi, hukuki denetim, yorum, uyuşmazlık çözme, hukuk yaratma ve boşluk doldurma işlevlerini yerine getirir¹⁰¹.

Bu kapsamda genel olarak üye devletlerin ve AB kurumlarının AB hukukuna uyup uymadığının denetlenmesine yönelik davalar ile ulusal mahkemelerde görülmekte olan davaların çözüme bağlanması için gerekli olduğunda AB hukukunun yorumlanmasına ilişkin davalara bakar. Avrupa Birliği Adalet Divanı Lüksemburg'da faaliyet göstermektedir.

2.4.6.2. Unutulma Hakkı Kararı

ABAD'ın kişisel verilerin korunmasına ilişkin son zamanlarda verdiği önemli bir karar bulunmaktadır. Divan, 13 Mayıs 2014 tarihli kararında dünyanın en popüler arama motorlarından olan “Google Inc” şirketi hakkında “*AB üyesi ülke vatandaşlarının talep etmeleri halinde kişisel verilerinin silinmesi*” konusunda önemli bir karar vermiştir. Kararın, kişilerin “*unutulma hakkı*”¹⁰² nın olduğunu vurgulaması açısından milat niteliğinde olduğu söylenebilir. Ayrıca karar, kişisel verilerin korunması yönelik tespitler yapılması ve uygulamaya doğrudan etki etmesi açısından son derece önemlidir.

Karara konu dava, 5 Mart 2010 tarihinde İspanya vatandaşı olan Mr. Costeja Gonzales, İspanya Veri Koruma Ofisine (Agencia Española de Protección de Datos - AEPD), Google Inc ve Google Spain şirketleri ile Lavanguardia isimli gazeteyi şikâyet etmesi üzerine başlamıştır. Bay Gonzales'ın şikâyeti, kendisi hakkında mülkiyetinde bulunan bir evin icra yoluyla satılması olayının google arama motorunda yer alması, daha doğrusu üçüncü kişilerin google da arama yaptıklarında Gonzales ile ilgili, Lavanguardia gazetesinin 19 Ocak ve 9 Mart 1998 tarihli linklerine ulaşabilmeleri nedeniyle bu bilgilerin google indekslerinden ve ilgili gazetenin sorvırlarından kaldırılması ve gelecekte bu bilgilere ulaşılmasının

¹⁰¹ <http://www.ab.gov.tr/index.php?p=45632&l=1> Erişim Tarihi: 01.05.2014

¹⁰² Bir insan hakkı olarak unutulma hakkının tanınmasında ve gündeme gelmesinde Avrupa Komisyonunun önerileri etkili olmuştur. Komisyonun önerisine göre eğer geçerli bir neden söz konusu değilse kişisel verilerin herhangi bir biçimde saklanmaması, silinmesi gerekmektedir. Bu çerçeveden hareketle unutulma hakkı; dijital hafızada yer alan bireye ait fotoğraf, kimlik bilgisi, adres ve diğer kişisel içeriğin, yine bireyin kendi talebi üzerine bir daha geri getirilemeyecek biçimde ortadan kaldırılması biçiminde tanımlanmıştır. Unutulma hakkı konusunda ayrıntılı bilgi için bkz. **Gülener, Serdar**, “Digital Hafızadan Silinmeyi İstemek; Temel Bir İnsan Hakkı Olarak Unutulma Hakkı”, TBB, 2012 (102), s. 219-240

engellenmesi konusunda gerekli tedbirlerin alınması için google emir verilmesine yöneliktir.

Şikâyeti inceleyen AEPD, 30 Haziran 2010 tarihinde bu talebin, gazeteye yönelik kısmını kabul etmemiş ancak Google ın Gonzalesin bilgilerinin indeksinde kaldırması gerektiği yönünde karar vermiştir. AEPD'in bu kararına karşı Google Inc, İspanya Yüksek Mahkemesine başvurmuştur. Başvuruyu inceleyen yüksek mahkeme, konunun aynı zamanda teknolojiyi ilgilendirdiğini ve bu teknolojinin AB'nin 95/46/EC sayılı Veri Koruma Direktifi kapsamında yorumlanması gerektiğini belirtip durma kararı vermiş ve konuyla ilgili ABAD'a bazı sorular sormuştur.

Bu şekilde davanın ABAD'a intikal etmesi üzerine, Divanın Büyük Dairesi 13.05.2014 tarihinde verildiği kararda; Google'ın, kullanıcılarına bazı durumlarda kendileri ile ilgili bilgilere yönlendiren linkleri silme hakkı tanınması gerektiğine karar vermiştir. Mahkeme, Avrupa genelinde tanınmış hale gelen “unutulma hakkı” kapsamında, silmemek için “özel/belirli bir neden” bulunmadıkça, Google gibi bir arama motorunun bir süre sonra kullanıcılar ile ilgili arama sonuçlarının silinmesine izin vermesi gerektiğini belirtmiştir¹⁰³. Divan, konuyla ilgili aşağıdaki tespitlerde bulunmuştur:

Divan, konuyu AB Temel Haklar Şartı ve AB'nin 95/46 EC sayılı Direktifi kapsamında incelemiştir.

Divan, arama motorlarının insanlar aradıklarını bulsunlar diye internete konulan bilgileri otomatik olarak indeksleme, geçici olarak depolama ve son olarak ta bu bilgileri internet kullanıcılarının hizmetine sunma aktivitelerini yaptığını, bu aktivitelerin de Direktif'in 2/b maddesi kapsamında kişisel verileri işleme olarak kabul edilmesi gerektiğini,

Arama Motorları operatörlerinin de bu işleme sürecinde Direktifin 2/d maddesi kapsamında “kontrolör”, yani veri işlemeden sorumlu kişilik olarak kabul edilmesi gerektiğini,

Arama motorlarının AB üyesi ülkelerde kurulduklarında bireylerle ilgili kişisel veri içeren ve üçüncü şahıslar tarafından yayınlanan web sitelerinin linklerinin

¹⁰³ http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0131&from=EN#Footnote* Erişim T: 23.10.2014

silme konusunda, direktifin 12. Maddesi kapsamında, arama motoru operatörlerinin sorumluluklarının olduğunu,

Mahkeme, Avrupa genelinde tanınmış hale gelen “unutulma hakkı” kapsamında, silmemek için “özel/belirli bir neden” bulunmadıkça, Google gibi bir arama motorunun bir süre sonra kullanıcılar ile ilgili arama sonuçlarının silinmesine izin vermesi gerektiğini,

Veri öznesinin talebi üzerine, (tarama sonuçları) listesindeki ilgili linkler, bu an itibarıyla, direktife aykırı bir konumda ise, linklerin ve sonuç listesindeki bilgilerin silinmesi gerektiğini,

Başlangıçta hukuka uygun bir şekilde işlenmiş doğru veriler bulunsada, zaman içerisinde, bu veriler, olayın tüm koşulları değerlendirildiğinde, elverişsiz, alakasız veya artık ilgili olmayan veya işleme amacını aşacak bir niteliğe gelmiş oldukları hallerde direktife aykırı hale gelebileceklerini,

Veri öznesinin sosyal hayatta oynadığı rol, bir arama yapılırken kamunun ilgili verilere erişebilmesindeki ağır basan bir menfaatini haklı kılmadıkça linklerin silinmesi gerektiğini, bir başka deyişle, kamunun ilgili verilere erişebilmeyi istemekte haklı olduğu veya kamunun bilgilenme hakkının üstün tutulduğu durumlarda, kamuya mal olmuş kimselerin bu taleplerinin yerine getirilmesinin gerekmeyebileceğini,

Belirtmiştir.

Karar metninde sorumluluğa atıf yapılırken “arama motoru” ifadesi kullanıldığından, Mahkemenin kararı yalnız Google için değil tüm arama motoru servisi sağlayan şirketler için de bağlayıcı bir konumdur.

Kararı veren otoritenin Avrupa Birliği Adalet Divanı olması hasebiyle karar Avrupa Birliği üye ülkeleri için uygulanabilir durumdadır. Ancak, unutulma hakkı kapsamında arama motorlarından link silme talebinde bulunabilmek için Avrupa vatandaşı olmak gerekmemektedir. Kararın bağlayıcı olduğu bir coğrafyada yaşıyor olmak yeterlidir.

Karar Google yetkilileri tarafından ifade özgürlüğünün kısıtlanması şeklinde yorumlansa da, karara uyan Google Inc şirketi, kendileriyle ilgili bilgilere

yönlendiren linklerin silinmesi için Avrupalılardan silme taleplerini, kurduğu özel bir sayfa üzerinden almaya başlamıştır¹⁰⁴.

3. MUKAYESELİ HUKUKTA KİŞİSEL VERİLERİN KORUNMASI HAKKININ İHLALİNE İLİŞKİN YAPTIRIMLAR

3.1.Genel Olarak

Kişisel verilerin korunmasına ilişkin hukuki düzenlemeler yapmış olan ülkelerin mevzuatlarına bakıldığında, kişisel verilerin korunmasına ilişkin yaptırım içeren düzenlemelerin bazı ülkelerde özel kanunlarda, bazı ülkelerde hem özel kanunlarda hem de ceza kanunlarında, bazı ülkelerde ise sadece ceza kanunlarında düzenlendiği görülmektedir¹⁰⁵. Ülkemizde ise henüz kişisel verilerin korunmasına ilişkin bir kanun olmadığından kişisel verilerin korunmasını sağlamaya yönelik suçlar, Fransa'dakine benzer şekilde, 5237 sayılı Türk Ceza Kanununda düzenlenmiştir (Ketizmen, 2008: s. 217).

Bu kapsamda bazı ülke düzenlemeleri incelemekte fayda vardır.

3.2. Almanya

Almanya'da, teknolojik gelişmeler neticesinde özel yaşama müdahale imkânlarının artması ve kolaylaşması nedeniyle, 1975 yılında yapılan reformla Ceza Kanununa yeni hükümler eklenmiştir. Bu kapsamda Alman Ceza Kanununun “Özel Hayat ve Gizli Alanının İhlâli” başlıklı 15. Bölümünde çeşitli suçlar düzenlenmiştir. Bunlar, Sözün (konuşmanın) güvenilirliğini ihlâl (m.201), Çok özel hayat alanını görüntü kaydederek ihlâl (m.201/a), Yazılı haberleşmenin ihlâli-mektubun açılması ve sahibine ulaşmasının engellenmesi (m.202), Verilerin ele geçirilmesi (m.202a), Meslek sırrının ifşası (başkasına ait özel sırrın ihlâli) (m.203), Başkasına ait özel sırrın (kazanç sağlamak üzere) değerlendirilmesi (m.204) suçlarıdır (Zafer, 2010: s. 76).

¹⁰⁴ Özer, Yusuf Mansur, “Avrupa Adalet Divanının Unutulma Hakkı Kararı ve Bu Hakkın Kapsamı” <http://www.statjus.com/2014/06/avrupa-adalet-divaninin-unutulma-hakki-karari-ve-bu-hakkin-kapsami/> Erişim T: 23.10.2014

¹⁰⁵ Bkz. Federal Almanya Veri Koruma Yasası (BDSG), m.43-44; İtalyan Veri Koruma Yasası, m. 167-172. Fransa'da ise Ceza Kanunu kapsamında yer almaktadır.

Alman Ceza Kanunu'nda özel hayatın kaydedilmesi suçu tanımlanmıştır. Alman CK m.201a-I'e göre, "her kim evinde veya bakışlardan korunmuş bir alanda bulunan bir kişinin yetkisiz olarak görüntüsünü kaydederse veya görüntüyü aktararak onun çok özel hayat alanını ihlâl ederse bir yıla kadar hapis cezasıyla veya para cezasıyla cezalandırılır". 201a/II'de, bu kayıtların kullanılması ve üçüncü kişilere verilmesi cezalandırılmıştır. 201a/III'te, hukuka uygun olarak birinci fıkrada belirtilen yerde yapılan kayıtların kullanılması ve üçüncü kişilere verilmesi ceza yaptırımına bağlanmıştır (Zafer, 2010: s. 76).

Kişisel verilerin ele geçirilmesi ise müstakil olarak Alman Ceza Kanunun 202a maddesinde suç olarak tanımlanmış ve cezai yaptırıma bağlanmıştır. Ayrıca Federal Almanya Veri Koruma Yasası (Bundesdatenschutzgesetz, BDSG)'nin 43 ve 44. maddelerinde de kişisel verilere karşı işlenen suçlar düzenlenmiştir (Küzeci, 2010: s. 286).

3.3. İngiltere

İngiltere'de kişisel verilere karşı işlenen suçlar özel kanun kapsamında yer almaktadır. Kişisel verilerin korunmasına ilişkin "Data Protection Act 1998" adlı Kanunun 55. maddesi uyarınca kişisel verilerin ele geçirilmesi, satılması, satışa sunulması veya bu amaçla reklâm yapılması suç oluşturmaktadır (Akyürek, 2011: s. 51).

3.4. Fransa

1 Mart 1994 tarihinde yürürlüğe giren yeni Fransız Ceza Kanununun "Kişilere Karşı İşlenen Cürüm ve Cünhalar" başlığını taşıyan ikinci kitabının altıncı bölümü "Kişiliğin İhlâli" başlığını taşımaktadır. Kişisel verilere karşı işlenen suçlarda bu bölümde düzenlenmiştir (Zafer, 2010: s. 67).

Fransız Ceza Kanununun, "*Elektronik Verilerle veya Verilerin İşlenmesi Suretiyle Kişilik Hakkının İhlâli*" adını taşıyan 226. maddenin beşinci alt kısmında, bir kişiye ait bilgilerin, kanunda öngörülen formaliteler yerine getirilmeden ihmal ile dahi olsa otomatikleştirilmesi, işlenmesi veya işletilmesi ceza yaptırımına bağlanmıştır (m.226-16). Aynı şekilde, bilgilerin değiştirilmesini, bu bilgilere zarar verilmesini veya bilgilerin yetkisiz üçüncü kişilere gönderilmesini engellemeye yönelik güvenlik önlemleri alınmadan kişiye ilişkin bilgilerin otomatik olarak işlenmesi, işletilmesi de

cezai yaptırıma bağlanmıştır (m.226-17). Yine bu kısımda, izin almadan hileyle, sessizce veri toplamak veya gerçek bir kişiye ait bilgileri onun hukuken geçerli itirazına rağmen otomatikleştirmek, işlemek suç olarak düzenlenmiştir. Aynı şekilde, sağlık alanında araştırma amacıyla kişiye ilişkin verilerin, hak sahibine haklarını hatırlatmadan otomatikleştirilerek işlenmesi hali de suç olarak düzenlenmiştir (m. 226-18, Zafer, 2010: s. 67).

Fransa Ceza Kanununda hassas verilerin rıza dışında kaydedilmesi de ayrıca düzenlenmiştir. Kanun'un 226-19. maddesinde Kanun'da öngörülen hallerin dışında, ilgilinin açık rızası olmaksızın, doğrudan doğruya veya dolaylı olarak bir kişinin etnik kökenini, siyasi, felsefi veya dini görüşlerini veya bir topluluğa mensubiyetini veya yaşam tarzını ortaya koyan kişiye ilişkin verileri, elektronik olarak kaydetmek veya muhafaza etmek eylemleri ceza yaptırımına bağlanmıştır. Kişisel verilerin işlenmesinde belirli bir amaç için işleme ve amaç için gerekli olan süre kadar muhafaza edilme ilkelerinin karşılanmasına yönelik olarak; ilgili kurumların (merkezi veri koruma makamlarının) onayı olmaksızın, kişisel nitelikteki bilgilerin, süresinden fazla muhafaza edilmesi suç olarak tanımlanmıştır (m. 226-20). Diğer yandan eldeki kişisel verilerin, kaydedilirken, gönderilirken, yönlendirilirken veya işleme tabi tutmanın herhangi bir şekli gerçekleştirilirken amacına yabancılaştırılması da ceza yaptırımına bağlanmıştır (m.226-21). Açıklandığı takdirde ilgisinin onurunu zedeleyecek bilgileri veya özel alanına zarar verecek nitelikteki kişisel bilgileri elde edip de bu bilgileri ilgilinin kabulü olmaksızın bilgileri almaya yetkili olmayan üçüncü kişilerin bilgisine sunmak da suç olarak düzenlenmiştir (m. 226-22, Zafer, 2010: s. 67).

Görüldüğü üzere Fransız Ceza Kanununda kişisel verilere karşı işlenen suçlar ayrıntılı olarak düzenlenmiştir. Hatta verilerin hukuka aykırı olarak taksirle işlenmesi (m. 226-16) ile birlikte kasten veya taksirle üçüncü kişilere iletilmesi de (m. 226-22) suç oluşturmaktadır. Keza kişisel verileri Avrupa Birliği dışındaki bir ülkeye göndermek de özel bir suç olarak düzenlenmiştir (m. 226-22-1). Bu konudaki tüm suçların yaptırımı, beş yıl hapis cezası ile 300000 Euro para cezası olarak öngörülmüştür (Akyürek, 2011: s. 51).

3.5. İsviçre

İsviçre'de kişisel verilerin hukuka aykırı olarak ele geçirilmesi üç yıla kadar hapis cezası veya para cezası ile cezalandırılmakta (İsviçre CK m. 179 novies); söz konusu verileri ifşa eden görevliler de para cezası ile cezalandırılmaktadır¹⁰⁶.

Bu hükme göre, serbestçe ulaşılması mümkün olmayan, özel olarak korunmaya değer kişisel verileri veya kişilik profillerini (özelliklerini), yetkisi olmadan veri kütüğünden temin eden kişi, şikâyet üzerine cezalandırılmaktadır (m. 179novies). 1 Temmuz 1993'te İsviçre Veri Koruma Kanunuyla İsviçre Ceza Kanununa eklenerek yürürlüğe giren bu hükmün amacı, Verilerin Korunması Kanunu'nun uygulanmasını güçlendirmek, kişisel verilerle bağlantılı olarak bireyin kişiliğini ve temel haklarını korumak olarak belirtilmiştir. Bu hükümle, İsviçre Veri Koruma Kanununda belirtilen tüm kişisel veriler değil, örneğin kişinin dini görüşüne, dünya görüşüne, mesleki faaliyetlerine ve sağlığına ilişkin veriler, yani hassas nitelikli veriler, korunmaktadır. Kişilik profili kavramı ise, İsviçre Veri Koruma Kanunu'nun 3/d. maddesinde tanımlanmıştır. Bu hükme göre kişilik profili kavramı, bir gerçek kişinin kişiliğinin önemli unsurları hakkında hüküm vermeye imkân veren önemli bilgilerin bir araya getirilmesi olarak tanımlanmıştır (Döner, 2006: s. 462; Zafer, 2010: s. 74).

3.6. Amerika Birleşik Devletleri

Bilindiği gibi Amerika Birleşik Devletlerinde (ABD) Avrupa ülkelerinde olduğu gibi müstakil olarak kişisel verilerin korunmasına yönelik bir kanun bulunmamaktadır. Konu, genel olarak özel hayatın gizliliği içinde bireysel mahremiyet ya da veri mahremiyeti kavramları içerisinde değerlendirilmektedir. ABD'de, kamu mercilerinin yalnızca gerekli kişisel verileri depolaması, veri sujesi için ölçülü şekilde bilgi toplanması, kayıtların doğru ve eksiksiz şekilde muhafaza edilmesi, kayıtların güvenliğinin sağlanması için idari ve teknik güvenceler oluşturulması yükümlülüklerini getiren 1974 tarihli "The Privacy Act" (The Privacy Act of 1974, 5 U.S.C. § 552a) adlı Federal Kanun bulunmaktadır (Gür, 2010: s. 120).

¹⁰⁶ 19.06.1992 tarihli Yasanın 35. Maddesi. Kanunun çevirisi için bkz. **Döner, Ayhan**, Kişisel Verilerin Korunması Hakkında Federal Kanun, (19 Haziran 1992) AÜEHFD, C. X, S. 1-2, 2006, s. 474; Aynı yönde bkz. **Akyürek**, 2011: s. 51

Ayrıca ABD’de 2001 yılında çıkan özel bir Kanun ile sağlık kuruluşlarında çalışanlar ve sağlık hizmeti sağlayanlar açısından özgü bir suç yaratılmış ve “bireysel olarak belirlenebilir sağlık bilgilerinin, ticari yarar, kişisel kazanç veya zarar verme amacıyla satılması, iletilmesi veya kullanılması” eylemleri 250.000 dolar para cezası ve 10 yıla kadar hapis cezası ile cezalandırılmaya başlanmıştır¹⁰⁷.

1974 tarihli Özel Yaşamın Gizliliği Yasasında federal kurumlarda bulunan kişisel verilerin toplanması, kullanılması ve yayılmasına ilişkin bazı ilkeler belirlenmiştir. Ancak yasada yer alan çeşitli istisnaların bu hükümlerin etkili bir şekilde uygulanmasına engel oluşturacak nitelikte oldukları, özellikle kurumların görevleri dolayısıyla kişisel verileri rutin kullanımlarının istisnalar arasında sayılması, özel yaşamın korunmasında önemli bir sorun oluşturduğu gerekçesiyle eleştirilmiştir¹⁰⁸.

¹⁰⁷ **Ferrier, Patricia**, There Ought To Be A Law, Michigan, 2006, s. 122-123. (Aktaran: Akyürek, 2011: s. 50); ABD’de ayrıca özel sektör için de veri mahremiyeti konusunda birden çok kanun bulunmaktadır. Ayrıntılı bilgi için bkz. **Gür**, 2010: s. 129 vd.

¹⁰⁸ **Henderson, Harry**, Privacy in the Information Age, Facts of File, ABD 2006, s. 59-60. (Aktaran, Küzeci, 2010: s. 109)

ÜÇÜNCÜ BÖLÜM

TÜRK HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASI

1. GENEL OLARAK

Günümüz dünyasında bir yandan kişisel verilere daha yüksek oranda gereksinim duyulurken, diğer yandan kişilerin temel haklarına yönelik saldırılar da hızla artmış ve konuya ilişkin hukuksal düzenlemeler yapılması zorunluluğunu beraberinde getirmiştir. Nitekim çalışmamızın ilk bölümünde açıklandığı üzere BM, OECD, AK ve AB gibi uluslararası örgütler konuya ilişkin çalışmalar yaparak tüm dünyada etki doğuran ve rehber niteliğinde belge ve Sözleşme düzenlemişlerdir. Birlik hukukunun bağlayıcı olması nedeniyle AB üyesi ülkelerde kişisel verilerin korunmasına ilişkin yasal düzenlemeler yapmışlar, hatta 95/46/EC sayılı Direktifin yürürlüğe girmesinden sonra ilgili kanunlarda değişiklik yaparak Direktifle uyumlu hale getirmişlerdir.

Türkiye kişisel verilerin korunması alanına AK'nin 1981 tarihli ve 108 nolu Sözleşmesini imzalamakla adım atmış olmasına, rağmen kişilerin bu konuda hukuksal güvencelere kavuşturulmasında, gelişmiş devletlerin gerisinde kalmıştır. Ülkemizde müstakil olarak kişisel verilerin korunmasına ilişkin bir kanun bulunmamaktadır. Aşağıda incelenecek olan Kişisel Verilerin Korunması Kanun Tasarısı, halen yasalaşmayı beklemektedir. 108 nolu Sözleşme, Türkiye tarafından 28 Ocak 1981 tarihinde imzalanmış olmasına karşın konuya ilişkin yasal düzenleme olmadığından, çalışmanın yazıldığı dönem itibarıyla onaylama işlemi tamamlanamamıştır.

Ancak bu durum kişisel verilerin tamamen korumasız olduğu anlamına gelmemektedir. Aşağıda inceleneceği üzere kişisel verilerin korunmasının Anayasada oldukça sağlam dayanakları bulunmaktadır. Türk Medeni Kanunu, Türk Ceza Kanunu gibi temel kanunlarda bazı güvencelerin tanındığı görülmektedir. Bunun yanında mevzuatımızda dağınık bir şekilde yer alan konuya ilişkin hükümler de bulunmaktadır.

Bu kapsamda, öncelikle mevzuatımızdaki temel düzenlemeler incelenecek, ardından da öne çıkan tartışma noktaları ile mevzuatımızdaki eksikliklere değinilecektir.

2. 1982 ANAYASASINDA KİŞİSEL VERİLERİN KORUNMASI

2709 sayılı Türkiye Cumhuriyeti Anayasasında kişisel verilerin korunması hakkı, “özel hayatın gizliliği hakkı” altında özel olarak düzenlenmiştir¹⁰⁹. Nitekim kişisel verilerin korunması alanında kapsayıcı hukuksal düzenlemeleri benimsemiş ülkelerin büyük bir bölümünde de durum böyledir. Birçok ulusal hukuk sisteminde bu önemli alan, anayasal kaynağını özel hayatın gizliliği hakkında bulur. Bunun yanında örneğin Fransa’da kişisel verilerin korunması hakkı anayasada yer alan “özgürlük” hakkına dayandırılmıştır¹¹⁰. Almanya’da ise, daha önce belirttiğimiz gibi, genel kişilik hakkı çatısı altında “*bilgilerin geleceğini belirleme hakkı*”nda anayasal temelini bulmaktadır (Aksoy, 2008: s. 238). Bu nedenle kişisel verilerin korunmasının anayasal temelini, başta özel yaşamın gizliliği hakkı, bilgilerin geleceğini belirleme hakkı olmak üzere, çağdaş ve demokratik anayasalarda korunan çeşitli temel hak ve özgürlüklerde bulduğunu söyleyebiliriz (Küzeci, 2010: s. 261).

Bununla birlikte Portekiz, Hollanda ve İspanya Anayasalarında özel olarak bir kişinin kişisel verilerine ulaşma ve onu denetleme hakkının düzenlendiği de görülmektedir (Avrupa Birliği Bazı Ülkelerin Anayasaları, 2011: s. 397-451-543).

Türkiye’de 7 Mayıs 2010 tarihinde kabul edilen ve 1 Eylül 2010 tarihinde yapılan halkoylaması ile yürürlüğe giren 5982 sayılı Kanun ile Anayasanın 20. Maddesine üçüncü bir fıkra elenerek kişisel verilerin korunması hakkı anayasal güvenceye kavuşturulmuştur.

1982 Anayasanın özel hayatın gizliliği başlıklı 20. maddesinin üçüncü fıkrası;

"Herkes kendisi ile ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak, kişinin kendisi ile ilgili kişisel veriler hakkında bilgilendirilme, bu

¹⁰⁹ Bkz. Anayasa m. 20/3.

¹¹⁰ **International Encyclopedia of Laws**, haz. R. BLANPAIN, Constitutional Law, C. 3, haz. A. Alen, Fransa Bölümü 8Bu bölüm Michael Front tarafından hazırlanmıştır) Kluwer Law International, Hollanda 1999, s. 256-259 (Aktaran, Küzeci, s. 262)

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 rızası ile işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir". Şeklindedir.

Hüküm, kişisel verilerin anayasal dayanağını açıkça oluşturması nedeniyle önemlidir. Ancak bazı eksiklikleri bulunduğu doktrinde dile getirilmiştir. Bazı yazarlara göre, ABTHŞ’nda belirtilmesine rağmen maddede kişisel verilerin işlenmesini denetleyecek bağımsız bir kuruma yer verilmediği, kişisel verilerin ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilmesi kuralının da Anayasanın 13. maddesi ile çeliştiği, zira 13. madde de temel hakların yalnızca Anayasa da belirtilen sebeplerle sınırlanabileceği, maddedeki düzenlemenin ise sınırlama sebeplerini belirleme yetkisini kanuna verdiği, bu nedenle bu düzenlemenin kişisel verilerin etkin şekilde korunmasının önünde engel oluşturabileceği ifade edilmiştir (Küzeci, 2010: s. 266).

Nitekim temel hak ve özgürlükleri sınırlamanın sınırlarını belirleyen Anayasanın 13. maddesinde temel hak ve hürriyetlerin nasıl sınırlanacağı, sınırlamayı yapan kanunun hangi standartta olacağı belirlenmiştir. Ayrıca, daha önce de değinildiği üzere, 13. maddede 2001 yılında yapılan değişiklikle, genel sınırlama rejimden vazgeçilerek her hakkın niteliğine özgü sınırlama sebepleri kabul edilmiştir (Yokuş, 2003: s. 212). Anayasanın 13. maddesi:

“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 laik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz.” Şeklindedir.

Bu hüküm nedeniyle Anayasanın temel hakları düzenleyen maddelerinde her hak ve özgürlük için ayrı bir sınırlama sebebi öngörülmüştür.

Örneğin Anayasasının 20. maddesinde özel hayatın gizliliği hakkı güvence altına alınmıştır. Hükmün birinci fıkrasına göre, *“Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının*

gizliliğine dokunulamaz.” 20. Maddenin ikinci fıkrasında ise bu hakkın hangi hallerde sınırlanabileceği hüküm altına alınmıştır.

Fıkraya göre, “Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak, usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; kimsenin üstü, özel kâğıtları ve eşyası aranamaz ve bunlara el konulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını el koymadan itibaren kırksekiz saat içinde açıklar; aksi halde, el koyma kendiliğinden kalkar.”

Bu hükümde kişilerin üstünün, özel kâğıtlarının ve eşyasının aranması ve bunlara el konulmasının hangi koşullar altında gerçekleşebileceği belirlenmiştir. Bir başka anlatımla özel hayatın ve aile hayatının gizliliği hakkının sınırları çizilmiştir.

Aynı durum konut dokunulmazlığı ve haberleme hüriyeti açısından da geçerlidir. Bu maddelerde de (m. 21-22) herkesin bu hakka sahip olduğu belirtildikten sonra bu hakların hangi sebeplerle ve nasıl sınırlanacağı açıkça düzenlenmiştir.

Kişisel verilerin korunması hakkının düzenlendiği 20. Maddenin üçüncü fıkrasında ise böyle bir düzenlemeye yer verilmemiş sadece hakkın sınırlama yönteminden bahsedilmiştir.

Doktrinde, Anayasanın özel yaşamın gizliliği ve haberleşme özgürlüğüne ilişkin hükümleri ile temel hak ve özgürlüklerin sınırlanmasının sınırlarını belirleyen 13. madde hükmünün birlikte okunması gerektiği, 13. madde hükmünde açıkça temel hak ve özgürlüklerin "yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak" sınırlandırılabilmesi ifade edildiği, 20. maddenin ikinci fıkrasındaki sınırlama ise yalnızca kişilerin üstünün, özel kâğıtlarının ve eşyasının aranması ve bunlara el konulmasına ilişkin olduğu, belirli açılardan kişisel verilerin korunması kapsamında değerlendirilebilecek konut dokunulmazlığı ve haberleşme özgürlüğüne getirilebilecek sınırlamaların kurallarının ise 21. ve 22. maddelerde

düzenlendiği, bu nedenle özel yaşamın gizliliği hakkının, belirtilen özel görünümleri dışında Anayasa'da mutlak olarak korunduğu, kişisel verilerin korunması hakkını da bu kapsamda değerlendirerek bu korunmadan yararlanması gerektiği belirtilmiştir Küzeci, 2010: s. 269).

Kanaatimizce, Anayasanın bu fıkrasına da diğer maddelerde olduğu gibi kişisel verilerin korunması hakkının sınırlama sebepleri, uluslararası belge ve sözleşmelerde belirlenen ilke ve kurallar dikkate alınarak açıkça yazılmalıdır.

Ayrıca kişisel veriler, kanunda belirlenen hallerde işlenebilecek olsa bile bu kanunun mutlaka 13. maddede belirlenen kurallara uyun olması gerekmektedir.

Diğer yandan kişisel veriler sadece özel hayatı gizliliği hakkı ile ilişkili değildir. Anayasa da kişisel verileri dolaylı da olsa koruyan başka hükümler de bulunmaktadır. Anayasanın 17. maddesinde düzenlenen “kişinin maddi ve manevi varlığını geliştirme hakkı” ve “düşünce ve kanaat hürriyeti” bu kapsamdadır. Nitekim, 2010 Anayasa değişikliğinden önce bizimde görüşlerine katıldığımız bazı yazarlar kişisel verilerin korunmasının anayasal dayanağını Anayasanın 17. maddesindeki “kişinin maddi ve manevi varlığını geliştirme hakkı” nda bulduğunu ifade etmişlerdir (Şimşek, 2008: s. 111; Özdemir, 2009: s. 80-81; Aksoy, 2010: s. 71).

Yine bireylerin temel hak ve hürriyetlerinin daha özelde kişisel verilerinin meşru bir temele dayanmadan işlendiği durumlarda kişilerin birtakım güvencelere sahip olduğu Anayasanın “temel hak ve hürriyetlerin korunması” başlıklı 40. maddesinden anlaşılmaktadır. 40. maddenin birinci fıkrasında, Anayasa ile tanınmış hak ve hürriyetleri ihlal edilen herkesin, yetkili makama geciktirilmeden başvurma imkânının sağlanmasını isteme hakkına sahip olduğu, ikinci fıkrasında ise devletin işlemlerinde, ilgili kişilerin hangi kanun yolları ve mercilere başvuracağını ve sürelerini belirtmek zorunda olduğu hüküm altına alınmıştır. Bu kapsamda kişisel verilerinin korunması hakkının ihlal edildiğini iddia eden kimseler, henüz kişisel verilerin korunmasını ülke çapında denetleyecek bir Kişisel Verileri Koruma Kurulu veya Veri Denetim Otoritesi oluşturulmadığından, bu durumun düzeltilmesi için ilgili kurum veya kuruluşa başvurabileceği gibi yargı organlarına da başvurabileceklerdir.

Kişisel verilerin korunması ile ilişkili bir diğer önemli Anayasa hükmü ise “Milletlerarası andlaşmaları uygun bulma” başlıklı 90. maddededir. 90. maddenin son fıkrası uyarınca göre yürürlüğe konulmuş uluslararası antlaşmalar kanun hükmündedir ve bunlar hakkında Anayasaya aykırılık iddiası ile Anayasa Mahkemesine başvurulamaz. Maddenin son fıkrasının son cümlesinde ise, *“usulüne göre yürürlüğe konulmuş temel hak ve özgürlüklere ilişkin milletlerarası andlaşmalarla kanunların aynı konuda farklı hükümler içermesi nedeniyle çıkabilecek uyuşmazlıklarda milletlerarası andlaşma hükümlerinin esas alınacağı”* belirtilmiştir. Konuyla ilgili olarak burada karşımıza AİHS ve kişisel verilerin korunmasına ilişkin 108 nolu AK Sözleşmesi çıkmaktadır. 108 nolu Sözleşme henüz onaylanmadığı için ülkemiz açısından yürürlüğe girmemiş olsa da, AİHS, Anayasanın 90. maddesi gereği bir iç hukuk kuralı haline gelmiştir. Çalışmamızın başında da belirtildiği üzere, Sözleşmenin yorumlayıcısı olan AİHM kişisel verilerin korunmasını Sözleşmenin 8. maddesi kapsamında değerlendirmektedir (Şen, 1996: s. 70). Bu nedenle AİHS kapsamı ve AİHM içtihatları iç hukukumuz açısından büyük önem arz etmektedir.

Anayasa Mahkemesi de, AİHM’ne benzer şekilde, kişisel verilerin korunmasını Anayasanın 20. ve 25. maddeleri kapsamında yorumlamıştır. Mahkemenin 20.03.2008 tarihinde 5429 sayılı Türkiye İstatistik Kurumu Kanunu’nun, istatistiksel birimlerin kendilerinden istenen veri veya bilgileri, vermekle yükümlü olduklarına ilişkin 8. maddesi ve bu yükümlülüğe uymayanların para cezası ile cezalandırılmalarını öngören 54. maddesinin ikinci fıkrasının (b) bendinin iptaline ilişkin verdiği karar bu kapsamdadır¹¹¹. Mahkeme kararında aşağıdaki hususlar belirtilmiştir:

“Başvuru kararında, 5429 sayılı Yasa’da yer alan, istatistiki birimlerin kendilerinden istenen veri veya bilgileri, Başkanlığın belirleyeceği şekil, süre ve standartlarda eksiksiz, doğru ve ücretsiz olarak vermekle yükümlü olduklarına ilişkin 8. maddesiyle bu yükümlülüğe uymayanların para cezasıyla cezalandırılacaklarına ilişkin 54. maddesinin ikinci fıkrasının (b) bendi hükümlerinin eşitlik ilkesi, temel hak ve hürriyetlerin niteliği, kişi hürriyeti ve güvenliği, özel hayatın gizliliği, düşünce ve

¹¹¹ AYM’nin, 25 Haziran 2008 tarihli ve 26917 sayılı Resmi Gazetede yayınlanan 2006/167 Esas; 2008/86 Karar ve 20.3.2008 tarihli kararı

kanaat hürriyetine ilişkin düzenlemelere aykırı olduğu, temel hak ve hürriyetlerin kanunla sınırlanabileceği ve bu sınırlamanın demokratik toplum düzeninin gereklerine aykırı olamayacağı, kişilerin her ne sebeple ve amaçla olursa olsun düşünce ve kanaatlerini açıklamaya zorlanarak yerine getirmeyenlerin cezai ya da idari bir yaptırımla karşı karşıya bırakılmasının hukuk devleti ilkesine aykırılık teşkil edeceği düşüncesiyle itiraz konusu kuralların, Anayasa'nın Başlangıç'ı ile 2., 5., 6., 10., 11., 12., 13., 17., 19., 20. ve 25. maddelerine aykırı olduğu ileri sürülmüştür.

İstatistik, verilerin toplanması, düzenlenmesi ve uygun yöntemlerle analiz edilerek sonuçların yorumlanmasıdır. İstatistikten söz edebilmek için önce "veri"ye ihtiyaç vardır. Veriler, araştırma yapılacak konu ile ilgili bilinen veya herhangi bir kaynaktan doğrudan ya da dolaylı olarak elde edilen bilgilerdir. Verilerin doğrudan toplanmasında anket, gözlem, deney gibi yöntemlerin kullanıldığı bilinmektedir. Anket en çok kullanılan yöntem olup, bu yöntem de önceden hazırlanan anket formu/formları çeşitli şekillerde veri kaynağına (istatistik birimlerine) ulaştırılmaktadır.

5429 sayılı Yasa'nın 2. maddesinin (h) bendine göre istatistiki birim, yapılan sayım veya örnekleme çalışmalarına konu olan, hakkında veri toplanacak gerçek ve tüzel kişiler ile kurum ve kuruluşları ifade etmektedir.

İtiraza konu 8. madde hükmüyle sayım ve örnekleme çalışmalarına konu olan, hakkında veri toplanacak gerçek ve tüzel kişiler ile kurum ve kuruluşların yetkililerine cevap verme yükümlülüğü getirilmiş, bu yükümlülüğe uymayanların da 54. maddede gösterilen biçimde idari para cezasıyla cezalandırılması öngörülmüştür.

Maddede açıklayıcı bir düzenleme bulunmadığı için, "kişisel veri" veya "isteme bağlı veri" olarak adlandırılan, belirli veya belirlenebilir kişilerle ilgili her türlü bilgilerin istenebileceği kuşkusuzdur. İstatistiki birimlerin kendilerinden istenen bilgileri belirlenen şekil ve sürede eksiksiz ve hatasız olarak vermek zorunluluğuna uyulmaması idari para cezası yaptırımına bağlanmış olmasına karşın, istenilecek veri ve bilginin kapsamı ya da sınırlarının ne/neler olacağına, başka bir anlatımla temel hak ve özgürlüklere müdahale niteliğinde olan veri ve bilgilerin bu zorunluluk kapsamında bulunup bulunmadığına ilişkin herhangi bir düzenlemeye rastlanmamaktadır. Dolayısıyla, istatistikî birimler kendilerinden istenildiği takdirde

her türlü bilgiyi temel hak ve özgürlüklerine müdahale niteliğinde olsa bile vermek zorundadırlar. Anayasa 'nın 20. maddesinde herkesin özel hayatına ve aile yaşayışına saygı gösterilmesini isteme hakkına sahip olduğu; 25. maddesinde de herkesin düşünce ve kanaatlerini açıklama hürriyetine sahip olduğu, her ne sebep ve amaçla olursa olsun kimsenin düşünce ve kanaatlerini açıklamaya zorlanamayacağı hüküm altına alınmıştır. 20. madde gerekçesinde, özel hayatın korunmasının her şeyden önce bu hayatın gizliliğinin korunması, resmi makamların özel hayata müdahale edememesi anlamına geldiği belirtilmiştir. AİHM kararlarında belirtildiği gibi, özel hayat bütün unsurlarıyla tanımlanamayacak kadar geniş bir kavram olup devletin yetkili temsilcileri tarafından ilgililerin rızası olmaksızın bilgi toplamasının her zaman söz konusu özel hayatını ilgilendireceği kuşkusuzdur. Anket formlarında yer alan bazı sorular özel yaşamın gizliliği ile düşünce ve kanaatin açıklanması sonucunu doğurabilir. Bir ülkede en güçlü veri tekeli idaredir. Bu gücün sınırlandırılması özel yaşamın ve düşünce ve kanaat özgürlüğünün korunması bakımından önemlidir. Anayasa 'nın 20. ve 25. maddelerinde yer alan güvencelere rağmen itiraza konu 8. madde hükmüyle kişiler, bilgi toplama, saklama, işleme ve değiştirme tekeli olan idareye ve diğer kişilere karşı korumasız bırakılmış, veri toplamanın sınırlarına yasal düzenlemede yer verilmemiştir. Açıklanan nedenlerle itiraz konusu kuralların Anayasanın 20. ve 25. maddelerine aykırı olduğundan iptali gerekir” (Küzeci, 2010, s. 274).

3. KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN YASAL DÜZENLEMELER

Kişisel verilerin korunmasına ilişkin daha önce de değinildiği üzere gerek kamu hukuku gerek özel hukuk dallarında çeşitli koruyucu hükümler bulunmaktadır.

3.1. 4721 sayılı Türk Medeni Kanun

Dah öncede değinildiği üzere kişisel verilerin korunması hakkı kişilik hakkının özel bir görünümüdür (Aksoy, 2010: s. 80). Nitekim Anayasada da bu şekilde bir tercih yapılarak özel hayatın gizliliği, kişisel verilerin korunması, haberleşme hürriyeti gibi haklar kişinin hak ve ödevleri bölümünde düzenlenmiştir. Bu nedenle, kişisel verilerin 4721 sayılı Türk Medeni Kanun'un (TMK) kişiliği koruyan hükümleri çerçevesinde korunabilecektir. Bu kapsamda kişisel verilerin hukuka aykırı işlenmesi durumunda bireyler TMK'nın 24. maddesi çerçevesinde

kişilik haklarının saldırıya uğradığını iddia ederek korunmasını talep edebileceklerdir.

Türk Medeni Kanununun 24. maddesi:

“Hukuka aykırı olarak kişilik hakkına saldırılan kimse, hâkimden, saldırıda bulunanlara karşı korunmasını isteyebilir.

Kişilik hakkı zedelenen kimsenin rızası, daha üstün nitelikte özel veya kamusal yarar ya da kanunun verdiği yetkinin kullanılması sebeplerinden biriyle haklı kılınmadıkça, kişilik haklarına yapılan her saldırı hukuka aykırıdır.” Şeklindedir.

TMK’nın 24. maddesiyle kişilik haklarına saldırı durumunda kişilik haklarının korunması düzenlenmiştir. Buna göre maddede sayılan haklı sebepler yokken kişinin haklarına saldırı hukuka aykırı olacaktır.

Bu kapsamda kişinin, gizli ve özel yaşam alanına yönelen saldırılara karşı Türk Medeni Kanunu kapsamında belirli oranda koruma bulunmaktadır. Kişinin gizli alanına sızarak sırlarını öğrenme, teknik aygıt ve araçlarla kaydetme, resmini ve filmini çekme, ayrıca bunları yayma ve aktarma bu kapsamda kişiye yönelebilecek saldırıların türlerini oluşturmaktadır ve bu eylemler Medeni Kanunun 24. Maddesi uyarınca hukuka aykırı olacaktır (Küzeci, 2010: s. 276).

TMK’nın 25. maddesinde ise kişilik haklarına hukuka aykırı saldırı durumunda açılacak davalar düzenlenmiştir. 25. Madde:

“Davacı, hâkimden saldırı tehlikesinin önlenmesini, sürmekte olan saldırıya son verilmesini, sona ermiş olsa bile etkileri devam eden saldırının hukuka aykırılığının tespitini isteyebilir.

Davacı bunlarla birlikte, düzeltmenin veya kararın üçüncü kişilere bildirilmesi ya da yayımlanması isteminde de bulunabilir.

Davacının, maddî ve manevî tazminat istemleri ile hukuka aykırı saldırı dolayısıyla elde edilmiş olan kazancın vekâletsiz iş görme hükümlerine göre kendisine verilmesine ilişkin istemde bulunma hakkı saklıdır.

Manevî tazminat istemi, karşı tarafça kabul edilmiş olmadıkça devredilemez; mirasbırakan tarafından ileri sürülmüş olmadıkça mirasçılara geçmez.

Davacı, kişilik haklarının korunması için kendi yerleşim yeri veya davalının yerleşim yeri mahkemesinde dava açabilir.” Şeklindedir.

Görüldüğü üzere kişisel verilerinin hukuka aykırı bir şekilde kaydedildiğini veya kullanıldığını düşünen bir kişi Medeni Kanun hükümlerinden yararlanarak bu ihlalin önlenmesini, durdurulmasını veya tespitini isteyebileceği gibi, bu ihlal nedeniyle bir zarara uğramış ise bu zararların da tazminini isteyebilecektir.

Aynı şekilde benzer bir koruma da 6098 sayılı Türk Borçlar Kanununda bulunmaktadır. Türk Borçlar Kanunun 49. Maddesine göre, haksız bir fiille bir başkasına zarar veren kişi bu zararı gidermekle yükümlü tutulmuştur. Madde metni:

“Kusurlu ve hukuka aykırı bir fiille başkasına zarar veren, bu zararı gidermekle yükümlüdür.

Zarar verici fiili yasaklayan bir hukuk kuralı bulunmasa bile, ahlaka aykırı bir fiille başkasına kasten zarar veren de, bu zararı gidermekle yükümlüdür.” Şeklindedir.

Kişisel verilerin hukuka aykırı şekilde ele geçirilmesi, kaydedilmesi, başkalarına verilmesi eylemleri suç oluşturmalarının yanında aynı zamanda haksız fiil de oluşturmaktadır. Yapılan bu haksız fiilin sonucu olarak ta kişinin maddi ve manevi tazminat hakları bulunmaktadır (BK m. 51-52).

Diğer taraftan Medeni Kanun’da bu alana yönelen saldırıların meşru görüldüğü durumlar da bulunmaktadır. Verileri hukuka aykırı olarak ele geçirilen veya kullanılan kişinin rızasının bulunması, müdahalenin kamu yararının gerekliliklerinden kaynaklanması, verilerin tarihsel ve bilimsel amaçlarla kullanılması ya da başkalarının haklı çıkarlarının bulunması bu duruma örnek verilebilir¹¹².

Görüldüğü üzere Medeni Kanun, kişisel verileri dolaylı da olsa belirli oranda korumaktadır. Ancak bu koruma yetersizdir. Zira Medeni Kanundaki düzenlemelere bakıldığında kişilik hakkına müdahale gerçekleştikten sonra yapılabilecek işlemleri kapsadığı görülecektir. Yani önleyici nitelikte değildir. Kişisel verilerin hukuka

¹¹² Nitekim Medeni Kanunun 24. maddesinin ikinci fıkrası, “Kişilik hakkı zedelenen kimsenin rızası, daha üstün nitelikte özel veya kamusal yarar ya da kanunun verdiği yetkinin kullanılması sebeplerinden biriyle haklı kılınmadıkça, kişilik haklarına yapılan her saldırı hukuka aykırıdır.” Şeklinde hukuka uygunluk nedenlerinin varlığı halinde müdahalenin meşru olacağını belirtmiştir.

uygun bir şekilde işlenmesi düzenlenmemiştir. Bu nedenle konuyla ilgili kapsayıcı, temel ilkeleri, işleme koşullarını, denetleyici otoriteyi ve hak ihlalleri olduğunda uygulanabilecek yaptırımları düzenleyen müstakil bir kanuna ihtiyaç bulunmaktadır.

3.2. 4857 sayılı İş Kanunu

4857 sayılı İş Kanunda kişisel verilerin korunmasına yönelik yeterli olmasa da bir kısım düzenlemeler bulunmaktadır. Bu düzenlemelerden en önemlisi, işverenin özlük dosyası tutma yükümlüğünün düzenleyen 75. maddedir¹¹³.

Buna göre işveren, çalıştırdığı her işçi için bir özlük dosyası düzenlemek ve bu dosya da işçinin kimlik bilgilerinin yanında, düzenlemek zorunda olduğu her türlü belgeyi saklamak ve bunları istendiği zaman yetkili memur ve mercilere göstermekle yükümlü tutulmuştur. Ayrıca Kanun işverene, işçi hakkında edindiği bilgileri dürüstlük kuralları ve hukuka uygun olarak kullanma ve gizli kalmasında işçinin haklı çıkarı bulunan bilgileri açıklamama ödevi de getirmiştir.

Buna göre, işçi hakkında, işveren tarafından kaydedilen veriler ister fiziki ortamlarda ister elektronik ortamda depolansın tüm verilerin 75. maddenin ikinci fıkrasındaki korumadan yararlanması gerekir. Bu aynı zamanda işverenin gözetme borcunun da bir gereğidir (Sevimli, 2006: s. 118).

Ancak görüleceği üzere buradaki düzenleme işçi işveren ilişkisi başladıktan sonra devreye girmektedir. İş akdi kurulmadan önce de verilerin kaydedilmesi gerekebilir. Örneğin işveren, iş sözleşmesi yapmayı düşündüğü kişiden karar verme aşamasında bazı bilgiler isteyebilir. Başvuran kişinin, adı, soyadı, ikametgâh adresi, eğitim durumu, daha önce çalıştığı yerler ve buralardan aldığı referanslar bu kapsamda sayılabilir. Bu aşamada eğer iş ilişkisi oluşmazsa bu bilgilerin akıbetinin ne olacağına ilişkin bir hüküm bulunmamaktadır. Bu bilgiler hasas verilere ilişkin olması durumunda kişinin görebileceği zarar daha da büyük olabilecektir (Küzeci, 2010: s. 280).

¹¹³ “İşçi özlük dosyası” başlıklı madde şöyledir:

Madde 75 – “İşveren çalıştırdığı her işçi için bir özlük dosyası düzenler. İşveren bu dosyada, işçinin kimlik bilgilerinin yanında, bu Kanun ve diğer kanunlar uyarınca düzenlemek zorunda olduğu her türlü belge ve kayıtları saklamak ve bunları istendiği zaman yetkili memur ve mercilere göstermek zorundadır.

İşveren, işçi hakkında edindiği bilgileri dürüstlük kuralları ve hukuka uygun olarak kullanmak ve gizli kalmasında işçinin haklı çıkarı bulunan bilgileri açıklamamakla yükümlüdür.”

Bu alanda üzerinde durulması gereken diğ er bir hususta, iř inin internet ve e-posta kullanımının denetlenmesine iliř kin  zel bir d zenleme bulunmamasıdır. Ger ekten de bu konuda iř  hukukuna iliř kin mevzuatımızda a ık h k mler bulunmamaktadır. Bu konuda  ıkan veya  ıkabilecek ihtilaflar, ancak, Anayasa  er evesinde, Medeni Kanunda yer alan genel h k mlere (m. 24, 25) ve T rk Ceza Kanununda yer alan h k mlere bařvurularak   z lebilmektedir (Sevimli, 2006: s. 118).

Bu nedenle hukukumuz bakımından, kiř isel verilerin korunmasına iliř kin bir yasal d zenleme yapılması ve bunun iř i-iř veren iliř kisinde nasıl uygulanacağına iliř kin  alıřmalar yapılması ve mevcut İř  Kanunu ile alt d zenlemelerin kiř isel verilerin korunmasına iliř kin kanun ile uyumlu hale getirilmesinin elzem olduėu deėerlendirilmektedir.

3.3. 5490 sayılı N fus Hizmetleri Kanunu

Sosyal devletin gerekliliklerinin yerine getirilmesi, planlama hizmetleri, g venliėin saėlanması, su luluėun  nlenmesi ve su luların yakalanması gibi g revleri dolayısıyla devletler, kiř isel verileri toplamakta, iř lemekte ve kullanmaktadırlar. Bu veri toplama iř lemi kiř inin doėumundan  l me kadar s rmektedir. Bu nedenle idare,  ok b y k bir bilgi g c ne sahiptir.

Bu kapsamda Devletlerin  ncelikli olarak topladıkları veriler kiř ilerin kimlik ve adres bilgileridir. 5490 sayılı N fus Hizmetleri Kanunun 1. maddesinde kanunun amacının “Kiř inin doėumundan  l m ne kadar kiř isel ve medeni durumuna, uyrukluėuna ve bunlarda meydana gelebilecek deėiř ikliklere ait doėal ve hukuki olayların belirlenip saptanması, bu ama la d zenlenmiř  k t klere yazılması, elektronik ortamda ulusal adres veri tabanının oluřturulması, n fus kayıtları ile adres bilgilerinin iliř kilendirilmesini saėlamak” olduėu ifade edilmiř tir.

Bu amacın ger ekleřtirilmesi i in idare kiř inin doėumuyla birlikte adı, soyadı, kimlik numarası, ailesinin kimlik bilgileri ve adres bilgilerini kayetmekte ve bunları kamu hizmetlerinin verilmesinde kullanmaktadır.

N fus Kanunun 7. maddesinde de aile k t klerine kaydedilecek kiř isel verilerin hangileri olduėu belirtilmiř tir. 7. Maddeye g re;

a) T rkiye Cumhuriyeti kimlik numarası,

b) Kayıtlı bulunduğu il, ilçe, köy veya mahalle adı ile cilt, aile ve birey sıra numarası,

c) Kişinin adı ve soyadı, cinsiyeti, baba ve ana adı ile soyadları, evli kadınların önceki soyadları,

ç) Doğum yeri ile gün, ay ve yıl olarak doğum tarihi ve kütüğe kayıt tarihi,

d) Evlenme, boşanma, soybağının kurulması veya reddi, ölüm, vatandaşlığın kazanılması veya kaybedilmesi gibi kişisel durumda meydana gelen değişiklik veya yetkili makamlarca yapılan düzeltmeler,

e) Dini,

f) Medenî hali,

g) Yerleşim yeri adresi,

ğ) Fotoğrafi,

Aile kütüğüne kaydedilmektedir.

Ancak bu kayıtların kişilerin özel hayatının korunması ve kişisel verilerinin korunması açısından gizli olması gerekmektedir. Bu nedenle Nüfus Kanunun 9. Maddesinde bu kayıtların gizli olduğu hüküm altına alınmıştır. “Gizlilik” başlıklı 9. madde metni şöyledir:

“(1) Nüfus kayıtları ve bu kayıtların tutulmasına dayanak olan belgeler gizlidir. Bunlar, yetkili ve sorumlu memurlar ile teftiş ve denetim yetkisi olanlar dışında kimse tarafından görülüp incelenemez. Mahkemeler bu hükmün dışındadır.

(2) Nüfus kayıtlarına bu bilgileri işleyen memurlar ve Kimlik Paylaşımı Sistemi kapsamında nüfus kayıtlarından faydalanan diğer görevliler de bu gizliliğe uymak zorundadırlar. Bu yükümlülük, kamu görevlilerinin görevlerinden ayrılmalarından sonra da devam eder.”

Ülkemizde idare, üzerine düşen görevleri yerine getirebilmek için kişisel verileri toplamakta, kullanmakta, işlemekte ve kimi zaman üçüncü kişilere aktarmaktadır. Bu işlemleri yaparken de artan oranda bilişim sistemlerinden yararlanıldığı görülmektedir. Bu kapsamda Merkezi Nüfus İdaresi Sistemi (MERNİS), Kimlik Paylaşım Sistemi, kullanılan elektronik sistemlerdir. Nüfus

kanunun 45. Maddesine göre¹¹⁴, Kimlik Paylaşımı Sistemi veri tabanındaki bilgilerin tamamı veya bir kısmı toplu halde hiçbir kuruma veya diğer kişilere verilemez. Kurumlar ve diğer kişiler kendi iş ve işlemlerine esas olmak üzere sadece kayıtlarını tuttukları kişilerin bilgilerini alabilirler. Bu hüküm önemlidir. Zira devletin birçok kurumu neredeyse kişilerin bütün bilgilerine ulaşmak istmektedirler. Bu hükme göre ise kurumlar ancak görev alanlarına giren konularda sadece ilgili kişilerin bilgilerini talep edebileceklerdir.

3.4. 213 sayılı Vergi Usul Kanunu

Kişisel verilerin toplanmasına ilişkin olarak 213 sayılı Vergi Usul Kanunu'nda, Maliye Bakanlığının vergi yükümlüleri hakkında bilgi toplama ve saklamaya yetkisine ilişkin özel hükümler bulunmaktadır. 148. madde konuya örnek olarak verilebilir. Maddeye göre; kamu idare ve müesseseleri, mükellefler veya mükelleflerle muamelede bulunan diğer gerçek ve tüzel kişiler, Maliye Bakanlığının veya vergi incelemesi yapmaya yetkili olanların isteyecekleri bilgileri vermeye mecburdurlar. Bilgiler yazı veya sözle istenilir (Kılınç, 2012:s. 1135).

Maliye Bakanlığının topladığı bu bilgilerin saklanmasında gizlik esastır. Nitekim Vergi Usul Kanunun “İstihbarat arşivi” başlıklı 152. maddesinde toplanan bilgilerin istihbarat arşivinde gizli olarak saklanacağı hüküm altına alınmıştır¹¹⁵.

¹¹⁴ Nüfus Kanunun “Kimlik ve Adres Paylaşımı Sistemlerinin kullanılması” başlıklı 45. Maddesi şöyledir:

MADDE 45- (1) Bakanlık, Kimlik Paylaşımı Sistemi ve Adres Paylaşımı Sistemi veri tabanlarında tutulan bilgileri bu Kanunda belirtilen esas ve usüller çerçevesinde kurumlar ile diğer kişilerin hizmetine açabilir. Yerleşim yeri adresi bilgileri ancak kurumlar ile 5411 sayılı Bankacılık Kanunu çerçevesinde faaliyette bulunan bankaların ve 3/6/2007 tarihli ve 5684 sayılı Sigortacılık Kanunu çerçevesinde faaliyette bulunan sigorta ve emeklilik şirketleri ile Güvence Hesabının paylaşımına açılabilir.

(2) Kimlik Paylaşımı Sistemi veri tabanındaki bilgilerin tamamı veya bir kısmı toplu halde hiçbir kuruma veya diğer kişilere verilemez. Kurumlar ve diğer kişiler kendi iş ve işlemlerine esas olmak üzere sadece kayıtlarını tuttukları kişilerin bilgilerini alabilirler.

(3) Kurumlar aldıkları bilgileri tanımlanmış hizmetlerin yerine getirilmesi dışında başka hiçbir amaçla kullanamaz; ilgisi veya bu Kanunun 44 üncü maddesinde belirtilenler dışında kimseye veremez. Sistemin bütün aşamalarında görev yapan yetkililer de bu kurallara uymakla yükümlüdür. Bu yükümlülük, kamu görevlilerinin görevlerinden ayrılmalarından sonra da devam eder.

(4) Genel Müdürlükten alınan bilgilerin iş ve işlemlerde kullanılmasının hukukî sonuçları bilgiyi alan kurumun sorumluluğundadır.

(5) Bu Kanun ile kurulacak veri tabanlarının istatistik amaçlı kullanımında 10/11/2005 tarihli ve 5429 sayılı Türkiye İstatistik Kanunu hükümleri uygulanır.”

¹¹⁵ “**Madde 152** – 150 nci maddedekiler hariç olmak üzere bu bölümde yazılı kaynaklardan toplanacak bilgiler istihbarat arşivlerinde gizli olarak saklanır.

Bu arşivlerden kimlerin ve ne suretle faydalanabileceği Maliye Bakanlığınca tesbit olunur.”

Ancak maddenin ikinci fıkrasıyla bunun usul ve esaslarının Maliye Bakanlığınca belirlenecek olması bir başka deyişle bu hususun idarenin takdirine bırakılması, temel haklara ilişkin konuların kanunla düzenlenmesi gerektiği kuralına uymadığını düşünmekteyiz.

Vergiye ilişkin kişisel veriler veya verilerin korunması ile ilgili olarak, Danıştay'ın da kararları bulunmaktadır¹¹⁶. Bu kararlarda da gizlilik vurgusu yapılmıştır.

3.5. 2559 sayılı Polis Vazife ve Salahiyet Kanunu

2559 sayılı Polis Vazife ve Salahiyet Kanununda (PVSK) çeşitli kamu hizmetlerinin verilmesi ve kamu güvenliğinin sağlanması ile suçun önlenmesi amaçları için bazı kişisel verilerin toplanabilmesine izin verilmektedir. PVSK'da kişisel veri niteliğinde olan kişilerin, parmak izi ve fotoğrafların kayda alınması ile istihbarat amaçlı iletişimin tespiti konularında özel hükümler bulunmaktadır.

PVSK'nın 5. maddesine göre polis, her çeşit silah ruhsatı, sürücü belgesi, pasaport veya pasaport yerine geçen belge almak için başvuruda bulunan, başta polis olmak üzere, genel veya özel kolluk görevlisi ya da özel güvenlik görevlisi olarak istihdam edilen, Türk vatandaşlığına başvuruda bulunan, sığınma talebinde bulunan veya gerekli görülmesi halinde, ülkeye giriş yapan sair yabancı ve gözaltına alınan kişilerin parmak izini alır ve buna ilişkin oluşturulan sisteme kaydeder.

