

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

YÜKSEK LİSANS TEZİ

**KOLLUK VE ADLİ MAKAMLAR TARAFINDAN
İŞLENEN KİŞİSEL VERİLERİN KORUNMASI**

Neslihan CAN

2501171545

Tez Danışmanı

Prof. Dr. Adem SÖZÜER

İstanbul, 2020

ÖZ

KOLLUK VE ADLİ MAKAMLAR TARAFINDAN İŞLENEN KİŞİSEL VERİLERİN KORUNMASI

NESLİHAN CAN

Kişisel veriler; yalnız sağlık, finans, sigortacılık gibi sektörlerde hizmet sunmak amacıyla işlenmeyip suç işlenmesinin önlenmesi ve suçların aydınlatılması amacıyla da işlenmektedir. O kadar ki sokağa çıkan birey için kamera sistemleri ile izlenmek, kontrol noktasından geçmek, genel bilgi toplamaya tabi tutulmak günümüzde yaşamanın âdeta bir gereği olmuştur.

Kişisel verilerin korunmasını, özel yaşama tanınan korumayla sağlamak günümüz ihtiyaçlarına cevap vermemektedir. Bu nedenle gerek Avrupa Konseyi ve Avrupa Birliği gerekse de Türk hukuku; kişisel verilerin hukuka uygun işleme şartları, veri sahibinin hakları, veri ihlali halinde öngörülen yaptırımları düzenleyerek bu kişisel verilerin korunması ihtiyacına cevap vermeye çalışmıştır.

Avrupa ve Türkiye’de kişisel verilerin korunması mevzuatı; ulusal güvenlik, suç işlenmesinin önlenmesi, ceza muhakemesinin yürütülmesi ve cezaların infazı söz konusu olduğunda devre dışı kalmaktadır. Ancak 2018 yılında yürürlüğe giren Kolluk ve Ceza Adaleti Direktifi; suçların önlenmesi, soruşturulması, ortaya çıkarılması, kovuşturulması ve cezaların infazında kolluk makamları ve diğer adli makamların hangi hallerde kişisel verileri işleyebileceğini, bu verilerin neler olabileceğini ve veri sahibinin hakları gibi pek çok hususu düzenlemiştir.

Tezimizde Avrupa Konseyi ve Avrupa Birliği’nde kişisel veri korumasının tarihsel gelişimi incelenmiş ve Direktif’e genel bir bakış sağlanmaya çalışılmıştır. Direktif’te yer alan süjeler ve bu süjelerin yetki, hak ve yükümlülükleri incelenmiştir. Nihayet suçların önlenmesi, ceza muhakemesi ve cezaların infazı sürecinde kişisel veri elde etme yöntemleri incelenmiştir.

Anahtar Kelimeler: Kolluk Makamları, Kişisel Veri, İstihbarat, Kolluk ve Ceza Adaleti Direktifi, CCTV.

ABSTRACT

**THE PROTECTION OF THE PERSONAL DATA PROCESSED
BY LAW ENFORCEMENT AND JUDICIAL AUTHORITIES**

NESLIHAN CAN

Personal data is not limited to being processed only in sectors such as health, finance or insurance to provide services, but also for the prevention of crime and illumination of the crimes committed. For the individual living today on the street, being watched with camera systems, passing through the checkpoint, being subject to law enforcement database have become indispensable.

Providing the protection of personal data with the protection granted to the right to privacy does not respond to today's needs. For this reason both the Council of Europe and the European Union and Turkish law tried to respond to the need to protect personal data by regulating lawfully processing of personal data, the rights of the data subject and the sanctions in case of data breach.

The legislation on the protection of personal data in Europe and Turkey has been excluded when it comes to national security, prevention of crimes, execution of criminal proceedings and criminal penalties. However, the Law Enforcement and Criminal Justice Directive that came into force in 2018 regulated many issues in prevention, investigation, detection, prosecution of crimes and execution of penalties such as the situations in which law enforcement and other judicial authorities can process personal data, what these data might be and the rights of the data subject.

In our thesis, the historical development of personal data protection in the Council of Europe and the European Union has been examined and we try to present general perspective of the Directive. The subjects of the Directive and their competence, rights and obligations are examined. Finally the methods of personal data processing through preventive and protection measures applied in the process of preventing crimes, criminal procedure and execution of sentences are discoursed.

Keywords: Law Enforcement Authorities, Personal Data, Intelligence, Law Enforcement and Criminal Justice Directive, CCTV.

ÖNSÖZ

Günümüzde sağlıktan eğitime yaşamın herhangi bir alanında faaliyet gösterebilmek için bireylerin kişisel verilerinin işlenmesi kaçınılmazdır. Bu denli yoğun kişisel veri işlenmesi karşısında da yeni bir hukuki değer olarak kişisel verilerin korunması ihtiyacı doğmuştur. Avrupa Veri Koruma Reformu ve Türkiye’de KVKK’nin yürürlüğe girmesi ile birlikte kişisel verilerin korunması hukuku alanı oldukça rağbet gören bir alan olmuştur. Ancak gerek AB düzeyinde gerek Türkiye’de söz konusu veri işleme faaliyeti, adli makamların suç önleyici ve bastırıcı amaçlarına ilişkin olduğunda, bu makamların işlediği kişisel veriler mevzuatın korunaklı alanının dışında kalmaktadır. Avrupa Birliği Kolluk ve Ceza Adaleti Direktifi de adli makamların işlediği kişisel veriler için korunaklı bir alan yaratmaya çalışmıştır.

Tezin konusu olan suçların önlenmesi, soruşturulması, ortaya çıkarılması, kovuşturulması ve cezaların infazında gündeme gelen kişisel verilerin işlenmesi Türk hukukunda bağımsız bir hukuki düzenlemeye konu olmamıştır. Yalnız PVSK, TCK, CMK, CGİK, MİT Kanunu gibi farklı kanunlarda kişisel verilerin korunmasına hizmet edebilecek sınırlı düzenlemeler bulunmaktadır. Türkiye her ne kadar AB üyesi ülke olmasa da AB üye ülke adaylığı devam etmekte ve Avrupa’daki eğilime uygun olarak suçların önlenmesi, ceza muhakemesi ve cezaların infazı aşamasında işlenen kişisel verilerin korunması önem arz etmektedir. Bu nedenle tez konusu olarak GDPR’ın gölgesinde kalmış, tabiri caizse “unutulmuş” Kolluk ve Ceza Adaleti Direktifi bağlamında kişisel verilerin korunmasına ilişkin bir çalışma yapmak istedim.

Kolluk ve Ceza Adaleti Direktifi’nin resmî bir Türkçe çevirisi olmadığı için çoğu maddeyi bizzat çevirip tezimde bunlara yer verdim. Ayrıca kolluk ve adli makamların faaliyetlerinde işlenen kişisel verilerin korunmasına dair karşılaştırmalı hukuk ve Türk hukukunda oldukça sınırlı kaynak bulunduğu için esas kaynak olarak Kolluk ve Ceza Adaleti Direktifi’nin resital denilen gerekçesinden yararlandım.

Tez danışmanlığımı üstlenen, akademik yaşamımda beni destekleyen ve öğrencisi olmakla gurur duyduğum kıymetli hocam Prof. Dr. Adem SÖZÜER’e çok teşekkür ederim. Destek ve yardımına ihtiyaç duyduğum her an büyük bir nezaketle

beni karřılayan kıymetli hocam Prof. Dr. Hakan HAKERİ'ye minnetlerimi sunarım. Birlikte alıřtıđımız süre boyunca desteđini hep gördüğüm ve yabancı kaynaklara ulaşmamı sağlayan Do Dr. Murat Volkan DÜLGER'e, yüksek lisans boyunca yardımlarını benden esirgemeneyen Do. Dr. Sercan GÜRLER'e ve alıřmalarımı yürüttüğüm sırada bana huzurlu bir alıřma ortamı sağlayan Dr. Öğretim Üyesi Namık Kemal TOPÇU'ya ok teşekkür ederim.

Tezi okuyarak deđerli fikirlerinden istifade etmemi sağlayan kıymetli dönem arkadaşım Av. İrem YAMANER'e ve özellikle tez savunma sürecinde kaygı ve sevincime ortak olan kıymetli dönem arkadaşım Hakim Abdurrahman Burak KARAHAN'a ok teşekkür ederim. Tez yazma süreci boyunca yaşadığım pek ok zorlukta beni motive eden ve her zaman yanımda olan Av. Yahya YAVUZ'a ok teşekkür ederim.

Son olarak varlıklarıyla yaşamımı anlamlı kılan, beni tüm gücümle abalamaya ve alıřmaya iten canım aileme sonsuz minnetlerimi sunarım.

İstanbul, 2020

Neslihan CAN

İÇİNDEKİLER

ÖZ.....	ii
----------------	-----------

ABSTRACT	iii
ÖNSÖZ.....	iv
İÇİNDEKİLER.....	v
KISALTMALAR LİSTESİ	xiii
GİRİŞ	1

BİRİNCİ BÖLÜM

AVRUPA'DA VERİ KORUMA HUKUKUNUN TARİHSEL GELİŞİMİ ve KOLLUK VE CEZA ADALETİ DİREKTİFİ

I. AVRUPA KONSEYİ BAĞLAMINDA KİŞİSEL VERİLERİN KORUNMASI

7

- A. Avrupa İnsan Hakları Sözleşmesi (1953) 7
- B. 108 Sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulmasında Bireylerin Korunmasına Dair Avrupa Konseyi Sözleşmesi (1981), 181 Sayılı Ek Protokol (2001) ve 108+ Sözleşmesi (2018).....10
- C. R(87)/5 Sayılı Polis Veri Tavsiye Kararı (1987).....13

II. AVRUPA BİRLİĞİ BAĞLAMINDA KİŞİSEL VERİLERİN KORUNMASI

13

- A. 95/46 Sayılı Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Direktifi (1995).....15
- B. Avrupa Birliği Temel Haklar Şartı (2000).....18
- C. 2002/58/AT Sayılı Elektronik İletişim Alanında Özel Yaşamın Gizliliğinin Korunması ve Kişisel Verinin İşlenmesine İlişkin Direktif (2002).....19
- D. 2006/24/AT Sayılı İletişim Trafik Verilerinin Saklanması Direktifi (2006)
19
- E. 2008/977/JHA Sayılı Çerçeve Karar (2008) 21
- F. Avrupa Birliği'nin İşleyişi Hakkında Antlaşma (2012).....22
- G. 2016/679 Sayılı Genel Veri Koruma Tüzüğü (2018).....22

III. KOLLUK VE CEZA ADALETİ DİREKTİFİ	25
A. Kolluk ve Ceza Adaleti Direktifi'nin Ortaya Çıkışı	25
B. Kolluk ve Ceza Adaleti Direktifi-GDPR İlişkisi.....	30
C. Kolluk ve Ceza Adaleti Direktifi'nin Kapsamına Dâhil Olmayan Veri İşleme Faaliyetleri.....	35
1. Tamamen Kişisel veya Ev İçi Faaliyetler Gereği Veri İşlemeler	35
2. Avrupa Birliği Organ ve Kurumlarının Faaliyetleri Gereği Veri İşlemeler	
37	
a. Europol.....	38
b. Eurojust	40
c. Schengen Bilgi Sistemi (SIS).....	41
d. Vize Bilgi Sistemi (VIS).....	42
e. ECRIS	43
3. Kolluk ve Ceza Adaleti Direktifi'nden Önce Yürürlüğe Giren Antlaşmalar Gereği Veri İşlemeler	44
a. AB ve Bazı Ülkeler Arasında PNR Veri Aktarımı.....	45
b. Avrupa Siber Suçlar Sözleşmesi	49
4. Ulusal Güvenlik Faaliyetleri Gereği Veri İşlemeler	49
a. Ulusal Güvenliğin Anlamı	49
b. İstihbaratın Tanımı ve Türleri	51
c. Ön Alan Soruşturmaları ve İstihbarat İlişkisi.....	54
d. Türk Hukukunda İstihbarat Faaliyetleri Gereği Veri İşlemeler	56
e. Güvenlik Soruşturmaları Gereği Veri İşlemeler	61

İKİNCİ BÖLÜM

KOLLUK VE CEZA ADALETİ DİREKTİFİ'NDE YER ALAN SÜJELER

I. VERİ SAHİBİ.....	65
----------------------------	-----------

A. Tanım	65
B. Veri Sahibinin Hakları	67
1. Bilgilendirilme Hakkı.....	68
a. Tanım	68
b. Ek Bilgilendirilme Hakkı	69
c. Ek Bilgilendirilme Hakkının Sınırlandırılması	70
2. Erişim Hakkı	71
a. Tanım	71
b. Erişim Hakkının Sınırlandırılması.....	72
3. Kişisel Verinin Düzeltilmesi ve Silinmesini Talep Hakkı	73
a. Tanım	73
b. Silinmeye Alternatif Olarak İşlemenin Sınırlandırılması	75
c. Kişisel Verinin Düzeltilmesi, Silinmesi veya İşlenmesinin Sınırlandırılması Hakkının Sınırlandırılması	76
d. Unutulma Hakkı ile İlişkisi	76
4. Anonimlik Hakkı.....	83
a. Tanım	83
b. Anonimlik ve Büyük Veri İlişkisi	84
5. Denetleyici Makama Başvuru Hakkı	86
6. Tazminat Hakkı.....	87
II. VERİ SORUMLUSU	88
A. Tanım ve Türleri.....	88
B. Türk Hukukunda Veri Sorumlusu Olabilecek Makamlar	91
1. Adli-İdari Kolluk.....	92
2. Genel-Özel Kolluk	96
3. Özel Güvenlik Görevlileri	97

C. Veri Sorumlusunun Yükümlülükleri	99
1. Teknik ve İdari Tedbirler Almak	99
a. Nesnelerin İnterneti ve Veri Güvenliği	101
b. Büyük Veri Bakımından Alınacak Tedbirler	102
2. Logging Kayıtları Tutmak	103
3. Veri İhlal Bildiriminde Bulunmak	105
a. Bildirimin Denetleyici Makama ve Üye Devletin Veri Sorumlusuna Yapıldığı Haller	105
b. Bildirimin Doğrudan Veri Sahibine Yapıldığı Haller	106
4. Veri Koruma Görevlisi Tayin Etmek	107
5. Tasarımdan ve Başlangıçtan İtibaren Veri Koruma Yükümlülüğü	108
6. Veri Koruma Etki Değerlendirmesi	109
7. Denetleyici Makamın Görüşüne Başvurmak	111
III. VERİ İŞLEYEN	112
A. Tanım	112
B. Veri İşleme	113
1. Yetkili Makam Tarafından İşleme	113
2. Veri Koruma İlkelerine Riayet	114
a. Hukuka ve Dürüstlük Kurallarına Uygunluk	114
b. Amaçla Bağlılık	116
(1) Verinin Sonraki Kullanımı ve Amaçla Bağlılık	118
(2) Büyük Veri ve Amaçla Bağlılık	120
c. Veri Minimizasyonu	121
d. Güncel Olma İlkesi	122
e. Sürelilik İlkesi	123

3. Özel Nitelikli Kişisel Veriler Bakımından Gerekli Güvencenin Bulunması	126
4. Otomatik Karar Alma Mekanizması ve Veri İşleme.....	129
a. Profillemeye ve Otomatik Karar Alma Mekanizması İlişkisi	129
b. Büyük Veri ve Otomatik Karar Alma Mekanizması İlişkisi.....	131
IV. VERİ ALICISI	132
A. Tanım	132
B. Veri Aktarımı	132
1. Veri Aktarımının Şartları.....	136
a. Amaç	136
b. Yetkili Makam.....	137
c. Ön İzin	137
d. Yeterli Düzeyde Veri Koruması.....	138
(1) Yeterlilik Kriterleri	138
(2) Yeterlilik Kararının Aranmadığı Haller	140
2. Veri Aktarımının Doğrudan Veri Alıcısına Yapılması	141
a. Uluslararası Antlaşma Temeline Dayanmayan Doğrudan Veri Aktarımı	141
b. Uluslararası Antlaşma Temeline Dayanan Doğrudan Veri Aktarımı.	142
3. Türk Hukukunda Veri Aktarımı.....	143
V. VERİ KORUMA GÖREVLİSİ	143
VI. DENETLEYİCİ MAKAM.....	144
VII. AVRUPA VERİ KORUMA KURULU	146

ÜÇÜNCÜ BÖLÜM

KOLLUK VE CEZA ADALETİ DİREKTİFİ'NİN UYGULAMA ALANINDA KİŞİSEL VERİ ELDE ETME YÖNTEMLERİ

I. ÖNLEYİCİ KOLLUK FAALİYETLERİ	147
A. Kimlik Sorma ve Kimlik Tespiti	147
B. Parmak İzi ve Fotoğrafların Kaydı	150
1. Biyometrik Veri İşleme	150
a. Tanım	150
b. Yüz Tanıma Teknolojisi	155
2. Türk Hukukunda Durum	156
C. Elektronik Gözetim Sistemleri	159
1. Tanım.....	159
2. Kamusal Alanda Hukuka Uygun Elektronik Gözetim	160
3. Türk Hukukunda Durum	164
a. Mobil Elektronik Sistem Entegrasyonu (MOBESE).....	164
(1) Mevcut Uygulama	164
(2) Olması Gereken Uygulama	168
b. Araç Plakasının Okunması.....	170
c. Çocuk Bakım Kuruluşlarında Güvenlik Kamerası Uygulaması	170
D. Telekomünikasyon Yoluyla İletişimin Denetlenmesi.....	172
1. AİHM ve ABAD'nin Yaklaşımı	172
2. Türk Hukukunda Durum	175
a. İletişimin Denetlenmesinde Önleyici Kolluk ve İstihbari Kolluk Faaliyeti Ayrımı.....	176
b. Kaybolan Çocukların Bulunması Amacıyla İletişimin Denetlenmesi	178
E. Teknik Araçlarla İzleme.....	179
F. Banka Hesaplarının İncelenmesi	179
II. CEZA MUHAKEMESİ İŞLEMLERİ.....	180
A. Fizik Kimliğinin Tespiti.....	180

B. Genel Bilgi Toplama (GBT)	181
1. Tanım.....	181
2. Hukuka Uygunluk Değerlendirmesi.....	183
C. Beden Muayenesi, Vücuttan Örnek Alınması ve Moleküler Genetik İnceleme 186	
1. Tanım.....	186
2. DNA Verilerinden Ceza Muhakemesinde Yararlanılması	187
3. Türk Hukukunda Durum	190
D. Adli Bilişim	193
1. Tanım.....	193
2. Türk Hukukunda Adli Bilişim Uygulamaları	195
a. UYAP Bilişim Sistemi	196
(1) UYAP Kolluk Bilişim Sistemi	196
(2) Mobil Arananlar Bilgi Sistemi	196
(3) SEGBİS.....	196
b. Polnet	197
c. Jandarma Entegre Muhabere ve Bilgi Sistemi (JEMUS)	198
d. Balistika	198
E. Arama ve Elkoyma	199
1. CMK’de Yer Alan Arama ve Elkoyma Tedbirleri.....	199
2. IP Adresi	200
F. Özel Soruşturma Yöntemleri.....	203
1. Telekomünikasyon Yoluyla İletişimin Denetlenmesi	207
a. İletişimin Denetlenmesi Şartları	207
b. Trafik Verisi	209
c. Türk Hukukunda Durum.....	211

2. Gizli Gözetleme ve Teknik Araçla Takip.....	215
3. Gizli Soruşturmacı Görevlendirilmesi.....	217
G. Mahkeme Tutanakları ve Kararları	220
III. CEZALARIN İNFAZI	221
A. Adli Sicil Kaydının Tutulması	221
1. Türk Hukukunda Durum	221
2. Sicil Bilgilerinin Kamuya Açıklanması	224
B. Parmak İzi Alınması	226
C. Elektronik İzleme	226
1. Tanım.....	226
2. Türk Hukukunda Elektronik İzleme.....	228
D. Hükümlünün İletişiminin Denetlenmesi	231
E. Seyirden Yasaklanma.....	232
SONUÇ.....	235
KAYNAKÇA.....	239

KISALTMALAR LİSTESİ

AB

: Avrupa Birliği

ABAD	: Avrupa Birliđi Adalet Divanı
ABD	: Amerika Birleşik Devletleri
AFIS	: Otomatik Parmak İzi Tanıma Sistemi (Automated Fingerprint Identification System)
A.g.e.	: Adı geçen eser
AİHK	: Avrupa İnsan Hakları Komisyonu
AİHM	: Avrupa İnsan Hakları Mahkemesi
Akt.	: Aktaran
AÜEHFD	: Atatürk Üniversitesi Erzincan Hukuk Fakültesi Dergisi
AÜHFD	: Ankara Üniversitesi Hukuk Fakültesi Dergisi
BD	: Büyük Daire
BGE	: İsviçre Federal Mahkemesi Resmi Toplama Kararlar (Bundesgerichtsentscheid)
Bkz.	: Bakınız
BM	: Birleşmiş Milletler
CCTV	: Kapalı Devre Televizyon (Closed Circuit Television)
CD	: Yargıtay Ceza Dairesi
CGİK	: Ceza ve Güvenlik Tedbirlerinin İnfazı Hakkında Kanun
CHD	: Ceza Hukuku Dergisi
CHKD	: Ceza Hukuku ve Kriminoloji Dergisi
CIA	: Merkezi İstihbarat Ajansı (Central Intelligence Agency)
CMK	: 5271 sayılı Ceza Muhakemesi Kanunu
CMUK	: 1412 sayılı Ceza Muhakemeleri Usulü Kanunu
Çev.	: Çeviren
DMK	: Devlet Memurları Kanunu
ECRIS	: Avrupa Adli Sicil Bilgi Sistemi (European Criminal Records Information System)
Ed.	: Editör
EJN	: Avrupa Yargı Ağı (European Judicial Network)
Eurodac	: Avrupa Daktiloskopi (European Dactyloscopy)
Europol	: Avrupa Polis Teşkilatı

FBI	: Federal Soruřturma Brosu (Federal Bureau of Investigation)
GBT	: Genel Bilgi Toplama
GDPR	: Genel Veri Koruma Tzg (General Data Protection Regulation)
GPS	: Coğrafi Konum Sistemi (Global Positioning System)
GSHFD	: Galatasaray niversitesi Hukuk Fakltesi Dergisi
HD	: Yargıtay Hukuk Dairesi
HGK	: Yargıtay Hukuk Genel Kurulu
IP	: İnternet Protokol
İKHFD	: İstanbl Kltr niversitesi Hukuk Fakltesi Dergisi
İHFD	: İnn niversitesi Hukuk Fakltesi Dergisi
İHFM	: İstanbl niversitesi Hukuk Fakltesi Mecmuası
KHK	: Kanun Hkmnde Kararname
KİHBİ	: Kaçakçılık İstihbarat, Harekât ve Bilgi Toplama Dairesi
KVKK	: Kiřisel Verilerin Korunması Kanunu
m.	: Madde numarası
MI5	: Askeri İstihbarat Blm 5 (Military Intelligence Section 5)
MİT	: Milli İstihbarat Teřkilatı
MHF-HAD	: Marmara niversitesi Hukuk Fakltesi Hukuk Arařtırmaları Dergisi
OHAL KHK	: Olağnst Hal Kanun Hkmnde Kararnamesi
OLAF	: Avrupa Yolsuzlukla Mcadele Ofisi (Office Europen de Lutte Antifraude)
PACE	: Polis ve Ceza Delili Kanunu (The Police and Criminal Evidence Act)
para.	: Paragraf
PNR	: Yolcu İsim Kaydı (Personal Name Record)
POFA	: zgrlklerin Korunması Kanunu (The Protection of Freedoms Act)

PVSK	: Polis Vazife ve Salahiyet Kanunu
R.G.	: Resmi Gazete
SEGBİS	: Ses ve Görüntü Bilişim Sistemi
Sirene	: Ulusal Girişte Ek Bilgi Talebi
SIS	: Schengen Bilgi Sistemi (Schengen Information System)
StPO	: Alman Ceza Muhakemesi Kanunu (Strafprozeßordnung)
TBB	: Türkiye Barolar Birliği
TCK	: Türk Ceza Kanunu
TEU	: Avrupa Birliği Antlaşması (Treaty on European Union)
TFEU	: Avrupa Birliği'nin İşleyişi Hakkında Antlaşma (Treaty on the Functioning of the European Union)
UYAP	: Ulusal Yargı Ağı Projesi
vd.	: Ve devamı
WP29	: Avrupa Birliği Veri Koruma Çalışma Grubu (Working Party Article 29)
YÜHFD	: Yeditepe Üniversitesi Hukuk Fakültesi Dergisi
Y.Y.	: Yazar yok

GİRİŞ

Günümüzde özellikle bilişim sistemleri aracılığıyla işlenen suçlarda faillerin bıraktıkları dijital izlerden yararlanılması ve faillerin tespiti için gözetim sistemleri ve büyük veri analizi gibi yeni soruşturma yöntemleri kullanılmaktadır. Bu yöntemler de kolluk ve adli makamlar tarafından işlenen kişisel verilerin hukuki düzenlemelerle korunması ihtiyacına yol açmıştır¹. Zira kişisel verilerin adli makamların faaliyetlerini gerçekleştirmesi amacı ile bu makamlar tarafından işlenmesi, özel yaşamın gizliliğine saygı hakkı ve kişisel verilerin korunması hakkına müdahale oluşturmaktadır. Avrupa Konseyi'nde bu türden veri işleme faaliyetleri, AİHS m. 8 ve 108 sayılı Sözleşme; AB'de ise özel olarak 2016/680 sayılı Suçların Önlenmesi Soruşturulması, Ortaya Çıkarılması veya Kovuşturulması ya da Cezaların İnfazı Amacıyla Yetkili Makamlarca Kişisel Verilerin İşlenmesine İlişkin Olarak Gerçek Kişilerin Korunması ve Bu Verilerin Serbest Dolaşımı ile İlgili Avrupa Parlamentosu ve Konseyi Direktifi² kapsamında incelenmektedir.

AB Veri Koruma Reformu çerçevesinde genel olarak kişisel verilerin korunmasına ilişkin hükümler GDPR ile ihdas edilmiş, kolluk ve ceza adalet faaliyetleri çerçevesinde kişisel verilerin işlenmesi ise Kolluk ve Ceza Adaleti Direktifi'nde düzenlenmiştir. Zira Reform çalışmaları esnasında Avrupa Birliği Bölgeler Komitesi; kolluk ve adli makamlar tarafından işlenen kişisel verilerin muhtaç olduğu korumanın, kişisel verilerin korunması mevzuatındaki genel düzenlemelerden farklı olduğunu belirtmiştir ve koruma kapsamının buna göre net çizilmesi gerektiğine ilişkin görüş ileri sürmüştür³. Kolluk ve Ceza Adaleti Direktifi'nin benimsediği veri

¹ Juraj Sajfert, Teresa Quintel, "Data Protection Directive (EU) 2016/680 For Police and Criminal Justice Authorities", **Cole/Boehm GDPR Commentary**, Edward Elgar Publishing, 2019, s. 2 Çevrimiçi https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3285873 04.03.2020.

² Tezin bizzat konusunu oluşturan bu Direktif, kapsayıcı ve kısa bir terminolojiyi sağlamak amacıyla bundan sonra "Kolluk ve Ceza Adaleti Direktifi" olarak anılacaktır.

³ Bilişim ve Teknoloji Hukuku Enstitüsü, **Avrupa Parlamentosu ve Konseyi'nin 2016/680 sayılı ve 27 Nisan 2016 Tarihli Kişisel Verilerin Yetkili Otoritelerce Suçların Önlenmesi, Soruşturulması, Ortaya Çıkarılması veya Kovuşturulması veya Cezaların İnfazı Amacıyla İşlenmesiyle İlgili Gerçek Kişilerin Korunmasına ve Bu Verilerin Serbest Dolaşımına İlişkin ve 2008/977/JHA sayılı Konsey Çerçeve Kararı'nı Yürürlükten Kaldıran Direktif Hakkında Bilgi Notu**, İstanbul Bilgi Üniversitesi, İstanbul, 2019, s. 4.

koruma ilkeleri esas olarak GDPR ile paralellik arz etmektedir. Ancak Kolluk ve Ceza Adaleti Direktifi'nde adli makamlarca işlenen kişisel verilerin korunmasında özellikle ceza muhakemesi sürecinin kendine has işlerliği dolayısıyla farklı düzenlemeler öngörülmüştür.

Türk mevzuatında ise adli makamlarca işlenen kişisel verilerin korunmasına hasredilen düzenlemeler bir hayli sınırlıdır. Bununla birlikte 765 sayılı TCK'de kişisel veriler için öngörülen yetersiz korumanın aksine, Türk Ceza Hukuku Reformu sonucu TCK m. 132-140 ile yeni suç tiplerine ve CMK'de bazı veri koruma hükümlerine yer verilerek özel yaşam ve kişisel verilere koruma sağlanmıştır⁴. Anayasa m. 20/3'te kişisel verilerin korunması hakkı, özel yaşamın gizliliği hakkından bağımsız bir hak olarak tanınmıştır⁵. Ancak özel yaşamın gizliliği hakkından ayrı olarak hakka müdahalenin sınırlarını çizen özel sınırlama sebepleri sayılmamıştır ve kanunda düzenlenen haller ve ilgilinin açık rızası ile bu hakka müdahale edilebileceği düzenlenmiştir.