Sisteme kaydedilen bilgiler, kimlik tespiti, suçun önlenmesi veya yürütülmekte olan soruşturma ve kovuşturma kapsamında maddî gerçeğin ortaya çıkarılması amacıyla mahkeme, hâkim, Cumhuriyet savcısı ve kolluk tarafından kullanılabilir (m. 5/6).

Yine 5. maddenin sekizinci fıkrasına göre, sistemde kayıtlı bilgilerin hangi kamu görevlisi tarafından ve ne amaçla kullanıldığının denetlenebilmesine imkân tanıyan bir güvenlik sistemi kurulur. Sistemde yer alan kayıtlar gizlidir ve 5. maddede belirlenen amaçlar dışında kullanılamaz. Sisteme kayıtlı olan parmak izi ve

¹¹⁶ Danıştayın 1984 tarihli bir kararında; kamu yönetimlerinin, vergi sırrı bağlamında elde ettiği bazı kişisel verileri diğer kamu birimlerine iletmesini, kamu idaresinin bir bütün olduğundan bahisle verip veremeyeceği tartışılmış ve sonuç olarak bu veri gizliliğinin kişilerin buna duyduğu güven sayesinde vergi gelirlerini artırdığı belirtilmiştir. Ayrıca gizli belge ve bilgilerin sırf bu sebeple açıklanmaması gerektiğine karar verilmiştir. Bkz. Danıştay. 1. D. 20.12.1984 T. E. 1984/291, K.1984/294

fotoğraflar, kişinin ölümünden itibaren on yıl ve her halde kayıt tarihinden itibaren seksen yıl geçtikten sonra sistemden silinir (m. 5/9-10).

Ayrıca PVSK'nın EK 7. maddesi uyarınca polisin istihbarat kapsamında bilgi toplama ve iletişimi denetleme yetkisi de bulunmaktadır. Buna göre Polis, Devletin ülkesi ve milletiyle bölünmez bütünlüğüne, Anayasal düzenine ve genel güvenliğine dair önleyici ve koruyucu tedbirleri almak, emniyet ve asayişini sağlamak üzere, ülke seviyesinde istihbarat faaliyetlerinde bulunur, bu amaçla bilgi toplar, değerlendirir, yetkili mercilere veya kullanma alanına ulaştırır. Devletin diğer istihbarat kuruluşlarıyla işbirliği yapar. Belli suçların işlenmesini önlemek amacıyla hâkim kararı veya gecikmesinde sakınca bulunan hallerde Emniyet Genel Müdürü veya İstihbarat Dairesi Başkanının yazılı emriyle, telekomünikasyon yoluyla yapılan iletişim tespit edilebilir, dinlenebilir, sinyal bilgileri değerlendirilebilir veya kayda alınabilir.

Bu madde hükümlerine göre yürütülen faaliyetler çerçevesinde elde edilen kayıtlar, birinci fıkrada belirtilen amaçlar dışında kullanılamaz. Elde edilen bilgi ve kayıtların saklanması ve korunmasında gizlilik ilkesi geçerlidir. Bu fıkra hükümlerine aykırı hareket edenler hakkında, görev sırasında veya görevden dolayı işlenmiş olsa bile Cumhuriyet savcılarınca doğrudan soruşturma yapılır (m. Ek 7/7).

3.6. 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu

Devlet istihbaratının istihsalı ve kullanılması ile Milli İstihbarat Teşkilatının kuruluş, görev ve faaliyetlerine ait esas ve usulleri düzenleyen 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunuyla Milli İstihbarat Teşkilatına¹¹⁷, kişisel verilerin toplanması ve kaydedilmesi ve kullanılmasına ilişkin önemli yetkiler verilmiştir. Hatta 26.04.2014 tarihli Resmi Gazetede yayınlanarak yürürlüğe giren 17.04.2014 tarihli ve 6532 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanununu ile Milli İstihbarat Teşkilatı Kanununda Değişiklik Yapılmasına Dair Kanunla, 2937 sayılı Kanunda önemli değişiklikler yapılarak, MİT'e, görevi ile ilgili de olsa, sınırsız bir şekilde veri toplama yetkisi verilmiştir. MİT'in toplayacağı veriler içerisinde kişisel verilerin de olduğu muhakkaktır.

¹¹⁷ Bundan sonra "MİT" olarak kullanılacaktır.

MİT'in veri toplama, kaydetme ve analiz etme yetkilerine geçmeden önce, yukarıda belirtilen kapsamlı kanun değişikliği nedeniyle, MİT'in görev ve yetkilerini kısaca açıklamakta fayda bulunmaktadır.

2937 sayılı Kanunun 4. maddesine göre MİT'in görevleri şunlardır:

*“a) Türkiye Cumhuriyetinin ülkesi ve milleti ile bütünlüğüne, varlığına, bağımsızlığına, güvenliğine, Anayasal düzenine ve milli gücünü meydana getiren bütün unsurlarına karşı içten ve dıştan yöneltilecek mevcut ve muhtemel faaliyetler hakkında **milli güvenlik istihbaratını Devlet çapında oluşturmak ve bu istihbaratı Cumhurbaşkanı, Başbakan, Genelkurmay Başkanı, Milli Güvenlik Kurulu Genel Sekreteri ile gerekli kuruluşlara ulaştırmak.***

b) Devletin milli güvenlik siyasetiyle ilgili planların hazırlanması ve yürütülmesinde; Cumhurbaşkanı, Başbakan, Genelkurmay Başkanı, Milli Güvenlik Kurulu Genel Sekreteri ile ilgili bakanlıkların istihbarat istek ve ihtiyaçlarını karşılamak.

c) Kamu kurum ve kuruluşlarının istihbarat faaliyetlerinin yönlendirilmesi için Milli Güvenlik Kurulu ve Başbakana tekliflerde bulunmak.

d) Kamu kurum ve kuruluşlarının istihbarat ve istihbarata karşı koyma faaliyetlerine teknik konularda müşavirlik yapmak ve koordinasyonun sağlanmasında yardımcı olmak.

e) Genelkurmay Başkanlığınca Silahlı Kuvvetler için lüzum görülecek haber ve istihbaratı, yapılacak protokole göre Genelkurmay Başkanlığına ulaştırmak.

f) Milli Güvenlik Kurulunda belirlenecek diğer görevleri yapmak.

g) İstihbarata karşı koymak.

*h) **Dış güvenlik, terörle mücadele ve millî güvenliğe ilişkin konularda Bakanlar Kurulunca verilen görevleri yerine getirmek**¹¹⁸.*

*i) **Dış istihbarat, millî savunma, terörle mücadele ve uluslararası suçlar ile siber güvenlik konularında her türlü teknik istihbarat ve insan istihbaratı usul,***

¹¹⁸ 17.04.2014 tarihli ve 6532 sayılı Kanunun 1 maddesiyle eklenmiştir.

araç ve sistemlerini kullanmak suretiyle bilgi, belge, haber ve veri toplamak, kaydetmek, analiz etmek ve üretilen istihbaratı gerekli kuruluşlara ulaştırmak¹¹⁹.

j) İstihbarat kapasitesini, niteliğini ve etkinliğini artırmak amacıyla çağdaş istihbarat usul ve yöntemlerini araştırmak, teknolojik gelişmeleri takip etmek ve uygun görülenleri temin etmek¹²⁰.”

6532 sayılı Kanunla 2937 sayılı Kanunda değişiklik yapılmadan önce MİT’in görevi, temel olarak ülkemizin bütünlüğüne, varlığına, bağımsızlığına, güvenliğine, Anayasal düzenine ve milli gücünü meydana getiren bütün unsurlarına karşı içten ve dıştan yöneltilecek mevcut ve muhtemel faaliyetler hakkında milli güvenlik istihbaratını Devlet çapında oluşturmak ve bu istihbaratı ilgili kurum ve kuruluşlara ulaştırmak iken, 6532 sayılı Kanunla MİT’e yeni ve önemli görevler verilmiştir.

Buna göre MİT, dış güvenlik, terörle mücadele ve millî güvenliğe ilişkin konularda Bakanlar Kurulunca verilen görevleri yerine getirmekle görevlidir. Dış güvenlik ve terörle mücadele kavramları hukuk sistemimizde yeri olan kavramlar olması nedeniyle görevin kapsamını belirginleştirmek mümkündür. Ancak “millî güvenliğe ilişkin konular” kapsamında MİT’e Bakanlar Kurulunca ne gibi görevler verilebileceğini açıklamak biraz zordur¹²¹.

Dış istihbarat, millî savunma, terörle mücadele ve uluslararası suçlar ile siber güvenlik konularında her türlü teknik istihbarat ve insan istihbaratı usul, araç ve sistemlerini kullanmak suretiyle bilgi, belge, haber ve veri toplamak, kaydetmek, analiz etmek ve üretilen istihbaratı gerekli kuruluşlara ulaştırma görevi de MİT’e verilen yeni bir görevdir. Buna göre MİT, dış istihbarat, millî savunma, terörle mücadele ve uluslararası suçlar ile siber güvenlik konularında her türlü bilgi, belge, haber ve veri toplamak, kaydetmek, analiz etmek ve üretilen istihbaratı gerekli kuruluşlara ulaştıracaktır. Bu kapsamda MİT, görevi ile ilgili kişisel verileri de toplayabilecek, kaydedebilecek ve üçüncü kişilerle paylaşabilecektir.

¹¹⁹ 17.04.2014 tarihli ve 6532 sayılı Kanunun 1 maddesiyle eklenmiştir.

¹²⁰ 17.04.2014 tarihli ve 6532 sayılı Kanunun 1 maddesiyle eklenmiştir.

¹²¹ Bu husus 6532 sayılı Kanunun TBMM İçişleri Komisyonunda görüşülmesi sırasında tartışma konusu olmuş ve bazı milletvekilleri tarafından bu madde için karşı oy yazısı yazılmıştır. Bkz. İçişleri Komisyonu raporu 2/2011 Karar no 17, 563 nolu Sırasıyla,

http://www.tbmm.gov.tr/develop/owa/tasari_teklif_sd.onerge_bilgileri?kanunlar_sira_no=149900

Erişim T: 01.06.2014

Burada dikkat edilmesi gereken husus MİT'in veri toplama yetkisinin görevine giren konularla sınırlı olmasıdır. MİT'in veri/kişisel veri toplayabilmesi için somut durumda verisini toplayacağı kişinin dış istihbarat, millî savunma, terörle mücadele ve uluslararası suçlar ile siber güvenlik konularında, ülke güvenliği için bir tehdit oluşturacak bir durum içerisinde olması gerekir.

Nitekim Avrupa İnsan Hakları Mahkemesi de birçok kararında bu hususa değinmiştir. Mahkeme *Klass ve Diğerleri v. Almanya* davasında¹²², istihbarat örgütlerinin gizli izleme yoluyla bireylerin haklarına yönelik gerçekleştirdikleri müdahalelerin etkili bir denetime tabi olması gerektiğini kabul etmiş ve ulusal güvenlikten kaynaklanan ihtiyaçlara her durumda öncelik verilemeyeceğini, Avrupa ülkelerinin casusluk ve terörizmle mücadeleyi gerekçe göstererek uygun gördükleri her türlü tedbiri alamayacaklarını belirtmiş, mektupların ve telgrafların okunmasına, telefon görüşmelerinin dinlenmesi ve kaydedilmesine olanak tanıyan bir yasanın Sözleşme'ye uygunluğunu incelemiş; genel olarak gizli izleme yöntemlerine demokratik kurumların korunması için kesinlikle zorunlu olması durumunda başvurulabileceğini kabul etmiştir. Ayrıca Mahkeme bu konuda devletlerin sınırsız bir takdir yetkisinin olmadığını, sınırsız önlemler alınmasına izin veren bir yasanın demokrasi için tehdit oluşturacağını, gizli izlemeye olanak tanınması durumunda bunun kötüye kullanılmasının engellenmesi için yeterli ve etkili güvencelerin sağlanması gerektiğini kararında belirtmiştir¹²³.

Benzer şekilde AİHM, 26 Mart 1987 tarihli *Leander-İsveç* kararında¹²⁴, Bay Leander hakkındaki bilgilerin devletin güvenlik birimlerince saklanması, demokratik bir toplumda ulusal güvenliği sağlamak için gerekli olduğuna karar vermiş, ancak söz konusu sicilin varlığının ve kullanımının bazı koruyucu önlemlere tâbi olması gerektiğini belirtmiştir¹²⁵.

MİT'in kişisel verilerin toplanması, kaydedilmesi ve analiz edilmesine ilişkin yetkileri ise 2937 sayılı Kanunun 6. Maddesinde düzenlenmiştir. Buna göre MİT:

Kamu kurum ve kuruluşları, kamu kurumu niteliğindeki meslek kuruluşları, 19/10/2005 tarihli ve 5411 sayılı Bankacılık Kanunu kapsamındaki kurum ve

¹²² *Klass and Others v. Germany*, 5029/71, 06.09.1978.

¹²³ **Atak**, s. 103-104; AİHM Kararları başlıklı kısımdan kararın ayrıntılarına bakılabilir.

¹²⁴ 26 Mart 1987, Seri A No. 116, s. 22 ve 25-27, paragraf 48, 60, 65 ve 67

¹²⁵ **Dutertre**, s. 309. AİHM Kararları başlıklı kısımdan kararın ayrıntılarına bakılabilir.

kuruluşlar ile diğer tüzel kişiler ve tüzel kişiliği bulunmayan kuruluşlardan bilgi, belge, veri ve kayıtları alabilir, bunlara ait arşivlerden, elektronik bilgi işlem merkezlerinden ve iletişim alt yapısından yararlanabilir ve bunlarla irtibat kurabilir (m. 6/1-b).

26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununun İkinci Kitap Dördüncü Kısım Dört, Beş, Altı ve Yedinci bölümlerinde yer alan suçlara (318, 319, 324, 325 ve 332 nci maddeleri hariç olmak üzere) ilişkin soruşturma ve kovuşturmalarda ifade tutanaklarına, her türlü bilgi ve belgeye erişebilir, bunlardan örnek alabilir (m. 6/1-c).

Telekomünikasyon kanallarından geçen dış istihbarat, millî savunma, terörizm ve uluslararası suçlar ile siber güvenlikle ilgili verileri toplayabilir (m. 6/1-g).

Yukarıda değinildiği üzere, Kanunun 6. Maddesiyle MİT'e verilen bu yetkiler MİT'in görev alanıyla sınırlıdır. MİT'in ülke güvenliğini ilgilendirmeyen alanlarda kişisel veri toplaması ve bunları kullanması yasal düzenlemeler karşısında mümkün değildir. Aksi durum ilerki bölümde açıklanacağı üzere kişisel verilere karşı işlenmiş suçları oluşturabilecektir.

MİT ayrıca, 2937 sayılı Kanunun 4 üncü maddesinde sayılan görevlerin yerine getirilmesi amacıyla Anayasanın 2 nci maddesinde belirtilen temel niteliklere ve demokratik hukuk devletine yönelik ciddi bir tehlikenin varlığı halinde Devlet güvenliğinin sağlanması, casusluk faaliyetlerinin ortaya çıkarılması, Devlet sırrının ifşasının tespiti ve terörist faaliyetlerin önlenmesine ilişkin olarak, hâkim kararı veya gecikmesinde sakınca bulunan hallerde MİT Müsteşarı veya yardımcısının yazılı emriyle telekomünikasyon yoluyla yapılan iletişimi tespit edebilir, dinleyebilir, sinyal bilgilerini değerlendirebilir ve kayda alabilir (m. 6/2).

İletişimin tespiti yoluyla elde edilen kayıtları kişisel veri niteliğinde olduğundan bu yetki de önem arz etmektedir. Bu nedenle kanunun 6. maddesinin üçüncü fıkrasında verilerin güvenliği için düzenleme yapılarak, uygulanan tedbirin sona ermesi halinde, dinlemenin içeriğine ilişkin kayıtlar en geç on gün içinde yok edileceği hüküm altına alınmıştır. Ayrıca bu fıkra hükümlerine göre yürütülen faaliyetler çerçevesinde elde edilen kayıtlar, bu Kanunda belirtilen amaçlar dışında kullanılamaz. Elde edilen bilgi ve kayıtların saklanması ve korunmasında gizlilik

ilkesi geçerli olduğu da belirtilmek suretiyle kişisel veri niteliğinde olan iletişimin tespiti kayıtlarının korunmasına yönelik hükümlerde düzenlenmiştir (m. 6/4).

MİT'e verilen diğer bir önemli yetkide MİT'in önleyici istihbarat elde etmek ve analiz yapabilmek amacıyla yukarıda belirtilen hükümlere ve diğer kanunlardaki düzenlemelere bağlı kalmaksızın; MİT Müsteşarı veya yardımcısının onayıyla yurt dışında veya yabancılar tarafından gerçekleştirilen iletişim ile ankesörlü telefonlarla gerçekleştirilen iletişim ve MİT mensuplarının, MİT'te görev almış olanların veya görev almak üzere başvuranların iletişimi tespit edebilmesi, dinleyebilmesi, sinyal bilgileri değerlendirebilmesi ve kayda alabilmesidir (m. 6/11). Burada hemen şunu belirtmek gerekir ki 2937 sayılı Kanunun 6. Maddesine 17/4/2014 tarihli ve 6532 sayılı kanunun 3. maddesiyle eklenen bu fıkra geçen "önleyici istihbarat" kavramı doğru bir kavram değildir. Zira MİT'in önleyici kolluk adli kolluk gibi görevleri bulunmamaktadır. MİT'in görevleri yukarıda belirtildiği üzere ülke güvenliğinin sağlanmasına yönelik istihbarat toplamaktır. Bu nedenle istihbaratın önleyicisi diye bir kavramla ne demek istendiği anlaşılamamıştır. Madde gerekçesine bakıldığında¹²⁶; "*Maddeyle, Milli İstihbarat Teşkilatının, görevlerini daha etkin ve verimli olarak yerine getirilmesi amacıyla mevzuatta yer alan yetkilerinin yeniden düzenlenmesi, güncellenmesi ve ihtiyaçları karşılayacak hale getirilmesi öngörülmektedir. Bu bağlamda Milli İstihbarat Teşkilatının yabancı unsurların ülkenin ve vatandaşların iletişim güvenliğini tehdit eden faaliyetlerinin engellenmesine yönelik çalışmalar yapabilmesi ve görevlerini yerine getirirken gizli çalışma usul, prensip ve tekniklerini kullanabilmesi sağlanmaktadır. Ayrıca madde ile, MİT mensuplarının görev suçlarından dolayı soruşturulması Başbakanın iznine tabi olduğundan 6 ncı maddedeki bazı hükümler yürürlükten kaldırılmaktadır.*" Şeklinde genel ve yetersiz ifadeler kullanılmıştır. Bu nedenle bu kavramın ve bu düzenlemenin bu kanunun diğer hükümleriyle çeliştiğini ve düzeltilmesi gerektiğini düşünmekteyiz.

Ayrıca bu maddenin Anayasaya uygunluk açısından sorunlu bir madde olduğunu düşünmekteyiz. Zira Anayasanın 22. Maddesine göre, kişiler arasındaki haberleşmenin hakim kararıyla yapılabileceği, gecikmesinde sakınca bulunan bir hal var ise bu durumda yetkili merciin yazılı emriyle iletişimin denetlenebileceği ancak

¹²⁶ http://www.tbmm.gov.tr/develop/owa/tasari_teklif_sd.onerge_bilgileri?kanunlar_sira_no=149900
Erişim T: 01.06.2014

bu kararında en kısa zamanda hakim onayına sunulmak zorunda olduğu belirlenmiştir. Anayasanın amir hükmüne göre, iletişimin denetlenmesine hâkim karar vermektedir. Ancak bu fıkra da diğer fıkralardan farklı olarak MİT müşteşarı veya yardımcısının kararıyla telefon dinlemesi yapılabilecektir. İletişimin tespiti sonucu elde edilen ses kayıtları, telefon bilgileri, kişisel veri niteliğinde olduğundan bu madde konumuz açısından önem arz etmektedir. Bu nedenle bu fıkra da verilen yetkinin de hâkim kararına istinaden yapılması gerektiğinde değiştirilmesi gerektiğini düşünüyoruz¹²⁷.

3.7. 5809 sayılı Elektronik Haberleşme Kanunu

5.11.2008 tarihinde kabul edilip, 10.11.2008 tarihinde yürürlüğe giren ve elektronik haberleşme sektöründe düzenleme ve denetleme yoluyla etkin rekabetin tesisi, tüketici haklarının gözetilmesi, ülke genelinde hizmetlerin yaygınlaştırılması, kaynakların etkin ve verimli kullanılması, haberleşme alt yapı, şebeke ve hizmet alanında teknolojik gelişimin ve yeni yatırımların teşvik edilmesi ve bunlara ilişkin usul ve esasların belirlenmesi amaçlanan 5809 sayılı Elektronik Haberleşme Kanununda, kişisel verilerin korunmasıyla ilgili hükümler bulunmaktadır.

Kanunun 12. maddesinde kişisel verilerin gizliliğinin sağlanması işletmecilerin hak ve yükümlülükleri arasında sayılmıştır.

Kanunun 51. maddesi kişisel verilerin korunması alanında büyük öneme sahiptir. Zira kamuoyunda ve medyada bu hüküm, fişlemelere zemin hazırladığından eleştirilmişti¹²⁸.

Nitekim “Kurum, elektronik haberleşme sektörüyle ilgili kişisel verilerin işlenmesi ve gizliliğinin korunmasına yönelik usul ve esasları belirlemeye yetkilidir”. Şeklindeki 51. madde, Anayasa Mahkemesi’nin 9/4/2014 tarihli ve 2013/22 Esas, 2014/74 Karar sayılı kararı ile iptal edilmiş, kararın, Resmi Gazete’de yayımlandığı

¹²⁷ Benzer eleştiriler için bkz. Şen, Ersan, “MİT’e Verilmesi Düşünülen Yeni Yetki”, <http://www.adalet.org/forum2/goster.php?konu=Mit+e+verilmesi+dusunulen+yeni+yetki&fid=459143&alan=Mesleki+Konular> Erişim Tarihi:17.06.2014

¹²⁸ Keskin, Adnan, “Fişlemeye Altı Ay Devam” <http://www.taraf.com.tr/haber-fislemeye-alti-ay-devam-152505/> Erişim Tarihi: 1.5.2014

26/7/2014 tarihinden başlayarak altı ay sonra yürürlüğe girmesi hüküm altına alınmıştır¹²⁹.

Anayasa Mahkemesi verdiği bu kararla, Bilgi Teknolojileri Kurumunun (BTK) elektronik haberleşme sektörüyle ilgili kişisel verilerin işlenmesi ve gizliliğinin korunmasına ilişkin usul ve esasları belirleme yetkisi veren bu hükmü iptal etmiştir.

AYM, bu sektörde faaliyet gösteren kişi ve kurumlar ile bu hizmetlerden yararlanan abonelerin ve vatandaşların kişisel bilgileriyle ilgili bu yetkilerin BTK gibi kurumların çıkaracağı yönetmeliklerle değil, ancak kanunla yapılabileceğine dikkat çekmiştir.

AYM ayrıca bu kararında, kişisel verinin ne olduğu, kişisel verilerin korunması hakkının kaynağını hangi temel haktan aldığı ve kişisel verilerin korunması konusunda 2010 yılında Anayasanın 20. Maddesine eklenen fıkranın kapsamı konusunda tespitler de bulunması nedeniyle, karar, önem arz etmektedir.

AYM'nin gerekçeli kararının ilgili kısmı¹³⁰:

“Kişisel veri kavramı, belirli veya kimliği belirlenebilir olmak şartıyla, bir kişiye ilişkin bütün bilgileri ifade etmektedir. Bu bağlamda adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil; telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri genetik bilgiler, IP adresi, e-posta adresi, hobiler, tercihler, etkileşimde bulunan kişiler, grup üyelikleri, aile bilgileri gibi kişiyi doğrudan ve dolaylı olarak belirlenebilir kılan tüm veriler kişisel veri kapsamındadır.

Kişisel verilerin korunması hakkı, kişinin insan onurunun korunmasının ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak, bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır. Bilişim teknolojilerindeki gelişmeler sonucunda, geleneksel yöntemlerle mümkün olmayan çok sayıda verinin toplanabilmesi; daha önce birbirinden ilişiksiz şekilde tutulan pek çok verinin merkezi olarak bir araya getirilebilmesi; verilerin, veri eşleştirme ve veri

¹²⁹ İptal başvurusunun ayrıntıları için bkz. **Akgül, Aydın**, Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları ışığında Kişisel Verilerin Korunması, Beta, İstanbul, 2014, s. 243

¹³⁰ <http://www.resmigazete.gov.tr/main.aspx?home=http://www.resmigazete.gov.tr/eskiler/2014/07/20140726.htm&main> Erişim T: 01.08.2014

madenciliği gibi ileri teknolojik imkânlarla analize tabi tutulmak suretiyle, veriden yeni veriler üretme kapasitesinin artması; verilere erişim ve veri transferinin kolaylaşması; kişisel verilerin ticari işletmeler için kıymetli bir varlık kazanması neticesinde, özel sektör unsurlarınca yaratılan risklerin daha yaygın ve önemli boyutlara ulaşması ve terör ve suç örgütlerinin kişisel verileri ele geçirme yönündeki faaliyetlerinin artması gibi etkenler, günümüzde kişisel verilerin en üst seviyede korunmasını zorunlu kılmaktadır. Bu bağlamda Anayasanın 20. maddesinin üçüncü fıkrasının son cümlesinde, “Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir” hükmüne yer verilerek kişisel verilerin korunması hakkı anayasal güvenceye bağlanmış ve bu şekilde kamu makamlarının keyfi müdahalelerine karşı koruma altına alınmıştır. Yasama yetkisinin devredilemezliği ilkesi gereğince, anayasanın açıkça kanunla düzenlenmesini öngördüğü konularda yürütme organına doğrudan ve ilk elden düzenleyici işlem yapma yetkisi verilemez. Elektronik haberleşme sektörüyle ilgili kişisel verilerin işlenmesi ve gizliliğin korunmasına yönelik usul ve esasları belirleme yetkisini Bilgi Teknolojileri ve İletişim Kurumuna veren itiraz konusu kural, Anayasanın 20. Maddesinde öngörülen kişisel verilerin korunmasına ilişkin usul ve esasların ancak kanunla düzenlenebileceğine ilişkin güvenceye aykırıdır. Açıklanan nedenlerle, itiraz konusu kural Anayasa’nın 20. Maddesine aykırıdır. İptali gerekir.” Şeklinde.

AYM’nin bu kararına göre hangi kurum veya kuruluş ya da hangi alanda olursa olsun kişisel verilerin işlenmesine yönelik düzenleme mutlaka kanunla yapılmalıdır. Bu konuda idarenin düzenleme yapma yetkisi bulunmamaktadır.

Ayrıca AYM’nin bu iptal kararıyla, 24.07.2012 tarihli ve 28363 sayılı Resmi Gazetede yayınlanarak yürürlüğe giren “Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik” in de kanuni dayanağı ortadan kalkmaktadır.

Diğer taraftan 5809 sayılı Kanunda kişisel verilerin korunmasına dolaylı yönden hizmet edecek hükümlerde bulunmaktadır. Kanunun 55. maddesine göre, Kurum tarafından izin verilmedikçe, abone kimlik ve iletişim bilgilerini taşıyan özel bilgiler veya cihazın teşhisine yarayan elektronik kimlik bilgileri yeniden oluşturulamaz, değiştirilemez, kopyalanarak çoğaltılamaz veya herhangi bir amaçla dağıtılamaz. Kanunun 56. maddesine göre ise, abone kimlik ve iletişim bilgilerini

taşıyan özel bilgiler ile cihazların elektronik kimlik bilgilerini taşıyan her türlü yazılım, kart, araç veya gereç yetkisiz ve izinsiz olarak kopyalanamaz, muhafaza edilemez, dağıtılamaz, kendisine veya başkasına yarar sağlamak maksadıyla kullanılamaz.

3.8. 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun

İçerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcıların yükümlülük ve sorumlulukları ile internet ortamında işlenen belirli suçlarla içerik, yer ve erişim sağlayıcıları üzerinden mücadeleye ilişkin esas ve usûlleri düzenlemek amacıyla kabul edilen ve 23/05/2007 tarihinde yürürlüğe giren 5651 sayılı Kanunda da kişisel veriler doğrudan telaffuz edilmese de kişisel verilerin korunmasına ilişkin çeşitli hükümler bulunmaktadır.

5651 sayılı Kanunun “İçeriğin Yayından Çıkarılması ve Erişimin Engellenmesi” başlıklı 9. Maddesi ve “Özel hayatın Gizliliği Nedeniyle İçeriğe Erişimin Engellenmesi” başlıklı 9/A maddeleri kişisel verilerin korunmasına dolaylı yönden hizmet eden önemli maddelerdir. Söz konusu maddeler, 6.2.2014 tarihli ve 6518 sayılı Kanunla ve 10.9.2014 tarihli ve 6552 sayılı Kanunlarla değiştirilerek bugünkü halini almıştır.

“İçeriğin Yayından Çıkarılması ve Erişimin Engellenmesi” başlıklı 9. Maddeyle, İnternet ortamında yapılan yayın içeriği nedeniyle kişilik haklarının ihlal edildiğini iddia eden gerçek ve tüzel kişiler ile kurum ve kuruluşlar, içerik sağlayıcısına, buna ulaşamaması hâlinde yer sağlayıcısına başvurarak uyarı yöntemi ile içeriğin yayından çıkarılmasını isteyebileceği gibi doğrudan sulh ceza hâkimine başvurarak içeriğe erişimin engellenmesini de isteyebilmektedirler¹³¹.

Kişisel verilerin korunması hakkı çalışmamızın ilk bölümünde izah edildiği üzere kişilik hakkının görünüm türlerinden biri olduğundan, bu madde kapsamında değerlendirilebilir. Örneğin bir internet sitesinde bir kişiyle ilgili kişisel verilerin kişinin rızası dışında yayınlanması durumunda, kişi 5651 sayılı Kanunun 9. Maddesi

¹³¹ Erişimin engellenmesi ile internet ortamında bulunan hukuka aykırı içerik, söz konusu internet sayfasından çıkarılmamakta, sadece içeriğe belirli bir ülke sınırları içinden ulaşılmasına engel olunmakta, daha doğru ifadesi ile zorlaştırılmaktadır. Erişimin engellenmesi konusunda ayrıntılı bilgi için bkz. **Memiş, Tekin**, “Erişimin Engellenmesi, Hukuki Sorunlar ve Çözüm Önerileri”, EÜHFD, C. XIII, S. 3-4, 2009, s. 161 vd.

kapsamında ilgili internet sitesine, siteye ulaşamaması halinde yer sağlayıcısına (TTnet ve Superonline gibi) başvurarak kişisel verilerinin internet sitesi içeriğinden çıkarılmasını talep edebileceklerdir. Aynı talebi doğrudan Sulh Ceza Mahkemesinden de isteyebileceklerdir. İnternet sitesinde kişisel verilerin rıza dışında yayınlanması suç da teşkil edebileceğinden, ilerde açıklanacağı üzere, kişi ayrıca TCK'nın 136. Maddesinin ihâl edildiği iddiasıyla suç duyurusunda da bulunabilecektir.

“Özel hayatın Gizliliği Nedeniyle İçeriğe Erişimin Engellenmesi” başlıklı 9/A maddesi ise, 9. Maddeye göre daha spesifik bir alanın düzenlemektedir. Maddeye göre, internet ortamında yapılan yayın içeriği nedeniyle özel hayatının gizliliğinin ihlal edildiğini iddia eden kişiler, Telekomünikasyon İletişim Başkanlığına (TİB) doğrudan başvurarak içeriğe erişimin engellenmesi tedbirinin uygulanmasını isteyebileceklerdir. Örnek vermek gerekirse, kişinin gizlice evinin içerisinin görüntülerinin bir internet sitesinde yayınlanması veya kişinin, haber değeri de olmadığı halde, kız arkadaşıyla bir kafede yemek yerken çekilmiş fotoğraflarının bir internet sitesinde yayımlanması halinde kişi, özel hayatının gizliliğinin ihâl edildiği iddiasıyla TİB'e başvurarak içeriğe erişimin engellenmesini isteyebileceklerdir.

TİB, kendisine gelen bu talebi uygulanmak üzere derhâl Erişim Sağlayıcıları Birliğine bildirmekle, erişim sağlayıcıları da bu tedbir talebini derhâl ve en geç dört saat içinde yerine getirmekle yükümlüdürler (m. 9/A/3).

Erişimin engellenmesi ise, özel hayatın gizliliğini ihlal eden yayın, kısım, bölüm, resim, video ile ilgili olarak (URL şeklinde) içeriğe erişimin engellenmesi yoluyla uygulanmaktadır (m. 9/A/4).

Özel hayatın gizliliği hakkı da daha önce açıklandığı üzere kişilik hakkının görünüm türlerinden bir tanesi olup, kişisel verilerin korunması hakkı ile yakından ilişkilidir. Kişinin görüntüsü ve sesi, özel hayatın gizliliği kapsamında; duruma göre hayatın genel alanı, gizli alanı ve sır alanı kapsamında çeşitli düzeyde korunmaktadırlar. Özel hayat kapsamında olan kişinin görüntüsü ve sesi de, AİHM ve Yargıtay kararları ile doktrinde, aynı zamanda kişisel veri olarak kabul edilmektedir. Bu nedenle kişinin görüntüsünün veya sesinin meşru bir sebebi olmadan internet ortamında yayımlanması eylemleri karşısında yukarıda belirtilen tedbirler yoluyla koruma sağlanabilecektir.

3.9. 5237 sayılı Türk Ceza Kanunu

3.9.1. Genel Olarak

5237 sayılı Türk Ceza Kanunu kişisel verilerin korunması alanındaki suçları düzenleyen ilk ceza kanunu olmuştur. Zira 765 sayılı ve daha önceki Ceza Kanunlarında özel olarak kişisel verilere karşı işlenen suçlar yer almamıştı¹³².

5237 sayılı TCK'nun "Kişilere Karşı Suçlar" kısmının "Özel Hayata ve Hayatın Gizli Alanında Karşı Suçlar" adlı dokuzuncu bölümünde yer alan 135, 136 ve 138. maddelerde kişisel verilere karşı işlenen suçlar düzenlenmiştir. Maddelerin kanundaki yeri dikkate alındığında, kişisel verilerin "özel hayat" kavramı içerisinde değerlendirildiği görülmektedir. Kanunun 135. maddesinde kişisel verilerin hukuka aykırı olarak kaydedilmesi; 136. maddesinde kişisel verilerin hukuka aykırı olarak başkasına verilmesi, yayılması veya ele geçirilmesi; 138. maddesinde ise, sistemdeki verilerin yasal süresinde yok edilmemesi suç olarak düzenlenmiştir.

Ayrıca, kamu görevlisinin, görevinin verdiği yetkiyi kötüye kullanması veya failin belli bir meslek veya sanatın sağladığı kolaylıktan yararlanması suretiyle 135 ve 136. maddelerdeki suçları işlemesi halinde, suçun cezası yarı oranında artırılacaktır(m. 137).

Çalışmamızın konusunu oluşturan bu suçların ayrıntılı incelemesi son bölümde yapılacağından burada bu kadar bilgi verilmesi yeterli görülmüştür.

Öte yandan, Türk Ceza Kanununda kişisel verilerin korunması açısından çalışmamızın konusunu oluşturan suçlardan ayrı olarak, dolaylı olarak koruma sağlayan çeşitli suçlar da düzenlenmiştir. Genellikle bu suç tipleri, maddi konusu ve koruduğu hukuki değer itibarıyla kişisel verilere karşı işlenen yukarıda belirtilen suçlarla benzerlik taşımaktadırlar.

Türk Ceza Kanunun 132. Maddesinde düzenlenen "*haberleşmenin gizliliğini ihlal*", 133. maddesinde düzenlenen "*kişiler arası konuşmaların dinlenmesi ve kayda*

¹³² Bu kapsamda yer alan, "haberleşmenin gizliliğini ihlal"(m. 132), "kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması"(m.133) ve "özel hayatın gizliliğini ihlal"(m. 134) suçları ceza hukuku sisteminde 765 sayılı TCK'da da hüküm altına alınmıştı. Bkz. 756 sayılı TCK m. 525-a

alınması" ve 134. maddesinde düzenlenen "*özel hayatın gizliliğini ihlal*" bu suçlara verilebilecek ilk örneklerdir.

Bunların yanında sırrın açıklanması ile ilgili suçlar da bulunmaktadır. Mevzuatımızda meslek sırrı içerisinde değerlendirilebilecek çeşitli konulara ilişkin düzenlemeler bulunmaktadır. Bu kapsamda banka ve sağlık personelinin, muhasebecilerin, vergi memurlarının ya da benzeri görev gören diğer kişilerin meslekleri dolayısıyla edindikleri bilgileri açıklamama yükümlülüğünü doğuran çeşitli düzenlemeler hüküm altına alınmıştır. Bu yükümlülüklerin Türk Ceza Kanunundaki karşılıkları ise 239. ve 258. maddelerdir.

Son olarak TCK'nun "*Bilişim Suçları*" başlıklı üçüncü kısmın onuncu bölümünde yer alan suçların da kimi durumlarda dolaylı olarak kişisel verilerin korunmasına yardımcı olacağı söylenebilir. Özellikle "*bilişim sistemine girme*"(m. 243) ve "*sistemi engelleme, bozma, verileri yok etme veya değiştirme*" (m. 244), suçları, verilerin güvenliğinin sağlanması konusunda önemli düzenlemelerdir¹³³.

Bu suçlara, benzer ve farklı yönlerini görmek açısından, kısaca değinmekte fayda bulunmaktadır.

3.9.2. Kişisel Verilere Dolaylı Yönden Koruma Sağlayan Suç Tipleri

3.9.2.1. Haberleşmenin Gizliliğini İhlal Suçu

Türk Ceza Kanunun 132. Maddesinde düzenlenen haberleşmenin gizliliğini ihlal suçunun madde metni¹³⁴:

“(1) Kişiler arasındaki haberleşmenin gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Bu gizlilik ihlali haberleşme içeriklerinin kaydı suretiyle gerçekleşirse, verilecek ceza bir kat artırılır.

¹³³ Bu konuda ayrıntılı bilgi için bkz. **Ketizmen**, Bilişim Suçları, s. 57-188; **Kurt, Levent**, Açıklamalı-İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması, Seçkin Yayınevi, Ankara, 2005, s. 139-278; **Karagülmez, Ali**, Bilişim Suçları ve Soruşturma Kovuşturma Evreleri, Seçkin Yayınevi, Ankara 2005, s. 185 vd.

¹³⁴ Maddede düzenlenen suç için öngörülen cezalar, 2/7/2012 tarihli ve 6352 sayılı Yargı Hizmetlerinin Etkinleştirilmesi Amacıyla Bazı Kanunlarda Değişiklik Yapılması ve Basın Yayın Yoluyla İşlenen Suçlara İlişkin Dava ve Cezaların Ertelenmesi Hakkında Kanunla, artırılmak suretiyle değiştirilmiştir.

(2) Kişiler arasındaki haberleşme içeriklerini hukuka aykırı olarak ifşa eden kimse, iki yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(3) Kendisiyle yapılan haberleşmelerin içeriğini diğer tarafın rızası olmaksızın hukuka aykırı olarak alenen ifşa eden kişi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Ifşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur¹³⁵. ”

Şeklindedir.

Bu hüküm kaynağını, 1982 Anayasasında düzenlenen özel yaşamın ve haberleşmenin gizliliği hakkına ilişkin hükümlerinden almıştır. Bu haklar ise daha önce de belirttiğimiz üzere kişisel verilerin korunması hakkı ile yakından ilişkilidir. Bu nedenle bu suçla korunan hukuki değer, özel hayatın gizliği ve haberleşme hürriyetidir. Bir başka deyişle suçla, kişiler arasındaki haberleşmenin gizliliği korunmaktadır.

Suçun maddi konusu haberleşme ve haberleşme içerikleridir (Sevük, 2007-2008: s. 177). Haberleşme, zorunlu olarak iki kişi arasında, kişilerin başkalarıyla paylaşmaması sebebiyle özel olan, doğrudan doğruya değil, bir araç vasıtasıyla yapmış oldukları iletişim olarak tanımlanmaktadır (Sevük, 2007-2008: s. 168-169). Gizliliğin ihali ise, haberleşen kişiler arasındaki konunun haberleşmeyi yapan kişiler hilafına üçüncü kişilerce öğrenilmesidir (Zafer, 2010: s. 98). Maddede haberleşmeden bahsedildiğinden haberleşmenin hangi araçla yapıldığının önemi yoktur. Bu kapsamda, haberleşme, mektupla, telefonla, telgraf, faks veya elektronik posta yoluyla yapılabilir. Ancak burada dikkat edilmesi gereken husus haberleşmenin belirli kişiler arasında yapılması gerektiğidir. Bu nedenle, kişilerin özel hayat alanına girmeyen reklam broşürleri, kullanma talimatları gibi anonim ve genel nitelikteki gönderiler, bu suçun konusunu oluşturmazlar (Parlar ve Banko, 2014: s. 374).

Maddenin birinci fıkrasında suçun temel şekli düzenlenmiştir. Haberleşmenin gizliliğinin sadece dinlemek veya okumak suretiyle ihlâl edilmesi, bu suçun temel şeklini oluşturmaktadır. Ancak, bu gizlilik ihlâlinin, haberleşme içeriklerinin yanı sıra konu konuşulanların veya yazılanların kayda alınması suretiyle yapılması, bu suçun

¹³⁵ Fıkranın son cümlesi 2/7/2012 tarihli ve 6352 sayılı Kanunla eklenmiş, maddenin dördüncü fıkrasında aynı Kanunla yürürlükten kaldırılmıştır.

ağırlaştırıcı neden olarak düzenlenmiştir¹³⁶. Telefon konuşmalarının teknik bir cihaz vasıtasıyla kayda alınması buna örnek verilebilir.

Maddenin ikinci ve üçüncü fıkraları suçun nitelikli hallerini oluşturmaktadır. İkinci fıkrafta, kişiler arasındaki haberleşme içeriklerini hukuka aykırı olarak ifşa etme eylemi, üçüncü fıkrafta ise kendisiyle yapılan haberleşmelerin içeriğini diğer tarafın rızası olmaksızın hukuka aykırı olarak alenen ifşa etme eylemi cezalandırılmaktadır. İkinci fıkrafta suçun faili sozkonusu haberleşmenin tarafı olmayan kişidir. Üçüncü fıkrafta ise fail, haberleşmenin tarafı olan kişidir.

Ifşa etme eylemi, haberleşme içeriklerini başkalarının bilgisine sunma, başkaları tarafından ulaşılabilir hale getirme olarak açıklanabilir. Burada 136. maddede düzenlenen kişisel verileri hukuka aykırı olarak verme yayma ve ele geçirme suçuna benzer bir eylem söz konusudur.

Söz konusu suç, kişisel veriler açısından da dolaylı yönden koruma sağlamaktadır. Nitekim daha öncede açıklandığı üzere kişilerin haberleşme özgürlüğünün ihlali suretiyle elde edilen kayıtlar, kişisel veri niteliğindedir. Bu suçu işleyen kişiler, aynı zamanda kişilerin kişisel verilerine vakıf olmakta, bu verileri ele geçirmekte ve verileri ifşa etmedirler. Bu nedenle bu suçu oluşturacak eylemlerin yapılmasıyla kişisel verilere karşı suçlar da işlenmiş olmaktadır. Ancak bu suç sadece haberleşme ve haberleşmenin gizliliğine mahsus olarak düzenlenmiş olduğundan bu suç uygulama alanı bulacaktır.

3.9.2.2. Kişiler Arasındaki Konuşmaların Dinlenmesi ve Kayda Alınması Suçu

Kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması suçu 5237 sayılı TCK'nun 133. maddesinde düzenlenmiştir. Madde:

“(1) Kişiler arasındaki aleni olmayan konuşmaları, taraflardan herhangi birinin rızası olmaksızın bir aletle dinleyen veya bunları bir ses alma cihazı ile kaydeden kişi, iki yıldan beş yıla kadar hapis cezası ile cezalandırılır.

¹³⁶ Bkz. 132. Maddenin gerekçesi

(2) Katıldığı aleni olmayan bir söyleşiyi, diğer konuşanların rızası olmadan ses alma cihazı ile kayda alan kişi, altı aydan iki yıla kadar hapis veya adli para cezası ile cezalandırılır.

(3) Kişiler arasındaki aleni olmayan konuşmaların kaydedilmesi suretiyle elde edilen verileri hukuka aykırı olarak ifşa eden kişi, iki yıldan beş yıla kadar hapis ve dörtbin güne kadar adli para cezası ile cezalandırılır. Ifşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur.” Şeklinde.

Madde metni, 2.7.2012 tarihli ve 6352 sayılı Kanunla değişikliğe uğrayarak bugünkü halini almıştır.

Maddenin birinci fıkrasında kişiler arasındaki aleni olmayan konuşmaların dinlenilmesi veya kayda alınması eylemleri, ikinci fıkrasında, katıldığı aleni olmayan bir söyleşiyi diğer konuşanların rızası olmadan ses alma cihazıyla kayda alma eylemi düzenlenmiştir. Üçüncü fıkra ise, kişiler arasındaki aleni olmayan konuşmaların kaydedilmesi suretiyle elde edilen verileri hukuka aykırı olarak ifşa etme eylemi düzenlenmiş, ifşa edilen verilerin basın yayın yoluyla yayımlanması eylemi de aynı kategoride değerlendirilerek üçüncü fıkra uyarınca cezalandırılması öngörülmüştür.

Suçla korunan hukuki yarar kişilerin özel hayatının gizliliğidir. Zira kişiler arasındaki aleni olmayan konuşmalar, Avrupa İnsan Hakları Sözleşmesinin 8. maddesinde ve 1982 Anayasasının 20 ve 22. maddelerinde belirtildiği üzere özel hayat alanına dâhildir. Bir başka deyişle suçla, aleni olmayan sözler koruma altına alınmaktadır (Zafer, 2010: s. 142-143).

Suçun maddi konusunu ise kişiler arasındaki aleni olmayan konuşmalar ya da aleni olmayan söyleşiler oluşturmaktadır. Madde metninde aleni olmayan konuşma ve söyleşiden söz edildiğinden buradaki konuşmalar, yüz yüze yapılan konuşmalardır (Özbek, 2008: s. 933). Bir araç vasıtasıyla yapılan konuşmalar haberleşme niteliğinde olacağından, bu suçun konusunu oluşturmazlar.

Aynı şekilde görüntü gibi konuşma dışında kalan kayıtlar da, bu suçun konusunu değil TCK’nun 134. maddesinde düzenlenen özel hayatın gizliliğini ihlal suçunun konusunu oluşturacaktır.

Söyleşi karşılıklı konuşma, hasbıhâl, sohbet, belli bir konuda alanla ilgili kişilerin katıldığı bilgilendirme toplantısı anlamlarına gelmektedir¹³⁷. Algılanabilir, sesli düşünce açıklaması olarak ifade edilen konuşma da benzer bir nitelik taşıdığından doktrinde iki kavram arasındaki farkın katılanların sayısına göre belirlenebileceği, madde gerekçesinde yer alan "söyleşiye katılan kişilerden biri" ibaresinin söyleşiye ikiden fazla kişinin katılacağı izlenimi yarattığı savunulmuştur (Özbek, 2008: s. 934). Gerçekten iki kişi arasındaki konuşma da söyleşi niteliği taşıyabileceğinden, iki fıkra arasındaki farkın katılımcıların sayısına göre belirlenmesi zorunludur. Bu durumda Ceza Kanunundaki düzenleme itibarıyla söyleşi, en az üç kişinin katıldığı bir toplantıyı ifade etmektedir (Zafer, 2010: s. 155).

Aleni olmayan konuşma ya da söyleşi, herkesçe bilinmesi gerekmeyen, bilinmesi istenmeyen, gizli kalması istenen, üçüncü kişilerle paylaşımına sunulmamış konuşma ya da söyleşidir. Konuşma ya da söyleşiyi yapan bunu kimlerle paylaştığını bilir ve bu kişileri belirleme yeteneğine sahiptir. Konuşma ya da söyleşinin gizliliğine yönelik bir tertibat almak yeterlidir. Önemli olan konuşma ya da söyleşiyi gerçekleştiren kişinin bunu üçüncü kişilerle paylaşmama iradesini ortaya koymuş olmasıdır. Örneğin bu nedenle konuşma ya da söyleşiye belli kişilerin davet edilmesi; girişte kontrol yapılması, şifre kullanılması ya da telsiz gibi araçlara başvurulması yeterlidir. Üçüncü kişilerin şifreyi kırması, telsiz frekansına girebilme imkânı önemli değildir. Bu yönüyle konuşma ya da söyleşi bakımından mutlak bir koruma alanı yaratmak zorunlu değildir¹³⁸.

Ayrıca kişiler arasında yapılan konuşmanın aleni olmayan konuşma olarak kabulü için, madde gerekçesinde de belirtildiği üzere, konuşmanın yapıldığı yerin de önemi yoktur. Bu bakımdan, örneğin bir parkta iki kişi arasında geçen konuşmanın başkaları tarafından ancak özel gayret gösterilerek duyulabilecek olması hâlinde, aleni olmayan konuşma söz konusudur. Keza, örneğin bir evde sınırlı sayıda kişiler arasında yapılan konuşma, aleni olmayan bir konuşmadır¹³⁹.

¹³⁷ <http://www.tdk.org.tr/TR/SozBul.aspx7F6E10F8892433CFFAAAF6AA849816B2EF4376734BED947CDE&Kelime=yarar> Erişim Tarihi 15.12.2009.

¹³⁸ Özbek, TCK İzmir Şerhi, 2008, s. 933; Aynı şekilde bkz. Şen, Ersan, "5237 sayılı Türk Ceza Kanunu'nda Özel Hayata Karşı Suçlar", İBD, C. 79, S. 3, 2005, s. 714

¹³⁹ Bkz. Madde gerekçesi; Erol, Haydar, Türk Ceza Kanunu, C.1, Ankara, 2008, s.1533; Meran, Necati, Açıklamalı İçtihatlı Türk Ceza Kanunu, 2. Bası, Seçkin Yayınevi, Ankara, 2007, s.683

Birinci fıkrada düzenlenen suçun faili, aleni olmayan konuşmanın tarafı olmayan bir kişidir. İkinci fıkrada düzenlenen aleni olmayan söyleşiler açısından ise ancak söyleşiye katılan kişi bu suçu işleyebileceğinden fail, söyleşiye katılan kişilerden biridir.

Birinci fıkrada düzenlenen suç, kişiler arasındaki aleni olmayan konuşmaların bir aletle dinlenilmesi veya bunların bir ses alma cihazıyla kaydedilmesi suretiyle oluşmaktadır. Dinlemek veya kayda almak eylemlerinden birinin yapılması suçun oluşması için yeterlidir. Ancak dinlemenin bir aletle yapılması zorunlu olduğundan çıplak kulakla dinleme, bu madde kapsamına girmeyecek, koşulları varsa özel hayatın gizliliğini ihlal (134.md.) suçunu oluşturacaktır (Hafızoğulları ve Özen, 2009: s. 14).

Kişiler arasındaki aleni olmayan konuşmaların kaydedilmesi suretiyle elde edilen verileri hukuka aykırı olarak ifşa etme, haberleşmenin gizliği suçundaki düzenleye ve kişisel verileri hukuka aykırı olarak verme, yayma ve ele geçirme suçuna benzer bir eylemdir. Ifşa etmek, bu verileri başkalarının bilgisine sunma, başkaları tarafından ulaşılabilir hale getirmektir. Bu kapsamda elde edilen verileri, bir internet sitesinde yayınlamak ifşa etme suçunu oluşturacaktır.

Belirli veya belirlenebilir bir kişiyle ilgili bütün bilgiler kişisel veri olarak kabul edildiğinden, 133. Madde kapsamında kayıt edilen verilerde kişisel veri niteliğinde değerlendirilebilir. Ancak buna özgü bir suç düzenlenmiş olduğundan kişiler arasındaki aleni olmayan konuşmaların veya söyleşilerin kaydedilmesi ve ifşa edilmesi hallerinde 133. Madde uygulama alanı bulacaktır.

3.9.2.3. Özel Hayatın Gizliliğini İhlal Suçu

Özel hayatın gizliliğini ihlal suçu TCK'nun 134. maddesinde düzenlenmiştir. Madde metni:

“(1) Kişilerin özel hayatının gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Gizliliğin görüntü veya seslerin kayda alınması suretiyle ihlal edilmesi halinde, verilecek ceza bir kat artırılır.

(2) Kişilerin özel hayatına ilişkin görüntü veya sesleri hukuka aykırı olarak ifşa eden kimse iki yıldan beş yıla kadar hapis cezası ile cezalandırılır. Ifşa edilen bu

verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur.” Şeklinde dir.

Hüküm, 2.7.2012 tarihli ve 6352 sayılı Kanunla değişikliğe uğrayarak bugünkü halini almıştır.

Bu suçla, Avrupa İnsan Hakları Sözleşmesinin 8, 1982 Anayasanın 20. maddesinde düzenlenen özel hayatın gizliliği hakkının korunması amaçlanmıştır. Bu nedenle bu suçla korunan hukuki yarar kişilerin özel hayatlarının gizliliğinin korunmasıdır. Özel hayat ve özel hayatın gizliliği kavramları hakkında çalışmamızın birinci bölümünde ayrıntılı açıklamalarda bulunulduğundan burada sadece suçun unurlarına yönelik açıklamalar yapılacaktır¹⁴⁰.

Bu suçun maddi konusu özel hayat alanına giren tüm faaliyetler ve yaşam olayları oluşturur. Ancak konuşma ve haberleşme ile kişisel veri niteliğindeki hususlar, bu konularda özel düzenlemeler bulunması nedeniyle, bu suçun konusunu değil, ilgili suçların konusunu oluşturacaktır (Özbek vd, 2013: s. 520; Zafer, 2010: s. 188).

Maddenin birinci fıkrasıyla özel hayatın gizliliğinin ihlali suç sayılmıştır. Maddeyle özel hayatın gizliliğinin ihlalinin suç sayılmasına rağmen bu ihlalin ne şekilde gerçekleşeceği konusunda kanunda bir sınırlama bulunmamaktadır. Dolayısıyla burada serbest hareketli bir suç söz konusu olup, gizliliğe müdahale niteliğindeki her türlü davranış ihlal için yeterli olacaktır. Gizliliğin ihlali, gizli bilgilerin bunu öğrenmeye yetkili olamayan bir kişi tarafından öğrenilmesiyle gerçekleşmiş olacaktır. Bunların açıklanması ya da birden fazla kişinin gizli bilgileri öğrenmesi gerekmemektedir (Özbek vd, 2013: s. 522).

Komşunun yatak odasının pencereden seyredilmesi veya evinin içinin herhangi bir şekilde gözetlenmesi; çalıştığı işyerinde ne olduğunu merak ederek arkadaşının masasının gözüne bakılması; bir kimsenin çantasının karıştırılması; posta kutusuna bakılması; otel, pansiyon vs. çalışanının müşterinin odasında eşyasını

¹⁴⁰ Özel hayat kavramıyla ilgili ayrıntılı bilgi için bkz. **Polater, Yusuf Ziya**, Özel Hayatın Gizliliği ve Korunması, Adalet Yayınevi, Ankara, 2010; Suçla ilgili ayrıntılı bilgi için bkz. **Akyürek, Güçlü**, Özel Hayatın Gizliliğini ihlal Suçu, 2. Baskı, Seçkin Yayınevi, Ankara, 2014

karıştırması; kimin kimle beraber olduğunun araştırılması, özel hayatın gizliliğinin ihlaline örnek olarak verilebilir (Hafizoğulları ve Özen, 2009: s. 17).

Gizliliğin görüntü veya seslerin kayda alınması suretiyle ihlal edilmesi hali, aynı fıkra da ağırlaştırıcı neden olarak düzenlenmiştir. Bu kapsamda kişileri rızası dışında fotoğraflarının çekilmesi, evinin bahçesindeki havuzunda yüzerken görüntülerinin kameraya alınması bu durumlara örnek verilebilir.

Maddenin ikinci fıkrasında ise, *Kişilerin özel hayatına ilişkin görüntü veya sesleri hukuka aykırı olarak ifşa etme suçu düzenlenmiş, ifşa edilen bu verilerin basın ve yayın yoluyla yayımlanması hali de aynı kategoride değerlendirilerek aynı cezaya hükmolunacağı belirtilmiştir.* Ifşa etme eylemi, özel hayata ilişkin görüntü veya sesleri başkalarının bilgisine sunma, başkaları tarafından ulaşılabilir hale getirme olarak açıklanabilir. Ifşa etme eylemi, 132 ve 133. maddelerdeki suçlarla aynı anlamda düzenlenmiştir.

İkinci fıkradaki suçun konusu ise birinci fıkraya göre daha dardır. Özel hayat alanının sadece görüntü ve seslere ilişkin kısmı bu suçun konusunu oluşturmaktadır. Ifşa etme eylemi açısından da yöntem olarak herhangi bir sınırlama öngörülmediğinden, herhangi bir yöntemle yapılabilecektir. Bu kapsamda kişinin özel hayatına ilişkin bir video kaydının internette sosyal paylaşım sitelerinde yayınlanması bu fıkradaki suçu oluşturacaktır. Kişinin çıplak fotoğraflarının rızası dışında hukuka aykırı olarak bir gazetede yayınlanmasında ikinci fıkradaki suçu oluşturacaktır.

Dikkat edilecek olursa bu suç, kişisel verilerin korunması açısından da bir koruma getirmektedir. Zira daha önce de açıklandığı üzere kişinin sesi ve görüntüsü kişisel veri niteliğindedir. Bu verilerin hukuka aykırı olarak ele geçirilmesi, yayılması, başkalarına verilmesi, kaydedilmesi kişinin kişisel verilerin korunması hakkını da ihlal etmektedir. Ancak suç tekniği açısından kişilerin özel hayatına ilişkin görüntü veya seslerin ifşa edilmesi 134. Maddein ikinci fıkrası kapsamında değerlendirilmelidir.

Nitekim Yargıtay da bir kararında¹⁴¹, “.....bir özel hayat görüntüsü ya da sesinin, “kişisel veri” olduğunda kuşku bulunmamakta ise de, kişinin özel hayatına ilişkin görüntüsü ya da sesinin, bilgisi dışında, resim çekme veya kaydetme özelliğine sahip aletle belli bir elektronik, dijital, manyetik yere sabitlenmesi 5237 sayılı TCK'nın 134/1. maddesinin 2. cümlesinde; 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 özel hayatın gizliliğini ihlal suçu kapsamında düzenlendiğinden, kişinin özel hayatına ilişkin görüntüsü, fotoğrafı ya da sesinin, yasal anlamda, 5237 sayılı TCK'nın 135. maddesi kapsamında kişisel veri olarak değerlendirilemeyeceği,...” şeklinde belirtmek suretiyle bu hallerde 134. Maddenin uygulanması gerektiğine hükmetmiştir.

3.9.2.4. Ticari Sır, Bankacılık Sırrı veya Müşteri Sırrı Niteliğindeki Bilgi ve Belgelerin Açıklanması Suçu

TCK'nın 239. maddesinde *"ticari sır, bankacılık sırrı veya müşteri sırrı niteliğindeki bilgi ve belgelerin açıklanması"* düzenlenmiştir.

Madde metni:

(1) Sıfat veya görevi, meslek veya sanatı gereği vakıf olduğu ticari 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 beşbin güne kadar adli para cezası ile cezalandırılır. Bu bilgi veya belgelerin, hukuka aykırı yolla elde eden kişiler tarafından yetkisiz kişilere verilmesi veya ifşa edilmesi halinde de bu fıkra göre cezaya hükmolunur.

(2) Birinci fıkra hükümleri, fenni keşif ve buluşları veya sınai uygulamaya ilişkin bilgiler hakkında da uygulanır.

¹⁴¹ Bkz. Yargıtay 12. CD. Esas no: 2012/16872, Karar no: 2012/18221
www.portal.uyap.gov.tr/kararlar/yargitaykararlari

(3) Bu sırlar, Türkiye'de oturmayan bir yabancıya veya onun memurlarına açıklandığı takdirde, faile verilecek ceza üçte biri oranında artırılır. Bu halde şikayet 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.” Şeklindedir.

Bu suç, TCK'nın Ekonomi, Sanayi ve Ticarete İlişkin Suçlar başlıklı dokuzuncu bölümde düzenlenmesi itibariyle koruduğu hukuku yarar açısından, kişisel verilerin kaydedilmesi suçlarından farklıdır. Zira bu suçla, toplumun korunması ile ekonomi, sanayi ve ticaret alanındaki güven ilişkisi korunmaktadır (Özbek vd, 2011: s. 518).

Hükümde bu türdeki bilgi veya belgeleri yetkisiz kişilere veren veya ifşa eden kişinin şikâyet üzerine cezalandırılacağı belirtilmiştir. Bilgi veya belgeleri açıklayan kişinin bunları hukuka uygun ya da aykırı elde etmesi arasında da bir ayrım öngörülmemiştir. Bunların ticari sır, bankacılık veya müşteri sırrı niteliğinde olup olmadığı ise ilgili yasalarda belirlenen ölçütler göz önünde tutularak hâkim tarafından belirlenecektir¹⁴².

TCK' nun 239. maddesi kişisel verilerin korunması açısından özellikle müşteri sırrını koruması açısından önemlidir. Nitekim ticari sır ve bankacılık sırrı daha çok gerçek kişilerin değil, tüzel kişilerin korunmasına yönelik olarak düzenlenmiştir¹⁴³.

¹⁴² Ayrıntılı bilgi için bkz. **Tekşen, Mustafa Gökhan**, Ticari Sır, Bankacılık Sırrı veya Müşteri Sırrı Niteliğindeki Bilgi ve Belgelerin Açıklanması Suçu (TCK m. 239), Yetkin Yayınevi, Ankara, 2012, s. 15 vd.

¹⁴³ Ticari Sır, Banka Sırrı ve Müşteri Sırrı Hakkında Kanun Tasarısında bu deyimlerin tanımları yer almaktadır. Tasarının 2. maddesi uyarınca *"Bu kanunda geçen a) Ticari sır: Bir ticari işletme veya şirketin faaliyet atanı ite ilgili yalnızca belirli sayıdaki mensupları ve diğer görevlileri tarafından bilinen, elde edilebilen, özellikle rakipleri tarafından öğrenilmesi halinde zarar görme ihtimali bulunan ve üçüncü kişilere ve kamuya açıklanmaması gereken, işletme ve şirketin ekonomik hayattaki başarı ve verimliliği için büyük önemi bulunan; iç kuruluş yapısı ve organizasyonu, malî, iktisadî, kredi ve nakit durumu, araştırma ve geliştirme çalışmaları, faaliyet stratejisi, hammadde kaynakları, imalatının teknik özellikleri, fiyatlandırma politikaları, pazarlama taktikleri ve masrafları, pazar payları, toptancı ve perakendeci müşteri potansiyeli ve ağırları, izne tâbi veya tâbi olmayan sözleşme bağlantılarına ilişkin veya bu gibi bilgi ve belgeleri, b) Banka sırrı: Bankanın yönetim ve denetim organlarının üyeleri, mensupları ve diğer görevlileri tarafından bilinen malî, iktisadî, kredi ve nakit durumu ile ilgili bilgilerle, bankanın müşteri potansiyeli, kredi verme, mevduat toplama, yönetim esasları, diğer bankacılık hizmet ve faaliyetleri, risk pozisyonlarına ilişkin her türlü bilgi ve belgeleri, c) Müşteri sırrı: Ticari işletme ve şirketlerin, bankaların, sigorta şirketlerinin, sermaye piyasasında ve*

Kişisel verilerin korunması, insan hakları kapsamında ele alındığından bu suç, ancak gerçek kişilere ilişkin bilgiler söz konusu olduğunda gündeme gelebilir. Tüzel kişilere ilişkin bilgiler, ceza hukukunda, kişisel verilere karşı işlenen suçlar kapsamında değerlendirilmemektedir. Müşteri sırrı ise daha çok müşteriye yani bireye yönelik olması nedeniyle, kişisel verilerin korunması kapsamında değerlendirilebilir. Nitekim müşteri sırrı, ticarî işletme ve şirketlerin, kendi faaliyet alanlarıyla ilgili olarak müşteriyle ilişkilerinde, müşterinin şahsî, iktisadî, malî, nakit ve kredi durumuna ilişkin doğrudan veya dolayısıyla edindikleri tüm bilgi ve belgeleri, ifade etmektedir (Dursun, 2009: s. 202).

3.9.2.5. Göreve İlişkin Sırrın Açıklanması Suçu

TCK'nın 258. maddesinde ise kamu görevlileri açısından “*göreve ilişkin sırrın açıklanması*” suçu düzenlenmiştir. Madde metni:

“(1) Görevi nedeniyle kendisine verilen veya aynı nedenle bilgi edindiği ve gizli kalması gereken belgeleri, kararları ve emirleri ve diğer tebligatı açıklayan veya yayınlayan veya ne suretle olursa olsun başkalarının bilgi edinmesini kolaylaştıran kamu görevlisine, bir yıldan dört yıla kadar hapis cezası verilir.

(2) Kamu görevlisi sıfatı sona erdikten sonra, birinci fıkrada yazılı fiilleri işleyen kimseye de aynı ceza verilir.” Şeklindedir.

Buna göre, görevi nedeniyle kendisine verilen veya aynı nedenle bilgi edindiği ve gizli kalması gereken belgeleri, kararları ve emirleri ve diğer tebligatı açıklayan ve yayınlayan veya ne suretle olursa olsun başkalarının bilgi edinmesini kolaylaştıran kamu görevlisi bu suçun faili olacaktır.

Bu suç, TCK'nın dördüncü kısmının Kamu İdaresinin Güvenilirliğine ve İşleyişine Karşı Suçlar başlıklı birinci bölümünde düzenlenmiş olup, düzenlendiği bölüm itibarıyla kamu idaresi yani devlete yönelik bir koruma getirmektedir. Kişisel verilerin korunmasının bireye yönelik olması nedeniyle, koruduğu kişi ve değer

malî piyasalarda faaliyet gösteren aracı kurumların, kendi faaliyet alanlarıyla ilgili olarak müşteriyle ilişkilerinde, müşterinin şahsî, iktisadî, malî, nakit ve kredi durumuna ilişkin doğrudan veya dolayısıyla edindikleri tüm bilgi ve belgeleri, ifade eder”. Bkz. <http://www.kgm.adalet.gov.tr/Tasariasamalari/Tbmmkms/Tbmmkom/ticarisir.pdf> Erişim Tarihi: 02.09.2013

açısından farklılık arz etmekle birlikte maddede belirtilen nitelikteki belgeler, kişisel veriler de içerebileceğinden bu hükmünde, kişisel veriler açısından dolaylı da olsa bir koruma getirdiği söylenebilir (Özgenç, 25 Mayıs 2010: s. 287).

3.9.2.6. Sistemi Engelleme, Bozma, Verileri Yok etme veya Değiştirme Suçu

Sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu TCK'nın 244. Maddesinde düzenlenmiştir. Madde metni:

“(1) Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(2) Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır.

(3) Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır.

(4) Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adli para cezasına hükmolunur.” Şeklindedir.

Suç, TCK'nın bilişim alanında suçlar başlıklı onuncu bölümünde düzenlenmiştir. Ancak bu suç, suçun konusu, korunan hukuki değer ve maddi unsurlar açısından kişisel verilere karşı işlenen suçlardan ayrılmaktadır.

Nitekim 244. maddenin ikinci fıkrasında düzenlenen “sistemdeki verileri bozma, değiştirme ve yok etme” suçunun konusunu her türlü veri oluşturmaktadır. Bu veriler kişilere, kurumlara veya maddelere, buluş veya icatlara yönelik olabileceği gibi, şifre ve parola gibi veriler de olabilir. Bu durumda korunan hukuki değerde suçun konusuna göre değişiklik arz etmektedir. Korunan hukuki değer somut olaya göre, bilgisayar verilerini ve bilgisayar programlarını, fiziksel nesneleri, kasıtlı zarar verme girişimlerine karşı koruma altına almak olabileceği gibi, mülkiyet hakkının, fikri mülkiyet hakkının, özel hayatın gizliğinin veya ticari sırların gizliğinin korunması da olabilmektedir.

Maddi unsurlar açısından da bu suçta birden fazla seçimlik hareket bulunmaktadır. Kişisel verilere karşı işlenen suçlardan farklı olarak “bozmak, değiştirmek, erişilmez kılmak, sisteme veri yerleştirmek, var olan verileri başka bir yere göndermek” fiilleri de tipte düzenlenmiştir.

Ayrıca her iki suç arasında suçun işleniş amaçları açısından da farklılık bulunmaktadır. Kişisel verilere karşı işlenen suçlarda amaç, kişinin verilerini ele geçirmek veya yaymak suretiyle onun özel hayatının gizliliğinin ihlal etmek olmakla birlikte, bilişim sistemindeki verilerin bozulması yok edilmesi suçunda amaç, çoğu zaman bilişim sistemine zarar verme, kişiyi maddi zarara uğratma, önemli bazı ticari verilere çalma ve menfaat elde etmektir (Artuk vd, Özel Hükümler, 2013; s. 854; Parlar ve Hatipoğlu, 2007: s. 1700; Karagülmez, 2005: s. 188-189).

Yine de bu suçunda, bilişim sistemindeki verilerin kişisel veri olması durumunda dolaylı açıdan koruma sağlayacağı söylenebilir.

3.10. 5271 sayılı Ceza Muhakemesi Kanunu

3.10.1. Genel Olarak

Suç işlendikten sonra şüphelinin tespiti ve yakalanması ve delillerin toplanması gibi gerekçelerle parmak izi, DNA profili gibi kişisel verilerin toplandığı ve incelendiği, şüpheli veya sanığın telefon görüşmelerinin dinlendiği ya da görüntülerinin kayıt altına alındığı ve soruşturma ve kovuşturma aşamalarında kullanıldığı bilinmektedir. Bir taraftan bu tedbirlerin etkin şekilde uygulanarak soruşturma ve kovuşturmanın amacına ulaşmasının sağlanmasının temini, bir taraftan da temel hak ve özgürlüklerin ihlal edilmemesi amaçlarıyla bu tedbirler sıkı kurallara bağlanmıştır.

Bu kapsamda adli olaylarla ilgili yürütülen soruşturma ve kovuşturmalarda, elde edilecek veya kullanılacak kişisel veriler konusunda 5271 sayılı Ceza Muhakemesi Kanunu (CMK) ayrıntılı ve koruyucu hükümler içermektedir.

3.10.2. Ceza Muhakemesi Kanunda Kişisel Verilerin Korunmasına İlişkin Hükümler

3.10.2.1. Vücut Muayenesi ve Vücuttan Örnek Alınması

Ceza Muhakemesi Kanununun 75. maddesinde şüpheli veya sanığın beden muayenesi ve vücudundan örnek alınması, 76. maddesinde mağdurun beden

muayenesi ve vücudundan örnek alınması hususları düzenlenmiştir. Maddede sayılan kişilerden kan veya benzeri biyolojik örneklerle saç, tükürük, tırnak gibi örnekler alınması kural olarak hâkim kararına bağlanmış ve ancak üst sınırı iki yıl ve daha fazla suçlarda delil elde edebilmek amacıyla bu yola başvurulabileceği belirtilmiştir. Bu kişilerin vücudundan alınan kan ve doku örnekleri, kişiyi dolaylı yünden tanımlama ve belirleme imkânı verdiğiinden kişisel veri niteliğinde olduğu hususunda kuşku bulunmamaktadır (Öztürk vd, 2006: s. 585). Zira Kanunun 78 ve 79. maddelerinde ilgili kişilerden alınan örnekler üzerinde genetik incelemelerin nasıl yapılacağı açıklandıktan sonra 80. maddede inceleme sonuçlarının kişisel veri niteliğinde olduğu, bu verilerin başka bir amaçla kullanılamayacağı, ilgisiz kişilere verilemeyeceği ve ne zaman yok edileceği açıkça düzenlenmiştir.

Buna göre, alınan örnekler üzerinde bu amaçlar dışında tespitler yapılması yasaklanmış olup, moleküler genetik inceleme yapmaya yalnızca hâkimin karar verebilmesi öngörülmüştür(m. 79). CMK'nın 75-78. maddelerindeki düzenlemeler uyarınca kişiden alınan örnekler ile yapılan inceleme sonuçlarının başka bir amaçla kullanılamayacağı ve dosya içeriğini öğrenme yetkisine sahip bulunan kişiler tarafından bir başkasına verilemeyecektir.

Ayrıca bu bilgilerin, "kovuşturmaya yer olmadığı kararına itiraz süresinin dolması, itirazın reddi, beraat veya ceza verilmesine yer olmadığı kararı verilip kesinleşmesi", yani kişinin suçla ilgisinin kalmaması hâllerinde Cumhuriyet savcısının huzurunda derhâl yok edilmesi, bu hususun da, dosyasında muhafaza edilmek üzere, tutanağa geçirilmesi gerekmektedir (m. 80).

3.10.2.2. Parmak İzi Alınması ve DNA Analiz Kaydı

Ceza Muhakemesi Kanunu'nun "fizik kimliğinin tespiti" başlıklı 81. maddesinde, üst sınırı iki yıl ve daha fazla hapis cezasını gerektiren bir suçtan dolayı şüpheli veya sanığın kimliğinin tespiti amacıyla, fotoğrafı, beden ölçüleri, parmak izi, avuç içi izi, bedeninde yer almış olup teşhisini kolaylaştıracak diğer özellikleri ile sesi ve görüntüsünün, kayda alınabileceği ve soruşturma ve kovuşturma dosyasına konulabileceği düzenlenmiştir. Madde de sayılan kişisel veri niteliğindeki bilgilerin alınabilmesi ancak Cumhuriyet savcısının emri ile yapılacaktır. Ayrıca maddenin ikinci fıkrasında bu verilerin ne zaman yok edileceği açıkça belirtilmiştir.

Konuyla bağlantılı olarak 2559 sayılı Polis Vazife ve Salahiyetleri Kanunu'nun 5. maddesi ile 5275 sayılı Ceza ve Güvenlik Tedbirlerinin İnfazı Hakkında Kanun'un 21/3 maddesi uyarınca da, fiziki kimliğin tespiti maksadıyla, kişisel veri niteliğinde olan parmak izi alınabilmektedir¹⁴⁴. Bu çerçevede, 1 Haziran 2005 tarih ve 25832 sayılı Resmi Gazete'de yayınlanan Ceza Muhakemesinde Beden Muayenesi, Genetik İncelemeler ve Fiziki Kimliğin Tespiti Hakkında Yönetmeliğin 15, 16 ve 17. maddelerinde bu kayıtların hangi suretle, kimler tarafından ve ne kadar süre ile saklanacağı ve nasıl imha edileceği ayrıntılı bir şekilde düzenlenmiştir.

Moleküler genetik incelemelere ilişkin yukarıda belirtilen kişinin suçla ilişkisinin kalmaması durumunda kayıtların yok edilmesine ilişkin ilke burada da kabul edilmiştir (m. 81/2). Bu düzenleme oldukça önemlidir. Zira kişilerin genetik profilleri, parmak izleri ile karşılaştırıldığında daha hassas nitelikte olsalar da, parmak izinin benzersiz bir niteliği olduğu unutulmamalıdır. Bu nedenle parmak izi kayıtlarının tutulması da özel yaşamın gizliliği hakkına müdahale oluşturacağından, temel hak ve özgürlüklerin sınırlandırılmasına yönelik ilkelere tabi tutulmuş ve CMK'da sıkı kurallara bağlanmıştır.

3.10.2.3. İletişimin Tespiti

Kişilerin özel haberleşmelerinin içerikleri önemli oranda kişisel veri içerdiğinden hem haberleşme özgürlüğü, hem de kişisel verilerin korunması hakkının kapsamında değerlendirilmektedir (Küzeci, s. 299). AİHM de özel haberleşmeye yapılan müdahaleyi Sözleşmede özel yaşamın gizliliği hakkının düzenlendiği 8. maddesi kapsamında değerlendirmektedir. Mahkeme, özel haberleşme şekilleri arasında da bir ayrım öngörmemektedir. Her ne kadar AİHS'nde iletişim şekillerine ilişkin bir ifade yer almasa da Mahkeme, birbirini izleyen kararlarında, telefon görüşmelerini¹⁴⁵, görüşülen kişilerin numaralarını, ses kaydını, e-posta ve internet

¹⁴⁴ Polis Vazife ve Salahiyet Kanunu'nun 5. maddesinde; polisin, gönüllülerin, her çeşit silah ruhsatı, sürücü belgesi, pasaport veya pasaport yerine geçen belge almak için başvuruda bulunanların, başta polis olmak üzere, genel veya özel kolluk görevlisi ya da özel güvenlik görevlisi olarak istihdam edilen kişilerin, Türk vatandaşlığına başvuruda bulunanların, sığınma talebinde bulunan veya gerekli görülmesi halinde, ülkeye giriş yapan sair yabancıların, gözaltına alınanların parmak izini alabileceği belirtilmiştir. Parmak izinin kişisel veri niteliğinde olduğuna yönelik ayrıntılı bilgi için bkz. **Aslan**, s. 2

¹⁴⁵ Klass and Others v. Germany, 5029/71, 06.09.1978.

aracılığıyla yapılan iletişimi özel hayatın gizliğini kapsamında kabul etmiştir (Küzeci, s. 299).

AİHS, AİHM içtihatları ve Anayasanın 22. Maddesi hükümleri dikkate alınarak Türkiye'de iletişime müdahale kural olarak yasaklanmış buna aykırı hareket edenlerin TCK'nın 132. maddesi uyarınca cezalandırılacakları hüküm altına alınmıştır. Diğer taraftan iletişime kamu gücüyle müdahale imkanı da çok sıkı koşullara bağlanmıştır.

Ceza Muhakemesi Kanunun 135-138. maddelerinde “*telekomünikasyon yoluyla yapılan iletişimin denetlenmesi*” düzenlenmiştir. 135. madde uyarınca bazı suçlarla ilgili olarak yapılan soruşturma ve kovuşturmada, ağır ceza mahkemesi veya gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısının kararıyla şüpheli veya sanığın telekomünikasyon yoluyla iletişimi tespit edilebilir, dinlenebilir, kayda alınabilir ve sinyal bilgileri değerlendirilebilir. Bu yola başvurulabilmesi için suç işlendiğine ilişkin somut delillere dayanan kuvvetli şüphe sebeplerinin bulunması ve başka şekilde delil elde edilememesi şartları birlikte aranmaktadır. Ayrıca madde metninde 21/2/2014 tarihli ve 6526 sayılı Kanunla yapılan değişiklik ile bu hüküm uyarınca alınacak tedbire ağır ceza mahkemesince oy birliğiyle karar verilebilecektir¹⁴⁶.

CMK'nın 135. maddesine göre iletişimin kayda alınması tedbirine ancak madde de sayılan suçlar için başvurulabilecektir. Bu suçlara bakıldığında uyuşturucu ticareti, adama öldürme gibi ağır nitelikli suçlar olduğu görülecektir. Basit nitelikli suçlar için bu hakka müdahalenin kabul edilmemesi önemli bir güvence oluşturmaktadır.

CMK'da bu tedbir açısından amaç gerçekleştiğinde veya usule ilişkin şartlar oluşmadığında verilerin yok edilmesine ilişkin hükümler de bulunmaktadır. Buna göre şüpheli hakkında kovuşturmaya yer olmadığına dair karar verilmesi ya da mahkemenin onayının yirmidört saat içinde alınmaması halinde, uygulamaya son verilmekte ve tespit veya dinlemeye ilişkin kayıtlar Cumhuriyet savcısının denetimi altında en geç on gün içinde yok edilmektedir. Bu durumda soruşturma evresinin

¹⁴⁶ İletişimin denetlenmesi ile ilgili ayrıntılı bilgi için bkz. **Taşkın, Mustafa**, Adli ve İstihbari Amaçlı İletişimin Denetlenmesi, Seçkin Yayınevi, Ankara, 2011, s. 122; **Centel, Nur/Zafer, Hamide**, Ceza Muhakemesi Hukuku, 10. Bası, Beta, İstanbul, 2013, s. 403-415

bitiminden başlayarak, en geç onbeş gün içinde, tedbirin nedeni, kapsamı, süresi ve sonucu hakkında Cumhuriyet Başsavcılığınca ilgisine yazılı olarak bilgi verilmek zorundadır (m. 137/3-4, Centel ve Zafer, 2013: s. 412). Bu yükümlülüğe aykırı hareket eden kamu görevlileri ise TCK'nın 138. maddesinde düzenlenen “verileri yok etmeme” suçunu işlemiş olacaklardır.

Adli olaylarda kişilerin bu yöntemle özel hayatlarına müdahale çok sıkı koşullara bağlanmışken idari olaylar ve idari düzenlemeler için aynı şeyi söylemek mümkün değildir.

Türkiye'de idari kolluk faaliyetleri çerçevesinde de iletişimin tespiti, kayda alınması, sinyal bilgilerinin değerlendirilmesi yapılmaktadır. Polis Vazife ve Selahiyet Kanunun ek 7. maddesi ve Jandarma Teşkilat Görev ve Yetkileri Kanununun ek 5. maddesi, bu yetkinin dayanağını oluşturmaktadır. Ancak idari aşamada mili güvenlik, anayasal düzen, ülkenin bütünlüğü ve genel güvenliğin sağlanması amaçları için alınan bu tedbir sonucu elde edilen verilerin durumu ne olacaktır? Bu soruya cevap verebilmek için ikili bir ayırım yapmak gerekir. İlk olarak, konu idari aşamadan adli aşamaya intikal ettiği takdirde sorun bulunmamaktadır. Zira yukarıda izah edildiği üzere CMK da bu tür veriler için yeterli koruma mekanizmaları bulunmaktadır. Ancak konu adli aşamaya intikal etmemiş ise veya etme ihtimali yok ise bu durumda bu tedbirin uygulanması sonucu elde edilen kişisel veriler ne olacaktır?

Bu konuda verilerin ne olacağına ilişkin PVSK ve JTGHK'da bir hüküm bulunmamaktadır. Bu husus 10.11.2005 tarihli ve 25989 sayılı Resmi Gazete yayınlanarak yürürlüğe giren “Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti, Dinlenmesi, Sinyal Bilgilerinin Değerlendirilmesi ve Kayda Alınmasına Dair Usul ve Esaslar İle Telekomünikasyon İletişim Başkanlığının Kuruluş, Görev ve Yetkileri Hakkında Yönetmelik” in 11. maddesinde düzenlenmiştir. Ancak bu konu yönetmelikle düzenlenebilecek bir konu değildir. Zira bu tedbir doğrudan anayasada güvence altına alınan özel hayatın gizliliği ve haberleşme özgürlüğü temel haklarına müdahale niteliğini taşımaktadır. O yüzden ki, adli aşamada o kadar yasal güvence bulunmasına rağmen bu konu CMK'nın 137. Maddesinde düzenlenmiştir. Bu nedenle idari aşamada yapılan dinlemeler sonucu elde edilen kayıtların nasıl ve ne zaman yok edileceğinin de ilgili Kanunda düzenlenmesi gerekmektedir.

3.10.2.4. Teknik Araçlarla izleme

Çalışmamızın ilk bölümünde de belirtildiği üzere kişinin sesinin yanında görüntüsü de kişisel veri niteliğindedir. Bu nedenle kişilerin görüntülerinin kayda alınması bu kayıtların kullanılması veya üçüncü kişilerle paylaşılması, kişisel verilerin korunması kapsamında değerlendirilmektedir. Ayrıca kişilerin görüntülerinin hukuka aykırı olarak kaydedilmesi özel hayatın gizliğini ihlal edecek niteliktedir. Bunun için gerek AİHS 8, gerek Anayasa 20. maddelerinde bu hakka müdahale sebepleri açıkça belirtilmek suretiyle bu hak koruma altına alınmıştır. Hakka müdahale yönetimleri ise kanunlarda düzenlenmiştir.

Ceza Muhakemesi Kanununda düzenlenen “teknik araçlarla izleme tedbiri” de bu hakka müdahale yöntemlerinden biridir. CMK’nın 140. maddesine göre¹⁴⁷

¹⁴⁷ “*Teknik araçlarla izleme*”

Madde 140 – (1) Aşağıdaki suçların işlendiği hususunda somut delillere dayanan kuvvetli şüphe sebepleri bulunması ve başka suretle delil elde edilememesi hâlinde, şüpheli veya sanığın kamuya açık yerlerdeki faaliyetleri ve işyeri teknik araçlarla izlenebilir, ses veya görüntü kaydı alınabilir:

a) Türk Ceza Kanununda yer alan;

1. Göçmen kaçakçılığı ve insan ticareti (madde 79, 80),

2. Kasten öldürme (madde 81, 82, 83),

3. Nitelikli hırsızlık (madde 142) ve yağma (madde 148, 149),⁽¹⁾

4. Uyuşturucu veya uyarıcı madde imal ve ticareti (madde 188),⁽¹⁾

5. Parada sahtecilik (madde 197),

6. **(Mülga:21/2/2014–6526/14 md.)**

7. Fuhuş (madde 227)

8. İhaleye fesat karıştırma (madde 235),

9. Rüşvet (madde 252),

10. Suçtan kaynaklanan malvarlığı değerlerini aklama (madde 282),

11. Silahlı örgüt (madde 314) veya bu örgütlere silah sağlama (madde 315),

12. Devlet Sırlarına Karşı Suçlar ve Casusluk (madde 328, 329, 330, 331, 333, 334, 335, 336, 337),

Suçları.

b) Ateşli Silahlar ve Bıçaklar ile Diğer Aletler Hakkında Kanunda tanımlanan silah kaçakçılığı (madde 12) suçları.

c) Kaçakçılıkla Mücadele Kanununda tanımlanan ve hapis cezasını gerektiren suçlar.

d) Kültür ve Tabiat Varlıklarını Koruma Kanununun 68 ve 74 üncü maddelerinde tanımlanan suçlar.

(2) Teknik araçlarla izlemeye ağır ceza mahkemesi tarafından oy birliğiyle karar verilir. İtiraz üzerine bu tedbire karar verilebilmesi için de oy birliği aranır.

(3) Teknik araçlarla izleme kararı en çok üç haftalık süre için verilebilir. Bu süre gerektiğinde bir hafta daha uzatılabilir. Ancak, örgütün faaliyeti çerçevesinde işlenen suçlarla ilgili olarak gerekli görülmesi hâlinde, mahkeme yukarıdaki süreler ek olarak her defasında bir haftadan fazla olmamak ve toplam dört haftayı geçmemek üzere uzatılmasına karar verebilir.

(4) Elde edilen deliller, yukarıda sayılan suçlarla ilgili soruşturma ve kovuşturma dışında kullanılamaz; ceza kovuşturması bakımından gerekli olmadığı takdirde Cumhuriyet savcısının gözetiminde derhâl yok edilir.

maddede belirtilen suçlardan birinin işlendiği konusunda somut delillere dayan kuvvetli şüphe sebeplerinin bulunması ve başka şekilde delil elde edilememesi durumunda, şüpheli veya sanığın kamuya açık yerlerdeki etkinlikleri ve işyeri teknik araçlarla izlenebilir, ses veya görüntü kaydı alınabilir.

Bu tedbire başvurulabilmesi için ağır ceza mahkemesi tarafından oy birliğiyle karar verilmesi aranmıştır. Ayrıca her suç içinde bu tedbire başvurulamamaktadır. Bu tedbir maddede sayılan suçlar için geçerlidir (CMK m. 140/2).

Ayrıca CMK da bu tedbir neticesinde elde edilen verilerin toplanma amacı dışında kullanılamayacağı ve verilerin yok edilmesine ilişkin hükümler de bulunmaktadır. Buna göre, elde edilen deliller, maddede sayılan suçlarla ilgili soruşturma ve kovuşturma dışında kullanılamaz; ceza kovuşturması bakımından gerekli olmadığı takdirde Cumhuriyet savcısının gözetiminde derhâl yok edilir (CMK m. 140/4)

Diğer taraftan hükümde belirtilen koşullar gerçekleşmeden yapılan izleme ve kaydetme, TCK'nın 134. maddesinde düzenlenen özel yaşamın gizliliğini ihlal suçunu, verilerin belirlenen zamanda yok edilmemesi ise TCK'nın 138. maddesindeki verileri yok etmeme suçunu oluşturabilecektir.

Görüldüğü üzere, iletişim dinlenmesi, kayda alınması tedbirinde olduğu gibi adli olaylarda bu tedbire başvurma, diğer bir deyişle özel hayatın gizliliğine ve kişisel verilerin korunması hakkına müdahale yöntemleri çok sıkı koşullara bağlanmış; verilerin gizli olduğu, amacı dışında kullanılamayacağı ve amaç hasıl olduğunda veya tutulmasına artık ihtiyaç kalmadığında verilerin derhal yok edilmesi hüküm altına alınmıştır.

Adli olaylarda kişilerin bu yöntemle özel hayatlarına müdahale çok sıkı koşullara bağlanmışken idari olaylar ve idari düzenlemeler için aynı şeyi söylemek mümkün değildir.

Polis, Jandarma ve MİT tarafından somut bir suç şüphesi bulunmadan istihbarat ya da suçların önlenmesi amacıyla kişilerin görüntülerinin izlenebilmekte

(5) Bu madde hükümleri, kişinin konutunda uygulanamaz.”

ve kayda alınabilmektedir. Bu faaliyetin en bilinen örneği Emniyet Müdürlükleri bünyesinde faaliyete geçirilen *"kent bilgi ve güvenlik sistemi"* olarak adlandırılan MOBESE'dir¹⁴⁸. Sistem içerisinde yer alan çeşitli unsurların yanında *"bölge görüntüleme sistemi"* denilen sistem aracılığı ile halkın yoğun olarak bulunduğu ve geçiş güzergâhı olarak bilinen yerlere konulan kameralar ile bu kameralardan alınan görüntülerin merkeze sürekli olarak aktarılıp kaydedilmesi söz konusudur. Asayiş, güvenlik gerekçeleriyle pek çok demokratik devlette benzer uygulamaların bulunduğu görülmektedir. Ancak buradaki sorun, sistemin kurulması değil, bu konuya ilişkin herhangi bir yasal düzenlemenin bulunmamasıdır (Küzeci, 2010: s. 210).

Oysa bu tür tedbirler temel hak ve özgürlüklere müdahale oluşturmaktadır. Dolayısıyla bu müdahalenin meşru olabilmesi için, sınırlamanın kanunla belirlenmesi, ölçülü olması ve Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olması gerekir (AY m. 13). Ayrıca görüntülerin bir kişinin kimliğini belirlenebilir kılması durumunda kişisel verilerin korunması ilkeleri dikkate alınmalıdır (Şimşek, 2008: s. 169).

Diğer taraftan meşru bir sebebe dayanılarak yapılan müdahalelerde amaca bağlılık ilkesi hiçbir zaman göz ardı edilmemelidir. Buna göre kamera sistemleri ile gözetimde kişinin kimliği ile ilişkilendirme gerekli değilse kayıtlar anonim olarak tutulmalıdır. Bunun yanında görüntülerin yalnızca izlenmesi yeterli ise ayrıca bunları kayıt altına almamak gerekir. Nitekim P.G. ve J.H. Birleşik Krallık'a karşı kararında AİHM de bu görüşü destekler şekilde tespitlerde bulunmuştur. Mahkemeye göre: *"Bir kişinin evinin veya özel mülkünün dışında alınan önlemlerin, kişinin özel hayatına dâhil olup olmadığının belirlenmesinde göz önünde bulundurulması gereken bir kaç unsur vardır. İnsanlar bazen kamuya açık bir biçimde kaydedilebilen veya rapor edilebilen faaliyetlere bilerek veya kasten dâhil olabildikleri için, kişinin mahremiyet hakkındaki makul beklentileri, kararı belirleyen faktör olmasa da, önemli bir faktör olabilir. Sokakta yürüyen bir kişi, kaçınılmaz olarak orada bulunan diğer kişiler tarafından görünür olacaktır. Teknolojik yöntemlerle aynı kamusal mekânın izlenmesi de (örneğin kapalı devre televizyon ile güvenlik görevlilerinin izlemesi) benzer özelliktedir. Ancak kamu alanındaki bu tür*

¹⁴⁸MOBESE'nin tam açılımı, "Mobil Elektronik Sistem Entegrasyonu"dur.

bilgilerin sistematik veya kalıcı olarak kaydı söz konusu olunca, özel hayatla ilgili konular ortaya çıkmaktadır. İşte bu nedenle güvenlik görevlileri tarafından belirli bir birey hakkında toplanan dosyalar, söz konusu bilgi müdahaleci ve gizli bir yöntemle toplanmamış olsa bile, 8. madde kapsamına girer¹⁴⁹”.

3.10.2.5. Duruşmanın Kapalı Yapılması

Yine kişisel verilerin gizliliğinin sağlanması açısından önemli bir düzenleme de “duruşmada okunması zorunlu belge ve tutanaklar” başlıklı CMK’nun 209. maddesidir. Maddenin ikinci fıkrası, “*sanığa veya mağdura ilişkin kişisel verileri içeren belgelerin, açıkça istemeleri halinde kapalı duruşmada okunmasına karar verilebileceği*” şeklindedir. Maddeyle ilgisiz kişilerin davanın taraflarına ait kişisel verileri öğrenmelerinin engellenmesi amaçlanmıştır. Ayrıca Anayasaya uygun olarak kişisel verilerin açıklanması kişinin rızasına bırakılmıştır.

3.11. 6100 sayılı Hukuk Usulü Muhakemeleri Kanunu

Ceza Muhakememesi Kanununda olduğu gibi Hukuk Usulü Muhakemeleri Kanununda da duruşma yapılırken davanın taraflarının kişisel verilerinin korunmasına ilişkin hükümler bulunmaktadır. Bilindiği üzere açık yargılama ilkesinin bir gereği olarak duruşmalar alenidir. Davanın tarafları haricinde davayı izlemek isteyenlerde duruşmalara katılabilmektedirler. Ancak Kanunda belirtilen bazı durumlar için duruşmaların gizli yapılmasına karar verilebilmektedir. Bu durumu düzenleyen 6100 sayılı Kanunun 28. Maddesinin ikinci fıkrası, “*Duruşmaların bir kısmının veya tamamının gizli olarak yapılmasına ancak genel ahlâkın veya kamu güvenliğinin kesin olarak gerekli kıldığı hâllerde, taraflardan birinin talebi üzerine yahut resen mahkemece karar verilebilir.*” Şeklindedir. Bu hükme göre taraflar duruşmanın gizli yapılmasını talep edebilmektedirler. Ancak bunun için genel ahlâkın veya kamu güvenliğinin kesin olarak gerekli kıldığı hallerin bulunması gerekmektedir.

Konuya kişisel verilerin korunması açısından bakılacak olursa, davanın tarafları, kendi özel hayatlarına ilişkin kişisel verilerin üçüncü kişilerce öğrenilmesini engel olmak için bu verilerin ifaışının genel ahlâka aykırı olacağı iddiasıyla duruşmanın gizli yapılmasını hâkimden isteyebileceklerdir.

¹⁴⁹ Küzeci, s. 311; P.G. ve J.H., Birleşik Krallık'a karşı, par. 57 bkz. *Duetrtre*, s. 286-287.

Hukuk Usulü Muhakemeleri Kanununda kişisel verilerin korunmasına yönelik bir başka hükümde, 6100 sayılı Kanunun Kısıt ve yayın yasağı başlıklı 153. Maddesidir. Maddenin birinci fıkrası, *“Duruşma sırasında fotoğraf çekilemez ve hiçbir şekilde ses ve görüntü kaydı yapılamaz. Ancak, dava dosyasında saklı kalmak kaydıyla, yargılamanın zorunlu kıldığı hâllerde, mahkemece çekim yapılabilir ve kayıt alınabilir. Bu şekilde yapılan çekim ve kayıtlar ile kişilik haklarını ilgilendiren konuları içeren dava dosyası içindeki her türlü belge ve tutanak, mahkemenin ve ilgili kişilerin açık izni olmadıkça hiçbir yerde yayımlanamaz.”* Şeklinde dir. Maddeye göre, yargılamanın zorunlu kıldığı hallerde duruşma sırasında yapılan kayıtlar, bu kayıtlar taraflara ait kişisel verileri içereceğinden, mahkemenin ve ilgili kişilerin izni olmadıkça yayımlanamayacaktır. Bu hükümde, Anayasal düzenleme gereği, kişisel verilerin işlenmesinde ilgili kişinin rızasının alınması gerekliliği kuralına uygun bir hükümdür.

4. DİĞER DÜZENLEMELER

4.1. Kişisel Verilerin Korunmasına İlişkin Kanun Tasarısı

Avrupa Konseyinin 108 nolu Sözleşmesinin 28 Ocak 1981 tarihinde ülkemiz tarafından imzalanmasıyla, kişisel verilerin korunması alanında mevzuat çalışmaları başlatılmış, ancak yapılan çalışmalar 2000’li yıllara kadar taslak oluşturmaktan öteye geçememiştir. Adalet Bakanlığı tarafından 2004 yılında oluşturulan bir bilim komisyonu tarafından hazırlanan Kişisel Verilerin Korunması Kanunu Tasarısı, 2006 yılında ancak Başbakanlığa gönderilebilmiştir. Taslak, Bakanlar Kurulunca 07.04.2008 tarihinde kabul edilmesi üzerine Tasarı haline gelmiş ve TBMM’ye kanunlaşması için gönderilmiştir. Ancak araya yerel seçimlerin girmesi nedeniyle o dönem yasalaşamayınca İktüzüğünün 77. maddesi gereğince hükümsüz sayılmış ve Başbakanlığa iade edilmiştir.

Tasarının iade edilmesinden sonra Adalet Bakanlığı tarafından konuyla ilgili yeni bir süreç başlatılmış, mevcut Tasarı, yapılan eleştiri ve öneriler doğrultusunda yeniden kaleme alınmış ve 08/06/2012 tarihinde ‘Kişisel Verilerin Korunması Kanunu Tasarısı’ adı altında tekrardan Başbakanlığa sevk edilmiştir.

Tasarının şu anda Başbakanlıkta bulunduğu ve henüz TBMM’ye sevk edilmediği bilinmektedir. Tasarıyla getirilen düzenlemelere bakıldığında:

Tasarıyla, kişisel verilerin işlenmesinde kişinin dokunulmazlığı, maddi ve manevi varlığı ile temel hak ve özgürlüklerinin korunması ve kişisel verileri işleyen gerçek ve tüzel kişilerin uyacakları esas ve usullerin düzenlenmesi amaçlanmaktadır¹⁵⁰.

Yenilenen Tasarı ile sadece gerçek kişilerin verileri korunmakta¹⁵¹, kişisel verilerin işlenmesinde temel ilkeler belirlenmekte, kişisel verilerin işlenmesinin hangi şartlarda mümkün olduğu yani hangi durumlarda hukuka uygun şekilde veri işlenebileceği açıklığa kavuşturulmakta, özel nitelikli veriler (hassas veriler) için işlem yasağı getirilmekte, veri işleyenlere kişileri aydınlatma konusunda ve verilerin güvenliğini sağlama konusunda yükümlülükler yüklenmekte, ayrıca verileri işlenen kişilere, verileri hakkında bilgi sahibi olma, verilerin düzeltilmesini ve silinmesini isteme gibi bazı haklar tanınmaktadır.

Tasarıyla ayrıca verileri işlenen kişilerin haklarını korumak ve şikayetleri konusunda karar vermek, ver işleyenlerin Kanunla belirlenen yükümlülüklerine uyup uymadığını denetlemek üzere “Kişisel Verileri Koruma Kurulu” kurulması öngörülmektedir¹⁵².

Bu olumlu düzenlemelerin yanında Tasarıda sorunlu bazı düzenlemeler de bulunmaktadır. Tasarının “istisnalar” kısmında bazı kurum ve kuruluşların tasarı hükümlerinin tamamından istisna tutuldukları görülmektedir. Devletin İstihbarat birimleri, basın kuruluşları ve MASAK gibi kurumlar, kişisel verilerin korunması sistemi kapsamına alınmamıştır. Bu durum şu açılardan sakıncalıdır:

Öncelikle kişisel verilerin korunması sistemi bir bütün olup, sadece verilerin elde edilmesi ve kaydedilmesi aşamasıyla sınırlı değildir. Verilerin elde edilmesinden silinmesine kadar geçen bütün aşamaları kapsamaktadır. Ayrıca kişisel

¹⁵⁰ Tasarı hakkındaki eleştiriler için bkz. **Şen, Ersan**, Yorumluyorum, Ceza Hukuku Perspektifinden Güncel Olaylara Bakış, Seçkin Yayınevi, Ankara, 2011, s. 196 vd.; **İlkiz, Fikret**, “Kişisel Verilerin Korunması ve Kanun Tasarısı”, Güncel Hukuk Dergisi, Temmuz 2009/7-67, s. 12-23; **Özdemir, Hayrunnisa**, “Türkiye’de Kişisel Verilerin Korunması”, <http://inet-tr.org.tr/inetconf14/bildiri/81.doc> Erişim T: 21.02.2012

¹⁵¹ Tasarının ilk halinde tüzel kişilerin de verileri kapsam dâhilinde iken yenilenen Tasarıda sadece gerçek kişilerin verileri korunma kapsamına alınmıştır. Bkz. <http://www.kgm.adalet.gov.tr/Tasariasamalari/Basbakanlik/Basbakanlik.html> Erişim T: 30.04.2014

¹⁵² Bu Kurulun bağımsızlığı konusunda yapılan eleştiri ve Kurulun yapısına ilişkin öneriler konusunda ayrıntılı bilgi için bkz. **Civelek**, 2011: s. 156-177

verilerin korunması sisteminde asıl önemli olan bu kanunda öngörülen kural ve ilkelerin veri işleyen tüm kişi ve kuruluşlarda uygulanmasıdır. Bir istihbarat kurumunun sadece kendi kanununa tabi olması halinde, kendi kanuna göre verileri kaydetme imkânı olabilir. Ancak kaydettikten sonra verilerin korunması nasıl sağlanacak, üçüncü kişilere aktarımı, ilgili kişinin hakları, aydınlatma yükümlülüğü, kişinin başvuru ve şikâyet haklarını kullanabilmesi, veri koruma kurulunun denetimi hususları nasıl sağlanacaktır.

Diğer taraftan özellikle Avrupa ülkeleri ile veri paylaşımında sorunlar yaşanacaktır. Zira AB ülkeleri kişisel verileri yeterli düzeyde korumayan lkelerle veri paylaşımı yapmamaktadır. Ülkemizde istihbarata ilişkin verilerin yeterli düzeyde, bu konuya özgü bir kanun ile korunmaması nedeniyle bu ülkeler istihbari bilgileri paylaşmayacaklardır. Çünkü verdikleri bilgileri koruyacak bir kanun bulunmamakta veya bulunmakta ise de bu kurumlar istisna tutulduğu için korunmadığı anlamına gelecektir.

Bu nedenle Tasarının istisnaları düzenleyen hükümleri, sadece kişisel ve ailevi faaliyetlerde kişisel veri işlenmesi ile sınırlı tutulmalı, bunun haricinde kişisel veri işleyen tüm kişi ve kurumları kapsama alınmalıdır. Ancak yine Tasarıda öngörülen bir kısım yükümlülüklerden istisnalar getirilebilir. Örneğin istihbarat kurumlarının ilgili kişileri aydınlatma yükümlülüğüne tabi tutulmaması gibi.

Tasarı kanunlaşması halinde, Anayasadaki düzenlemelerin nasıl uygulanacağı konusunda rehberlik etmenin yanı sıra, tezin ilerleyen kısımlarında da belirtileceği üzere, Türk Ceza Kanununda kişisel verilere karşı işlenen suçlarda suçun konusu ve hukuka uygunluk nedenleri gibi sorunlu alanlarda uygulamaya ışık tutacaktır.

Diğer yandan da hem hukuk sistemimizdeki kişi hak ve özgürlüklerin güvence altına alınması ile ilgili boşluğu doldurmak hem de kişisel verilerle ilgili olarak başka ülkelerden aktarılması istenilen bilgilerin elde edilmesinde yaşanan zorlukları gidermek için Tasarının kanunlaşması elzem görülmektedir¹⁵³.

¹⁵³ “Kişisel Verilerin Korunması” 1. Bilişim Şurası Hukuk Raporu, 10-12 Mayıs 2002, Ankara, <http://www.scribd.com/doc/19952426/1-Bilisim-Surasi-Hukuk-Raporu?query=ki%C5%9Fisel+verilerin+korunmas%C4%B1>. s. 31, Erişim Tarihi:20.03.2012

4.2. Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik

Elektronik haberleşme sektöründe kişisel verilerin işlenmesi, saklanması ve gizliliğinin korunması için bu alanda faaliyet gösteren işletmecilerin uyacakları usul ve esasları düzenlemek amacıyla, “Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik” kabul edilmiştir¹⁵⁴.

Bu Yönetmelik ile güvenlik, trafik verilerinin işlenmesi, kullanım risklerini bildirme yükümlülüğü, iletişim gizliliği, istek dışı haberleşmeler (spam) gibi konularda hemen hemen Avrupa Birliği düzenlemelerine denk hükümler getirilmiştir (Özdemir, 2012: a.g.m.; Küzeci, 2010: s. 301). Yönetmelikteki düzenlemelere bakıldığında, ilkeler ve kurallar açısından, Kişisel Verilerin Korunması Kanun Tasarı ile benzer hükümler içerdiği görülecektir¹⁵⁵.

¹⁵⁴ Yönetmelik 24.07.2012 tarihli ve 28363 sayılı Resmi Gazetede yayınlanarak yürürlüğe girmiştir.

¹⁵⁵ Yönetmelik metni için bkz.

<http://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=7.5.16405&MevzuatIliski=0&sourceXmlSearch=Erişim T: 30. 04.2014>

DÖRDÜNCÜ BÖLÜM

5237 SAYILI TÜRK CEZA KANUNUNDA KİŞİSEL VERİLERİN HUKUKA AYKIRI OLARAK KAYDEDİLMESİ, VERİLERİ HUKUKA AYKIRI OLARAK VERME VEYA ELE GEÇİRME, VERİLERİ YOK ETMEME SUÇLARI

1. GENEL OLARAK

Kişisel verilerin korunmasına ilişkin hukuki düzenlemeler yapmış olan ülkelerin mevzuatlarına bakıldığında, kişisel verilerin korunmasına ilişkin yaptırım içeren düzenlemelerin bazı ülkelerde özel kanunlarda, bazı ülkelerde hem özel kanunlarda hem de ceza kanunlarında, bazı ülkelerde ise sadece ceza kanunlarında düzenlendiği görülmektedir¹⁵⁶. Ülkemizde ise henüz kişisel verilerin korunmasına ilişkin bir kanun olmadığından kişisel verilerin korunmasını sağlamaya yönelik suçlar, Fransa'dakine benzer şekilde, 5237 sayılı Türk Ceza Kanununda düzenlenmiştir (Ketizmen, 2008: s. 217).

Bu tercihten hareketle, kişisel verilerin korunması açısından oldukça önemli olan ve 765 sayılı TCK'da karşılığı olmayan 135, 136 ve 138. maddelerde yer alan suçlar ceza hukuku mevzuatımıza 5237 sayılı Türk Ceza Kanunu ile girmiştir. Kişisel verilerin hukuka aykırı olarak bir yerlere kaydedilmesi veya başkalarına aktarılması eylemlerinin, insanların fişlenmesi ve çoğu zamanda özel hayatın gizliliğinin ihlal edilmesi sonucunu doğurması nedeniyle, suç olarak tanımlanması yerinde olmuştur (Parlar ve Hatipoğlu, 2008: s. 2042; Özen, 2009: s. 13).

Türk Ceza Kanunun 135. maddesinde “kişisel verilerin kaydedilmesi” suçu, 136. maddesinde “kişisel verileri hukuka aykırı olarak verme veya ele geçirme” suçu, 138. maddesinde ise, “verileri yok etmeme” suçu düzenlenmiştir. Bu suçların TCK'daki düzenleme yerine bakıldığında ise TCK'nun “Kişilere Karşı Suçlar” başlıklı ikinci kısmının “Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar” başlıklı dokuzuncu bölümünde yer aldığı görülmektedir.

¹⁵⁶ Bkz. Federal Almanya Veri Koruma Yasası (BDSG), m.43-44; İtalyan Veri Koruma Yasası, m. 167-172. Fransa'da ise Ceza Kanunu kapsamında yer almaktadır.

TCK'nın bu bölümü; haberleşmenin gizliliğini ihlal (TCK. m. 132), kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması (TCK. m. 133), özel hayatın gizliliğinin ihlali (TCK. m. 134), kişisel verilerin kayıt edilmesi (TCK. m. 135), verileri hukuka aykırı olarak verme veya ele geçirme (TCK.m. 136) ve kişisel verileri yok etme de suçlarından (TCK. m. 138) oluşmaktadır. 137. maddede, nitelikli haller madde başlığı altında suçu ağırlaştıran nedenlere yer verilmiştir. 139. maddede, bu suçların takibini düzenlemiştir. Bazı suçlar res'en, bazı suçlar şikâyet üzerine soruşturulmakta ve kovuşturulmaktadır. Ayrıca suça karışan tüzel kişiler hakkında da güvenlik tedbirleri uygulanması öngörülmüştür (TCK m. 140).

Maddelere bakıldığında düzenlenen suçların aynı hukuki yararı koruduğu ancak işleniş bakımından farklı suçlar olduğu görülecektir. 132 ve 133. Maddelerde temelde kişilerin özel hayatının gizliliği korunmakta, özelde ise kişilerin haberleşme hürriyeti korunmaktadır. 134. maddede ise doğrudan kişinin özel hayatının gizliliğini korumaktadır. 135 vd. maddelerde düzenlenen suçlar ise temelde özel hayatın gizliliği korunmakta ise de özelde kişisel verilerin gizliliği korunmaktadır¹⁵⁷.

Kişisel verilere karşı işlenen suçların düzenlendiği yer itibarıyla kişisel verilerin korunmasının özel hayatın gizliliğinin korunması hakkı kapsamında değerlendirildiği söylenebilir de, önceki bölümde de belirtildiği üzere, bazen alenilemiş verilerin de korunması gerektiği, kişinin alenileşen ve herkes tarafından bilinebilen verilerinin de istismar edilerek kişilik haklarının ihlal edilebilme imkanı olduğu ve bu suretle de TCK'daki bu suçlara konu olabileceği, bu nedenle kişisel verilere karşı işlenen bu suçları, salt özel hayata karşı işlenen suçlar olarak değerlendirmenin mümkün olmadığı kanısındayız.

Nitekim Lizbon Antlaşmasının 1 Aralık 2009 tarihinde yürürlüğe girmesi ile bağlayıcı hale gelen Avrupa Birliği Temel Haklar Şartında, kişisel verilerin korunması, özel hayatın gizliliği hakkından ayrı, müstakil bir temel hak olarak düzenlenmiştir. Keza 2010 yılında yapılan Anayasa değişikliği ile kişisel verilerin korunmasını isteme hakkı temel bir hak olarak 20. maddesinin üçüncü fıkrasında

¹⁵⁷ Benzer görüş için bkz. **Hafizoğulları, Zeki/Özen, Muharrem**, Türk Ceza Hukuku, Özel Hükümler, Kişilere Karşı Suçlar, US-A Yayıncılık, Ankara 2011, s. 256. Ayrıca bu yazarlara göre, özel hayatın gizliliğinin düzenlendiği anayasanın 20. maddesi ile TCK'nın özel hayata ve hayatın gizli alanına karşı işlenen suçların uyumlu olmadığı; TCK'da aile hayatının gizliliğinin ihlali ile hayatın gizli alanının ihlalden söz edilmediğini ifade etmişlerdir. Bkz. **Hafizoğulları/Özen**, 2011: s. 256

yerini almıştır. Anayasada, kişisel veriler, özel hayata ilişkin olan veya olmayan şeklinde bir ayrıma da tabi olmadığından tüm kişisel veriler koruma altına alındığı kanısındayız.

Diğer taraftan TCK' da kişisel verilerin korunması hakkının ihlaline yönelik yaptırımlar düzenlenmiş ise de bu noktada eksiklik, kişisel verilerin korunmasına yönelik bütüncül bir yasal düzenlemenin halen yürürlüğe girmemiş olmasıdır. Nitekim kişisel verilerin hukuka uygun şekilde nasıl işleneceği tam olarak açıklığa kavuşturulmadan hukuka aykırı şekilde işlenmesi halleri suç olarak tarif edilmiştir. Bu durumda uygulamada sorunlar yaratmakta, uygulayıcıların farklı farklı kararlar vermesine sebep olmaktadır.

Ayrıca TCK' da aşağıda incelenecek hükümlerin varlığına karşın kişisel verilerin tanımlanmamış olması, özellikle konuya ilişkin özel yasanın halen kabul edilmediği dikkate alındığında, bir başka önemli sorun olarak karşımıza çıkmaktadır. Biz bu çalışmada aşağıdaki hükümler yorumlanırken kişisel veriyi, uluslararası sözleşmeler ve Kişisel Verilerin Korunması Kanun Tasarısında benimsenen *"belirli ya da belirlenebilir bir kişiye ilişkin her türlü bilgi"* olarak kabul edeceğiz¹⁵⁸.

Öte yandan, TCK'da yer alan kişisel verilerin korunmasına yönelik suçları yorumlarken başta 108 sayılı AK Sözleşmesi olmak üzere uluslararası düzenlemeler hep göz önünde tutulmalıdır. Nitekim yasa koyucunun belirtilen düzenlemeleri benimserken özellikle AK Sözleşmesini dikkate aldığını 135. maddenin gerekçesi ortaya koymaktadır. 135. maddenin gerekçesinde, 108 sayılı AK Sözleşmesinin ilgili hükümlerine geçerlilik tanındığı belirtilmektedir¹⁵⁹. Benzer şekilde bazı yazarlar da gerekçede yer alan bu ifade dolayısıyla maddenin açıklanması ve yorumlanması bakımından AK Sözleşmesi hükümlerinden yararlanmanın olanaklı olduğunu ifade etmişlerdir (Özbek vd, 2011: s. 947).

¹⁵⁸ Kişisel verinin ceza hukuku uygulamasında kabul edilen tanımı için bkz. **Özbek**, TCK İzmir Şerhi, 2008: s. 947.

¹⁵⁹ Gerekçe için bkz. **Artuk, M. Emin/Gökçen, Ahmet/Yenidünya, Ahmet Caner**, Türk Ceza Kanunu Şerhi, Özel Hükümler, C. 4, Turhan Kitabevi, Ankara, 2009, s. 3214; **Özgenç, İzzet**, Türk Ceza Kanunu Gazi Şerhi (Genel Hükümler), 2. Baskı, Seçkin, Ankara 2005

2. KİŞİSEL VERİLERİN HUKUKA AYKIRI OLARAK KAYDEDİLMESİ SUÇU

2.1. Genel Olarak

TCK'nın 135. maddesinde “*kişisel verilerin hukuka aykırı olarak kaydedilmesi*” eylemi suç olarak düzenlenmiştir. Maddenin birinci fıkrasında, kişisel verilerin hukuka aykırı olarak kayıt eden kimseye bir yıldan üç yıla kadar hapis cezası verileceği; ikinci fıkrasında ise, kişilerin siyasi, felsefi veya dini görüşlerine, ırkı kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimseye de aynı hüküm uyarınca ceza verilmesi öngörülmüştür¹⁶⁰.

Maddede öngörülen hapis cezasının miktarı, 6 Mart 2014 tarihinde yürürlüğe giren 21/2/2014 tarihli ve 6526 sayılı Terörle Mücadele Kanunu ve Ceza Muhakemesi Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun ile artırılarak altı ay olan cezanın alt sınırı bir yıla çıkarılmıştır. Değişikliğe gerekçe olarak, “*Anayasanın 20 nci maddesinde, herkesin kendisiyle ilgili kişisel verinin korunmasını isteme hakkına sahip olduğu düzenlenmiştir. Kişisel verilerin ve özel hayatın daha etkin korunması amacıyla kişisel verileri hukuka aykırı olarak kaydedenlere verilecek ceza artırılmaktadır.*” Hususları belirtilmiştir¹⁶¹.

Madde gerekçesinden de anlaşılacağı üzere, Anayasamızın 20. Maddesine eklenen üçüncü fıkrayla özel hayatın gizliliğinin korunması hakkı altında temel bir hak olarak düzenlenen kişisel verilerin korunmasını hakkının daha etkin bir şekilde korunabilmesi, bu konuda caydırıcılığın artırılması amacıyla bu suç nedeniyle verilecek ceza artırılmıştır.

¹⁶⁰ TCK'nın 135. maddesi şöyledir: “(1) Hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir.

(2) Kişilerin siyasî, 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.”

¹⁶¹ Değişiklik gerekçesi için bkz.

http://www.tbmm.gov.tr/develop/owa/tasari_teklif_sd.onerge_bilgileri?kanunlar_sira_no=148569

Erişim T: 10/5/2014

Bu deęişiklik yerinde olmakla birlikte maddede, ilerde ayrıntılı olarak belirtileceęi üzere, sorunlu bir kısım konularda ise herhangi bir deęişiklik yapılmamıştır. Nitekim kişisel verinin ne olduęu ve hukuka uygun olarak nasıl kayıt edilmesi gerektięi konusunda kanuni düzenleme yapılmadıęından cezai yaptırım öngören bu maddenin uygulaması sorunlu olduęu, uygulamacı yazarlar tarafından ileri sürölmüştür (Albayrak, 2013: s. 12).

Bu kapsamda madde metninde, kişisel veri tanımının yapılmaması nedeniyle doktrinde tereddütler oluşmuş ve kişisel verinin ne olduęu konusunda madde gerekçesinden ve dięer düzenlemelerden yararlanarak bir tanım yapılmaya çalışılmıştır. Bazı yazarlarca kişisel veri, kişi ile ilgili, kişiye ilişkin ve kişinin kendi malı olan kişisel bilgiler olarak nitelendirilmiştir. Ancak suçta ve cezada kanunilik ilkesi gereęi kişisel verinin yasa ile açıkça düzenlenmesi gerekmektedir (Tezcan, 2013: s. 1162).

Ayrıca maddenin ikinci fıkrasında sınırlı şekilde sayılan veriler, dięer kişisel verilerden farklı olarak hukuka aykırı kaydedilmeleri durumunda ayrımcılıęa yol açabilecek nitelikte olmaları bakımından bireyler açısından özellikli bir yere sahip olup, bu verilerin kaydedilmesi ile dięer kişisel verilerin kaydedilmesi eylemleri hakkında aynı cezanın öngörölmüş olması yerinde olmamıştır. Bu tür verilerin bireyler açısından taşıdıkları önem göz önüne alınarak daha ağırcezaı gerektiren nitelikli hal olarak öngörölmeleri daha yerinde olacaktır (Şener, 2011: s. 76).

2.1. Korunan Hukuki Deęer

Bu suçla korunan hukuki deęer kişinin özel hayatının gizlilięi ve kişisel verilerinin korunması hakkıdır (Özbek vd, 2013: s. 527; Soyaslan, 2006: s. 272; Hafizoęulları ve Özen, 2011: s. 276). Bir kısım yazarlar, kişisel verilerin korunmasının, kişinin manevi şahsiyetini korumak amacıyla kabul edilmiş bir koruma olduęunu, bu alanın da kişinin özel hayatının önemli bir kısmını oluşturduęunu ifade etmiştir (Albayrak, 2013: s. 12). Dięer bir kısım yazarlar ise suçla korunan hukuki yararın, Avrupa İnsan Hakları Sözleşmesinin 8. ve Anayasanın 20. maddelerinde güvence altına alınan kişilerin özel hayatının gizlilięi ve korunması hakkı olduęunu savunmuşlardır (Yaşar vd 2010: s. 4117; Özen, 2009: s. 14).

Doktrinde bu konuda görüş birliđi olmadığı gör÷lmektedir. Bunun nedeninin Anayasa ve Türk Ceza Kanunundaki kavram birliđinin sađlanamamasından kaynaklandığını söyleyebiliriz. 12/10/2004 tarihinde yürürlüđe giren 5237 sayılı TCK'da kişisel verilerin korunmasının ve gizliđinin ihlaline yönelik olarak yaptırımlar düzenlenmiş olmasına rağmen, kişisel verilerin korunması hakkı, Anayasada 2010 yılına kadar yer almamış ve özel hayatın gizliđi ve korunması hakkı kapsamında mütalaa edilmiştir. 7/5/2010 tarihli ve 5982 sayılı Kanunla Anayasanın 20. Maddesinde yapılan deđişiklikle, kişisel verilerin korunması hakkı temel bir hak olarak düzenlenmiştir.

Kanaatimizce bu deđişiklikten sonra artık TCK'da düzenlenen bu suçla korunmak istenen hukuki deđerin, özel hayatın gizliliđi ve kişisel verilerin korunması hakkı olduđuunda kuşku bulunmamaktadır.

Nitekim daha öncede değinildiđi gibi, kişisel verilerin korunması bütüncül bir sistem olup, verilerin toplanmasından kaydedilmesine, depolanmasından üçüncü kişilere aktarılmasına ve silinmesine kadar geçen tüm aşamaları kapsamaktadır. Bu aşamaların tümünde veri işleyenlerin hukuka uygun davranma mecburiyetleri olduđu gibi, kişinin de verileri hakkında bilgi alma, bu verilerinin silinmesini veya güncellenmesini talep etme gibi hakları bulunmaktadır. Bu aşamaların herhangi birinde hukuka aykırı davranılması veya kişinin belirtilen haklarını kullanmasının engellenmesi bu hakkın ihlali anlamına gelecektir.

Bu hak, 2010 yılından itibaren anayasal güvenceye de kavuşturulmuştur. Anayasanın 20. Maddesinin üçüncü fıkrasına göre, herkes kendisi ile ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak, kişinin kendisi ile ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsamaktadır. İşte TCK'nun 135. maddesindeki bu suç, kişinin Anayasa ile güvence altına alınan kişisel verilerin korunması hakkının ihlalini yaptırım altına alan bir düzenleme olarak karşımıza çıkmaktadır. Bu nedenle de bu suçla, özel hayatın gizliliđinin ihlalinden çok kişisel verilerin korunması hakkı korunmaktadır.