2016 yılında yürürlüğe giren KVKK ile Türk hukukunda ilk kez kişisel verinin tanımından Kişisel Verileri Koruma Kurumunun ihdasına kadar uzanan geniş düzenlemeler yapılmıştır. KVKK'de hangi hallerde kişisel verilerin korunması hakkına müdahale edilebileceği de öngörülmüştür. Buna göre önleyici, koruyucu faaliyetler ve istihbarat faaliyetleri gereği kişisel verilerin işlenmesinde yahut yargı ve infaz makamlarınca kişisel verilerin işlenmesinde KVKK uygulanmayacaktır⁶. Öte yandan KVKK m. 28/2'de bazı hallerde KVKK'nin sayılan bazı hükümleri dışında veri işleme faaliyetlerine uygulanacağı düzenlenmiştir. Bu hallerden biri de *suç işlenmesinin önlenmesi veya ceza soruşturması için gerekli olması halinde veri*

⁴ Fatih Selami Mahmutoğlu, "Ceza ve Caza Yargılama Hukukunda Özel Yaşam", **Özel Yaşamın Gizliliği Paneli**, Ankara, TBB Yayınları, 2009, s. 107.

⁵ Bazı yazarlarca kişisel verilerin korunması hakkı, ayrı bir maddede düzenlenmediğinden ve hakka müdahale sebepleri ayrıca zikredilmediğinden bu hak anayasal düzeyde bağımsız bir hak değildir. Bkz. Muhammet Sefa Mutlu, **Kişisel Verilerin Soruşturma Evresinde İşlenmesi ve İnsan Hakları Kapsamında Korunması**, Ankara, Adalet Yayınevi, 2020, s. 51.

⁶ M. 28/1 "ç) *Kişisel verilerin millî savunmayı, millî güvenliğini, kamu güvenliğini, kamu düzenini veya ekonomik güvenliğini sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi.*

d) *Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi.*"

*işlemedir*⁷. Suç işlemenin önlenmesi veya ceza soruşturması sırasında veri işlendiğinde KVKK'nin amaç ve ilkelerine uyulacak; ancak *veri sorumlusunun aydınlatma yükümlülüğü, zararın giderilmesini talep hariç veri sahibinin hakları ve veri sorumluları siciline kayıt hükümleri uygulanmayacaktır*. Maddenin birinci fıkrasında önleyici faaliyetler kapsamında işlenen kişisel veriler KVKK'nin uygulama alanı dışında tutulmuşken, ikinci fıkrasında suçların önlenmesi sırasında işlenen kişisel veriler KVKK'nin uygulama alanında bırakılmıştır.

Benzer durum *soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz makamları tarafından kişisel verilerin işlenmesi* hükmü ve KVKK m. 28/2 arasında da bulunmaktadır. Zira KVKK m. 28/1-d hükmü uyarınca soruşturma evresinde yargı makamları tarafından, yani 5235 sayılı Kanun'da belirtilen ceza mahkemeleri ve savcılıklar tarafından gerçekleşen veri işleme faaliyetleri KVKK kapsamı dışındadır. Ancak ceza soruşturmalarında söz gelimi kolluk tarafından gerçekleşen kişisel veri işleme faaliyeti ise KVKK kapsamındadır. Ancak m. 28/2 uyarınca bu veri işleme faaliyetine KVKK'nin bazı hükümleri uygulanmayacaktır. Anlaşılabacağı üzere maddenin lafzı bir hayli belirsizdir. Doktrinde bu hükümlerden hareketle ceza muhakemesi ve infaz faaliyetleri sırasında işlenen kişisel verilerin tamamen korunaksız olduğu sonucuna varılmaması gerektiği belirtilmiştir⁸. Zira bu hallerde KVKK dışındaki diğer hukuk normları gündeme gelerek işlenen veriler kişilik haklarına tanınan korumadan yararlanabilecektir.

Suçların önlenmesinde, ceza muhakemesinde ve cezaların infazında işlenen kişisel verilerin açık biçimde korunması, PVSK ve CMK'de bulunan sınırlı sayıda hüküm ile sağlanmaktadır. Ancak şüphesiz adli makamlarca işlenen kişisel verilerin korunmasında da Türk hukukunda yeterli bir düzeye ulaşılmış olmalıdır. Zira Türkiye her ne kadar AB üyesi olmasa da üyelik süreci devam etmektedir. Türkiye suç ve suçlulukla mücadelede, adli işbirliği sözleşmeleri kapsamında AB üyesi devletlerden kişisel veri talep ettiğinde bu talebin karşılanması için kişisel verilerin korunmasında yeterli bir düzeyde olmak zorundadır. Bu nedenle de çalışma boyunca Türk hukukunda

⁷ KVKK m. 28/2-a.

⁸ Bkz. Baran Kızıllırmak, "Kişisel Verilerin İşlenmesinde Adli ve Önleyici Amaçla Öngörülen İstisnaların Ulusal ve Uluslararası Hukuka Göre Değerlendirilmesi", **Kadir Has Üniversitesi Hukuk Fakültesi Dergisi**, c. 7, s. 2, 2019, s. 252.

eksik olduğuna inandığımız hususlar Kolluk ve Ceza Adaleti Direktifi hükümleri ışığında ele alınmıştır.

Kişisel veriler bir insan hakkı olarak korunmaya değerdir. Bunun haricinde kişisel veriler tıpkı bir dijital para gibi ekonomik bir değer ifade etmektedir⁹. Ancak bu tez kapsamında suçların önlenmesi, ceza muhakemesi ve infaz aşamasında başvurulacak kişisel veriler, yalnız korunmaya muhtaç bir insan hakkı olarak değerlendirilmiştir. Bu aşamalarda kişisel verilerin nasıl korunacağına ilişkin tek kapsamlı belge olan Kolluk ve Ceza Adaleti Direktifi ekseninde konu ele alınmıştır.

Tezin birinci bölümünde Avrupa Konseyi ve Avrupa Birliği'nin birincil ve ikincil düzenlemeleri, kişisel verilerin korunması hakkının tarihsel gelişimi içinde sunulmuştur. Kolluk ve Ceza Adaleti Direktifi'nin maddi bakımdan ve yer bakımından uygulama alanı çizilerek ayrıca GDPR ile arasındaki ilişki ve Kolluk ve Ceza Adaleti Direktifi'nin kapsam dışında bıraktığı alanlar incelenmiştir.

Tezin ikinci bölümünde Kolluk ve Ceza Adaleti Direktifi'nde yer alan veri sahibi, veri sorumlusu, veri işleyen, veri alıcısı, veri koruma görevlisi, denetleyici makam ve Avrupa Veri Koruma Kurulu anlatılmıştır. Veri sahibinin hakları ve veri sorumlusunun yükümlülüklerine detaylıca yer verilmiştir. Veri işleme faaliyetinin zorunlu süjesi olmamakla birlikte veri işleyene de yer verilmiş, bu meyanda veri koruma ilkeleri ışığında hukuka uygun veri işleme anlatılmıştır.

Tezin üçüncü bölümünde ise bazı önleyici kolluk faaliyetleri Kolluk ve Ceza Adaleti Direktifi'nin hükümleri ve Türkiye'de mevcut uygulama ile karşılaştırmalı olarak incelenmiştir. Ardından ceza muhakemesi sürecinde başvurulacak koruma tedbirlerinin uygulanması sırasında gündeme gelen kişisel verilere değinilmiştir. Son olarak da cezaların infazında gündeme gelen kişisel verilere temas edilmiştir. Tezin bu bölümündeki önleyici kolluk faaliyetleri, koruma tedbirleri ve infaz faaliyetleri yalnız kişisel verilerin işlenmesi ile mevcut bağlantıları gözetilerek anlatılmıştır.

⁹ Svetlana Yakovleva, "Should Fundamental Rights to Privacy and Data Protection be a Part of the EU's International Trade 'Deals'?", **World Trade Review**, c. 17, s. 3, 2018, s. 481.

Kişisel veriler, modern zamanın altını¹⁰ olarak değerlendirilip de akademik çalışmalarda pek çok yazar tarafından altına hücum edildiği için kişisel verilerin korunması konusundaki bu çalışmalarda detaylıca açıklanmış terimler, bu tez kapsamında uzun uzadıya açıklanmamıştır. Bununla birlikte tez boyunca terim birliğinin sağlanması için çeşitli açıklamalara giriş kısmında yer verilmiştir. Ayrıca sınırlama yapabilmek adına, içerik olarak her biri ayrı bir çalışma konusu olabilecek unutulma hakkı, büyük veri, anonimleştirme gibi terimlere yalnızca adli makamlarca işlenen kişisel verilerin korunması ile ilgileri olduğu ölçüde değinilmiştir.

Tez boyunca kişisel veriden anlaşılması gereken, belirli ya da belirlenebilir bir gerçek kişi ile ilişkilendirilebilir her türlü bilgidir¹¹. Bu tanım geniş, esnek ve teknolojik gelişmeler ile uyumludur. Söz gelimi GDPR sübjektif olarak gerçek bir kişinin belirlenmesinde, veri sorumlusu ya da bir üçüncü kişinin yeteneğini aramamış; verinin işlendiği zamandaki teknolojinin durumunu belirlenebilirliğe ilişkin makul olasılık (*reasonable likelihood*) testine tabi tutmuştur¹². Ayrıca verinin kişisel veri niteliğine sahip olup olmadığı, bulunduğu bağlam özelinde bir analizle yapılmaktadır. Söz gelimi elde edildiği anda anonim olan veri, teknolojik gelişmeler sonucu kişisel veri mahiyetini kazandığında kişisel veri korunmasından yararlanacaktır¹³. Son olarak belirtilmelidir ki kişisel verinin mahrem olması gerekmemektedir¹⁴.

¹⁰ Son yıllarda, verilerin değerli bir varlık haline geldiği ve hatta geleceğin para birimi olarak adlandırıldığına dair bkz. Paul Voigt, Axel von dem Bussche, **The EU General Data Protection Regulation (GDPR) A Practical Guide**, Springer, 2017, s. 1; Büyük verinin ise 21. yüzyılın petrolü olduğuna ilişkin bkz. Peter Sondergaard, “Big Data Fades to the Algorithm Economy”, Çevrimiçi <https://www.forbes.com/sites/gartnergroup/2015/08/14/big-data-fades-to-the-algorithm-economy/#69161c9851a3> 22.10.2019.

¹¹ AYM de kişisel veriler ve özel yaşamın gizliliğine ilişkin başvurularda bu tanımlı benimsemektedir. Bkz. AYM, E.2014/74, K.2014/201, 25.12.2014; E.2013/122, K.2014/74, 09.04.2014; E.2014/149, K.2014/151, 02.10.2014; E.2013/84, K.2014/183, 04.12.2014; E.2014/180, K.2015/30, 19.03.2015; Bülent Kaya [GK], B. No: 2013/2941, 11.05.2016, para. 49; Turgut Duman, B. No: 2014/15365, 29.05.2019, para. 57 Çevrimiçi <https://www.anayasa.gov.tr/tr/kararlar-bilgi-bankasi/> 29.03.2020.

¹² GDPR resital m. 26; Nadezhda Purtova, “The Law of Everything: Broad Concept of Personal Data and Future of EU Data Protection Law”, **Law, Innovation and Technology**, c. 10, s. 1, 2018, s. 44. *Dülger*’e göre belirlenebilirlik, tamamlayıcı verinin bulunduğu yer, verinin tutulduğu süre, verinin işleme amacı dikkate alınarak tespit edilebilir. Bkz. Murat Volkan Dülger, **Kişisel Verilerin Korunması Hukuku**, 2. Baskı, İstanbul, Hukuk Akademisi, 2019, s. 97; Aynı yönde bkz. Şeyma Sert, **Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması**, İstanbul, Seçkin Yayıncılık, 2019, s. 32.

¹³ Purtova, **a.g.e.**, s. 44.

¹⁴ Dülger, **Kişisel Verilerin Korunması Hukuku**, s. 5; Kişisel verilerin korunması hakkının, özel yaşamın korunması hakkı ile korunmaya layık görmek, *Dülger*’e göre bu hakkın korunması bakımından devlete yalnız negatif yükümlülük yükler. Oysa özel yaşama tanınan korumadan sıyrılarak korunması

Kişisel veri, ancak gerçek kişi ile ilişkilendirilebilir veridir. Türk hukukunda KVKK başta olmak üzere genel eğilim de kişisel veri sahibinin ancak gerçek kişi olabileceğidir. Ancak Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik'te istisnai olarak tüzel kişilere ait verilerin de kişisel veri olduğu kabul edilmiştir¹⁵. Kolluk ya da adli makamlar, kişisel veri harici belirli bir konuya ilişkin de veri işleyebilmektedir. Konuya ilişkin verilere uçağın kalkış saati, kapı numarası örnek verilebilir, ancak bu veriler belirli bir gerçek kişi ile ilişkilendirilemediği takdirde kişisel veri değildir ve veri işleme kurallarına uymaksızın yetkili makamlar bu verilerden yararlanabilir¹⁶.

Kişisel verilerin korunması hakkı ise Alman Federal Anayasa Mahkemesi'nin Nüfus Sayımı Kararı'ndan beri kabul edilen, bireylerin kişisel verileri üzerinde olan ve bu verilerin geleceğini belirleme hakkıdır. Bu hak, insan onuru ve kişiliğin serbestçe geliştirilmesi hakkı ile sıkı ilişki içerisinde¹⁷. Devletler 1970'lerden itibaren bilişim alanındaki önemli gelişmeler üzerine¹⁸ başta elektronik ticarete kullanılan kişisel verilere koruma sağlayarak elektronik ticareti geliştirmek ve AB hukukunda yeknesaklık sağlamak için kişisel verilerin korunması hakkına ilişkin düzenlemeler ihdas etmişlerdir¹⁹.

ise devletin veri işleme şartlarını düzenlemek ve koruyucu kamu kuruluşu ihdas etmek gibi pozitif yükümlülüklerini yerine getirmesi ile mümkündür. Bkz. Dülger, **Kişisel Verilerin Korunması Hukuku**, s. 21.

¹⁵ Bkz. R.G. Sayısı: 28363, R.G. Tarihi: 24.07.2012, m. 3/1-h.

¹⁶ Örneğin Bavyera Polis Kanunu m. 20 "konuya ilişkin veri" kavramına sahiptir. Bkz. Feridun Yenisey, **Kolluk Hukuku**, 2. Baskı, İstanbul, Beta Yayıncılık, 2015, s. 320.

¹⁷ Doğan Kılınç, "Anayasal Bir Hak Olarak Kişisel Verilerin Korunması", **AÜHFD**, c. 61, s. 3, 2012, s. 1098; Kişisel verilerin korunması hakkı, insan onuru ile ilişki içerisinde. Zira kişinin yaşam ilişkilerinin incelenerek kişisel verilerinin toplanması ve ona dair bir profil çıkarılması bireyin "basit bir obje" haline gelmesine yol açmaktadır. Bkz. Oğuz Şimşek, **Anayasa Hukukunda Kişisel Verilerin Korunması**, İstanbul, Beta Yayıncılık, 2008, s. 132.

¹⁸ Durmuş Tezcan, "Özel Hayat Açısından Kişisel Verilerin Korunması", **İKÜHFD**, c. 16, s. 1, 2017, s. 18.

¹⁹ Kılınç, **a.g.e.**, s. 1107.

BİRİNCİ BÖLÜM

AVRUPA'DA VERİ KORUMA HUKUKUNUN TARİHSEL GELİŞİMİ ve KOLLUK VE CEZA ADALETİ DİREKTİFİ

I. AVRUPA KONSEYİ BAĞLAMINDA KİŞİSEL VERİLERİN KORUNMASI

A. Avrupa İnsan Hakları Sözleşmesi (1953)

Kişisel verilerin korunması hakkı, bireylere kişisel verilerinin geleceğini belirleme yetkisi veren yani verilerinin işlenmesi üzerinde söz sahibi olmalarına olanak sağlayan bir haktır²⁰. AİHS sisteminde kişisel verilerin korunması hakkı başlı başına bağımsız bir hak olarak tanınmamışsa da bu hak özel yaşamın²¹ korumasından yararlanmaktadır. Zira AİHM, özel yaşamı geniş yorumlamaktadır²². Buna göre bireyler özel yaşamın gizliliğine saygı hakkı gereği kendilerine ilişkin bilgileri kontrol

²⁰ Dülger, **Kişisel Verilerin Korunması Hukuku**, s.15. Bu hakkın hukuki mahiyetinin ne olduğu ve bağımsız bir hak olup olmadığına ilişkin detaylı bilgi için bkz. Dülger, **Kişisel Verilerin Korunması Hukuku**, s. 16-24.

²¹ Günümüz ihtiyaçlarına cevap vermesi ve kapsamının daha geniş olduğu gözetildiğinde “özel yaşamın gizliliği hakkı” yerine “özel yaşam hakkı” ifadesinin tercih edilmesi gerektiği ileri sürülmüştür. Bkz. Sultan Tahmazoğlu Üzeltürk, “Özel Hayatın Korunmasına İlişkin Başlıca Sorunlar”, **GSÜHFD**, c. 7, s. 1, İstanbul, 2008, s. 99.

²² AİHM, her somut olayı kendi şartları içinde değerlendirmekte ve zamanın ihtiyaç ve gerçeklerini göz önüne alarak AİHS’de geçen terimlerin içeriğini doldurmaktadır. Bu nedenle kişinin sağlığı, iş yaşamı, haberleşmesi, kitlesel gözetimi de özel yaşam içinde değerlendirilmektedir. Bkz. Bahri Öztürk, Elif Altınok Çalışkan, **Kişisel Verilerin Korunması Kanunu Hakkında Genel Değerlendirmeler ve Anayasaya Aykırılık Sorunu**, **Fasikül Hukuk Dergisi**, c. 10, s. 100, 2018, s. 284; Maria Tzanou, **The Fundamental Right to Data Protection**, Oregon, Hart Publishing, 2017, s. 45; Tezcan, **a.g.e.**, s. 21; A. Şeref Gözübüyük, Feyyaz Gölcüklü, **Avrupa İnsan Hakları Sözleşmesi ve Uygulaması**, 11. Bası, Ankara, Turhan Kitabevi, 2016, s. 349; Kathleen M. Burch, “Protecting Privacy in the Digital Age: Europe and The United States”, **Prof. Dr. Feridun Yenisey’e Armağan**, c. 2, İstanbul, Beta Yayıncılık, 2014, s. 1716; Juliane Kokott, Christoph Sobotta, “The Distinction Between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR”, **International Data Privacy Law**, c. 3, s. 4, 2013, s. 223; Mahmutoglu, **a.g.e.**, s. 102-103; Ursula Kilkely, “Özel Yaşama ve Aile Yaşamına Saygı Gösterilmesi Hakkı”, **İnsan Hakları El Kitapları No.1**, Almanya, Avrupa Konseyi, 2001, s. 16; Nitekim AİHM, *Costello-Roberts v. Birleşik Krallık* kararında özel yaşam kavramının geniş olduğu ve kapsamlı bir tanım yapılmaya müsait olmadığını belirtmiştir. Bkz. *Niemeitz v. Almanya*, B. No: 13710, 16.12.1992, para. 29; *Costello-Roberts v. Birleşik Krallık*, B. No: 13134/87, 05.03.1993, para. 36, aynı yönde bkz. *Perry v. Birleşik Krallık*, B. No: 63737, 17.10.2003, para. 36; *S ve Marper v. Birleşik Krallık*, B. No: 30562/04 ve 30566/04, 04.12.2008, para. 103; *Uzun v. Almanya*, B. No: 35623, 02.12.2010, para. 43 Çevrimiçi <https://hudoc.echr.coe.int/> 29.03.2020.

edebilmektedir²³. Özel yaşamın gizliliği de kişiye toplumdan çekilme, mahremiyet, tanınmazlık ve saklama imkânları tanımaktadır²⁴. Kişinin kendisi ve özel yaşamına dair bilgi elde etme aracı olarak kişisel veriler kullanılmaktadır ve bunlar özel yaşamın gizliliğine saygı hakkının alt kategorilerinden olan veri mahremiyeti korumasından yararlanır²⁵. Yani verinin korunması, salt soyut bir kavram olan verinin değil, esasen kişisel verisi korunmak suretiyle bireyin özel alanının korunmasıdır²⁶. AİHS bağlamında kişisel verilerin korunması, AB üyesi olmayıp da Avrupa Konseyi üyesi olan ülkeler açısından bu hakkın hukuki mahiyetini tespit edebilmek açısından önemlidir²⁷. Genellikle AİHM içtihatlarında; suçların önlenmesinde, ceza muhakemesinde kişisel verilerin kullanılması ve ulusal güvenlik amacıyla kolluk güçleri tarafından kişisel verilerin kullanılması üzerinde durulmaktadır²⁸.

Bilişim ve gözetim teknolojilerinin gelişmesi ile birlikte küresel bir eğilim olarak kişisel verilerin başlı başına korunması gereken bir değer olduğu görüşü hukuki düzenlemelere de yansımıştır²⁹. Pek çok Avrupa Konseyi üyesi devlet, kişisel verilerin korunmasını temel ve bağımsız bir hak olarak değerlendirmiştir³⁰. Hatta Almanya bir

²³ Aydın Akgül, “Kişisel Verilerin Korunmasında Yeni Bir Hak: ‘Unutulma Hakkı’ ve AB Adalet Divanı’nın ‘Google Kararı’”, **TBB Dergisi**, c. 27, s. 116, 2015, s. 19; Gülay Arslan Öncü, “Özel Yaşama ve Aile Yaşamına Saygı Hakkı”, **Anayasa Mahkemesine Bireysel Başvuru El Kitapları Serisi-8**, 2019, Çevrimiçi https://www.anayasa.gov.tr/media/5604/ozel_yasam_hakki.pdf 30.03.2020, s. 78.

²⁴ Sulhi Dönmezer, Köksal Bayraktar, **Basın Hukuku**, Genişletilmiş 6. Baskı, İstanbul, Beta Yayıncılık, 2016, s. 348; Tahmazoğlu Üzeltürk, **a.g.e.**, s. 98.

²⁵ Avrupa Konseyi Parlamenterler Meclisi’nin 1165(1998) nolu Kararı m. 5’e göre kişisel verilerin toplanması ve kullanılmasını mümkün kılan yeni iletişim teknolojileri göz önüne alındığında kişinin kendi verilerini kontrol etme hakkının da mahremiyet hakkı ifadesine eklenmesi gerekmektedir. Bkz. Çevrimiçi <https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=16641&lang%20=en> 04.03.2020; Muammer Ketizmen, **Türk Ceza Hukukunda Bilişim Suçları**, Ankara, Adalet Yayınevi, 2008, s. 192-193. Özel yaşamın gizliliği kişinin bedeni, eşyası, kağıtları ve konutunun yararlanması gereken bölgesel mahremiyet; kişinin mektupları, telefon görüşmeleri özetle haberleşmesinin yararlanması gereken haberleşme mahremiyeti; kişinin vücut dokunulmazlığının yararlanacağı vücut bütünlüğüne ilişkin mahremiyet ve nihayet kişisel verilerinin işlenmesine ilişkin veri mahremiyetinden oluşmaktadır. Veri korumasını bilgi mahremiyeti olarak değerlendiren eser için bkz. Neslihan Can, “Tıp Hukuku Bağlamında Çocuk Hastanın Mahremiyet Hakkı”, **3. Uluslararası Tıp Hukuku Kongresi Bildirileri Kitabı**, Ed. Hakan Hakeri, Cahid Doğan, Ankara, Adalet Yayınevi, 2019, s. 1140; Kişisel verilerin korunmasındaki amacın özel yaşamın korunması olduğuna dair bkz. Güçlü Akyürek, **Özel Hayatın Gizliliğini İhlal Suçu**, Güncellenmiş ve Genişletilmiş 2. Baskı, Ankara, Seçkin Yayıncılık, 2014, s. 52.

²⁶ Şimşek, **a.g.e.**, s. 4.

²⁷ Dülger, **Kişisel Verilerin Korunması Hukuku**, s. 55.

²⁸ Kilkely, **a.g.e.**, s. 58.

²⁹ Dülger, **Kişisel Verilerin Korunması Hukuku**, s. 6.

³⁰ İlk kez 1970 yılında Almanya’nın Hessen eyaletinde, 1973’te İsveç’te, 1978’de Fransa’da kişisel verilerin korunmasına ilişkin kanunlar yürürlüğe girmiştir. Bkz. Şimşek, **a.g.e.**, s. 10.

adım daha ileri giderek Alman Anayasası'nda yer almasa da kişilik hakkının uzantısı olarak *enformasyonel self-determinasyon hakkı* kavramsallaştırmasını yapmıştır³¹. Bir kişisel verinin mahrem kalması yani veri sahibinin rızası olmaksızın açıklanamaması, ifşa edilememesi ve bu veriye başka kişilerce erişilememesi, bireyin kendisi hakkındaki bilgilerin geleceğini tayin etme hakkının gereğidir³². 2008 yılında ise Alman Anayasa Mahkemesi daha da ileri giderek dijital özel yaşamın korunması (*bilgi teknolojisi sisteminin güvenilirliğinin ve bütünlüğünün korunması*) temel hakkını da kabul etmiştir³³.

Avrupa Konseyi üyesi Türkiye'de ise kişisel verilerin başlı başına bir hak olarak tanınması, AY m. 20/3 ve KVKK ile gerçekleşmiştir. Bundan önce ise kişisel veriler, insan onuru³⁴, kişinin maddi ve manevi varlığını koruma ve geliştirmesi³⁵ ve özel yaşam³⁶ çerçevesinde değerlendirilmiştir.

³¹ Bkz. Alman Anayasa Mahkemesi'nin 1983 yılında verdiği Volkszählungsurteil kararı; Şehriban İpek Aşıkoğlu, **Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri**, İstanbul, On İki Levha Yayınları, 2018, s. 181; Tevfik Sönmez Küçük, "Kişisel Verilerin Korunması Hakkı Çerçevesinde Kamuya Açık Alanların Kamu Tüzel Kişileri Tarafından Video Kamera Aracılığı İle Önleyici Amaçla İzlenmesi", **YÜHFD**, c. 15, s. 1, 2018, s. 60; Murat Önok, "Kişisel Verilerin Korunması Bağlamında 'Unutulma Hakkı' ve Türkiye Açısından Değerlendirmeler", **İKÜHFD**, c. 16, s. 1, 2017, s. 159; İkbâl Gür, **Kişisel Verilerin Korunması Hususunda AB ile ABD Arasında Çıkan Uyuşmazlıklar ve Çözüm Yolları**, Ankara, Turhan Kitabevi, 2010, s. 147; Nilgün Başalp, **Kişisel Verilerin Korunması ve Saklanması**, Ankara, Yetkin Yayınları, 2004, s. 31; Almanya'da veri koruması Persönlichkeitsrechte (kişilik hakları), İsviçre'de integritet (kişi bütünlüğü) kavramlarında mündemiç olarak görülmüştür; Anayasal düzeyde kişisel verilerin korunması hakkının tanındığı devletler ise Hollanda, Portekiz, Estonya, Polonya, Azerbaycan ve İspanya'dır. Danimarka, Fransa, İngiltere ve İrlanda'da ise anayasal bir hüküm bulunmamaktadır. Bkz. Şimşek, **a.g.e.**, s. 40-41; Küçük, **a.g.e.**, s. 64; Akyürek, **a.g.e.**, s. 60, dipnot 203.

³² Arslan Öncü, "Özel Yaşama ve Aile Yaşamına Saygı Hakkı", s. 311.

³³ Renzo Orlandi, "Telekomünikasyon Yoluyla İletişimin Önleme ve Adli Amaçlı Denetlenmesi-Özel Yaşamın Gizli Alanı, Teknik Araçla İzleme, Online Arama ve Kendi Kişisel Bilgileri Üzerinde Karar Verebilme Hakkı", Çev. Ali Kemal Yıldız, **Dünyada ve Türkiye'de Ceza Hukuku Reformları Kongresi**, c. 1, Ed. Adem Sözüer, İstanbul, On İki Levha Yayıncılık, 2013, s. 140.

³⁴ KVKK'nın yürürlüğünden evvel, 5809 sayılı Elektronik Haberleşme Kanunu m. 51 ile kişisel verilerin işlenmesi ve gizliliğinin korunmasına ilişkin düzenlemenin AY'ye aykırı olduğu gerekçesiyle açılan iptal davasında AYM, "*Kişisel verilerin korunması hakkı, insan onurunun korunması ve kişiliğin serbestçe geliştirilmesi hakkının özel bir biçimi olarak, bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır.*" değerlendirmesini yapmıştır. Bkz. AYM, E.2025/61, K.2016/172, R.G. Sayısı: 29913, R.G. Tarihi: 9.12.2016, para. 192; Yüksel'e göre de Avrupa'da özel yaşamın gizliliği, insan onuruna saygı üzerine kurulu iken ABD'de ise kişisel serbestlik veya kişi özgürlüğü üzerinedir. Bkz. Saadet Yüksel, **Özel Yaşamın Bir Parçası Olarak Telekomünikasyon Yoluyla Yapılan İletişimin Gizliliğine Önleyici Denetimle Müdahale**, İstanbul, Beta Yayıncılık, 2012, s. 126.

³⁵ Yener Ünver, "Kişisel Verilerin Korunması", **GSÜHFD**, c. 7, s. 1, İstanbul, 2008, s. 174.

³⁶ Kişisel verilerin korunmasını, özel yaşama saygı hakkı çerçevesinde değerlendiren bazı eserler için bkz. Durmuş Tezcan, Mustafa Ruhan Erdem, R. Murat Önok, **Teorik ve Pratik Ceza Özel Hukuku**, Güncellenmiş 17. Baskı, Ankara, Seçkin Yayıncılık, 2019, s. 654; Handan Yokuş Sevrük,

Kişisel verilerin korunması hakkına yönelik kamu makamlarından gelen bir müdahalenin hukuka uygun olabilmesi için AIHS m. 8/2'deki müdahale şartlarını taşıması gerekir. Özellikle ceza muhakemesi sürecinde başvurulacak telekomünikasyon yoluyla iletişimin denetlenmesi, teknik araçla takip gibi görece olarak yeni koruma tedbirleri ve bu tedbirler sırasında elde edilen kişisel verilere ilişkin detaylı iç hukuk mevzuatı mevcut olmalıdır³⁷. Bu mevzuat ulaşılabilir ve öngörülebilir olmalıdır. Ayrıca hakka müdahale demokratik bir toplumda gerekli ve orantılı olmalıdır.

AIHM, *Ekimdzhev ve diğerleri v. Bulgaristan*³⁸ kararında kişisel verilerin korunması için asgari standartlarını da açıklamıştır. Buna göre, başvurulacak tedbirler suçun yapısına uygun olmalı, tedbirin uygulanmasında sübjektif sınırlamalar bulunmalı, kişisel verilerin işlenmesi kanun ile düzenlenmiş olmalı, kişisel verilerin ilk işlendiği makam harici makamlarca işlenmesine özel önlemler almak suretiyle izin verilmeli ve kanun verilerin silinme ve yok edilme şartlarını düzenlemelidir³⁹.

B. 108 Sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulmasında Bireylerin Korunmasına Dair Avrupa Konseyi Sözleşmesi (1981), 181 Sayılı Ek Protokol (2001) ve 108+ Sözleşmesi (2018)

Türk Ceza Hukuku Özel Hükümler, Genişletilmiş ve Gözden Geçirilmiş 2. Baskı, Ankara, Adalet Yayınevi, 2019, s. 267; Kişisel verilerin korunması hakkının bir negatif statü hakkı olarak özel yaşamın gizliliği hakkına dayandığına ilişkin örneğin bkz. Kılınç, **a.g.e.**, s. 1099. Ancak *Küçük*, kişisel verilerin korunması hakkının, bu hakkı koruyucu iç hukuk mekanizmaları ve hukuki düzenlemeler ihdasını gerektirdiğini ve bu nedenle devlete yalnız negatif yükümlülük değil, pozitif yükümlülük de yüklediği kanaatindedir. Bkz. *Küçük*, **a.g.e.**, s. 65.

³⁷ Nitekim AIHM'nin verdiği ihlal kararlarının ardından taraf devletler de bu düzenlemeleri yapma yoluna girmişlerdir. Örneğin *Kruslin v. Fransa* başvurusunda verilen ihlal kararının ardından telefon dinlemeye ilişkin Fransız Ceza Muhakemesi Kanunu m. 100 ve devamında ayrıntılı düzenlemeler yapılmış, *Malone v. Birleşik Krallık* başvurusunun ardından ise Birleşik Krallık Haberleşmenin İzlenmesi Kanunu yürürlüğe girmiştir. Bkz. Osman Doğru, İnsan Hakları Avrupa Mahkemesi Kararlarının İç Hukuklara Etkileri, Çevrimiçi <https://www.anayasa.gov.tr/media/4671/dogru.pdf> 08.01.2020, s.216-217; Adem Sözüer, "Türkiye'de Karşılaştırmalı Hukukta Telefon, Teleks, Faks ve Benzeri Araçlarla Yapılan Özel Haberleşmenin Bir Ceza Yargılaması Önlemi Olarak Denetlenmesi", **İÜHF**, c. 55, s. 3, 1997, s. 92.

³⁸ *Ekimdzhev ve diğerleri v. Bulgaristan*, B. No: 70078/12, 02.05.2019 Çevrimiçi <https://hudoc.echr.coe.int/> 29.03.2020.

³⁹ Orlandi, **a.g.e.**, s. 141.

AİHS'nin kişisel verilerin korunmasına ilişkin açık bir hüküm içermemesi, 108 sayılı Sözleşme'nin ihdasına yol açmıştır⁴⁰. 108 sayılı Sözleşme, Avrupa Konseyi'ne üye devletlerin egemenlik sahasında kişisel verilerin korunması alanında yeknesak bir hukuk düzeni sağlamayı hedeflemektedir⁴¹. Sözleşme, Avrupa Konseyi üyesi olmayan devletlerin de imzasına açık olması⁴² ve uluslararası alanda kişisel verilerin korunması ile ilgili bağlayıcı tek metin olması nedeniyle etki bakımından büyük bir potansiyele sahiptir⁴³. Sözleşme, kişisel verilerin korunması hakkını, özel yaşamın koruması bağlamında değerlendirmektedir⁴⁴. Kamu- özel sektör ayrımı gözetmeksizin adli makamlar tarafından işlenen kişisel veriler de dâhil bu Sözleşme ile koruma altındadır⁴⁵. Ancak yalnızca otomatik yolla işlenen veriler, Sözleşme'nin korumasından yararlanmaktadır. Bu, her ne kadar Sözleşme'nin uygulama alanını sınırlamışsa da veri işleme sürecinde kısmen otomatik yöntemlere başvurulması da verileri bu Sözleşme korumasından yararlandırmaktadır⁴⁶. Öte yandan Sözleşme'nin 9. maddesine göre devletin güvenliği, kamu güvenliğinin sağlanması, devletin ekonomik menfaatlerinin korunması ve suçların önlenmesi amaçlarıyla kişisel verilerin işlenmesi halinde devletler bu halleri Sözleşme'nin kapsamı dışında bırakabilecektir. Dolayısıyla bu hükümle kişisel verilerin korunması sınırlanmaktadır.

⁴⁰ Yakovleva, **a.g.e.**, s. 485; Güray Dağ, “Kişisel Verilerin Ceza Muhakemesi Hukukunda Delil Olarak Kullanılması”, **Marmara Üniversitesi Sosyal Bilimler Enstitüsü**, Yayınlanmamış Doktora Tezi, İstanbul, 2011, s.17; Şimşek, **a.g.e.**, s. 21.

⁴¹ Başalp, **Kişisel Verilerin Korunması ve Saklanması**, s. 24.

⁴² Sözleşme'nin 23. maddesi, Konsey üyesi olmayan devletlerin, taraf devletlerin oybirliği ile Sözleşme'ye katılmasına cevaz vermiştir. Örneğin Konsey üyesi olmayan Arjantin, Burkina Faso, Cabo Verde, Mauritius, Meksika, Fas, Senegal, Tunus ve Uruguay için bağlayıcı olan bu Sözleşme'yi Türkiye 28.01.1981 yılında imzalamış, 01.09.2016 tarihinde iç hukukuna dâhil etmiştir. Türkiye'nin Sözleşme hükümlerini bu denli geç iç hukuka dâhil etme nedeni Sözleşme m. 4'ün taraf devletlere kişisel verilerin korunmasına ilişkin iç hukuk düzenlemesi yapma yükümlülüğü getirmesidir, Türkiye'de ise KVKK'nin yürürlüğünden önce bu türden bir düzenleme mevcut değildi. Ünver, “Kişisel Verilerin Korunması”, s. 189.

⁴³ Elif Küzeci, **Kişisel Verilerin Korunması**, 4. Baskı, İstanbul, On İki Levha Yayıncılık, 2020, s. 144; Bu nedenle Sözleşme, veri koruma hukukunun ana enstrümanı (*mother instrument*) olarak kabul edilmiştir. Bkz. Thomas Marquenie, “The Police and Criminal Justice Authorities Directive: Data Protection Standards and Impact on the Legal Framework”, **Computer Law and Security Review**, c. 33, 2017, s. 325.

⁴⁴ Hüseyin Murat Develioğlu, **6698 Sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku**, İstanbul, On İki Levha Yayınları, 2017, s. 9.

⁴⁵ Lauri J. Pajunoja, “The Data Protection Directive on Police Matters 2016/680 Protects Privacy-The Evolution Of EU'S Data Protection Law and Its Compatibility With The Right To Privacy”, **University of Helsinki**, Yayınlanmamış Yüksek Lisans Tezi, Helsinki, 2017, s.13; Şimşek, **a.g.e.**, s. 22.

⁴⁶ Küzeci, **a.g.e.**, s. 145-146.

Sözleşme kişisel verilerin korunması amacının yanında, taraf devletler arasında kişisel verilerin serbestçe aktarımını da hedeflemektedir. Yani genel geçer biçimde özel yaşamın gizliliğine dayanılarak veri aktarımı sınırlandırılmamalıdır. Nitekim Sözleşme'nin temel amaçları mahremiyetin korunması ve serbest veri aktarımının sağlanmasıdır. Ancak pek tabii veri koruması ihtiyacı daha ağır basmaktadır⁴⁷. Veri aktarımının istisnası m. 12/3'te öngörülmüştür. Belirli veri kategorileri için özel bir koruma mevcut ve aktarımın yapılacağı devlette bu türden eş değer bir koruma bulunmamakta ise veya aktarım Sözleşme'nin tarafı olmayan üçüncü bir devlet aracılığıyla yapılacak ise aktarım yasaklanabilir veya özel bir izne tabi tutulabilir⁴⁸.

2001 yılında kabul edilen Ek Protokol⁴⁹ ile de taraf devletlere kişisel verilerin korunmasına ilişkin bağımsız ve özerk denetleyici makam oluşturma yükümlülüğü getirilmiştir⁵⁰. Denetleyici makam araştırma ve müdahale etme yetkileri ile donatılmalıdır ve Sözleşme'de öngörülen hakların ihlal edildiği iddiası ile iç hukukun öngördüğü ulusal yargı organına da başvurma yetkisine sahip olmalıdır⁵¹. Ayrıca Ek Protokol ile yurtdışına veri aktarılması halinde kişisel verilerin korunmasında yeterli düzeye ulaşmamış devlet ya da organizasyona veri aktarımı yasaklanmıştır⁵².

Doktrinde sıklıkla 108+ olarak bilinen Kişisel Verilerin İşlenmesine İlişkin Bireylerin Korunmasına İlişkin Sözleşmede Değişiklik Yapılmasına Dair Protokol ise bilişim teknolojileri ile uyumlu bir veri koruma ihtiyacından doğmuş ve 108 sayılı Sözleşme modernize edilmiştir⁵³. 108+ ile özel nitelikli kişisel veri kategorilerine genetik ve biyometrik veriler eklenmiş ve taraf devletler, bu verilere ilişkin ayrımcılık riskine karşı güvence sağlamakla yükümlendirilmişlerdir. Ayrıca GDPR ile paralel olarak veri koruma etki analizi, ön değerlendirme yapma yükümlülüğü, veri işleme

⁴⁷ Yakovleva, **a.g.e.**, s. 485-486.

⁴⁸ Küzeci, **a.g.e.**, s. 147.

⁴⁹ 08.11.2001'de imzaya açılan 181 Sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'ne Ek Denetleyici Makamlar ve Sınır Aşan Veri Akışına İlişkin Protokol. Türkiye Ek Protokolü 08.11.2001 tarihinde imzalamış, 05.05.2016'da iç hukukuna dâhil etmiştir.

⁵⁰ Bu organın 108 sayılı Sözleşme yerine Ek protokol ile getirilmesinin, üye devletler arasındaki görüş ayrılıkları olduğu ileri sürülmüştür. Bkz. Şimşek, **a.g.e.**, s. 27.

⁵¹ Şimşek, **a.g.e.**, s. 28.

⁵² Songül Atak, "Avrupa Konseyi'nin Kişisel Veriler Açısından Sağladığı Temel Güvenceler", **TBB Dergisi**, c. 22, s. 87, 2010, s. 94.

⁵³ Dülger, **Kişisel Verilerin Korunması Hukuku**, s. 29.

yönteminde tasarımdan itibaren ve başlangıçtan itibaren veri korumasının sağlanması gibi kavramlar dâhil edilmiştir⁵⁴.

C. R(87)/5 Sayılı Polis Veri Tavsiye Kararı (1987)

108 sayılı Sözleşme, özel olarak kolluk ve adli makamlar tarafından işlenen kişisel verilerin korunmasını kapsam dışı bırakmadığından taraf devletler bu tür kişisel verileri de Sözleşme hükümlerinin korumasından yararlandırmakla yükümlüdür. Ancak Avrupa Konseyi, daha da incelikli noktalarda başvurulmak üzere yol gösterici mahiyette R(87)/5 sayılı Polis Veri Tavsiye Kararı'nı yayımlamıştır. Polis Veri Tavsiye Kararı, kişisel verilerin kolluk faaliyetleri kapsamında kullanımını düzenlemiştir.

Polis Veri Tavsiye Kararı, Avrupa Konseyi üyesi devletlere; veri sahiplerinin şüpheli/ sanık/ mağdur/ tanık vs. sıfatlarla sınıflandırılarak, verinin tutulduğu faaliyetin de adli ve idari biçimde ayrılarak kişisel verilerin muhafaza edilmesini tavsiye etmiştir⁵⁵. Karara göre iç hukuk ve uluslararası hukuk düzenlemelerine dayanılarak veya bu türden bir düzenlemenin olmaması halinde kamu güvenliğine yakın, ağır ve muhakkak bir tehdide dayanılarak ya da ağır bir suçun işlenmesinin önlenmesi için üye devletler tarafından kişisel verilerin aktarımına izin verilmiştir⁵⁶. Ayrıca uluslararası hukuk düzenlemeleri ile kastedilen yalnız cezai konularla ilgili adli yardım anlaşmaları değildir; Interpol ile yapılan işbirliği çerçevesinde de polis ve adli makamların veri paylaşımına izin verilmiştir⁵⁷.

II. AVRUPA BİRLİĞİ BAĞLAMINDA KİŞİSEL VERİLERİN KORUNMASI

⁵⁴ Aşıkoğlu, **a.g.e.**, s. 46.

⁵⁵ Gülşah Bostancı Bozbayındır, “Avrupa Birliği Ceza Hukuku’nda Polis ve Ceza Adaleti Otoritelerine Yönelik 2018/680 Sayılı Direktif: Kişisel Verilerin Ceza Adalet Mekanizmalarında Korunmasına Getirilen Standartlar ve Direktife Yönelik Eleştiriler”, **GSÜHFD**, c. 17, s. 2, 2018, s. 61.

⁵⁶ Bostancı Bozbayındır, **a.g.e.**, s. 61.

⁵⁷ Bostancı Bozbayındır, **a.g.e.**, s. 61.

AB'nin temel hedefi; malların, kişilerin, hizmetlerin ve sermayenin serbest dolaşımıdır ve bu hedefin gerçekleşmesi için kişisel verilerin işlenmesi âdeta bir zorunluluktur⁵⁸. Bu nedenle AB düzeyinde veri işlemenin birtakım kural ve ilkelere bağlanması ve işlenen kişisel verilerin korunması gerekmektedir. 108 sayılı Sözleşme varken niçin AB'nin ayrı bir korumaya ihtiyaç duyduğu düşünülebilir. 108 sayılı Sözleşme'nin 4. maddesine göre taraf devletler Sözleşme'de yer alan ilkeleri iç hukuklarına aktarmakla yükümlüdür. Ancak taraf devletlerin iç hukukları arasında tam bir yeknesaklık sağlanması, 108 sayılı Sözleşme ile hedeflenmemiştir. Oysa AB'de veri işleme ve veri koruma mevzuatı arasında bir yeknesaklık olması gerekmektedir, zira aksi durum iç pazarın işleyişine ket vurabilir⁵⁹.

Belirtilmelidir ki AB'nin kişisel verilerin korunması hakkına ilişkin düzenlemelerini, Avrupa Konseyi düzenlemelerinden ayıran temel fark, kişisel verilerin korunması hakkının özel yaşamın gizliliğine saygı hakkından bağımsız, başlı başına bir hak olarak tanınmasıdır⁶⁰.

Detaylı açıklamalardan önce AB düzeyinde veri korumaya dair genel bir çerçeve çizmek gerekirse, TFEU m. 16 ve Lizbon Anlaşması'nın yürürlüğünden sonra AB'nin üç ayaklı sütunlu yapısının⁶¹ tasfiyesi ile kişisel verilerin korunmasında yegâne temel başvuru kaynağı 95/46 sayılı Direktif olmuştur. Ancak daha kapsayıcı bir hukuki çerçevede veri koruma mekanizması ihtiyacı hasıl olmuştu. Zira 95/46 sayılı Direktif; veri işlemede veri sahibinin açık rızası veya açık kanun hükmü arayan Alman yaklaşımı, özel nitelikli verilere özel bir koruma arayan Fransız yaklaşımı ve veri sorumlusunun kayıt altına alınmasını öngören İngiliz yaklaşımı⁶² gibi AB'nin önde gelen devletlerinin yaklaşımını mezcetmenin ötesine geçememiştir. Yani 95/46 sayılı Direktif kişisel verilerin korunması hakkına ilişkin AB düzeyinde yeknesaklığı sağlayamamıştır. Bu nedenle AB Veri Koruma Reformu⁶³ kapsamında GDPR ile

⁵⁸ Başalp, **Kişisel Verilerin Korunması ve Saklanması**, s. 25.

⁵⁹ Küzeci, **a.g.e.**, s. 184.

⁶⁰ Develioğlu, **a.g.e.**, s. 11.

⁶¹ İç piyasa faaliyetleri kapsamında kişisel verilerin korunması birinci sütunda olup 95/46 sayılı Direktif'e tabi iken; üçüncü sütunda olan polis ve adli işbirliğine ilişkin kişisel verilerin korunması ise 2008/977/JHA çerçeve kararına tabiydi.

⁶² Gür, **a.g.e.**, s. 26.

⁶³ 2018 yılı Mayıs ayı "AB'de Veri Korumada Yeni Bir Çağ" olarak bilinen yeni dönemin başlangıcı olmuş ve bu tarihte GDPR, Kolluk ve Ceza Adaleti Direktifi ve PNR Direktifi yürürlüğe girmiştir. Bkz.

kişisel verilerin işlenmesinde temel amaç ve ilkeler ortaya konulmuş, Kolluk ve Ceza Adaleti Direktifi ile de kişisel verilerin korunması ve işlenmesinde adli makamlar ve ulusal cezai süreçler arasında işbirliğine olanak sağlanmıştır.

AB üyesi pek çok devlette kolluk ve adli makamlar tarafından işlenen kişisel veriler, genel kişisel veri korumasından ayrı tutulmuştur ve bunlar GDPR koruması dışındadır. Örneğin Hollanda’da Polis Veri Kanunu (*Wet politiegegevens/WPG*) suçlu, şüpheli, tanık ve diğer kişilerin polis tarafından işlenen kişisel verilerine uygulanmaktadır. Adalet ve Ceza Muhakemesi Veri Kanunu (*Wet justitiële en strafvorderlijke gegevens/WJSG*) ise savcılık ve mahkemeler tarafından işlenen kişisel veriler ve tüzel kişilerle ilgili verilere uygulanmakta ve verilerin ne kadar süre muhafaza edileceğini düzenlemektedir. Ayrıca WJSG uyarınca kişisel veriler davranış sertifikalarının değerlendirilmesi için işlenebilir⁶⁴. WJSG hakkında daha fazla ayrıntı sağlayan adalet ve ceza muhakemesi verileri hakkında bir kararname de bulunmaktadır. Hem WPG hem de WJSG, Hollanda veri koruma otoritesi tarafından denetlenmektedir. Her iki kanun da açıkça bu alanlarda GDPR’ın korumasını hariç tutmuştur⁶⁵.

A. 95/46 Sayılı Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Direktifi (1995)

Kişisel verilerin korunmasına ilişkin AB’nin 95/46 sayılı Direktif’i; kişisel verilerin serbest dolaşımını sağlamak ve bu sayede AB düzeyinde kişisel veri koruma standardı yakalayarak üye devletler arasında ortak pazar ve ekonomik menfaatlerin de korunmasını hedeflemekteydi⁶⁶. Zira 95/46 sayılı Direktif’ten önce AB düzeyinde

Avrupa Komisyonu, “A New Era for Data Protection in the EU What Changes After May 2018”, Çevrimiçi https://ec.europa.eu/info/sites/info/files/data-protection-factsheet-changes_en.pdf 19.03.2020.

⁶⁴ Davranış sertifikası (*verklaring omtrent gedrag-vog*), kişinin geçmiş davranışının belirli bir görevi veya işi gerçekleştirmesine engel teşkil etmediğini gösteren bir belgedir. Bkz. Çevrimiçi <https://www.netherlandsworldwide.nl/living-working/applying-for-consular-declarations/certificate-of-conduct-vog> 13.03.2020.

⁶⁵ Bart Custers, Alan M. Sears, Francien Dechesne, Ilina Georgieva, Tommaso Tani, Simone van der Hof, **EU Personal Data Protection in Policy and Practice**, The Hague, Springer, 2019, s. 34-35.

⁶⁶ Cemil Kaya, **Assessing the Transfer of Personal Data in the European Union in the Light of the Data Protection Directive**, İstanbul, On İki Levha Yayınevi, 2011, s. 4-5. Ancak bu dengeyi kurmak

ortak bir veri koruma standardı bulunmayıp devletler, veri cenneti olarak tabir edilebilecek düşük veri koruma düzeyine sahip devletlerde veri işleme faaliyetlerini yürütmekteydi⁶⁷. 95/46 sayılı Direktif'in hedeflediği koruma esas olarak kişisel verilerin korunması saldırılarına karşı önleyici mahiyette bir korumadır⁶⁸.

95/46 sayılı Direktif'in ihdasından sonra ABAD, içtihatları ile veri koruma hukukuna dikkatleri çekmiştir. Divan'ın kişisel verilere ilişkin içtihatları genel olarak tanım içtihatları (*definition cases*) ve dengeleme içtihatları (*balancing cases*) olarak ayrılabilir. *Lindqvist*⁶⁹, *Breyer*⁷⁰, *Digital Rights Ireland*⁷¹ gibi tanım içtihatlarında 95/46 sayılı Direktif'in bazı maddeleri ve kavramlarının yorumlanması sağlanırken, *Google Spain*⁷² ve *Bavarian Lager*⁷³ gibi dengeleme içtihatlarında ise kişisel verilerin korunması hakkı ve bu hakla yarışan diğer hak ve özgürlükler arasında dengenin gözetilmesine ilişkin kriterler geliştirilmiştir⁷⁴.

95/46 sayılı Direktif, 108 sayılı Sözleşme'nin aksine yalnız otomatik vasıtalarla işlenen verileri değil, manuel işlenen verileri de koruma kapsamına almıştır. Manuel işlenen kişisel veriler, yapısal olarak bir dosyalama işleminin parçasını

kolay olmamaktadır. Kişisel verilerin serbest dolaşımında, kişisel verilerin korunması ve veri akışının sağlanması gibi yarışan iki menfaat söz konusu olmaktadır. Veri koruması tam olarak sağlanmak isteniyorsa AB düzeyinde kişisel verilerin de serbest dolaşımına imkân sağlayan veri aktarımı tamamen yasaklanmalıdır. Ancak günümüzde bireylerin ve çok uluslu şirketlerin, piyasaların etkin şekilde faaliyetlerini gerçekleştirebilmeleri için veri aktarımına muhtaç oldukları izahtan varestedir. Öte yandan veri koruma hedefinden vazgeçmek de mahremiyet hakkı gözetildiğinde imkânsızdır. Olması gereken, küresel ticaretin gerçekleşmesi için veri aktarımının mahremiyet gözetilerek sağlanması yani bu iki menfaat arasında dengeyi sağlamaktır. 95/46 sayılı Direktif'in çıkış noktası da sonraki tüm uluslararası ve ulusal veri koruma mevzuatlarında olduğu gibi budur; Dağ, **a.g.e.**, s. 52; Gür, **a.g.e.**, s. 24.

⁶⁷ Örneğin Almanya'da şirketlerin veri işleme faaliyetlerinde veri koruma sorumlusu atamak gerekli iken İtalya'da 95/46 sayılı Direktif'ten önce veri koruma kanunu mevcut değildi. Pek çok şirket de veri cenneti olan İtalya'da faaliyet sürdürmekteydi. Bkz. Başalp, **Kişisel Verilerin Korunması ve Saklanması**, s. 29.

⁶⁸ Başalp, **Kişisel Verilerin Korunması ve Saklanması**, s. 31.

⁶⁹ *Bodil Lindqvist v Åklagarkammaren i Jönköping* Başvurusu, B. No: C-101/01, 06.11.2003 Çevrimiçi https://curia.europa.eu/jcms/jcms/j_6/en/ 29.03.2020.

⁷⁰ *Patrick Breyer v. Bundesrepublik Deutschland* Başvurusu, B. No: C-582/14, 19.10.2016 Çevrimiçi https://curia.europa.eu/jcms/jcms/j_6/en/ 29.03.2020.

⁷¹ *Schrems Digital Rights İrlanda Ltd.* Başvurusu [BD], B. No: C-362/14, 06.10.2015 Çevrimiçi https://curia.europa.eu/jcms/jcms/j_6/en/ 29.03.2020.

⁷² *Google Spain v AEPD ve Mario Costeja González* Başvurusu, B. No: C-131/12, 13.05.2014 Çevrimiçi https://curia.europa.eu/jcms/jcms/j_6/en/ 29.03.2020.

⁷³ *The Bavarian Lager Co. Ltd* Başvurusu, B. No: C-28/08, 29.06.2010 Çevrimiçi https://curia.europa.eu/jcms/jcms/j_6/en/ 29.03.2020.

⁷⁴ Susanna Lindroos-Hovinheimo, "Who Controls Our Data? The Legal Reasoning of the European Court of Justice in Wirtschaftsakademie Schleswig-Holstein and Tietosuojavaltuutettu v Jehovan Todistajat", **Information and Communications Technology Law**, c. 28, s. 2, 2019, s. 228-229.

oluşturuyorsa bu halde 95/46 sayılı Direktif uygulanacaktır⁷⁵. Ayrıca 95/46 sayılı Direktif kişisel verilerin korunması hakkının etkin şekilde korunması ve alanın aktüelitesini de gözeterek ulusal denetleyici makamların oluşturulması gerektiğini belirtmiş ve aynı zamanda WP29’u oluşturmuştur. WP29, AB üyesi devletlere ve Avrupa Komisyonu’na tavsiyelerde bulunarak kişisel verilerin korunmasına ilişkin AB düzeyinde yeknesaklığı sağlamaya çalışmıştır⁷⁶. Ayrıca WP29, AB düzeyinde kişisel verilere sağlanan korumayı zedeleyen devletleri ve hukuki düzenlemeler arasındaki farklılıkları belirleyerek Komisyon’a bilgi verme görevi de üstlenmiştir⁷⁷.

95/46 sayılı Direktif’in AB Antlaşması 6. başlığı altında düzenlenmiş *Adli Konularda Polis ve Adli İşbirliğine İlişkin Hükümler* ve gerçek kişilerin kişisel ve aile içi yaşamlarında gerçekleştirilen veri işlemler bakımından zorlayıcılığı bulunmamaktadır⁷⁸. Nitekim AB’nin veri koruma düzenlemelerinde söz konusu kolluk faaliyetleri olduğunda bu, ulusal hukuk düzenlemelerine bırakılmaktadır⁷⁹. Ayrıca Direktif’in Europol ve Schengen Antlaşmaları’nın uygulanmasında da etkisi bulunmamaktadır. Yine Direktif, havayolu şirketlerinin yolcu bilgilerini ABD’nin yetkili mercileri ile paylaşması⁸⁰ konusunda da bir düzenleme getirmemektedir. Zira yolcuların kişisel verilerinin işlenmesi, her ne kadar ulusal güvenliğin sağlanması amacına dayansa da başka amaçlarla da kullanılabilir. Ayrıca yolcu bilgilerinin aktarılması somut bir terör olayı ile mücadele olmayıp olasılık üzerinden bir veri

⁷⁵ Bkz. 95/46 sayılı Direktif m. 3/1; Dosyalamadan anlaşılacak olan, kişisel verilerin bir dosyada yer alması ve veriye erişimin organize edilmiş olmasıdır. Organize edilmekten kasıt da verilerin alfabetik yahut kronolojik olarak sıralanmasıdır. Bkz. Başalp, **Kişisel Verilerin Korunması ve Saklanması**, s. 33.

⁷⁶ Develioğlu, **a.g.e.**, s. 11; Direktif’in, üye devletlerin iç hukukunda yeknesaklık sağlamayı değil, üye devletlerin veri koruma mevzuatı arasında uyum yakalamayı hedefleyip devletlere tanınan “manevra alanı” ile bu uyumun, iç hukuk düzenlemelerinde gerçekleşeceğine dair bkz. Kaya, **Assessing the Transfer of Personal Data in the European Union in the Light of the Data Protection Directive**, s. 11.

⁷⁷ Şimşek, **a.g.e.**, s. 51.

⁷⁸ 95/46 sayılı Direktif m. 3/2.

⁷⁹ Francesca Bignami, “Protecting Privacy Against the Police in the European Union: The Data Retention Directive”, **Duke Law School Faculty Scholarship Series**, paper 76, 2007, Çevrimiçi http://lsr.nellco.org/duke_fs/76 23.03.2020, s. 5.

⁸⁰ 11 Eylül saldırıları sonrası ABD’de ulusal güvenlik nedeniyle yapılan hukuki düzenlemelerden biri de bu husustur. Sivil uçakların kullanıldığı terör saldırılarında havayolu taşımacılığında güvenlik ihtiyacı artmıştır. ABD’de *The Aviation and Transportation Security Act* yürürlüğe girmiştir. Buna göre çıkış ya da varış yeri ABD olan ya da transfer yeri ABD olan uçuşlarda havayolu taşıma şirketleri, ABD makamlarına yolcuların kişisel bilgilerini iletecektir. PNR denen bu kayıtlarda yer alan yolcunun uyuğu, sağlık durumu, dini inancı, yemek tercihi gibi pek çok veriye ABD makamları ulaşabilmektedir. Bkz. Küzeci, **a.g.e.**, s. 205.

toplamaktır⁸¹ ve 95/46 sayılı Direktif bu konuda özel bir düzenlemeye sahip değildir. 95/46 sayılı Direktif, GDPR’ın ihdası ile yürürlükten kalkmıştır.