Diğer taraftan kişisel verilerin korunması, daha öncede değinildiği üzere, AİHS’de müstakil olarak yer almaması nedeniyle, sözleşmenin uygulamakla görevli olan AİHM tarafından, Sözleşmenin 8. Maddesinde düzenlenen özel hayatının gizliliği ve korunması hakkı kapsamında değerlendirilmektedir (Gözübüyük ve Gölcüklü, 2004: s. 331; Üzeltürk, 2004: s. 168-170; Şen, 1996: s. 70). Nitekim çoğu zaman kişinin başkaları tarafından bilinmeyen, hayatının özel ve gizli alanına ilişkin verilerin kaydedilmesi durumunda kişisel verilerin korunması hakkının yanında özel hayatın gizliliği hakkı da ihlal edilmektedir.

2.3. Suçun Unsurları

Dış dünyada değişiklik meydana getiren iradi insan davranışının ceza hukuku anlamında suç sayılması için mutlaka bulunması gereken unsurlara suçun unsurları denilmektedir. Diğer bir ifadeyle suçun unsurları denildiğinde tüm suçlar bakımından ortak olan ve bu unsurlardan herhangi birinin bulunmaması halinde fiilin suç sayılmasının mümkün olmadığı unsurlar anlaşılmaktadır (Artuk vd, Genel Hükümler, 2013: s. 198; Öztürk ve Erdem, 2012: s. 137 vd). Ancak suçun unsurların nelerden ibaret olduğu hususunda doktrinde görüş birliği bulunmamakla birlikte, hukukumuzda genellikle suçun dört unsurunun bulunduğu kabul edilmektedir. Bunlar; tipiklik, maddi unsurlar, manevi unsur ve hukuka aykırılık unsurlarıdır¹⁶². çalışmamızın konusunu oluşturan suçları bu unsurlar çerçevesinde inceleyeceğiz.

2.3.1. Tipiklik

Tipiklik, doktrinde “*suç sayılan fiilin ceza normundaki soyut tasviri*” olarak tanımlanmaktadır (Artuk vd, Genel Hükümler, 2013: s. 203). Bu nedenle, tipiklik unsuru için öncelikle, “*bir fiili suç sayan ve buna bir yaptırım öngörmüş bulunan bir kanun maddesinin var olması*” gerekmektedir (Hakeri, 2013: s. 125).

Tipiklik unsurunu belirlerken öncelikli olarak ilgili kanuna bakmak gerektiğinden, kişisel verilerin kaydedilmesi suçunun tipiklik unsurunu belirlemek için TCK’nın 135. maddesine bakmak gerekmektedir.

Maddenin birinci fıkrasında; “*hukuka aykırı olarak kişisel verileri kaydeden kimseye*” ceza verileceğinin düzenlendiği, ikinci fıkrasında ise; “*kişilerin siyasî,*

¹⁶² Suçun unsurları konusunda farklı gruplandırmalar için bkz.; Artuk/Gökçen/Yenidünya, Genel Hükümler, 2013: s. 201; Özgenç, Genel Hükümler, s. 158; Öztürk ve Erdem, 2012, s. 140.

*felsefî veya dinî görüşlerine, ırkî kökenlerine; hukuka aykırı olarak ahlâkî eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimsenin” cezalandırılacağı*nın düzenlendiği görülmektedir.

O halde birinci fıkradaki suçta suçun tipiklik unsuru yönünden, kişisel verilerin hukuka aykırı olarak kaydedilmesi aranmaktadır.

İkinci fıkradaki suçta ise kişilerin siyasî, felsefî veya dinî görüşlerine, ırkî kökenlerine ilişkin bilgilerin kişisel veri olarak kaydedilmesi ile kişilerin hukuka aykırı olarak ahlâkî eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgilerinin kişisel veri olarak kaydedilmesi aranmaktadır. İkinci fıkradaki suçun oluşabilmesi için sadece fıkra sayılan bilgilerin kaydedilmesi gerekmektedir. Sayılanlar dışındaki verilerin kaydedilmesi durumunda bu fıkra açısından fiil tipik sayılmayacaktır. Diğer taraftan kişilerin siyasî, felsefî veya dinî görüşlerine, ırkî kökenlerine ilişkin bilgilerin kişisel veri olarak kaydedilmesi suçunda hukuka aykırılık durumu aranmadığı için bu verilerin kaydedilmesi ile fiil tipik hale gelecek ve suç oluşacaktır.

Tipiklik unsuru suçun nitelikli halleri açısından da geçerli olup (Artuk vd, Genel Hükümler, 2013: s. 204), 137. maddede bu suç için uygulanacağı belirtilen ağırlaştırıcı nedenin uygulanabilmesi içinde fiilin tipik olması gerekmektedir.

2.3.2. Maddi Unsurlar

2.3.2.1. Suçun Konusu

Suçun konusu kişisel veridir (Özbek vd, 2013: s. 527; Yaşar vd, 2010: s. 4117; Parlar ve Hatipoğlu, 2008. S. 2043). Kişisel verinin ne olduğu veya bundan ne anlaşılması gerektiği konusunda madde metninde bir açıklık bulunmamaktadır. Bu yönüyle düzenleme, kanunilik ilkesinin bir gereği olarak açıklık ve belirlilik ilkelerine uygunluğu yönünden eleştirilmiştir (Şen, 2006. S. 601; Albayrak, 2013: s. 12). Doktrinde bazı yazarlar tarafından, kanun koyucunun bazı kavramları tanımlamayıp, içeriğinden ne anlaşılması gerektiğini öğreti ve uygulamaya bırakmasının doğal karşılanması gerektiği, suç tiplerinde değerlendirici unsurlara yer verilmesinin olağan olduğu, tipte yer alan unsurların ne anlama geldiğinin, kıyas yasağını ihlal etmeden, yorum yoluyla ortaya konabileceği de ileri sürülmüştür

(Özbek vd 2013: s. 527).

Bu görüşten hareketle mevzuatımızda kişisel verilere ilişkin düzenlemelere bakmak gerekmektedir.

Ülkemizin de imzaladığı Avrupa Konseyi'nin 108 nolu "Kişisel Nitelikteki Verilerin Otomatik İşleme Tâbi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme" nin 2 inci maddesinin birinci fıkrasının (a) bendinde kişisel veri, "*kimliği belirtilen veya belirtilebilen gerçek kişiyle ilgili tüm bilgiler*" olarak tanımlanmıştır (Handbook on European Data Protection Law , 2014: s. 36).

Avrupa Birliği'nin 95/46/EC sayılı Direktifinin 2. maddesinin birinci fıkrasının (a) bendinde kişisel veri, "*tanımlanan ya da tanımlanabilir gerçek kişiyle ilgili herhangi bir bilgi*" olarak tanımlanmıştır (Handbook on European Data Protection Law , 2014: s. 36).

Henüz kanunlaşmasa da çalışmaları devam eden Kişisel Verilerin Korunması Kanunu Tasarısında da benzer bir tanım yapılmıştır. Tasarıya göre kişisel veri, "*belirli veya kimliği belirlenebilir bir kişiye ilişkin bütün bilgilerdir*"¹⁶³ (m. 3).

Söz konusu Tasarısının gerekçesinde, "kişisel veriler; sadece bireyin adı, soyadı, doğum tarihi ve doğum yeri gibi onun kesin teşhisini sağlayan bilgiler değil, aynı zamanda kişinin aklı, psikolojik, fizikî, kültürel, ekonomik, sosyal ve sair özelliklerine ilişkin verilerdir. Bir kişinin belirli veya belirlenebilir olması, mevcut verilerin herhangi bir şekilde bir gerçek kişiyle ilişkilendirilmesi suretiyle, o kişinin tanımlanabilir hale getirilmesini ifade eder. Yani verilerin; kişinin fiziksel, ekonomik, kültürel, sosyal veya psikolojik kimliğini ifade eden somut bir içerik taşıması veya kimlik, vergi, sigorta numarası gibi herhangi bir kayıtla ilişkilendirilmesi sonucunda kişinin belirlenmesini sağlayan tüm halleri kapsar. İsim, telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler gibi veriler dolaylı da olsa kişiyi belirlenebilir kılabilmek özellikleri nedeniyle kişisel veridirler" biçiminde geniş bir şekilde açıklanmıştır¹⁶⁴.

¹⁶³ Bkz. <http://www.kgm.adalet.gov.tr/Tasariasamalari/Basbakanlik/Basbakanlik.html> Erişim T: 10.04.2014

¹⁶⁴ <http://www.kgm.adalet.gov.tr/Tasariasamalari/Basbakanlik/Basbakanlik.html> Erişim T: 10.04.2014

Doktrinde ise kişisel veri, “bireyin şahsi, mesleki ve ailevi özelliklerini gösteren, o bireyi diğer bireylerden ayıran ve niteliklerini ortaya koymaya elverişli her türlü bilgi” şeklinde tanımlanmıştır (Şen, 2006: s. 601).

Anayasa Mahkemesi de bir kararında kişisel veri kavramı ile ilgili tespitlerde bulunmuştur. Kararda¹⁶⁵:

“Kişisel veri kavramı, belirli veya kimliği belirlenebilir olmak şartıyla, bir kişiye ilişkin bütün bilgileri ifade etmektedir. Bu bağlamda adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil; telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri genetik bilgiler, IP adresi, e-posta adresi, hobiler, tercihler, etkileşimde bulunan kişiler, grup üyelikleri, aile bilgileri gibi kişiyi doğrudan ve dolaylı olarak belirlenebilir kılan tüm veriler kişisel veri kapsamındadır.” Şeklinde açıklanmıştır.

Yargıtay da bir kararında kişisel verinin tanımını yapmıştır. Kararda¹⁶⁶:
“suçun maddi konusunu oluşturan “kişisel veri” kavramından, kişinin, yetkisiz üçüncü kişilerin bilgisine sunmadığı, istediğinde başka kişilere açıklayarak ancak sınırlı bir çevre ile paylaştığı, herkes tarafından bilinmeyen ve/veya kolaylıkla ulaşılması ve bilinmesi mümkün olmayan, kişinin kimliğini belirleyen veya belirlenebilir kılan, kişiyi toplumda yer alan diğer bireylerden ayıran ve onun niteliklerini ortaya koymaya elverişli, gerçek kişiye ait her türlü bilginin anlaşılması gerektiği...”, belirtilmiştir.

Kişiyile ilgili tüm bilgiler kişisel veri olarak tanımlanmış olduğuna göre örneğin, kişinin adı, soyadı, ana-baba adı, vatandaşlık numarası gibi kimlik bilgileri, adresi, mesleği, sağlık bilgileri, banka hesap bilgileri, telefon numarası vb. pek çok bilgi kişisel veri sayılmalıdır.

Ceza Muhakemesi Kanunumuz da kişisel veriler açısından oldukça fazla hüküm içermektedir. Örneğin CMK’nın 75 ve 76. maddelerine göre “beden muayenesi ve/veya vücuttan örnek alınması suretiyle elde edilen veriler”, 78 ve 80.

¹⁶⁵ AYM’nin 2013/122 Esas, 2014/74 Karar ve 9.4.2014 tarihli kararı. bkz.

http://www.resmigazete.gov.tr/main.aspx?home=http://www.resmigazete.gov.tr/eskiler/2014/07/2014_0726.htm&main Erişim T: 01.08.2014

¹⁶⁶ Yargıtay 12. CD’nin Esas no: 2012/16872 Karar no: 2012/18221 sayılı kararı

maddeye göre yapılan “moleküler genetik incelemeler sonucu elde edilen veriler”, 81. Maddeye göre kaydedilen “kişinin fotoğrafı, beden ölçüleri, parmak ve avuç içi izi, bedeninde yer almış olup teşhisini kolaylaştıracak diğer özellikleri ile sesi ve görüntüleri” ile 135. maddeye göre kayda alınan “telekomünikasyon yoluyla yapılan iletişimin kayda alınması suretiyle elde edilen veriler” de kişisel veri olarak kabul edilmektedir (Özen, 2009: s. 15).

O halde 135. maddenin birinci fıkrasında düzenlenen suç bakımından gerçek kişiyle ilgili olan her türlü bilgi kişisel veri olarak kabul edilmelidir.

TCK’nın 135. maddesinin 2. fıkrasında tanımlanan suçun konusu ise; kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine, ahlaki eğilimlerine, cinsel yaşamlarına sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgilerdir (Parlar ve Hatipoğlu, 2008: s. 2043). Maddenin ikinci fıkrasında sayılan kişisel veriler, çalışmanın ilk kısmında tanımlar bölümünde de açıklandığı üzere, özel nitelikli (hassas) kişisel verilerden oldukları için ikinci fıkra da özellikle vurgulanarak gösterilmiştir (Yaşar vd, 2010: s. 4118).

Bir işverenin çalışanlarının sendika üyeliği kaydı, bir uçak yolcusunun dini inancına uygun yemek tercihinin gösteren bilgi; belirli bir kişi için tekerlekli sandalye erişiminin gerekli olduğunu belirten otel rezervasyon bilgisi; bir çalışanın apandisit ameliyatı için hastanede olduğunu gösteren kayıt; bir müşterinin striptiz kulüplerine gitmeyi sevdiğini açıklayan piyasa bilgisi; bir kişinin uyuşturucu madde bağımlısı olduğunu gösteren hastane kayıtları, bir kişinin kara para aklama suçunu işlediğini gösteren bilgiler hassas verilere örnek olarak gösterilebilir (Kaya, 2013: s. 322-323).

Bu verilerin ayrı bir fıkra da vurgulanarak düzenlenmesi yerinde olmakla birlikte, uygulanacak yaptırımın birinci fıkrayla aynı olması anlaşılabilir. Zira bu verilerin hukuka aykırı kaydedilmesi sonucunda oluşacak zarar ile basit bir telefon numarası veya adres bilgisinden oluşan kişisel verinin hukuka aykırı kaydedilmesi sonucu oluşan zarar farklı olacak; hassas verilerin işlenmesi nedeniyle kişi daha büyük zararlara maruz kalabilecektir. Kamuoyunda fişleme diye tabir edilen yasal olmayan bir şekilde kişilerin hassas verilerinin kaydedilmesi ile kişinin ayrımcılığa tabi tutulması, dışlanması, onurunun, şeref ve haysiyetinin zedelenmesi gibi çok büyük manevi zararların yanında kişi, işten atılmak veya fiziki saldırılara maruz kalabilmek gibi maddi zararlara da uğrayabilmektedir.

Diğer taraftan hemen belirtelim ki TCK m. 135/2'deki "*Kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykın olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimse, yukarıdaki fıkra hükmüne göre cezalandırılır*" şeklindeki düzenleme yerinde olmamıştır. Zira bu hüküm söz konusu "...bilgileri kişisel veri olarak kaydeden" ibaresine yer vermek suretiyle sanki bu verilerin kişisel veri olmadığı gibi bir anlam ortaya koymaktadır. Hâlbuki yukarıda yer alan tanımdan da anlaşılacağı üzere bu veriler de kişisel veridir. Hatta diğer verilere göre daha özel bir nitelik taşıdığı için kanımızca daha ağır cezayı gerektiren suçun nitelikli halleri arasında sayılması daha doğru olacaktır. Nitekim hem Kişisel Nitelikteki Verilerin Otomatik İşleme Tâbi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme hem de Kişisel Verilerin Korunması Kanunu Tasarısı söz konusu verileri *özel nitelikli veri* kategorisinde düzenlemiştir. Söz konusu Sözleşme'nin 6. maddesine göre "*iç hukukta uygun güvenceler sağlanmadıkça, ırk menşei, politik düşünceleri, dini veya diğer inançları ortaya koyan kişisel nitelikteki verilerle sağlık veya cinsel yaşamla ilgili kişisel nitelikteki veriler ve ceza mahkûmiyetleri, otomatik bilgi işlemine tâbi tutulamazlar.*" Yine Tasarının 7. Maddesinin birinci fıkrasında, "*Kişilerin ırk, siyasî düşünce, felsefi inanç, din, mezhep veya diğer inançları; demek, vakıf ve sendika üyeliği, sağlık ve özel yaşamları ve her türlü mahkûmiyetleri ile ilgili kişisel veriler işlenemez*" düzenlemesi getirilmiş ve söz konusu verilerin işlenmesinin özel hayatın ve aile hayatının gizliliğinin korunmasını sağlayacak yeterli önlemlerin alınması şartıyla belli koşullar altında işlenmesinin mümkün olabileceği açıkça ifade edilmiştir (Özbek vd, 2013: s. 528).

Bu açıklamalardan da anlaşılacağı gibi, maddede düzenlenen suçun konusuna, gerçek bir kişinin tanımlanması için kullanılabilecek her türlü bilgi dâhil edilmiştir. Bu nedenle, çok geniş bir alanı kapsamaktadır. Nerede ise, kişiyi diğer kişilerden ayıran tüm özellikler bu kapsamdadır (Yaşar vd, 2010: s. 4118).

O halde, kişilerin ırk, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançları, dernek, vakıf veya sendika üyeliği, sağlık veya özel yaşamları, her türlü mahkûmiyetleri, mezun olduğu okullar, kökenlerinin nereden geldiği, nereli oldukları, hangi yasal ve yasa dışı kurum kuruluş ve örgütleri destekledikleri,

hangilerine antipatiyle baktıkları, hangi takımı tuttıkları gibi tüm bilgiler bu kapsamda değerlendirilebilecektir.

Ancak, uygulamada bazı yazarlar tarafından, kişisel verinin bu kadar geniş şekilde tanımlanması, ceza hukukunda bir suçun kapsamının bu kadar geniş olmasının, önceden öngörülemeyen olumsuz sonuçlar doğurabileceği gerekçesiyle eleştirilmiş; Kişisel veri tanımının yapılmamasının, suçun konusunu oluşturan kişisel veri kavramının çok geniş yorumlanmasına ve suçta ve ceza kanunilik ilkesini ihlal edecek uygulamaların ortaya çıkmasına sebebiyet verebileceği, bu nedenle maddedeki suçun konusunu oluşturabilecek kişisel verilerin sadece kişinin özel hayatını ilgilendiren, kişinin başkalarının bilmesini istemediği kişisel bilgiler olması gerektiği öne sürülmüştür¹⁶⁷.

Kanaatimizce bu görüşe katılmak mümkün değildir. Zira Kanun da kişisel veriler ile ilgili bir sınırlama yapılmamıştır. Maddenin ikinci fıkrasında ise sınırlı şekilde sayılan hassas verilerin kişisel veri olara kaydedilmesi vurgulanmıştır. Bu konuda Anayasada da bir sınırlama olmadığına göre, her türlü kişisel verinin kaydı suç oluşturabilecektir. Burada failin kişisel verileri kaydetme amacına, daha doğrusu suçun işlenme amacına, kişinin rızası olup olmadığına ve diğer hukuka uygunluk nedenlerinin bulunup bulunmasına göre her somut olayda değerlendirme yapmak suretiyle belirleme yapılmalıdır.

Zira bu düşünceye göre kişinin adı veya telefon numarası gibi çoğu kişi tarafından bilinen verileri korumasız kalabilecektir. Örneğin, bu görüşe göre, kamuya açık yerlerde bina duvarlarına, umumi tuvaletlerin kapılarına veya internet üzerindeki sosyal paylaşım sitelerine kişilerin rızaları ve haberleri olmadan sırf kişileri zor durumda bırakmak için “*arkadaşlık için arayınız denilip kişinin adı soyadı ve telefon numarası yazıldığında*” bu eylem suç olmayacaktır. Veya suç olsada başka bir suç, örneğin hakaret suçu oluşabilecektir. Halbuki bu örneğe bakıldığında kişisel verilerin hukuka aykırı şekilde yayılması sözkonudur. Verinin

¹⁶⁷ **Yaşar/Gökcan/Artuç**, s. 4118; **Mahmutoğlu, Fatih Selami**, “Sır Saklama yükümlülüğü Kapsamında Hastaya Ait kişisel Verileri Hukuka Aykırı Olarak Verme veya Yayma Suçu”, cezahukuku.istanbul.edu.tr/ders-gerecleri/tiphukuku/sir-saklama.docx, E.T: 21.02.2012; **Albayrak**, 2013. s. 12, Diğer taraftan aynı yazarlar tarafından madde metninde kişisel verinin tanımının yapılmamasının faydalı yönünün, teknolojinin ve sosyal hayatın gelişmesi sonucu ortaya çıkan bilgilerin kanunlarda değişiklik yapılmadan kişisel veri kavramı içerisinde değerlendirilmesinin mümkün hale getirebilmesi olduğu, belirtilmiştir. Bkz. **Albayrak**, 2013: s. 12

basit veya birçok kiři tarafından bilinip bilinmemesi önemli deęildir. Kiři bazı kiřisel verilerini kendisi alenileřtirmiş te olabilir. Örneęin kiři, kendine ait internet sitesinde kimlik, adres ve telefon bilgilerini iletiřim amacıyla sitesine koymuş ve herkesin eriřimine açmış olabilir. Bu örnekte de kiřinin bu verilerinin sitesine girilerek kopyalanıp, müstehcen bir sitede arkadař arıyorum ve benzeri şekillerde yayınlanması durumunda da aynı řey söz konusudur. Bu nedenle veriler arasında bir tasnif yapmadan kiřiyle ilgili her türlü veri kiřisel veri olarak kabul edilmelidir.

Yine TCK'nun 135. maddesinin ikinci fıkrasında sayılan veriler arasında da bir ayırım yapılmış, “kiřilerin siyasi, felsefi veya dini görüşlerine, ırkı kökenlerine iliřkin bilgileri” *mutlak dokunulmaz* veriler olarak kabul edilirken; “ahlaki eğilimlerine, cinsel yaşamlarına, saęlık durumlarına veya sendikal baęlantılarına iliřkin bilgileri” *nisbi dokunulmaz* veriler olarak kabul edilmiştir. Dięer bir deyişle ilk grupta yer alan veriler hiçbir şekilde kaydedilemeyecektir. Buna karřılık, hükümde yer alan “hukuka aykırı olarak” ibaresi nedeniyle, ikinci grup verilerin kaydedilmesi mümkündür. Ancak bunun için mevzuatta, bu tür verilerin işlenmesine izin veren hükümler bulunmalıdır (Özbek vd, 2013: s. 529).

Öte yandan 135. maddeyle sadece gerçek kiřilere iliřkin veriler koruma altına alınmıştır. Bu nedenle maddedeki verilerin doğrudan gerçek bir kiřiye ait olan ve kiřinin üzerinde tek başına tasarrufta bulunabileceęi veriler olarak anlařılması gerekmektedir. Gerçekten bazı bilgiler, örneęin, bir anonim řirketin ticari sırları gibi, veri nitelięinde olmakla birlikte kiřisel olmaktan çok kurumsal olabilir. TCK'nun 239. maddesi ile ticarî sır, bankacılık sırrı veya müşteri sırrı ile fenni keřif ve buluřlar veya sınaî uygulamaya iliřkin bilgiler ayrı bir hükümde koruma altına alınmıştır. Bu nedenle ticarî sır, bankacılık sırrı veya müşteri sırrı nitelięindeki veriler ile fenni keřif ve buluřlar veya sınaî uygulamaya iliřkin bilgiler 135. madde ve devamındaki hükümlerde yer alan suçların konusunu oluřturmaz (Özbek vd, 2011: s. 518).

2.3.2.2. Fail ve Maędur

Hükümde “kimse” ibaresine yer verildięinden bu suçun faili herkes olabilir. Bu nedenle bu suç fail aęısından özellik arz etmemektedir. Ancak bu suçun, kamu görevlisi tarafından ve görevinin gerektirdięi yetki kötüye kullanılmak suretiyle veya

belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenmesi halinde, bu husus artırım nedenidir. Bu durumda, suçun faili kamu görevlisi olursa veya suçun işlenmesinde kolaylık sağlayacak belli bir meslek veya sanatı yapan kimse olursa, verilecek ceza, aynı Yasanın 137. maddesi uyarınca artırılacaktır (Özbek vd, 2013: s. 529; Yaşar vd, 2010: s. 4117; Hafizoğullar ve Özen, 2011: s. 276).

Bu suçun mağduru da herkes olabilir (Özbek vd, 2013: s. 529; Yaşar vd, 2010: s. 4117; Hafizoğullar ve Özen, 2011: s. 276). Mağdur açısından madde metninde özel bir düzenleme bulunmasa da burada mağdur açısından tereddütler olduğu bazı yazarlar tarafından dile getirilmiştir¹⁶⁸.

Suçun mağdurunun gerçek kişi ve/veya tüzel kişi mi olacağı konusunda oluşan bu tereddüt aslında kişisel verilerin korunması hukukunda konuya nasıl bakıldığı ve ceza hukukunda bu alanda hangi hukuki değerin korunduğu sorusunda yatmaktadır.

Çalışmamızın önceki bölümlerinde de açıklandığı üzere, kişisel verilerin korunması alanında ilk düzenlemelerin yapıldığı Kıta Avrupasında konu, kişinin temel kişilik hakları ve kişinin bilgilerinin mahremiyeti kapsamında ele alınmıştır. Nitekim bu konuda Avrupa Konseyi tarafından hazırlanan 1981 tarihli ve 108 nolu Sözleşmede, gerçek kişilerin verilerinin korunması konusunda devletlere yükümlülükler verilmiştir. Sözleşmenin amacı bu konuda aydınlatıcıdır. Sözleşmenin amacı 1. maddede, *“Bu Sözleşmenin amacı her Akit Devlet ülkesinde, uyruğu veya ikametgahı ne olursa olsun tüm gerçek kişilerin, temel hak ve özgürlüklerini ve özellikle kendilerini ilgilendiren kişisel nitelikteki verilerin, otomatik bilgi işleme tabi tutulması karşısında özel yaşam haklarını güvence altına almaktır”*. Şeklinde belirtilmiştir. Ancak akit devletlerin, koruma alanını genişletip tüzel kişileri de bu kapsama dâhil edebilecekleri de ayrıca belirtilmiştir (m. 3/2-b). AB tarafından hazırlanan 95/46/EC sayılı Direktifte aynı yönde olup, Direktifin amacı, *“Üye Devletler, bu direktife uyumlu olarak, kişisel verilerin işlemesine saygı çerçevesinde gerçek kişilerin temel hak ve özgürlüklerini ve özellikle onların mahremiyet haklarını*

¹⁶⁸ Bazı yazarlarca, mağdurun gerçek kişi ve/veya tüzel kişi mi olacağı konusunda madde metninde açıklık bulunmadığı, bu nedenle suçun mağduru açısından belirsizlik olduğu ileri sürülmüştür. Bkz. **Işık, Dilan**, “Kişisel Verilerin Kaydedilmesi Suçu”, Suç ve Ceza- Ceza Hukuku Dergisi, S. 4, Ekim Kasım Aralık 2010, s. 175

koruyacaklardır.” Şeklinde belirtilmiştir (m. 1).

5237 sayılı TCK’ya da bakıldığında, kişisel verilere karşı işlenen suçlar, TCK’nın “Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar” başlıklı Dokuzuncu Bölümünde düzenlenmiştir. Bu bölümde kişinin temel haklarından özel hayatın gizliliği hakkının ihal eden eylemler düzenlenmiş olup, bu bölüm gerçek kişilere yönelik suçları hüküm altına alınmıştır. 135. maddenin gerekçesine bakıldığında da, maddeyle AK’nin 108 nolu Sözleşmesine uygun olarak düzenleme yapıldığı belirtilmiş, ayrıca madde gerekçesinde kişisel veri, “gerçek kişiyle ilgili her türlü bilgi” olarak tanımlanmıştır. Bu da maddeyle gerçek kişilerin kişisel verilerinin korunduğu anlamına gelmektedir.

Bu nedenlerle, TCK’daki mevcut düzenleme itibariyle bu suçun mağduru gerçek kişilerdir. Bu bakımdan herhangi bir gerçek kişi bu suçun mağduru olabilmektedir.

Tüzel kişiler ise bu suçun faili ve mağduru olamazlar. Ancak, eylem bir tüzel kişinin faaliyeti kapsamında ve tüzel kişinin yararına olarak işlenmişse TCK’nın 140. maddesindeki şartlar doğrultusunda, tüzel kişilik hakkında güvenlik tedbiri uygulanabilecektir.

2.3.2.3. Hareket ve Netice

Kişisel verilerin kaydedilmesi suçunun hareket unsuru, “kişisel verileri kaydetmek” tir (Özen, 2009: s. 15). Ancak bu suçun oluşması için, kişisel verilerin hukuka aykırı biçiminde kaydedilmesi gerekmektedir.

Nitekim Yargıtay’da 11.09.2012 tarihinde verdiği bir kararında¹⁶⁹; “5237 sayılı TCK’nın 135. maddesinde düzenlenen kişisel verilerin kaydedilmesi suçunun oluşabilmesi için, belirli veya belirlenebilir bir kişiye ait her türlü bilginin, hukuka aykırı olarak kaydedilmesi gerekmekte olup...” şeklinde karar vererek bu hususu teyit etmiştir.

Maddede düzenlenen suç iki fıkra halinde düzenlenmiş olup, hareket unsuru açısından fıkralar arasında terim birliği bulunmadığından her iki fıkrayı arasındaki bağlantı veya uyumu belirlemek için ayrı incelemek gerekmektedir.

¹⁶⁹ Yargıtay 12. CD’nin Esas no: 2012/16872 Karar no: 2012/18221 sayılı kararı

Birinci fıkrada “*kişisel verilerin kaydedilmesi*” ifadesine yer verilmişken ikinci fıkrada sınırlı şekilde sayılan bazı verilerin “*kişisel veri olarak kaydedilmesi*” ibarelerine yer verilmiştir. Diğer bir ifadeyle birinci fıkrada tüm kişisel verilerin kaydedilmesi düzenlenmişken, ikinci fıkrada bazı verilerin kişisel veri olarak kaydedilmesi düzenlenmiştir.

Bazı yazarlar tarafından her iki eylemin farklı anlamlar içerdiği savunulmuş ise de¹⁷⁰, kanaatimizce, bura da suçun hareket unsuru “*kaydetmektir*”. Kanun koyucu ikinci fıkrada özel nitelikli verilerin daha sıkı korunduğunu vurgulamak amacıyla böyle bir ifade kullanmıştır. Esas itibarıyla her iki hareketin neticesi de aynıdır. Bu açıdan bu ayrımın pratikte bir faydası bulunmamaktadır.

Ancak ikinci fıkra metninin daha düzgün şekilde kaleme alınmasında fayda vardır. Zira kişilerin felsefi veya dini inançlarına ilişkin bilgiler de kişisel veridir. Bu nedenle fıkra metni “*kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgilerin kaydedilmesi halinde....*” şeklinde yazılmasının daha uygun olacağını değerlendirmekteyiz.

Kişisel verilerin kaydından anlaşılması gereken ise, onları tekrar ve başkaları tarafından gerektiğinde kullanılabilecek durumda hazır etmektir. Kaydetmek, verileri kâğıt ve benzeri şeyler üzerine yazmak, çizmek, işaretlemek biçiminde olabileceği gibi, ses bantlarına, CD'lere, ya da bilgisayar veya harddisk gibi dijital ortama almak biçiminde de olabilir. Nitekim bu husus madde gerekçesinde, “*kişisel verilerin bilgisayar ortamında veya kâğıt üzerinde kaydedilmesi arasında bir ayrım gözetilmemiştir*” şeklinde açıklanmıştır. Ancak, veri kaydetmenin gerçekleşmesi için, mutlaka bir yere bilgilerin yazılması, depolanması, saklanması veya şerh

¹⁷⁰ **Hafizoğulları/Özen**, konuya farklı bir bakış açısı getirmiştir. Yazarlara göre, “TCK’nın 135. Maddesinin birinci fıkrasında “kişisel verileri kaydetmek” fiili suç sayılmakta, ikinci fıkrada, kişinin bazı niteliklerine ilişkin bilgileri “kişisel veri olarak kaydetmek” fiili suç sayılmaktadır. Böyle olunca, Kanun, aynı maddede, belirtilen yönleri farklı, ancak diğer yönleri aynı olan farklı iki suça yer vermiş olmaktadır. Maddedeki tanımlar karşısında, kişisel verileri kaydetmek başka şeydir, bazı kişisel bilgileri, kişisel veri olarak kaydetmek başka şeydir”. Bkz. **Hafizoğulları/Özen**, 2011: s. 276-277. Ancak suçun konusu başlığı altında da açıklandığı üzere, burada iki ayrı suç olmayıp, bazı özel nitelikli/hassas veriler için vurgu yapılmak istenmesinden dolayı bir ayrım yapılmıştır. Burada bir ayrım yapılacaksa konu itibarıyla bir ayrım yapmanın daha doğru olacağı, zira kişisel verileri kaydetme eylemi ile bazı özel nitelikli verileri kişisel veri olarak kaydetme eylemlerinin özünde aynı şey olduğunu düşünmekteyiz.

düşülmesi gerekir¹⁷¹. Bu kapsamda bir kimsenin kişisel verileri, okumak ya da dinlemek suretiyle hafızasına alması ya da daha sonra kullanmak üzere ezberlemesi durumu, buradaki kaydetme olarak kabul edilmemektedir (Malkoç, 2013: s. 912; Yaşar vd, 2010: s. 4120; Özbek vd, 2013: s. 530).

Bir bilişim sisteminde kayıtlı olmayan ya da yazılı olarak bulunmayan bir kişisel verinin sisteme girilmesi veya yazılı hale getirilmesi veya aslında başka bir kayıtta hukuka uygun olarak bulunan bir verinin bir sisteme ya da kişisel dosyaya hukuka aykırı olarak girilmesi de kaydetme olarak kabul edilmektedir (Dülger, 2004: s. 271; Şener, 2011: s. 77).

Kişisel verilerin korunmasına ilişkin hukuksal düzenlemelerin kabulünde bilgisayar ve diğer bilişim sistemlerindeki gelişmeler etki etmişse de hukuksal açıdan kâğıt üzerindeki veriler ile elektronik ortamda yer alan veriler arasında bir ayrım bulunmamaktadır. Bu nedenle maddede bu konuda bir ayrım yapılmaması yerinde olmuştur. Buna göre suçun oluşabilmesi için verilerin sistemli olarak kayıt edilmesi, bu kayıtların bilişim sistemlerinde tutulması gibi koşullar aranmamaktadır. Suçun, kişisel verilerin herhangi bir şekilde kayıt edilmesi ile gerçekleşmesi olanaklıdır. Ayrıca suçun oluşması için kişisel verilerin yayınlanması, başkasının kullanımına açılması ya da bir zararın oluşması gerekmez. Suçun gerçekleşmesi için kayıt etme işleminin gerçekleşmesi yeterlidir (Dülger, 2004: s. 269; Küzeci, 2010: s. 290; Ketizmen, 2008: s. 233).

Öte yandan kişisel verinin hukuka aykırı olarak hangi araç gereçle kaydedilmiş olduğu da önemsizdir. Bu kapsamda kişisel veriler kamera, bilgisayar gibi elektronik ya da manyetik cihazlarla kayıt edilebileceği gibi, kalem benzeri fiziki aletlerle de kaydedilebilir. Bu nedenle verileri bir kâğıda kalemle yazıp muhafaza etmek te bir nevi kayıt sayılmaktadır.

Kişilerin sağlık bilgilerinin hastanelerce kaydedilmesi, kişilerin ekonomik, sosyal ve sair özelliklerine ilişkin bilgilerin emniyet birimleri tarafından kaydedilmesi, kişilerin özgeçmişlerinin ve görüntülerinin istihbarat birimlerince

¹⁷¹ Yaşar/Gökcan/Artuç, s. 4120; Hafizoğulları/Özen, s. 277; Parlar/Hatipoğlu, 2008, s. 2044; Özen, s. 16; Işık, s. 175; Diğer yandan Özbek, “kâğıt üzerine yazmayı” kaydetme olarak kabul etmemiş, kaydetmenin mutlaka elektronik ya da manyetik bir araç ile yapılması gerektiğini ileri sürmüştür. Bkz. Özbek ve Diğerleri, Özel Hükümler, 2013, s. 530

kaydedilmesi, kişinin kimlik ve adres bilgileri ile teflon bilgilerinin GSM şirketleri tarafından şirketin sistemine kaydedilmesi, genetik bilgilerinin Sağlık Bakanlığı tarafından kaydedilmesi veya kolluk birimleri tarafından önceden hakkında soruşturma yapılan kimselerle ilgili GBT kayıtlarının tutulması hususları, kaydetme eylemine örnek olarak verilebilir. Ancak bu eylemlerin suç olarak kabul edilebilmesi için ilerde açıklanacağı üzere hukuka aykırı olarak yapılması gerekmektedir.

Kayıt etme eylemi, icra hareketi olduğundan, bu suç ihmal hareketi ile işlenemez. Suç, neticesiz yani sırf hareket suçu şeklinde düzenlenmiştir. Bu çerçevede suç neticesi harekete bitişik olduğundan kişisel verilerin hukuka aykırı olarak kaydedilmesi ile tamamlanır (Hafizoğulları ve Özen, 2011: s. 277; Özbek vd, 2013: s. 530). Bu nedenle, suçun oluşması için, verileri kaydedilen kimsenin, herhangi bir zarara uğraması zorunlu değildir. Kişisel verinin kaydedilmesiyle suç oluşacaktır (Parlar ve Hatipoğlu, 2008: s. 2044; Yaşar vd, 2010: s. 4120).

Maddenin ikinci fıkrasındaki suçta, kişilerin siyasî, felsefî veya dinî görüşlerine, ırkî kökenlerine; hukuka aykırı olarak ahlâkî eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydetmenin cezalandırılacağı belirtildiğinden, bu suç, bağlı hareketli bir suçtur. Suç, sadece maddede sayılanlarla sınırlıdır. Sayılanların dışında kalan şeylere ilişkin bilgilerin kişisel veri olarak kaydedilmesi, halinde ikinci fıkradaki suç oluşmaz. Bu yönüyle de suç aynı konuyu düzenleyen 135. maddenin birinci fıkrası, 136. madde ve 138. maddelerden ayrılır (Hafizoğulları ve Özen, 2011: s. 277; Özbek vd, 2013: s. 530).

Kanımızca kanunilik ilkesinin bir sonucu olarak kaydetmekten ne anlaşılacağına ilişkin olarak suç tipinde ayrı bir düzenlemeye yer verilmelidir (Özbek vd, 2013: s. 530). Nitekim bazı yazarlar, bu suçun bir tür “*veri hırsızlığı*” olarak ta nitelendirilebileceğini öne sürmüşlerdir (Özbek vd, 2013: s. 530). Ancak bu suçtan ziyade 136. maddede düzenlenen “verileri hukuka aykırı olarak ele geçirme” suçu veri hırsızlığı nitelemesine daha çok uymaktadır.

135. maddenin ikinci fıkrasında tanımlanan suçun maddi unsuru, kişilerin siyasî, felsefî veya dinî görüşlerine, ırkî kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgilerin kişisel veri olarak kaydedilmesidir.

Kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine ilişkin bilgilerin kişisel veri olarak kaydedilmesi, vatandaşlar arasında bu sayılan etmenlere dayanan grup mensubiyeti nedeniyle ayrımlar yapılması yürürlükteki ulusal kanun ve kurallar ile uluslararası düzenlemelerin izin vermediği bir durum olduğundan, bu tür bilgilerin kişisel veri olarak kaydedilmesi başlı başına hukuka aykırılık içeriği taşımaktadır. Kanun koyucu, bu düzenleme ile aslında bireyler arasında bölücülük yapılmasını önlemek ve özel hayatın gizliliği ve korunması ve hassas nitelikteki verilerin korunması hakkına güvence sağlamak amacını gütmüştür (Parlar ve Hatipoğlu, 2008: s. 2044). Bu verilerin devlet tarafından işlenmek istenmesi ile özel sektör tarafından işlenmesi halleri için kanunda bir ayırım yapılmadığı için, her halde bu verilerin kişisel veri olarak kaydedilmesi suç oluşturacaktır.

Uygulama açısından bakıldığında da bir kamu görevi gereği veya istihbarat veya kolluk birimleri tarafından bir suçun işlenmesini önlemek amacıyla veri işlemek gerektiğinde, kişilerin dini görüşlerine veya ırki kökenlerine ilişkin bilgilerin toplanmasının ne faydası olacağı düşünüldüğünde; esasında bu bilgilerin toplanması ile suçun önlenmesi, ülke güvenliğinin sağlanması arasında bir bağlantı kurulamamaktadır. Zira öteden beri bilindiği üzere bir kısım terör örgütleri sağ görüşe, bir kısım terör örgütleri sol görüşe sahip, bir kısım terör örgütleri ise herhangi bir görüşe veya inanca sahip değildirler. Onların bu yönlerinin bilinmesine rağmen, ancak eylem ve yapılarına ilişkin bilgiler elde edilerek önlem alınabilmektedir. Bu nedenle ikinci fıkradaki (kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine ilişkin) hassas nitelikteki verilere mutlak dokunulmazlık verilmesi faydalı bir düzenleme olmuştur.

Bu suçun oluşması için, kişisel verilerin kaydedilmesi yeterlidir. Ayrıca, bu kişisel verilerin kullanılması veya bu verilerden bir fayda sağlanması zorunlu değildir (Yaşar vd, 2010: s. 4120).

Yine bu suç neticesi bakımından ani bir suç olduğu için kaydedilme ile tamamlanır. Bunun için belli bir süre geçmiş olması, kişisel verinin belli bir süre kayıtlı bulunması aranmamıştır. Bu yönüyle suç mütemadi bir nitelik taşımaz.

Suçun tamamlanmış sayılması için fiil nedeniyle herhangi bir zarar bir zarar

doğması da da aranmadığından suç bir tehlike suçudur¹⁷². Hatta suç tipinde hareket ile tehlike neticesi arasında bir nedensel ilişkinin varlığını araştırmak yönünde zorunluluk bulunduğu ilişkin ifade yer almaması, diğer bir deyişle suç tipinde hareketin bir tehlike yaratabilecek nitelikte olması gerektiğine ilişkin düzenlemenin yer almaması nedeniyle de suç, soyut tehlike suçu olarak kabul edilmektedir (Özbek vd, 203: s. 530).

Doktrinde, TCK' nun 135. maddesinde yalnızca verilerin işlenmesinin bir türü olan kayıt etmenin suç olarak belirlenmesi bir eksiklik olarak ifade edilmiştir. Bu görüşü savunan yazarlara göre, “kişisel verilerin işlenmesi yalnızca kayıt etmeyi değil, toplanma, kullanılma, aktarılma gibi çeşitli eylemleri içeren bir süreçtir. Anayasanın 20. maddesinin üçüncü fıkrasında da “verilerin işlenmesinden” bahsedilmektedir. TCK' nun aşağıda incelenecek hükümlerinde (m. 136 ve 138) bu eylemlerin bir kısmına ilişkin düzenlemeler bulunmaktadır. Ancak özellikle kişisel verilerin hukuka aykırı olarak kullanılmasına ilişkin düzenlemeye yasada yer verilmediği görülmektedir. Bu durumda hukuka uygun şekilde toplanan ve kayıt altına alınan kişisel verilerin sonraki kullanımlarında oluşabilecek aykırılıkların yaptırımsız kaldığı sonucu çıkmaktadır. Bu durum, amaçla bağlılık ilkesi ile uyumlu değildir. Nitekim bu ilkenin meşru olmayan ikincil ve daha sonraki işlemleri sınırlandırmaya yönelik işlevi TCK'nın 135. maddesinde dikkate alınmamıştır (Küzeci, 2010: s. 290; Ketizmen, 2008; s. 233; Keklik, 2012: s. 305)”.

Bu görüş, bir veriyi kaydetmeden veya ele geçirilmeden kullanmak mümkün gözükmediğinden eleştirilebilir ancak bu durumda konu teknolojinin öngörülemezliğine takılmaktadır. Zira verileri kaydetmeden kullanmak bugünkü veya yarınki teknolojik imkanlar neticesinde yapılabilir mi? Bu soruyu teorik olarak cevaplandırabilmek pek mümkün gözükmemektedir. Bunun için somut olayda

¹⁷²Suç ile korunan hukuki yarar açısından ya bir zarar meydana getirilir veya bir zarar tehlikesi oluşturulur. Somut bir zarar var ise artık ortada bir zarar suçu var demektir. Eğer bir zarar tehlikesi söz konusu ise ve kanun koyucu bu tehlikeyi suç olarak düzenlemişse söz konusu suça tehlike suçu adı verilir. Dolayısıyla fiilin suçun koruduğu hukuki yarar üzerinde gösterdiği etkiye göre suçları tehlike suçları ve zarar suçları olarak ayırmak mümkündür. Suçun oluşması için zarar meydana gelmesinin arandığı suçlara zarar suçu, zarar meydana gelmesinin aranmadığı, sadece zarar tehlikesinin oluşmasıyla yetinilen suçlara ise tehlike suçları denilmektedir. Tehlike suçlarında bir zararın meydana gelmesi aranmamakta, zarar tehlikesinin oluşması yeterli olmaktadır. Tehlike suçları hakkında ayrıntılı bilgi için bkz. **Polat, Halil**, “Genel Güvenliğin Tehlikeye Sokma Suçu ile Bu Suçun Diğer Suçlarla İctimai”, TAAD, S. 1, Nisan 2010

hem hukuki hemde teknik deęerlendirme yapmak gerekmektedir.

2.3.3. Manevi Unsur

Bu suç genel kastla işlenebilir. Kast, suçun kanuni tanımındaki unsurların bilerek ve isteyerek gerçekleştirilmesidir (TCK m. 21/1, Koca ve Üzülmöz, 2013: s. 144). Diğer bir deyişle, suçun kanuni tanımındaki bütün unsurlar fail tarafından bilinmedikçe kasten işlenen bir suçtan bahsedilemeyecektir. Bu suç açısından ise failin, mağdurun kişisel verilerini kaydedecek nitelikteki davranışları bilerek ve isteyerek yapması suçun oluşması için yeterlidir. Saik önemli değildir. Suçun taksirle işlenebilen hali de TCK’da düzenlenmediğinden bu suç, taksirle işlenemez Hafızoğulları ve Özen, 2011: s. 278; Parlar ve Hatipoğlu, 2008: s. 2045; Şen, 2006: s. 607). Dolayısıyla fail, kişisel verileri taksirli hareketiyle kaydederse sorumlu olamayacaktır (Dülger, 2004: s. 274).

Nitekim Yargıtay da bir kararında¹⁷³; “*sanığın, hastane veri sistemine giriş yapıp, katılanın 27.04.2004-06.09.2004 tarihleri arasında Aydın Devlet Hastanesi Psikiyatri Polikliniğine başvuruda bulunduğuna ilişkin bilgileri kaydederek, elde ettiği katılanın kimlik bilgileri, hangi polikliniğe başvurduğu, muayene olacağı hekim ismi ve sıra numarasını gösteren 8 adet hastahane müracaat belge örneklerini, katılana hakaret ettiği iddiasıyla görülmekte olan davanın 17.09.2007 tarihli oturumunda, iddiasına ispat olarak sunması şeklinde gelişen olayda, yapılan yargılama sonucunda, sanığa yüklenen suçun yasal unsurlarının oluşmadığı gerekçeleri gösterilerek mahkemece kabul ve takdir kılınmış olduğundan...*” şeklinde belirtmek suretiyle sanığını suç kastıyla hareket etmediğinden suçun oluşmayacağına karar vermiştir.

Genel kastla işlenebilen suçun kural olarak olası kastla işlenmesi de mümkündür. Bu nedenle bazı yazarlar, kişisel verilerin kaydedilmesi suçunun olası kastla da işlenebileceğini savunmuşlardır (Özbek vd, 2013: s. 537). Olası kast, failin neticeyi öngörmesi ancak meydana gelmesi konusunda kayıtsız kalması; meydana gelememesi için çaba sarf etmemesi, neticeyi göze almasıdır (Özgenç, 2013: s. 237-246; Artuk vd, Genel Hükümler, 2013: s. 300-307; İçel, 2007: s. 65). Ancak madde metninde hukuka aykırılık ibaresine yer verilmesi nedeniyle failin suçu işleyebilmesi

¹⁷³ Yargıtay 12. CD’nin Esas No: 2011/23504 Karar No: 2012/14795

için verileri kaydetmesinin hukuka aykırı olduğunu bildiği halde verileri kaydetmesi gerektiğinden, bu suçun her iki fıkrasının da doğrudan kastla işlenebileceğini, olası kastla işlenmeyeceğini düşünmekteyiz (özen, 2009: s. 6).

2.3.4. Hukuka Aykırılık Unsuru

2.3.4.1. Genel Olarak

Suçun bir diğer unsuru da, hukuka aykırılıktır. Hukuka aykırılık, “*kanundaki tarife uygun bulunan fiile hukuk düzenince cevaz verilmemesi, fiilin yalnız ceza hukuku ile değil, bütün hukuk düzeni ile çelişki ve çatışma halinde bulunması*” demektir (Artuk vd, Genel Hükümler, 2013: s. 369; Alacakaptan, 1975: s. 95). Bu unsurun gerçekleşebilmesi için, aşağıdaki iki koşulun bir arada bulunması zorunludur (Alacakaptan, 1975: s. 96):

- 1) Fiil, ceza kanunlarında yer alan tanıma uygun olmalıdır.
- 2) Bu hareketin yapılması, başka bir hukuk dalına ait bir kural tarafından uygun görülmüş ya da emredilmiş olmamalıdır.

Diğer taraftan Ceza Kanununun suç saydığı bir fiilin işlenmesine diğer bir hukuk kuralı izin veriyorsa, o fiilin hukuk düzeni tarafından yasaklanmadığı, yani suç olmadığı sonucuna varılır. Bu şekilde ceza normunun yasakladığı bir fiilin işlenmesine izin vererek, onun hukuka aykırı olmasını önleyen kurala da “hukuka uygunluk sebebi” denmektedir (Artuk vd, Genel Hükümler, 2013: s. 370).

Hukuka uygunluk sebepleri, hukuka aykırılığı ortadan kaldırıp fiili hukukun meşru saydığı bir hareket haline getirirler. Örneğin, herhangi bir suç işleyen kişinin mahkemece hapis cezasına çarptırılması ve kesinleşmiş hükme ve cezanın infazını düzenleyen kurallara uygun olarak hapis cezasını infazının gerçekleşmesi nedeniyle, infazda görevli kişilerin, kişiyi hürriyetinden yoksun kılma fiillerinin hukuka aykırı bulunması ve suç olarak nitelendirilmesi mümkün değildir. Ayrıca, hukuka uygunluk sebepleri, hukuka aykırılık unsuru gerçekleştikten yani fiil hukuka aykırı bir şekilde işlendikten sonra etki yaparak hukuka aykırılığı ortadan kaldırmaz. Aksine fiilin doğrudan doğruya hukuka uygun bir biçimde ortaya çıkmasını sağlar (Artuk vd, Genel Hükümler, 2013: s. 370).

5237 sayılı TCK’da hukuka uygunluk sebepleri, “Ceza Sorumluluğunu Kaldıran ve Azaltan Nedenler” başlıklı İkinci Bölümde, “Kusurluluğu ortadan

kaldıran ve azaltan sebepler” ile birlikte düzenlenmiştir. Buna göre TCK’da; kanun hükmünü yerine, bir başka deyişle görevin ifası (TCK. m.24/1), meşru savunma (TCK. m.25/1), hakkın icrası (TCK. m.26/1) ve ilgilinin rızası (TCK. m.26/2) yer hukuka uygunluk nedeni olarak yer almaktadır.

Diğer yandan, kural olarak hukuka aykırılık, tipikliğin maddi bir unsuru değil, suçun genel bir unsurudur. Ancak bazı suç tiplerinde, “hukuka aykırı olarak”, “hukuka aykırı başka bir davranışla” veya “hukuka aykırı yolla” gibi ifadelerle ayrıca yer verilmiştir. Bu durumlarda, hukuka aykırılık tipikliğe ait bir unsur özelliği kazanmakta, ilgili suç tipinde fiilin hukuka aykırılığına özellikle işaret edilmektedir. Örneğin kişiyi hürriyetinden yoksun kılma suçunun düzenlendiği TCK.’nun 109 uncu maddesinde; *"bir kimseyi hukuka aykırı olarak bir yere gitmek veya bir yerde kalmak hürriyetinden yoksun bırakan kişiye, bir yıldan beş yıla kadar hapis cezası verilir"* denilmiştir. Aynı şekilde TCK.’nun 135/1 nci maddesinde; *"kişisel verileri hukuka aykırı olarak kaydeden kimse, ... cezalandırılır"* denilmiştir. Bu suç bakımından da failin diğer hususlara ilaveten ayrıca kişisel verileri hukuka aykırı olarak kaydettiğini bilmesi gerekmektedir.

Hukuka özel aykırılık olarak da adlandırılan bu durumlarda fiilin tipe uygun olması, hukuka da aykırı olduğu anlamına gelmemektedir. Bu hallerde hâkim fiilin hukuka aykırı olduğunu ayrıca belirlemek zorundadır. Bu suçlarda failin kusuru hukuka aykırılığı da kapsmalıdır. Yani failin tipte yer alan diğer unsurlar yanında yine tipte özellikle ve ayrıca belirtilmiş bulunan hukuka aykırılık unsurunu da biliyor ve istiyor olması gerekir (Özbek vd, 2013: s. 534).

Hukuka aykırılığın suç tipinde ayrıca belirtilmesi, esasında o tipte yer alan fiilin hukuka uygun da olabileceğini ifade etmek içindir. Gerçekten suç oluşturan fiil, hukuk düzeninin birliği ilkesinin bir sonucu olarak, hukukun tamamı bakımından hukuka aykırı olmalıdır. Ancak bazı fiiller hukukun değişik dallarındaki düzenlemeler nedeniyle hukuka uygun olabilir. Ancak bu tür fiillerin söz konusu düzenlemelere aykırı olarak işlenmesi durumunda suç olarak cezalandırılması gerekebilir. İşte bu hallerde yasakoyucu o fiili suç haline getirmek için “hukuka aykırı olarak” şeklinde bir ifadeye suç tipinde yer vermek zorundadır. Bu durumda aslında tipte yer alan fiil mevzuata uygun ise hukuka aykırı olmamaktadır. Tipte cezalandırılan, mevzuata aykırı olan fiildir (Özbek vd, 2013: s. 534).

TCK’da yer alan suçların önemli bir kısmı bakımından böyle bir ibareye gerek bulunmamaktadır. Zira örneğin, kasten öldürme, hırsızlık, dolandırıcılık, cinsel saldırı gibi suç tiplerinin bir hukuk kuralı ile hukuka uygun hale getirilmesi mümkün değildir. Bir başka deyişle bu suçları oluşturan eylemler doğası gereği hukuka aykırıdır. Ancak örneğin, kişisel verinin ne şekilde kaydedilebileceğinin koşulları bir hukuk kuralı ile belirlenmiş ise buna uygun olduğu sürece söz konusu fiil cezalandırılmaz. Bu nedenle TCK’da bazı suçlar için “hukuka aykırı olarak” ibaresine yer verilmesi gerekmektedir (Özbek vd, 2013: s. 534).

Bu kapsamda örneğin, adli sicil kayıtlarının, mahkûmiyetlerin Adalet Bakanlığınca kaydedilmesi, 5352 sayılı Adli Sicil Kanunu gereğidir. Ayrıca parmak izi ve fotoğrafların kayda alınması hususu da 2559 sayılı Polis Vazife ve Salahiyat Kanunun 5. Maddesinin verdiği yetkiye dayanılarak yapılmaktadır. Bu Kanunlara uygun olarak mahkûmiyetlerin kaydedilmesi veya parmak izlerinin ve fotoğraflarının arşivlenmesi hukuka aykırı sayılmayacaktır. Ancak, kanaatimizce kişisel verinin kaydedilmesinin hukuka uygun sayılabilmesi için, bu konuda yetkili makama kanun tarafından verilmiş açık bir yetkinin olması gerekir. Kanun tarafından verilmiş açık bir yetki olmadan kişisel verileri kaydetmek, TCK’nın 135. maddesinde düzenlenen suç oluşturacaktır (Yaşar vd, 2010: s. 4118-4119).

O halde kişisel veri hukuka aykırı olarak kaydedilmediği sürece suç oluşturmaz. Somut olayda hâkim mevzuatta buna imkân veren düzenlemelerin mevcut olup olmadığını araştırmak zorundadır (Özbek vd, 2013: s. 535).

Burada dikkat çekilmesi gereken husus, kanun koyucunun hükmün birinci fıkrasında ve ikinci fıkranın belirtilen bölümünde suçun oluşabilmesi için kaydın “hukuka aykırı” olarak yapılmasını ararken “kişilerin siyasi, felsefî veya dini görüşlerine, ırki kökenlerine” ilişkin bilgilerin kayıt edilmesi açısından bu ibareye yer vermemiş olmasıdır. Bu ibare doktrinde tartışma konusu olmuş ve farklı görüşler ileri sürülmüştür¹⁷⁴.

¹⁷⁴ Hafizoğulları/Özen, bu konuyu şu şekilde değerlendirmiştir: *"Kişilerin siyasi, felsefî veya dini görüşlerine, ırki kökenlerine ilişkin bilgilerin kişisel veri olarak kayıtlı edilmesi söz konusu olduğunda, Kanunun "hukuka aykırı olarak" hükmüne yer vermediği gözlenmektedir. İfadeden, bu bilgilerin kişisel veri olarak kaydedilmesinin, her zaman, mutlak olarak, hukuka aykırı olduğu sonucu çıkmaktadır. Kanunun, hem maddenin birinci fıkrası hükmünde, hem ikinci fıkrasında diğer durumlar için hukuka aykırı olmak hükmüne yer vermişken, bu hali, onlardan niçin ayırık tuttuğu, anlaşılamamaktadır.*

Bir kısım yazarlara göre, maddenin 2. fıkrasında suçun konusu olan veriler sınırlı sayıda düzenlenmiş; bunlardan bir kısmının hukuka aykırı olarak kaydedilmesi özellikle vurgulanmış, diğer kısmı için böyle bir vurgu yapılmamıştır. Fıkra metninde kişilerin *siyasi, felsefî veya dini görüşleri ile ırkî kökenlerine ilişkin bilgileri* kişisel veri olarak kaydeden kimsenin cezalandırılacağı vurgulanmış, bunun için eylemin hukuka uygun veya aykırı olması arasında bir fark yokmuş gibi düzenleme yapılmıştır. Bu nedenle bu tür kişisel verileri hukuka uygun olarak kaydetmenin bile, TCK'nın 135. maddesinde düzenlenen suçu oluşturacağını savunmuşlardır¹⁷⁵.

Bir kısım yazarlar ise, hükümdeki ifadeden bu bilgilerin kişisel veri olarak kaydedilmesinin her zaman, mutlak olarak hukuka aykırı olacağı sonucu çıktığını, ancak kanunun, hem maddenin birinci fıkrası hükmünde, hem ikinci fıkrasında diğer durumlar için hukuka aykırı olmak hükmüne yer vermişken, bu hali, onlardan niçin ayırık tuttuğunun anlaşılamadığını belirtmişlerdir (Hafızoğulları ve Özen, 2011: s. 277; Özen, 2009: s. 15).

Maddenin kaleme alınış şeklinden yola çıkan yazarlar ise maddenin düzenlemesine göre, siyasi, felsefî, dini görüşler ile ırkî kökene dair kişisel verilerin hiçbir şart altında işlenemeyeceği, bu tür verilerin işlenmesine izin veren bir kanun dahi çıkarılamayacağı, bu verilerin mutlak dokunulmaz veriler olduğunu buna karşın, ahlaki eğilim, cinsel yaşam, sağlık durumu ve sendikal bağlantılara ilişkin verilerin, kanunun izin verdiği sınırlar içinde işlenebileceğini, fıkra metnindeki “Hukuka aykırı olarak” ibaresinin fıkranın başına değil, belli tür veriler sayıldıktan sonra, sadece kendisinden sonra sayılanlar için geçerli olacak şekilde ortasına yazılmasının bu anlama geldiğini savunmuşlardır (Özbek vd, 2011: s. 518).

Diğer bir kısım yazarlar ise maddede bazı veri türlerinin özel nitelikte görülmesi nedeniyle farklı bir düzenlemeye tabi tutulduğunu, özellikle devlet kurum ve kuruluşlarının kamu hizmetlerini yerine getirirken bu türdeki bilgileri kişisel veri

Kanunun hazırlık çalışmalarında ve gerekçede bu konuya ilişkin bir açıklamaya rastlanmamıştır". Hafızoğulları/Özen, 2011: s. 269.

¹⁷⁵ **Parlar/Hatipoğlu**, 2008, s. 2044-2045. Bu yazarlara göre, “yasa koyucu bu düzenleme ile aslında bireyler arasında bölücülük yapılmasını önlemek ve özel hayatın gizliliği ve korunması hakkında müdahale içeriği taşıyan bu fiilleri yaptırım altına almak suretiyle bu hakka güvence sağlamak amacını gütmektedir.”; Aynı yönde bkz. **Şener**, s. 79; **Değirmenci, Olgun**, “2004 Türk Ceza Kanunun Bilişim Suçları Açısından Değerlendirilmesi”, TBB Dergisi, S. 58, Y. 2005, s. 202

olarak tutmalarından herhangi bir yarar beklemenin güç olduğunu, bir hukuk devletinde, yönetimin bu bilgiler karşısında gözlerinin bağlı olması gerektiğini, bu maddenin de bunu sağlamaya yönelik olduğunu belirtmişlerdir (Küzeci, 2010: s. 288).

Başka bir yazar, burada sorunun, maddenin kaynağını oluşturan Fransız Ceza Kanununda yer alan kişisel verilerin korunmasına ilişkin suçların eksik norm olarak düzenlenmesinden kaynaklandığını, bu ülkede kişisel verilerin korunmasına ilişkin kanunun varlığı nedeniyle, söz konusu kanunda gösterilen usul ve esaslara uyulmamasının müeyyide altına alınmakla yetnildiğini belirtmiştir. Bu yazara göre, “TCK'nin 135. maddesinde düzenlenen suç bakımından, Fransız hukukunda olduğu şekliyle, eksik norm olarak bağlantı kurulabilecek kişisel verilerin korunmasına ilişkin genel bir düzenleme bulunmamaktadır. Bu nedenle, maddede yer alan hukuka aykırı olarak kaydetmenin yorumlanması gerekmektedir” (Ketizmen, 2008: s. 235).

Düzenlemenin sonuçlarından yola çıkan bir kısım yazarlar ise, 135. maddenin ikinci fıkrasındaki düzenlemenin, zaten kişisel veri niteliği taşıyan bazı bilgi türlerinin sıralanmasından ibaret olduğunu, bu tür verilerin diğerlerinden ayrı düzenlenmesinin asıl sebebinin, bunların daha iyi korunmaları amacını gerçekleştirmeye yönelik olsa da, bunun gerçekte mümkün olmadığını, bu maddede hassas verilerin ayrıca düzenlenmiş olmasının, kişisel verilerin kaydedilmesi suçu açısından hiçbir değişiklik yaratmayacağını, çünkü düzenlemenin niteliği itibarıyla bu amacı gerçekleştirme kudretine sahip olmadığını savunmuşlardır (Akdağ, 2013: s. 35).

Yine bu yazara göre, belli tür kişisel verilerin işlenmesinin mutlak olarak yasaklanması, ancak böyle bir düzenlemenin Anayasa'da yer almasıyla mümkün olabilecektir. TCK'nun 135. maddesinin 2. fıkrası bu amacı taşıyor olsa dahi daha sonraki bir tarihte yürürlüğe giren veya TCK'ndan daha özel nitelikli bir kanunda, işlenmesi yasaklanan verilerin işlenmesine izin veren veya işlenmesini emreden bir hükmün yer alması durumunda, bu veriler işlenebilir hale gelecektir. Kanunlar, normlar hiyerarşisinde aynı seviyede yer aldıkları için TCK'nun bu yasağı, özel nitelikli veya sonraki tarihli olan bu kanun açısından bir değer ifade etmeyecektir. Dolayısıyla bu düzenleme, ancak normlar hiyerarşisinde kanunun altında yer alan düzenlemeler açısından anlam ifade edecektir (Akdağ, 2013: s. 36-37).

Diğer bir kısım yazarlar ise maddedeki düzenlemenin kişinin kendi rızasıyla alenileştirdiği hasas verilerinin kaydedilmesi durumunda sorun yaşatacağını ifade etmişlerdir. Bu yazara göre, bir kişi, kendi iradesi ile siyasi, felsefi veya dini görüşünü, ırksal kökeni açıklayabilir, hatta bunu çeşitli iletişim araçları ile duyurabilir. O zaman açıklanan bu bilgilerin kayıt altına alınması her durumda suç oluşturacak mıdır? 135. maddenin gerekçesinde *"kişinin kendi rızası ile kendisiyle ilgili bilgilerin kayda alınmasının suç oluşturmayacağı muhakkaktır"* ifadesi yer almaktadır¹⁷⁶. Yazara göre, ilgili kişinin özgür iradesinin yansıması olan rızası ile bu bilgilerin kayıt altına alınmasının herhangi bir sakıncası olmamalı hatta o kişinin düşünceyi açıklama özgürlüğü çerçevesinde kabul görmelidir. Bu nedenle bu suçta TCK'nın 24 vd. maddelerinde düzenlenen genel hukuka uygunluk nedenlerine başvurmak ve TCK'ın 26/2. maddesinde düzenlenen *"Kişinin üzerinde mutlak surette tasarruf edebileceği bir hakkına ilişkin olmak üzere, açıkladığı rızası çerçevesinde işlenen fiilden dolayı kimseye ceza verilmez"* hükmünün burada da geçerli olduğunu kabul etmek gerekir (Küzeci, 2010: s. 289).

Bir kısım yazarlar ise TCK ile hukuka aykırı olarak veri kaydetme cezalandırıldığını, kaydedilen verilerin kişinin yaşamına, mesleğine, ahlaki eğilimlerine, siyasi, felsefi veya dini görüşlerine, ırki kökenlerine ilişkin olması arasında bir fark olmadığını (Soyaslan, 2006: s. 273), kanun koyucu milli güvenlik, milli savunma, kamu düzeni ve kamu güvenliğinin korunması amacıyla bir istihbarat birimine kişilerin siyasi, felsefi veya dini görüşlerine veya ırki kökenlerine ilişkin bilgileri toplama ve depolama görevi vermesi halinde bile, bu suçun oluşacağını düşünmenin mümkün gözükmediğini, bu nedenle, TCK'nın 135. maddesinin her iki fıkrasında düzenlenen ve kişisel veri sayılan tüm hususların hukuka aykırı olarak kaydedilmesi halinde bu suçun oluşacağını, fıkra metninde belirtilen hukuka aykırılık ibaresinin suçun konusunu oluşturan tüm öğeler için geçerli olduğunu savunmuşlardır (Yaşar vd, 2010: s. 4119).

Maddenin ikinci fıkrasının gerekçesine bakıldığında, *"Maddenin ikinci fıkrasında kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine, ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kayda almak, suç olarak tanımlanmıştır. Ancak, bunlardan kişilerin*

¹⁷⁶ 135. maddenin gerekçesi için bkz., Artuk/Gökçen/Yenidünya, Türk Ceza Kanunu Şerhi, s. 3214

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.” Şeklinde yetersiz bir açıklama bulunmaktadır. Zira böyle önemli bir maddede kanun koyucunun iradesinin daha net anlaşılabilmesi için fıkranın amacının daha açık ifadelerle izah edilmesi gerekirdi. Yinede madde gerekçesinde az da olsa kanunkoyucu iradesini yansıtmıştır. Zira kişisel veriler günlük hayatta gerek kamu gerek özel sektör tarafından sıkça işlenmekte, bu işleme bazen kamu görevinden bazen kişinin verdiği rıza ile olabilmektedir. Bu kapsamda örneğin sağlık bilgileri, sağlık hizmetlerinin yerine getirilebilmesi amacıyla sağlık kuruluşları tarafından, sendika üyeliğine ilişkin bilgiler, üyelerin haklarının korunmasının sağlanması ve aidatların yatırılabilmesi amacıyla sendikalar ve işverenler tarafından kaydedilmektedir. Bu kayıtlar ancak hukuka aykırı olduğu zaman suç oluşturacaktır.

Diğer bir deyişle bu veriler kamu kurumları tarafından verilen kamu hizmetinin gereği olarak veya kanunla verilen yetkiye dayanarak; özel sektör tarafından ise verilen hizmetin yerine getirilebilmesi için zorunlu olması, kişinin rızası olması veya aralarındaki sözleşmenin ifası için gerekli olması gibi nedenlerle normal hayatta kaydedilebilen veriler olması nedeniyle, kanun koyucu tarafından ancak hukuka aykırı şekilde işlenmeleri hali suç sayılmıştır.

Ancak kişinin siyasi, dini ve felsefi görüşü ile ırki kökeni normal şartlarda kaydedilen bilgiler değildir. Bu bilgilerin üçüncü kişiler tarafından öğrenilmesi çoğunlukla kişinin ayrımcılıkla karşı karşıya kalmasına sebebiyet verebilecektir. Bu nedenledir ki bu bilgiler kişinin hayatının gizli alanını oluşturmaktadır ve anayasal güvence altındadır (AY m. 20). Ayrıca Anayasanın 24. Maddesi de bu hükmü desteklemektedir. Zira bu maddede herkesin vicdan, dini inanç ve kanaat hürriyetine sahip olduğu belirtilmiş, bu hakkın sınırlanma nedenleri ne ise Anayasada yer verilmemiştir. Anayasanın 13. maddesindeki kural gereği anayasada sayılmayan nedenlerden ötürü de bir hakkı kısıtlamak mümkün olmadığından bu hakkın “bu bilgilerin toplanması, kaydedilmesi ve paylaşılması” yoluyla sınırlanması da mümkün değildir. İşte kanun koyucu kişinin ayrımcılığa uğramasına engel olmak amacıyla kişinin hayatının en mahrem alanına giren bu bilgilerin kaydedilmesini

mutlak olarak yasaklamıştır. Esasında bu fıkra, “fişlemeyi” suç haline getiren bir hükümdür. Dikkat edilecek olursa “...” bilgileri kişisel veri olarak kaydeden kişinin cezalandırılacağı belirtilmektedir. Bu nedenle fıkranın düzenlenme amacı itibarıyla yerinde bir hüküm olduğunu değerlendirmekteyiz.

Her ne kadar yukarıda belirtilen bir kısım yazarlar, yeni bir kanun veya özel kanun bu verilerin işlenmesine izin verirse eylemin suç olmayacağı savunmuşlarsa da, kanaatimizce yorumlar mevcut düzenlemelere göre yapılmalıdır. İlerde bu verilerin işlenmesine izni veren başka bir kanun çıkarsa ne olacaktır? Bu durum kanunkoyucunun takdirindedir. Somut duruma göre bir değerlendirme yapılacaktır. Ancak şu aşamada 135. maddenin ikinci fıkrasındaki düzenleme, madde gerekçesiyle birlikte değerlendirildiğinde, kişilerin “siyasi, felsefi veya dini görüşlerine, ırki kökenlerine” ilişkin bilgilerin kişisel veri olarak kaydedilmesi her durumda suç olacaktır. Kanunkoyucu da zaten bunu amaçlamıştır. Ancak yine de doktrinde de dile getirildiği üzere, bu hususun kişisel verilerin korunması hakkını düzenlendiği 20. maddenin üçüncü fıkrasında da düzenlemesi hukuk tekniği açısından faydalı ve gerekli olacaktır.

Kişilerin ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal faaliyetlerine ilişkin bilgilerin kişisel veri olarak kaydedilmesinin ikinci fıkradaki suçu oluşturabilmesi için ise bu eylemin hukuka aykırı olarak işlenmesi gerekmektedir. Hukuka aykırılık, fiile herhangi bir hukuk kuralınca cevaz verilmemesidir. Bu tür bilgilerin kayda alınmasına kanunlarda, özellikle suçlulukla mücadele bağlamında, adli işlemlerde suç ve suçluların ortaya çıkarılmasını sağlamak amacıyla belli ölçüde izin verilebilmektedir. Hukuka aykırılık yoksa bu hallerde suç oluşmayacaktır (Parlar ve Hatipoğlu, 2008: s. 2045).

2.3.4.2. Hukuka Uygunluk Sebepleri

Günümüz toplumunda kişisel verilerin kaydedilerek muhafaza edilmesinde ilgili kişinin bizzat kendisinin yararı olabilir. Örneğin, hastanelerde hastaların, kredili alışveriş yapılan mağazalarda müşterilerin, kredi çekilen bankalarda kredi çekenlerin kişisel verileri alınmakta ve muhafaza edilmektedir. Bu tür alım ve muhafaza etmeler, hem veri sahibi kişinin yararına hem de istenilen hizmetin yerine getirilmesi için adeta zorunluluk halini almıştır. Bu durumlarda esasen veriler ilgilinin rızasıyla

ve bir görevin icrası kapsamında alınmakta ve verilen hizmetin ifası için kullanılmaktadır. Bu nedenle burada **ilgilinin rızası ve mesleğin icrası** gibi hukuka uygunluk nedenleri bulunmaktadır (Soyaslan, 2006: s. 273).

Bazen de kişisel veriler ilgili kanun hükümlerine çerçevesinde çeşitli kamu hizmetlerinin gereği olarak kamu kurumları tarafından işlenmektedir. Bu durumlarda da kanun hükmü işleme fiilini hukuka uygun hale getirmektedir.

Madde metnin de ise bu suç için olabilecek hukuka uygunluk nedenlerinden bahsedilmemiştir. Bu nedenle Türk Ceza Kanunun genel hükümler kısmında yer alan ceza sorumluluğu kaldıran veya azaltan nedenler başlığı altında düzenlenen kanun hükmü ve amirin emri, hakkın kullanılması ve ilgilinin rızası, meşru savunma ve zaruret hali, cebir şiddet, korkutma ve tehdit gibi nedenler bu suç açısından da kısmen uygulama olanağı olabilir. Ancak çalışmamızın ilk bölümlerinde belirtildiği üzere, gerek Avrupa Konseyinin 108 nolu Sözleşmesi, gerek Avrupa Birliğinin 95/46/EC sayılı Direktifinde ve bu uluslararası düzenlemelere esas alınarak hazırlanan Kişisel Verilerin Korunması Kanun Tasarısında, kişisel verilerin işlenmesini hukuka uygun kılan nedenlere yer verilmiştir. Bu nedenlerin bir kısmının TCK'dakilerle uyuştuguda görölmektedir. Bu nedenle uluslararası belgelerdeki düzenlemeler ile TCK ve Tasarıdaki düzenlemeler birlikte değerlendirilerek kişisel verilerin kaydedilmesinin hukuka uygun kılabilcek nedenler aşağıda açıklanmaya çalışılmıştır.

2.3.4.2.1. İlgili Kişinin Rızası

İlgili kişinin yani kişisel verileri işlenen kişinin rızası bu suç bakımından fiili suç olmaktan çıkarır. Çünkü kişilerin kendilerine ait bilgileri üzerinde mutlak surette tasarruf hakları bulunmaktadır. Örneğin bir kuruma yapılan iş başvurusunda, bankaya yapılan kredi başvurusunda ve sınav için yapılan başvuruda, kişisel verinin sahibi olan kişi kendi rızasıyla bu verileri vermektedir (Yaşar vd, 2010: s. 4121; Hafizoğulları ve Özen, 2010: s. 278; Özbek vd, 2013: s. 536; Özen, 2009: s. 17). Ancak belirtmek gerekir ki, fiilin suç teşkil etmemesi için gösterilen rızanın sınırları içinde kalınmalıdır. Sadece kayda rıza gösterilmiş ise, bu kaydın ifşa edilmesi, başkalarına aktarılması ya da kullanılması başka bir suçu oluşturabilecektir (Özen, 2009: s. 17). Örneğin facebook gibi sosyal paylaşım sitelerinde site üyelerinin, kendi hesapları

üzerinden kişisel verilerini internete yüklemesi ve sadece kendi arkadaşlarının bu verilere ulaşmasına izin vermesi durumunda, bu arkadaşlarının verileri kaydetmeleri durumunda suç oluşmayacaktır. Ancak izin verilenlerin haricindeki kişilerin bir şekilde bu verileri ele geçirmeleri durumunda artık rızanın varlığından söz edilemeyecektir.

Diğer taraftan kişinin verileri kaydedilmeden önce yapılacak işlem ile ilgili bilgilendirilmesi gerekmektedir. Yani kişi kayıttan önce konu hakkında bilgilendirilmeli, aydınlatılmalıdır¹⁷⁷. Geçerli bir rıza için bunun şart olduğunu düşünüyoruz.

Anayasanın 20. Maddesinin üçüncü fıkrasında da, kişisel verilerin kişinin açık rızasıyla işlenebileceği hüküm altına alınmıştır. Henüz Anayasadaki bu kuralın uygulamasını gösterecek kişisel verilerin korunmasına ilişkin bir kanun çıkmamış olsa da, Anayasanın bu hükmü yürürlükte olduğu için uygulama alanı bulacaktır.

Nitekim Anayasanın bu hükmü, TCK'daki hukuka uygunluk nedenlerinden olan "ilgilinin rızası" ile uyumaktadır.

Bir hukuka uygunluk sebebi olarak "*ilginin rızası*" TCK'nun 26/2. maddesinde düzenlenmiştir. Maddeye göre, kişinin üzerinde mutlak surette tasarrufta bulunabileceği bir hakkına ilişkin olmak üzere açıkladığı rızası çerçevesinde işlenen fiilden dolayı kimseye ceza verilmez. İlgilinin rızasının geçerli bir hukuka uygunluk sebebi olabilmesi için;

- 1- Kişinin üzerinde serbestçe tasarrufta bulunabileceği bir hakkının olması,
- 2- Kişinin rızaya ehil olması,
- 3- Rıza beyanında bulunulması,

Şartlarının bir arada gerçekleşmesi gerekmektedir.

Bireyin üzerinde mutlak şekilde tasarrufta bulunabileceği bir hak yoksa rızanın varlığı herhangi bir etki doğurmayacaktır. Böyle bir hakkın var olup olmadığı bütün hukuk düzenine hâkim olan genel ilkelere göre belirlenir. Öncelikle korunan hak veya yararın ve suç tipinde belirtilen konunun kişiye ait olması gerekir (Özbek vd, 2013: s. 536).

¹⁷⁷ Bkz. TCK'nın 26. maddesinin gerekçesi.; Aynı yönde bkz. **Işık**, 2010: s. 178

Bir kısım yazarlar, kural olarak soruşturulması ve kovuşturulması şikâyet tabi suçlar bakımından mağdurun üzerinde tasarrufta bulunabileceği bir hakkın var olduğu kabul edildiğini, *Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar* başlığı altında düzenlenmiş bulunan suçlardan kişisel verilerin kaydedilmesi suçunun şikâyet tabi olmadığını, bu nedenle kişisel verilerin hukuka aykırı olarak kaydedilmesi suçu bakımından ilgilinin rızası hukuka uygunluk sebebinin uygulanabilir olmadığını belirtmişler ise de (Özbek vd, 2013: s. 537), bu görüşe katılmak mümkün değildir. Zira şikâyet, suçun unsurlarından değildir. Suçun soruşturulabilmesi veya kovuşturulabilmesi için aranan bir usul hükmüdür. Şikâyetin olmaması suçun oluşmasına engel olmaz. Ancak şikâyet olmadığında suçun soruşturması veya kovuşturması yapılamaz. Rıza ise bir hukuka uygunluk nedenidir ve hukuka uygunluk nedenleri suçun unsurları içindedir. Hukuken geçerli bir rızanın varlığı eylemi suç olmaktan çıkarmaktadır. Bu nedenle kişinin üzerinde mutlak surette tasarrufta bulunabilecek hakkı belirlenirken suçun şikâyet tabi olup olmaması önemli değildir.

Diğer taraftan mevzuat hükümleri çerçevesinde yapılacak kayıta hukuka uygunluk sebebi bakımından ilgilinin rızası değil, kanun hükmünün yerine getirilmesi söz konusudur. Bu durumda kişinin rızasına bakılmaz. Bu nedenle mevzuata uygun olarak gerçekleştirilmeyen kaydı da ilgilinin rızası hukuka uygun hale getirmeyecektir (Özbek vd, 2013: s. 537).

Bu konuda AİHM, 03.04.2007 tarihli İngiltere'ye karşı Copland kararında, işyerlerindeki internet ve e-mail kullanımı ile trafik bilgilerinin denetlenmesinin de özel hayata ilişkin AİHS'in 8. Maddesi kapsamına girdiğini, çalışanların iletişimine yönelik müdahalenin hukuka uygunluğunun "yasayla öngörülmüş" olması koşuluna bağlı olduğunu hüküm altına almıştır. AİHM'in bu görüşü esas alındığında, hukukumuzda işverenlerin hangi koşullar altında çalışanlara işyeri tarafından tahsis edilen işyeri uzantılı e-posta adresiyle ilgili iletişimine müdahale edebileceğini gösteren açık bir düzenleme bulunmadığı için, bu tür e-mail üzerinden yapılan yazışmaların önceden haber verilmeksizin denetlenmesi halinde, bu suçun oluşacağı düşünülebilir. Zira AİHM'e göre, işyeri telefonundan personelin yaptığı özel konuşmaların önceden haber verilmeksizin işveren tarafından denetlenmesi özel yaşama bir müdahale sayılır. Aynı durum, internet üzerinden yapılan e-mail ve

uzantıları için de geçerlidir(par.42). Başvuranın bilgisi olmaksızın yaptığı konuşmalarına ilişkin kişisel nitelikli verilerinin, e-postalarının ve internet üzerinden yaptığı görüşmelerin m. 8 anlamında özel yaşama ve haberleşme özgürlüğüne müdahale oluşturacağı sonucuna varılmalıdır (par.44, Tezcan, 2013: s. 1160).

Yukarıda belirtildiği üzere mağdurun rızası hukuka uygunluk sebebi sayıldığından, önceden iş sözleşmesine konulan bir madde ile işyeri uzantılı e-posta adresi üzerinden yapılacak haberleşmenin denetleneceği kendisine bildirilmiş ve çalışan da bu denetlemeyi kabul etmiş ise, mağdurun rızası çerçevesinde yapılan müdahale hukuka uygun sayılacaktır (Tezcan, 2013: s. 1160).

Nitekim konu İş Hukuku bakımından da tartışılmış ve Yargıtay 9. Hukuk Dairesi, gerek 13 Aralık 2010 tarih ve E.2010/447, K.2010/37516 sayılı kararında¹⁷⁸, gerekse aynı Dairenin 13.12.2010 tarih ve 2009/447 Esas-2010/37516 sayılı kararlarında¹⁷⁹, işçinin rızası olan hallerde bu denetimin mevzuata aykırı olmadığı sonucuna varılmıştır (Tezcan, 2013: s. 1161).

¹⁷⁸ "İşçiye, şirketin işlerini yürütmesi için işveren tarafından bilgisayar ve e-mail adresleri verilmiştir. İşçi bu bilgisayar ve e-mail adreslerini kullanarak, bazı yazışmalar yapmış ve bu yazışmalar sırasında işverenin şahsına yönelik hakaret niteliğinde ifadeler kullandığı ve işyeri sırrı sayılabilecek konularda da yazışmalar yaptığı anlaşılmıştır. İşverenin, kendisine ait bilgisayar ve e-mail adresleri ile bu adreslere gelen e-postaları, her zaman denetleme yetkisi bulunmaktadır." (Yargıtay 9. Hukuk Dairesi, 13 Aralık 2010 Tarih ve E.2010/447, K.2010/37516 sayılı kararı-<http://www.muhassebedergisi.com/sukru-kizilot--hurriyet-gazetesi/isverenin-bilgasayar-ve-e-postalari-denetleme-yetkisi-var.html>)

¹⁷⁹ "Dosyadaki yazılara toplanan delillerle kararın dayandığı kanuni gerektirici sebeplere göre davacının tüm, davalının aşağıdaki bendin kapsamı dışında kalan temyiz itirazlarının yerinde olmaması nedeni ile reddine. Temyiz nedenlerine göre davacının iş akdine haklı nedenle son verilip verilmediği konusunda taraflar arasında ihtilaf bulunmaktadır. Davacı vekili dava dilekçesinde davacının davalıya ait işyerinde 20.03.1998-02.03.2002 tarihleri arasında teknisyen olarak çalıştığını, çalışmalarının SSK'ya bildirilmediğini, işverenden sigorta işlemlerinin yapılmasını ve geçmişe yönelik haklarını talep etmesi üzerine davalı işverenlikçe işten çıkarılmakla tehdit edilerek ve geçmişe yönelik alacağı ve hakkı olmadığı yönünde belge imzalatılmak istendiğini, ancak müvekkilinin bu belgeyi imzalamaması üzerine 02.03.2002 tarihinde işveren tarafından işten çıkarıldığını belirterek kıdem ve ihbar tazminatı ile diğer bazı işçilik alacaklarının davalıdan tahsilini talep etmiştir. Davalı vekili cevap dilekçesinde ve atamalarındaki beyanlarında dava dilekçesindeki haksız fesih iddiasının gerçek dışı olduğunu, davacının internet üzerinden teknik bilgi ve servis işlerini yapabilmesi için kendisine tahsis edilen ve şifresi yalnızca kendisi tarafından bilinen mail adresinden internet üzerinden 3. kişilerle yaptığı mesaj ve haberleşme ile işyerini kötüleyici, firmayı ve işvereni zarara sokucu ve işyerinin sırlarını ifşa edici haberleşmeler yapmak suretiyle kötü niyetli ve işyerini zarara uğratici davranışlarda bulunduğunu, davacının hotmail.com" adresinden işveren yetkilisinin okuması için hakaret dolu metinler gönderdiğini, suç teşkil eden bu eylemleri nedeniyle C. Savcılığına ihbarda bulunulduğunu ve hakkında Bakırköy Asliye Hukuk Mahkemesinde tazminat davası açıldığını,

Diğer taraftan rıza konusunda üzerinde durulması gereken önemli bir hususta Anayasada verilerin işlenmesi için aranan rızanın “açık rıza” olması meselesidir. Ancak açık rızanın mevzuatımızda tanımı yapılmamıştır. Kişisel Verilerin Korunması Kanun Tasarısı hazırlanırken referans alınan AB’nin 95/46/EC sayılı Veri koruma Direktifinde rıza, kişinin kendisiyle ilgili verilerin işlenmesini kabul ettiğini gösteren belirli ve aydınlatılmış iradesinin her türlü işareti olarak tanımlanmış, hassas verilerin işlenmesi söz konusu olduğunda bu rızanın açık olması şartı aranmıştır. Bu düzenleme nedeniyle doktrinde açık rıza için, rızaya ilişkin diğer şartların yanında rızanın açık şekilde verilmesinin de gerekli olduğu belirtilmiştir. Yani ilgili kişinin verilerinin işlenmesini kabule yönelik iradesini ortaya koyan müsbet bir hareket yapması gerekmektedir (Küzeci, 2010: s. 240).

Ceza hukukundaki düzenlemelere bakıldığında rızanın geçerliliği, kural olarak şekil şartına bağlı değildir. Karşı tarafta şüpheye yer bırakmayacak nitelikte olduğu sürece, herhangi bir şekilde açıklanmış olabilir. Bu minvalde rızanın zımni de olabilmektedir (Akdağ, 2013: s. 113).

davacının işyerine karşı olumsuz eylemlerde bulunduğunu, işyerinin mahremiyetini internet aracılığı ile bozarak, sırlarını ifşa ettiğini, 3 gün üst üste işyerine gelmemesi üzerine iş akdinin feshedildiğini beyanla haksız davanın reddini talep etmiştir. Davacı vekili cevaba cevap dilekçesinde ise, bahse konu maillerin davacı ile (...) isimli kişi arasındaki tamamen haberleşme amacı ile yapıldığını, davalı işverenin hedef alınmadığını, yazıların işverene ulaştırılmasının amaçlanmadığını, kaldı ki internet aracılığıyla yapılan bu yazışmaların kişinin özel hayatı ile ilgili olduğunu, hukuki bakımdan korunması gerektiğini bunların hukuka aykırı yollarla elde edildiğini ve hükme esas alınamayacağını belirtmiştir. Mahkemece davalı tarafça davacı hakkında tanzim edilen 5 ve 6 Mart 2002 tarihli devamsızlık tutanakları sunulmasına rağmen fesih ihtarnamesinin ibraz edilip tanıklar dinletilerek tutanaklarının doğruluğunun teyit ettirilmediğini, SSK kayıtlarında davacının çıkışının 30 Nisan 2002 tarihinde yapıldığı, işverenin fesih hakkını 6 iş günü içinde kullanmadığı, davacının hakaret içerdiği iddia edilen mailleri sunmadığı ve bu hali ile işverenin haklı feshi somut olarak kanıtlayamadığı gerekçesi ile davacının kıdem ve ihbar tazminatı taleplerinin kabulüne karar verilmiştir. Somut uyumsuzlukta, dosya kapsamına göre davacının görevi gereği işverenin işlerini yürütmesi için kendisine verilen bilgisayar ve e-mail adreslerini kullanarak iş akdi daha önce feshedilen (.) ile işle ilgili olmayan elektronik yazışmalar yaptığı, bu yazışmalar sırasında işverenin şahsına yönelik hakaret niteliğinde sözler sarf ettiği işyeri sırrı sayılabilecek konularda da yazışmalar yaptığı anlaşılmıştır. İşverenin kendisine ait bilgisayar ve email adresleri ile bu adreslere gelen e-postaları her zaman denetleme yetkisi bulunmaktadır. Davalı işverene ait bilgisayarları ve e-mail adreslerini özel yazışmalarda kullanıp işverene hakaret niteliğinde sözler sarf etmenin, işveren açısından 4857 sayılı Yasa’nın 25 II-b maddesi uyarınca sataşma niteliğinde haklı fesih nedeni oluşturacağı anlaşılmakla davacının ihbar ve kıdem tazminatı taleplerinin reddi yerine yazılı gerekçe ile kabulü hatalı olup bozmayı gerektirmiştir. Temyiz olunan kararın yukarıda yazılı sebepten bozulmasına, oybirliğiyle karar verildi." (Yargıtay 9 Hukuk Dairesinin 13.12.2010 tarih ve 2009/447 Esas- 2010/37516 sayılı kararı- <http://kanberkilinc.com.tr/isverene-elektronik-postada-hakaret-etmek-hakli-fesih-sebebi-sayilir.htm>)

Rızaya ilişkin bu geçerlilik şartları diğer suçlar açısından uygulanabilir olsa da, kişisel verilerin kaydedilmesi suçu söz konusu olduğunda, hareketsiz kalmanın rıza kabul edilmesi ya da rızanın sadece varsayılması mümkün değildir. Anayasada ve Tasarıda yapılan “açık rıza” vurgusu da bu görüşümüzü destekler niteliktedir (Akdağ, 2013: s. 114).

Bu suçta geçerli bir rızadan bahedilebilmesi için kişiye, kişisel verisinin işleneceği, bu işlemenin sınırı ve amaçları, hatta muhtemel sonuçları hakkında bilgi verilmesi gerekmektedir. Aksi halde, geçerli bir rızadan bahsetmek mümkün değildir (şimşek, 2008: s. 106).

Ayrıca rıza, sadece kişisel veriler kaydedilirken bildirilen kaydetme amaçları için geçerli olur. Bunların dışındaki amaçlarla kişisel verilerin kaydedilmesi durumunda, veri süjesinin rızasından bahsedilemez. Rızanın bu özellikleri, çalışmamızın ikinci bölümünde anlatılan uluslararası belgelerdeki veri koruma ilkelerine ve Anayasamızdaki düzenlemeye uygundur (Ketizmen, 2008: s. 237-238; Akdağ, 2013: s. 114).

2.3.4.2.2. Kanun Hükmünün Yerine Getirilmesi

Diğer yandan çeşitli kamu hizmetlerinin verilmesinde ise kişisel verilerin kaydedilmesi kanunlardan kaynaklanabilmektedir. Kişisel veriler ilgili kanun hükümlerine dayalı olarak çeşitli kamu hizmetlerinin verilmesi amacıyla, örneğin Sağlık Bakanlığı, Adalet Bakanlığı veya İçişleri Bakanlığı tarafından görev, çalışma ve hizmet alanları ile sınırlı olmak şartıyla kaydedilmektedirler (Parlar ve Hatipoğlu, 2008: s. 2044). Bu durumlarda kişinin rızası olmasa dahi ilgilinin verileri kaydedilmektedir. Nüfus müdürlükleri tarafından kimlik ve adres bilgilerinin; Adalet Bakanlığı tarafından da adli sicil kayıtlarının tutulması gibi. Burada yapılan kaydetme eylemi suç teşkil etmemektedir. Zira burada da hukuka uygunluk sebebi olarak **kanun hükmünün yerine getirilmesi** durumu söz konusudur.

Anayasanın 20. Maddesinin üçüncü fıkrasında da belirtildiği üzere kişisel veriler kanunda öngörülen hallerde işlenebilmektedir. Bu durumda kişinin rızasına gerek bulunmamaktadır. Ayrıca kanu hükmünün yerine getirilmesi, TCK’nın 24. maddesinin birinci fıkrasında da ceza sorumluluğunu kaldıran nedenler arasında sayılmıştır (Bakıcı, 2008. S. 542 vd).

TCK'daki kanun deyiminden "kanun kuralı" anlaşılması gerekmekte olup, bu kanun, Türk Ceza Kanunu olabileceği gibi, Ceza Muhakemesi Kanunu, Nüfus Hizmetleri Kanunu veya PVSK gibi diğer kanunlarda olabilecektir.

Doktrinde yetkili makamlarca usulüne uygun tarzda yürürlüğe konulan tüzüklerin ve yönetmeliklerin, dayandıkları kanunun verdiği yetki sınırları çerçevesinde, bu kapsamda değerlendirilebileceği ileri sürülmüştür (Artuk vd, Genel Hükümler, 2013: s. 376; Özgenç, 2013: s. 294; Bakıcı, 2008: s. 544). Ancak bu görüşler diğer suçlar için kabul edilebilirse de kişisel verilerin kaydedilmesi suçu açısından kabul edilemeyeceği kanısındayız. Zira verilerin korunması anayasada güvence altına alınmış bir temel haktır. Ve Anayasada bu hakkın ancak rıza ile kanunlarda öngörülen hallerde sınırlanabileceği belirtilmiştir. Yönetmelik ve tüzükler ise kanunun uygulanmasını gösteren idari belgelerdir. Bir kişisel verinin hangi şartlarda işlenip işlenemeyeceğini belirleme gücüne sahip değildirler.

Diğer yandan verilerin işlenmesine izin veren kanun hükmünün uygulayıcılar tarafından da usulüne uygun tarzda icra edilmesi gerekmektedir. Örneğin; Göreviyle bağlantılı olarak öğrendiği bir suçu yetkili makamlara bildiren kamu görevlisinin (TCK. m.279), şikâyetle bağlı suçlarda şikâyet hakkını kullanan müştekinin (TCK. m.73), sanığın savunmasını yapan müdafinin veya faile ceza veren hâkimin, usulüne uygun olarak bu işleri yapmasından dolayı cezalandırılması mümkün değildir. Aynı şekilde kolluk kuvvetlerinin görevleri sırasında şartları dâhilinde silah kullanma yetkisine başvurmaları halinde de, fiil hukuka uygun kabul edilecektir (Artuk vd, Genel Hükümler, 2013: s. 376; Özgenç, 2013: s. 294).

Bazı fiillerin Ceza Muhakemesi Kanununda öngörülen usul ve esaslar çerçevesinde bir koruma tedbiri olarak uygulanması halinde de, kanundan kaynaklanan bir yetki kullanıldığı için fiil hukuka uygun olmaktadır (Özgenç, 2013: s. 294). Örneğin, kişiler arasındaki haberleşmenin ihlali ve konuşmaların rızaları dışında kaydedilmesi ile özel hayatlarının gizliliğinin ihali TCK'nun 132, 133 ve 134. maddelerinde suç olarak düzenlenmesine rağmen, bu eylemler CMK'daki kural ve şartlara göre yapıldığında suç teşkil etmeyecek, fiil hukuka uygun sayılacaktır.

Kişilerin nüfus ve kimlik bilgilerinin toplanması 5490 sayılı Nüfus Hizmetleri Kanunu, istatistik üretmek için Türkiye İstatistik Kurumu tarafından kişisel verilerin

toplanması 5429 sayılı Türkiye İstatistik Kanunu, mahkûmiyet bilgilerinin tutulması 5252 sayılı Adli Sicil Kanunu, idari kolluk faaliyetleri kapsamında parmak izi bilgilerinin alınması 2559 sayılı PVSK, moloküler genetik inceleme amacıyla DNA verilerinin alınması CMK gereği yapıldığından, bu kişisel veri toplama ve işleme eylemleri hukuka uygun hale gelmektedir.

Ayrıca, usulüne uygun olarak alınmış yetkili merci kararı varsa, bu suç unsurları itibariyle oluşmayacaktır (Yaşar vd, 2010: s. 4121). Bu kapsamda Cumhuriyet Savcısının emri veya mahkeme kararı gereği kolluk tarafından şüpheli veya sanığın sosyal ve ekonomik verileri ile suç bilgilerinin araştırılması ve kaydedilmesi durumunda eylem hukuka uygun sayılmaktadır. Ancak burada dikkat edilmesi gereken husus kanunla verilen kişisel veri toplama yetkisinin açık olması ve sınırlarının çizilmiş olmasıdır. Nitekim Anayasa Mahkemesi 5429 sayılı Türkiye İstatistik Kanununun 8. Maddesinin birinci fıkrasını, istatistik kurumunun hakkın özüne dokunacak şekilde sınırsız veri toplama yetkisi veren ve kişilerin de buna uymak mecburiyeti getirdiği gerekçesiyle iptal etmiştir¹⁸⁰.

Yukarıda da belirttiğimiz üzere kanaatimizce kişisel verinin kaydedilmesinin hukuka uygun sayılabilmesi için, bu konuda yetkili makama kanun tarafından verilmiş açık bir yetkinin olması gerekir. Kanun tarafından verilmiş açık bir yetki olmadan kişisel verileri kaydetmek, TCK'nın 135. maddesinde düzenlenen suç oluşturacaktır (Yaşar vd, 2010: s. 4118-4119).

Diğer taraftan kanunla verilen veri toplama yetkisinin, veri toplayan veya kaydeden kişi veya kurumun görevi kapsamı ve sınırları dâhilinde yapılması gerekmektedir. Bu kapsamda kolluk görevlilerinin suç önlenmesi görevi kapsamında suçla ilgili verileri, istihbarat birimleri de istihbarat görevi kapsamında sadece görev alanları dâhilindeki kişisel verileri işleyebileceklerdir. Ancak kanunla verilen görevin sınırları aşılararak kişisel veriler işlenmiş ise, bu durumda kanun hükmünü ifadan söz edilmeyecek ve görevli eyleminden dolayı sorumlu tutulacaktır (Bakıcı, 2008: s. 544).

Son olarak kişisel verilerin kaydedilmesini düzenleyen 135. Maddeinin ikinci fıkrasından da bahsetmek gerekir. 135. maddenin ikinci fıkrasına göre kişilerin

¹⁸⁰ Bkz. Anayasa Mahkemesi'nin 20/3/2008 tarihli ve E.: 2006/167, K.: 2008/86 sayılı Kararı.

siyasi, felsefi veya dini görüşlerine, ırki kökenlerine ilişkin verilerin kişisel veri olarak kaydedilmesi mutlak olarak yasaklandığından (Parlar ve Hatipoğlu, 2008. S. 2045; Özbek vd, 2013: s. 529; Hafizoğulları ve Özen, 2011: s. 269), burada bu bilgilerin kanunun verdiği veri toplama yetkisi dâhilinde toplanıp toplanamayacağı hususu doktrinde tartışma konusu olmuştur¹⁸¹.

Kanaatimizce buradaki sorun, Anayasada kişisel verilerin korunmasına ilişkin düzenlemelerin yetersiz oluşu ve kişisel verilerin korunması alanını bütüncül bir şekilde düzenleyen kişisel verilerin korunmasına ilişkin bir kanununumuz olmadığından kaynaklanmaktadır. Zira TCK'da kişilerin siyasi, dini ve felsefi görüşleri ile ırki kökenlerine ilişkin bilgilerin kişisel veri olarak kaydedilmesi her halde cezalandırılan bir eylem olarak düzenlenmiştir.

Bu konuda yukarıda tartışıldığı için tekrar üzerinde durulmayacaktır.

2.3.4.2.3. Bir Sözleşmenin İfası İçin Gerekli Olma

Bu hukuka uygunluk nedeni, TCK'da düzenlenmemiştir. Ancak AB'nin 95/46/EC sayılı Direktifinde ve Kişisel Verilerin Korunması Kanunu Tasarısında veri işlemeyi hukuka uygun kılan nedenler arasında sayılmıştır. Her ne kadar, sözleşmeler genel de rıza beyanı içerse de, kişisel verilerin işlenmesi açısından bu hususun ayrı değerlendirilmesinde fayda bulunmaktadır. Zira bazen kişinin rızası olmasa da sözleşmenin ifası için gerekli olması nedeniyle kişinin verileri kaydedilebilmektedir. Daha doğru bir deyimle, kişi esasında rızası olmasa bile sözleşmenin kurulması ve ifası için gerekli olduğundan verilerinin işlenmesine rıza göstermek zorunda kalmaktadır.

Bunun için veri işlemenin bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması gerekir. Örneğin; sözleşme gereği ödemenin yapılması için banka hesap numarasının alınması, mal teslimi için adresin alınması, bir çalışanın maaşının yatırılması için banka hesap numarasının ve iletişim bilgilerinin alınması,

¹⁸¹ Küzeci, kişinin rızasının eylemi hukuka uygun hale getireceğinden, burada madde metnine rızası haricinde ibaresinin eklenmesini önermiştir. **Küzeci**, 2010: s. 289; Ketizmen ise, buradaki sorunun maddenin Fransız Ceza Kanunundan iktibas edilmiş olması nedeniyle yaşandığını, zira Fransada Ceza Kanunundaki düzenleme haricinde kişisesel verilerin korunmasına dair kanun olduğunu, hukuka uygunluk hallerinin bu kanuna bakılarak çözülebildiğini, ancak Türkiyede kişisel verilerin korunmasına ilişkin müstakil bir kanun olmadığından TCK'daki bu maddenin eksik hüküm olduğunu belirtmiştir. **Ketizmen**, 2008: s. 235

kredi sözleşmesi için kişinin sahip olduğu mal varlığının belgeleriyle birlikte alınması, ayrıca adli sicil kaydının istenmesi, sözleşme yapmadan önce sözleşme yapacağı kişi ya da şirketin mali ve idari durumu, çalışanları, alacakları, borçlarıyla ilgili bilgilerin alınması gibi.

2.3.4.2.4. Bir Hakkın Tesisi ve Kullanılması İçin Zorunlu olma

Kişinin bir hakkının kullanması hukuka uygunluk nedenidir. Hukuk düzeni bir kimseye belirli bir hakkı kullanma yetkisi verirken, o hakkın icrası fiillerini de hukuka uygun saymaktadır. TCK'nın 26. Maddesinin birinci fıkrasında “hakkını kullanan kimseye ceza verilmez.” Hükmüne yer verilmek suretiyle, hakkın kullanılması hukuka uygunluk nedenleri arasında düzenlenmiştir (Özgenç, 2012: s. 287-288, Bakıcı, 2008: s. 578). Ayrıca bu hukuka uygunluk nedeni AB'nin 95/46/EC sayılı Direktifinde ve Kişisel Verilerin Korunması Kanunu Tasarısındada düzenlenmiştir.

Hukuk düzeni bir kimseye belirli bir hakkı vermekle; o hakkın icra edilmesini de hukuka uygun saymış olmaktadır. Bu bakımdan o hakkın kullanılması, başkalarının menfaatleriyle çatışsa dahi hukuk, hakkını kullanan kimsenin eylemine üstünlük tanıyıp onun icrasını korumaktadır (Artuk vd, Genel Hükümler, 2013: s. 396).

Hakkın icrası niteliğinde olan hukuka uygunluk sebeplerine ilişkin mevzuatımızda birçok düzenleme bulunmaktadır. Bir iş, meslek, sanat, bilim veya spor faaliyetlerinin icrası hakkı, savunma hakkı, şikâyet hakkı, bir insan hakkı olarak düşünce hürriyeti vs. hakkın icrasına örnek olarak gösterilebilir.

Kişisel verilerin kaydedilmesi suçu açısından bakıldığında, eğer bir hakkın kullanılması açısından verileri kaydetmek zorunlu ise, bu durumda suç oluşmayacaktır. Örneğin, Anayasanın 74. Maddesiyle kişilere tanınan dilekçe hakkı ve bilgi edinme hakkı kapsamında verilerin kaydedilmesi, 5187 sayılı Basın Kanununa uygun olarak; basın, yayın ve haber verme hakkı kapsamında veri kaydedilmesi, TCK'nın 128. Maddesinde düzenlenen iddia ve savunma hakkının kullanılması amacıyla veri kaydedilmesi ve bu verilerin bu amaçla kullanılması hallerinde eylem hukuka uygun sayılacaktır (Özn, 2009: s. 17; Bakıcı, 2008: s. 580).

2.3.4.2.5. Hukuki Yükümlüğün Yerine Getirilmesi

Bu hukuka uygunluk nedeni de, TCK'da düzenlenmemiştir. Ancak AB'nin 95/46/EC sayılı Direktifinde ve Kişisel Verilerin Korunması Kanunu Tasarısında veri işlemeyi hukuka uygun kılan nedenler arasında sayılmıştır. Buna göre kişisel verilerin veri işleyenler tarafından tabi oldukları mevzuat çerçevesinde işlenmeleri durumunda işleme eylemi hukuka uygun olacaktır. Bu hukuka uygunluk nedeni daha çok vergi hukuku ve iş ve sosyal güvenlik hukuku kapsamında gündeme gelebilmektedir (Başalp, 2004: s. 41; Uygun, 2010: s. 58). Örneğin, çalışmanın ilgili kısmında da belirtildiği üzere, İş Kanunun 75. Maddesi gereğince işçinin özlük dosyasının tutulması, işçinin sosyal güvenlik primlerinin yatırılması için işçinin iş ilişkisine dair tüm verilerin tutulması, belli oranda hükümlü çalıştırma zorunluluğu olan kurum veya kuruluşların işçilerin mahkûmiyet kayıtlarını tutmaları, vergi indiriminden yararlanan sakat bir kişinin sakatlığına ilişkin bilgilerin ilgili kurum tarafından kaydedilmesi bu kapsamda değerlendirilebilir. Esasında bu hukuka uygunluk nedeni genellikle kanundaki düzenlemelerden kaynaklanmaktadır. Bu nedenle bu hallerde kanun hükmünün yerine getirilmesi hukuka uygunluk nedeni de düşünülebilir.

2.3.4.2.6. Zorunluluk Hali

İlgili kişinin rızasını açıklayamayacak durumda olması halinde kendisinin veya başkasının hayatını veya beden bütünlüğünü korumak amacıyla kişisel verilerin kaydedilmesi halinde de verilerin işlenmesi hukuka uygun olacaktır. Bu hukuka uygunluk nedeni, AB'nin 95/46/EC sayılı Direktifinde ve Kişisel Verilerin Korunması Kanunu Tasarısında veri işlemeyi hukuka uygun kılan nedenler arasında sayılmıştır. Bu durum Türk Ceza Kanunun genel hükümler kısmında “Kusurluluğu Kaldıran veya Azaltan Nedenler” arasında yer alan “zorunluluk hali” ne de uymaktadır¹⁸². Her ne kadar TCK sistematığına göre, bu neden kusurluluğu kaldıran

¹⁸² Zorunluluk hali TCK'nın 25. Maddesinin ikinci fıkrasında düzenlenmiştir. Fıkra metni şöyledir:

“(2) Gerek kendisine gerek başkasına ait bir hakka yönelik olup, bilerek neden olmadığı ve başka suretle korunmak olanağı bulunmayan ağır ve muhakkak bir tehlikeden kurtulmak veya başkasını kurtarmak zorunluluğu ile ve tehlikenin ağırlığı ile konu ve kullanılan vasıta arasında orantı bulunmak koşulu ile işlenen fiillerden dolayı faile ceza verilmez.” Ayrıntılı bilgi için bkz. **Artuk/Gökçen/Yenidünya**, Genel Hükümler, 2013: s. 459

bir neden olarak kabul edilmiş ise de burada kişisel verilere karşı işlenen suçlarda hukuka uygunluk nedeni olarak kabul edilmiştir.

Bu hukuka uygunluk sebebi; bir kişinin zorunluluk hali için aranan tehlike durumuyla karşılaşması halinde, kendisinin ya da başkasının kişisel verisinin, bu tehlikeden kurtulmak için gerekli olması durumunda söz konusu olabilir (Akdağ, 2013: s. 137).

Kişisel verisi işlenmek zorunda olan kişinin, rıza göstermesinin mümkün olduğu ve bu rızayı şartlara uygun şekilde gösterdiği durumlarda, doğal olarak zorunluluk halinden doğan hukuka uygunluk nedeni gündeme gelebilecektir. Ancak bunun mümkün olmadığı durumların ortaya çıkması da mümkündür. Örneğin; kaçırılan kişinin yerinin belirlenmesi için telefon sinyali bilgilerinin tespiti, komadaki bir kişinin ameliyat edilmesi için daha önceki sağlık öz geçmişine ilişkin verilerin kaydedilmesi durumlarında hukuka aykırı bir eylemden bahsetmek mümkün değildir. Hatta başka bir kişinin hayatının kurtarılması için de bu verilerin kaydedilmesi durumunda da bu hal söz konusu olabilir. Bu durumda üçüncü bir kişinin yaşam hakkına yönelik ağır ve mevcut bir tehlikenin varlığı nedeniyle zorunluluk halinin tehlikeye ilişkin şartları da gerçekleşmiş olacaktır (Akdağ, 2013: s. 138).

Bu hukuka uygunluk nedeninde ilgili kişinin yaşam hakkına karşılık, diğer bir kişinin özel hayatının gizliliği hakkından feragat edilmektedir. Dolayısıyla, zaruret halinin savunmaya ilişkin şartları da olayda gerçekleşmektedir (Akdağ, 2013: s. 138).

2.4. Suçun Özel Görünüş Halleri

2.4.1. Teşebbüs

Söz konusu suçun teşebbüse elverişli olup olmadığı konusunda doktrinde görüş birliği yoktur. Bazı yazarlara göre suç, suç neticesi harekete bitişik olduğundan kişisel verilerin hukuka aykırı kaydedilmesiyle tamamlanır ve suç bu yönüyle kural olarak teşebbüse elverişli değildir (Özbek vd, 2013: s. 537). Nitekim verilerin ele geçirilmiş ancak henüz kaydedilmemiş olması durumunda da teşebbüsten söz etmek mümkün değildir. Zira verileri hukuka aykırı olarak ele geçirme de ayrıca suç olarak düzenlenmiş bulunmaktadır (bkz. TCK m. 136, Özbek vd, 2011: s. 526).

Diğer bir kısım yazarlar ise suçun teşebbüse elverişli olduğunu ileri sürmüşlerdir. Bu yazarlara göre, TCK'nın 135. maddesinde düzenlenen kişisel verilerin kaydedilmesi suçunun tamamlanması için, mağdurun herhangi bir zarara uğramasına gerek yoktur. Bu nedenle suç, sırf hareket suçu olduğundan hareketlerin bölünebildiği oranda teşebbüse elverişlidir. Örneğin, bir failin mağdur hakkında kişisel verileri depolamaya başladığı anda yakalanması durumunda eylem teşebbüs aşamasında kalmış olacaktır (Yaşar vd, 2010: s. 4122; Hafızoğulları ve Özen, 2011: s. 277; Parlar ve Hatipoğlu, 2008: s. 2045).

Kanaatimizce, suç kural olarak teşebbüse elverişlidir. Her ne kadar suç sırf hareket suçu olsa ve hareketin yapıldığı anda tamamlansa da hareketlerin bölünme imkânı olduğu müddetçe teorik olarak teşebbüse elverişli olduğunu söylemek mümkündür. Ancak uygulamada suçun teşebbüs aşamada kalmış haline rastlamak pek mümkün gözükmemektedir.

2.4.2. İştirak

Bu suça iştirakin her türlü mümkünüdür. Madde metninde iştirakle ilgili özel bir hüküm yer almamaktadır. Bu nedenle, genel hükümler uygulanacaktır (Yaşar vd, 2010: s. 4122; Parlar ve Hatipoğlu, 2008: s. 2045).

2.4.3. İçtima

Kişisel verilerin kaydedilmesi suçu, aynı suç işleme kararının icrası kapsamında olmak üzere aynı kişiye karşı birden fazla defa işlenmesi halinde, zincirleme suç hükümleri uygulanacaktır. Ayrıca, tek bir hareketle birden fazla kimsenin kişisel verilerin kaydedilmesi halinde de, zincirleme suç hükümleri uygulanacaktır¹⁸³.

Hukuka aykırı olarak kaydedilen verilerin daha sonra, bir başkasına verilmesi veya yayılması söz konusu ise 136. Maddedeki suç ta ayrıca oluşacağından, gerçek içtima hükümleri uygulanarak her iki suçtan ayrı ayrı ceza verilmesi gerekir. Kaydedilen bu verilerin ifşa edilmesi durumunda hakaret suçu da oluşuyorsa, yine gerçek içtima kuralları uygulanmalıdır (Parlar ve Hatipoğlu, 2008: s. 2046).

¹⁸³ Yaşar vd, 2010: s. 4122; Malkoç ise, verilerin ait olduğu kişi sayısının suç oluşacağını belirtmiştir. Bkz. Malkoç, 2013: s. 912

Benzer şekilde failin, maddenin ikinci fıkrasında sayılan hususlara ilişkin bilgileri kişisel verileri kaydetmesinin yanı sıra, ayrımcılık amacıyla 122. maddede sayılan biçimde kişileri bazı temel hak ve özgürlüklerinden yoksun kılma fiillerini de işlenmesi durumunda, 135/2 ve 122. maddede tanımlanan iki ayrı suç oluşacaktır.

Öte yandan, fail hukuka aykırı olarak kişisel veriyi kaydetmek ile başkasına vermek ya da yaymak fiillerini aynı anda gerçekleştirebilir. Örneğin, kişisel verinin ulaşılabilir bir internet sitesine kaydedilmesi ile aynı zamanda yaymak fiili de gerçekleşmiş olur. Kişisel verileri hukuka aykırı olarak yaymak fiili, 136. maddede ayrı bir suç olarak düzenlenmiş olduğundan, bu durumda fikri içtima hükmü gereği daha ağır cezayı gerektiren 136. madde uygulanmalıdır. Zira bu durumda verileri kaydetmenin haksızlık içeriği verileri yayma fiilinin haksızlık içeriğinde erimektedir (Özbek vd, 2013: s. 537; Özen, 2009: s. 19).

3. VERİLERİ HUKUKA AYKIRI OLARAK VERME VEYA ELE GEÇİRME SUÇU

3.1. Genel Olarak

TCK' nun 136. maddesinde kişisel verileri hukuka aykırı olarak başkasına vermek, yaymak ve ele geçirmek suçu düzenlenmiştir. Madde metni; “*Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır.*” şeklindedir¹⁸⁴.

Maddede öngörülen hapis cezasının alt sınırı, 6 Mart 2014 tarihinde yürürlüğe giren 21/2/2014 tarihli ve 6526 sayılı Terörle Mücadele Kanunu ve Ceza Muhakemesi Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun ile artırılarak bir yıldan iki yıla çıkarılmıştır. Değişiklik Anayasanın 20 nci maddesinde düzenlenen kişisel verilerin korunması hakkının ve özel hayatın gizliğinin daha etkin korunması amacıyla yapılmıştır¹⁸⁵.

Maddeyle, bir şekilde elde edilmiş veya kaydedilmiş kişisel verileri başkalarına vermek, yaymak veya bu verileri ele geçirmek fiilleri suç sayılmıştır.

¹⁸⁴ Madde başlığının “Yayma” eylemini kapsamaması nedeniyle, madde gerekçesi de yetersiz olması nedeniyle bazı yazarlar tarafından eleştirilmiştir. Bkz. **Hafızoğulları ve Özen**, 2011: s. 278

¹⁸⁵ Değişiklik gerekçesi için bkz.

http://www.tbmm.gov.tr/develop/owa/tasari_teklif_sd.onerge_bilgileri?kanunlar_sira_no=148569

Erişim T: 10/5/2014

Verme, yayma ve ele geçirmek eylemleri açısından söz konusu veriler, hukuka uygun olarak elde edilmiş veya kaydedilmiş olabileceği gibi hukuka aykırı olarak da elde edilmiş veya kaydedilmiş olabilir (Soyaslan, 2006: s. 273; Hakeri, a.g.m).

Kişisel verilerin hukuka aykırı olarak verme ve yayma hareketlerinin yaptırımı bağlanmasındaki amaç, yetkisiz üçüncü kişilere aktarılmasını ve verilerin yetkisiz üçüncü kişilerce ele geçirilmesini önlenmektir. Bu durumda kişisel verileri, daha önceden kaydedilmiş olsun ya da olmasın hukuka aykırı olarak ele geçiren kişi 136. madde hükmünce cezalandırılacaktır (Küzeci, 2010: s. 291; Ketizmen, 2008: s. 240).

Bu husus madde gerekçesinde de *“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”* şeklinde ifade edilmiştir.

136. maddede yer alan düzenleme kişisel verilerin korunmasını sağlayıcı bir nitelikte olup çok önemlidir. Zira verilerin hukuka aykırı olarak ele geçirilmesi, başkalarına verilmesi veya yayılmasında, kaydetme suçuna nazaran kişi daha büyük zararlara uğrayabilmektedir. Bu suçla kişinin özel hayatının gizliğinin ihlalinin yanında, kişi; şantaja maruz kalabilme, verilerinin herkes tarafından öğrenilebilecek olması nedeniyle toplumda küçük düşme, onurunun kırılması, itibarının zedelenmesi veya ayrımcılığa uğrama gibi ağır nitelikli zararlara da karşılaşabilmektedir.

Diğer taraftan madde metninin düzenleniş biçimi bazı yazarlar tarafından eleştirilmiştir (Özen, 2009: s. 20). Bizimde katıldığımız bu görüşe göre, madde metninde “yayma” fiili düzenlenmişken madde başlığında bu fiilden bahsedilmemesi nedeniyle suçun düzenleniş şekli ile madde başlığı, kanun yapma tekniği açısından, birbirine uyumlu değildir.

Bununla ilgili başka bir husus, maddenin konusu kişisel veriler olduğu halde madde başlığında “veriler” kelimesine yer verilmesidir. Veri ve kişisel veri kavramlarının farklı anlamlara gelmesi nedeniyle, bu düzenleme doğru olmamıştır. Bu nedenlerle madde metninin düzeltilmesi kanun yapım tekniği açısından faydalı olacaktır.

3.2. Korunan Hukuki Yarar

Bu suçla korunan hukuki yarar, özel hayatın gizliğı ve kişisel verilerin korunmasına ilişkin ferdi-toplumsal yarardır. Korunan hukuku değeri, kişisel verilerin kaydedilmesi suçu ile aynıdır. Bu suçu diğer suçlardan, suçun işleniş biçimi ayırmaktadır¹⁸⁶. Bu nedenle korunan hukuki değeri ile ilgili “kişisel verilerin kaydedilmesi suçu” altında yapılan açıklamalar bu suç açısından da geçerlidir.

3.3. Suçun Unsurları

Kişisel verilerin kaydedilmesi suçu incelenirken TCK sistematığında suçun unsurların nelerden ibaret olduğu hususunda doktrinde görüş birliğı bulunmadığını, ancak hukukumuzda genellikle suçun dört unsurunun bulunduğu kabul edildiğini, bunların da; tipiklik, maddi unsurlar, manevi unsur ve hukuka aykırılık unsurları olduğunu belirtmiştik. Bu suç açısından da aynı unsurlar çerçevesinde inceleme yapılacaktır.

3.3.1. Tipiklik

Tipikliğin, doktrinde, suç sayılan fiilin ceza normundaki soyut tasviri olarak tanımlandığı, tipiklik unsuru için öncelikle bir fiili suç sayan ve buna bir yaptırım öngörmüş bulunan bir kanun maddesinin var olması gerektiğini bir önceki suçun açıklamalarında izah etmiştik.

Bu açıklamalar çerçevesinde TCK’nın 136. maddesine tipiklik unsuru için bakıldığında; madde metninde, “*Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi*” nin cezalandırılacağı belirtildiğine göre, tipiklik unsuru açısından aranan husus, failin kişisel verileri, hukuka aykırı olarak bir başkasına vermesi, yayması veya ele geçirmesidir. Madde metninde kişisel veriler için bir tasnif veya sınırlandırma yapılmadığı için her türlü kişisel veriye karşı bu suç işlenebilecektir. Faili maddede sayılan şekilde hareket etmiş ise fiili tipik sayılacak ve suçun tipiklik unsuru gerçekleşecektir.

¹⁸⁶ **Hafizoğulları ve Özen**, 2011: s. 279; Bir kısım yazarlar, bu suçta korunan hukuki değeri sadece kişinin özel hayatının gizliliğı olduğunu savunmuşlarsa da, biz bu görüşlere katılmıyoruz. Bu görüşler için bkz. **Parlar ve Hatipoğlu**, 2007: s. 1043-1044; **Özbek vd**, 2013: s. 538

Tipiklik unsuru suçun nitelikli halleri açısından da arandığından (Artuk vd, Genel Hükümler, 2013: s. 204), 137. maddede bu suç için uygulanacağı belirtilen ağırlaştırıcı nedenin uygulanabilmesi içinde fiilin tipik olması gerekmektedir.

3.3.2. Maddi Unsurlar

3.3.2.1. Suçun Konusu

Suçun konusu “kişisel verilerin kaydedilmesi” suçunda ayrıntılı olarak izah edildiği üzere “kişisel veri” dir (Özbek vd, 2013: s. 538; Parlar ve Hatipoğlu, 2008. S. 2043; Yaşar vd, 2010: s. 4117). Kişisel veri kavramı, 5237 sayılı TCK ile hukuk sistemimize girmiştir ve TCK’nın 135. maddesinin gerekçesinde “*gerçek kişi ile ilgili her türlü bilgi*” olarak tanımlanmıştır.

Bu açıdan madde başlığında ve metninde kullanılan “veri” kelimesi isabetli olmamıştır. Kanaatimizce suçun konusu kişisel veri olduğuna göre, kanunilik ilkesi gereği madde metninde de kişisel veri ibaresinin kullanılması gerekmektedir.

Kişisel verilerin kaydedilmesi suçunda suçun konusu başlığı altındaki açıklamalar bu suç içinde geçerlidir. Bu nedenle kavramın kapsamı ve tartışmalı hususlar için önceki açıklamalara bakılmalıdır.