B. Avrupa Birliği Temel Haklar Şartı (2000)

Kişisel verilerin korunması hakkı, Avrupa Birliği Temel Haklar Şartı m. 8 ile yalnız AB kurum ve organlarında değil; aynı zamanda özel yaşamın gizliliğine saygı hakkının sınırlarını aşarak tüm AB üyesi devletlerde başlı başına temel bir hak olarak tanınmıştır⁸². Şart’ın 8. maddesine göre;

“Herkes, kendisine ilişkin kişisel verilerinin korunmasını isteme hakkına sahiptir.

Bu tür veriler, belirtilen amaçlar için ve ilgili kişinin muvafakatine veya yasa da öngörülen başka meşru temele dayalı olarak adil şekilde kullanılmalıdır. Herkes, kendisi hakkında toplanmış olan verilere erişme ve bunlarda düzeltme yaptırma hakkına sahiptir.

Bu kurallara uyulması, bağımsız bir makam tarafından denetlenecektir.”⁸³

Lizbon Antlaşması’nın yürürlüğü sonrası Temel Haklar Şartı hukuken bağlayıcı hale gelmiştir. Ancak Şart’ın hukuken bağlayıcı olmadığı dönemde dahi ABAD, kişisel verilerin korunması hakkını *Promusicae*⁸⁴ kararında tanımıştır⁸⁵. Şart’ın kişisel verilerin korunması hakkı bakımından önemi; özel yaşamın gizliliğinden bağımsız ve ayrı kişisel verilerin korunması hakkını tanıması ve AB üyesi devletlere anayasaları bakımından bir nevi yol göstermesidir⁸⁶.

⁸¹ Küzeci, **a.g.e.**, s. 208.

⁸² Zira Şart’ın ihdasından önce kişisel verilerin korunması hakkını Avrupa Toplulukları Mahkemesi, AİHS ile paralel olarak içtihat yoluyla tanımıştır. Bkz. Başalp, **Kişisel Verilerin Korunması ve Saklanması**, s. 26.

⁸³ Çevrimiçi

http://www.sbb.gov.tr/wp-content/uploads/2018/11/Avrupa_Birligi_Temel_Haklar_Sarti%E2%80%8B.pdf 05.03.2020.

⁸⁴ *Productores de Música de España (Promusicae) v Telefónica de España SAU* [BD], B. No: C-275/06, 29.01.2008, para. 64 Çevrimiçi https://curia.europa.eu/jcms/jcms/j_6/en/ 29.03.2020.

⁸⁵ Pajunoja, **a.g.e.**, s. 37.

⁸⁶ Küzeci, **a.g.e.**, s. 182.

C. 2002/58/AT Sayılı Elektronik İletişim Alanında Özel Yaşamın Gizliliğinin Korunması ve Kişisel Verinin İşlenmesine İlişkin Direktif (2002)

2002/58 sayılı Direktif, 95/46 sayılı Direktif'in tamamlayıcısı olup kişisel verilerin korunmasında temel ilkeler ve kurallar bakımından 95/46 sayılı Direktif'e atıf yapmıştır. 95/46 sayılı Direktif'ten farklı olarak yalnızca elektronik iletişim sektörü için ek koruyucu düzenlemelere yer vermiştir⁸⁷. Direktif'in uygulama alanı, kamusal ulaşılabilir iletişim hizmetlerinden ibaret olup tüm elektronik iletişim ağ ve hizmetleri, internet hizmet sağlayıcıları ve hizmet sunucularını kapsamaktadır⁸⁸. Direktif bağlamında iletişimin gizliliği daha çok özel hukuk ilişkisi çerçevesinde telekomünikasyon sektörüne ilişkindir⁸⁹. İletişim ağının güvenilirliğine ilişkin bir riskin bulunması halinde elektronik haberleşme sağlayıcısı, abonelere riski ve önlemleri bildirmekle yükümlüdür. Direktif'in korumasından yalnız gerçek kişiler değil, tüzel kişiler de yararlanmaktadır⁹⁰. Üye devletler mobil telefon, kısa mesaj, telefon hattı, e-posta gibi tüm araçlardan yapılan iletişimin trafik ve yer verilerini tespit edebilecek mevzuata sahip olacaktır. Direktif uyarınca trafik ve yer verisi işleme, ulusal güvenlik, kamu güvenliği, terörizmle ve diğer suçlulukla mücadele gibi gerekçelere dayanabilecektir⁹¹.

D. 2006/24/AT Sayılı İletişim Trafik Verilerinin Saklanması Direktifi (2006)

⁸⁷ Dülger, **Kişisel Verilerin Korunması Hukuku**, s. 36; Ayşe Çiğdem Ayözger, **Kişisel Verilerin Korunması**, İstanbul, Beta Yayıncılık, 2016, s. 137; Başalp, **Kişisel Verilerin Korunması ve Saklanması**, s. 27.

⁸⁸ Yüksel, **a.g.e.**, s. 99; Şimşek, **a.g.e.**, s. 57.

⁸⁹ Yüksel, **a.g.e.**, s. 99.

⁹⁰ Bkz. 2002/58 sayılı Direktif m. 1/2; ABAD ve AB düzeyinde kişisel verilerin korunması hakkında tüzel kişiler yararlanmamaktadır. Ancak AİHS m. 8 korumasından tüzel kişiler de istifade edebilmektedir. Bkz. Kokott, Sobotta, **a.g.e.**, s.225; *Bernh Larsen Holding ve diğerleri v Norveç*, B. No: 24117/08, 14.03.2013, para. 159 Çevrimiçi <https://hudoc.echr.coe.int/> 29.03.2020.

⁹¹ Küzeci, **a.g.e.**, s. 212; Pajunoja, **a.g.e.**, s. 21.

2006/24 sayılı Direktif⁹², suçların önlenmesi, soruşturulması, tespiti ve kovuşturulması amaçlarıyla hizmet sunucuları tarafından kişisel verilerin saklanması ilişkin AB üyesi devletlere mevzuat oluşturma yükümlülüğü yüklemiştir⁹³. Zira elektronik haberleşme ile elde edilen bu veriler soruşturma ve kovuşturmanın yürütülmesi için bir hayli önemli olup delil olarak kullanılabilecektir. 2006/24 sayılı Direktif'e göre hizmet sağlayıcıları, iletişim verilerini 6-24 ay boyunca tutmakla yükümlüdürler.

Verilerin saklanmasıdaki amaç; ciddi suçların araştırılması, soruşturulması ve kovuşturulmasıdır⁹⁴. Ancak Direktif kapsamında ciddi suçtan ne anlaşılması gerektiği müphemdir ve ciddi suçlara dayanarak devletlere, kişilerin bir suç işlediğine dair delil olmaksızın kişisel verileri tutmak için yetki verilmesi eleştiriye açıktır⁹⁵.

2006/24 sayılı Direktif kapsamında internet bağlantısı, telefon görüşmesi, kısa mesaj gönderimi yapılan kişinin adı, abone veya kayıtlı kullanıcının adı ve adresi, IP adresi, iletişimin kaynağı, mobil iletişimin yeri, iletişimin gerçekleştiği tarih ve saat, iletişim süresi ve sıklığı kayıt altına alınmaktadır⁹⁶. Ancak iletişimin içeriğine ilişkin kayıt yapılması, 2006/24 sayılı Direktif kapsamında mümkün değildir.

Kişinin iletişim ve trafik verilerinin kaydedilmesi, suç işlendiğine ilişkin somut bir belirti olmasa da gerçekleştiğinden masumiyet karinesi ve özel yaşamın gizliliğine saygı ile bağdaştırılamamıştır⁹⁷. Ayrıca verilerin saklanması kamu düzenine dayandırılmışken özel teşebbüs olan hizmet sağlayıcılarının da veri saklayabilmesi eleştirilmiştir⁹⁸. Nitekim ABAD, bu Direktif'i yürürlükten kaldırmıştır⁹⁹.

⁹² 2006/24 sayılı bu Direktif'in tam adı, "Halka Açık Elektronik İletişim Hizmetlerinin Veya Kamu İletişim Ağlarının Sağlanmasıyla Bağlantılı Olarak Üretilen veya İşlenen ve 2002/58/EC Sayılı Direktif'te Değişiklik Yapan 15 Mart 2006 Tarihli 2006/24 Sayılı Avrupa Parlamentosu ve Konseyi Direktifi"dir. Metin için bkz. Çevrimiçi <https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:32006L0024> 08.02.2020.

⁹³ 2006/24 Direktif resital m. 5.

⁹⁴ Pajunoja, **a.g.e.**, s. 21; Bignami, **a.g.e.**, s. 6.

⁹⁵ Aynı görüşte bkz. Dülger, **Kişisel Verilerin Korunması Hukuku**, s. 37; Dağ, **a.g.e.**, s. 57.

⁹⁶ Küzeci, **a.g.e.**, s. 217; Şimşek, **a.g.e.**, s. 66.

⁹⁷ Küzeci, **a.g.e.**, s. 218.

⁹⁸ Küzeci, **a.g.e.**, s. 218.

⁹⁹ Bkz. *Digital Rights Ireland ve Seitlinger ve diğerleri* [BD], B. No: C-293/12 ve C-594/12, 08.04.2014 Çevrimiçi https://curia.europa.eu/jcms/jcms/j_6/en/ 29.03.2020.

E. 2008/977/JHA Sayılı Çerçeve Karar (2008)

Cezai konularda adli makamların işlediği kişisel veriler 95/46 sayılı Direktif'in uygulama alanından hariç tutulduğundan, bu eksikliği gidermek için 2008/977 sayılı Çerçeve Karar yayımlanmıştır¹⁰⁰. Lizbon Antlaşması ile birlikte Avrupa Komisyonu, hem özel sektörde hem kamu sektöründe polis ve adli konularla ilgili kişisel verilerin işlenmesi ve korunmasında ortak kuralların ve mevzuatın oluşturulması çalışmalarına başlamıştır¹⁰¹. 2008/977 sayılı Çerçeve Karar'ın ihdas amacını Komisyon, Avrupa ve ABD'de gerçekleşen küresel terör eylemleri ile mücadele olarak belirtmiştir¹⁰². 2008/977 sayılı Çerçeve Karar, cezai konularda üye devletler arasında işbirliğini sağlamak için aktarılan veya üye devletler arasında hâlihazırda aktarılmış verilere uygulanmaktadır.

2008/977 sayılı Çerçeve Karar, normatif uyumlaştırılmayı sağlamayı devletlerin takdir yetkisine bıraktığından yani devletlerin gönüllüğü esasına dayandığından farklı iç hukuk uygulamalarına zemin hazırlamıştır¹⁰³. Çerçeve Karar; yalnız sınır ötesi veri aktarımına uygulanabilir durumda olup ilkelere neredeyse gönüllü olarak başvurulabilmektedir ki bu da kolluk ve adli makamların işlediği kişisel verilerin çok küçük bir alanını korumuş olmaktadır¹⁰⁴. Ayrıca ulusal güvenlik söz konusu olduğunda veri işleme faaliyeti Çerçeve Karar kapsamı dışında kalmaktadır¹⁰⁵. Bu nedenle bilgi, erişim ve düzeltme gibi bireysel haklar ve verilerin güvenlik nedeniyle işlenmesi arasında bir denge kurulamamıştır.

Sonuç olarak adli faaliyetler kapsamında kişisel veri işleyen yerel makamlar kapsam dışı bırakıldığı için 2008/977 sayılı Çerçeve Karar'ın etkisi dardır. Ayrıca AB ve ABD arasındaki PNR Anlaşması'na etkide bulunması beklenmekle birlikte,

¹⁰⁰ Bostancı Bozbayındır, **a.g.e.**, s. 64.

¹⁰¹ Y.Y., **Exchange of Information and Data Protection in Cross-Border Criminal Proceedings in Europe**, Ed: Angeles Gutierrez Zarra, Berlin, Springer, 2015, s. 4.

¹⁰² Murat Volkan Dülger, Onur Özkan, "Adli ve Kolluk Teşkilatında Kişisel Verilerin Korunması: 'Unutulan' Direktifin Kapsamlı ve Karşılaştırmalı Analizi", **CHD**, c. 15, s. 42, 2020, s. 94.

¹⁰³ TEU m. 249 gereği çerçeve kararlar, üye devletlerin iç hukuk düzenlemelerini yakınlaştırmayı amaçlamakta ve çerçeve kararda değinilen konuda şekil ve yöntemi üye devletlerin iç hukukuna bırakmaktadır ve de doğrudan etkiye sahip değildir. Dülger, Özkan, **a.g.e.**, s. 95; Gür, **a.g.e.**, s. 86.

¹⁰⁴ Marquenie, **a.g.e.**, s. 326.

¹⁰⁵ Pajunoja, **a.g.e.**, s. 22.

Çerçeve Karar üye devletler veya AB'nin üçüncü ülkelerle yaptığı ikili yahut çok taraflı anlaşmalardan kaynaklanan yükümlülükler ve taahhütlere uygulanmamaktadır. Yani Çerçeve Karar; Schengen Bilgi Sistemi, Europol ve Eurojust'ın faaliyetlerinde kullandıkları veri tabanlarını ve veri koruma kurallarını kapsamı dışında tutmuştur. Nitekim belirtilen eksiklikler nedeniyle Çerçeve Karar, Kolluk ve Ceza Adaleti Direktifi'nin ihdası ile yürürlükten kalkmıştır.

F. Avrupa Birliği'nin İşleyişi Hakkında Antlaşma (2012)

TFEU m. 16'da da kişisel verilerin korunması hakkı tanınmıştır. Maddeye göre;

“Herkes, kendisiyle ilgili kişisel verilerin korunması hakkına sahiptir.

Avrupa Parlamentosu ve Konsey, Birlik hukuku kapsamına giren faaliyetlerin yürütülmesinde, Birlik kurum, organ, ofis veya ajansları ile üye devletler tarafından kişisel verilerin işlenmesi sırasında bireylerin korunmasına ve bu bilgilerin serbest dolaşımına ilişkin kuralları olağan yasama usulü uyarınca belirler. Bu kurallara uyulması, bağımsız otoritelerin denetimine tabidir.

*Bu maddeye dayanarak kabul edilen kurallar, Avrupa Birliği Antlaşması'nın 39. maddesinde yer alan spesifik kurallara hâlel getirmez.”*¹⁰⁶

G. 2016/679 Sayılı Genel Veri Koruma Tüzüğü (2018)

Bilgisayar sistemlerinin gelişmesi sonucu bilişim araçları vasıtasıyla kişisel verilerin depolanması, işlenmesi ve eşleştirilmesi bir hayli kolaylaşmıştır. Özellikle akıllı bilgisayar, telefon, sosyal medya, bulut bilişimi gibi araç ve yöntemler ile bilgi ve teknolojiye çığır açılmış olup veri gözetimine bir tepki olarak kişisel verilerin

¹⁰⁶ Çevrimiçi <https://www.ab.gov.tr/files/pub/antlasmalar.pdf> 18.02.2020.

korunması için 95/46 sayılı Direktif'in ötesinde bilgi ve teknoloji çağı ile uyumlu bir hukuki çerçeveye ihtiyaç duyulmuştur¹⁰⁷.

AB'de kişisel verilerin korunması konusunda 108 sayılı Sözleşme ve direktifler bulunsa da devletler arasında farklı uygulamalar mevcuttu. Üye devletlerde veri korumanın parçalı yapısı ve bunun sonucunda ortaya çıkan yasal belirsizlikler, AB düzeyinde ekonomik faaliyetlerin işlemesine engel olmakta ve rekabetin bozulmasına yol açmaktaydı¹⁰⁸. Bu da Veri Koruma Reformu'nu gerektirmekteydi. Ayrıca Snowden Krizi de AB Veri Koruma Reformu'nu hızlandırmıştır¹⁰⁹. Belirtilen nedenlerle AB düzeyinde genel ve ticari kişisel verilerin korunmasında yeknesaklığı sağlamak üzere GDPR ihdas edilmiştir. Ancak suçların önlenmesi, soruşturulması, ortaya çıkarılması, kovuşturulması ve cezaların infazında kişisel veri işleme hallerinde GDPR'ın uygulama alanı bulmayacağı düzenlenmiştir.

GDPR; unutulma hakkı, veri taşınabilirliği hakkı, veri koruma etki değerlendirmesi, tasarımdan itibaren veri koruması, kişisel verilere usulsüz şekilde ulaşılması halini bilme hakkı, tutarlılık ve Avrupa Birliği Veri Koruma Otoriteleri arasında tek bir kaynaktan ulaşılabilir mekanizmaları (*one-stop-shop mechanisms*) ile var olan veri koruma düzenlemelerinden ayrılmıştır¹¹⁰. GDPR ayrıca veri koruma

¹⁰⁷ Aleksandar Skendzic, Bozidar Kovacic, Edvard Tijan, "General Data Protection Regulation-Protection Of Personal Data In An Organisation", **41st International Convention on Information and Communication Technology**, Electronics and Microelectronics, Opatija, 2018, s. 1372; Marquenie, **a.g.e.**, s. 327; Ketizmen, **a.g.e.**, s. 189-192; Nilgün Başalp, "Avrupa Birliği Veri Koruması Genel Regülasyonu'nun Temel Yenilikleri", **MÜHF-HAD**, c.21, s.1, 2015, s. 82.

¹⁰⁸ GDPR resital m. 9.

¹⁰⁹ Başalp, "Avrupa Birliği Veri Koruması Genel Regülasyonu'nun Temel Yenilikleri", s. 85.

¹¹⁰ Mutlu, **a.g.e.**, s.100 vd.; Custers, Sears, Dechesne, Georgieva, Tani, van der Hof, **a.g.e.**, s. 1-2; Skendzic, Kovacic, Tijan, **a.g.e.**, s. 1372-1373; Paul De Hert, Vagelis Papakonstantinou, "The New Police and Criminal Justice Data Protection Directive: A First Analysis", **New Journal of European Criminal Law**, c. 7, s. 1, Tilburg, 2016, s. 7; Yeniliklerin detaylı değerlendirmesi için bkz. Dülger, **Kişisel Verilerin Korunması Hukuku**, s. 42-44; 95/46 sayılı Direktif ile kıyaslandığında GDPR; birey merkezci anlayışı, bürokrasiyi devre dışı bırakması, coğrafi olarak daha geniş bir uygulama alanı sunması gibi nedenlerle veri koruma alanının "Kopernik Devrimi" olarak nitelendirilmiştir. Bkz. Tamer Soysal, "Unutulma Hakkının Avrupa Birliği'nin Genel Veri Koruma Tüzüğü Çerçevesinde İncelenmesi", **Uyuşmazlık Mahkemesi Dergisi**, Yıl 7, s. 13, Haziran 2019, s. 359; Ancak GDPR'ın bu denli yenilikçi yaklaşımı AB düzeyinde kişisel verilerin korunmasının ABD'deki gibi kişisel verilerin mülkiyet hakkı korumasından yararlandırılmasına benzetildiği biçiminde yorumlanmıştır. Bkz. Develioğlu, **a.g.e.**, s. 13; Ancak bu yenilikçi anlayış, en azından Kolluk ve Ceza Adaleti Direktifi bağlamında kişisel verilerin mülkiyet hakkı korumasından yararlandırılması biçiminde değildir, zira verilerin kişinin önleyici kolluk faaliyetleri, ceza muhakemesi sürecinde ve infaz aşamasında gündeme gelebilecek kişisel verileri o denli hassas niteliğe sahiptir ki en azından bu veriler bakımından kişilik hakkı korumasından yararlanılması ve bu haktan vazgeçilemeyeceği benimsenmelidir.

görevlisi belirleme zorunluluğu da getirmiştir. Veri işleme mahkemelerin yargısal faaliyetleri haricinde gerçekleşiyorsa, veri sorumlusu veya veri işleyenin faaliyeti işin mahiyeti itibariyle veri sahibinin büyük ölçekte izlenmesini gerektiriyorsa veya bu büyük ölçekte izlenmesi gereken veriler özel nitelikli veri ise bu durumda veri koruma görevlisi belirlenmesi gerekmektedir¹¹¹.

GDPR’ın getirdiği yeniliklerin yanı sıra AB sınırlarını aşan bir düzenleme olması da önemlidir. Zira m. 3’e göre AB sınırları dâhilinde mukim veri sorumlusu ve veri işleyen, faaliyet alanı gözetilmeksizin GDPR düzenlemelerine tabi olacaktır. Veri sorumlusu ve işleyen, AB içinde mukim olmasa dahi AB’deki bireylerin verilerinin işlenmesi halinde yine GDPR hükümlerine tabidir.

¹¹¹ Küzeci, **a.g.e.**, s. 306; Skendzic, Kovacic, Tijan, **a.g.e.**, s. 1373.

III. KOLLUK VE CEZA ADALETİ DİREKTİFİ

A. Kolluk ve Ceza Adaleti Direktifi'nin Ortaya Çıkışı

Kolluk ve Ceza Adaleti Direktifi'nden önce polis ve ceza adaleti faaliyetlerinde işlenen kişisel verilere ilişkin etraflıca bir koruma öngören düzenleme bulunmamaktaydı. Ancak özellikle 11 Eylül sonrası terörizmle mücadelede ABD başta olmak üzere devletlerin yürüttüğü önleyici ve koruyucu tedbir faaliyetleri kapsamında ulusal güvenlik lehine kişi hak ve özgürlüklerini sınırlayan düzenlemeler, mahremiyet hakkına da müdahale oluşturmıştır. Özellikle PNR ve Swift gibi verilerin terörle mücadelede kullanımı, kişisel verilerin korunmasına ilişkin düzenleme yapma ihtiyacı doğurmuştur¹¹².

Polis ve ceza adaletinin spesifik karakteri gereği bu alanda veri işlemenin önemli bir rolü bulunmaktadır ve genel veri işlemeye göre kamu güvenliği ilgili konularda işleme belirli bir düzeyde esneklik gerektirmektedir¹¹³. Örneğin tezin ilerleyen kısımlarında açıklayacağımız veri işlemede amaçla bağlılık ilkesi, katı bir şekilde uygulanamaz. Zira belirli bir amaç için toplanan verinin başka bir zaman diliminde beklenmedik bir amaç için kullanılması da mümkündür. Yahut bilgilendirilme ve erişim hakkı eğer çok geniş bir şekilde tanınırsa bu, bir suç şüphesi ile yapılan soruşturmayı etkisiz kılabilir. Nihayetinde kamu güvenliği ile ilgili özel ihtiyaçların, veri koruma düzenlemelerinin hazırlanması sırasında gözetilmesi gerekir; şüphesiz veri koruma amaçları ile güvenlik politikası hedefleri arasında bir denge kurma görevi de hassas ve zordur¹¹⁴.

Kolluk ve Ceza Adaleti Direktifi'nin ihdas amacı, 2008/977 sayılı Çerçeve Karar'daki kişisel verilerin korunması ilkelerini iç hukukta kolluk ve adli makamların veri işleme faaliyetlerine genişletmektir¹¹⁵. Kolluk ve Ceza Adaleti Direktifi, Çerçeve

¹¹² Gür, **a.g.e.**, s. 185.

¹¹³ De Hert, Papakonstantinou, **a.g.e.**, s. 9.

¹¹⁴ De Hert, Papakonstantinou, **a.g.e.**, s. 9.

¹¹⁵ Pajunoja, **a.g.e.**, s. 29.

Karar'ın kapsam darlığının aksine¹¹⁶ ülke sınırları ve sınır ötesi ayrımı yapmaksızın polis ve ceza adaleti bağlamındaki kişisel verilerin işlenmesini düzenlemektedir¹¹⁷. Böylece Çerçeve Karar'ın en büyük sınırlamalarından biri elimine edilmiştir. AB üyesi devletlerin güvenlikle ilgili makamlarının¹¹⁸ kişisel veri işleme faaliyetlerini Kolluk ve Ceza Adaleti Direktifi hükümleriyle uyumlu hale getirmesi gerekmektedir¹¹⁹. Ancak tüm AB düzeyinde bunun yapılması, üye ülkelerin teknoloji bakımından yeterlilik düzeylerinin farklı olması ve kolluk faaliyetlerinde yeni teknolojilerin kullanılması nedeniyle güçtür. Bu güçlük nedeniyle de AB üyesi ülkeler arasında veri işlemede farklılık düzeyi genişlemektedir¹²⁰. Ancak esas olarak Kolluk ve Ceza Adaleti Direktifi'nin ihdas amacı bu farklılık düzeyini asgariye çekmektir.

Kolluk ve Ceza Adaleti Direktifi m. 63'e göre üye devletler 6 Mayıs 2018'e kadar Kolluk ve Ceza Adaleti Direktifi hükümlerini iç hukuklarına aktarmakla yükümlü idi. Ancak Avusturya ve Almanya hariç diğer devletler bu tarihe uymamıştır. Gecikmelerden bağımsız olarak bazı üye ülkeler aynı çabayı göstermemiştir, zira bunların bazıları ceza hukukunda kişisel verilerin işlenmesi için hâlihazırda yürürlükte olan mevzuatlara sahip iken bazı ülkelerde ise bu alanda hiç mevzuat bulunmamaktaydı. Örneğin İsveç'te 1998 tarihli Polis Veri Koruma Kanunu polisin kişisel verileri nasıl işleyebileceğini düzenlemekteydi. Bu Kanun'a göre polis aynı zamanda sabıka kayıtları ve DNA verilerini tutma yetkisine de sahipti. 2012'de yeni olarak Polis Veri Koruma Kanunu yürürlüğe girmiştir. Fransa'da ise 2014 yılından bu yana Fransız polisi ve istihbarat teşkilatlarına mahkeme emri olmadan veri toplama da dâhil olmak üzere soruşturma yetkileri veren bir kanun mevcuttur. Romanya'da 21/2002 sayılı Polis Kanunu ve 238/2009 sayılı ceza hukukunda kişisel verilerin işlenmesine ilişkin olan Kanun'da kişisel verilere ilişkin hükümler bulunmaktadır¹²¹.

¹¹⁶ Bkz. "2008/977/JHA Çerçeve Karar" başlıklı bölüm.

¹¹⁷ Bilişim ve Teknoloji Hukuku Enstitüsü, **a.g.e.**, s.2; Bostancı Bozbayındır, **a.g.e.**, s. 67. Çek Cumhuriyeti ileri sürdüğü çekince ile ulusal düzeydeki veri işleme faaliyetlerini kapsam dışı bırakmış ve Direktif'in uygulama alanının sınır ötesi kişisel veri işleme faaliyetleri ile sınırlamıştır.

¹¹⁸ Bkz. Kolluk ve Ceza Adaleti Direktifi m. 3/7.

¹¹⁹ De Hert, Papakonstantinou, **a.g.e.**, s. 10.

¹²⁰ De Hert, Papakonstantinou, **a.g.e.**, s. 10.

¹²¹ Ancak Romanya 7 Ocak 2019'da 363/2018 sayılı Kanun ile Kolluk ve Ceza Adaleti Direktifi'nde öngörülen hususları iç hukukuna aktarmıştır. Böylece 238/2009 sayılı Kanun ilga edilmiştir. 7 Şubat 2019 tarihinden sonra Kanun'un öngördüğü düzenlemeler ile bağdaşmayan fiiller için Romanya Veri Koruma Otoritesi 21,350 Euro'ya kadar para cezası uygulayabilecektir. Bkz. Sergiu Drăgoianu, Daniel Alexie, "Romania Transposes Directive (EU) 2016/680", Çevrimiçi

İtalya’da da ceza soruşturması genel mevzuatı ve GDPR haricinde ceza hukukunda kişisel verilerin korunması için özel kanun veya düzenlemeler bulunmamaktadır¹²².

Suçların önlenmesi, soruşturulması, ortaya çıkarılması, kovuşturulması ve cezaların infazı amaçları ile yetkili olan makamların (kişi bakımından sınırlama) bu amaçlarla yürüttükleri veri işleme faaliyetlerine (madde bakımından sınırlama) Kolluk ve Ceza Adaleti Direktifi uygulanacaktır¹²³. Ancak suç tanımına Direktif’te yer verilmemiştir. Direktif resitalinde suçun ABAD tarafından yorumlanan otonom bir kavram olduğu belirtilmiştir¹²⁴. Üye devletlerin iç hukuklarında suç ve kabahat ayrımı mevcutsa kabahatlere de Kolluk ve Ceza Adaleti Direktifi’nin uygulanıp uygulanmayacağı metinden anlaşılmamaktadır. Suç kavramının ABAD tarafından yorumlanacağı belirtildiğinden suçun karşılığı olarak belirlenen yaptırım, ABAD ve AİHM içtihatları dikkate alınarak değerlendirilmelidir. *Engel ve diğerleri v. Hollanda* başvurusunda AİHM, m. 6 kapsamında cezai yaptırımı belirlerken birtakım kriterler geliştirmiştir. Taraf devletlerin iç hukukuna göre suçun tasnifi, suçun doğası ve ilgili kişinin maruz kalabileceği cezanın niteliği ve şiddet derecesi dikkate alınacaktır¹²⁵. Nitekim ABAD da fiili suç ya da kabahat olarak nitelendirirken AİHM kriterlerini esas almaktadır¹²⁶.

Kolluk ve Ceza Adaleti Direktifi’nin temel amacı; kişisel verilerin korunması için AB genelinde polis ve ceza adaleti bağlamındaki kişisel veri işlemeyi yasaklamak olmayıp, bilakis adli faaliyetlerde kişisel verilerin güçlü şekilde korunmasını sağlamak ve bu tür verilerin üye devletler arasında serbest dolaşımını kolaylaştırmaktır¹²⁷. Bunun haricinde Kolluk ve Ceza Adaleti Direktifi’nin ihdas amaçları arasında; bilişim sistemleri vasıtasıyla işlenen suçların artışı, suçlarla ilgili yürütülen ceza

<https://www.lexology.com/library/detail.aspx?g=719b914a-d5af-478b-a5a6-2b96c2b01ec3>
30.03.2020.

¹²² Custers, Sears, Dechesne, Georgieva, Tani, van der Hof, **a.g.e.**, s. 219-220.

¹²³ Sajfert, Quintel, **a.g.e.**, s. 3.