3.3.2.2. Fail ve Mağdur

Madde metninde “*Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi*” ibaresine yer verildiği için bu suçun faili herkes olabilir (Hafizoğulları ve Özen, 2011: s. 278; Parlar ve Hatipoğlu, 2008: s. 2048). Suçun bir kamu görevlisi tarafından işlenmiş olması cezayı artıran bir nitelikli hal olarak kabul edilmiştir (m. 137/1- a). Diğer taraftan verme ve yayma suçları açısından bu suçun faili, verileri bir şekilde uhdesinde veya sorumluluğunda bulunduran, verilere hâkim olan kimsedir (Soyaslan, 2006: s. 273).

Tüzel kişiler bu suçun faili olamazlar. Ancak TCK’nın 140. maddesindeki şartlar gerçekleştiğinde, tüzel kişilik hakkında güvenlik tedbiri uygulanabilecektir.

Bu suçun mağduru da herkes olabilir (Özbek vd, 2013: s. 538). Tabii ki burada kastedilen gerçek kişilerdir. Bir önceki suçta açıklandığı üzere, tüzel kişiler

bu suçun mağduru olamazlar¹⁸⁷.

3.3.2.3. Hareket ve Netice

Madde metninde, kişisel verileri bir başkasına verme, yayma ve ele geçirme eylemleri, suç olarak düzenlenmiştir. Bu yapısından ötürü, suç, seçimlik hareketli bir suçtur. İster hareketin biri, ister birkaçı birlikte yapılsın, birden çok suç oluşmaz, bir tek suç olur. Tabii, ceza tayin edilirken, bu husus göz önünde tutulacaktır (Hafizoğulları ve Özen, 2011: s. 279).

Maddede sayılan eylemler, kişisel verileri hukuka aykırı olarak; “*bir başkasına vermek*”, “*yaymak*” veya “*ele geçirmek*” tir.

Vermek, sözlük anlamı itibariyle, üzerinde, elinde veya yakınında olan bir şeyi birisine iletmek, eriştirmektir (Türkçe Sözlük, 2011: s. 2088). Vermek eylemini yapabilmek için verilerin failin elinde veya uhdesinde bulundurulması gerekir. Kuşkusuz ancak elde bulundurulmuş şey bir başkasına verilebilir. Buna göre vermek, iki kişi arasındaki bir eylemi ifade eder (Hafizoğulları ve Özen, 2011: s. 279).

Yaymak, sözlük anlamı itibariyle, bir şeyi birçok kimseye duyurmaktır. Kişisel verilerin korunması açısından ise yaymak, verilerin içeriğinin birçok kişinin öğrenebileceği şekilde başkalarının bilgisine sunulması, duyurulmasıdır. Yaymak fiili birden fazla kişiyi hedeflemektedir¹⁸⁸. Nitekim, “mağdura ait telefon numaralarının bir internet sitesinde verilen ilanda yayımlanması” eylemi Yargıtay kararına da konu olmuştur¹⁸⁹.

¹⁸⁷ **Hafizoğulları ve Özen**, 2011: s. 279; Özen ise tüzel kişilerin de bu suçun mağduru olabileceğini savunmuştur. Bkz. **Özen**, 2009: s. 22

¹⁸⁸ **Özbek vd**, 2013, s. 539; Benzer tanım için bkz. **Hafizoğulları ve Özen**, 2011: s. 280; **Soyaslan**, 2006: s. 273

¹⁸⁹ Bkz. Yargıtay 4. CD'nin 13.12.2010 tarih ve 2010/19559 E., 2010/20604 K. sayılı kararı: "Sanığın, cano6006@mynet.com elektronik posta adresini kullanarak mağdur adına bir internet sitesine verdiği ilanda, **mağdura ait olduğu anlaşılan telefon numaralarını yayımlayarak TCK'nun 136. maddesinde tanımlanan kişisel verileri hukuka aykırı şekilde yaymak suçunu işlediği iddiasıyla açılan davada**; mağdura ait kişisel verileri içeren elektronik posta gönderisinin, sanığa ait internet kafeden gönderildiğinin IP adresi ile tespit edilmesi, aynı elektronik posta adresi hesabının oluşturulması sırasında elektronik posta hizmeti veren şirkete beyan edilen bilgilerin de doğru olmadığının anlaşılması karşısında; elektronik posta adresi oluşturulurken kullanılan İP adresinin ve bu adresi kullanan kişinin, elektronik posta adresinin aktive edilmesi için mynet adlı internet sitesinin yedek elektronik posta adresi isteyip istemediğinin, istemişse bu adresin ne olduğu, hangi IP adresini kullandığı ve sahibinin kim olduğu cano6006@mynet.com adındaki elektronik posta adresinin gerçek kullanıcısının, gerekirse bu adresten elektronik posta alan kişiler

Vermek ve yaymak esasen verileri bir başkasına aktarmaktır ve aynı amaca hizmet etmektedir. Burada özellikle internet gibi sanal bir ağ üzerinde ya da haberleşme aracı kullanmak suretiyle iki ya da birden fazla kullanıcı arasında bir teati söz konusudur. Ancak vermek iki kişi arasındaki bir eylemi ifade eder. Bu yönüyle yaymak fiilinden ayrılır. Suç seçimlik hareketli olarak düzenlendiğinden ve suç tipinde yer alan hareketlerden birinin yapılması yeterli olduğundan hem vermek hem de yaymak hareketleri gerçekleştirilmiş olsa da iki ayrı suçun değil tek bir suçun var olduğu kabul edilmelidir. Öte yandan yaymak, kural olarak vermeyi de içine alabilir. Sonuç olarak vermek, verinin, yaymak niteliği taşımayacak bir şekilde, bir başka kişiye aktarılması şeklinde kabul edilmelidir (Özbek vd, 2013: s. 539).

Örneğin, 5352 sayılı Adli Sicil Kanunu'nun 7. maddesinde “adli sicil bilgileri verilebilecek olanlar” ve 8. maddesinde “adli sicil bilgilerini verebilecek merciler” açıkça gösterilmiş, 11. maddesinde ise, adli sicil ve arşiv bilgilerinin gizli olduğu, bu bilgilerin görevlilerce açıklanamayacağı ve bu kanun hükümlerine göre verilen kişi, kurum ve kuruluşlarca veriliş amacı dışında kullanılamayacağı hükme bağlanmıştır. Bu kapsamda adli sicil ve arşiv bilgilerini 7. maddeye aykırı olarak, örneğin özel bir kuruluşa veya ilgilinin vekili olmayan kişilere veren görevlinin eylemi ya da bu bilgileri verme yetkisi olmayan bir görevlinin bir başkasına verme eylemi, bu bilgileri veriliş amacı dışında kullanarak yayan kimsenin eylemi veya bu bilgileri başkaca hukuka aykırı bir eylemle (örneğin muhafaza edildiği yerden çalarak) ele geçiren kimsenin eylemi, bu suçu oluşturacaktır (Parlar ve Hatipoğlu, 2008: 2049; Özen, 2009: s. 20).

Benzer şekilde CMK'nın 80. maddesinin 1. fıkrası hükmüne göre, CMK'nun 75, 76 ve 78. madde hükümlerine göre şüpheli ya da 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 yapılması sonucu elde edilen veriler “kişisel veri” niteliğinde olduğundan bunlar başka bir amaçla kullanılamaz, dosya içeriğini öğrenme yetkisine sahip bulunan kişiler

de Telekomünikasyon İletişim Kurumu Başkanlığından sorulup, tespit edilerek dinlenilmek suretiyle belirlenmesinden sonra sanığın hukuki durumunun takdir ve tayini gerekirken eksik inceleme ile beraat kararı verilmesi" yasaya aylandır. Bkz. **Hafizoğulları ve Özen**, 2011: s. 279

tarafından bir başkasına verilemez. Bu hükme aykırı olarak anılan kişisel verileri başkasına veren, yayan veya ele geçiren kişilerin eylemi yine bu suç oluşturacaktır (Parlar ve Hatipoğlu, 2008: 2049).

Diğer taraftan, ister kamu ister özel olsun kurum ve kuruluşların, hukuka uygun şekilde kaydedip bilgisayar ortamlarında muhafaza ettikleri kişisel verileri, örneğin bir hastanenin hastalarına, otellerin, tatil veya gezi şirketlerinin, bankaların, kredili alışveriş yapılan mağazaların veya havayolu şirketlerinin müşterilerine ilişkin kişisel veri kapsamındaki kayıtları hukuka aykırı olarak bir başkasına vermeleri, basın organlarına servis etmeleri durumunda da 136. maddedeki suç oluşacaktır¹⁹⁰.

Yargıtay'da bir kararında¹⁹¹; 5237 sayılı TCK'nın 136/1. maddesinde düzenlenen “Verileri hukuka aykırı olarak verme veya ele geçirme” suçunun belirli veya belirlenebilir bir kişinin nüfus bilgisi, adresi, parmak izi, DNA bilgisi, cinsel eğilimi, sağlık bilgileri, etnik kökeni, siyasi görüşü, felsefi ve dini inancı gibi kişiye ilişkin her türlü bilginin, başkasına verilmesi, yayılması ya da ele geçirilmesi ile oluşacağı tespitinin yaptıktan sonra, *“elektronik mühendisi olan sanığın, teknik servis elemanı olarak çalıştığı sırada, Turgut Özal Tıp Merkezinde oluşturulan Corteks adlı bilgi sistemine girerek, psikiyatri anabilim dalında tedavi gören mağdure hemşirenin muayene bilgilerini okuyup, hastane çalışanlarına ifşa ettiğinin iddia edilmesi karşısında eyleminin 5237 sayılı TCK'nın 136/1. maddesindeki suçu oluşturacağı....”*. na karar vermiştir.

Kişisel verileri verme ve yayma fiilleri, kitle iletişim araçlarıyla yapılabileceği gibi doğrudan bir araç kullanmadan da yapılabilir. Örneğin eylemin bir ilan yada bildiri dağıtılması şeklinde yapılması yaymaya örnek verilebilir (Özen, 2009: s. 21).

¹⁹⁰Yargıtay bir kararında kişisel verilerin üçüncü kişilere aktarılmasını 136. Madde kapsamında değerlendirmiştir. Karar da özetle, “ katılana ait şirkette satış müdürü olarak çalışan sanığınişten ayrılmadan önce kendi şirketini kurup, çalıştığı şirketin müşterilerine ait tüm verileri kendi şirketinde kullanmak üzere hukuka aykırı olarak aktardığı,....., sabit olduğu halde yazılı şekilde hüküm kurulması....” Hususları belirtilmiştir.

¹⁹¹ Yargıtay 12. CD'nin Esas No: 2012/13104 Karar No: 2012/14146 sayılı kararı

Nitekim Yargıtay 26.04.2012 tarihinde verdiği bir kararında¹⁹²; “Gazete muhabiri olan sanığın mağdurla takma isim kullanarak yazmış olduğu kitap hakkında iki kez röportaj yaptığı, daha sonra mağdurun gerçek kimliğini tespit etmek amacıyla araştırma yaparak mağdurun İlköğretim okulunda ingilizce öğretmeni Y.Ç.Y olduğunu tespit ettiği, bu bilgileri Güneş Gazetesi'nin internet sitesinde "Kocasını 300 erkekle nasıl aldattığını kitabında ballandıra ballandıra anlatan kadının izini süren Güneş, insanın kanını donduran bir gerçeğe ulaştı" başlığıyla vererek haber verme sınırlarını aştığı, eyleminin kişisel verileri ele geçirmek ve yaymak suçunu oluşturduğu sabit olduğundan,.....hükümün isteme aykırı olarak onanmasına.....”, karar vermiştir.

Kişisel verileri ele geçirmek ise, başkalarına ait olan veya tasarrufu altında olan verileri kendi tasarruf alanına sokmaktır¹⁹³. Diğer bir deyişle, kişisel verileri bir şekilde elde etmek, uhdesine almaktır. Ele geçirme eylemi fiziki bir dosyanın içindeki belgelerde bulunan verileri elde etmek şeklinde olabileceği gibi, bilgisayar ortamında, özellikle internet üzerinde bulunan kişisel verileri, yine internet üzerinden elde etme şeklinde de gerçekleştirebilir. Bu anlamda ele geçirmek eylemi, kaydetmek şeklinde de tezahür edebilir. Ancak 135. madde kaydetmeyi ayrıca cezalandırdığına göre ele geçirmek ibaresi kaydetme dışında kalan eylemleri içerecek şekilde anlaşılmalıdır (Özbek vd, 2013: s. 539).

Suçun gerçekleşmesi bakımından, verilerin, örneğin bir hekim veya sağlık personeli tarafından bir tek kişiye verilmesi dahi yeterlidir. Herkesin öğrenmesi gerekmemektedir¹⁹⁴.

Bu suç ta sırf hareket suçu olarak düzenlenmiştir. Söz konusu hareketlerin gerçekleştirilmesiyle suç tamamlanmış olur. Diğer bir deyişle suçun tamamlanmış sayılması için kişisel verinin hukuka aykırı olarak verilmesi, yayılması ya da ele geçirilmesi yeterlidir; bundan bir zarar doğması da şart değildir. Ayrıca bu verilerin

¹⁹² Yargıtay 12. CD'nin Esas No: 2011/15721 Karar No: 2012/11074 sayılı kararı

¹⁹³ **Hafizoğulları/Özen**, s. 279; Özen, bu suçun hırsızlık suçuna benzediğini, hırsızlık suçunun özel şekli olduğunu da ifade etmiştir. Bkz. **Özen**, s. 21

¹⁹⁴ Belirtmek gerekir ki, hekimin bu yükümlülüğü kendi ailesi açısından da mevcuttur. Bu sebeple doktorun hastasıyla ilgili kişisel verileri eşi veya çocuklarıyla dahi paylaşmaması gerekir. Bkz. **Mahmutoğlu, Fatih Selami**, “Sır Saklama yükümlülüğü Kapsamında Hastaya Ait kişisel Verileri Hukuka Aykırı Olarak Verme veya Yayma Suçu”, cezahukuku.istanbul.edu.tr/ders-gerecleri/tiphukuku/sir-saklama.docx. E.T: 21.02.2012

kaydedilmesi de gerekmemektedir. Bu nedenle bu suç aynı zamanda tehlike suçudur (Özbek vd, 2013: s. 539).

Fiil gerçekleştirildikten sonra belli bir sürenin geçmesi veya verinin bir süre saklanması şart değildir. Yukarıda da değinildiği üzere suç, verilerin hukuka aykırı olarak verilmesiyle, yayılmasıyla veya ele geçirilmesiyle tamamlanmış olur. Bu yönüyle suç netice bakımından ani bir suçtur (Özbek vd, 2013: s. 539).

Kişisel verileri verme, yayma ve ele geçirme suçu, eylemlerin niteliği gereği ancak icrai hareketle işlenebilir. İhmali hareketle bu suç işlenemeyecektir (Özen, 2009: s. 21).

3.3.3. Manevi Unsur

Bu suç genel kastla işlenebilir. Kast, daha öncede değinildiği üzere, suçun kanuni tanımındaki unsurların bilerek ve isteyerek gerçekleştirilmesidir (TCK m. 21/1, Koca ve Üzülmmez, 2013, s. 144). Bu suç açısından kast, failin başka bir kimsenin kişisel verilerini bir başkasına verdiğini, yaydığını veya ele geçirdiğini bilmesi ve istemesidir (Hafızoğulları ve Özen, 2011: s. 280; Parlar ve Hatipoğlu, 2008: s. 2049; Soyaslan, 2006: s. 273). Saik önemli değildir. Bu suç, taksirle işlenemez (Hafızoğulları ve Özen, 2011: s. 278; Parlar ve Hatipoğlu, 2008: s. 2045; Şen, 2006: s. 601).

Nitekim Yargıtay da bir kararında¹⁹⁵; “Sanık ile katılanın aynı sitede oturduğu ve her ikisinin de site yöneticisi olmak istediği, sanığın arkadaşı olan S.D.’nin sanığa, katılanın kendisini önceki yıllarda dolandırdığını söyleyerek mahkeme ilamını sanığa verdiği; sanığın katılana ait ilamı hukuka aykırı bir yoldan elde etmediği, mahkeme kararlarının aleni olması ve sanığın katılanın site yönetiminde yer almaması gerektiği düşüncesiyle mahkeme ilamını dağıttığını savunması karşısında, kişisel verileri hukuka aykırı olarak ele geçirme veya yayma suçunun manevi unsurunun oluşmadığı gözetilmeden yerinde görülmeyen gerekçeyle hükümlülük kararı verilmesi,...” şeklinde belirterek bu suçun kast olmadan işlenemeyeceğini belirtmiştir.

¹⁹⁵ Yargıtay 4. CD’nin Esas No: 2010/17923, Karar No: 2012/10514 sayılı kararı

Genel kastla işlenebilen suçun kural olarak olası kastla işlenmesi de mümkündür (Özgenç, 2012: s. 237-246; Artuk vd, Genel Hükümler, 2013: s. 300-307). Bu nedenle bazı yazarlar, bu suçun olası kastla da işlenebileceğini savunmuşlardır (Özbek vd, 2013: s. 540). Olası kast, failin neticeyi öngörmesi ancak meydana gelmesi konusunda kayıtsız kalması; meydana gelememesi için çaba sarf etmemesi, neticeyi göze almasıdır (Özgenç, 2012: s. 237-246; Artuk vd, Genel Hükümler, 2013: s. 300-307). Ancak madde metnin de hukuka aykırılık ibaresine yer verilmesi nedeniyle failde hukuka aykırılık bilinci bulunmalıdır. Bu ise, suçun ancak doğrudan kastla işlenebileceğini göstermektedir (Özen, 2009: s. 21). Bu nedenle suçun, olası kastla işlenemeyeceğini düşünmekteyiz.

3.3.4. Hukuka Aykırılık Unsuru

3.3.4.1. Genel olarak

Madde metninde kişisel verilerin hukuka aykırı olarak bir başkasına verilmesi, yayılması veya ele geçirilmesinden söz edilmiş ve hukuka aykırılık ibaresine ayrıca yer verilmiştir (Özbek vd, 2013: s. 540). Hukuka özel aykırılık olarak da ifade edebileceğimiz bu durumla ilgili olarak yukarıda kişisel verilerin kaydedilmesi suçu altındaki açıklamalar bu suç açısından da geçerlidir.

Bu suçun oluşabilmesi için, kişisel verileri verme, yayma veya ele geçirme eylemlerine başak bir hukuk kuralı tarafından izin verilmemiş olması gerekmektedir. Başka bir hukuk kuralı bu eylemlere izin veriyorsa eylem suç teşkil etmeyecektir. Bu kapsamda bu suç için olabilecek hukuka uygunluk nedenlerini de kısaca açıklamak faydalı olacaktır.

3.3.4.2. Hukuka Uygunluk Sebepleri

Madde metnin de ise bu suç için olabilecek hukuka uygunluk nedenlerinden bahsedilmemiştir. Bu nedenle Türk Ceza Kanunun genel hükümler kısmında yer alan ceza sorumluluğu kaldıran veya azaltan nedenler başlığı altında düzenlenen kanun hükmü ve amirin emri, hakkın kullanılması ve ilgilinin rızası, meşru savunma ve zaruret hali, cebir şiddet, korkutma ve tehdit gibi nedenler bu suç açısından da kısmen uygulama olanağı olabilir. Ancak çalışmamızın ilk bölümlerinde belirtildiği üzere, gerek Avrupa Konseyinin 108 nolu Sözleşmesi, gerek Avrupa Birliğinin 95/46/EC sayılı Direktifinde ve bu uluslararası düzenlemelere esas alınarak

hazırlanan Kişisel Verilerin Korunması Kanun Tasarısında, kişisel verilerin işlenmesini hukuka uygun kılan nedenlere yer verilmiştir. Bu nedenlerin bir kısmının TCK'dakilerle uyuştğu da görölmektedir. Bu nedenle uluslararası belgelerdeki düzenlemeler ile TCK ve Tasarıdaki düzenlemeler birlikte değerlendirilerek kişisel verilerin verilmesi, yayılması ve ele geçirilmesini hukuka uygun kılabilcek nedenler aşağıda açıklanmaya çalışılmıştır.

3.3.4.2.1. İlgili Kişinin Rızası

Kişisel verilere karşı işlenen suçlarda hukuka uygunluk sebepleri arasında ilk akla gelen hukuka uygunluk sebebi, TCK'nın 26. Maddesinin ikinci fıkrasında da düzenlenmiş olan "ilgilinin rızasıdır" (Soyaslan, 2006: s. 274; Parlar ve Hatipoğlu, 2008: s. 2049). Gerçekten "rıza" fiili baştan itibaren hukuka uygun hale getirdiği için geçerli bir rızanın varlığı halinde suç oluşmayacaktır.

Verileri hukuka akırı olarak verme, yayma ve ele geçirme suçunda, rıza, tipiklikte yer alan bir unsur olarak belirlenmediğinden ve suç kişinin mutlak surette taarrufta bulunabileceği bir hakka yönelik olduğundan, rıza eylemi hukuka uygun kılacaktır¹⁹⁶.

Örneğin bir cinsel hastalık nedeniyle tedavi olduğu hekime eşcinsel olduğunu açıklayan bir kimsenin bu yönünün hekim tarafından hastanın bilgisi ve rızası ile bir başkasına bildirilmesi durumunda bu suç oluşmayacaktır (Hakeri, a.g.m.).

Kişisel verilerin kaydedilmesi suçunda da belirtildiği üzere, buradaki rızanın Anayasal düzenlememiz gereği açık olması gerekmektedir (m. 20/3). Yani kişinin verileri bir başkasına verilmeden veya yayılmadan önce yapılacak işlem ile ilgili bilgilendirilmesi gerekmektedir. Kişi bu işleme kabul ettiğini açıkça belirtmeli, müsbet bir hareket te bulunmalıdır. Bu nedenle kişisel verilerinin yayılmasına ilişkin zimni rıza eylemi hukuka uygun hale getirmeyecektir.

Mevzuat hükümleri çerçevesinde yapılacak verme veya ele geçirme durumunda ise ilgilinin rızası değil, kanun hükmünün yerine getirilmesi hukuka uygunluk sebebi söz konusu olacaktır. Bu nedenle mevzuata uygun olarak

¹⁹⁶ Keza, Anayasanın 20/3. maddesi ve Kişisel Verilerin Korunması Kanun Tasarısı'nın 5. maddesine göre, kişisel veriler kişinin açık rızasıyla işlenebilir.

gerçekleştirilmeyen verme veya ele geçirmeyi ilgilinin rızası da hukuka uygun hale getirmeyecektir (Özbek vd, 2013: s. 540).

Rızanın geçerlilik şartlarına ilişkin önceki suç için yapılan açıklamalar bu suç açısından da geçerlidir. O yüzden burada üzerinde daha fazla durulmayacaktır.

3.3.4.2.2. Kanun Hükmünün Yerine Getirilmesi

Bu suç bakımından söz konusu olabilecek diğer bir hukuka uygunluk sebebi TCK'nun 24. Maddesinde düzenlenen “kanun hükmünün yerine getirilmesidir (Soyaslan, 2006: s. 274)”. Bu husus ayrıca Anayasanın 20. Maddesinin üçüncü fıkrasında da öngörülmüştür. Anayasaya göre kişisel veriler kanunlarda öngörülen hallerde işlenebilecektir. İşlenme kavramının kişisel verilerin elde edilmesinden kaydedilmesine, üçüncü kişilerle paylaşılmasından silinmesine kadar geçen aşamada veriler üzerinde gerçekleştirilen her türlü eylemi kapsadığını daha önceki bölümlerde belirtmiştik.

Bu kapsamda kamu kurumlarının kanunlarda verilen yetki gereği sistemlerinde kayıtlı kişisel verileri paylaşmaları, bunları yetkili kişi ve kurumlara vermeleri durumunda eylem hukuka uygun olacaktır. Örneğin, kişilerin mahkûmiyet kayıtlarının Adli Sicil Kanunu gereği ilgili kurumlara verilmesi. Yine önleyici kolluk faaliyetleri veya istihbarat faaliyetleri kapsamında kişisel verilerin ele geçirilmesi durumunda, kanunda belirlenen görev dâhilinde ve sınırında ise, kanundan kaynaklanan yetki kullanıldığı için suç oluşmayacaktır.

Yine Umumi Hıfzıssıhha Kanunu (md. 57, 104, 113) gereğince bildirilmesi zorunlu hastalıkların ki bu hastalık kayıtları hassas nitelikte kişisel veriler olabilir, bildirilmesi durumunda bu suç oluşmayacaktır. Keza TCK 279 ve 280. maddeleri çerçevesinde kişisel verilerin verilmesi de hukuka uygun olacaktır. Zira bu maddeler ile sayılan kamu görevlilerine görevleri ile bağlantılı olarak vakıf oldukları suçları ilgili mercilere bildirim yükümlülüğü yüklenmiştir¹⁹⁷.

¹⁹⁷ TCK 279-280. maddelerin gerekçesi için bkz. **Özgenç, İzzet**, Türk Ceza Hukuku Mevzuatı, C. 1, 8. baskı, Ankara, 2012, s. 436; Tıp ve hukuk çevrelerinde sıklıkla dile getirilen Hekimlerin sır saklama yükümlülükleri ile suçu ihbar zorunluluğu hakkında ayrıntılı bilgi için bkz. **Mahmutoğlu**, a.g.m., s. 3

Ayrıca, koruyucu hekimlik, tıbbi teşhis, tedavi, bakım veya sağlık hizmetlerinin yürütülmesi amacıyla kişisel verilerin, sağlık kurumları, sigorta şirketleri, sosyal güvenlik kurumları, işyeri sağlık birimi oluşturmakla yükümlü işverenler, okullar ve üniversiteler tarafından ilgili kanunlara uygun olarak, hukuken veya meslek kurallarına göre sır saklama yükümlülüğü altında bulunan sağlık personeli tarafından işlenmesi de hukuka uygundur¹⁹⁸.

Ancak burada dikkat edilmesi gereken husus yukarıda da belirttiğimiz üzere kanunla verilen yetkinin açık olması ve sınırlarının çizilmiş olmasıdır. Kanaatimizce kişisel verinin kaydedilmesinin hukuka uygun sayılabilmesi için, bu konuda yetkili makama kanun tarafından verilmiş açık bir yetkinin olması gerekir. Kanun tarafından verilmiş açık bir yetki olmadan kişisel verileri vermek, yaymak veya ele geçirmek, 136. Maddedeki suçu oluşturacaktır (Yaşar vd, 2010: s. 4118-4119).

Diğer taraftan kanunla verilen veri toplama yetkisinin, veri toplayan veya kaydeden kişi veya kurumun görevi kapsamı ve sınırları dâhilinde yapılması gerekmektedir. Bu kapsamda kolluk görevlilerinin suç önlenmesi görevi kapsamında suçla ilgili verileri, istihbarat birimleri de istihbarat görevi kapsamında sadece görev alanları dâhilindeki kişisel verileri işleyebileceklerdir. Ancak kanunla verilen görevin sınırları aşılararak kişisel veriler işlenmiş ise, daha açık bir ifade ile örneğin, devletin istihbarat biriminin görevi kapsamında elde ettiği kişisel verileri medya organlarına servis etmesi halinde, bu durumda kanun hükmünü ifadan söz edilmeyecek ve görevli eyleminden dolayı sorumlu tutulacaktır (Bakıcı, 2008: s. 544).

3.3.4.2.3. Zorunluluk Hali

Kişisel verilerin kaydedilmesi suçunda olduğu gibi, bu suçta da ilgili kişinin rızasını açıklayamayacak durumda olması halinde kendisinin veya başkasının hayatını veya beden bütünlüğünü korumak amacıyla kişisel verilerin işlenmesi (verme, yayma veya ele geçirme) halinde, eylem hukuka uygun olacaktır. Bu hukuka uygunluk nedeni, AB'nin 95/46/EC sayılı Direktifinde ve Kişisel Verilerin

¹⁹⁸ **Hakeri, Hakan**, “Hasta Hakları Bakımından Yeni Türk Ceza Kanunu”, http://portal.hakanhakeri.com/index.php?option=com_content&task=view&id=27&Itemid=35. Er. T: 21.02.2012 (16-17 Kasım 2005 tarihlerinde Sağlık Bakanlığı ile Hasta Hakları ve Sağlıklı Yaşam Derneği tarafından Ankara’da düzenlenen „1. Hasta Hakları Ulusal Sempozyumu“nda sunulan bildiridir).

Korunması Kanunu Tasarısında veri işlemeyi hukuka uygun kılan nedenler arasında sayılmıştır. Bu durum Türk Ceza Kanunun genel hükümler kısmında “Kusurluluğu Kaldıran veya Azaltan Nedenler” arasında yer alan “zorunluluk hali” ne de uymaktadır¹⁹⁹. Bu hukuka uygunluk sebebi; bir kişinin zorunluluk hali için aranan tehlike durumuyla karşılaşması halinde, kendisinin ya da başkasının kişisel verisinin, bu tehlikeden kurtulmak için gerekli olması durumunda söz konusu olabilmektedir (Akdağ, 2013: s. 137).

Kişisel verisi işlenmek zorunda olan kişinin, rıza göstermesinin mümkün olduğu ve bu rızayı şartlara uygun şekilde gösterdiği durumlarda, doğal olarak zorunluluk halinden doğan hukuka uygunluk nedeni gündeme gelebilecektir. Ancak bunun mümkün olmadığı durumların ortaya çıkması da mümkündür. Örneğin; kaçırılan kişinin yerinin belirlenmesi için telefon sinyali bilgilerinin tespiti, komadaki bir kişinin ameliyat edilmesi için daha önceki sağlık öz geçmişine ilişkin verilerin kullanılması durumlarında hukuka aykırı bir eylemden bahsetmek mümkün değildir. Hatta başka bir kişinin hayatının kurtarılması için de bu verilerin kullanılması durumunda da bu hal söz konusu olabilir. Bu durumda üçüncü bir kişinin yaşam hakkına yönelik ağır ve mevcut bir tehlikenin varlığı nedeniyle zorunluluk halinin tehlikeye ilişkin şartları da gerçekleşmiş olacaktır (Akdağ, 2013: s. 138).

Bu hukuka uygunluk nedeninde ilgili kişinin yaşam hakkına karşılık, diğer bir kişinin özel hayatının gizliliği hakkından feragat edilmektedir. Dolayısıyla, zaruret halinin savunmaya ilişkin şartları da olayda gerçekleşmektedir (Akdağ, 2013: s. 138).

Böyle bir durumda, kişinin kişisel verilerini başka birine veren kişi cezalandırılmayacaktır. Zira zorunluluk hali durumu, fiili hukuka uygun hale getirir. Normalde bir kişinin cep telefonu vasıtasıyla nerede bulunduğu belirlenmesi ve bu bilginin üçüncü kişilere verilmesi suç olacakken, böyle bir durumda kişinin yaşam hakkının korunabilmesi için zorunlu olan bu hareket, hukuka uygun kabul edilmektedir (Akdağ, 2013: s. 138).

¹⁹⁹ Zorunluluk hali TCK’nın 25. Maddesinin ikinci fıkrasında düzenlenmiştir. Fıkra metni şöyledir:

“(2) Gerek kendisine gerek başkasına ait bir hakka yönelik olup, bilerek neden olmadığı ve başka suretle korunmak olanağı bulunmayan ağır ve muhakkak bir tehlikeden kurtulmak veya başkasını kurtarmak zorunluluğu ile ve tehlikenin ağırlığı ile konu ve kullanılan vasıta arasında orantı bulunmak koşulu ile işlenen fiillerden dolayı faile ceza verilmez.” Ayrıntılı bilgi için bkz. **Artuk vd**, Genel Hükümler, 2013: s. 459

3.3.4.2.4. Bir Sözleşmenin İfası İçin Gerekli Olma

Bu hukuka uygunluk nedeni için kişisel verilerin kaydedilmesi suçu kısmında yapılan açıklamalar bu suç açısından da geçerlidir. Örnek verilecek olursa, iki kişi arasında yapılan bir sözleşmede, sözleşmenin devletin kurumlarını da ilgilendirmesi halinde, sözleşme kapsamında taraflara ait kişisel verilerin devletin ilgili kurumlarına verilmesi halinde veya bir turizm firmasıyla yurt dışı seyahati için anlaşılan kişinin, konaklama ve seyahat bilgilerinin hatta yeme içmeye ilişkin tercihlerini içeren bilgilerin yurt dışındaki seyahat ve konaklama işlerini yürütecek acenteye aktarılması hallerinde, kişisel verilerin verilmesi suçu oluşmayacaktır. Zira burada sözleşmenin ifası, bu verilerin paylaşılması gerekmektedir.

3.3.4.2.5. Bir Hakkın Tesisi ve İcrası İçin Zorunlu olma

AB'nin 95/46/EC sayılı Direktifinde ve Kişisel Verilerin Korunması Kanunu Tasarısında düzenlenmiş olan bu hukuka uygunluk nedeni TCK'nın 26. Maddesinin birinci fıkrasındada düzenlenmiştir. Buna göre “hakkını kullanan kimseye ceza verilmez”

Kişinin bir hakkının kullanması hukuka uygunluk nedenidir. Hukuk düzeni bir kimseye belirli bir hakkı kullanma yetkisi verirken, o hakkın icrası fiillerini de hukuka uygun saymaktadır. (Özgenç vd, 2012: s. 237-238; Bakıcı, 2008: s. 578). Ayrıca hukuk düzeni bir kimseye belirli bir hakkı vermekle; o hakkın icra edilmesini de hukuka uygun saymış olmaktadır. Bu bakımdan o hakkın kullanılması, başkalarının menfaatleriyle çatışsa dahi hukuk, hakkını kullanan kimsenin eylemine üstünlük tanıyıp onun icrasını korumaktadır (Artuk vd, Genel Hükümler, 2013: s. 396).

Hakkın icrası niteliğinde olan hukuka uygunluk sebeplerine ilişkin mevzuatımızda birçok düzenleme bulunmaktadır. Bir iş, meslek, sanat, bilim veya spor faaliyetlerinin icrası hakkı, savunma hakkı, şikâyet hakkı, bir insan hakkı olarak düşünce hürriyeti vs. hakkın icrasına örnek olarak gösterilebilir.

Bu suç açısından değerlendirildiğinde örneğin bir işverenin, belirli teşvik primlerinden ya da vergi indiriminden yararlanabilmesi için yapmış olduğu yatırım

ya da çalıştırdığı personel ile ilgili verileri tutması ve bunları ilgili kamu kurumlarıyla ve vergi dairesiyle paylaşması bu kapsamda değerlendirilecektir.

3.3.4.2.6. Hukuki Yükümlülüğün Yerine Getirilmesi

TCK'da düzenlenmeyen bu hukuka uygunluk nedeni AB'nin 95/46/EC sayılı Direktifinde ve Kişisel Verilerin Korunması Kanunu Tasarısında veri işlemeyi hukuka uygun kılan nedenler arasında sayılmıştır. Buna göre kişisel verilerin, veri işleyenler tarafından tabi oldukları mevzuat çerçevesinde işlenmeleri durumunda işleme eylemi hukuka uygun olacaktır. Bu hukuka uygunluk nedeni daha çok vergi hukuku ve iş ve sosyal güvenlik hukuku kapsamında gündeme gelebilmektedir (Başalp, 2004: s. 41; Uygun, 2010: s. 58).

Örneğin; işçinin maaş ödemesi için mali bilgilerinin ve bakmakla yükümlü olduğu kişilere ilişkin bilgilerinin işveren tarafından ilgili kurumlara verilmesi, halinde işverenin verme eylemi hukuka uygun olacaktır.

3.4. Suçun Özel Görünüş Halleri

3.4.1. Teşebbüs

Bazı yazarlar, söz konusu suçun neticesi harekete bitişik bir suç olduğundan kural olarak teşebbüse elverişli olmadığını, verinin ele geçirilmiş ancak henüz kaydedilmemiş olması durumunda da teşebbüsten söz etmek mümkün olmadığını, zira verileri hukuka aykırı olarak ele geçirmenin de ayrıca suç olarak düzenlenmiş olduğunu savunmuşlardır (Özbek vd, 2011: s. 529).

Kanaatimizce, suç kural olarak teşebbüse elverişlidir. Her ne kadar suç sırf hareket suçu olsa ve hareketin yapıldığı anda tamamlansa da hareketlerin bölünme imkânı olduğu müddetçe teorik olarak teşebbüse elverişli olduğunu söylemek mümkündür. Çünkü örneğin, failin, elinde taşıdığı bir dosyada veya bilgisayar içinde bulundurduğu kişisel verileri hukuka aykırı şekilde bir başkasına vermek üzereyken yakalanması halinde suç teşebbüs aşamasında kalmış olacaktır.

Diğer görüşler için kişisel verileri kaydetme suçu altındaki açıklamalara bakılabilir.

3.4.2. İştirak

Bu suça iştirakin her şekli mümkün görünmektedir. Bu yönüyle iştirak açısından bir özellik göstermemektedir (Parlar ve Hatipoğlu, 2008: s. 2050; Özen, 2009: s. 22).

3.4.3. İçtima

Madde metninde içtima açısından özel bir düzenleme bulunmadığından genel hükümler çerçevesinde değerlendirme yapmak gerekmektedir.

Bu suçun zincirleme suç şeklinde işlenmesi mümkündür. Örneğin, fail aynı anda internet üzerinden birden fazla kişinin kişisel verilerini rızaları dışında veya herhangi bir kanun hükmüne dayanmadan yayınlaması durumunda TCK'nun 43/2 hükmüne göre zincirleme suç hükümleri uygulanabilir.

Öte yandan fail hukuka aykırı olarak kişisel veriyi kaydetme ile başkasına verme ya da yayma fiillerini aynı anda gerçekleştirebilir. Özellikle internet üzerinden yapılan iletişimde bu durum mümkün olabilmektedir. Bu durumda fıkri içtima hükmü gereği en ağır cezayı gerektiren hüküm uygulanmalıdır. Zira bu durumda verileri kaydetmenin fiili verileri yayma fiilinin içinde erimektedir (Özbek vd, 2013: s. 541).

Keza, kişinin özel hayatına ilişkin bir görüntünün ulaşılabilir nitelikte bir internet sitesine kaydedilmek suretiyle herkesin bilgisine sunulması halinde kişisel verilerin yayılması suçunun yanında TCK'nun 134/2 maddesindeki özel hayatın gizliği suçu da oluşacaktır. Bu durumda da fıkri içtima hükümleri gereği cezası daha ağır olan suçtan ceza verilmesi gerekecektir (bkz. TCK'nın 44, 134/2 ve 136. maddeleri).

Diğer yandan, kişiler arasındaki haberleşme içeriklerinin ifşa edilmesi eylemi TCK'nın 132. maddesinin ikinci fıkrasında düzenlenmiştir. İfşa edilen haberleşme içeriklerinin kişisel veriler ihtiva etmesi halinde her iki kanun hükmü de ihlal edilecektir. Ancak burada özel normun önceliği gereği, 132. madde uygulanacaktır. Çünkü ifşa edilen kişisel veriler haberleşmenin gizliği ihlal edilerek elde edilmiştir (Özen, 2009: s. 22).

3.5. Suçun Nitelikli Halleri

Verileri yok etmeme suçu (TCK m. 138) haricinde TCK'nun dokuzuncu bölümünde yer alan özel hayata karşı işlenen tüm suçlar için ortak iki ağırlatıcı sebep öngörülmüştür. Kişisel verilerin kaydedilmesi ve verileri hukuka aykırı olarak verme veya ele geçirme suçları da bu suçlar arasındadır. Buna göre söz konusu suçların; kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle veya belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenmesi halinde ilgili maddeye göre verilecek ceza yarı oranında artırılacaktır (TCK m. 137). Verileri yok etmeme suçu bakımından bu ağırlatıcı nedenlerin uygulanma olanağı bulunmamaktadır.

Bu suçlar bakımından daha az ceza verilmesini öngören herhangi bir neden ise düzenlenmemiştir.

3.5.1. Suçun Kamu Görevlisi Tarafından ve Görevinin Verdiği Yetki Kötüye Kullanılmak Suretiyle İşlenmesi Hali

Bu ağırlatıcı halin uygulanabilmesi için kişinin kamu görevlisi olması yeterli olmayıp; ayrıca suçun görevin verdiği yetkinin kötüye kullanılması suretiyle işlenmesi gerekir. Bu yönüyle suçun kamu görevi sırasında işlenmiş olması gerekmez. Diğer bir deyişle kamu görevliliği sıfatının suçun işlendiği anda bulunması gerekir. Failin suçun işlendiği anda mutlaka iş yerinde veya görev başında olması gerekmez. Ancak hükümde görevin verdiği yetkinin kötüye kullanılmasından söz edildiği için suçun kamu görevi nedeniyle işlenmiş olması ve failin halen kamu görevlisi olması gerekmektedir (Özbek vd, 2013: s. 531; Albayrak, 2012: s. 14; Soyaslan, 2006: s. 274; Parlar ve Hatipoğlu, 2008: s. 2051).

Kamu görevlisi, TCK'nun 6. maddesinde, kamusal faaliyetin yürütülmesine atama veya seçilme yoluyla ya da herhangi bir surette sürekli, geçici veya süreli olarak katılan kişi olarak tanımlanmıştır. Buna göre kamu görevlisi, ücretli, ücretsiz, ihtiyari, mecburi devamlı veya geçici olarak kamu adına bir görev ifa eden kimsedir²⁰⁰.

²⁰⁰ Soyaslan, 2006: s. 274; Kamu görevlisi konusunda geniş bilgi için bkz. Gökcan, Hasan Tahsin/Artuç, Mustafa, Kamu Görevlisi Kavramı ve Özel Soruşturma Usulleri, Seçkin Yayınevi, Ankara 2007, s. 25- 203

Kamusal faaliyet ise TCK'nun 6. maddesinin gerekçesinde, Anayasa ve kanunlarda belirlenmiş olan usullere göre verilmiş olan bir siyasal kararla, bir hizmetin kamu adına yürütülmesi olarak tanımlanmış, bu hizmetin yürütülmesine katılan kişilerin maaş, ücret veya sair bir maddi karşılık alıp almamalarının bir öneminin bulunmadığı, ceza kanunu bakımından idare hukuku anlamındaki kamu görevlisi²⁰¹ yerine daha geniş manadaki kamu görevlisi kavramının nazara alınması gerektiği belirtilmiştir. Buna göre avukatlık, noterlik, tanıklık, bilirkişilik, tercümanlık faaliyetleri kamusal faaliyettir (Özbek vd, 2013: s. 531).

Özetle bir kişinin ceza hukuku anlamında kamu görevlisi sayılması için ayırıcı ölçüt yaptığı faaliyetin kamusal bir faaliyet sayılmasıdır. Bu nedenle, mesleklerinin icrasını yaparken noterler, avukatlar, tanıklar, tercümanlar ve bilirkişilerde kamu görevlisi sayılacaklardır²⁰².

Öte yandan fiilin kamu görevi sırasında işlenmesi mümkün ise de yeterli değildir. Fiilîn ayrıca görevin verdiği yetki kötüye kullanılmak suretiyle işlenmesi gerekir (Özbek vd, 2013: s. 532). Yani verilere ilişkin 135 ve 136. maddelerdeki eylemleri yapmama yükümlülüğü kamu görevlisinin görevi ile ilgili değilse bu hal uygulanmayacaktır (Özen, 2009: s. 23).

Diğer bir anlatımla bu ağırlaştırıcı halin uygulanabilmesi için kamu görevlisinin aynı zamanda bu konuda bir yetkisinin de olmasıdır. Örneğin, kolluk görevlileri, adli görev kapsamında gerektiğinde mahkemeden karar alarak kişilerin özel hayatlarına müdahale edebilmektedirler. Ancak, herhangi bir hukuka uygunluk

²⁰¹ İdare hukukunda ise bir kişinin kamu görevlisi olması için kamu kesimindeki bir kurum veya kuruluşa bağlı olarak çalışması gerekir. Diğer bir deyişle, kamu hizmeti gören herkes kamu görevlisi sayılmaz. Anayasanın 128. maddesinde, Devletin, kamu iktisadi teşebbüsleri ve diğer kamu tüzel kişilerinin genel idare esaslarına göre yürütmekle yükümlü oldukları kamu hizmetlerinin gerektirdiği asli ve sürekli görevlerin, memurlar ve diğer kamu görevlileri eliyle görüleceği belirtilmiştir. Anayasaya göre kamu görevlilerinin ayırt edici niteliği, bunların genel idare esasları göre yürütülen kamu hizmetlerinin gerektirdiği asli ve sürekli görevleri görmeleridir. Böylece idare hukuku anlamında kamu görevlileri, memurlar ve diğer kamu görevlileri olarak kabul edilmiştir. Diğer kamu görevlilerinden maksat, genel idare esaslarına göre yürütülen asli ve sürekli görevleri yerine getiren ve fakat devlet memurlarından ayrı bir personel rejimine tabi tutulmuş bulunan görevlileri ifade etmektedir. Örneğin, hakimler ve savcılar, kamu iktisadi teşebbüsü personeli, Türk Silahlı Kuvvetleri personeli, üniversite Öğretim elemanları devlet memurlarından ayrı bir personel rejimine tabi olmakla, diğer kamu görevlilerini oluşturmaktadır. Bkz. **Özbek vd**, 2013, s. 531; Kamu görevlisi kavramı hakkında ayrıntılı bilgi için bkz. **Günday, Metin**, İdare Hukuku, 8. Baskı, İmaj Yayıncılık, Ankara, 2003, s. 516-527.

²⁰² **Özbek vd**, 2013, s. 531; Benzer görüş için bkz. **Soyaslan**, 2006, s. 274

nedeni olmadan örneğin karakola gelen kişilerin görüntülerinin çekilerek depolanması durumunda, kamu görevlisi yetkisini kötüye kullanarak bu nitelikli hali gerçekleştirmiş olacaktır. Yine örneğin CMK'nın 81. maddesinde “fizik kimliğin tespiti” tedbiri düzenlemekte olup, kişisel veri niteliğinde olan kişinin fotoğrafı, beden ölçüleri, parmak ve avuç içi izi, bedeninde yer almış olup teşhisini kolaylaştıracak diğer özellikleri ile sesi ve görüntülerinin kayda alınabilmesine imkan sağlamaktadır (m.81/1). Ancak bunun için kişinin üst sınırı iki yıl veya daha fazla hapis cezasını gerektiren bir suçtan dolayı şüpheli veya sanık konumunda olması gerekir. İşte kişinin bu nitelikleri taşıyamamasına rağmen söz konusu kişisel verilerinin kaydedilmesi durumunda bu nitelikli hal uygulanabilecektir (Özbek vd, 2013: s. 532).

Bu maddenin uygulanması sırasında kamu görevlisi yetkisini kötüye kullanarak bu eylemi gerçekleştirmiş olması nedeniyle aynı zamanda TCK'nın 257. maddesinde düzenlenen görevi kötüye kullanma suçunun da uygulanması gündeme gelebilecektir. Ancak TCK'nın 257. maddesinde düzenlenen görevi kötüye kullanma suçu genel nitelikte bir suç olup, başka suç oluşturmeyen eylemlerin bu madde kapsamına girmesi nedeniyle, bu durumda TCK'nın 257. maddesi değil, TCK'nın 135, 136 ve 137. maddeleri uygulanacaktır²⁰³.

Nitekim doktrinde bazı yazarlar tarafından 137. maddedeki bu nitelikli halin TCK'nın 257. maddesinde düzenlenen görevi kötüye kullanma suçunun özel bir şekli oluşturduğu belirtilmiştir (Özbek vd, 2013: s. 532). Buna göre kişisel verilerin görevin gereklerine aykırı hareket etmek suretiyle hukuka aykırı bir şekilde kaydedilmesi durumunda bu nitelikli halin uygulanması mümkündür. Ayrıca kişisel verilerin hukuka aykırı olarak kaydedilmesi fiilinin icrai bir hareketle işlenebileceğinden görevinin gereklerini yapmakta ihmal veya gecikme göstererek işlenmesi mümkün değildir²⁰⁴.

²⁰³ **Yaşar vd**, 2010: s. 4121; Özen ise, mevzuya farklı bir açıdan yaklaşmış ve TCK'nın 257. maddesindeki görevi kötüye kullanma suçunun zarar suçu olduğu, kişisel verilerin kaydedilmesi suçlarının tehlike suçları olduğu, bu nedenle burada görevin kötüye kullanılması suçu değil, 135 ve 136. Maddelerle birlikte 137. Maddelerdeki nitelikli hallerin uygulanacağını savunmuştur. Bkz. **Özen**, 2009: s. 23

²⁰⁴ **Özbek vd**, 2011, s. 532; Görevi kötüye kullanma suçu hakkında ayrıntılı bilgi için bkz. **Artuk vd**, Özel Hükümler, 2013, s. 1075-1094

Görevin verdiği yetkinin kötüye kullanılıp kullanılmadığı, hem kamu görevlisinin tabi olduğu mevzuata hem de kişisel verilerin kaydedilmesine ilişkin hüküm içeren mevzuata göre belirlenecektir. Bu bakımdan örneğin, Kişisel Verilerin Korunması Kanun Tasarısı, kişisel verilerin hangi hallerde kaydedilebileceğini açıkça düzenlemektedir. Tasarının kanunlaşması halinde, kamu görevlisinin kişisel verileri bu düzenlemelere aykırı olarak kaydetmesi söz konusu ağırlaştırıcı nedenin uygulanmasını gerektirecektir (Şener, 2011: s. 82). Bunun gibi 2559 sayılı PVSK'nın 5. maddesinde polisin idari kolluk faaliyetleri kapsamında kişilerin parmak izi ve fotoğraflarını alabileceği haller ve bunun usulü düzenlenmiştir. Bu madde kapsamındaki işlemleri yapmakla görevli polis memurunun bu maddeye aykırı olarak kişilerin parmak izi veya fotoğraflarını alması durumunda aynı durum söz konusudur.

Diğer yandan bu ağırlaştırıcı halin uygulanabilmesi için kişisel verilerin 135 ve 136. maddeki şekliyle işlenmesinde bir zararın ortaya çıkmış olması şart değildir. Önemli olan fiilin kamu görevlisinin görevini kötüye kullanmak suretiyle işlemiş olmasıdır (Özbek vd, 2013: s. 532).

Örneğin, kolluk memurunun CMK'nın 129. maddesi uyarınca hâkim kararı veya C.Savcısının emri uyarınca el koyduğu zarfları veya paketleri açma yetkileri olmadığı halde bunları açıp haberleşmenin içeriğini hukuka aykırı olarak öğrenmesi halinde, 132. maddede tanımlanan suçun nitelikli hali söz konusudur. Kolluk görevlisinin, CMK'nın 135. maddesinde belirlenen esas ve usuller dışında bir başkasının telekomünikasyon yoluyla iletişimini dinlemesi ve kayda alması veya kişiler arasındaki haberleşme içeriklerinin kanuna uygun olarak kaydedilmesine karşın bunları hukuka aykırı olarak ifşa etmesi, örneğin bir basın mensubuna verip gazetede yayınlanmasını sağlaması halinde yetkinin kötüye kullanılması söz konusudur. Yine bir bilirkişinin adli makamlarca kendisine tevdi edilen, kişilerin özel hayat alanıyla ilgili ses veya görüntü kayıtlarının içeriğini bir basın muhabirine vermesi halinde 134. ve 136. maddelere uyan suçundan dolayı kamu görevlisi sayılacağı ve bu suçu görevinin verdiği yetkiyi kötüye kullanarak işlediğinden cezası 137. madde uyarınca artırılacaktır (Parlar ve Hatipoğlu, 2008: s. 2052).

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

Bu ağırlaştırıcı nedenin uygulanabilmesi için, kamu görevlisi olmayan failin, 135 ve 136. maddede sayılan suçları, icra etmekte olduğu belli bir meslek veya sanatın sağladığı kolaylıktan yararlanarak işlemiş olması gerekir (Parlar ve Hatipoğlu, 2008: s. 2052).

“Belli bir meslek ve sanatın sağladığı kolaylık” tan ne anlaşılması gerektiği konusunda madde ve gerekçesinde bir açıklama bulunmamaktadır.

Öncelikle ifade etmek gerekir ki hükümde yer alan “ve” ibaresi “veya” olmalıdır. Zira maddedeki “meslek ve sanat” ibaresi, yapılan işin her iki niteliğe de sahip olması gerektiği gibi anlaşılmaktadır. Hâlbuki söz konusu nitelikli halinde uygulanması bakımından yapılan uğraşının hem meslek hem de sanat niteliğinde olması gerekmemekte; bunlardan birinin olması yeterli olmaktadır (Albayarak, 2012: s. 14).

Sözlük anlamı itibariyle ise meslek, bir kimsenin geçimini sağlamak için yaptığı sürekli iştir (Türkçe Sözlük, 2009: s. 1377). Meslek, insanın yaşamını sürdürebilmek için icra ettiği ve genellikle yoğun bir eğitim, çalışma, bilgi birikimi, seçilen mesleğe bağlı olarak yetenek geliştirmeyi gerektiren ve tüm bu sürecin sonunda kişilerin kazandığı ünvanın adı olarak ta tanımlanmaktadır. Ülkemizde resmi olarak tanımı yapılmış 600 civarında meslek olduğu bilinmektedir (Özbek vd, 2013: s. 533).

Sanat kavramı ise sözlük anlamı birden fazladır. Buna göre, bir duygu, tasarı, güzellik vb. nin anlatımında kullanılan yöntemlerin tamamı veya bu anlatım sonucunda ortaya çıkan üstün yaratıcılık; Belli bir uygarlığın veya topluluğun anlayış ve zevk ölçülerine uygun olarak yaratılmış anlatım; Bir şey yapmada gösterilen ustalık; Bir meslekte uyulması gereken kuralların tümü; Zanaat” anlamlarını ifade etmektedir (Türkçe Sözlük, 2009: s. 1695). Genellikle de sanat kelimesi ilk anlamı esas alınarak kullanılmaktadır. Doktrinde bu kavramın yerinde olmadığı belirtilmiş ve bizim de katıldığımız bu görüşe göre sanat terimi ile ifade edilmek istenen hususun esasında “zanaat” olduğu ifade edilmiştir (Özbek vd, 2013: s. 533). Zanaat ise “insanların maddeye dayanan gereksinimlerini karşılamak için yapılan, öğrenimle

birlikte deneyim, beceri ve ustalık gerektiren iş, sanat; el ustalığı isteyen işler” anlamlarına gelmektedir (Türkçe Sözlük, 2009: s. 2223).

Görüldüğü üzere meslek ve sanat (zanaat) farklı kavramları ifade etmekte olup, bir mesleğin zanaat niteliğinde olması şart değildir. Ancak bir zanaat meslek niteliğine sahip olabilir (Özbek vd, 2013: s. 533).

Hükümde belli bir meslek ve sanattan söz edilmekte ancak bunun hangi meslek ve sanat olduğuna ilişkin bir açıklık yer almamaktadır. O halde herhangi bir meslek ve sanat bu nitelikli halin uygulanması bakımından gerekir ve yeterlidir. Ancak bunun için söz konusu meslek ve sanatın sağladığı kolaylıktan yararlanılmak gerekir. Bu yönüyle meslek veya sanatın söz konusu suçu işlemek yönünde elverişli olması gerekir. Yani meslek ve sanatın icrası ile suçun işlenmesi arasında bir nedensellik bağlantısı kurulabilmelidir (Şen, 2006: s. 609; Özen, 2009: s. 24).

Yani fail icra ettiği meslek veya sanatın sağladığı kolaylıktan faydalanmak suretiyle mağdur hakkında kişisel veriye ulaşabilmelidir. Diğer bir deyişle bazı meslek veya sanatların icra edilmesi ile kişilerin verilerine ulaşmak kolay olmakta çoğu zaman yapılan iş gereği kişisel veriler kaydedilmektedir. Örneğin, bir hastanede çalışan hemşire ya da doktor burada kayıtlı hastalara ait verilere, bir banka memuru bankanın müşterilerinin kayıtlı müşteri bilgilerine ulaşabilir ve bu verileri kolayca kaydedebilir. Keza, bir mali müşavirin iş sahibi hakkında, bir gazetecinin haber konusu kişi hakkında veri toplaması, diğerlerine nazaran daha kolaydır (Özen, 2009: s. 24; Albayrak, 2012: s. 14).

Ayrıca bu ağırlaştırıcı nedenin uygulanması için, failin icra etmekte olduğu belli bir meslek veya sanatın sağladığı kolaylıktan yararlanarak kişisel verileri kaydetmesi veya hukuka aykırı olarak başkalarına vermesi, yayması veya ele geçirmesi gerekir. Daha açık bir ifadeyle, failin yaptığı meslek veya sanat kişisel verilerin kaydedilmesi konusunda faile bir kolaylık sağlamalı ve failin de bu kolaylığı kullanarak bu suçu işlemesi gerekmektedir. Örneğin, yukarıda da değinildiği gibi serbest olarak çalışan bir doktorun kendisine muayeneye gelen ve tahlil yaptıran kimselerin tahlil sonuçlarını ve genetik yapılarını bilgisayarında depolaması, bir bilgisayar tamircisinin sistemde depolanan başkalarına ait kişisel verileri ele geçirmesi, bir sauna işleticisinin yerleştirdiği gizli kamera ile müşterilerine ait görüntüleri kaydettikten sonra bu verileri başkalarına vermesi veya

internette yayınlaması durumlarında bu ağırlaştırıcı hal uygulanacak ve faile işlediği suça göre verilecek ceza yarı oranında artırılarak uygulanacaktır (Yaşar vd, 2010: s. 4122; Soyaslan, 2006: s. 274).

4. VERİLERİ YOK ETMEME SUÇU

4.1. Genel Olarak

Daha öncede açıklandığı üzere kişisel verilerin işlenmesi, kişisel verilerin elde edilmesinden, kaydedilmesine, üçüncü kişilere aktarılmasından yok edilmesine kadar geçen süreçte veriler üzerinde yapılan her türlü işlemi ifade etmektedir. Kişisel verilerin korunması da bütüncül bir sistem olup, sadece verilerin kaydedilmesini korumamakta, tüm veri işleme hallerini korumaktadır. Bu husus Anayasanın 20. Maddesinin üçüncü fıkrasıyla da teyit edilmektedir. Buna göre, herkes kendisi ile ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak, kişinin kendisi ile ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya **silinmesini talep etme** ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Anayasal düzenlememize göre, kişisel verilerin korunması hakkı, aynı zamanda kişinin verilerinin silinmesini talep etme hakkını da kapsamaktadır.

Diğer yandan kişisel veriler, nerede ve ne maksatla bulunursa bulunsunlar, kişinin özel hayatına dâhildir ve dolayısıyla cezai himayenin konusunu oluşturmaktadır. Bazı kişisel veriler, süresiz olarak başkalarının bilgisine açıkken bazı kişisel veriler, kullanılma amaçları yönünden, kanunla saklanmaları bir süre ile sınırlandırılabilir. Bu süre sonunda, kişisel verilerin korunmasının zorunlu sonucu olarak bu verilerin bulundukları yerde yok edilmeleri gerekmektedir. Yok etmeme ise, kişisel verilerin korunması hakkının ihlali anlamına gelmektedir. Bu nedenle “Verileri yok etmeme” başlıklı TCK’nın 138. maddesinde, kanunların belirlediği sürelerin geçmiş olmasına karşın, kişisel verileri bulundukları sistem içinde yok etmekle yükümlü kişilerin görevlerini yerine getirmemeleri, yani görevlerini ihmal etmeleri suç olarak düzenlenmiştir (Hafizoğulları ve Özen, 2011: s. 280).

Madde metni, “(1) Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde bir yıldan iki yıla kadar hapis cezası verilir²⁰⁵”.

(2) Suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması hâlinde verilecek ceza bir kat artırılır²⁰⁶.” Şeklinde dir.

Bu suçun oluşması için, hukuka uygun olarak kaydedilmiş kişisel verilerin bulunması, bu verilerin silinmesi konusunda kanunların belirli süreler belirlemiş olması ve bu verilerin silinmesi konusunda yetkisi ve görevi olan failin, bu süreler geçmiş olmasına karşın, görevlerini yerine getirmemiş olması gereklidir. Maddede tanımlanan suçun, TCK’ nın 257/2. maddesinde düzenlenen ihmal suretiyle görevi kötüye kullanma suçunun özel bir şekli olduğu doktrin ve uygulamacılar tarafından kabul edilmiştir (Malkoç, 2013: s. 915).

Maddede belirtildiği şekilde bir görevi ihmal durumu varsa, artık TCK’ nın 257. maddesi değil, TCK’nun 138. maddesi hükümleri uygulanacaktır (Yaşar vd, 2010. S. 4132).

Verileri yok etmeme eyleminin suç olarak tanımlanmasıyla kişisel verilerin korunmasında temel ilkeler arasında bulunan “sürenin sınırlı olması” karşılanmıştır. Bu ilkeye göre kişisel veriler, toplandıkları amaç için gerekli olandan daha uzun süre tutulmamalıdır. Kişisel verilerin süresiz olarak tutulmaması gerekliliği, amaçla bağlantılılık ilkesi açısından da oldukça önemlidir. Artık gereksinim duyulmayan verilerin silinmesi veya anonimleştirilerek kişisel niteliğinin ortadan kaldırılması keyfi uygulamaların önüne geçilmesi için gereklidir²⁰⁷.

²⁰⁵ 21/2/2014 tarihli ve 6526 sayılı Terörle Mücadele Kanunu ve Ceza Muhakemesi Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanunun 5. maddesiyle bu fıkra da yer alan “altı aydan bir yıla kadar hapis” ibaresi “bir yıldan iki yıla kadar hapis” şeklinde değiştirilerek suçun cezası artırılmıştır.

²⁰⁶ Bu fıkra, 21/2/2014 tarihli ve 6526 sayılı Kanunun 5. maddesiyle, suçu ağırlaştırıcı neden olarak maddeye eklenmiştir

²⁰⁷ **Küzeci**, 2010: s. 291; Nitekim Kişisel Verilerin Korunması Kanunu Tasarısının 7. Maddesinde de verilerin silinmesi ve yok edilmesi düzenlenmiş olup, “kanun hükümlerine uygun olarak işlenmiş olmasına rağmen artık ihtiyaç bulunmayan kişisel veriler silinir, yok edilir veya anonim hale getirilir.” Şeklinde düzenlenmiştir.

138. maddedeki suçun unsurlarını incelemeye geçmeden önce maddeyle ilgili doktrinde eleştiri konusu olan bazı hususlara bakmakta fayda bulunmaktadır.

İlk olarak, maddeyle kişisel verilerin yok edilmemesi düzenlemiş olmasına rağmen madde başlığı ve madde metninde salt “veri” ibaresi kullanılmıştır. Veri ve kişisel veri kelimeleri, çalışmamızın ilk bölümünde açıklandığı üzere farklı anlamlara gelmektedir. 136. maddede de benzer bir yazım usulü tercih edilmiş olmakla birlikte bu yazımın kanun yapım tekniği açısından doğru olmadığını düşünmekteyiz. Bu nedenle kanunilik ilkesi ve belirlilik ilklerinin bir gereği olarak madde başlığı ve metnin de “veri” yerine “kişisel veri” ibaresinin kullanılması gerekmektedir (Özen, 2009: s. 24).

İkinci olarak, hükümde suçun oluşabilmesi için “kanunların belirlediği sürelerin geçmiş olması” ölçütü esas alınmış, verinin toplanma amacı ile bir bağlantı kurulmamıştır (Ketizmen, 2008: s. 241). Bir başka anlatımla verilerin toplanma amacı ortadan kalkmış ya da gerçekleşmiş olsa bile bunlar yasada belirtilen süreler boyunca saklanabilecektir. Bu durum amaca bağlılık ilkesi ile bağdaşmamaktadır (Küzeci, 2010: s. 291-292).

Üçüncü olarak maddede “*verileri sistem için de yok etmek*” ten bahsedilmektedir. Bu ibare belirtilen suçun otomatik yollarla işlenen verilere ilişkin olduğu izlenimini yaratmaktadır. Nitekim yukarıda incelenen kişisel verilerin kaydedilmesi ve hukuka aykırı olarak verme, yayma ve ele geçirme suçlarında böyle bir ibareye yer verilmemiştir. Bu farklılık, verileri yok etmeme suçunun diğerlerinin tersine yalnızca otomatik yolla işlenen verilere ilişkin olduğu yönünde şüphe yaratmaktadır. Bu nedenle doktrinde, bizim de katıldığımız bir görüşe göre buradaki şüphenin giderilmesi için “sistemde bulunmaya” ilişkin ibarenin madde metninden çıkartılması gerektiği belirtilmiştir (Küzeci, 2010: s. 292; Ketimen, 2008: s. 242).

4.2. Korunan Hukuki Yarar

Bu suçla korunan hukuki yarar, yukarıda diğer suçlar açıklanırken belirtildiği üzere, kişisel verilerin korunması hakkıdır²⁰⁸. Bu suç, diğer suçlardan işleniş biçimi

²⁰⁸ **Hafizoğulları ve Özen**, 2011: s. 279; Bir kısım yazarlar, bu suçta korunan hukuki değeri sadece kişinin özel hayatının gizliliği olduğunu savunmuşlarsa da, biz bu görüşlere katılmıyoruz. Bu görüşler için bkz. **Parlar ve Hatipoğlu**, 2008, s. 2053

itibariyle ayrılmaktadır. Bu nedenle korunan hukuki yarar ile ilgili olarak “kişisel verilerin kaydedilmesi suçu” altında yapılan açıklamalar bu suç açısından da geçerlidir.

Ancak bu suçla korunan hukuki yararın “kişisel verilerin korunması hakkı” olduğu daha açık şekilde anlaşılmaktadır. Çünkü burada kişisel veriler hukuka uygun şekilde kaydedilmiş ve halen sistem içinde muhafaza edilmektedir. Bu verilerin kanunda belirlenen süre geçmiş olmasına rağmen silinmemesi her zaman kişilerin özel hayatını ihlal edebilecek bir durum değildir. Zaten veriler öğrenmesi gerekenler tarafından öğrenilmiştir. Veriler sistem içinde kaldığı müddetçe de başkaları tarafından öğrenilmesi durumu da yoktur.

Diğer taraftan, daha öncede değinildiği gibi, kişisel verilerin korunması bütüncül bir sistem olup, verilerin toplanmasından, kaydedilmesine, depolanmasına, üçüncü kişilere aktarılmasına veya silinmesine kadarki geçen tüm aşamaları kapsamaktadır. Bu aşamaların tümünde veri işleyenlerin hukuka uygun davranma mecburiyetleri olduğu gibi, kişinin de verileri hakkında bilgi alma, bu verilerinin silinmesini veya güncellenmesini talep etme hakları bulunmaktadır. Nitekim bu husus anayasal güvenceye de kavuşturulmuştur. Anayasanın 20. Maddesinin üçüncü fıkrasına göre, herkes kendisi ile ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak, kişinin kendisi ile ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya ***silinmesini talep etme*** ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. İşte TCK’nun 138. maddesindeki bu suç, kişinin daha önceden hukuka uygun şekilde kaydedilen verilerinin silinmesini talep etme hakkının ihlalini yaptırım altına alan bir düzenleme olarak karşımıza çıkmaktadır. Bu nedenle de bu suçla, kişisel verilerin korunması hakkı korunmaktadır.

4.3.Suçun Unsurları

Kişisel verilerin kaydedilmesi suçu incelenirken TCK sistematığında suçun unsurların nelerden ibaret olduğu hususunda doktrinde görüş birliği bulunmadığını, ancak hukukumuzda genellikle suçun dört unsurunun bulunduğu kabul edildiğini, bunların da; tipiklik, maddi unsurlar, manevi unsur ve hukuka aykırılık unsurları

olduğunu belirtmiştik. Bu suç açısından da aynı unsurlar çerçevesinde inceleme yapılacaktır.

4.3.1. Tipiklik

Tipikliğin, doktrinde, suç sayılan fiilin ceza normundaki soyut tasviri olarak tanımlandığı, tipiklik unsuru için öncelikle bir fiili suç sayan ve buna bir yaptırım öngörmüş bulunan bir kanun maddesinin var olması gerektiğini “kişisel verilerin kaydedilmesi suçu” nun açıklamalarında izah etmiştik.

Bu açıklamalar çerçevesinde TCK’nın 138. maddesine bakıldığında; madde metninde, *"Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanların görevlerini yerine getirmediklerinde"* cezalandırılacakları belirtildiğine göre, tipiklik unsuru açısından aranan husus, kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olan failin kişisel verileri, görevini yerine getirmemek suretiyle yok etmemesidir. Fail maddede sayılan şekilde hareket etmiş ise fiili tipik sayılacak ve suçun tipiklik unsuru gerçekleşecektir.

Tipiklik unsuru suçun nitelikli halleri açısından da arandığından (Artuk vd, Genel Hükümler, 2013: s. 204), maddenin ikinci fıkrasındaki ağırlaştırıcı nedenin uygulanabilmesi içinde fiilin tipik olması gerekmektedir. Bu kapsamda, failin sistem içinde yok etmekle görevli olduğu halde yok etmediği veriler, CMK hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması hâlinde ancak tipiklik unsuru gerçekleşecek ve bu ağırlaştırıcı neden uygulanabilecektir.

4.3.2. Maddi Unsurlar

4.3.2.1. Suçun Konusu

Suçun konusu, hukuka uygun olarak kaydedilmiş olan kişisel verilerdir (Parlar ve Hatipoğlu, 2008: s. 2053). Daha doğrusu bu maddedeki suçun konusu olan kişisel veriler, hukuka uygun olarak kaydedilmiş olan ve belli süre geçmesi halinde silinmesi kanunla belirlenmiş olan kişisel verilerdir. Kişisel verilerin hukuka uygun kaydedilip kaydedilmediği önemlidir. Zira veriler hukuka aykırı olarak kaydedilmiş ise, bu suç değil, TCK’nın 135. maddesinde düzenlenen suç oluşacaktır (Yaşar vd, 2010: s. 4133).

Bu açıdan madde başlığında ve metninde kullanılan “veri” kelimesi isabetli olmamıştır. Kanaatimizce suçun konusu kişisel veri olduğuna göre, kanunilik ilkesi gereği madde metninde de kişisel veri ibaresinin kullanılması gerekmektedir.

Kişisel veri kavramı hakkında “kişisel verilerin kaydedilmesi” suçu altındaki açıklamalar, bu suç açısından da geçerlidir.

Maddede belirtilen kişisel verilerin tutulduğu sistemin, bir bilişim sistemi mi olduğu yoksa fiziki bir dosyalama sistemi mi olduğu hususunda hükümde bir açıklık yoktur. Madde gerekçesinde, hukuka uygun şekilde kaydedilmiş verilerin belirlenen sürelerde yok edilmemesinin suç olarak tanımlandığı belirtilmiştir. Bu açıdan gerekçede de bir açıklık yoktur. Ancak 135. maddedeki suçta kaydetme eylemi açısından fiziki kayıt ile otomatik bir sisteme kayıt arasında fark görülmektedir. Kanunlarda da sadece bilişim sisteminde tutulan verilere özgü bir düzenleme olmadığından, kanaatimizce burada “sistemi” ibaresini geniş olarak yorumlamak gerekmektedir. Bu nedenle bir dosya içinde tutulan veriler de suçun konusu oluşturacağı gibi, UYAP, MERNİS gibi bilişim sistemlerinde tutulan verilerde bu suçun konusunu oluşturabileceklerdir.

Suçun konusunun CMK hükümlerine göre yok edilmesi gereken veriler olması hali, ikinci fıkrada ağırlatıcı neden olarak öngörülmüştür. CMK hükümlerine göre yok edilmesi gereken verilerin hangileri olduğu, suçun ağırlaştırıcı nedenleri başlığı altında ayrıntılı olarak açıklanmıştır.

4.3.2.2. Fail ve Mağdur

Suçun faili, madde metninde “verileri sistem içinde yok etmekle yükümlü olanlar” olarak belirlenmiştir. Bu nedenle suç fail bakımından özellik arz etmektedir. Bu suçu ancak “verileri sistem içinde yok etmekle yükümlü olanlar” işleyebilir. Bu özelliği nedeniyle bu suç, özgü suçlardır (Hafizoğulları ve Özen, 2011: s. 281; Özen, 2009: s. 26). Bu kişiler kamu görevlisi olabileceği gibi, kamu görevlisi olmayan kişiler de olabilir. Burada önemli olan, bir kimsenin kanunların belirlediği sürelerde sistemde kayıtlı olan kişisel verileri yok etmekle yükümlü olup olmadığıdır (Yaşar vd, 2010: s. 4132; Şen, 2006: s. 611; Malkoç, 2013: s. 915).

Bu çerçevede fail bir kamu görevlisi olabileceği gibi bir meslek ve sanat sahibi de olabileceğinden kanun koyucu doğal olarak 137. maddede diğer suçlar bakımından kabul ettiği cezayı ağırlaştıran nedenleri, bu suç bakımından öngörmemiştir (Özbek vd, 2013: s. 542).

Bu suç mağdur bakımından da özellik taşımaktadır. Maddedeki düzenleme itibariyle bu suçun mağduru da sadece kişisel verileri sistemde kayıtlı bulunan kişiler olabilir. Gerçekten suç, verileri sistem içinde yok etme yükümlülüğünün yerine getirilmemesi suretiyle işlenebildiğine göre, suçun konusu sistem içinde bulunan kişisel veri ve mağdur da bu verinin sahibi olan kişidir²⁰⁹.

4.3.2.3. Hareket ve Netice

Suçu oluşturan hareket, kişisel verilerin konulduğu sistemde yok edilmesi yükümlülüğünün yerine getirilmemesi, ihmal edilmesidir (Hafizoğulları ve Özen, 2011: s. 281; Parlar ve Hatipoğlu, 2008. S. 2055).

Sözlük anlamı itibariyle yok etmek; varlığına son vermek, ortadan kaldırmak, izale etmektir (Türkçe Sözlük, 2009: s. 2187). Kişisel verilerin korunması sistemi açısından yok etmek ise veriyi, bir yerde kullanılabilir olmaktan çıkartmak, silmek, ortadan kaldırmaktır. Burada esas olan verinin kimsenin eline geçmemesini, bir daha kullanılamamasını sağlamaktır (Hafizoğulları ve Özen, 2011: s. 281). O halde maddedeki anlamı itibariyle yok etmeme fiilini; bir veriyi tamamen ortadan kaldırmama, dış dünyadan beş duyu organı ile algılanmayacak hale getirmeme şeklinde anlamak gerekir (Özen, 2009: s. 25).

Yok etme eylemi, bilgisayardaki bilgiler için; tüm kopyalarının silinmesi, herhangi bir örneğinin kalmaması, fiziki belgeler için ise; geri dönüşü olmayacak şekilde ortadan kaldırılmasını belirtir (Yaşar vd, 2010: s. 4134).

Suçun oluşması için; kanunların belirlediği sürelerin geçmiş olması, failin verileri sistem içinde yok etmekle yükümlü olması ve failin verileri yok etmemesi gerekmektedir (Özbek vd, 2013: s. 541).

²⁰⁹ Özbek vd, 2013, s. 542; Yaşar vd, 2010: s. 4132; Bir kısım yazar da bu suçun mağdurunun herkes olabileceğini savunmuşlardır. Bkz. Hafizoğulları ve Özen, 2011: s. 281. Biz bu görüşe katılmıyoruz. Çünkü madde deki düzenleme itibariyle bu suçun mağduru ancak verileri sistem içinde kayıtlı olan kişilerdir.

Çoğunlukla kanunlar verilerin yok edilmesinin ne kadar sürede yapılması gerektiğini göstermektedirler. Örneğin, CMK'nın 137. maddesinin üçüncü fıkrasının son cümlesinde, "...Bu durumda, yapılan tespit veya dinlemeye ilişkin kayıtlar Cumhuriyet savcısının denetimi altında en geç **on gün içinde yok edilerek**, durum bir tutanakla tespit edilir." şeklindedir. Buna göre, CMK'nın 135. Maddesine göre verilen kararlar üzerine elde edilen kişisel veriler, kovuşturmaya yer olmadığına dair karar verilmesi ya da aynı maddenin birinci fıkrasına göre hâkim onayının alınamaması halinde en geç on gün içinde yok edilmelidirler. En geç on içinde yok edilmediği takdirde bu suç oluşacaktır (Özen, 2009: s. 25).

Sürenin açıkça gösterildiğine bir diğer örnek te CMK'nın 80. Maddesidir. Maddeye göre, CMK'nın 75, 76 ve 78. madde hükümlerine göre alınan örnekler üzerinde yapılan inceleme sonuçları, kişisel veri niteliğinde olup, başka bir amaçla kullanılamaz; dosya içeriğini öğrenme yetkisine sahip bulunan kişiler tarafından bir başkasına verilemez. Bu bilgiler, kovuşturmaya yer olmadığı kararına itiraz süresinin dolması, itirazın reddi veya hükmün kesinleşmesi hallerinde en geç on gün içinde Cumhuriyet savcısının huzurunda yok edilir ve bu husus dosyasında muhafaza edilmek üzere tutanağa geçirilir (Özbek vd, 2013: s. 543).

Verilerin ne zaman silinmesi gerektiği sadece CMK'da düzenlenmemiştir. 5352 sayılı Adli Sicil Kanununun 9²¹⁰ ve 12²¹¹. Maddelerinde de kamu görevlilerine

²¹⁰ "Adli sicil bilgilerinin silinmesi" başlıklı 9. Madde şöyledir:

"Madde 9- (1) Adli sicildeki bilgiler;

- a) Cezanın veya güvenlik tedbirinin infazının tamamlanması,
- b) Ceza mahkûmiyetini bütün sonuçlarıyla ortadan kaldıran şikayetten vazgeçme veya etkin pişmanlık,
- c) Ceza zamanaşımının dolması,
- d) Genel af,

Halinde Adli Sicil ve İstatistik Genel Müdürlüğünce silinerek, arşiv kaydına alınır.

(2) Adli sicil bilgileri, ilgilinin ölümü üzerine tamamen silinir.

(3) Türk vatandaşları hakkında yabancı mahkemelerce verilmiş olup 4 üncü maddenin birinci fıkrasının (f) bendine göre adli sicile kaydedilen hürriyeti bağlayıcı cezaya mahkûmiyet hükümleri, kesinleştiği tarihten itibaren mahkûmiyet kararında belirtilen sürenin geçmesiyle, Adli Sicil ve İstatistik Genel Müdürlüğünce adli sicil kayıtlarından çıkartılarak arşiv kaydına alınır. Adli para cezasına mahkûmiyet hükümleri ile cezanın ertelenmesine ilişkin hükümler, adli sicil kaydına alınmadan doğrudan arşive kaydedilir."

²¹¹ Adli sicil ve arşiv bilgilerinin silinmesi başlıklı 12. Madde şöyledir:

"Madde 12- (1) Arşiv bilgileri;

- a) İlgilinin ölümü üzerine,
- b) Anayasanın 76 ncı maddesi ile Türk Ceza Kanunu dışındaki kanunlarda bir hak yoksunluğuna neden olan mahkûmiyetler bakımından kaydın arşive alınma koşullarının olduğu tarihten itibaren;
 1. Yasaklanmış hakların geri verilmesi kararı alınması koşuluyla onbeş yıl geçmesiyle,
 2. Yasaklanmış hakların geri verilmesi kararı alınması koşulu aranmaksızın otuz yıl geçmesiyle,

kişisel veri niteliğinde olan adli sicil kayıtlarını ne zaman silmeleri gerektiği açıkça zaman dilimi gösterilmek suretiyle düzenlenmiştir.

Bu şekilde net bir sürenin gösterildiği hallerde, fail sürenin üst sınırı olan zaman dilimi tamamlanmadan bu görevi yerine getirmekle yükümlüdür. Ancak, mevzuatta süre belirlenmeyip de “derhal yok edilir”, “hemen silinir” gibi ibarelerle zaman belirlenmiş ise, bu durumda görevlinin içinde bulunduğu somut olaya göre, makul olan en kısa sürede bu yok etme işleminin tamamlanması gerekir (Yaşar vd, 2010: s. 4134; Parlar ve Hatipoğlu, 2008. S. 2056).

Verilerin kanunlarda belirlenen sürelerde, diğer bir deyişle zamanında yok edilmesi önemlidir. Bazen fail, sistemde kayıtlı olan kişisel veriyi yok etmiş veya silmiş olabilir. Eğer bu yok etme işlemi süresi içerisinde yapılmamış ise, yetkili makamların kişisel verilerin yok edilmediğini öğrenmesinden önce bu verileri silinmiş olsa bile, yine de bu suç oluşacaktır. Örneğin, dinleme işlemi yapan fail, şüpheli hakkında takipsizlik kararı kesinleştikten sonra dinlenen şahıs yeni bir suç işlediğinde önceki dinleme kayıtlarının bir suretinin kendisinde olduğunu bildirirse, kişisel veri içeren kayıtları silmediği anlaşıldığından, bu suçu işlemiş sayılacaktır (Yaşar vd, 2010: s. 4134).

Diğer yandan madde metnindeki “kanun” kavramından hem maddi hem de şekli kanun yani herhangi hukuk kuralının anlaşılması gerektiği doktrinde bazı yazarlarca ileri sürülmüş ise de (Özbek vd, 2013: s. 542), kanun metninde açıkça “kanunlarda” belirlenen sürelerin geçmiş olmasından bahsedildiğinden kanımızca, buradaki kanun ifadesinden sadece kanunları anlamak gerekmektedir. Zira daha öncede değinildiği gibi temel hak ve özgürlüklere ilişkin sınırlama veyahut düzenleme içeren hukuk metinleri en azından kanun düzeyinde olmalıdır. Hukuk sistemimizde de yönetmelikler kanunların uygulanmasını göstermek için çıkarıldığından kanunda belirtilmeyen bir sürenin yönetmelikle düzenlenemeyeceği,

c) Diğer mahkûmiyetler bakımından kaydın arşive alınma koşullarının oluştuğu tarihten itibaren beş yıl geçmesiyle,

tamamen silinir.

(2) Fiilin kanunla suç olmaktan çıkarılması halinde, bu suçtan mahkûmiyete ilişkin adli sicil ve arşiv kayıtları, talep aranmaksızın tamamen silinir.

(3) Kanun yararına bozma veya yargılamanın yenilenmesi sonucunda verilen beraat veya ceza verilmesine yer olmadığı kararının kesinleşmesi halinde, önceki mahkûmiyet kararına ilişkin adli sicil ve arşiv kaydı tamamen silinir.”

kanunda bir düzenleme olduđu durumlarda da kanunun esas alınması gerektiđi, zaten yönetmeliklerde kanuna aykırı olmayacağından kanundaki sürelerin aynen belirtilmesi gerektiđi, bu nedenle buradaki kanun ibresinden sadece kanun metinlerinin anlaşılması gerektiđi değerlendirilmektedir.

Diğer yandan dikkat edilmesi gereken bir nokta da bu suçun oluşması için failin verileri yok etmekle yükümlü olması ve bu yükümlüğün failin görev alanına giriyor olması gerekmektedir. Bu durum da failin tabi olduđu mevzuat hükümlerine göre belirlenecektir. Örneğin, Ceza Muhakemesinde Beden Muayenesi, Genetik İncelemeler ve Fizik Kimliğin Tespiti Hakkında Yönetmeliđi 16. Maddesi, *“Kovuşturmaya yer olmadığı kararına itiraz süresinin dolması, itirazın reddi, beraat veya ceza verilmesine yer olmadığı kararı verilip kesinleşmesi hâllerinde bu Yönetmeliğin 15’inci maddesi hükümleri uyarınca elde edilen veriler, Cumhuriyet savcısının huzurunda ve uygun göreceđi usullerle derhâl yok edilir ve bu husus tutanađa geçirilir.”* hükmünü havidir. Aynı Yönetmeliğin 17. Maddesi ise *“Mahkûmiyet kararı verilmesi hâlinde bu Yönetmeliğin 15’inci maddesinin birinci ve ikinci fıkrası uyarınca elde edilen veriler kolluk tarafından, üçüncü fıkrasında belirtilen dış izleri ise bu işlemi yapan sağlık kuruluşu tarafından arşivlenir”* düzenlemesini içermektedir. Her iki hüküm birlikte değerlendirildiğinde verileri yok etme yükümlülüğünün asıl olarak Cumhuriyet savcısına verildiđi görölmektedir. Ancak bu savcının imha ile görevli olması daha açık bir ifadeyle o dosyaya bakmakla görevli savcı olması gerekir. Nitekim aynı Yönetmeliğin 22. Maddesine göre *“Cumhuriyet başsavcılıklarınca yapılan iş bölümlerinde, bu Yönetmelik kapsamında elde edilen verilerin imha edilmesi ve diğer işlemlerin yürütülmesi amacıyla yeterli sayıda Cumhuriyet savcısı görevlendirilir”* hükmünü içermektedir (Özbek vd, 2013: s. 543).

Verileri yok etmeme suçunun yalnızca ihmal yoluyla işlenebilecek bir suçtur. Yasal yükümlölük altında bulunanlar ihmalen bunu yerine getirmediğinde suç gerçekleşmiş olacaktır (Hafizoğulları ve Özen, 2011: s. 141-142; Ketizmen, 2008: s. 241; Soyaslan, 2006: s. 275). Bu bağlamda süre aşıldıktan sonra verilerin yok edilmesi, eylemi suç olmaktan çıkarmayacağı gibi, mağdurun rızası da fiili hukuka uygun hale getirmeyecektir (Hafizoğulları ve Özen, 2011: s. 141). Ayrıca burada sözü geçen sürenin mutlaka altı ay veya iki yıl gibi kesin bir zaman dilimi olarak

düşünülmemesi gerekir. Örneğin CMK'nın 81/2 hükmüne göre, şüpheli veya sanığın fizik kimliğinin saptanması için kaydedilen fotoğrafı, parmak izi gibi verileri; itirazın reddi ve beraat kararı verilmesi gibi durumlarda Cumhuriyet savcısının huzurunda derhal yok edilmesi gerekmektedir. Bu kurala uygun hareket etmeyen görevli, maddede belirtilen suçu işlemiş olacaktır (Küzeci, 2010: s. 292).

Suçun tamamlanmış sayılması için kişisel verinin yükümlüğe aykırı olarak yok edilmemiş olması yeterlidir; bundan bir zarar doğması da şart değildir. Bu nedenle suç bir *tehlike suçudur*. Suç tipinde hareket ile tehlike neticesi arasında bir nedensel ilişkinin varlığını araştırmak yönünde zorunluluk bulunduğu ilişkin ifade yer almaması nedeniyle suçun *soyut tehlike suçu* olduğu söylenebilir. Ayrıca suç, hareketin yapılmasıyla daha doğrusu yükümlülüğün yerine getirilmemesiyle tamamlandığından ayrıca ani hareketli bir suç olduğu da söylenebilir (Özbek vd, 2013: s. 544).

4.3.3. Manevi Unsur

Bu suç, genel kastla işlenen bir suçtur. Failin kişisel verileri sistem içinde yok etme yükümlülüğünü kasten yerine getirmemesi gerekir. Fail sürelerin geçmiş olduğunu bilmesine rağmen verileri silmemelidir. Saik önemli değildir. Bu suçun taksirle işlebilen hali kanunda düzenlenmediği için, taksirle işlenemez (Yaşar vd, 2010: s. 4136; Parlar ve Hatipoğlu, 2008: s. 2056; Şen, 2006: s. 611; Soyaslan, 2006. S. 275). Bu nedenle, verilerin yok edilmesi için kanunda belirlenen sürelerin taksirle (örneğin unutulması) yok edilmemesi halinde bu suç oluşmayacaktır (Özen, 2009: s. 26).

Genel kastla işlenebilen suçun kural olarak olası kastla işlenmesi de mümkündür (Özgenç, 2012: s. 237-246; Artuk vd, Genel Hükümler, 2013: s. 300-307). Bu nedenle bazı yazarlar, bu suçun olası kastla da işlenebileceğini savunmuşlardır (Özbek vd, 2013: s. 544). Olası kast, failin neticeyi öngörmesi ancak meydana gelmesi konusunda kayıtsız kalması; meydana gelememesi için çaba sarf etmemesi, neticeyi göze almasıdır (Özgenç, 2012: s. 237-246; Artuk vd, Genel Hükümler, 2013: s. 300-307). Ancak söz konusu suç şekli bir suç olup, kanunda belirtilen hareketin yapılmasıyla, daha doğrusu yapmama eylemi ile oluşacağından, suçun olası kastla işlenemeyeceğini düşünmekteyiz.

Kanunda belirtilen süreler konusunda hata yapılması halinde ise, sorun hataya ilişkin genel kurallar çerçevesinde çözülecektir. Örneğin, kanunda belirtilen sürenin hesabında hata yapılarak belirtilen süreden daha sonraki bir sürede yok etme işlemi yapılırsa fail hatasından yararlanacaktır²¹².

4.3.4. Hukuka Aykırılık Unsuru

Hukuka aykırılık, daha öncede değinildiği üzere, “kanundaki tarife uygun bulunan fiile hukuk düzenince cevaz verilmemesi, fiilin yalnız ceza hukuku ile değil, bütün hukuk düzeni ile çelişki ve çatışma halinde bulunması” demektir (Artuk vd, Genel Hükümler, 2013: s. 369; Alacakaptan, 1975: s. 95). Bu suç açısından da fiil, hukuka aykırı olmalıdır. Ancak burada hukuka aykırı ibaresine diğer suçlarda olduğu gibi yer verilmemiştir. Esasında suçun düzenlenişi itibariyle burada kanun koyucu hukuka aykırılık müessesesini daraltmıştır. Bu suçta kanuna aykırılık söz konusudur. Gerçekten de Kanunda belirtilen süre sonunda kişisel verilerin yok edilmemesi halinde eylem hukuka aykırı olmakta ve diğer unsurlarında varlığı halinde suç oluşmaktadır. Başka bir deyişle kişisel verilerin yok edilmemesi zorunlu bazı nedenler yüzünden yok edilmemesini öngören başka bir kanun hükmü olmadıkça, hukuka aykırı sayılacaktır. Bu suçta kanuna aykırılık arandığı çin mağdurun rızası eylemi hukuka uygun hale getirmeyecektir (Hafizoğulları ve Özen, 2011: s. 281). Çünkü kanunlarda ilgilinin rızasına bakılmaksızın verilerin yok edilmesi emredici hüküm olarak kabul edilmiştir (Özen, 2009: s. 26).

5271 sayılı CMK’nın 75. ve 76. maddelerine göre, şüpheli veya sanık veya diğer kimselerin vücudundan kan veya benzeri biyolojik örneklerle saç, tükürük, tırnak gibi örnekler alınması halinde, bu örnekler üzerinde yapılan inceleme sonuçları kişisel veri niteliğinde olup, başka bir amaçla kullanılamaz, dosya içeriğini öğrenme yetkisine sahip bulunan kişiler tarafından bir başkasına verilemez, aynı Kanunun 80. maddesine göre de, bu bilgiler kovuşturmayaya yer olmadığı kararına itiraz süresinin dolması, itirazın reddi, beraat veya ceza verilmesine yer olmadığı kararı verilip kesinleşmesi hallerinde C. Savcısının huzurunda derhal yok edilir ve bu husus tutanağa geçirilir.

²¹² Özen, 2009: s. 26; Hata konusunda ayrıntılı bilgi için bkz. Artuk vd, Genel Hükümler, 2013: s. 521-538

CMK'nın 81. maddesine göre de, şüpheli veya sanığın kimliğinin tespiti için gerekli olması halinde, fotoğrafı, beden ölçüleri, parmak ve avuç içi izi, bedende yer almış olup teşhisini kolaylaştıracak diğer özellikleri ile sesi ve görüntüleri kayda alınarak soruşturma ve kovuşturma dosyasına konulabilir. Aynı maddenin 2. fıkrasına göre de, şüpheli veya sanık hakkında da kovuşturmaya yer olmadığı kararına itiraz süresinin dolması, itirazın reddi, beraat veya ceza verilmesine yer olmadığı kararı verilip kesinleşmesi halinde, söz konusu kayıtlar C. Savcısının huzurunda derhal yok edilir.

CMK'nın 135. maddesinde düzenlenen iletişimin tespiti, dinlenmesi ve kayda alınması durumunda şüpheli hakkında kovuşturmaya yer olmadığına dair karar verilmesi, ya da C. Savcısı tarafından bu konuda verilen kararn hâkim tarafından onaylanmaması hallerinde CMK'nın 137. maddesine göre, bu tedbire C. Savcısı tarafından derhal son verilir ve yapılan tespit ve dinlemeye ilişkin kayıtlar en geç on gün içinde yok edilerek, durum bir tutanakla tespit olunur.

5352 sayılı Adli Sicil Kanununun 9. maddesine göre, adli sicildeki bilgiler, cezanın veya güvenlik tedbirinin infazının tamamlanması, ceza mahkûmiyetini bütün sonuçlarıyla ortadan kaldıran şikâyetten vazgeçme veya etkin pişmanlık, ceza zamanaşımının dolması ve genel af halinde Adli Sicil ve İstatistik Genel Müdürlüğünce silinerek arşiv kaydına alınır. Aynı Kanunun 12. maddesine göre de, arşiv bilgileri ilgilinin ölümü üzerine ve herhalde kaydın girildiği tarihten itibaren seksen yıl geçmesi, fiilin kanunla suç olmaktan çıkarılması, kanun yaranna bozma veya yargılanmanın yenilenmesi sonucunda verilen beraat veya ceza verilmesine yer olmadığı kararının kesinleşmesi, hallerinde silinir.

Görüldüğü gibi, bu yasal düzenlemeler kişiler hakkında hukuka uygun olarak kaydedilen kişisel verilerin nasıl silineceğini de göstermektedir. Bu sürelerin sonunda verilerin yok edilmemesi hukuka aykırı olacak ve suç oluşacaktır.

Diğer suçlarda olduğu gibi bu suç açısından da hukuka aykırılığı ortadan kaldıran nedenler olabilir.

Bu suç bakımından ilginin rızası hukuka uygunluk sebebi olabileceği düşünülebilirse de kanunlarda ilgilinin rızasına bakılmaksızın verilerin yok edilmesi

emredici hüküm olarak kabul edildiğinden ilgilinin rızası, fiili, hukuka uygun hale getirmez²¹³.

Dokrinde bazı yazarlar tarafından TCK'nın 26. Maddesinin ikinci fıkrasında düzenlenmiş olan zorunluluk halinin bu suçta hukuka uygunluk nedeni olarak kabul edilebileceği belirtilmiş (Özen, 2009: s. 26) ise de, biz bu görüşe katılmıyoruz. Zira 26. maddenin ikinci fıkrası *“Gerek kendisine gerek başkasına ait bir hakka yönelik olup, bilerek neden olmadığı ve başka suretle korunmak olanağı bulunmayan ağır ve muhakkak bir tehlikeden kurtulmak veya başkasını kurtarmak zorunluluğu ile ve tehlikenin ağırlığı ile konu ve kullanılan vasıta arasında orantı bulunmak koşulu ile işlenen fiillerden dolayı faile ceza verilmez.”* Hükmünü ihtiva etmektedir. Madde metninden de anlaşılacağı üzere burada bazı nedenlerden dolayı fail icrai bir fiil yapmakta, bir suç işlemektedir. Örneğin, hırsızlık, mala zarar verme suçlarında kişi, içinde bulunduğu tehlikeden kurtulmak amacıyla başkasının malını çalabilir veya bu mala zarar verebilir. Ancak kişisel verilerin yok edilmemesi suçu şekli bir suç olup, kanundaki sürenin geçmiş olmasına rağmen verilerin yok edilmemesi halinde oluşmaktadır. Kişinin elinde olmayan nedenlerle veya deprem ve sel gibi mücbir sebeplerle verileri zamanında yok edememesi durumunda ise kişinin kastı veya taksirine bakılarak sorun çözülmelidir²¹⁴.

Yine benzer şekilde bu suç açısından TCK'da düzenlenen bir cebir ve tehdit ve korkutma halinin bu suç açısından da geçerli olabileceği ve bu durumlarda suçun oluşmayacağı aynı yazar tarafından ileri sürülmüş ise de (Özen, 2009: s. 26), zorunluluk halinde olduğu gibi bu hal de 5237 sayılı TCK sistemetiğinde “ceza sorumluluğunu kaldıran veya azaltan nedenler” arasında düzenlenmiştir. Yani burada esasında bir suç vardır. Fakat bu suçtan failin sorumlu tutulup tutulamayacağı düzenlenmektedir. Nitekim TCK'nın 28. Maddesinin birinci fıkrası, *“Karşı koyamayacağı veya kurtulamayacağı cebir ve şiddet veya muhakkak ve ağır bir*

²¹³ **Hafizoğulları ve Özen**, 2011: s. 281; **Özen**, 2009: 26; **Özbek** ise, “kural olarak soruşturulması ve kovuşturulması şikayete tabi suçlar bakımından mağdurun üzerinde tasarrufta bulunabileceği bir hakkın var olduğu kabul edilebileceğinden ve 138. Maddede yer alan bu suç şikayete bağlı bulunmadığından bu suç bakımından ilgilinin rızası hukuka uygunluk sebebi, uygulanabilir değildir” şeklinde farklı bir gerekçeyle bu suçta ilgilinin rızasının hukuka uygunluk nedeni olamayacağını savunmuştur. Bkz. **Özbek vd**, 2011: s. 544

²¹⁴ Zorunluluk hali TCK'da hukuka uygunluk nedeni olarak değil, ceza sorumluluğunu kaldıran bir neden olarak sayılmıştır. Ancak bu husus tartışmalı olup, ayrıntılar için bkz. **Artuk vd**, Genel Hükümler, 2013: s. 459; **Özgenç**, 2012: s. 382

korkutma veya tehdit sonucu suç işleyen kimseye ceza verilmez”. Hükümünü ihtiva etmektedir. Bu hükme göre, cebir veya şiddetin etkisi altında herhangi bir suç işleyen kimseye ceza verilmeyecek, tehdit veya cebirde bulunan kimse suçun faili sayılacaktır²¹⁵. Örneğin verileri yok etmekle görevli kişinin cebir ve tehdit altında kalarak verileri yok edememesi durumunda, görevlinin eylemi suç oluşturacaktır. Ancak görevli bu eylemi cebir veya tehdit altında yaptığı için bu suçtan sorumlu tutulmayacaktır.

Bu suçta, başka bir kanun hükmü hukuka uygunluk nedeni olabilir (Hafizoğulları ve Özen, 2011: s. 281). Zira normlar hiyerarşisinde kanunların birbirlerine üstünlüğü olmayıp, kanunların hepsi en üst norm olan Anayasaya uygun olmak zorundadır (Teziç, 1998: s. 6-9; Gözler, 2010: s. 13). Bazen sonradan çıkan kanun önceki kanundaki süreleri değiştirmiş olabilir. Veya sonradan çıkan kanun önceki kanuna göre özel düzenlemeler içerebilir. Veyahutta kanunkoyucunun ihmali nedeniyle önceki kanun yürürlükten kaldırılmamış olabilir. Bu durumlarda verileri sistem içinde yok etmekle görevli olan kişi, başka bir kanun hükmünün verinin silinmesine izin vermemesi nedeniyle verileri yok etmez ise, eylemi hukuka aykırı olmayacaktır. Zira kanunlarda çelişki olması faili ilgilendirmemektedir. Burada önemli olan verilerin yok edilmemesini öngören kanunun yürürlükte ve failin de bu kanuna uygun davranmasıdır.

4.4. Suçun Özel Görünüş Halleri

4.4.1. Teşebbüs

Suçun tamamlanması için, mağdurun herhangi bir zarara uğramasına gerek yoktur. Süre geçmiş olmasına karşın, sistem içinde kişisel verilerin yok edilmemesiyle suç tamamlanmış olur. Bu nedenle, bu suçun teşebbüse müsait olmadığı konusunda doktrinde ve uygulamacı yazarlar arasında büyük oranda görüş birliği mevcuttur²¹⁶.

²¹⁵ Ayrıntılı bilgi için kz. **Artuk vd**, Genel Hükümler, 2013: s. 468-470; **Özgenç**, 2012: s. 380

²¹⁶ **Özbek vd**, 2013, s. 544; **Yaşar vd**, 2010: s. 4136; **Şen**, 2006: s. 611; **Parlar ve Hatipoğlu**, 2008: s. 2056; Diğer taraftan Özen bu suçta, istisnai de olsa icra hareketleri kısımlara bölünebiliyorsa teşebbüsün mümkün olduğunu savunmuştur. Bkz. **Özen**, 2009: s. 26

4.4.2. İştirak

Bu suçu, yukarıda da açıklandığı üzere, kişisel verileri sistem içinde yok etmekle yükümlü olan kimseler işleyebilecektir. Bu nedenle özgü suçlardan olan bu suça²¹⁷, bu şekilde bir görevi veya yetkisi olmayan kimseler, TCK'nın 40/2. maddesi uyarınca, ancak azmettiren veya yardım eden olarak katılabileceklerdir²¹⁸.

4.4.3. İçtima

Söz konusu suçun, aynı suç işleme kararının icrası kapsamında olmak üzere aynı kişiye karşı birden fazla defa işlenmesi halinde, zincirleme suç hükümleri uygulanacaktır. Ancak, aynı kişisel veriyle ilgili uzun zaman silmeme, yok etmeme durumunda eylem, tek suç olarak kalacaktır, zincirleme suç hükümleri uygulanmayacaktır (Yaşar vd, 2010: s. 4139; Parlar ve Hatipoğlu, 2008: s. 2056).

Ayrıca yok etmeme eylemi, birden fazla kimsenin kişisel verileri ile ilgili olursa, yine zincirleme suç hükümleri uygulanabilecektir. Çünkü fail tek bir eylemle (yok etmeme) birden fazla kişiye karşı aynı suçu işlemektedir (m. 43/2)

Kişisel verileri yok etmekle görevli olan fail, verileri yok etmeyip, aynı zamanda bu verileri bir başkasına verir veya yayarsa bu durumda, TCK'nın 136. ve 138. maddelerindeki suçlar oluşacak ve gerçek içtima hükümleri uygulanacaktır (Yaşar vd, 2010: s. 4139; Parlar ve Hatipoğlu, 2008: s. 2056).

4.5. SUÇUN NİTELİKLİ HALİ

4.5.1. Genel Olarak

TCK'nun 138. maddesine 21/2/2014 tarihli ve 6526 sayılı Kanunla eklenen fıkra ile yok edilmesi gereken verilerin Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması hâli ağırlaştırıcı neden olarak öngörülmüştür. Fıkra metni “*Suçun konusunun Ceza Muhakemesi Kanunu*

²¹⁷ Özgü suçlar konusunda ayrıntılı bilgi için bkz. **Kaymaz, Seydi**, “ 5237 Sayılı Türk Ceza Kanuna Göre İştirak Halinde İşlenen Suçlarda Nitelikli Hallerin Diğer Suç Ortaklarına Geçiş Sorunu”, GÜHFD, C. XVI, S. 2, Y. 2012, s. 121; **Dülger, Murat Volkan**, “Yeni Türk Ceza Kanununda Suç Ortaklığı”, Yeditepe Üniversitesi HFD, C. I, S. 2, Ocak 2005, s. 85–137, s. 31

²¹⁸ **Yaşar vd**, 2010: s. 4138; **Parlar ve Hatipoğlu**, 2008: s. 2056; Özbek, bu suça iştirakin her çeşidinin mümkün olduğunu, iştirak açısından bu suçun bir özellik göstermediğini beyan etmiş ise de, bu görüşe katılmak, yukarıda açıklanan gerekçeler nedeniyle, mümkün değildir. Bkz. **Özbek vd**, 2013, s. 544

hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması hâlinde verilecek ceza bir kat artırılır.” Şeklindedir.

Değişiklik gerekçesi olarak, “*Özel hayatın gizliliği konusunda Anayasada yer alan önemli bir düzenleme de kişisel verilerin korunmasına ilişkindir. Anayasanın 20 nci maddesinde herkesin kendisiyle ilgili kişisel verinin korunmasını isteme hakkına sahip olduğu düzenlenmiştir. Teklifte kişisel verilerin korunmasına ilişkin önemli düzenlemeler yapılmaktadır. Bu amaçla Türk Ceza Kanununda düzenlenen kişisel verileri; kaydetme, hukuka aykırı olarak verme, ele gecirme ve yok etmeme suçlarının cezaları önemli ölçüde artırılmaktadır. Ayrıca, yok edilmesi gereken verinin Ceza Muhakemesi Kanunu hükümlerine göre elde edilen bir veri olması durumunda daha ağır bir ceza verilmesi öngörülmektedir. Bu şekilde Ceza Muhakemesi Kanunu kapsamında uygulanan koruma tedbirleri vasıtasıyla elde edilen kişisel veri niteliğindeki bilgilerin daha etkin bir korumaya kavuşturulması amaçlanmaktadır.*” Hususları belirtilmiştir²¹⁹.

4.5.2. Ceza Muhakemesi Kanununa Göre Ortadan Kaldırılması veya Yok Edilmesi Gereken Veriler

Ceza Muhakemesi Kanuna göre ortadan kaldırılması veya yok edilmesi gereken verilerin neler olduğu 5271 sayılı Ceza Muhakemesi Kanununda, muhtelif maddelerde, açıkça düzenlenmiştir. Bunları aşağıdaki şekilde özetleyebiliriz:

4.5.2.1. Moleküler Genetik İncelemeler Sonucu Elde Edilen Kişisel Veriler

CMK’nın 75 ve 76. maddeleri uyarınca bir suça ilişkin delil elde etmek için şüpheli, sanık, mağdur veya diğer kişilerin vücudu üzerinde iç veya dış beden muayenesi yapılması sonucu bunlardan alınan kan veya benzeri biyolojik örnekler, saç, tükürük, tırnak gibi doku örnekleri üzerinde CMK’nın 78. Maddesi uyarınca yapılan moleküler genetik incelemeler sonucu elde edilen sonuçlar “kişisel veri” niteliğinde olup (m. 80) bu bilgilerin, 80. maddenin ikinci fıkrası uyarınca kovuşturmaya yer olmadığı kararına itiraz süresinin dolması, itirazın reddi, beraat

²¹⁹ Söz konusu ağırlştırıcı nedenin kabul ediliş gerekçesi için bkz.

http://www.tbmm.gov.tr/develop/owa/tasari_teklif_sd.onerge_bilgileri?kanunlar_sira_no=148569

Erişim T: 10/3/2014

veya ceza verilmesine yer olmadığı kararı verilip kesinleşmesi hallerinde Cumhuriyet Savcısının huzurunda derhal yok edilmesi gerekir.

Görüldüğü üzere CMK'nın 80. Maddesinde bu verilerin kişisel veri olduğu ve bunlara ihtiyaç kalmadığında yok edilmesi gerektiği açıkça düzenlenmiştir.

4.5.2.2. Kimlik Teşhisi İçin Elde Edilen Kişisel Veriler

CMK'nın 81. maddesine göre, üst sınırı iki yıl veya fazla hapis cezasını gerektiren bir suçtan dolayı şüpheli veya sanığın kimliğinin teşhisi için gerekli olması halinde, Cumhuriyet Savcısının emriyle fotoğrafı, beden ölçüleri, parmak ve avuç içi izi, bedeninde yer almış olup teşhisini kolaylaştıracak diğer özellikleri ile sesi ve görüntüleri kayda alınarak, soruşturma ve kovuşturma işlemlerine ilişkin dosyaya konulabilmektedir. Ancak, madde hükmüne göre, söz konusu kayıtların, kovuşturmayla yer olmadığı kararına itiraz süresinin dolması, itirazın reddi, beraat veya ceza verilmesine yer olmadığı kararı verilip kesinleşmesi hallerinde Cumhuriyet Savcısının huzurunda derhal yok edilmesi ve bu hususun tutanağa geçirilmesi gerekmektedir.

4.5.2.3. Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi Sonucu Elde Edilen Kişisel Veriler

CMK'nın 135. maddesinde sayılan suçlardan biri dolayısıyla yapılan soruşturma ve kovuşturmada belirli koşullarla şüpheli veya sanığın telekomünikasyon yoluyla iletişimi tespit edilebilmekte, dinlenebilmekte, kayda alınabilmekte ve sinyal bilgileri değerlendirilmektedir. Maddenin üçüncü fıkrasına göre, şüpheli veya sanığın tanıklıktan çekinebilecek kişilerle arasındaki iletişimi, kayda alınamaz. Kayda alma gerçekleşikten sonra bu durumun anlaşılması halinde ise, alınan kayıtların derhal yok edilmesi zorunludur.

Diğer yandan CMK'nın 137. maddesinin üçüncü fıkrası uyarınca, iletişimin tespiti, dinlenmesi ve kayda alınması işleminin Cumhuriyet savcısının kararına dayalı olarak yapılması ve hakim onayının alınamaması ya da bu husustaki kararın uygulanması sırasında şüpheli hakkında kovuşturmayla yer olmadığına karar verilmesi hallerinde, tedbirin uygulanmasına Cumhuriyet savcısı tarafından derhal son verilmesi, bu durumda, yapılan tespit veya dinlemeye ilişkin kayıtların

Cumhuriyet savcısının denetimi altında geç on gün içinde yok edilerek durumun bir tutanakla tespit edilmesi gerekmektedir²²⁰.

4.5.2.4. Gizli Soruşturmacı Görevlendirilmesi Sonucu Elde Edilen Kişisel Veriler

CMK'nın 139. Maddesine göre gizli soruşturmacı görevlendirilmesi suretiyle elde edilen kişisel bilgiler de yok edilmesi gereken kişisel verilerdendir. Maddeye göre, *“gizli soruşturmacı görevlendirilmesi suretiyle elde edilen kişisel bilgiler, soruşturmacının görevlendirildiği ceza soruşturması ve kovuşturması dışında kullanılamaz. Suçla bağlantılı olmayan kişisel bilgiler derhâl yok edilir.”* (m. 139/6)²²¹.

Burada kanun koyucu verilere ilişkin bir daraltma yapmamıştır. Kimliği belli veya belirlenebilir bir kişiyle ilgili her türlü bilgi kişisel veri kabul edildiğinden, burada gizli soruşturmacı tarafından, görevlendirildiği olaydaki şüpheli hakkında toplanan bilgiler kişisel veri olarak kabul edilecek ve bu veriler CMK hükümlerine göre yok edilmesi gereken verilerden sayılacaktır.

4.5.2.5. Teknik Araçlarla İzleme Sonucu Elde Edilen Kişisel Veriler

CMK'nın 140. Maddesinde sayılan suçların işlendiği hususunda somut delillere dayanan kuvvetli şüphe sebepleri bulunması ve başka suretle delil elde edilememesi hâlinde, şüpheli veya sanığın kamuya açık yerlerdeki faaliyetleri ve işyeri teknik araçlarla izlenebilir, ses veya görüntü kaydı alınabilir (m. 140/1)²²². Kişinin sesi ve görüntüsünün kişisel veri olduğu çalışmamızın birinci bölümünde açıklanmıştı.

CMK'nın 140. maddesine göre teknik araçlarla izleme tedbiriyle elde edilen deliller, maddede sayılan suçlarla ilgili soruşturma ve kovuşturma dışında kullanılamaz; ceza kovuşturması bakımından gerekli olmadığı takdirde Cumhuriyet savcısının gözetiminde derhâl yok edilir (m. 140/6). Bu delillerden, örneğin kişinin

²²⁰ Ayrıntılı bilgi için bkz. **Centel ve Zafer**, 2013: s. 403-415

²²¹ CMK'da gizli soruşturmacı görevlendirilmesi usul ve esasları hakkında ayrıntılı bilgi için bkz. **Sezer, Yasin/İpek, Ali İhsan/Parlak, Engin**, Adli ve İstihbari Amaçlı İletişimin Denetlenmesi Gizli Soruşturmacı ve Teknik Araçlarla İzleme, Seçkin Yayınevi, Ankara, 2012, s. 251

²²² Ayrıntılı bilgi için bkz. **Sezer vd.**, 2012: s. 278

sesi veya görüntüsü, kişisel veri niteliğinde olduğundan CMK hükümlerine göre yok edilmesi gereken veri olarak kabul edileceklerdir.

İşte CMK’da düzenlenen bu kurallara uygun şekilde elde edilen verilerin, yine CMK da belirtilen usul ve sürede yok edilmemesi halinde 138. maddedeki suç oluşacak, ayrıca bu verilerin CMK hükümleri uyarınca yok edilmesi gereken veriler olması nedeniyle failin cezası bir kat artırılacaktır (m. 138/2).

5. YARGILAMA USULLERİ

5.1. Genel Olarak

Kişisel verilere karşı işlenen suçlarda yargılama usulleri benzer olması nedeniyle tek başlık altında açıklanmıştır. Bu kapsamda çalışmamıza konu suçların soruşturma usulü, görevli ve yetkili mahkemenin neresi olduğu ve yargılama sonucunda verilecek cezaların neler olduğu açıklanacaktır.

5.2. Soruşturma Usulü

Aynı bölümde yer alan özel hayatın gizliliğini koruyan diğer suçların (m. 132, 133 ve 134) aksine, bu suçların soruşturma ve kovuşturması için, şikâyet koşulu aranmamaktadır. Kanun koyucu, bu suçların soruşturma ve kovuşturulmasında kişisel yarara bakmamış, toplumsal yararı üstün tutmuştur (Akyürek, 2011: s. 56). Bu nedenle bu suçların takibi şikâyete bağlı değildir. Bu suçların işlendiğini resen veya ihbar üzerine öğrenen kolluk veya Cumhuriyet savcılıklarının resen harekete geçerek soruşturma başlatması gerekmektedir.

Nitekim Yargıtay da bir kararında²²³; “*Dosya kapsamına göre; erkek arkadaşının sanık Demet ile kendisini aldattığını düşünen sanık Ayla’nın, bir sosyal paylaşım sitesine □ Olga Erçin□ adıyla üyelik işlemleri yaparak, elektronik posta adresi oluşturduğu sitede, bir başka bayana ait göğüs dekolteli bir resim koyup, sanık Demet’e ait cep telefonu numarasına da yer vermesi sonucu, tanımadığı kişiler tarafından telefonundan aranarak cinsel içerikli arkadaşlık teklifleri alan sanık Demet’in, cep telefonu numarasını yayan kişinin sanık Ayla olduğunu öğrenmesi üzerine, kendisini telefonundan arayan tanımadığı kişilere, telefon numarasını değiştirdiğini belirterek, sanık Ayla’nın kullanımındaki cep telefonu numarasını*

²²³ Yargıtay 12. CD. nin Esas No: 2012/22005 Karar No: 2013/24489 sayılı kararı.

verdiği ve sanık Ayla'nın da tanımadığı kişiler tarafından telefonundan aranarak rahatsız edilmesi üzerine her iki sanığın birbirlerinden şikâyetçi olup, bilahare şikâyetlerinden vazgeçtikleri olayda; TCK'nın 139/1. maddesi gereğince, sanıkların üzerlerine atılı verileri hukuka aykırı olarak verme veya ele geçirme suçunun, soruşturulması ve kovuşturulmasının şikâyetle bağlı olmadığı gözetilmeden, kovuşturma aşamasında her iki mağdur sanığın şikâyetlerinden vazgeçtiklerinden bahisle, yazılı şekilde düşme kararı verilmesi,... bozmayı gerektirmiştir.” Şeklinde tespitte bulunarak bu suçların takibinin şikâyetle bağlı olmadığını belirtmiştir.

Kamu görevlilerinin görevi sebebiyle bu suçlardan herhangi birini işlemesi halinde, soruşturmanın, 4483 sayılı Memurlar ve diğer Kamu Görevlilerinin Yargılanması Hakkında Kanuna göre yetkili merciden soruşturma izni alındıktan sonra yapılması gerekir. Bu hallerde ön soruşturmacının (muhtakik) atanmasından soruşturma izni kararının kesinleşmesine kadar zamaşıımı duracaktır²²⁴.

5.3. Görevli Mahkeme

Ceza mahkemelerinin görevleri, yani hangi suçlara ilişkin davalara bakabilecekleri, 5235 sayılı Adli Yargı İlk Derece Mahkemeleri İle Bölge Adliye Mahkemelerinin Kuruluş, Görev Ve Yetkileri Hakkında Kanunun 10 ila 14. maddeleri arasında belirlenmiştir. Buna göre; Kanunların ayrıca görevli kıldığı hâller saklı kalmak üzere, sulh ceza hâkimliği ve ağır ceza mahkemelerinin görevleri dışında kalan dava ve işlere, daha açık bir ifadeyle kanunda suç için öngörülen cezanın üst sınırı on yıla kadar (on yıl dâhil) olan davalara asliye ceza mahkemelerinde; on yıldan fazla hapis cezası öngörülen suçlar ise ağır ceza mahkemelerinde görülecektir (m. 10-11-12)²²⁵. Ancak bazı suçlar için kanunda öngörülen hapis cezası miktarına bakılmaksızın ağır ceza mahkemesinde görülmeleri gerekir. Bunlar da yağma, irtikâp, resmi belgede sahtecilik, nitelikli dolandırıcılık suçlarıdır (m. 12).

²²⁴ Yaşar/Gökcan/Artuç, s. 4122

²²⁵ 18/6/2014 tarihli ve 6545 sayılı Türk Ceza Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanunun 46 ncı maddesiyle 5235 sayılı Kanunun 8. maddesinde yer alan, “sulh ceza,” ibaresi madde metninden çıkarılmak suretiyle sulh ceza mahkemeleri kaldırılmış, yerine sadece belli işlere bakmakla görevli sulh ceza hâkimlikleri kurulmuştur.

Çalışmamıza konu suçlara bakıldığında;

TCK'nın 135. maddesinde düzenlenen suç için öngörülen hapis cezası, “bir yıldan üç yıla kadar olduğundan” bu suç, 5235 sayılı Yasanın 10-14. maddeleri uyarınca Asliye Ceza Mahkemelerinde görülecektir.

TCK'nın 136. Maddesinde düzenlenen suç için öngörülen hapis cezası, “iki yıldan dört yıla kadar olduğundan” bu suç, 5235 sayılı Yasanın 10-14. maddeleri uyarınca Asliye Ceza Mahkemelerinde görülecektir.

TCK'nın 138. maddesinde düzenlenen suç için öngörülen hapis cezası, “bir yıldan iki yıla kadar olduğundan”, bu suç, 5235 sayılı Yasanın 10-14. maddeleri uyarınca Asliye Ceza Mahkemelerinde görülecektir.

5235 sayılı Kanunun 14. maddesi uyarınca mahkemelerin görevlerinin belirlenmesinde ağırlaştırıcı veya hafifletici nedenler gözetilmemektedir. Bu nedenle, 135 ve 136. maddelerdeki suçlar için öngörülen örneğin, Suçun kamu görevlisi tarafından görevinin verdiği yetki kötüye kullanılması suretiyle işlenmesi ya da belli bir meslek veya sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenmesi halinde, cezanın artırılacak olması, görevli mahkemeyi değiştirmeyecektir. Keza 138. Maddenin ikinci fıkrasındaki ağırlaştırıcı nedenin uygulanmasında da görevli mahkeme değişmeyecektir (Yaşar vd, 2010: s. 4122).

5.4. Yetkili Mahkeme

CMK'nın 12. Maddesine göre, davaya bakmak yetkisi, suçun işlendiği yer mahkemesine aittir. Soruşturma yapma yetkisinde bu mahkeme çevresindeki savcılığa daha açık bir ifade ile suçun işlendiği yer savcılığına aittir.

Buna göre; Kişisel Verilerin Kaydedilmesi suçunda yetkili savcılık ve mahkeme kaydın gerçekleştirildiği; Verileri Yok Etmeme suçunda ise verilerin tutulduğu sistemin bulunduğu yer savcılıkları ve mahkemeleridir.

Verilerin Verilmesi Yayılması ve Ele Geçirilmesi suçunda ise, suçun işlendiği yeri ilk etapta tespit etmek kolay değildir. Verme ve ele geçirme suçunda verme ve ele geçirme eyleminin yapıldığı yer suçun işlendiği yer olarak kabul edilebilir. Ancak yayma suçunda ise genellikle bu eylem internet gibi sanal ağlar üzerinden veya basın

yayın yoluyla yapıldığı için somut olaya göre değerlendirme yapmak gerekmektedir. CMK'nın 12. Maddesinin üçüncü fıkrasına göre, *“Suç, ülkede yayımlanan bir basılı eserle işlenmişse yetki, eserin yayım merkezi olan yer mahkemesine aittir. Ancak, aynı eserin birden çok yerde basılması durumunda suç, eserin yayım merkezi dışındaki baskısında meydana gelmişse, bu suç için eserin basıldığı yer mahkemesi de yetkilidir.”* Aynı şekilde CMK'nın 12. Maddesinin beşinci fıkrasına göre, *“Görsel veya işitsel yayınlarda da bu maddenin üçüncü fıkrası hükmü uygulanır. Görsel ve işitsel yayın, mağdurun yerleşim yerinde ve oturduğu yerde işitilmiş veya görülmüşse o yer mahkemesi de yetkilidir.”* Buna göre kişisel verileri yayma suçu, kitap, dergi veya gazete gibi basılmış eserler vasıtasıyla işlenmişse, suçun işlendiği yer kural olarak eserin yayım merkezinin bulunduğu yerdir. Ancak bu eserin birden çok yerde basılması durumu varsa ve suç, eserin yayım merkezi dışındaki baskısında meydana gelmişse, bu suç için eserin basıldığı yer mahkemesi de yetkili olacaktır (Kunter vd, 2006: s. 343).

Diğer yandan kişisel verileri yayma suçunun görsel ve işitsel yayınlarla yani televizyon, radyo ve internet siteleri üzerinden işlenmesi halinde de kural olarak bu yayınların yayım merkezi mahkemeleri yetkilidir. Ancak burada bu yayınların aynı anda dünyanın her yerinden işitilmesi veya görülmesi olanağı bulunduğundan kanun koyucu burada bir kolaylık sağlamak suretiyle görsel ve işitsel yayının, mağdurun yerleşim yerinde ve oturduğu yerde işitilmiş veya görülmüşse o yer mahkemesinin de yetkili olacağını hüküm altına alınmıştır. Buna göre televizyon, radyo veya internet üzerinden işlenen verileri yayma suçu mağdurun yerleşim yeri mahkemeleri ve savcılıklarında görülebilecektir.

5.5. Yaptırım

Kişisel verilere karşı işlenen bu suçların için TCK'da öngörülen hapis cezalarının miktarı, daha öncede açıklandığı üzere, 6 Mart 2014 tarihinde yürürlüğe giren 21/2/2014 tarihli ve 6526 sayılı Terörle Mücadele Kanunu ve Ceza Muhakemesi Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun ile artırılmıştır. Değişiklik gerekçesi, *“Anayasanın 20 nci maddesinde, herkesin kendisiyle ilgili kişisel verinin korunmasını isteme hakkına sahip olduğu düzenlenmiştir. Kişisel verilerin ve özel hayatın daha etkin korunması amacıyla*

kişisel verileri hukuka aykırı olarak kaydedenlere verilecek ceza artırılmaktadır.” şeklindedir²²⁶.