¹²⁴ Kolluk ve Ceza Adaleti Direktifi resital m. 13; Resitalin bu maddesinin kaçınılmaz bir sonucu olarak AB düzeyinde veri koruma kurallarında yeknesaklığın sağlanamayacağı ileri sürülmüştür. Sajfert, Quintel, **a.g.e.**, s. 4.

¹²⁵ *Engel ve diğerleri v. Hollanda*, B. No: 5100/71; 5101/71; 5102/71; 5354/72; 5370/72, 08.06.1976, para. 82 Çevrimiçi <https://hudoc.echr.coe.int/> 29.03.2020.

¹²⁶ Bkz. *Bonda* [BD], B. No: C-489/10, 05.06.2012, para. 37; *Akeberg Fransson* [BD], B. No: C-617/10, 26.02.2013 para. 35 Çevrimiçi https://curia.europa.eu/jcms/jcms/j_6/en/ 29.03.2020.

¹²⁷ Dülger, Özkan, **a.g.e.**, s. 91; De Hert, Papakonstantinou, **a.g.e.**, s. 11.

muhakemesinde dijital ve teknolojik yeni araçlara başvurulması ve tüm bu gelişmelere karşın eski düzenlemelerin uyumlaştırma ve icra edilebilirliğinin zayıf olması ile mücadele gösterilebilir¹²⁸.

Adli makamların fonksiyonlarını icra edebilmesi için GDPR’da yer alan bazı ilke ve haklar, Kolluk ve Ceza Adaleti Direktifi’nde bulunmamaktadır. Zira bunların bulunması halinde ceza adalet faaliyetleri ciddi bir biçimde sekteye uğrayabilecektir. Söz gelimi kişisel verilere erişim hakkı, Kolluk ve Ceza Adaleti Direktifi’nde GDPR ile aynı koruma düzeyinde tanınsaydı, soruşturmanın gizliliği ilkesi zedelenecek olup şüphelinin kaçması ya da delil karartması konusunda daha yüksek bir risk doğacaktı. Ayrıca GDPR’da kişisel verilerin işlenmesi için veri sahibinin açık rızası aranmakta iken Kolluk ve Ceza Adaleti Direktifi kapsamındaki kişisel verilerin işlenmesi için kanunda bu yönde düzenleme olması gerekmektedir. Temel hak ve özgürlüklere müdahalede kanunilik ilkesi gereği devletler Kolluk ve Ceza Adaleti Direktifi kapsamında gündeme gelecek kişisel verilerin işlenme amacını, türlerini, hedeflerini ulusal mevzuatlarında belirtmelidirler¹²⁹. Suçların önlenmesi, soruşturulması, ortaya çıkarılması, kovuşturulması ve cezaların infazında kamu yararı mevcuttur ve veri işleme faaliyetlerinde veri sahibinin rızasına hukuki sonuç bağlanmamıştır¹³⁰. Ancak bazı üye ülke kanunlarında Kolluk ve Ceza Adaleti Direktifi kapsamındaki bir faaliyette veri sahibinin rızasına hukuki sonuç bağlanmıştır. Örneğin, Kolluk ve Ceza Adaleti Direktifi, soruşturmada DNA testi yapılması ya da cezaların infazında elektronik etiket vasıtasıyla yer bildirme gibi durumlarda kişisel verilerin işlenmesinde veri sahibinin muvafakatının aranmasına da cevaz vermektedir¹³¹.

Kolluk ve Ceza Adaleti Direktifi’nde kişisel verilerin işlenmesine ilişkin şüpheli, sanık, tanık ve mağdur gibi farklı veri sahipleri öngörülerek düzenlemeler

¹²⁸ Dülger, Özkan, **a.g.e.**, s. 87-88.

¹²⁹ Bilişim ve Teknoloji Hukuku Enstitüsü, **a.g.e.**, s. 9.

¹³⁰ Bkz. Mark Leiser, “Directive 2016/680 Personal Data in Law Enforcement”, **Introduction of The Data Protection Reform to The Judicial System Inform**, Çevrimiçi <https://www.universiteitleiden.nl/binaries/content/assets/rechtsgeleerdheid/instituut-voor-metajuridica/inform-project/leiser-inform-workshop.pdf> 13.03.2020, s. 8.

¹³¹ Bostancı Bozbayındır, **a.g.e.**, s. 80; Elektronik etiket, hapis cezasına alternatif olarak kişinin genellikle ayağına takılan bir cihazın sinyali vasıtasıyla bulunduğu yerin infaz makamlarınca bilinmesine olanak sağlayan bir infaz yöntemidir. Detaylı bilgi için bkz. “Elektronik İzleme” başlıklı bölüm.

yapılması gerektiği belirtilmiştir¹³². Veri sahipleri arasında böyle bir ayırım gözetilmesi Kolluk ve Ceza Adaleti Direktifi ile gelen bir yeniliktir. Bu biçimde veri sahipleri arasında yapılacak tasnifin organizasyonel olarak kolaylık sağlayacağı şüphesizdir. Ancak farklı veri sahipleri arasında yapılan bu ayırımı masumiyet karinesi gözetilmelidir¹³³.

Ayrıca Kolluk ve Ceza Adaleti Direktifi olgulara dayalı olan kişisel veriler ile kişisel değerlendirmelere dayalı olan kişisel veriler arasında ayırım yapılmasını öngörmüştür¹³⁴. Kişisel değerlendirmeye dayalı olan kişisel verilerin doğruluğu, olgulara dayalı olan verilere nazaran daha tartışmalı ve düşüktür. Bu nedenle veri türleri arasında böyle bir ayırım yapılması isabetlidir¹³⁵. Yanlış, eksik, güncel olmayan bir kişisel verinin aktarılması ve erişilebilir olmamasını yetkili makamlar sağlamalıdır. Veri aktarımı halinde, alıcıya verinin doğru, güncel ve tam olduğuna ilişkin gerekli bilgiler de iletilmelidir¹³⁶.

Kolluk ve Ceza Adaleti Direktifi ile amaç, kolluk güçlerinin faaliyetleri ile kişisel verilerin korunması arasındaki dengeyi kurmaktır¹³⁷. Yani Kolluk ve Ceza Adaleti Direktifi bir yandan özel yaşamın gizliliğine saygı hakkı sınırlarını aşar şekilde ceza muhakemesi ve önleyici faaliyetlerde işlenebilecek kişisel verilerin korunmasını öngörmekte; diğer yandan bu minvalde kişisel verilerin yetkili makamlar arasında paylaşımının, gerçek kişilerin korunması gibi basmakalıp gerekçelere dayanmasını engelleyerek veri aktarımının kolaylaşmasını sağlamaya çalışmaktadır¹³⁸.

Kolluk ve Ceza Adaleti Direktifi'nin birinci bölümü genel hükümler, ikinci bölümü kişisel veri işlemede genel ilkeler, üçüncü bölümü veri sahibinin hakları, dördüncü bölümü veri sorumlusu, veri işleyen ve bu sükelerın yükümlölükleri, beşinci bölümü verilerin üçüncü ölke veya uluslararası organizasyonlara aktarımı, altıncı

¹³² Detaylı bilgi için bkz. "Veri Sahibi" başlıklı bölüm.

¹³³ Kızılırmak, "Kişisel Verilerin İşlenmesinde Adli ve Önleyici Amaçla Öngörölün İstisnaların Ulusal ve Uluslararası Hukuka Göre Değerlendirilmesi", s. 245.

¹³⁴ Kolluk ve Ceza Adaleti Direktifi m. 7/1.

¹³⁵ İbrahim Korkmaz, **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, Güncellenmiş 2. Baskı, Ankara, Seçkin Yayıncılık, 2019, s. 244.

¹³⁶ Kolluk ve Ceza Adaleti Direktifi m. 7/2.

¹³⁷ Küzeci, **a.g.e.**, s. 226.

¹³⁸ Bilişim ve Teknoloji Hukuku Enstitüsü, **a.g.e.**, s. 2.

bölümü denetleyici makam, yedinci bölümü AB üyesi devletler arasında işbirliği, sekizinci bölümü yargı yolları, sorumluluk ve ceza, dokuzuncu bölümü uygulama hükümleri ve nihayet onuncu bölümü nihai hükümler olmak üzere Direktif toplam on bölümden oluşmaktadır.

B. Kolluk ve Ceza Adaleti Direktifi-GDPR İlişkisi

Genel kişisel veri korumasını AB'nin neden bir tüzük ile sağlamaya çalıştığı değerlendirilmelidir. AB hukukunun kaynakları birincil ve ikincil hukuk kaynakları olarak ayrılmaktadır. AB topluluğunu kuran ve değiştiren antlaşmalar birincil hukuk kaynakları, kurucu antlaşmalarda öngörülen usullerle yapılan ve AB organlarıncı kendilerine tanınan yetki çerçevesinde oluşturulan düzenlemeler ise ikincil hukuk kaynaklarını oluşturmaktadır. Tüzük ve direktifler de ikincil hukuk kaynaklarındandır¹³⁹.

AB hukukunda TFEU m. 288'e göre tüzükler yayımlandıkları andan itibaren üye devletlerin onayı, iç hukuklarına aktarmaları gerekmeksizin doğrudan bağlayıcı¹⁴⁰ ve etkilidir¹⁴¹. Tüzüklerin bu etkisi ile uluslararası hukuktaki normun iç hukuka aktarılması şeklinde düalist yapıdaki uzun ve hantal sürecin önüne geçilmektedir¹⁴². Üye devletler, tüzük hükümlerini ulusal çıkarlarına uygun geldiği biçimde tam ve mutlak olarak uygulamakla yükümlüdür¹⁴³. Direktifler ise Avrupa Birliği'nin

¹³⁹ Diğer ikincil hukuk kaynakları ise kararlar ve tavsiyelerdir. Kararların muhatabının tüm üye devletler olması gerekli olmayıp belirli bir üye devlet, gerçek ya da tüzel kişi olabilir. Kararlar muhatapları yönünden bağlayıcı olup iç hukuka aktarmak gerekmez. Tavsiyeler ise bağlayıcı olmayan kaynaklardır. Bkz. Başalp, **Kişisel Verilerin Korunması ve Saklanması**, s. 28.

¹⁴⁰ AB Komisyonu, sektör bazında hareket ederek Schengen vize uygulaması ve tarımda AB sübvansiyonlarını konu alan düzenlemeleri tüzük ile yapma yoluna gitmiştir. Bu bakımdan GDPR bir tüzük olduğundan etki sahası oldukça geniş ve dikkate değerdir. Bkz. Başalp, "Avrupa Birliği Veri Koruması Genel Regülasyonu'nun Temel Yenilikleri", s. 84.

¹⁴¹ Doğrudan etkili olma, harici kaynaktan gelen hukuk kuralının AB üyesi devletlerin hukuk sisteminde kendiliğinden, sisteme devletin kendi kurallarıymışçasına dâhil olabilmesi ve uygulanması manasına gelmektedir. Geniş anlamıyla doğrudan etki, AB hukukunun bir normunun ulusal mahkemeler önünde ileri sürülmesi iken dar anlamıyla doğrudan etki ise bireylerin ulusal mahkemeler önünde ileri sürebilecekleri bireysel haklar sağlanmasıdır. Detaylı bilgi için bkz. Paul Craig, Grainne de Burca, **EU Law Text Cases and Materials**, 5. Baskı, New York, Oxford University Press, 2011, s. 105; Işıl Özkan, **Avrupa Birliği Kamu Hukuku**, Ankara, Seçkin Yayıncılık, 2011, s. 116-117; İlke Göçmen, **Avrupa Birliği Hukukunda Direktiflerin Bireyler Arasındaki İlişkilere Etkileri**, Ankara, Yetkin Yayınları, 2008, s. 81-82.

¹⁴² Craig, de Burca, **a.g.e.**, s. 105

¹⁴³ Göçmen, **a.g.e.**, s. 36.

amaçlarını gerçekleştirmek için mevzuat yaklaştırmaları ve uyumluluğunu sağlayan topluluk tasarruflarındandır ve genellikle hükümlerinin izin verdiği kapsam ve alan dâhilinde ulusal çeşitliliğe cevaz veren düzenlemelerdir. Üye devletler, belirli konularda yapacakları düzenlemeleri tüzük ya da direktif ile düzenleme konusunda serbesttir¹⁴⁴. Bireylere haklar tanıyan bir direktif hükmünün, AB üyesi devlet vatandaşları tarafından iç hukukta ileri sürülebilmesi için direktifin iç hukuka aktarılması gerekmektedir¹⁴⁵. Direktifler üye devletler için doğrudan bağlayıcı olmayıp hükümlerinin üye devletlerin iç hukukuna aktarılması gerektiğinden, örneğin 95/46 sayılı Direktif yalnız yol gösterici mahiyete sahiptir. Kişisel verilerin korunması amacıyla yapılan düzenlemenin direktif yerine tüzük ile yapılması üye devletler arasındaki uygulamalarda standardizasyonu sağlaması ve dijital ortak pazar stratejisinin işletilmesi bakımından önemlidir¹⁴⁶.

Genel kişisel veri koruması GDPR gibi bir tüzükle yapılırken suçların önlenmesi, soruşturulması, ortaya çıkarılması, kovuşturulması ve cezaların infazı faaliyetlerinde işlenen kişisel verilerin niçin bir direktif ile koruma altına alındığı da değerlendirilmelidir. AB üyesi devletler arasında cezai meselelerde işbirliğine ciddi katkı sağlayacak kişisel veri işlenmesi ve aktarımının; doğrudan bağlayıcı olmayan bir form ile korunması, verilerin kullanım amacından kaynaklanmaktadır. Polis ve ceza adaleti faaliyetlerinde veri işlemenin genel düzenleme olan GDPR yerine Kolluk ve Ceza Adaleti Direktifi ile düzenlenmesi bu alanın mahiyetinin sonucudur¹⁴⁷. Zira veriler suçların önlenmesi, ceza muhakemesi ve cezaların infazı amacıyla işlenecek ve aktarılacaktır. Doktrinde AB düzeyinde cezai meselelerde yapılacak işbirliğinin minimum harmonizasyon içinde yapılması önerilmiştir¹⁴⁸. Yani bu öneriye göre cezai meselelerde veri aktarımı yapılırken AB düzeyinde standart kurallardansa AİHS referansları ve uluslararası hukuk enstümanları ile harmonizasyon sağlanmalıdır.

¹⁴⁴ Göçmen, **a.g.e.**, s. 37.

¹⁴⁵ Enver Bozkurt, Arif Köktaş, **Avrupa Birliği Hukuku**, Güncellenmiş 7. Baskı, Ankara, Legem Yayıncılık, 2018, s. 187.

¹⁴⁶ Develioğlu, **a.g.e.**, s. 12.

¹⁴⁷ Kişisel verilerin GDPR yerine Direktif ile korunmasının; alanın daha fazla sınırlamaya tabi tutulmak istenmesi veya işin niteliği ile ilgili olmayıp ayrı bir hukuki düzenleme ile korunmak istediği ileri sürülmüştür. Bkz. Mutlu, **a.g.e.**, s. 110.

¹⁴⁸ Bozkurt, Köktaş, **a.g.e.**, s. 379.

AB üyesi devletler, direktiflerin sağlamak istediği hedefleri gerçekleştirirken iç hukuk düzenlemelerinde takdir marjına sahiptirler. Yani üye devletlerin direktiflerde belirlenen ilke ve kurallarla uyumlu düzenlemeler ihdas etmesi veya hâlihazırdaki mevzuatı revize etmesi gerekmektedir¹⁴⁹. Direktifler de üye devletlerin iç hukuklarını yaklaştırmak amacıyla ihdas edilirler¹⁵⁰. Yani iç hukuka aktarılmaksızın direktifler bağlayıcı olmamaktadır. Direktifler ancak ulaşmak istedikleri hedefler bakımından bağlayıcıdır¹⁵¹. Katmanlı yetki ilkesince (*principle of subsidiarity*)¹⁵² üye devletler, direktifte öngörülen kuralları iç hukuklarına aktarmaksızın direktifler doğrudan uygulanmayacaktır¹⁵³. Ancak genel kuralların belirlendiği direktif hükümlerine göre ulusal mevzuatta düzenlemeler yapılacaktır¹⁵⁴. Bu ulusal düzenlemeler hukuken bağlayıcı olmalı, hukuk güvenliği ve açıklık ilkeleri gözetilmelidir¹⁵⁵. Üye devletlerin direktif hükümlerini iç hukuklarına aktarmaması halinde TFEU m. 258 gereği devlet, antlaşmalardan doğan yükümlülüklerini yerine getirmediği gerekçesiyle ihlal davasının muhatabı olabilir¹⁵⁶. Kolluk ve Ceza Adaleti Direktifi'nden önce yalnızca çerçeve niteliğinde bir düzenleme varken, Kolluk ve Ceza Adaleti Direktifi ile AB düzeyinde direktif ile de olsa uyum sağlamak amaçlanmıştır¹⁵⁷.

¹⁴⁹ Küzeci, **a.g.e.**, s. 352; Bostancı Bozbayındır, **a.g.e.**, s. 69.

¹⁵⁰ Ahmet M. Güneş, **Avrupa Birliği Hukukuna Giriş**, 2. Baskı, İstanbul, On İki Levha Yayıncılık, 2016, s. 148; Craig, de Burca, **a.g.e.**, s. 106; Özkan, **a.g.e.**, s. 117.

¹⁵¹ Güneş, **a.g.e.**, s. 148; Özkan, **a.g.e.**, s. 117.

¹⁵² Katmanlı yetki ilkesi, AB ile üye devletler arasında yetkilerin kullanımını düzenleyen ve AB Anlaşması m. 5'te bulunan bir ilkedir. İlkenin amacı, Birliğin federalist eğilimini azaltmaktır. Bu ilke uyarınca, münhasır yetkisine girmeyen alanlarda AB, ancak öngörülen eylemin amaçlarının üye devletler tarafından gerektiği şekilde gerçekleştirilemeyeceği ve söz konusu eylemin boyutları ve etkileri itibarıyla kendisi tarafından daha iyi yerine getirilebileceği durumlarda harekete geçebilmektedir. Aksi takdirde söz konusu eylem; ulusal, bölgesel veya yerel düzeyde, üye devletler tarafından gerçekleştirilmektedir. Katmanlı yetki ilkesi terimi için, "yetki ikamesi", "ikincillik", "yerindenlik" gibi terimler de kullanılmaktadır. Lizbon Antlaşması'nın yürürlüğünden sonra ilke, TEU m. 5/3-4 ve Katmanlı Yetki ve Orantılılık İlkelerinin Uygulanması Hakkında Protokol'de düzenlenmiştir. Ancak Protokol'e yalnız hukuki düzenleme taslaklarında danışmak amacıyla başvurulacaktır. Detaylı bilgi için bkz. AB Sözlüğü, Çevrimiçi <http://ekutup.dpt.gov.tr/ab/sozluk.pdf> Çevrimiçi 02.09.2019; Bart van der Sloot, "Legal Consistency After the General Data Protection Regulation and the Police Directive", **European Journal of Law and Technology**, c. 9, s. 3, 2018, s. 8; Craig, de Burca, **a.g.e.**, s. 94; Özkan, **a.g.e.**, s. 117.

¹⁵³ Dülger, **Kişisel Verilerin Korunması Hukuku**, s. 33.

¹⁵⁴ Dülger, **Kişisel Verilerin Korunması Hukuku**, s. 35.

¹⁵⁵ Güneş, **a.g.e.**, s. 150.

¹⁵⁶ Güneş, **a.g.e.**, s. 152.

¹⁵⁷ Başalp, "Avrupa Birliği Veri Koruması Genel Regülasyonu'nun Temel Yenilikleri", s. 84.

Genel olarak bakıldığında Kolluk ve Ceza Adaleti Direktifi; risk temelli yaklaşımı, özel yaşamın ve kişisel verilerin korunması başta olmak üzere temel hak ve özgürlüklerin korunması için yeterli önlemlerin alınması gibi temel ilkeler ve veri koruma etki değerlendirmesi, veri koruma görevlisi, tasarımdan itibaren veri korunması ve başlangıçtan itibaren veri korunması gibi müesseseleri ile GDPR ile uyumludur¹⁵⁸. GDPR, AB veri koruma hukuku bakımından *lex generalis* olup yalnız polis ve ceza adaleti faaliyetleri kapsamında olan kişisel verilerin korunmasını hedefleyen Kolluk ve Ceza Adaleti Direktifi ise *lex specialis*’tir¹⁵⁹. Söz gelimi ülke sınırlarına yetkili izinleri sağlamaksızın giren kişinin fiilinin suç olarak düzenlendiği devletlerde, kolluk makamlarının bu fiilleri tespit etmek ve suçu önlemek için yürüttüğü kişisel veri işleme faaliyetlerinde Kolluk ve Ceza Adaleti Direktifi uygulanırken, göç hareketleri, iltica başvurularında işlenen kişisel verilerin korunması için ise *lex generalis* olan GDPR uygulanacaktır¹⁶⁰.

Kolluk makamlarının yetkilerini kullanırken ceza muhakemesi mevzuatı gereği mi idare hukuku mevzuatı gereği mi hareket ettiğini tespit bazen güç olabilmektedir. Tespitin bir sonucu olarak veri işleme faaliyetine Kolluk ve Ceza Adaleti Direktifi hükümlerinin uygulanıp uygulanmayacağı belirlenecektir. Bu güçlük pek tabidir ki üye devletlerin iç hukuk düzenlemelerine bakılarak aşılabilir. Ancak adli ve idari kolluk ayrımının bulunmadığı devletlerde, kişisel verilerin hangi düzenlemelere¹⁶¹ göre korunacağına ve amaçla bağlılık ilkesine rağmen önleyici ya da bastırıcı faaliyetler için bu verilerin kullanılıp kullanılamayacağının tespitine ilişkin güçlük devam etmektedir.

¹⁵⁸ Bilişim ve Teknoloji Hukuku Enstitüsü, **a.g.e.**, s. 1.

¹⁵⁹ Dülger, Özkan, **a.g.e.**, s. 97; Custers, Sears, Dechesne, Georgieva, Tani, van der Hof, **a.g.e.**, s. 217.

¹⁶⁰ Catherine Jasserand-Breeman, “Reprocessing of Biometric Data for Law Enforcement Purposes: Individuals’ Safeguards Caught at the Interface between the GDPR and the Police Directive?”, University of Groningen, **Yayımlanmamış Doktora Tezi**, Groningen, 2019, s. 25.

¹⁶¹ Kolluğun önleyici ya da bastırıcı faaliyette bulunurken elde ettiği bir kişisel verinin, baştaki amaç haricinde bir diğer önleyici ya da bastırıcı faaliyette kullanılıp kullanılamayacağı, kişisel verilerin işlenmesinde amaçla bağlılık ilkesi karşısında incelikli bir husustur. Ancak bazı ülkeler iç hukuklarında açık bir düzenlemeye sahiptirler. Örneğin Baden-Württemberg Polis Kanunu’na göre amaç değişikliğinin bulunması halinde hukuka uygun şekilde verinin kullanılabileceği haller mevcuttur (BWPöG 37-38). Buna göre sadece önleme amacıyla işlenmiş kişisel verinin, ceza muhakemesi faaliyeti sırasında kullanılması ancak StPO’da hüküm olması halinde mümkündür. Bkz. Zeynep Bayram, “Kolluğun Suç Öncesi ve Sonrası Kişisel Veri Toplama Yetkisi”, **Bahçeşehir Üniversitesi Sosyal Bilimler Enstitüsü**, Yayımlanmamış Yüksek Lisans Tezi, İstanbul, 2009, s. 14.

Kolluğun hangi faaliyeti kapsamında hareket ettiğinin bilincinde olmayarak veri işlediği hallerde ve gösteri, spor müsabakası gibi hallerde kamu düzeninin korunması amacıyla veri işlediği hallerde, Kolluk ve Ceza Adaleti Direktifi'nin uygulama alanı bulacağı görüşü ileri sürülmüştür¹⁶². Kanaatimizce de bu yorum isabetlidir. Zira Kolluk ve Ceza Adaleti Direktifi'nin resitalinde de spor müsabakası gibi büyük çaplı spor etkinliklerinde veya ayaklanmalarda kamu güvenliğini sağlamak için kolluk makamlarının hareket ettiği hallerin de Direktif'in koruması kapsamında olduğu belirtilmiştir ki bu haller de esasen suç işlenmesinin önlenmesine ilişkin faaliyetlerdendir. Ancak kolluğun söz gelimi halk sağlığı ya da kamunun ekonomik menfaatlerini korumak için hareket ettiği bir halde kişisel veri işlemesi durumunda, bu kişisel verilere sağlanacak koruma GDPR'a tabi olacaktır. Bir diğer örnek olarak kolluk makamlarının sınır kontrolleri veya göç hareketlerinde kimlik tespiti faaliyeti değerlendirilebilir. Schengen sınırını geçen bir kimsenin kimlik tespiti yapılırken gerçekleşen veri işlemede, düzensiz sınır geçişi o ülkenin iç hukukuna göre suç olarak düzenlenmişse Kolluk ve Ceza Adaleti Direktifi uygulama alanı bulacaktır. Ancak sınır geçen bu kimsenin fiilinin suç olmaması halinde iltica işlemleri için kolluk tarafından yapılan veri işleme faaliyetine GDPR uygulanacaktır¹⁶³.

Suçların önlenmesi, ceza muhakemesi ya da cezaların infazında Kolluk ve Ceza Adaleti Direktifi'ne uygun olarak işlenen kişisel verilerin kamu yararı, bilimsel veya tarihi araştırma amaçlarıyla veya istatistiki amaçlarla arşivlenmesi halinde artık bu veriler, Kolluk ve Ceza Adaleti Direktifi'nin kapsamında korunmayacak ve lex generalis olan GDPR'ın korumasından yararlanacaktır¹⁶⁴. Kolluk ve Ceza Adaleti Direktifi'ne göre işlenen kişisel verinin arşivlenmesi durumunda esasen veri sahibinin rızasına dayanmayan bir ikinci işleme vardır ve bu arşivleme ise suç önleme, ceza muhakemesi veya cezanın infazı amacına hizmet etmemektedir. Dolayısıyla bu ikinci işlemenin GDPR'a tabi tutulması veri sahibine de daha geniş haklar tanınmasına imkân sağlamaktadır.

¹⁶² Dülger, Özkan, **a.g.e.**, s. 89.

¹⁶³ Sajfert, Quintel, **a.g.e.**, s. 3; Leiser, **a.g.e.**, s. 5.

¹⁶⁴ Kolluk ve Ceza Adaleti Direktifi m. 9/2.

Kişisel verilerin kısmen veya tamamen otomatik araçlarla ya da manuel olarak işlenmesi Kolluk ve Ceza Adaleti Direktifi'nin uygulanmasında farklılık göstermemektedir. Ancak manuel olarak işlenen kişisel veriler, bir dosyalama sisteminin parçası olmalıdır ya da verilerin dosyalama sisteminin parçası olması amacıyla tutulması gerekmektedir. Resital m. 18'de belirtildiği üzere dosyalama için verilerin elektronik ortamda tutulması da gerekmemektedir. Ancak manuel yolla işlenen verinin bir dosyalama sisteminin parçası olarak kabul edilebilmesi için belgelerin numara, veri sahibinin sıfatı veya suç tipine göre tasnif edilmesi gerekir. Bu tasnif kriterleri sınırlı sayıda değildir, ancak tasnifte bir sistematüğün gözetildiğine ilişkin kriterler bulunmalıdır. Bu türden bir dosyalama işlemi yoksa; söz gelimi polisin kişiyi durdurup önleme araması yaptığı olayda, Kolluk ve Ceza Adaleti Direktifi uygulama alanı bulmayacağı gibi¹⁶⁵ dosyalama sistemi bulunmadığı için GDPR da uygulama alanı bulmayacaktır.

C. Kolluk ve Ceza Adaleti Direktifi'nin Kapsamına Dâhil Olmayan Veri İşleme Faaliyetleri

1. Tamamen Kişisel veya Ev İçi Faaliyetler Gereği Veri İşlemeler

Bir gerçek kişi tarafından tamamen kişisel veya ev içi faaliyetler (*purely personal or household activity*) esnasında işlenen kişisel veriler, 95/46 sayılı Direktif ve GDPR'ın koruma alanı dışında tutulmuştur¹⁶⁶. Kolluk ve Ceza Adaleti Direktifi'nde ise böyle bir hüküm bulunmamaktadır.

Kanaatimizce Kolluk ve Ceza Adaleti Direktifi'nin kapsamının çizildiği maddede bu faaliyetlerin kapsam haricinde tutulmaması bilinçli bir tercihtir. Zira Kolluk ve Ceza Adaleti Direktifi'ne göre veri işleme; suç önleme, ceza muhakemesi ve infaz faaliyetleri çerçevesinde gerçekleşmektedir. Tamamen kişisel ve ev içi faaliyet gereği işlenen kişisel verilere, her nasılsa suç önleme, ceza muhakemesi ve

¹⁶⁵ Bostancı Bozbayındır, **a.g.e.**, s. 74.

¹⁶⁶ Bkz. 95/46 sayılı Direktif m. 3/2, GDPR m. 2/2-c.

infaz faaliyetlerini yerine getiren yetkili makamlarca ulaşılmışsa bu durum makamın faaliyetine göre değerlendirilmelidir.

Öncelikle ev içi faaliyet için kişinin günlüğüne kaydettiği kişisel verilerden ceza muhakemesinde yararlanılabilecek midir? Kişinin yaşadıklarını aktardığı bir günlük veya anı defterinde yazdıkları, onun giz alanına dâhildir ve bunun sadece açıklanması değil, içeriğinin hukuka aykırı biçimde öğrenilmesi kişisel verilerin korunması hakkı ve özel yaşamın gizliliğine saygı hakkı ile bağdaşmamaktadır¹⁶⁷. Türk hukukunda CMK uyarınca hukuka uygun bir arama ve elkoyma kararının bulunması halinde bu günlüğe elkonulması ve içindeki kişisel verilerden yararlanılması mümkün olacaktır. Ayrıca tamamen kişisel veya ev içi faaliyet çerçevesinde işlenen veri kolluk veya adli makamlarla paylaşıldığında veya alenileştirildiğinde Kolluk ve Ceza Adaleti Direktifi uygulama alanı bulmalıdır¹⁶⁸. Örneğin TCK m. 226/4 minvalinde bir düzenlemenin mevcut olduğu bir devlette doğal olmayan yollarla cinsel ilişkide bulunmuş bir kişi, bu ana dair fotoğraf ve videolar çekmiştir. Tamamen kişisel amaçla, kendi şahsi fantazileri için kişisel veri olarak fotoğrafını kaydeden bu kimse, kaydettiği görüntüleri sosyal medya üzerinden paylaştığında artık kişisel veri tamamen kişisel faaliyet çerçevesinde kalmamaktadır ve bu veri ceza muhakemesinde kullanılabilecektir.

Ancak veri işlemenin hiçbir safhasında söz konusu kolluk veya adli makamlar devreye girmemişse kişinin salt kendisi için günlük tutması halinde veri işleme faaliyeti Kolluk ve Ceza Adaleti Direktifi'nin uygulama alanına girmeyecektir. Zira suç işlendiği şüphesinin bulunmadığı hallerde bireylerin tamamen kişisel ve özel çıkarlarına ilişkin alanlarının kolluk veya adli makamlar ile bir ilgisi yoktur. Kamu düzeni ile de bir ilgisi yoktur ve bu haller, totaliter olmayan rejimlerde kolluğun müdahale edemeyeceği

¹⁶⁷ Dağ, **a.g.e.**, s. 80.

¹⁶⁸ Nitekim KVKK'de de tamamen ev içi veya kişisel faaliyet için işlenen verilerin paylaşılması veya alenileştirilmesi halinde KVKK'nin uygulama alanı bulacağı ifade edilmiştir. Bkz. Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi**, Çevrimiçi <https://www.kvkk.gov.tr/Icerik/4197/Kisisel-Verilerin-Korunmasi-Kanununa-Iliskin-Uygulama-Rehberi> 16.03.2020, s. 41.

alandadır¹⁶⁹. Bu nedenle kolluk ya da adli makamların veri işleme faaliyetleri kapsamı haricindedir.

Ayrıca tamamen kişisel ve ev içi faaliyet kavramı da dar yorumlanmamalıdır. *Tietosuojaualtuutettu v Jehovan Todistajat* başvurusunda¹⁷⁰ Yehova Şahitleri topluluğuna mensup kişiler kapı kapı dolaşarak misyonerlik faaliyetinde bulunmaktadır. Ayrıca misyonerler tarafından artık ziyaret edilmek istemeyen kişilerin adları da toplulukça listelenip derlenmektedir. ABAD, topluluğun vaazları sırasında, topluluk üyelerince toplanan verilerin en azından bir kısmının potansiyel olarak sınırsız sayıda insana erişilebilir olduğunu belirtmiş ve bu nedenle kişisel veri işleme faaliyetinin tamamen kişisel ve ev içi faaliyeti çerçevesinde işleme olmadığı sonucuna varmıştır ve topluluğun 95/46 sayılı Direktif'e göre veri sorumlusu olduğuna hükmetmiştir¹⁷¹.

2. Avrupa Birliği Organ ve Kurumlarının Faaliyetleri Gereği Veri İşlemeler

Kolluk ve Ceza Adaleti Direktifi, AB hukuku kapsamı dışındaki faaliyetler ve AB kurum, organ ve ajanslarının veri işleme faaliyetlerinde uygulama alanı bulmayacaktır¹⁷². Kolluk ve Ceza Adaleti Direktifi'nin kapsam dışı bıraktığı bu hal, genel olarak *ad hoc* veri koruma rejimlerini uygulamaya devam edecek gibi görünen AB kurum ve organları bakımından önemlidir. Örneğin Europol, Eurojust, OLAF ve Gümrük Bilgi Sistemi gibi güvenlik faaliyetleri ile ilgili veri tabanlarının veri işleme faaliyetleri Kolluk ve Ceza Adaleti Direktifi'ne tabi değildir¹⁷³.

AB üyesi devletler, içişleri ve adli meselelerde işbirliği için gerek Avrupa Konseyi gerek BM çapında iki taraflı veya bölgesel anlaşmalar yapmışlardır. AB'nin adalet alanındaki faaliyetlerini gerçekleştirebilmesi için polis ve cezai meselelerde

¹⁶⁹ Metin Günday, **İdare Hukuku**, Güncellenmiş ve Gözden Geçirilmiş 10. Baskı, Ankara, İmaj Yayınevi, 2015, s. 290-291.

¹⁷⁰ *Tietosuojaualtuutettu v Jehovan Todistajat* [BD], B. No: C-25/17, 10.07.2018 Çevrimiçi https://curia.europa.eu/jcms/jcms/j_6/en/ 29.03.2020.

¹⁷¹ Lindroos-Hovinheimo, **a.g.e.**, s. 236.

¹⁷² Bkz. Kolluk ve Ceza Adaleti Direktifi m. 2/3.

¹⁷³ De Hert, Papakonstantinou, **a.g.e.**, s. 11.

karşılıklı yardımlaşma ve kişisel verilerin işlenmesi gerekmektedir. Bu çerçevede kişisel veri aktarımına ilişkin önemli mekanizmalar olan Schengen, Europol ve Eurojust değerlendirilmelidir. Bunlar o denli önemli mekanizmalardır ki Türkiye’de KVKK’nin ihdas nedenlerinden biri de Europol ve Eurojust ile işbirliği ve elektronik veri paylaşımına zemin hazırlamaktı¹⁷⁴.

a. Europol

Maastricht Antlaşması’nın uyuşturucu kaçakçılığı ve organize suçluluğu kapsayacak bir Merkezi Avrupa Ceza Soruşturma Bürosu’nun tam olarak kurulmasına yönelik bir taahhüdü üzerine Europol Sözleşmesi¹⁷⁵ ile Europol¹⁷⁶ kurulmuştur. AB üyesi ülkelerin kolluk güçleri arasındaki işbirliğini geliştirerek daha güvenli bir Avrupa yaratmayı amaçlayan Europol Sözleşmesi’nin hükümleri, TFEU m. 88 özgürlük, güvenlik ve adalet alanına girmektedir. 2009 yılındaki Europol Konsey Kararı’nın ardından Europol, Avrupa Parlamentosu’na hesap veren ve fiilleri nedeniyle ABAD’ye karşı sorumlu olan bir AB kuruluşu haline gelmiştir¹⁷⁷.

Europol’ün amacı AB üyesi devletler arasında bilgi değişimini kolaylaştırarak stratejik analizler yapmak, sınır ötesi operasyonlara yardım ederek ve bunları koordine ederek kolluk güçlerini desteklemek ve terörizm, uyuşturucu ve Euro sahteciliği gibi suçlarda bilgi paylaşımı yapmaktır¹⁷⁸. Europol’ün kendi başına icra gücü bulunmasa da AB üyesi devletler arasında sınır aşan suçlarda veri alışverişine imkân sağlamaktadır. Yani Europol’ün görevi, esas olarak AB üyesi devletler arasında veri

¹⁷⁴ Küzeci, **a.g.e.**, s. 349.

¹⁷⁵ Europol Sözleşmesi 26 Temmuz 1995’te imzalanmış, 1 Ekim 1998’de yürürlüğe girmiştir.

¹⁷⁶ Esasında Europol’den evvel faaliyetleri geçici olan Europol Drugs Unit kurulmuştur. Bu birimin temel amacı, üye ülkeleri etkileyen suçlarla ilgili bilgi ve istihbarat değişimini sağlamak, örgütlü suçlarla devletlerin ulusal makamları ile işbirliği halinde uluslararası düzeyde mücadele etmektir. Zamanla bu birimin faaliyet alanına giren suçlar göçmen kaçakçılığından motorlu araç kaçakçılığına kadar genişlemiştir. 1 Temmuz 1999’da Europol’ün çalışmaya başlaması ile birimin yönetimi Europol’ün faaliyet alanına dâhil olmuştur. Bkz. Ertan Beşe, **Terörizm, Avrupa Birliği ve İnsan Hakları**, İstanbul, Seçkin Yayıncılık, 2002, s. 95.

¹⁷⁷ Yenisey, **Kolluk Hukuku**, s. 100.

¹⁷⁸ Çevrimiçi <https://eur-lex.europa.eu/summary/glossary/europol.html> 14.02.2020.

alışverişi yapmaktır¹⁷⁹. Bu sayede istihbarat analizi yapılacak ve operasyonlar koordinasyon içinde gerçekleşecektir¹⁸⁰.

Europol'ün belirtilen amaçlarını yerine getirebilmek için kurulmuş elektronik bilgi sistemi olan *Europol Bilgi Sistemi* bilişim sistemi, dosyalar ve index olmak üzere üç bölümden oluşmaktadır¹⁸¹. Bilişim sistemi kısmında kişisel veriler depolanmakta, değişimleri ve kullanımları sağlanmaktadır. Sistem dâhilindeki kişisel veriler, AB üyesi devletlerin kanunlarına göre Europol'ün alanına giren bir suç¹⁸² işlendiğinde bu suçta şüpheli kişi ve suçların sisteme işlenmesi ile elde edilen verilerdir. Europol Sözleşmesi m. 10'a göre tanık, mağdur, muhbir gibi kişilerin de bilgileri veri tabanında saklanmaktadır¹⁸³. Ancak sınır aşan bir suçta şüpheli olmayan kişinin de verilerinin işlenmesi, sınır aşan suçlulukla mücadele amacı ile açıklanamamaktadır¹⁸⁴.

Bilgi sistemine kişilerin yaşı, uyruğu, fiziksel özellikleri, organize suç örgütü ile iltisakı olduğunu düşündüren hususlar, suçun işlendiği yer ve zaman, suçta kullanılan araçlar gibi oldukça kapsamlı türden veriler işlenir¹⁸⁵. Veriler, bilgi (*factual information*) ve istihbarat (*soft intelligence*) verileri olarak ayrılabilir. İstihbarat verileri arasında sübjektif değerlendirmeler de yer aldığından bunların kullanılması sakıncalıdır. Veri tabanındaki veriler, gizlilik durumu ve verinin ifşa edilmesi halinde bir ya da birden çok AB üyesi devletin çıkarlarına zarar verme düzeyine göre *EU restricted*, *EU confidential*, *EU secret* ve *EU top secret* olarak gruplandırılmaktadır¹⁸⁶.

Europol'ün elde ettiği kişisel veriler, somut bir hazırlık soruşturmasında kullanılabileceği gibi soruşturmalardan bağımsız olarak verinin stratejik doğası

¹⁷⁹ Şimşek, **a.g.e.**, s. 75.

¹⁸⁰ Ali Rıza Çam, **Adli Bilişim ve Kolluk**, İstanbul, On İki Levha Yayıncılık, 2015, s. 124.

¹⁸¹ Çam, **a.g.e.**, s. 124.

¹⁸² Europol'ün görev alanına giren suçlar külli olarak AB bakımından da tehdit olarak görülen suçlardır. Terör suçları, insan ticareti, ekonomik suçlar, sahte Euro basmak (Euro counterfeiting) çevre suçları, para kuryeliği (money muling) gibi pek çok suç tipi Europol'ün görev alanına girmektedir. Suç listesi için bkz. Çevrimiçi <https://www.europol.europa.eu/crime-areas-and-trends/crime-areas> 06.02.2020.

¹⁸³ Yenisey, **Kolluk Hukuku**, s. 106.

¹⁸⁴ Dağ, **a.g.e.**, s. 57; Şimşek, **a.g.e.**, s. 77.

¹⁸⁵ Çam, **a.g.e.**, s. 124.

¹⁸⁶ Detaylı açıklama için bkz. Yenisey, **Kolluk Hukuku**, s. 106-107.

nedeniyle de tutulabilir¹⁸⁷. Bu sisteme; ulusal bürolar, irtibat görevlileri, Europol Direktörü ve yetkilileri erişebilmektedir¹⁸⁸.

Türkiye ve Europol arasında 2004 yılında kişisel veri paylaşımına imkân veren esas operasyonel işbirliği anlaşması yerine teknik ve stratejik düzeyde işbirliği anlaşması imzalanmıştır. Operasyonel işbirliği anlaşması, Türkiye'nin 108 sayılı Sözleşme'ye taraf olmaması ve Türk hukukunda kişisel verilerin korunmasına ilişkin bir düzenleme olmaması nedeniyle imzalanmamıştır ve bu, Europol ve Türkiye arasındaki veri aktarımına ket vurmuştur¹⁸⁹.

b. Eurojust

Eurojust¹⁹⁰, üye devletlerin savcılık makamları arasında etkili bir işbirliği ve üye devletlerin adli mercileri ile Europol'ün koordine bir biçimde çalışmasını, sınır dışı etme işlemlerinin infazını sağlamayı hedeflemektedir¹⁹¹. Nitekim TFEU m. 85/1'e göre Eurojust cezai soruşturma başlatma ve ulusal yetkili otoritelerce cezai soruşturma yapılmasını talep etme yetkisine sahip olarak koordinasyon ve işbirliği bakımından ciddi bir katkıda bulunmaktadır¹⁹². Ayrıca Europol analizlerine dayanarak EJN ile yakın işbirliği yapmakta ve organize suçların soruşturulmasında ilerleme kaydetmektedir¹⁹³.

¹⁸⁷ Şimşek, **a.g.e.**, s. 77.

¹⁸⁸ Beşe, **a.g.e.**, s. 96, dipnot 71.

¹⁸⁹ 2015 AB-Türkiye İlerleme Raporu'na göre KVKK, AB-Türkiye müktesebatının ayaklarından biridir ve buna ilişkin bir kanunun bulunması belirtilen organizasyonlarla işbirliği antlaşmalarının yapılması, terörizmle mücadele edilmesi için bir gerekliliktir. Bkz. AB Türkiye İlerleme Raporu 2015, Çevrimiçi https://www.ab.gov.tr/files/000files/2015/11/2015_turkiye_raporu.pdf 08.01.2020, s.67. Gizem Gültekin Varkonyi, "Yolcu İsim Kayıtlarının Terörle Mücadele Kapsamında Yurt Dışına Yasal Aktarımı: Avrupa Birliği Uygulamaları ve Türkiye", **TBB Dergisi**, c. 30, s. 32, 2017, s. 365; Türkiye ve Europol 2004 yılında teknik ve stratejik veri aktarımı ile suçların tanımlanması, kontrolü, önlenmesine ilişkin Türkiye Cumhuriyeti ve Avrupa Polis Teşkilatı Arasında İşbirliğine İlişkin Anlaşma (15.7.2007 tarih ve 25523 sayılı RG) imzalamıştır. Ancak Türkiye'de kişisel verilerin korunması kanunu bulunmadığı için Anlaşma yürürlüğe girmemiştir. Gültekin Varkonyi, **a.g.e.**, s. 374.

¹⁹⁰ Eurojust'un kurulması, 21.09.2001'de Brüksel'de terörle mücadele için gerçekleşen olağanüstü Konsey Zirvesi'nde yayımlanan eylem planına dayanmaktadır. 01.01.2002'den itibaren faaliyete geçmek üzere hakim, savcı ve polis yetkililerinden ibaret özel bir yapının kurulması da eylem planının bir parçası idi. Bkz. Beşe, **a.g.e.**, s. 107.

¹⁹¹ Bozkurt, Köktaş, **a.g.e.**, s. 382; Çam, **a.g.e.**, s. 132.

¹⁹² **Exchange of Information and Data Protection in Cross-border Criminal Proceedings in Europe**, s. 16.

¹⁹³ Arif Köktaş, "Özgürlük, Güvenlik ve Adalet Alanı", **Avrupa Birliği**, Ed. Belgin Akçay, İlke Göçmen, Gözden Geçirilmiş ve Güncellenmiş 3. Baskı, Ankara, Seçkin Yayıncılık, 2016, s. 513. EJN,

c. Schengen Bilgi Sistemi (SIS)

SIS, AB üyesi devletlerin güvenlik güçlerinin uyumlu bir şekilde çalışması için aralarında bilgi alışverişini sağlamayı hedeflemektedir. SIS, yetkili makam olan polis ve gümrük muhafaza memurlarının kişiler ve nesneler hakkında uyarı (*alert*)¹⁹⁴ girmesini ve bu hususta danışmalarına olanak sağlamaktadır¹⁹⁵. SIS'in veri koruma yaklaşımı esas olarak sisteme uyarı girenin, durumun içeriğinden sorumlu olmasıdır. Bu hususta ulusal veri koruma otoriteleri, kendi ülkelerinde veri koruma kurallarının uygulanmasından sorumlu olup aynı zamanda Avrupa Veri Koruma Kurulu da EU LISA¹⁹⁶ tarafından yönetilen merkezi sistem için veri koruma kurallarının uygulanmasını denetlemektedir¹⁹⁷. Zira sistemde işlenen verileri ile ilgili veri sahipleri, taleplerini iç hukuk çerçevesinde ulusal makamlara yönelteceklerdir¹⁹⁸. SIS, güncellenmiş olup ikinci nesil olarak SIS II kullanılmaktadır. Sisteme kişisel veri işleme, üye devletlerin ulusal sistemlerine bilgi girmesi ile gerçekleşmektedir¹⁹⁹.

SIS'te işlenen kişisel verilerin korunmasına ilişkin hükümler, Avrupa Parlamentosu ve Konseyi'nin 1987/2006 sayılı İkinci Nesil Schengen Bilgi Sistemi'nin (SIS II) Kurulması, İşletilmesi ve Kullanımı Hakkında Tüzük ve 2007/53/JHA sayılı İkinci Nesil Schengen Bilgi Sistemi'nin Kurulması, İşletilmesi ve Kullanımı Hakkında Konsey Kararı'nda yer almaktadır²⁰⁰. AB üyesi devletler, SIS'te

sınır aşan örgütlü suçlar ve uluslararası terörizm başta olmak üzere cezai konularda yargı makamları arasında adli işbirliği ve yardımlaşmanın standardını yükseltmek için kurulmuş bir sistemdir.

¹⁹⁴ Uyarıdan (*alert*) anlaşılması gereken, SIS II'ye giren yetkili makamların belirli bir eylemi gerçekleştirecek bir kişiyi tanımlamasına izin veren bir dizi veridir. Bkz. 1987/2006 sayılı Tüzük m. 3/a.

¹⁹⁵ Çevrimiçi <https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system/access-rights-and-data-protection> 06.02.2020.

¹⁹⁶ Avrupa Birliği Özgürlük, Güvenlik ve Adalet Alanında Büyük Ölçekli IT Sistemlerinin Operasyonel Yönetimi Ajansı. EU LISA, AB'nin özgürlük, güvenlik ve adalet alanında büyük ölçekli IT sistemlerinin kesintisiz çalışmasını sağlamak için 2011 yılında kurulmuştur.

¹⁹⁷ Çevrimiçi <https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system/access-rights-and-data-protection> 06.02.2020.

¹⁹⁸ Şimşek, **a.g.e.**, s. 80.

¹⁹⁹ Çam, **a.g.e.** s. 130.

²⁰⁰ 10.12.2006 tarihli bu Tüzük'ün tam metni için bkz. Çevrimiçi <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32006R1987&from=EN> 06.02.2020; 12.06.2007 tarihli bu Konsey Kararı'nın tam metni için ise Çevrimiçi <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32007D0533&from=EN> 06.02.2020.

yer alan kişisel verileri ülkelerine girme veya kalmayı talep eden veri sahiplerini reddetmek veya kabul etmek amacıyla işleyebilir²⁰¹.

SIS'te yer alan kişisel veri kategorisi sınırlı sayıdadır. Bu veriler arasında kişinin adı, değişmeyecek spesifik fiziksel özellikleri, uyruğu, doğum yeri, fotoğrafları ve parmak izi yer almaktadır. Her ne kadar özel nitelikli kişisel verilerin işlenmesi 95/46 sayılı Direktif'e tabi ise de²⁰² bu Direktif'te biyometrik veriler tanımlanmadığından parmak izi de Tüzük uyarınca işlenmektedir. SIS'te kişisel verileri işlenen veri sahibi bu verilere erişim talep etme²⁰³ ve bunların doğru ve hukuka uygun olarak girildiğinden emin olma, veriler doğru değilse düzeltme veya silme talebinde bulunma hakkına²⁰⁴ sahiptir. SIS II'de tutulan kişisel verilere Europol ve Eurojust tarafından erişilmesi mümkündür. Europol veya Eurojust tarafından yapılan bir araştırmada SIS II bağlamında bir uyarının bulunduğu sonucuna varılırsa, Europol Sözleşmesi'nde belirtilen kanallar vasıtasıyla Europol veya Eurojust üye devlete bilgi vermekle yükümlüdür²⁰⁵.

Schengen polis ve adli işbirliği Sirene ofisleri aracılığıyla yürütülmektedir. Bu ofisler adli merciler tarafından çıkarılan Avrupa Tutuklama Müzekkeresi kayıtlarını SIS kaydı olarak A formu biçiminde Schengen sistemine aktarırlar²⁰⁶.

d. Vize Bilgi Sistemi (VIS)

²⁰¹ 1987/2006 sayılı Tüzük m. 31/1.

²⁰² 1987/2006 sayılı Tüzük m. 40.

²⁰³ 1987/2006 sayılı Tüzük m. 41/1-4; Ancak veri sahibinin bu verilere erişip erişemeyeceği kişisel veriyi SIS II'ye işlemiş olan AB üyesi devletin kanunlarında öngörülmüşse, kanunda öngörülen usullere göre belirlenecektir. Ancak Tüzük m. 41/6 "*Kişinin başvurduğu tarihten itibaren altmış gün içinde veya veriyi işleyen devletin iç hukukunda daha kısa bir süre öngörülmüşse bu süre içinde bilgilendirme yapılmak zorundadır*" hükmü AB üyesi devlete bilgilendirme yükümlülüğünü yerine getirmesi için azami altmış günlük süre belirlemekle Kolluk ve Ceza Adaleti Direktifi'nden daha yüksek bir koruma sağlamıştır.

²⁰⁴ Bu talebin değerlendirilme süresi de azami bir süreye Tüzük m. 41/7 ile bağlanmıştır. "*Düzeltilme ve silme hakkı da mümkün olan en kısa sürede ve her halükârda veri sahibinin düzeltme veya silme başvurusunda bulunduğu tarihten itibaren en geç üç ay içinde veya iç hukukta daha kısa süre öngörülmüşse bu süre içinde talebi hakkında bilgilendirilecektir.*"

²⁰⁵ 2007/553 sayılı Konsey Kararı m. 41/2 ve m. 42/2.

²⁰⁶ Yenisey, **Kolluk Hukuku**, s. 109.

VIS AB üyesi devletler arasında vize verilebilmesi için kişisel verilerin alışverişine olanak sağlayan bir sistemdir²⁰⁷. Merkezi bir IT sisteminden ve bu merkezi sistemi ulusal sistemlere bağlayan bir iletişim altyapısından oluşur. VIS, AB üyesi olmayan ülkelerdeki konsoloslukları ve Schengen Devletleri'nin tüm dış sınır geçiş noktalarını birbirine bağlar. Kısa süreli vizelerin Schengen Bölgesi'ni ziyaret etmesi veya geçmesi için başvurulara ilişkin verileri ve kararları işler. Sistem tanımlama ve doğrulama amacıyla başta parmak izleri olmak üzere biyometrik eşleştirme yapabilir²⁰⁸. VIS verilerine erişebilecek kişiler, görevlerini yerine getiren yetkili personel ile sınırlıdır. Veriler VIS'te beş yıl tutulur. Bu saklama süresi verilen vizenin son tarihinden, olumsuz bir kararın alındığı tarihten veya verilen vizeyi değiştirme kararının alındığı tarihten başlar. Herhangi bir kişi VIS'teki verileri hakkında bilgilendirilme hakkına sahiptir. Kişiler, hakkındaki yanlış verilerin düzeltilmesini ve yasa dışı olarak kaydedilen verilerin silinmesini isteyebilir²⁰⁹. VIS kapsamında verilerin tutulma süresinin düzenlenmiş olması veri koruma açısından olumludur.

e. ECRIS

ECRIS, AB düzeyinde polis ve adli birimler arasında adli sicil kayıtlarının paylaşımının güvenli olmasını hedefleyen bir sistemdir²¹⁰. Yapı olarak dağıtık bilişim üzerine kurulu olan ECRIS'te AB üyesi devletlerin veri tabanlarında tutulan verilerin karşılıklı değişimi mümkündür²¹¹. 2009/315 sayılı Çerçeve Karar m. 9 uyarınca adli sicil kayıtlarının paylaşımı halinde kişisel verilerin nasıl korunacağı düzenlenmiştir. Buna göre kişisel veriler ancak paylaşıma neden olan suçun muhakemesinde kullanılmalı, muhakeme harici bir nedenle veri paylaşılmışsa, üye devletin kanunlarında bu neden öngörülmüş olmalıdır. Ancak üye devletin kamu güvenliğini tehdit eden ciddi ve acil bir tehdit varsa bu şartlar aranmaksızın veri paylaşılır.

²⁰⁷ VIS, AB Konseyi'nin 8 Haziran 2004 tarihli 2004/512 sayılı kararı ile kurulmuştur.

²⁰⁸ Çevrimiçi https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/visa-information-system_en 06.02.2020.

²⁰⁹ Çevrimiçi https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/visa-information-system_en 06.02.2020.

²¹⁰ Çam, **a.g.e.**, s. 125.

²¹¹ Çam, **a.g.e.**, s. 126.

3. Kolluk ve Ceza Adaleti Direktifi'nden Önce Yürürlüğe Giren Antlaşmalar Gereği Veri İşlemeler

AB düzeyinde kolluk ve adli makamların kullandığı kişisel verilerin aktarılmasına ilişkin ortak bir standart bulunmadığı için veri aktarımı ve korunması ikili antlaşmalar ile düzenlenmekteydi²¹². AB üyesi devletlerin kişisel verileri üçüncü bir devlete aktarmasına ilişkin genel kural, verilerin alıcı devlet tarafından yeterli şekilde korunur durumda olmasıdır. Ancak üye devletler için Komisyon düzeyinde yeterlilik düzeyinin belirlenmesi, günümüze kadar ancak birkaç ülkece yapılabilen uzun ve hantal bir süreç olmuştur. Polis ve ceza adaletine ilişkin kişisel verilerin aktarımı konusunda esasen uluslararası suçlar nedeniyle kamu yararı da bulunmaktadır. Bu nedenle pek çok devlet, yeterlilik şartı ve diğer korumaları göz ardı ederek diğer ülkelerle yaptığı ikili antlaşmalarla veri aktarımını sağlamaktadır²¹³. Türkiye Cumhuriyeti Polonya Cumhuriyeti Hükümeti Arasında Örgütlü Suçlar, Terörizm ve Diğer Suçlarla Mücadelede Adli İşbirliği Antlaşması²¹⁴, Türkiye Cumhuriyeti ve Slovenya Cumhuriyeti Hükümeti Arasında Örgütlü Suçlar, Uyuşturucu Madde Kaçakçılığı, Uluslararası Terörizm ve Diğer Ciddi Suçlarla Mücadelede İşbirliği Antlaşması²¹⁵, Bulgaristan ile Polis İşbirliği Antlaşması²¹⁶ bu minvalde adli işbirliği antlaşmalarındandır.

Kolluk ve Ceza Adaleti Direktifi'nin yürürlüğünden sonra bu ikili antlaşmaların akıbeti Kolluk ve Ceza Adaleti Direktifi m. 61'de düzenlenmiştir. Buna göre Kolluk ve Ceza Adaleti Direktifi'nin yürürlüğe girdiği tarihten önce imzalanmış ve bu tarihten

²¹² Marquenie, **a.g.e.**, s. 324.

²¹³ De Hert, Papakonstantinou, **a.g.e.**, s. 15.

²¹⁴ Antlaşma ile veri aktarımının yapılacağı makamlar belirtilmiş ve bunlar harici makamlar arasında veya taraf ülkeler dışına veri aktarımı yapılabilmesi için taraflar arasında yazılı izin prosedürünün işletilmesi gerektiği belirtilmiştir. Gültekin Varkonyi, **a.g.e.**, s. 372.

²¹⁵ Antlaşma esas olarak uyuşturucu ve insan kaçakçılığını önlemeyi hedeflemektedir, ancak genel olarak terörizm başta olmak üzere suçla mücadeleye de değinmiştir. Antlaşmanın kişisel veriler konusunda önemi ise verileri aktarılan kişilerin aktarıma ilişkin bilgilendirilmesine olanak tanıyarak şeffaflıktan bahsetmesidir. Bkz. Gültekin Varkonyi, **a.g.e.**, s. 373.

²¹⁶ Polonya ve Slovenya ile yapılan adli işbirliği antlaşmalarına büyük oranda benzetmekle birlikte verilerin yok edilmesine ilişkin hüküm barındırması nedeniyle önemlidir. Taraf devletlerden biri, aktarılan verilerin kapsam dışı kullanıldığı veya güncel olmadığını tespit etmesi halinde verileri yok etmelidirler. Aksi halde veriler taraf devletlerde zaman sınırı olmaksızın kalabilmektedir. Bkz. Gültekin Varkonyi, **a.g.e.**, s. 373.