Bu değişiklikten sonra 135. maddede düzenlenen kişisel verilerin kaydedilmesi suçu için öngörülen ceza, “bir yıldan üç yıla kadar hapis” cezasıdır. Maddenin ikinci fıkrasında belirtilen hasas verilerin kaydedilmesi durumunda ise fıkra metninde “yukarıdaki fıkra hükümlerine göre cezalandırılır “ ibaresine yer verildiğinden bu durumda da verilecek ceza birinci fıkrayla aynı nitelikte olacaktır. Ancak ikinci fıkrada sınırlı şekilde sayılan veriler, diğer kişisel verilerden farklı olarak hukuka aykırı kaydedilmeleri durumunda ayrımcılığa yol açabilecek nitelikte olmaları bakımından bireyler açısından özellikli bir yere sahip olup, bu verilerin kaydedilmesi ile diğer kişisel verilerin kaydedilmesi eylemleri hakkında aynı cezanın öngörülmüş olması yerinde olmamıştır. Bu tür verilerin bireyler açısından taşıdıkları önem göz önüne alınarak daha ağırceza gerektiren nitelikli hal olarak öngörülmesi daha yerinde olacaktır (Şener, 2011: s. 76).

Diğer yandan madde metnindeki düzenleme aynı cezayı öngörmüş olsa da suçun konusunun önemi nedeniyle TCK’nın 61. maddesi uyarınca temel ceza belirlenirken alt sınırdan uzaklaşılabilir.

TCK’nın 136. Maddesinde düzenlenen suç için öngörülen hapis cezası, “iki yıldan dört yıla kadar” dır.

TCK’nın 138. maddesinde düzenlenen suç için öngörülen hapis cezası, “bir yıldan iki yıla kadar” dır. Maddenin ikinci fıkrasında suçun konusunun ceza muhkamesince yok edilmesi gereken veriler olması halinde verilecek ceza bir kat artırılacağından, verilecek ceza iki yıldan dört yıla kadar çıkabilecektir.

Benzer şekilde, 135 ve 136. Maddedeki suçların, kamu görevlisi tarafından görevinin verdiği yetki kötüye kullanılması suretiyle işlenmesi ya da belli bir meslek veya sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenmesi halinde verilecek ceza yarı oranında artırılacaktır. Örneğin 135. Maddeye göre alt sınırdan bir yıl hapis cezası verilmesi halinde yarı oranında artırılarak bir yıl altı ay hapis cezası verilebilecektir.

²²⁶ Değişiklik gerekçesi için bkz.

http://www.tbmm.gov.tr/develop/owa/tasari_teklif_sd.onerge_bilgileri?kanunlar_sira_no=148569

Erişim T: 10/3/2014

SONUÇ

Çağdaş dünyanın, teknolojinin gelişimine koşut olarak en güncel konularından biri olan kişisel verilerin korunması sorunu, son derece geniş olup aslında her gün defalarca karşılaşılan bir alandır. Bir kişinin evindeki bilgisayarından internet üzerindeki herhangi bir siteye girmesinden, alışveriş merkezinde indirim kuponu kazanmasına kadar her alanda kişisel verilerin, bilerek veya bilmeyerek üçüncü kişilere iletilmesi, hatta verilerin söz konusu kişilerce ya da başkalarınca işlenmesine olanak sağlanması söz konusudur (Akyürek, 2011: s. 59).

Sürekli içinde bulunulan bu alanda, kişilerin kişilikleri ve özel hayatlarının gizliliği korunarak özgürce hareket etmelerinin sağlanabilmesi için kişisel verilerin korunmasına yönelik ayrıntılı, güncel düzenlemelerin yapılması gerekmektedir.

Konuyu uzun yıllardır tartışan ülkeler, gerek anayasal ve yasal kurallarla, idari düzenlemelerle gerekse yargısal kararlar ışığında hayli önemli bir mesafe kat etmişlerdir. Bu kapsamda, uluslararası alanda kişisel verilerin korunması konusu, somut olarak ilk defa İktisadi İşbirliği ve Kalkınma Teşkilatı (OECD) tarafından 1980 yılında ele alınmış ve kişisel verilerin işlenmesi konusunda temel ilkelerin belirlendiği “OECD Rehber İlkeler” i çıkarılmıştır.

Temel amacı, üye ülkeler arasında hukuk birleştirmesi ve uyumu olan Avrupa Konseyi ise ülkeler arasında gelişmiş telekomünikasyon araçlarıyla gerçekleştirilen hızlı sınır ötesi bilgi akışı karşısında, kişilik haklarının korunmasında üye devletler milli mevzuatının yetersiz kalması karşısında, kişisel verilerin korunması alanında uluslararası bir sözleşme hazırlamak üzere çalışmalar yapmıştır. Bu bağlamda, “Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması”na ilişkin 108 sayılı Avrupa Konseyi Sözleşmesi 28 Ocak 1981 tarihinde imzaya açılmış ve aynı tarihte Konsey üyesi devletler ile birlikte Türkiye tarafından da imzalanmıştır. Söz konusu Sözleşmenin 4. maddesi gereğince sözleşmenin onaylanmış sayılması için, imzalayan devletin sözleşmede öngörülen ilkeler çerçevesinde bir Kanun kabul etmesi zorunludur. Ancak Türkiye, Kişisel Verilerin Korunması Kanunu Tasarısını hazırlamış olmasına rağmen Tasarı henüz kanunlaşamadığı için, bu sözleşme hukukumuzda uygulanabilir hale gelememiştir.

AK'nin 108 sayılı Sözleşmesi, bir taraftan Konseye üye ülkelerde bireylerin kişiliklerinin yeknesak bir düzeyde korunmasını sağlamış, diğer taraftan da sınır ötesi veri akışının standartlarını belirlemiştir. Öyle ki, Sözleşmenin 12 nci maddesine göre, bir devlet verilerin korunması konusunda bunların eşdeğer düzeyde korunmasına ilişkin mevzuatı bulunmayan diğer bir devlete, sınır ötesi veri aktarımını yasaklayabilir. Nitekim bu bağlamda Türkiye'de yasal düzenleme bulunmamasının sonuçları uygulamada da görülmeye başlanmıştır. Örneğin, adli yardım anlaşmalarının uygulanması çerçevesinde, başta Almanya olmak üzere, Konseye üye diğer devletler, Türk mahkemelerince yapılan kişiler hakkındaki adres tespiti, istinabe gibi istemleri, Türkiye'nin konuya ilişkin eşdeğer koruma mevzuatı bulunmadığı için geri çevirmektedirler. Aynı şekilde, bu durum Avrupa Birliği ile gerçekleştirilen gümrük birliği çerçevesinde, Türkiye ile Avrupa Birliği üyesi devletler gümrük idareleri arasındaki bilgi akışını da olumsuz yönde etkilemektedir.

Öte yandan, Avrupa Konseyinin anılan Sözleşmesinden sonra Avrupa Birliği de konuya ilişkin çalışmalarını sürdürmüş ve üye devlet bireylerinin verilerin korunması, üye ülke mevzuatları arasındaki farklılık ve çelişkilerin giderilmesi ve kişisel verilerin korunması konusunda belli bir standart sağlanarak Birlik içerisinde verilerin serbest dolaşımını sağlamak üzere, 30 Ekim 1995 tarihinde 95/46/EC sayılı Kişisel Verilerin Korunması Direktifini kabul ederek yürürlüğe sokmuştur. Direktifle, bütün üye ülkelerdeki bireylerin kişisel verilerinin gizliliğinin üst düzeyde korunması ve kişisel verilerin Avrupa Birliği içerisinde özgür dolaşımını sağlayacak açık ve kalıcı bir düzenleme yapılması amaçlanmıştır. Avrupa Birliği ile Türkiye arasında gümrük birliği antlaşması yapılmasından sonra 10-11 Aralık 1999 tarihlerinde gerçekleştirilen Avrupa Birliği Helsinki Zirvesi sonucunda, Türkiye'nin tam üye adayı olarak kabul edilmiş olmasıyla, tam üyeliğe yönelik katılım süreci çerçevesinde birçok alanda mevzuat uyumu çalışmaları yapıldığından, kişisel verilerin korunmasına ilişkin yasa çalışmalarında da, Birlik mevzuatı ile Türk mevzuatı arasında uyum sağlamanın yerinde olacağı düşünülmüş ve bu amaçla çalışmalarda söz konusu direktif de göz önünde tutulmuştur.

Ayrıca, kişisel verilerin korunması konusunda bir kanun hazırlanması, Ülkemizin Katılım Ortaklığı Belgesine cevap olarak hazırladığı 2003 Ulusal

Programında taahhüt ettiđi yükümlölüklerdendir. Ancak, Türkiye bu yükümlölüğü yerine getirerek anılan kanunu çıkarmamıştır (Yaşar vd, 2010: s. 4116).

Bunun karşısında Türkiye’de kişisel verilerin korunması konusunda çeşitli adımlar atılmıştır.

Kişisel verilerin korunması Medeni Hukuk alanında kişilik haklarının ihlali kapsamında değerlendirilmiş ve Türk Medeni Kanunun 24 ve 25. maddelerine göre bir kısım koruma getirilmiştir. Nitekim kişisel verilerin korunması, kişinin manevi şahsiyetini korumak amacıyla kabul edilmiş bir korumadır. Bu alan kişinin özel hayatının önemli bir kısmını oluşturmaktadır.

İdare hukuku açısından, kişisel verilerin korunması büyük önem arz etmektedir. Çünkü günümüzde en büyük veri toplayıcısı devlettir. Devlet, sosyal devlet olmanın gereklerini yerine getirebilmek, halkın huzur ve refahını sağlayabilmek amacıyla vatandaşlarının doğumundan ölümlerine kadar verilerin toplamakta ve arşivlemektedir. Bu nedenle bu alanda da çeşitli düzenlemeler yapılmıştır. Kamu kurumlarının kamu hizmetlerinin yürütülmesinde veya kanundan kaynaklanan veri toplama yetkisi kapsamında topladıkları, kaydettikleri veya başka kurumlarla paylaştıkları verilerin korunması amacıyla, Nüfus Kanunu, Adli Sicil Kanunu, Polis Vazife ve Selahiyet Kanunu gibi çeşitli kanunlarda bu verilerin toplanma usul ve esasları ile gizliliğinin nasıl sağlanacağına ilişkin düzenlemeler yapılmıştır.

Ceza Muhakemesi Hukuku açısından da kişisel veriler korunması hayati önem arz ettiğinden bu alanda ayrıntılı ve koruyucu hükümler bulunmaktadır. Bu kapsamda, yürütölen soruşturma ve kovuşturmalar esnasında, delilerin toplanması ve değerlendirilmesi amacıyla, şüpheli, sanık veya mağdurdan alınan parmak izi, DNA profili gibi kişisel veriler ile şüpheli veya sanığın iletişiminin tespiti sonucu ya da teknik takip sonucu elde edilen kişisel veri niteliğinde kayıtların, alınması, kullanılması ve yok edilmesi aşamalarının CMK’da ayrıntılı şekilde düzenlendiğı görölmektedir.

Diğer taraftan kişisel verilerle ilgili belkide mevzuatımızdaki en önemli gelişme ve düzenleme ise kişisel verilerin korunması hakkının anayasal güvenceye kavuşturulmasıdır. 2010 yılında yapılan halkoylamasıyla kabul edilip yürürlüğe giren

5982 sayılı Kanunla Anayasanın özel hayatın gizliğini düzenleyen 20. Maddesine bir fıkra eklenerek; Herkesin kendisi ile ilgili kişisel verilerin korunmasını isteme hakkına sahip olduğu, bu hakkın, kişinin kendisi ile ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsadığı, kişisel verilerin, ancak kanunda öngörülen hallerde veya kişinin açık rızası ile işlenebileceği, kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği hüküm altına alınmıştır.

Anayasada öngörülen bu düzenlemede kişisel verilerin nasıl işleneceği yani bu hakka nasıl hukuka uygun şekilde müdahale edileceği, anayasanın diğer temel hak ve özgürlükleri düzenleyen maddelerinden farklı bir şekilde düzenlenmiştir. Buna göre kişisel veriler ancak kanunda öngörülen hallerde veya kişinin açık rızası ile işlenebilecektir. Anayasaya göre kanunda bir düzenleme yoksa veya verilerinin işlenmesine kişinin açık rızası yoksa veri işleme hukuka aykırı olacaktır. Ancak bu konuda Anayasada düzenlenen hususların uygulamasını gösterecek bir kanun henüz yürürlüğe girmediği için bu hakka müdahalenin hangi hallerde hukuka aykırı olacağı hususunda tereddütler giderilebilmiş değildir.

Kişisel verilerin korunması hakkının ihlal edilmesi halleri 12/10/2004 tarihinde yürürlüğe giren 5237 sayılı TCK'da ilk defa suç olarak düzenlenmiştir. Bu kapsamda TCK'nun "Kişilere Karşı Suçlar" başlıklı ikinci kısmının "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" başlıklı dokuzuncu bölümünde; 135. maddede "kişisel verilerin kaydedilmesi" suçu, 136. maddede "kişisel verileri hukuka aykırı olarak verme veya ele geçirme" suçu, 138. maddede, "verileri yok etmeme" suçu düzenlenmiştir. Bu suçların kamu görevlileri tarafından görevin verdiği yetkinin kötüye kullanılması suretiyle veya belli bir meslek veya sanatın sağlığı kolaylıktan yararlanmak suretiyle işlenmesi hali 137. maddede ağırlaştırıcı neden olarak düzenlenmiştir.

135. maddede düzenlenen kişisel verilerin kaydedilmesi suçunda; kişisel verileri hukuka aykırı olarak kaydeden kişi maddedeki şekilde cezalandırılacaktır. Burada suçun konusunu oluşturan kişisel veri, belirli veya kimliği belirlenebilir bir kişiye ilişkin her türlü bilgidir. Bu verilerin kişinin hayatın gizli ve özel alanına

ilişkin olabileceği gibi, hayatın ortak diğer bir deyimle genel alanına yönelikte olabilir. Zira madde metninde kişisel veri için herhangi bir sınırlama getirilmemiştir. Burada önemli olan verinin bir kişiyle ilişkilendirilmesidir. Suçun konusunu oluşturan kişisel verinin bu tanımı ve kapsamı diğer suçlar açısından da geçerlidir

Maddenin ikinci fıkrasında ise kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimseye de aynı hüküm uyarınca ceza verilmesi öngörülmüştür. Burada dikkat edilmesi gereken husus kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine ilişkin verilerin kişisel veri olarak kaydedilmesi mutlak olarak yasaklanmış, bunlar için eylemin hukuka aykırı olmasına gerek duyulmamıştır. Kanunkoyucu burada bu verilerin hassas veriler olması kişilerin bu verilerin kaydedilmesi nedeniyle ayrımcılığa uğraması riski nedeniyle bu şekilde bir düzenleme yapmıştır. Ayrıca kamuoyunda fişleme olarak bilinen kişilerin hassas verilerin yasadışı şekilde kaydedilerek arşivlenmesi ve bu verileri kişilerin aleyhine kullanılmasının engellenmesi amaçlanmıştır. Kişilerin ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgiler ise devletin suçla mücadelesi ve bazı kamu hizmetlerinin verilebilmesi için işlenebilen veriler olması nedeniyle bunlar sadece hukuka aykırı olarak kaydedilmeleri halinde suç oluşturacaklardır.

Ayrıca buradaki kaydetme kavramı, onları tekrar ve başkaları tarafından gerektiğinde kullanılabilecek durumda hazır etmek anlamına gelmektedir. Kaydetmek, verileri kâğıt ve benzeri şeyler üzerine yazmak, çizmek, işaretlemek biçiminde olabileceği gibi, ses bantlarına, CD'lere, ya da bilgisayar veya harddisk gibi dijital ortama almak biçiminde de olabilir. Nitekim bu husus madde gerekçesinde, “kişisel verilerin bilgisayar ortamında veya kâğıt üzerinde kaydedilmesi arasında bir ayrım gözetilmemiştir” şeklinde açıklanmıştır.

136. maddede düzenlenen kişisel verileri verme ve ele geçirme suçunda; kişisel verileri hukuka aykırı olarak bir başkasına veren, bu verileri yayan veya ele geçiren kişi cezalandırılacaktır. Suçun konusu yukarıda açıklandığı gibi kişisel veridir. Madde metninde kişisel veriler için bir tasnif veya sınırlandırma yapılmadığı için her türlü kişisel veriye karşı bu suç işlenebilecektir Bu suçta da hukua aykırılık

ibaresi tipikliğin bir unsuru olarak düzenlenmiştir. Buna hukuka özel aykırılık halleride denilmektedir. Burada suçun tipik olabilmesi için ceza kanunu haricindeki herhangi bir kanun tarafından bu eylemlere izin verilmemesi gerekmektedir. Eğer bir başka kanun tarafından verileri bir başkasına verme eylemine izn veriliyorsa eylem hukuka uygun kabul edilecektir. Diğer yandan verme, kişisel verileri bir başka kişiye herhangi bir yöntemle iletmektir. Yaymak, verilerin içeriğinin birçok kişinin öğrenebileceği şekilde başkalarının bilgisine sunulması, duyurulmasıdır. Bu nedenle verme eylemi iki kişiyi ilgilendirirken, yaymak fiili birden fazla kişiyi hedeflemektedir. Burada ağırlıklı olarak kişilerin özel yaşamlarının gizliliği korunmaktadır. Zira kişinin verilerinin, istemi dışında veya kanuna aykırı olarak başkalarının bilgisine sunulması kişinin birçok açıdan zararına neden olabilecektir. Örneğin, adli sicil kayıtlarının, CMK hükümlerine göre yasal tespit sonucu elde edilen telefon konuşma içeriklerinin, malvarlığı bilgilerinin, uçak seyahatlerinin, konaklama bilgilerinin, bazı internet sitesi üyeliklerinin ilişkin verilerin başkalarına verilmesi kişinin en genel olarak kişilik haklarının ihlali niteliğinde olacaktır.

138. maddede düzenlenen verileri yok etmeme suçunda ise, kanunların belirlediği sürelerin geçmiş olmasına rağmen verileri sistem içinde yok etmekle yükümlü olanların bu yükümlülüklerini yerine getirmemeleri cezalandırılmaktadır. Burada bu suçu sadece kamu görevlileri değil, kanunla verileri yok etme yükümlüğü yüklenen kişiler de işleyebilecektir. Bu suçta hukuka aykırılık ibaresine yer verilmemiştir. Esasında burada doğrudan kanuna atıf yapılmakla birlikte, kanuna aykırıktan bahsedilebilir. Nitekim kanunlarda belirlenen süreler dolmadan bu suç işlenemeyecektir. Burada suçun konusunu oluşturan veriler hukuka uygun şekilde sistem içinde tutulan kişisel verilerdir. Maddeye 21/2/2014 tarihli ve 6526 sayılı Kanunla eklenen fıkra ile yok edilmesi gereken verilerin Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması hâli ağırlaştırıcı neden olarak öngörülmüştür.

Maddede belirtilen sistemin, bir bilişim sistemi mi olduğu yoksa fiziki bir dosyalama sistemi mi olduğu hususunda bir açıklık yoktur. Madde gerekçesinde, hukuka uygun şekilde kaydedilmiş verilerin belirlenen sürelerde yok edilmemesinin suç olarak tanımlandığı belirtilmiştir. Bu açıdan gerekçede de bir açıklık yoktur. Ancak 135. Madde deki suçta kaydetme eylemi açısından fiziki kayıt ile otomatik

bir sisteme kayıt arasında fark görülmemektedir. Kanunlarda da sadece bilişim sisteminde tutulan verilere özgü bir düzenleme olmadığından, kanaatimizce burada “sistemi” geniş olarak yorumlamak gerekmektedir. Bu nedenle bir dosya içinde tutulan verilerde suçun konusu oluşturacağı gibi, UYAP, MERNİS gibi bilişim sistemlerinde tutulan verilerde suçun konusunu oluşturabileceklerdir.

Yukarıda açıklanan kişisel verilere karşı işlenen suçlar, yerinde olmakla birlikte bazı konularda tereddütler, bazı konularda da eksiklikler bulunmaktadır. Bu sorunlara ilişkin eleştiriler çalışmanın ilgili kısımlarında da belirtildiği üzere doktrin ve uygulamacılar tarafından da zaman zaman dile getirilmiştir.

İlk olarak “kişisel veri” kavramı yasal düzeyde henüz tanımlanmış değildir. Avrupa ülkelerinde uygulanan Avrupa Birliği Direktifi'ndeki tanımın yanında ona paralel olarak yasal tanımlamalar da yapılmıştır (Örneğin Fransa'da 78-17 sayılı yasa m. 2). Oysa Türk Hukuku açısından bu tanımlamayı yapan “Kişisel Verilerin Korunması Kanunu Tasarısı” henüz yasalaşamamıştır. Tasarı'nın 3. maddesinin 1. fıkrasının (ç) bendinde kişisel veri, “Belirli veya kimliği belirlenebilir bir gerçek kişiye ilişkin bütün bilgiler” olarak açıklanmaktadır. Ancak TCK'nın gerek tanımlar başlıklı 6. maddesinde gerek kişisel verilere karşı suçların düzenlendiği maddelerde böyle bir tanım yapılmamış olması nedeniyle, kişisel verinin kapsamı, hangi verilerin özel hayatın gizliği alanına girdiği veyahutta günlük hayatta herkes tarafından bilinebilen kişisel verilerin suç boyutuyla kişisel veri olarak değerlendirilip değerlendirilmeyeceği hususları netlik kazanmış değildir. Daha doğrusu bu husus hatalı uygulamalara neden olabilmektedir. Zaten ilgili hükümlerinin yaklaşık dokuz yıldır yürürlükte olmasına rağmen uygulamasının yok denecek kadar az olması da bu belirsizliklerin göstergesidir.

İkinci sorun ise kişisel verilerin hangi hallerde, hangi koşullar altında işlenebileceğinin yasal olarak belirlenmemiş olmasıdır. Anayasa'nın 20. maddesinin 2010 yılında eklenen 3. fıkrasının “Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir” hükmü karşısında her seferinde yasal bir düzenlemenin veya ilgilinin açık rızasının bulunması anayasal bir gerekliliktir. Örneğin 5464 sayılı Banka ve Kredi Kartları Kanunun 23. maddesinde ve 5490 sayılı Nüfus Hizmetleri Kanunun 9. maddesinde veya mahkumiyet kayıtlarının Adalet Bakanlığınca tutulmasını düzenleyen 5352 sayılı Adli Sicil Kanununda kişisel

verilerin nasıl işlenebileceği belirtilmiştir. Dolayısıyla en azından bu alanlarda yasallık ilkesine uyulmaktadır. Bunun dışında açık yasal düzenlemenin olmadığı hallerde, kişinin açık rızası da yoksa ciddi sorunların doğabileceği kesindir²²⁷.

Ceza Hukuku açısından hukuka uygunluk sebeplerinin mutlaka yasal olarak düzenlenmiş olması gerekliliği bulunmasa da, gerek kişisel verilerin korunması sistemindeki “belirlilik” kuralı, gerekse Anayasa'nın 20. maddesinin yeni 3. fıkrası ve başka bir yasal düzenleme olmaması nedeniyle, en azından bu alanda, ya Ceza Kanununda düzenleme yapılması ya da Kişisel Verilerin Korunması Kanun Tasarısının kanunlaşması gerekmektedir²²⁸.

TCK'da söz konusu suçlar incelenirken karşımıza çıkan diğer bir problem de 135. maddenin ikinci fıkrasındaki düzenlemedir. 135. maddenin birinci fıkrasında, kişisel verilerin hukuka aykırı olarak kayıt eden kimseye bir yıldan üç yıla kadar hapis cezası verileceği; ikinci fıkrasında ise, kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimseye de aynı hüküm uyarınca ceza verilmesi öngörülmüştür. Bu fıkra da kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine ilişkin bilgilerin kişisel veri olarak kayıt edilmesi mutlak olarak yasaklanmıştır. Zira bu sayılan veriler, uluslararası belgelerde ve Kişisel Verilerin Korunması Kanunu Tasarısında özel nitelikli veriler (hassas veri) olarak kabul edilmekte ve işlenmeleri normal verilere göre daha sıkı koşullara bağlanmaktadır .

Nitekim bu verilerin hukuka aykırı kaydedilmesi sonucunda oluşacak zarar ile basit bir telefon numarası veya adres bilgisinden oluşan kişisel verinin hukuka aykırı

²²⁷ Tasarı'nın 4. maddesi kişisel verilerin işlenebilmesi açısından yasallık ilkesini, hiçbir istisna bırakmaksızın net biçimde koymuştur. Bir sonraki maddede ise verilerin işlenmesinde hukuka uygunluk, belirlilik, amaca uygunluk, doğruluk ve süreye bağlılık gibi ilkeler konmaktadır. 6. maddede hangi sebeplerin hukuka uygunluk oluşturduğu başta ilgilinin rızası olmak üzere açık ve sınırlandırıcı biçimde sıralanmıştır. 7. maddede de özel niteliği olan ve "hassas veriler" olarak tanımlanan; (kişinin) "ırk, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançları, dernek, vakıf ve sendika üyeliği, sağlık ve özel yaşamları ve her türlü mahkûmiyetleri ile ilgili kişisel verilerin işlenmesi belirli yasal istisnaların dışında açıkça yasaklanmıştır. Tasarı'nın 8. maddesinde kişisel verilerin üçüncü kişilere nasıl ve hangi önlemlerle aktarılacağı, 9. maddede ne zaman yok edilmesi gerektiği, 14. maddede ise yurtdışına aktarım koşulları düzenlenmektedir. Örneğin Birlik mevzuatında asgari koşulları ve koruma standartlarını kabul eden Avrupa Birliği ülkelerinden üçüncü ülkelere veri aktarılması, çok dar istisnalar dışında yasaklanmıştır. Bkz. **Akyürek**, 2011: s. 57

²²⁸ **Akyürek**, 2011: s. 58

kaydedilmesi sonucu oluşan zarar farklı olacak; hassas verilerin işlenmesi nedeniyle kişi daha büyük zararlara maruz kalabilecektir. Kamuoyunda fişleme diye tabir edilen yasal olmayan bir şekilde kişileri hassas verilerinin kaydedilmesi ile kişinin ayrımcılığa tabi tutulması, dışlanması, onurunun, şeref ve haysiyetinin zedelenmesi gibi çok büyük manevi zararların yanında kişinin işten atılması, fiziki saldırılara maruz kalabilmesi gibi maddi zararlarda ortaya çıkabilmektedir.

Bu fıkra kamuoyunda, fişleme olarak bilinen ve yasadışı veri toplama ve arşivleme ve bu verileri kişilerin aleyhine kullanma eylemlerini yasaklayan bir fıkra olması itibariyle yerinde bir düzenleme olmakla birlikte, uygulanacak yaptırımın birinci fıkrayla aynı olması anlaşılammıştır. Bu suçun cezasının diğer verilerin hukuka aykırı kaydedilmesiyle aynı tutulması ceza adaleti açısından uygun gözükmemektedir. Zira AİHM’de bir kararında DNA verilerini diğer verilere göre daha önemli olduğunu ve daha sıkı koşullara tabi tutulması gerektiğini belirtmiştir. Bu nedenle bu fıkradaki suçun cezasının birinci fıkradaki suçun cezasından daha fazla olması gerektiğini düşünmekteyiz.

Ayrıca yine bu suçta suçun maddi unsurlarından hareket eylemlerinin daha fazla sayılması yerinde olabilir. Zira maddede sadece kaydetme eylemi düzenlenmiştir. Benzer bir suç olan TCK’nın 244. Maddesinin ikinci fıkrasında ise, verileri bozma, değiştirme, engelleme gibi bu suçta düzenlenmeyen fiillere de yer verilmiştir. Teknolojinin ilerlemesiyle paralel olarak verileri işleme metodlarında da farklılıklar ve yenilikler olabileceğinden bu eylemlerin de hükümde belirtilmesi faydalı olabilir.

Kişisel verileri yok etmeme suçunda, kişisel verilerin korunmasında temel ilkeler arasında bulunan süre sınırının karşılanmış olması olumlu bir gelişmedir. Bu ilkeye göre kişisel veriler, toplandıkları amaç için gerekli olandan daha uzun süre tutulmamalıdır. Kişisel verilerin süresiz olarak tutulmaması gerekliliği, amaçla bağlantılılık ilkesi açısından da oldukça önemlidir. Artık gereksinim duyulmayan verilerin silinmesi veya anonimleştirilerek kişisel niteliğinin ortadan kaldırılması keyfi uygulamaların önüne geçilmesi için gereklidir.

Ancak 138. madde hükmü açısından iki hususa işaret etmek gerekir. Birincisi, belirtilen hükümde suçun oluşabilmesi için “kanunların belirlediği sürelerin geçmiş olması” ölçütü esas alınmıştır. Bu bağlamda verinin toplanma

amacı ile bir bağlantı kurulmamıştır. Bir başka anlatımla verileri toplanma amacı ortadan kalkmış ya da gerçekleşmiş olsa bile bunlar yasada belirtilen süreler boyunca saklanabilecektir. Bu durum amaca bağlılık ilkesi ile uyumlu değildir. Zira kanunda belirtilen süreler genellikle kamu kurumları için öngörülmektedir. Ancak kişisel verileri sadece kamu kurumları işlememekte, özel hukuk tüzel kişileri ve gerçek kişilerde veri işlemektedirler. Bu kapsamda, GSM şirketlerinin abonelik sözleşmesi kapsamında abonelerine ilişkin verileri, otellerin müşterilerine ait tutmuş oldukları konaklamalarına ilişkin bilgiler, seyahat ve turizm firmalarının müşterilerine seyahatlarına ve gezilerine ait tuttıkları verilerinin ne zamana kadar silineceğine ilişkin bir kanunlarda herhangi bir süre bulunmamaktadır. Bu durumda bu verilerin silinmemesinin yaptırımı ne olacaktır? Bu nedenle burada verilerin toplanma amacıyla bağlantı kurularak bir düzenleme yapılmalıdır. Kişisel veriler kural olarak, toplanma amacı hâsıl olduğunda, aksine bir kanun hükmü yok ise silinmeli ve yok edilmelidir. Bu kuralın ihlali yaptırım altına alınmalıdır.

İkinci olarak şu noktaya dikkat çekmek gerekir: burada *"verileri sistem için de yok etmek"* ten söz edilmektedir. Bu ifade belirtilen suçun otomatik yollarla işlenen verilere ilişkin olduğu izlenimini yaratmaktadır. Nitekim son bölümde incelenen verilerin kaydedilmesi ve hukuka aykırı olarak verme, yayma ve ele geçirme suçlarında böyle bir ifade yer almamaktadır. Bu farklılık, verileri yok etmeme suçunun diğerlerinin tersine yalnızca otomatik yolla işlenen verilere ilişkin olduğu yönünde şüphe yaratmaktadır. Bu şüphenin giderilmesi için, doktrinde bazı yazarlarca da belirtildiği üzere, "sistemde bulunmaya" ilişkin ifadenin madde metninden çıkartılması gerektiğini düşülmekteyiz.

Görüldüğü gibi Türk Ceza Kanunu kapsamında kişisel verilerin hukuka aykırı olarak kaydedilmesi, ele geçirilmesi, verilmesi, yayılması veya yok edilmemesi konularında belirli oranda bir koruma getirilmiştir. Kişisel verilere hukuka aykırı müdahalelerde cezai yaptırımının etkin bir şekilde uygulanabilmesi için öncelikle bu işlem ve eylemlerde uyulacak esasların belirlenmesi gerekir. Ancak halen bu alanda uygulanacak ilkeleri belirleyen kişisel verilerin korunmasına ilişkin bir kanun mevzuatımızda bulunmadığı için bu işlem ve eylemlere ilişkin uyulacak esaslar belirsizliğini korumaktadır.

Bu nedenlerle, 5237 sayılı Türk Ceza Kanunu'nun 135. Maddesinde düzenlenen kişisel verilerin kaydedilmesi, 136. Maddesinde düzenlenen kişisel verilerin hukuka aykırı olarak verilmesi, yayılması ve ele geçirilmesi ve 138. Maddesinde düzenlenen kişisel verilerin yok edilmemesi suçlarının hangi koşullarda hukuka uygun hale geleceğinin belli olması için, aynı zamanda Anayasa'nın 20. maddesinin üçüncü fıkrasındaki amir hüküm gereği, Kişisel Verilerin Korunması Kanunu Tasarısının yasalaşıp uygulanabilir hale gelmesi gerektiğini düşünmekteyiz.

KAYNAKÇA

Kitaplar

- **Avrupa Birliği Üyesi Bazı Ülkelerin Anayasaları** (Mayıs 2011). Ankara: Adalet Bakanlığı Yayın İşleri Dairesi Başkanlığı Yayınları.
- **Akılhoğlu, Tekin** (1995). İnsan Hakları I, Kavram, Kaynaklar ve Koruma Sistemleri, No. 17. Ankara: AÜSBF İnsan Hakları Merkezi Yayınları.
- **Akgül, Aydın** (2014). Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları ışığında Kişisel Verilerin Korunması. İstanbul: Beta.
- **Aksoy, Hüseyin Can** (2010). Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması. Ankara: Çakmak Yayınevi.
- **Akyürek, Güçlü**, (2014). Özel Hayatın Gizliliğini İhlal Suçu, 2. Baskı. Ankara: Seçkin Yayınevi,
- **Alacakaptan, Uğur** (1975). Suçun Unsurları. Ankara: AÜHF Yayınları.
- **Artuk, M. Emin, Ahmet Gökçen, Ahmet Caner Yenidünya** (2009). Türk Ceza Kanunu Şerhi Özel Hükümler C. 4, Ankara: Turhan Kitabevi.
- **Artuk, M. Emin, Ahmet Gökçen, Ahmet Caner Yenidünya** (2013). Türk Ceza Hukuku Genel Hükümler 7. Baskı. Ankara: Adalet Yayınevi.
- **Artuk, M. Emin, Ahmet Gökçen, Ahmet Caner Yenidünya** (2013). Türk Ceza Hukuku Özel Hükümler, 13. Baskı, Ankara: Adalet Yayınevi.
- International Encyclopedia of Laws, haz. **R. Blanpain** (1999). Constitutional Law, C. 3, haz. **A.Alen**, Fransa Bölümü (Bu bölüm **Michael Front** tarafından hazırlanmıştır) Kluwer Law International, Hollanda.
- **Bakıcı, Sedat** (2008). 5237 sayılı Yasa Kapsamında Ceza Hukuku Genel Hükümleri 2. Baskı. Ankara: Adalet Yayınevi.
- **Başalp, Nilgün** (2004). Kişisel Verilerin Korunması ve Saklanması. Ankara: Yetkin Yayınevi.
- **Berber, Leyla Keser, Mahir M. Ülgü, Cüneyd Er** (2009). Elektronik Sağlık Kayıtları ve Özel Hayatın Gizliliği. İstanbul: İst. Bilgi Üniv. Bilişim Teknolojisi Hukuku Araştırma Merkezi Yayınları.
- **Brin, David** (1998).The Transparent Society (Will Technology Force Us to Choose Between Privacy and Freedom), ABD: Addison-Wesley.

- **Carey, Peter** (2009). Data Protection: A Practical Guide to UK and EU Law Third Edition. Oxford: Oxford University Pres.
- **Centel, Nur/ Hamide Zafer** (2013). Ceza Muhakemesi Hukuku, 10. Bası. İstanbul: Beta.
- **Civelek, Dilek Yüksel** (Nisan 2011). Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi (Uzmanlık Tezi). Bilgi Toplumu Dairesi Başkanlığı Yayınları.
- **Çolak, N. İlker** (2013). Kitle İletişim Hukuku, İstanbul: Oniki Levha Yayıncılık.
- **Çubukçu, Faruk** (1987). Bilgisayar Terimleri Sözlüğü, Ankara: V Yayınları.
- **Doğru, Osman, Atilla Nalbant** (2013). İnsan Hakları Avrupa Sözleşmesi Açıklama ve Önemli Kararlar, 2. Cilt, (Avrupa Konseyi “Yüksek Yargı Kurumlarının Avrupa Standartları Bakımından Rollerinin Güçlendirilmesi Projesi” kapsamında basılmıştır). Ankara.
- **Dutertre, Gilles**, (2007). Avrupa İnsan Hakları Mahkemesi Kararlarından Örnekler. Ankara: Avrupa Komisyonu Yayınları.
- **Dülger, Murat Volkan** (2004). Bilişim Suçları. Ankara: Seçkin Yayınevi.
- **Erol, Haydar** (2008). Türk Ceza Kanunu C.1. Ankara.
- **Ferrier, Patricia** (2006). There Ought to Be a Law. Michigan.
- **Gökcan, Hasan Tahsin, Mustafa Artuç**, (2007). Kamu Görevlisi Kavramı ve Özel Soruşturma Usülleri. Ankara: Seçkin Yayınevi.
- **Gözler, Kemal** (2000). Türk Anayasa Hukuku. Bursa: Ekin Kitabevi Yayınları.
- **Gözler, Kemal** (2010). Anayasa Hukukuna Giriş. 15. Baskı, Bursa: Ekin
- **Gözübüyük, Ahmet Şeref, Feyyaz Gölcüklü** (2004). Avrupa İnsan Hakları Sözleşmesi ve Uygulaması, 5. Bası. Ankara: Turhan Kitabevi.
- **Gözübüyük, Şeref, Turgut Tan** (2006). İdare Hukuku (İdari Yargılama Hukuku), C. 2. Ankara: Turhan Kitabevi.
- **Günday, Metin** (2003). İdare Hukuku, 8. Baskı. Ankara: İmaj Yayıncılık.
- **Gür, İkbâl** (2010). Kişisel Verilerin Korunması Hususunda AB İle ABD Arasında Çıkan Uyuşmazlıklar ve Çözüm Yolları. Ankara: Turhan Kitabevi.

- **Hafizoğulları, Zeki, Muharrem Özen** (2010). Türk Ceza Hukuku, Özel Hükümler, Kişilere Karşı Suçlar, Ankara: US-A Yayıncılık.
- **Hafizoğulları, Zeki, Muharrem Özen** (2011). Türk Ceza Hukuku, Özel Hükümler, Kişilere Karşı Suçlar, Ankara: US-A Yayıncılık.
- **Hakeri, Hakan** (2013). Ceza Hukuku Genel Hükümler, 16. Baskı. Ankara: Adalet Yayınevi.
- **Handbook on European Data Protection Law** (2014). Belgium: Council of Europe.
- **Henderson, Harry** (2006). Privacy in the Information Age, ABD: Facts of File.
- **Karagülmez, Ali** (2005). Bilişim Suçları ve Soruşturma Kovuşturma Evreleri. Ankara: Seçkin Yayınevi.
- **Kaya, Cemil** (2005). İdare Hukukunda Bilgi Edinme Hakkı, Ankara: Seçkin.
- **Keklik, Ramazan** (2012). Özel Hayatın Gizliliğini İhlal Suçları. Ankara: Adalet Yayınevi.
- **Ketizmen, Muammer** (2008). Türk Ceza Hukukunda Bilişim Suçları, Ankara: Adalet Yayınevi.
- **Kilkelly, Ursula** (2003). Özel Hayata ve Aile Hayatına Saygı Gösterilmesi Hakkı, 2. Baskı, Ankara: Avrupa Konseyi Yayınları.
- **Koca, Mahmut, İlhan Üzülmaz** (2013). Türk Ceza Hukuku Genel Hükümler, 6. Baskı. Ankara: Seçkin Yayınevi.
- **Kunter, Nurullah, Feridun Yenisey, Ayşe Nuhoglu** (2006). Muhakeme Hukuku Dalı olarak Ceza Muhakemesi Hukuku, 14. Baskı, İstanbul: Arkan
- **Kurt, Levent** (2005). Açıklamalı-İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması. Ankara: Seçkin Yayınevi.
- **Küzeci, Elif** (2010). Kişisel Verilerin Korunması, Ankara: Turhan Kitabevi.
- **Lloyd, Ian J**, (2008). Information Tecnology Law, Fifth Edition. Oxford: Oxford University Pres
- **Meran, Necati**, (2007). Açıklamalı İçtihatlı Türk Ceza Kanunu, 2. Bası, Ankara: Seçkin Yayınevi.
- **Oğuzman, Kemal, Nami Barlas** (2008). Medeni Hukuk (Giriş, Kaynaklar, Temel Kavramlar), 15. Baskı. İstanbul: Vedat Kitapçılık.

- **Orwell, George** (2011). Bin Dokuz Yüz Seksen Dört, 34. Baskı (Çeviri: Celal Üster). Can Yayınları.
- **Özay, İlhan** (2002). Gün Işığında Yönetim. İstanbul: Alfa Yayınevi.
- **Özbek, Veli Özer** (2008). Yeni Türk Ceza Kanunun Anlamı (Açıklamalı, Gerekçeli, İçtihatlı), C. 2 (Özel Hükümler), Ankara: Seçkin Yayınevi.
- **Özbek, Veli Özer, Mehmet Nihat Kanbur, Koray Doğan, Pınar Bacaksız, İlker Tepe** (2011). Türk Ceza Kanunu Özel Hükümler, Ankara: Seçkin Yayınevi.
- **Özbek, Veli Özer, Mehmet Nihat Kanbur, Koray Doğan, Pınar Bacaksız, İlker Tepe** (2013). Türk Ceza Kanunu Özel Hükümler, Ankara: Seçkin Yayınevi.
- **Özdek, Yasemin** (2004). Avrupa İnsan Hakları Sözleşmesi ve Türkiye. Ankara.
- **Özdemir, Hayrunnisa** (2009). Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması. Ankara: Seçkin Yayınevi.
- **Özgenç, İzzet** (2005). Türk Ceza Kanunu Gazi Şerhi (Genel Hükümler), 2. Baskı. Ankara: Seçkin Yayınevi.
- **Özgenç, İzzet** (2012). Türk Ceza Hukuku Mevzuatı, C. 1, 8. Baskı. Ankara.
- **Özgenç, İzzet** (2012). Türk Ceza Hukuku Genel Hükümler, 7. Baskı. Ankara: Seçkin Yayınevi.
- **Öztan, Bilge** (2002). Medeni Hukukun Temel Kavramları, 8. Baskı. Ankara: Turhan Kitabevi.
- **Öztürk, Bahri, Mustafa Ruhan Erdem** (2012). Uygulamalı Ceza Hukuku ve Güvenlik Tedbirleri Hukuku, 12. Bası. Ankara: Seçkin Yayınevi.
- **Öztürk, Bahri, Mustafa Ruhan Erdem** (2006). Uygulamalı Ceza Muhakemesi Hukuku, 9. Baskı. Ankara: Seçkin Yayınevi.
- **Parlar, Ali, Muzaffer Hatipoğlu** (2007). 5237 sayılı Türk Ceza Kanunu Yorumu, II. Cilt. Ankara.
- **Parlar, Ali, Muzaffer Hatipoğlu** (2008). Türk Ceza Kanunu Yorumu, 2. Baskı, C. 2. Ankara: Seçkin Yayınevi.

- **Parlar, Ali, Meltem Banko** (2014). Cezai ve Hukuki Sorumluluk Boyutlarıyla Hakaret ve Özel Hayata Karşı Suçlar. Ankara: Adalet Yayınevi.
- **Polater, Yusuf Ziya** (2010). Özel Hayatın Gizliliği ve Korunması, Ankara: Adalet Yayınevi.
- **Prins, Corien** (2006). When Personal Data, Behavior And Virtual Identities Become A Commodity: Would A Property Rights Approach Matter, (personal data), Scripted, c. 3.
- **Sevimli, K. Ahmet** (2006). İşçinin Özel Yaşamına Müdahalenin Sınırları. İstanbul: Legal.
- **Sezer, Yasin, Ali İhsan İpek, Engin Parlak** (2012). Adli ve İstihbari Amaçlı İletişimin Denetlenmesi Gizli Soruşturmacı ve Teknik Araçlarla İzleme. Ankara: Seçkin Yayınevi.
- **Şen, Ersan** (1996). Devlet ve Kitle İletişim Araçları Karşısında Özel Hayatın Gizliliği ve Korunması. İstanbul: Kazancı Yay.
- **Şen, Ersan** (2006). Türk Ceza Kanunu Yorumu, C. I. İstanbul: Vedat Kitapçılık.
- **Şen, Ersan** (2011). Yorumluyorum Ceza Hukuku Perspektifinden Güncel Olaylara Bakış. Ankara: Seçkin Yayınevi.
- **Şimşek, Oğuz** (2008). Anayasa Hukukunda Kişisel Verilerin Korunması. Beta Yayınevi.
- **Tanör, Bülent** (1994). Türkiye'nin İnsan Hakları Sorunu, 3. Baskı. İstanbul: BDS Yayınları.
- **Taşkın, Mustafa** (2011). Adli ve İstihbari Amaçlı İletişimin Denetlenmesi, Ankara: Seçkin Yayınevi.
- **Tekşen, Mustafa Gökhan** (2012). Ticari Sır, Bankacılık Sırrı veya Müşteri Sırrı Niteliğindeki Bilgi ve Belgelerin Açıklanması Suçu (TCK m. 239). Ankara: Yetkin Yayınevi.
- **Tezcan, Durmuş, Mustafa Ruhan Erdem, Oğuz Sancakdar** (2004). Avrupa İnsan Hakları Sözleşmesi Işığında Türkiye'de İnsan Hakları Sorunu, 2. Baskı. Ankara: Seçkin Yayınevi.
- **Teziç, Erdoğan** (1998). Anayasa Hukuku. İstanbul: Beta Yayınevi.

- **Türkçe Sözlük** (2009). Onuncu Baskıdan Yapılan Tıpkı Basım. Ankara: Türk Dil Kurumu Yayınları.
- **Uygun, Murat** (2010). Avrupa Birliğinin 95/46 sayılı Yönergesi Işığında Kişisel Verilerin Korunması, Yayınlanmamış Yüksek Lisans Tezi. Ankara.
- **Üzeltürk, Sultan**, (2004). 1982 Anayasası ve İnsan Hakları Avrupa Sözleşmesine Göre Özel Hayatın Gizliliği Hakkı. İstanbul: Beta Yayınevi.
- **Zafer, Hamide** (2010). Özel Hayatın ve Hayatın Gizli Alanının Ceza Hukuku Yoluyla Korunması, İstanbul: Beta.

Makaleler

- **Akılhoğlu, Tekin**, “İdari Usul ve Kişisel Verilerin Korunması”, 11.08.2004, www.idare.gen.tr/akkillioglu-idariusul.htm
- **Aksoy, Hüseyin Can** (2008). “The Right to Personality and Its Different Manifestations As the Core of Personal Data”, Ankara Law Review, Vol. 5, No. 2.
- **Akyürek, Güçlü** (Temmuz- Ağustos- Eylül 2011). “Kişisel Veriler ve Özel Hayatın Gizliliği Hakkı” Suç ve Ceza- Ceza Hukuku Dergisi, S. 3.
- **Albayrak, Mustafa** (Nisan-Haziran 2013). “Kişisel Verilerin Kaydedilmesi Suçu”, HUKAB Dergisi, S. 5.
- **Arslan, Çetin** (Mart-Nisan 2011). “Avrupa Birliği Hukukunda Kişisel Verilerin Üçüncü Ülkelere Aktarılması” Kazancı Hakemli hukuk Dergisi, S. 79-80.
- **Aslan, Metin** (Ekim-Kasım-Aralık 2010). “Parmak İzime Dokunma”, Suç ve Ceza- Ceza Hukuku Dergisi, S. 4.
- **Atak, Songül** (2010). “Avrupa Konseyinin Kişisel Veriler İçin Sağladığı Temel Güvenceler” TBB Dergisi, S. 87.
- **Avrupa Birliği Temel Haklar Şartı**, Avrupa Birliği ile İlişkiler Genel Müdürlüğü, Kasım 2001, www.dpt.gov.tr/DocObjects/Download/2962/temelhak.pdf

- **Çolak, N. İlker** (Mayıs 2005). “Bilgi Edinme Hakkının Sınırları ve Sınırlama Ölçütleri”, e-akademi Hukuk, Ekonomi ve Siyasal Bilimler Aylık İnternet Dergisi, S. 39, , <http://www.e-akademi.org/makaleler/nicolak-2.htm>
- **Çolak, N. İlker**, “Bilgi Edinme Hakkı, Önemi ve Bilgi Verme Yükümlülüğü”, <http://www.ilkercolak.com.tr/bilgi-edinme-hakki-onemi-ve-bilgi-verme-yukumlulugu/>
- **Döner, Ayhan** (2006). “Kişisel Verilerin Korunması Hakkında Federal Kanun” (19 Haziran 1992), AÜEHFD, C. X, S. 1-2.
- **Dursun, Hasan** (2009). “Ticari Sır, Bankacılık Sırrı veya Müşteri Sırrı Niteliğindeki Bilgi ve Belgelerin Açıklanması Suçlarına Genel Bir Bakış” Kamu-İş C. 11, S. 1.
- **Dülger, Murat Volkan**, (Ocak 2005). “Yeni Türk Ceza Kanununda Suç Ortaklığı”, Yeditepe Üniversitesi HFD, C. I, S. 2.
- **Değirmenci, Olgun**, (2005). “2004 Türk Ceza Kanunun Bilişim Suçları Açısından Değerlendirilmesi”, TBB Dergisi, S. 58.
- **Ersoy, Eren**, “Gizlilik, Bireysel Haklar, Kişisel Verilerin Korunması”, <http://ab.org.tr/ab06/bildiri/6.doc>. Erişim T: 04.04.2012
- **Evcı, Özge**, “Facebook ve Kişisel Bilgi Güvenliği”, <http://hukukcu.com/modules/smartsection/item.php?itemid=205> et:21.02.2012
- **Güleç, Recep Aydın, Hatice Sarıtaş, Sevil Neşeli Demirbaş** (Haziran, 2008). “Kişisel Sağlık Verilerinin Mahremiyeti”, E-Yaklaşım Dergisi, S. 59.
- **Gülener, Serdar**, (2012). “Digital Hafızadan Silinmeyi İstemek; Temel Bir İnsan Hakkı Olarak Unutulma Hakkı”, TBBD, (102).
- **Hakeri, Hakan**, “Hasta Hakları Bakımından Yeni Türk Ceza Kanunu”, http://portal.hakanhakeri.com/index.php?option=com_content&task=view&id=27&Itemid=35
- **İktisadi İşbirliği ve Kalkınma Teşkilatı ve Türkiye**, <http://www.oecd.org/dataoecd/39/40/42122130.pdf>. (s.y, 23 Nisan 2009).

- <http://www.scribd.com/doc/19952426/1-Bilisim-Surasi-Hukuk-Raporu?query=ki%C5%9Fisel+verilerin+korunmas%C4%B1>, s. 31, Erişim Tarihi:20.03.2012
- **İçel, Kayıhan** (Güz 2007/2). “Ceza Hukukunda Temel Kusurluluk Şekli Kast”, İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi, Y. 6, S. 12.
- **İlkiz, Fikret**, (Temmuz 2009/7-67). “Kişisel Verilerin Korunması ve Kanun Tasarısı”, Güncel Hukuk Dergisi.
- **Işık, Dilan**, (Ekim Kasım Aralık 2010). “Kişisel Verilerin Kaydedilmesi Suçu”, Suç ve Ceza- Ceza Hukuku Dergisi, S. 4.
- **Jori, Andreas**, “dataprotection.eu”, <http://www.dataprotection.eu/>.
- **Kaya, Cemil** (2011). “Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi”, İÜHFM, C. LXIX, S. 1.
- **Keskin, Adnan**, “Fişlemeye Altı Ay Devam” <http://www.taraf.com.tr/haber-fislemeye-alti-ay-devam-152505/>
- **Ketizmen, Muammer**, “Kişisel Verilerin Korunması” Tebliğ, http://www.tbd.org.trusr_imgcdkamubib14raporlarPDFRP2-2008.pdf
- **Kaymaz, Seydi**, (Eylül-Ekim 2011). “Kişisel Veri Denetim Otoriteleri”, Kazancı Hakemli Hukuk Dergisi, S. 85-86.
- **Kaymaz, Seydi** (2012). “5237 Sayılı Türk Ceza Kanuna Göre İştirak Halinde İşlenen Suçlarda Nitelikli Hallerin Diğer Suç Ortaklarına Geçiş Sorunu”, GÜHFD, C. XVI, S. 2.
- **Kazancı, Behiye Eker** (2007). “Kişilerin İzinsiz Görüntülerinin Alınmasının TCK m. 134 Çerçevesinde Değerlendirilmesi”, DEÜHFD, C. 9, S. 1.
- “Kişisel Verilerin Korunması” 1. Bilişim Şurası Hukuk Raporu, 10-12 Mayıs 2002, Ankara, <http://www.scribd.com/doc/19952426/1-Bilisim-Surasi-Hukuk-Raporu?query=ki%C5%9Fisel+verilerin+korunmas%C4%B1>
- **Kurt, Emre**, <http://www.emrekurt.av.tr/2011/10/kisisel-verilerin-korunmasi/>, Erişim Tarihi: 12/12/2012
- **Mahmutoğlu, Fatih Selami**, “Sır Saklama yükümlülüğü Kapsamında Hastaya Ait Kişisel Verileri Hukuka Aykırı Olarak Verme veya Yayma

Suçu”, cezahukuku.istanbul.edu.tr/ders-gerecleri/tiphukuku/sir-saklama.docx, E.T: 21.02.2012

- **Memiş, Tekin** (2009). “Erişimin Engellenmesi, Hukuki Sorunlar ve Çözüm Önerileri”, EÜHFD, C. XIII, S. 3-4.
- **Metin, Yüksel** (2002). “Avrupa Birliği Temel Haklar Şartı” AÜSBFD, S. 57-4.
- **Özgenç, İzzet** (25 Mayıs 2010). “Devlet Sırrı ve Ceza Hukuku”, Dünyada ve Türkiye’de Ceza Hukuku Reformları Kongresinde Sunulan Tebliğ, İstanbul Üniv.
- **Özen, Mustafa**, (Mart 2009). “Kişisel Verilerin Kaydedilmesi, Verilmesi veya Ele Geçirilmesi ve Yok Edilmemesi Suçları, Kamu Hukuku Arşivi, KHukA, S. 1, Y. 12, Ankara.
- **Özbey, Özcan**, (2013). “Avrupa İnsan Hakları Sözleşmesi Işığında İfade Özgürlüğü Kısıtlamaları”, TBB Dergisi, S. 106.
- **Özdemir, Kenan** (Eylül 2005). “Türk Hukukunda ve Avrupa İnsan Hakları Sözleşmesi İle Avrupa İnsan Hakları Mahkemesi Kararlarında Özel Hayatın Gizliliği”, Adalet Dergisi, S. 23.
- **Özdemir, Hayrunnisa** (2010). “ İşyerinde İşçilerin İzlenmesi Ve İşçinin Kişilik Haklarının Korunması”, EÜHFD, C. XIV, S. 1-2.
- **Özdemir, Hayrunnisa**, “Türkiye’de Kişisel Verilerin Korunması”, <http://inet-tr.org.tr/inetconf14/bildiri/81.doc> Erişim T: 21.02.2012
- **Özer, Yusuf Mansur**, “Avrupa Adalet Divanının Unutulma Hakkı Kararı ve Bu Hakkın Kapsamı” <http://www.statjus.com/2014/06/avrupa-adalet-divaninin-unutulma-hakki-karari-ve-bu-hakkin-kapsami/> Erişim T: 23.10.2014
- **Polat, Halil**, (Nisan 2010). “Genel Güvenliğin Tehlikeye Sokma Suçu ile Bu Suçun Diğer Suçlarla İctimai”, TAAD, S. 1.
- **Salihpaşaoğlu, Yaşar** (2013). “Özel Hayatın Kapsamı: Avrupa İnsan Hakları Mahkemesi İctihatları Işığında Bir Değerlendirme”, GÜHFD, C. 17, S. 3.
- **Sevük, Handan Yokuş** (2007-2008). “Haberleşmenin Gizliliğini İhlal Suçu”, Dicle Üniversitesi Hukuk Fakültesi Dergisi, S. 16-19.

- **Şanver, Dinç**, “İnternet Ortamında Kişisel Bilgilerin Depolanması ve Kullanılması”, 27 Mart 2012,
[http://www.logyonetimi.com/web/Makaleler/12-03-27/%C4%B0nternet Ortam%C4%B1nda Ki%C5%9Fisel Bilgilerin Depolanmas%C4%B1](http://www.logyonetimi.com/web/Makaleler/12-03-27/%C4%B0nternet%20Ortam%C4%B1nda%20Ki%C5%9Fisel%20Bilgilerin%20Depolanmas%C4%B1). Erişim T: 09.04.2012
- **Şener, Emine Gülnihal** (Nisan 2011). “Kişisel Verilerin Hukuka Aykırı Olarak Kaydedilmesi Suçu”, Adalet Dergisi, S. 39.
- **Şen, Ersan** (2005). “5237 sayılı Türk Ceza Kanunu'nda Özel Hayata Karşı Suçlar”, İBD, C. 79, S. 3.
- **Şen, Ersan**, “MİT’e Verilmesi Düşünülen Yeni Yetki”,
[http://www.adalet.org/forum2/goster.php?konu=Mit e verilmesi düşünülen yeni yetki&fid=459143&alan=Mesleki Konular](http://www.adalet.org/forum2/goster.php?konu=Mit+e+verilmesi+d%C3%99%C5%9F%C3%BCn%C3%BClen+yeni+yetki&fid=459143&alan=Mesleki+Konular) Erişim Tarihi:17.06.2014
- **Tanrıkulu, Cengiz**, (2007). “Kişisel Verilerin Önemi Artıyor”, ATGV Dergisi, S. 3.
- **Tansuğ, Avniye** (Nisan 2005). “AB’ nin Yeni Ekonomik Silahı Veri Koruma Hukuku”, Güncel Hukuk Dergisi, S. 16.
- **Tezcan, Durmuş** (2013). “Özel Hayatın Gizliliğini İhlal ve Kişisel Verilerin Kaydedilmesi Suçu ile İlgili Bazı Gözlemler”, İHFM, C. 71, S. 1, (Prof. Dr. Füsun Sokullu- Akıncı’ya Armağan).
- **Tortop, Nuri** (Mart 2004). “İletişim ve Bilgi Edinme Hakkının Önemi”, AİD, C.37, S.1.
- **Yokuş, Handan Sevük**, Türk Alman Tıp Hukuku Sempozyumu, “Tıp Ceza Hukukunun Güncel Sorunları- Tıp Ceza Hukukunda Kişisel Verilerin Açıklanması”, Tebliğ, Ankara, 28 Şubat-1 Mart 2008
- **Yokuş, Sevtap** (2003). “Avrupa Birliğine Uyumda Siyasi Kriterler Doğrultusunda Türkiye’de Anayasal ve Yasal Dönüşüm Çabaları”, İÜHFM, C. LXI, S. 1-2, 185-254.

Yararlanılan İnternet Siteleri

- <http://www.ab.gov.tr/index.php?p=45632&l=1>
- http://curia.europa.eu/jcms/jcms/j_6/
- <http://ekutup.dpt.gov.tr/ah/hukuk/temelhak.pdf>
- http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0131&from=EN#Footnote*
- http://www.europarl.europa.eu/charter/default_en.htm
- <http://www.kgm.adalet.gov.tr/Tasariasamalari/Tbmmkms/Tbmmkom/ticarisir.pdf>
- <http://www.kgm.adalet.gov.tr/Tasariasamalari/Basbakanlik/Basbakanlik.html>
- <http://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=7.5.16405&MevzuatIliski=0&sourceXmlSearch>
- http://www.tbmm.gov.tr/develop/owa/tasari_teklif_sd.onerge_bilgileri?kanunlar_sira_no=148569
- http://www.tbmm.gov.tr/develop/owa/tasari_teklif_sd.onerge_bilgileri?kanunlar_sira_no=148569
- <http://tdkterim.gov.tr/bts/?kategori=verilst&kelime=politika&ayn=tam>
- www.portal.uyap.gov.tr/kararlar/yargitaykararlari
- <http://www.resmigazete.gov.tr/main.aspx?home=http://www.resmigazete.gov.tr/eskiler/2014/07/20140726>
- <http://www.scribd.com/doc/19952426/1-Bilisim-Surasi-Hukuk-Raporu?query=ki%C5%9Fisel+verilerin+korunmas%C4%B1>

ÖZGEÇMİŞ

1983 yılında Çankırı’da doğan yazar, ilk ve orta öğrenimini Çankırı’da tamamlamış, 2000 yılında Kocaeli Üniversitesi Hukuk Fakültesi’nde lisans eğitimine başlayıp, 2004 yılında mezun olmuştur. Lisans eğitimini tamamladıktan sonra, Kocaeli Üniversitesi Sosyal Bilimler Enstitüsü’nde 2004 yılı güz dönemi başladığı kamu hukuku yüksek lisans programını 2007 yılı bahar döneminde tamamlamış olup “Ceza Muhakemesi Hukukunda Koruma Tedbiri Olarak Arama ve Elkoyma” adlı tezi yazmıştır. 2004 yılı Ekim ayında Öğrenci Seçme ve Yerleştirme Merkezi tarafından yapılan adlî yargı hâkimlik ve savcılık sınavını kazanıp, 2005-2006 yılları arasında hâkim adaylığı dönemini bitirdikten sonra sırasıyla; Tokat/Almus, Şanlıurfa/Viranşehir Cumhuriyet Savcılıkları ile Adalet Bakanlığı Kanunlar Genel Müdürlüğü Tetkik Hâkimliği görevlerini yapmıştır. Halen Ankara/Çubuk Cumhuriyet Savcısı olarak görev yapmaktadır. Yazar evli olup, bir çocuğu bulunmaktadır.