önce geçerli olan uluslararası anlaşmalar, tadil, düzenlenme ve ilga edilene kadar yürürlükte kalacaktır. Örneğin Prüm Kararları, 1959 tarihli AB Üyesi Devletler Arasında Cezai Meselelerde Karşılıklı Yardım Sözleşmesi uyarınca yetkili makamlar tarafından işlenen kişisel verilere Kolluk ve Ceza Adaleti Direktifi hükümleri uygulanmayacaktır²¹⁷. Ahde vefa ilkesi gözetildiğinde bu madde anlaşılabilir. Ancak maddenin devletlerin geçmişte yaptıkları ikili anlaşmalar ile Kolluk ve Ceza Adaleti Direktifi'nin amacını gerçekleştirmekten imtina edeceklerine ilişkin çeşitli endişeler bulunmaktadır²¹⁸. Nitekim maddenin düzenleniş biçimi, anlaşmaları tadil etme, değiştirme ve ilga etme konusunda devletleri zorlayıcı değildir ve bu da Kolluk ve Ceza Adaleti Direktifi'nin asgari koruma standardını sağlamayan uygulamaların devamına zemin hazırlamaktadır.

a. AB ve Bazı Ülkeler Arasında PNR Veri Aktarımı

PNR verileri kimlik tespitini sağlayarak içerik açısından önemli olan ve gümrük teşkilatı başta olmak üzere kolluk ve göç bürolarının vereceği kararlarda etkili olan bilgilerdir²¹⁹. PNR Rehber İlkeleri'ne²²⁰ göre veriler iki gruba ayrılıp ilk grupta ad, soyad, adres, telefon numarası, e-posta, banka finansal bilgileri; diğer grupta ise rezervasyonun kim tarafından yapıldığı, uçak kapı bilgisi, bagaj, yemek seçimi gibi yolculuk bilgileri yer almaktadır²²¹. PNR verileri oluşturulduğu anda bu veriler havayolu şirketlerinin mülkiyet hakkına konu olmakta ve ulusal güvenlik gerekçesiyle yolcunun rızası olmaksızın üçüncü kişilerle paylaşılmaktadır²²².

11 Eylül terör saldırılarından sonra, Havacılık ve Ulaştırma Güvenliği Kanunu'na²²³ göre ABD'de yerleşik havayolu taşıma firmaları ve yabancı firmalar,

²¹⁷ Kolluk ve Ceza Adaleti Direktifi resital m. 94.

²¹⁸ Bkz. De Hert, Papakonstantinou, **a.g.e.**, s. 15.

²¹⁹ Gültekin Varkonyi, **a.g.e.**, s.341; Havayolu taşımacılık sistemlerinde tutulan veriler yalnız PNR verileri olmayıp kişilerin daha çok pasaport ve vize bilgilerinden oluşan API (*Advance Passenger Information-Detaylı Yolcu Bilgileri*) verileri de bulunmaktadır. PNR verileri havayolu şirketlerinin ticari amaçla oluşturduğu verilerdir. API sistemi ise ilgili yolculuğun gerçekleşeceği sınır ve güvenlik kontrol birimlerinin kalkıştan önce yolcu bilgilerinin aktarıldığı sistemlerdir. Gültekin Varkonyi, **a.g.e.**, s. 348.

²²⁰ International Civil Aviation Organization “Guidelines on Passenger Name Record (PNR) Data”.

²²¹ Gültekin Varkonyi, **a.g.e.**, s. 353-354.

²²² Gültekin Varkonyi, **a.g.e.**, s. 349.

²²³ “Aviation and Transportation Security Act”.

ABD Gümrük Komisyonu'na havayolu şirketleri ve uçuşları, uçuşlarda listelenen yolcuların kimlik bilgilerini sunmakla yükümlü olmuştur. Ancak bu verilerin işlenmesi ile yolcuların potansiyel terörist olarak sınıflandırılacağı ve ayrımcılığa maruz kalacağı endişesi de doğmuştur²²⁴. Bu nedenle de AB'den ABD'ye ticari amaçla kişisel veri aktarımında kişisel verilerin korunmasına ilişkin Safe Harbour İlkeleri kabul edilmiştir. Ancak ilkeler, verilerin aktarıldığı ABD şirketlerinin, aktarılan verileri güvenlik veya terörle mücadele kapsamında ABD'nin başka makamları ile paylaşıp paylaşmayacağı konusunda açıklık taşımamıştır²²⁵. Nitekim ABAD, AB ve ABD arasında imzalanan ve AB'den ABD'ye havaalanı yolcu bilgilerinin paylaşımına ilişkin anlaşmayı iptal etmiştir²²⁶. 2012 yılında AB ve ABD arasında PNR Verilerinin ABD İç Güvenlik Departmanı Tarafından Kullanımı ve Transferi Anlaşması imzalanmıştır²²⁷.

AB ve Kanada arasında da PNR verilerinin aktarılması ve işlenmesine ilişkin PNR Antlaşması müzakeresi yapılmıştır. AB Konseyi, Avrupa Parlamentosu'nun Antlaşma'yı onaylamasını istemiş ve Avrupa Parlamentosu öngörülen anlaşmanın AB hukukuna uygun olup olmadığını ve özellikle özel yaşama saygı ve kişisel verilerin korunmasına ilişkin hükümlerle uyumlu olup olmadığını tespit etmek amacıyla ABAD'nin görüşüne başvurmuştur. ABAD'nin, ilk kez bir uluslararası antlaşma taslağının AB Temel Haklar Şartı ile uyumluluğu hakkında bir karar vermesi için çağrıldığına dikkat edilmelidir²²⁸. Antlaşma, herhangi bir yolcu tarafından veya herhangi bir yolcu adına rezerve edilen her yolculuk için yolcunun adı, rezervasyon ve seyahat tarihleri, sık uçan yolcu üyeliği hakkında bilgi, iletişim bilgileri, ödeme bilgileri, seyahat programı, bagaj, koltuk bilgileri ve diğer bilgilerden oluşan PNR verilerinin toplanması ve paylaşılmasını öngörmektedir. Kanada makamları PNR

²²⁴ Gültekin Varkonyi, **a.g.e.**, s. 350.

²²⁵ Gültekin Varkonyi, **a.g.e.**, s. 357; Safe Harbour İlkeleri'nin geçersizliğine ilişkin bkz. "Yeterli Düzeyde Veri Koruma" başlıklı bölüm.

²²⁶ Birleştirilmiş başvurular C-317/07 ve C-318/04, European Parliament v. Council of the European Union (C-317/04) and European Parliament v. Comm'n of the European Communities (C-318/04) Çevrimiçi https://curia.europa.eu/jcms/jcms/j_6/en/ 29.03.2020.

²²⁷ "Agreement Between the United States of America and the European Union on the Use and Transfer of Passenger Name Records to the United States Department of Homeland Security". Anlaşma m. 26'ya göre yedi yıl geçerliliği bulunmaktadır. Bu Anlaşma ile PNR verilerinin terörle mücadelede küresel bir araç olarak kullanıldığı düşünülmüştür.

²²⁸ Court of Justice of The European Union Press Release No.84/17, 26.07.2017, Çevrimiçi <https://curia.europa.eu/jcms/upload/docs/application/pdf/2017-07/cp170084en.pdf> 23.03.2020.

verilerini terör suçları veya ciddi suçları önlemek, soruşturmak veya kovuşturmak amacıyla alabilirler. PNR verilerinin Kanada'ya aktarılmasının amacı, kamu güvenliğini sağlamak ve bu verilerin terör suçları ve ciddi sınır ötesi suçların önlenmesi için kullanılmasını sağlamaktır²²⁹. ABAD 1/15 nolu görüşünde yolcunun özel araç hizmet talebi ya da özel diyetinin olup olmadığı bilgisinin sağlığına ilişkin bilgi olduğu ve özel nitelikli veriler bakımından Antlaşma'nın yeterli koruma düzeyini sağlamadığını belirtmiştir²³⁰. ABAD, olması gereken PNR Antlaşması ile ilgili de tespitlerde bulunmuştur. Öncelikle aktarılacak belirli PNR verileri açık ve kesin olmalıdır. PNR verilerinin otomatik işlenmesi için kullanılan model ve kriterler spesifik, güvenilir ve ayrımcı olmamalıdır. Veri tabanları, Kanada tarafından terörizm ve ciddi sınır ötesi suçlarla sınırlı olarak kullanılmalıdır. PNR verileri, Kanada makamları tarafından AB üyesi olmayan bir üçüncü devlet ile ancak AB Komisyonu'nun bu kararına eş değer bir antlaşma olması halinde paylaşılmalıdır. Kanada'da bulundukları süre boyunca veya Kanada'dan ayrıldıktan sonra PNR verilerinin kullanılması halinde, yolculara bilgilendirilme hakkı tanınmalıdır. PNR verilerinin işlenmesi ile ilgili yolcuların korunmasına ilişkin kuralların gözetimi, bağımsız bir denetim makamı tarafından yapılmalıdır. Ancak bu şartlar görüşe konu olan PNR Antlaşması'nda sağlanmamıştır²³¹.

Türk hukukunda ise PNR veri aktarımını öngören kanuni mevzuat 2920 sayılı Türk Sivil Havacılık Kanunu'dur. Kanun *havayolu ile seyahat eden kişilerin bilgilerinin seyahatini kolaylaştırmak veya güvenlik ve risk değerlendirmesi yapmak amacıyla* işlenebileceğini öngörmüş²³² ancak bu kapsamda hangi veri kategorilerinin işleneceğini belirtmemiştir. Kanun'a göre İçişleri Bakanlığının uygun görüşünün olması halinde üçüncü devletlerin talebi ile bu bilgiler devletlerle paylaşılabilir. Kanun bu noktada üçüncü devletin veri koruma düzeyini değerlendirmeyi aramamış,

²²⁹ Maja Brkan, "The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning", **German Law Journal**, s. 20, 2019, s. 877.

²³⁰ Opinion of Advocate General Mengozzi, para. 212, Çevrimiçi <http://curia.europa.eu/juris/document/document.jsf?text=&docid=183140&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=491722> 23.03.2020.

²³¹ Çevrimiçi <https://curia.europa.eu/jcms/upload/docs/application/pdf/2017-07/cp170084en.pdf> 23.03.2020.

²³² Türk Sivil Havacılık Kanunu m. 40/5.

yalnız üçüncü devletin talebi ve Bakanlığın olurluğunu yeterli görmüştür. Ayrıca Kanun veri işleme bakımından KVKK'ye atıf yapmıştır. KVKK m. 9'a göre kişisel verilerin yurtdışına aktarımı için ilgilinin açık rızası gerekmektedir. Bu rızanın aranmadığı hallerden biri, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için veri aktarımının zorunlu olmasıdır²³³. Örneğin ABD ve Türkiye arasında havayolu taşımacılığının yapılabilmesi için veri aktarımı gereklidir²³⁴. Ancak belirtmelidir ki KVKK haricinde Türk havacılık mevzuatında yolcu hakkı olarak ya da havayolu şirketlerinin yükümlülüğü olarak yolcuların kişisel verilerinin korunmasına ilişkin etraflıca bir düzenleme bulunmaması ciddi bir eksiklik²³⁵.

Avrupa Veri Koruma Reformu'nun bir başka sonucu olarak AB ötesi uçuşlarda²³⁶ terör suçları ve ciddi suçların²³⁷ önlenmesi, ceza muhakemesinde PNR verilerinin kullanılması ve AB üyesi devletler arasında aktarımına ilişkin 2016/681 sayılı PNR Direktifi²³⁸ ihdas edilmiştir. PNR Direktifi uyarınca AB üyesi devletler, PNR verilerinin işlenmesinden sorumlu birimler olarak *Yolcu Bilgilendirme Birimi* oluşturmalıdır²³⁹. Bu birimler PNR verilerini iç hukuklarında belirledikleri makamlara, Europol'e, AB üyesi devlet ve diğer üçüncü devletlere aktarabilirler²⁴⁰. PNR Direktifi uyarınca PNR verisi, uçuşun gerçekleştiği devletin Yolcu Bilgilendirme Birimi'ne verinin aktarıldığı tarihten itibaren beş yılı aşmayacak bir zaman diliminde Birim'in veri tabanında tutulabilir; bu süreden sonra veri silinmelidir²⁴¹. Ayrıca verinin işlendiği tarihten itibaren altı ayın sonunda veri maskelenmelidir²⁴².

²³³ KVKK m. 5/2-ç.

²³⁴ Gültekin Varkonyi, **a.g.e.**, s. 369.

²³⁵ Gültekin Varkonyi, **a.g.e.**, s. 380.

²³⁶ AB ötesi uçuştan anlaşılması gereken PNR Direktifi m. 3/2 uyarınca üçüncü bir ülkeden uçan havayolu taşıma aracının bir AB üyesi devletin topraklarına inmesi veya AB üyesi devletin topraklarından uçuşu planlanan ve üçüncü bir ülkeye inmesi planlanan bir havayolu şirketi tarafından gerçekleştirilen tarifeli veya tarifesiz uçuştur.

²³⁷ Ciddi suçtan anlaşılması gereken PNR Direktifi'nin 2 nolu ekinde (*Annex*) yer alan suçlardır. Yirmi altı suç ciddi suç olarak değerlendirilmiştir. Suç örgütüne katılma, insan ticareti, suçtan kaynaklanan malvarlığı değerlerini aklama, Euro dâhil olmak üzere para sahtecilik, sabotaj bu suçlardan bazılarıdır.

²³⁸ 2016/681 sayılı Terör Suçlarının ve Ciddi Suçların Önlenmesi, Tespiti, Soruşturulması ve Kovuşturulması İçin Yolcu İsim Kaydı (PNR) Verilerinin Kullanımı Hakkında 27 Nisan 2016 tarihli Avrupa Parlamentosu ve Konsey Direktifi.

²³⁹ PNR Direktifi m. 4.

²⁴⁰ Korkmaz, **a.g.e.**, s. 247.

²⁴¹ PNR Direktifi m. 12/1.

²⁴² PNR Direktifi m. 12/2.

b. Avrupa Siber Suçlar Sözleşmesi

Sözleşme²⁴³ sanal ortamda işlenen suçlarla mücadelede uluslararası etkin bir işbirliği yapılması için ihdas edilmiştir. Sözleşme bilgisayar verisi ve trafik verileri ile ilgili de düzenlemeler öngörmüştür. Sözleşme taraf devletlere trafik verilerinin korunması, bilgisayar sistemlerinin mahremiyetinin sağlanması hususlarını ceza kanunlarında suç olarak düzenleme yükümlülüğü öngörmektedir.

Sözleşme taraf devletlere; bilgisayar sistemleri aracılığıyla işlenen suçların elektronik ortamdaki delillerini elde etmek için yürütülen soruşturma ve kovuşturmada başvurulacak koruma tedbirlerini iç hukuklarında düzenleme yükümlülüğü getirmiştir. Bu kapsamda başvurulacak koruma tedbirleri; depolanmış bilgisayar verilerinin hızlı şekilde korunması (m. 16), trafik verilerinin hızlı şekilde korunması ve kısmen açıklanması (m. 17), üretim emri (m. 18), bilgisayar verilerinin aranması ve elkoyma (m. 19), trafik verilerinin eş zamanlı toplanması (m. 20) ve içerik verilerinin denetlenmesidir (m. 21)²⁴⁴. Sözleşme'nin kişisel veriler bakımından önemi, taraf devletlere IP adresi ve trafik verilerinin belirli bir süre ile tutulmasını öngören mevzuat oluşturma yükümlülüğü öngörmesidir.

4. Ulusal Güvenlik Faaliyetleri Gereği Veri İşlemeler

a. Ulusal Güvenliğin Anlamı

Ulusal güvenlik nedeniyle veri işleme Kolluk ve Ceza Adaleti Direktifi'nin resitalinde²⁴⁵ yer alan ve Direktif'in kapsamını sınırlayan bir haldir. AB üyesi devletlerin ulusal güvenlik faaliyetlerinde ve AB'nin Ortak Dış Politika ve Güvenlik

²⁴³ 23.11.2001 yılında Budapeşte'de imzaya açılan Sözleşme 01.07.2004'te yürürlüğe girmiştir. Sözleşme Avrupa Konseyi üyesi olmayan devletlerin de imzasına açıktır. Nitekim Arjantina, ABD gibi devletler de Sözleşme'ye taraftır. Türkiye bu Sözleşme'yi 10.11.2001 tarihinde imzalamış, Sözleşme 01.01.2015 tarihinde yürürlüğe girmiştir.

²⁴⁴ Detaylı değerlendirme için bkz. Serap Keskin, "Avrupa Konseyi Siber Suçlar Sözleşmesinde Ceza Muhakemesine İlişkin Hükümlerin Değerlendirilmesi", **İÜHFİM**, c. 59, s. 1-2, 2001, s. 157 vd.

²⁴⁵ Kolluk ve Ceza Adaleti Direktifi resital m. 14 "Bu Direktif, AB hukuku kapsamı dışında kalan faaliyetlerde, ulusal güvenlikle ilgili faaliyetlerde, iç hukuk kurum ve organlarının ulusal güvenlikle ilgili faaliyetlerinde ve TEU V. Başlık 2. Bölümü'nde belirtilen faaliyetlerde kişisel verilerin işlenmesi hallerinde uygulanmaz."

Politikası faaliyetlerinde gündeme gelen veri işlemlere Kolluk ve Ceza Adaleti Direktifi uygulanmayacaktır. Belirtilmelidir ki ulusal güvenlik kapsam dışı bırakıldığından istihbarat faaliyetleri kapsamında işlenen kişisel veriler de Kolluk ve Ceza Adaleti Direktifi korumasından yararlanamayacaktır²⁴⁶.

Ulusal güvenlik, meşru amaçların sağlanması için birtakım haklara müdahaleleri meşrulaştıran bir kavramdır²⁴⁷. Özellikle AİHS sisteminde taraf devletlerin güvenlik ve anayasal düzeninin iç ve dış tehditlere karşı korunması için genellikle gizli biçimde iletişimin denetlenmesine başvurulduğunda özel yaşamın gizliliğine saygı hakkı ve ulusal güvenlik arasında denge gözetilmektedir²⁴⁸.

Meşru şiddet tekeline sahip devletin temel görevlerinden biri de vatandaşlarını iç ve dış tehditlerden korumak ve kamu düzenini sağlamaktır. Ancak günümüzde sınır aşan terörist faaliyetler, organize biçimde işlenen kaçakçılık suçları ve siber suçlar göz önüne alındığında ulusal güvenlik, yalnız klasik sıcak savaşlarla tehdit edilmemektedir. Ulusal güvenliğin tesis edilmesi; öncelikle ülkenin coğrafi sınırları dâhilinde muhtemel tehdit ve saldırıların olmaması, devletin sabotaj ve benzeri tehlikelere karşı korunaklı olması ve vatandaşlarının huzur içinde olması biçiminde iç güvenliğin sağlanmasıyla mümkündür. İç güvenlik haricinde bir de dış güvenliğin sağlanması gerekir. Bu da devletin; bir başka devlet ya da kurum, kuruluş ve organizasyonun boyunduruğunda olmamasını, yabancı devletlerin her türlü saldırısından uzak olmasını ve bunlara karşı koymasını gerektirmektedir. İç güvenliğin sağlanmasına hizmet edecek teşkilat, iç güvenlik istihbaratı ve kolluk iken dış güvenliği sağlamakla görevli makamlar ordu ve dış istihbarat organıdır²⁴⁹.

Ulusal güvenlik, AB üyesi devletlerin kendi iç hukuk sorunu olarak düşünülebilir. Ancak 95/46 sayılı Direktif'in yürürlükte olduğu dönemde ABAD; iç hukuk kapsamında ulusal bir veri sorumlusu ve mahkeme tarafından kişisel verilerin işlenmesinin AB hukuku kapsamı dışında olmadığını çeşitli kararlarında

²⁴⁶ Dülger, Özkan, **a.g.e.**, s. 89.

²⁴⁷ Zülküf Bayındır, "Özel Yaşamın Korunması Çerçevesinde İstihbarat Faaliyetleri", **Bahçeşehir Üniversitesi Sosyal Bilimler Enstitüsü**, Yayımlanmamış Yüksek Lisans Tezi, İstanbul, 2016, s. 33.

²⁴⁸ Gülay Arslan Öncü, **Özel Yaşamın Korunması Hakkı**, İstanbul, Beta Yayıncılık, 2011, s. 369.

²⁴⁹ Gökhan Kuloğlu, **İç Güvenlik İstihbaratı ve Kolluk**, İstanbul, Beta Yayınevi, 2015, s. 16-17.

belirtmiştir²⁵⁰. Ancak buna rağmen Kolluk ve Ceza Adaleti Direktifi metninde yer almasa da resitale göre ulusal güvenlik gerekçesiyle veri işlendiğinde bu kişisel veriler Kolluk ve Ceza Adaleti Direktifi'nin korumasından yararlanamamaktadır ve bu husus eleştiriye muhtaçtır²⁵¹. Ayrıca ulusal güvenlik gerekçesiyle veri işleme Kolluk ve Ceza Adaleti Direktifi'nin kapsamı dışında iken, kamu güvenliğine yönelik tehditlere karşı koruma gerekçesiyle veri işleme ise Direktif kapsamındadır. Ancak Direktif kamu güvenliği ve ulusal güvenlik arasındaki ayrımın ne olduğunu açıklamamıştır²⁵².

b. İstihbaratın Tanımı ve Türleri

İstihbarat; ulusal güvenliğin sağlanması için önem arz eden ve siyasi otoritelerin talep ettiği, istihbarat birimleri tarafından toplanan ve analiz edilen verilerin işlendiği bir süreçtir ve taktik, stratejik ve operasyonel olarak ayrılmaktadır²⁵³. Taktik istihbarat, kolluk tarafından veri toplanmasını gerektirip *terörizm ya da suç tehdidine ilişkin bilgi elde etme ya da geliştirme ve bu bilgiyi suçluları yakalama, hedefleri zorlaştırmada kullanma ve tehdidin ortadan kaldırılması ya da hafifletilmesine yarayan stratejiler kullanma* olarak tanımlanabilir. Stratejik istihbarat, iç güvenlik istihbaratının veri toplama faaliyeti olarak *tehditlere karşılık verme stratejileri gerçekleştirmek ve etkili bir önleme sağlayabilmek için gerektiği kadar kaynak tahsisi planlayabilmek amacıyla ortaya çıkan tehdidin yapısal özellikleri hakkında karar vericilere gereken bilgiyi sağlama* biçiminde tanımlanabilir. Operasyonel istihbarat ise devletin üst düzey yetkililerinden olup da istihbaratta son kararı vermeyen yetkililerin yaptığı stratejik ve taktik istihbarat arasında analitik bir istihbarat türüdür²⁵⁴.

İstihbarat sayesinde devletin güvenlik ve bekâ ihtiyacını karşılayacak stratejik veriler elde edilmekte ve bunlar sonucunda devletin strateji çizmesi sağlanmaktadır²⁵⁵.

²⁵⁰ Kararlar için bkz.Bostancı Bozbayındır, **a.g.e.**, s. 72.

²⁵¹ Eleştiri için bkz.Bostancı Bozbayındır, **a.g.e.**, s. 72.

²⁵² Marquenie, **a.g.e.**, s. 330.

²⁵³ Kuloğlu, **a.g.e.**, s. 17-19.

²⁵⁴ Bayındır, **a.g.e.**, s. 17.

²⁵⁵ Bayındır, **a.g.e.**, s. 5.

Devletin istihbarat kapsamında kişisel veri toplama ve değerlendirme yetkisi; askeri istihbarat, dış güvenlik ve iç güvenlik istihbaratı olarak üçe ayrılır²⁵⁶.

Kolluk istihbaratı suç örgütleri ile mücadele etmek, suç işlenmesini önlemek, işlenen suçların soruşturulması için suç bileşenlerinin hassasiyeti, niyeti ve suç işleme yöntemlerini öğrenmek amaçlarıyla; işlenen suçta adli bilimlere, olay yeri inceleme ve diğer delil elde etme imkânları ile soruşturma yürüterek faaliyetlerde bulunmaktadır. Kolluk istihbaratı ve iç güvenlik istihbaratı birbirinden farklıdır. Kolluk istihbaratı, suç odaklı faaliyetlerle ilgili iken²⁵⁷; iç güvenlik istihbaratı, idari kolluk faaliyeti olmayıp²⁵⁸ hükümet tarafından kapsamı belirlenen bir faaliyettir ki suçu önlemenin yanı sıra terörizmle mücadele ve casusluk faaliyetlerine karşı koyma gibi fonksiyonları da bulunmaktadır.

Suçun ve suçluluğun önlenmesi de kolluk ve iç güvenlik istihbaratı arasında koordinasyonun sağlanması ile mümkündür²⁵⁹. Koordine bir biçimde çalışma suçlulukla mücadele için gerekliyse de öncelikle askeri güçler, iç güvenlik hizmetlerinden hariç tutulmalı ve istihbarat servisleri operasyonel faaliyetlerde bulunmamalıdır. Kolluk ve istihbaratın duvarla ayrılması (*the wall of separation between law-enforcement and intelligence*) olarak ifade edilen ilkeye göre istihbarat makamı, esas olarak kolluğun yetki alanına girmeksizin ulusal güvenliğe yönelik tehditleri algılayarak karar mercilerine iletmekle görevlidir²⁶⁰.

İç güvenlik istihbarat teşkilatı, elde ettiği verilerden bir suçun işlendiği sonucuna varmışsa adli sürecin başlaması için bu veriyi kolluktaki ilgili birime iletmelidir²⁶¹. Ceza muhakemesi sürecinde de istihbarat yöntemlerinden

²⁵⁶ Yenisey, **Kolluk Hukuku**, s. 373.

²⁵⁷ Kuloğlu, **a.g.e.**, s. 36.

²⁵⁸ Kolluğun iç güvenlik istihbaratı faaliyetlerinin, suç öncesi döneme ait olduğundan idari kolluk faaliyeti olduğuna dair bkz. Hasan Semiz, “Uluslararası Terör Suçları Bakımından Terör Suçlarında Kolluk Yetkileri”, **Harp Akademisi Komutanlığı Stratejik Araştırmalar Enstitüsü**, Yayınlanmamış Yüksek Lisans Tezi, İstanbul, 2007, s. 77.

²⁵⁹ Kuloğlu, **a.g.e.**, s. 31-32.

²⁶⁰ Baran Kızılırmak, “Önleyici Amaçla Elde Edilen Verilerin Ceza Muhakemesinde Kullanılabilirliği”, **İstanbul Üniversitesi Sosyal Bilimler Enstitüsü**, Yayınlanmamış Yüksek Lisans Tezi, İstanbul, 2018, s.84; Bayındır, **a.g.e.**, s. 119.

²⁶¹ Kuloğlu, **a.g.e.**, s. 39; Kolluk ve iç güvenlik istihbaratının aynı teşkilat içinde olmaması gerektiği belirtilmiş ve ABD’de de kolluk ve iç güvenlik istihbarat faaliyetlerini birlikte yürüten FBI’nın teşkilatlanması eleştirilmiştir. Tartışma için bkz. Kuloğlu, **a.g.e.**, s. 49.

yararlanılabilir, ancak bu yöntemler sonucu elde edilen deliller maddi gerçeğin ortaya çıkarılması için; istihbarat, devletin güvenliği konusunda uzun vadeli ve stratejik bir politikanın oluşturulması amacıyla hizmet etmektedir²⁶². Alman hukukunda istihbarat faaliyetleri sırasında elde edilen veriler delil olarak kullanılabilirken Türk hukukunda kolluğun istihbarat amacıyla yürüttüğü faaliyetlerden elde ettiği veriler yalnız kanunda yazılı amaç için kullanılabilir²⁶³.

Kolluk ve Ceza Adaleti Direktifi, istihbarat faaliyetlerinde kişisel verilerin işlenmesi durumunda uygulanamayacaktır. Bunun nedeni, AB üyesi devletlerin istihbarat faaliyetlerinin AB hukukunun uygulama alanı dışında bulunmasıdır²⁶⁴. Kanaatimizce istihbarat gereği veri işlemlerin gizlilik içerisinde yürütülmesi, kişisel verilerin işlenmesinde şeffaflık arayan AB'nin kişisel veri koruması amacı ile bağdaşmamaktadır²⁶⁵. Nitekim istihbarat faaliyetleri kapsamında bazen biyometrik veriler²⁶⁶ gibi özel nitelikli veriler de dâhil pek çok kişisel veri işlenmektedir, ancak Direktif bu faaliyetleri kapsam dışı bırakarak veri sahiplerini korunaksız bırakmaktadır. Belirtelim ki ulusal güvenlik kapsamında veri işleme faaliyetleri Kolluk ve Ceza Adaleti Direktifi'nin korumasından yararlanamasa da AIHS kapsamında bu veri işlemler de m. 8'in korumasından yararlanmaktadır.

Rotaru v. Romanya başvurusunda başvuru, uzun yıllar evvel Romanya'daki komünist rejime karşı bir protesto eylemine katıldığından cezalandırılmıştır. Romanya İstihbarat Teşkilatı başvuru hakkında fişleme yaparak başvuru kişinin radikal ve antisemitist bir grubun üyesi olduğuna dair lekeleyici ve içeriği yanlış bir dosya

²⁶² Semiz, **a.g.e.**, s. 70.

²⁶³ Semiz, **a.g.e.**, s. 81

²⁶⁴ Kızıllırmak, "Kişisel Verilerin İşlenmesinde Adli ve Önleyici Amaçla Öngörülen İstisnaların Ulusal ve Uluslararası Hukuka Göre Değerlendirilmesi", s. 243.

²⁶⁵ Gizlilik üzerine kurulu olan istihbarat, bilgi edinme ve ifade özgürlüğünü de kısıtlar mahiyettedir. İstihbari faaliyetlerin gizliliği ile şeffaflık ve hesap verilebilirlik arasındaki dengenin istihbaratın sivil gözetimi ile sağlanabileceğine dair bkz. Bayındır, **a.g.e.**, s. 33.

²⁶⁶ Örneğin FBI'nın biyometrik verilerden yararlanması oldukça eski bir tarihe dayanmaktadır. Kimlik Bölümü Ulusal Parmak İzi Deposu (*The National Fingerprint Repository in Identification Division-ID*) 1924 yılında faaliyetlerine başlamıştır. 1992 yılında ID'nin yerine Ceza Adalet Bilgi Hizmetleri Bölümü (*Criminal Justice Information Services Division-CJIS*) kurulmuş ve kolluk güçleri için ulusal ceza tarihi deposu oluşturulmuştur. CJIS bünyesindeki sistemlerden biri de Entegre Otomatik Parmak İzi Tanımlama Sistemi (*Integrated Automated Fingerprint Identification System-IAFIS*) olup bu sistem Ulusal Ceza Tarihi Kayıt Dosyası'nda (*National Criminal History Record File*) bulunan 71.8 milyondan fazla kişinin parmak izini arayan FBI'nın mevcut parmak izi tanıma sistemidir. Bkz. Darin R. Walker, "Biometric Technology in Law Enforcement", **Neurosurgery**, c. 71, s. 2, Ağustos 2012, s. 197.

oluşturmuştur²⁶⁷. Başvurucu ise ülkedeki rejim değişikliğinin ardından İçişleri Bakanlığına başvurarak hakkında yapılan fişlemeyi öğrenmiştir. Başvurucuya dosya içeriğindeki verilerin aksini ispat etmek olanağı verilmeksizin bu verilerin tutulması, kullanılması ve uzun yıllar boyunca sistematik olarak işlenmesi, özel yaşama müdahale teşkil etmektedir²⁶⁸. Yapılan fişleme, istihbarat faaliyeti kapsamında yapılmıştır. İstihbarat servislerinin bireyleri başvuru konusu olaydaki gibi âdeta gizlice gözetlemesi; demokratik bir toplumda katı ve gerekli güvencelerin varlığı, müdahalenin hukuka uygun olması ve m. 8/2 kapsamında bir müdahale nedeninin bulunması halinde hukuka uygundur²⁶⁹. Ancak başvuruya konu olayda Romanya'nın mevzuatı ulusal güvenlik gerekçesiyle verilerin gizli şekilde toplanması, kaydedilmesi ve arşivlenmesine izin verse de söz konusu kanunda; veri kategorileri, hangi durumlarda kişilerin verilerinin işleneceği, işleme prosedürü, verilerin muhafaza süresi, bu verilerin hangi halde kullanılabileceğine ilişkin bir hüküm bulunmamaktadır²⁷⁰ ve m. 8, müdahalenin hukuka uygun olmaması nedeniyle ihlal edilmiştir.

c. Ön Alan Soruşturmaları ve İstihbarat İlişkisi

Günümüzde kolluk güçlerinin suçla mücadelede önleyici faaliyette bulunması; polisin gelecekteki tehlike ve tehditleri önleyebilmesi için birtakım hazırlıklar yapmış olmasını gerektirmektedir. Bu hazırlıklardan biri de kamu düzenini tehdit eden somut bir tehlike bulunmaksızın kolluğun müdahale alanını öne çekerek veri toplamasıdır²⁷¹. *Ön alan araştırması*²⁷² olarak adlandırılan bu süreçte, kolluğun veri toplama tedbirleri gizli olup istihbarata yöneliktir²⁷³. Zira özellikle günümüzdeki teknolojik imkânlardan

²⁶⁷ *Rotaru v. Romanya*, B. No: 28341/95, 04.05.2000, para. 13 Çevrimiçi <https://hudoc.echr.coe.int/> 29.03.2020.

²⁶⁸ *Rotaru v. Romanya*, para. 44 ve 46.

²⁶⁹ *Rotaru v. Romanya*, para. 47-48.

²⁷⁰ *Rotaru v. Romanya*, para. 57.

²⁷¹ Ramazan Karabulut, “Kişisel Verilerin Korunması ve Kolluk Hizmetleri”, **Dicle Üniversitesi Sosyal Bilimler Enstitüsü**, Yayınlanmamış Yüksek Lisans Tezi, Diyarbakır, 2014, s. 87.

²⁷² *Birtek* istihbarat amaçlı iletişimin denetlenmesi ve bu minvalde istihbari tedbirlerin suçun ortaya çıkmadığı ancak işlenmesi muhtemel suçlar bakımından uygulama alanı bulduklarından bahisle bunlar hakkında “suç önleyici tedbir” kavramının kullanılmasını önermiştir. Bkz. Fatih Birtek, “İstihbarat Amacıyla İletişim Özgürlüğüne Müdahale Edilmesi ve Müdahaleden Elde Edilen Materyallerin Delil Olarak Kabul Edilebilirliği”, **CHD**, c. 6, s. 16, Ağustos 2011, s. 110.

²⁷³ Karabulut, **a.g.e.**, s. 88.

yararlanarak örgüt faaliyeti çerçevesinde işlenen suçlar bakımından gerekli istihbaratın toplanması sayesinde henüz suç işlenmeden illegal oluşumlardan önde hareket ederek kamu düzeninin bozulmasının önüne geçilebilmektedir²⁷⁴.

Suç işlendiğine dair herhangi bir şüphe veya somut bir tehlike²⁷⁵ durumunun olmadığı ancak suçun önlenmeye çalışıldığı evreye doktrinde *ön alan* denilmektedir²⁷⁶. Ön alan; ceza soruşturmasını başlatacak basit şüphe bulunmadığı için savcının yapacağı incelemeden önceki aşama olup ayrıca kolluğun somut bir tehlike önleme faaliyetlerinden de farklı bir aşamadır²⁷⁷. Savcının soruşturma evresini başlatmasının mümkün olmadığı bu evrede bilgi toplamak mümkündür²⁷⁸. Örneğin PVSK'nin gelecekteki tehlikeleri önleyebilmek amacıyla öngördüğü polis tedbirleri, *ön alan araştırmaları* kavramını oluşturmuştur. Bu araştırmalar kapsamında da kolluk kuvvetlerinin bilgi edinme, saklama ve analiz etme yetkileri bulunmaktadır²⁷⁹. Yani tehlikenin ortadan kaldırılmasından ziyade tehlikenin önlenmesi için kolluk *ikincil nesil standart tedbirler* kullanarak kişisel veri toplamakta ve bu verileri analiz etmektedir²⁸⁰.

Ön alan araştırmaları; önleyici kolluk, ceza muhakemesi ve istihbarat faaliyetleri arasında net bir noktada bulunmadığı için bu evrede yetkinin kimde olduğu tartışmalıdır. Örneğin İtalya'da uyuşturucu madde ticareti, terörizm, kara para aklama gibi gizli soruşturma yöntemlerinin kullanıldığı suçlarda Terörle Mücadele Kanunu ve İstihbarat Hizmetlerinin Yeniden Düzenlenmesine İlişkin Kanun hükümlerine göre

²⁷⁴ Birtek, **a.g.e.**, s. 101.

²⁷⁵ Somut tehlikeyi *Özbek/Doğan/Bacaksız*, makul ve genel yaşam tecrübesine göre yakın zamanda kamu güvenliği ve kamu düzeninde bir zararın meydana geleceğine dair beklenti olarak tanımlamıştır. Bkz. Veli Özer Özbek, Koray Doğan, Pınar Bacaksız, **Ceza Muhakemesi Hukuku**, 12. Baskı, Ankara, Seçkin Yayıncılık, 2019, s. 151.

²⁷⁶ Bu terminolojiyi kullanan eserler için bkz. Özbek, Doğan, Bacaksız, **a.g.e.**, s. 149; Feridun Yenisey, Ayşe Nuhoglu, **Ceza Muhakemesi Hukuku**, 7. Baskı, İstanbul, Seçkin Yayıncılık, 2019, s. 276. *Yenisey/Nuhoglu*, polis hukukunun düzenlenmesini gerektiren tehlikenin önlenmesi ve bastırılmasını beyaz alan, suç işlendikten sonra başlayan ceza muhakemesini siyah alan, bunların arasında kalan ön alan araştırmalarını ise gri alan olarak sınıflandırmıştır. Yenisey, Nuhoglu, **a.g.e.**, s. 276.

²⁷⁷ Feridun Yenisey, "Ön Alan Araştırmaları", **Dünyada ve Türkiye'de Ceza Hukuku Reformları Kongresi**, c. 1, Ed. Adem Sözüer, İstanbul, On İki Levha Yayıncılık, 2013, s. 94.

²⁷⁸ Yenisey, "Ön Alan Araştırmaları", s. 92.

²⁷⁹ Yenisey, Nuhoglu, **a.g.e.**, s. 277.

²⁸⁰ Yenisey, **Kolluk Hukuku**, s. 346.

polis ve istihbarat birlikte çalışmaktadır ki bu durum, ön alan araştırmaları ile kişisel verilerin işlenmesinde temel haklara ciddi bir müdahale teşkil etmektedir²⁸¹.

Bilgi elde etmenin amaçlandığı ön alan araştırması evresinde kolluk güçleri kimi zaman özellikle organize suçlulukla mücadelede ceza muhakemesi sürecinden daha fazla etkinliğe sahip olmaktadır²⁸². Zira özellikle organize suçluluk ve gizli örgüt yapılanması ile mücadele ön alan araştırması ile mümkündür²⁸³ ki bu evrede örgüt yapısı hakkında bilgi toplanıp değerlendirilerek organizasyon tasfiye edilebilsin²⁸⁴. Bu yüzden doktrinde bazı yazarlarca her suç bakımından değil, ancak organize suçluluk bakımından ön alan araştırmalarının yapılması gerektiği ileri sürülmüştür²⁸⁵. Zira ön alan evresinde kolluğun sahip bulunduğu “önleyici adli” yetkiler ile her birey hakkında suç işleyeceği ihtimaline binaen bilgi toplandığında kişisel veri toplama tehlikesi ortaya çıkacaktır²⁸⁶.

Kolluk güçlerinin ön alan araştırması yetkileri kanuna dayanmalıdır. Türk hukukunda AY m. 13’ün bir gereği olarak temel hak ve özgürlüklere müdahaleye izin veren bu yetki pek tabii kanuna dayanmalıdır. Türk hukukunda ön alan araştırmasında yetkinin, CMK m. 161 ve 164’ün varlığı nedeniyle kanuna dayandığı düşünülebilirse de henüz bir suç işlendiği şüphesi bulunmadığından CMK hükümleri uygulama alanı bulmayacaktır. Dolayısıyla savcı ve adli kolluğun araştırma faaliyeti bu alanda bulunmadığından kişisel verilerin korunması hakkı ve özel yaşamın gizliliğine saygı hakkına yapılan bu türden müdahaleler hukuka aykırı olacaktır²⁸⁷.

d. Türk Hukukunda İstihbarat Faaliyetleri Gereği Veri İşlemeler

²⁸¹ Orlandi, **a.g.e.**, s. 144.

²⁸² Özbek, Doğan, Bacaksız, **a.g.e.**, s. 152.

²⁸³ Özbek, Doğan, Bacaksız, **a.g.e.**, s. 155; *Yenisey/Nuhoğlu*, ceza muhakemesindeki resen araştırma ilkesi gereği soruşturma başlamazdan evvel incelemenin zorunlu olduğunu vurgulamışsa da kanaatimizce ön alan soruşturmasındaki bu araştırmaların gerekçesi re’sen araştırma olmayıp önleme faaliyetindeki kamu düzeninin korunmasındaki temel amaçlardır. Bkz. Yenisey, Nuhoğlu, **a.g.e.**, s. 277.

²⁸⁴ Özbek, Doğan, Bacaksız, **a.g.e.**, s. 156.

²⁸⁵ Özbek, Doğan, Bacaksız, **a.g.e.**, s. 157.

²⁸⁶ Yenisey, “Ön Alan Araştırmaları”, s. 95; *Yenisey*, ön alan araştırmalarında kolluğun yetkilerini “önleyici adli görev” niteliğinde olduğunu ifade etmiştir.

²⁸⁷ Alman Saksonya Eyalet Anayasa Mahkemesi’nin verdiği bir kararda da kanun koyucunun ceza muhakemesinde ve önleyici faaliyetlerinde sonradan denetlenemeyen, objektif koşulları olmayan açık yetkilendirmeleri veremeyeceği belirtilmiştir. Bkz. Özbek, Doğan, Bacaksız, **a.g.e.**, s. 152-153.

Emniyet Teşkilatı Kanunu uyarınca yapılan idari, siyasi ve adli polis ayrımında siyasi polisin faaliyetleri, doktrinde kolluk faaliyetleri arasında sayılmamaktadır. Zira siyasi polisin amacı kamu düzeninin sağlanması değildir²⁸⁸. Dolayısıyla siyasi polisin kişisel veri işleme faaliyetleri Kolluk ve Ceza Adaleti Direktifi'nin uygulama alanında değildir. Ancak idari polisin suç işlenmesinin önlenmesi için yürüttüğü veri işleme faaliyetleri ise örneğin PVSK ek m. 7 gereği dinleme ve teknik araçla takip yetkisi çerçevesinde veri işleme faaliyeti Kolluk ve Ceza Adaleti Direktifi kapsamındadır. Yani devletin varlığını dıştan ve içten gelen saldırılara karşı korumak ve sürdürmek için giriştiği “gizli polis” faaliyetleri²⁸⁹ ve bu faaliyetler çerçevesinde kişisel veri işlemesi ceza muhakemesi ve kolluk faaliyetleri dışında bulunmaktadır ve bu veri işlemeye Kolluk ve Ceza Adaleti Direktifi ve KVKK uygulanmayacaktır.

2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu (MİT Kanunu) uyarınca Anayasa'da sayılan devletin temel niteliklerine ve demokratik hukuk devletine yönelik ciddi bir tehlikenin bulunması halinde, devletin güvenliğinin sağlanması, casusluk faaliyetlerinin ortaya çıkarılması, devlet sırrının ifşasının tespiti, terörist faaliyetlerin önlenmesi için telekomünikasyon yoluyla iletişim denetlenebilir²⁹⁰. Bu denetim kapsamında iletişimin tespiti, dinlenmesi, kayda alınması veya sinyal bilgilerinin değerlendirilmesi bulunmaktadır. İstihbari amaçla uygulanan bu tedbirin sona ermesi halinde dinlemenin içeriğine ilişkin kayıtlar en geç on gün içinde yok edilir²⁹¹.

MİT Kanunu m. 6/11'de sınırları belirsiz bir yetki bulunmaktadır. Buna göre *“Önleyici istihbarat elde etmek ve analiz yapmak amacıyla kanuni düzenlemelerle bağlı olmaksızın MİT mensupları, MİT'te görev alan veya görev almak üzere başvuranların yurt dışında veya yabancılar tarafından gerçekleştirilen, ankesörlü telefonlarla gerçekleştirilen iletişimi tespit edilebilir, dinlenebilir, sinyal bilgileri değerlendirilebilir, kayda alınabilir.”* Bu hal bakımından kayıtların ne kadar süre ile muhafaza edileceği, hangi hallerde silineceğine ilişkin hiçbir düzenlemenin olmayışı

²⁸⁸ Özge Okay Tekinsoy, “Kolluk”, **İdare Hukuku**, Ed. Turan Yıldırım, Güncelleştirilmiş 7. Baskı, İstanbul, On İki Levha Yayıncılık, 2018, s. 478.

²⁸⁹ Lütfi Duran, **İdare Hukuku Ders Notları**, İstanbul, Fakülteler Matbaası, 1982, s. 253.

²⁹⁰ MİT Kanunu m. 6/2.

²⁹¹ MİT Kanunu m. 6/5.

istihbarat gerekçesine dayanılarak kişisel verilerin korunması hakkını korunaksız bırakmaktadır.

Düzenlemenin yalnızca MİT'te görev alan veya görev almak üzere başvuran kimseleri ilgilendirmesi hasebiyle en azından kişilerin göreve, kişisel verilerin korunması hakkına müdahale edileceğini peşinen bilmeleri ve bunu kabullenerek başlamaları nedeniyle kabul edilebilir olduğu düşünülebilir. Ancak MİT çalışanı da olsa kişilerin görevle ilgili olmayan bir yaşam alanları bulunmaktadır ve bu alanda gerçekleşecek iletişim de korunmaya muhtaçtır. Ayrıca fıkra da herhangi bir suçun önlenmesi ya da personelin liyakatini tespit amacı da bulunmamaktadır, yalnızca genel olarak “önleyici istihbarat ve analiz” gerekçelerine yer verilmiştir. En azından bu fıkra gereği işlenen iletişim verilerinin tutulma süresi öngörülmelidir, aksi halde personelin görevi sona ermesine rağmen bu veriler tutulmaya devam edecektir.

MİT, “*kamu kurum ve kuruluşları, kamu kurumu niteliğindeki meslek kuruluşları, 5411 sayılı Bankacılık Kanunu kapsamındaki kurum ve kuruluşlar ile diğer tüzel kişiliği bulunsun bulunmasın kuruluşlardan bilgi, belge, veri ve kayıt temin edebilir ve bu kuruluşların arşivleri, elektronik bilgi işlem merkezi ve iletişim alt yapısından yararlanabilecektir. Talepte bulunulanlar da kendi mevzuatlarındaki hükümleri gerekçe göstererek bu talebin yerine getirilmesinden kaçınamayacaktır*”²⁹². Kişisel veri talep ve temin etme konusunda ayrıcalıklı olan MİT, ayrıca uhdesindeki veriler bakımından da korunaklı olup istihbari nitelikte bilgi, belge, veri ve kayıtlar ile yapılan analizler TCK'de yer alan *Devlet Sırlarına Karşı Suçlar ve Casusluk* hükümleri hariç olmak üzere adli mercilerce istenmeyecektir²⁹³.

İstihbarat faaliyetlerinin özel doğası gereği gizlilik, gerek istihbarat çalışanı personel gerekse de yürütülen istihbarat faaliyeti için bir hayli önemlidir. Bu nedenle Türk hukukunda kanun koyucu da genel kişisel veriler için sağladığı korumanın ötesinde düzenlemeler öngörmüştür. Örneğin MİT mensubu ve ailelerinin kimlik, görev ve faaliyetleri kişisel veridir ve bu kişisel verilerin ifşası TCK m. 136 gereği

²⁹² MİT Kanunu m. 6/1-b.

²⁹³ MİT Kanunu ek m. 1/1.

değil; MİT Kanunu m. 27/2²⁹⁴ uyarınca cezalandırılmaktadır. Hatta MİT Kanunu m. 27/3 gereği bu verilerin medya aracılığıyla yayımlanması, yayınlanması ve açıklanması halinde Basın Kanunu ve 5651 sayılı Kanun uyarınca sorumlular ve verileri yayanlar da cezalandırılmaktadır.

MİT mensubu kişi ölmüş olsa dahi bu suç işlenebilir. Kişinin ölümü ile kişilik hakkı sona erdiğinden kişisel verilerin korunması hakkından yararlanamayacağı düşünülebilir. Zira MİT Kanunu'nda kişinin ölümünden sonra da bu bilgilerinin korumadan yararlanabileceğine dair bir hüküm bulunmamaktadır. Ancak m. 27/2 ve m. 27/3 ile korunan hukuki değer MİT mensubunun kişilik hakkı değil, MİT'in istihbarat faaliyetlerinin gizlilik içinde yürütülmesidir²⁹⁵. Ayrıca suçun konusu yalnız MİT mensubunun verileri değil, ailesinin verileri de olabilir. Örneğin bir haberde MİT mensubunun ailesinin kimliğine ilişkin bilgilerin yer alması ve haber içeriğinde MİT mensubunun resmi kıyafet içindeki fotoğrafına yer verilmesi ailesinin tanınmasına da sebebiyet verebilir.

Bu meyanda ifade özgürlüğü ile ilgili AİHM'nin *The Observer ve The Guardian v. Birleşik Krallık* kararı da değerlendirilmelidir. Emekli olan ve Avustralya'da yaşayan Bay Wright, Birleşik Krallık'ta MI5 istihbarat servisinde çalıştığı döneme ait Spycatcher isimli bir kitap yazmıştır. Kitapta MI5'in illegal operasyonel işleyişi ve bilgi toplama yöntemlerine ait bilgiler vermiştir²⁹⁶. Kitaptaki bazı bölümlerden alıntılar başvuru gazetelerde yer almış ve gazetelere ihtiyati tedbir uygulanmıştır. Hükümet'in ihtiyati tedbir gerekçesi, meslek sırrını ifşa eden emekli istihbarat mensubundan doğrudan ya da dolaylı olarak elde edilecek bilgilerin yayımlanmasının önlenmesidir²⁹⁷. Ancak Spycatcher ABD'de dahi yayımlanmış bir kitaptır, yani piyasaya açılmıştır. Başvurucuların gerekçesi ise müdahalede acil toplumsal gereksinim olmadığıdır, zira istihbarat servisinin illegal faaliyetine dair

²⁹⁴ “MİT mensupları ve ailelerinin kimliklerini, makam, görev ve faaliyetlerini herhangi bir yolla ifşa edenler ile MİT mensuplarının kimliklerini sahte olarak düzenleyen veya değiştiren ya da bu sahte belgeleri kullananlara üç yıldan yedi yıla kadar hapis cezası verilir.”

²⁹⁵ Ömer Özmen Baştürk, **Milli İstihbarat Teşkilatı'na Ait Bilgi, Belge ve Kimliklere Karşı Suçlar**, Ankara, Adalet Yayınevi, 2019, s. 114.

²⁹⁶ *The Observer ve The Guardian v. Birleşik Krallık*, B. No: 13585/88, 26.11.1991, para. 11 Çevrimiçi <https://hudoc.echr.coe.int/> 29.03.2020.

²⁹⁷ *The Observer ve The Guardian v. Birleşik Krallık*, para. 67.

iddialar kamu için önemlidir ve zaten Bay Wright'ın meslek sırrını ifşa etmesi ile bu iddialar kamunun da malumu olmuştur. AİHM başvuru gazetelerin yayım faaliyetini iki tarihe ayırarak incelemiştir: 1986-30 Temmuz 1987 arasında gazeteler yalnızca Avustralya'daki duruşma ve MI5 hakkındaki iddialara ilişkin kamunun ilgisini çeken iki kısa haber yapmıştır²⁹⁸. Bu tarihler arasında Spycatcher yalnız Avustralya'da yayımlanmıştır. AİHM çoğunluğuna göre Bay Wright'ın istihbarat anılarına bu tarihlerde ulaşmak kolay olmadığı için başvuru gazetelerin haberlerinin ardından ihtiyati tedbire başvurulması demokratik bir toplumda gereklidir ve ifade özgürlüğünün ihlali değildir²⁹⁹. Ancak 14 Temmuz 1987'de ise kitap ABD'de yayımlanmış ve Bay Wright'ın anıları Birleşik Krallık'ta yaşayanlar bakımından da ulaşılabilir olmuştur³⁰⁰. Bu tarihten sonra gazetelerdeki tedbirin devam etmesi ise kamunun ilgisini çeken bir konuda bilgi verme hak ve görevine engel olmuştur ve m. 10 ihlal edilmiştir³⁰¹.

Kanaatimizce MİT mensubu ve ailesine ilişkin bir haber yapılması halinde, durumun ifade özgürlüğü kapsamında olup olmayacağı söz konusu AİHM kararı ışığında değerlendirilmelidir. MİT mensubunun ad soyad biçiminde kimliği veya ailesine ilişkin bilgi ve fotoğrafların yer aldığı haber, hâlihazırda toplumun malumu olan bir husus ise bu durumda basın özgürlüğü gündeme gelmelidir. Aileye tanınan koruma, bir birey olarak aile üyelerine veya aile kurumuna tanınan bir koruma değildir; aileden yararlanılarak MİT mensubunun ortaya çıkmaması için tanınan bir korumadır. Bu suçun ihdas amacı MİT mensubiyetine ilişkin hususların ifşa olmasının engellenmesidir, açıklanan husus kamunun malumu ise suç oluşmayacaktır³⁰². Ancak suçun konusunu oluşturan hususlar açıklanmış olmasına rağmen kitlelerce öğrenilmemişse ve basın yayım organları açıklanmış bu hususları geniş kitlelere ulaştırmak için fiili işlemiş ise suç oluşacaktır³⁰³.

Bireyin kendi kişisel verisi üzerinde tasarruf hakkı bulunmaktadır, yani birey bu verilerini yayabilir, açıklayabilir ve ifşa edebilir. Bu halde de hukuka uygunluk

²⁹⁸ *The Observer ve The Guardian v. Birleşik Krallık*, para. 61.

²⁹⁹ *The Observer ve The Guardian v. Birleşik Krallık*, para. 65.

³⁰⁰ *The Observer ve The Guardian v. Birleşik Krallık*, para. 66.

³⁰¹ *The Observer ve The Guardian v. Birleşik Krallık*, para. 69.

³⁰² Baştürk, **a.g.e.**, s.115.

³⁰³ Baştürk, **a.g.e.**, s.140.

sebebinden yararlanır ve kişisel verilerin yayılması ve ele geçirilmesi suçu oluşmaz. Ancak bu tasarruf hakkı MİT mensuplarına tanınmamıştır. Zira m. 27/5 gereği MİT mensubu kimliğini, görev ve faaliyetini ifşa ettiğinde bu, üçte bir oranında cezayı artıran bir haldir.

e. Güvenlik Soruşturmaları Gereği Veri İşlemeler

Kamu görevine başlarken veya kamu görevlisinin görevi sırasında gizli mahiyetteki bir veriye erişiminin uygun olup olmadığına ilişkin bir değerlendirme; özellikle istihbarat faaliyetleri, kolluk ve diğer ceza adalet faaliyetlerinde çalışacak personelin liyakatini tespit için gereklidir³⁰⁴. Bir kişi hakkında bir kurum ya da kuruluşun talebi üzerine, güvenlik ya da haber alma faaliyeti yürüten makamlarca belirli amaçlarla kullanılmak üzere rapor düzenlenmekte ve bu raporun makama iletilmesi ile güvenlik soruşturması süreci yürütülmektedir. Bu süreçte kişiye dair ceza mahkûmiyetinden sağlık verilerine kadar pek çok kişisel veri, ilgili makamlar arasında dolaşmaktadır³⁰⁵.

Güvenlik soruşturmaları; kamu hizmetine girişte ve atamalarda bazı hizmetlerin gerektirdiği gizlilik, kamu görevine atanacak personelin güvenilirliği ve ulusal güvenliğin sağlanması amacıyla hizmet etse de soruşturmanın sınırını haddinden fazla genişletmek, kişilerin maddi ve manevi varlığına tehdit oluşturabilmektedir³⁰⁶. Örneğin Türkiye’de 1990’lı yılların başında memuriyete girişte internetten yararlanılarak güvenlik soruşturmalarının denetimsiz bir şekilde yapılması, özel yaşamın gizliliğine oldukça zarar vermiştir³⁰⁷.

Türkiye’de Güvenlik Soruşturması Kanunu’na göre *gizlilik dereceli birimler, Genelkurmay Başkanlığı, Milli Savunma Bakanlığı, jandarma, emniyet, sahil güvenlik ve istihbarat teşkilatlarında çalıştırılacak kamu personeli ve ceza infaz kurumları ve tutukevlerinde çalışacak personel* hakkında güvenlik soruşturması yapılmaktadır³⁰⁸.

³⁰⁴ Kuloğlu, **a.g.e.**, s. 9.

³⁰⁵ Karabulut, **a.g.e.**, s. 80.

³⁰⁶ Küzeci, **a.g.e.**, s. 552.

³⁰⁷ Tezcan, **a.g.e.**, s. 18.

³⁰⁸ 4045 sayılı Güvenlik Soruşturması, Bazı Nedenlerle Görevlerine Son Verilen Kamu Personeli ile Kamu Görevine Alınmayanların Haklarının Geri Verilmesine ve 1402 Numaralı Sıkıyönetim

Ancak 676 sayılı KHK ve 7070 sayılı Kanun ile DMK m. 48'e hüküm eklenmiş ve "güvenlik soruşturması ve/veya arşiv araştırmasının yapılmış olması" tüm memuriyetlere atamada bir şart olarak belirlenmiştir. Güvenlik soruşturması ve arşiv araştırmasını yapacak makam ise Güvenlik Soruşturması ve Arşiv Araştırması Yönetmeliği³⁰⁹ m. 7'de MİT Başkanlığı, Emniyet Genel Müdürlüğü ve mahalli mülki idare amirlikleri olarak belirtilmiştir. Güvenlik soruşturması ve arşiv araştırmasının kapsamı ise kişinin kolluk ve istihbarat birimlerinde kaydının olup olmadığı bilgisinden, ahlak ve adaba uygun davranıp davranmadığı ve paraya düşkün olup olmadığı bilgisine kadar geniş ve belirsizdir³¹⁰. Oysa güvenlik soruşturmasında kullanılan kriterlerin hukuki ve nesnel olması gerekmektedir³¹¹.

Kişisel verilerin neredeyse sınırsız olarak işlenmesine imkân sağlayan güvenlik soruşturmaları son dönemde pek çok AYM kararına da konu olmuştur. *Fatih Saraman* başvurusunda başvurusunun adli sicil kaydı güvenlik soruşturması kapsamında idari makamla paylaşılmıştır. Başvurucunun adli siciline işlenen önceki mahkûmiyetine konu fiilin işlendiği sırada başvuru, suça sürüklenen çocuktur. Adli Sicil Kanunu'na göre de on sekiz yaşın altındaki kimselerle ilgili adli sicil kayıtlarının ancak bir soruşturma ve kovuşturma kapsamında Kanun'da sınırlı olarak sayılan kişiler ile paylaşılması mümkündür³¹². Başvurucunun adli sicil kaydı ise infaz ve koruma memuru olarak kamu görevine atanması öncesinde yapılan güvenlik soruşturmasında Emniyet Müdürlüğü tarafından atamanın yapılacağı Kocaeli Adli Yargı İlk Derece

Kanununda Değişiklik Yapılmasına İlişkin Kanun m. 1 ("Güvenlik Soruşturması Kanunu" olarak anılacaktır).

³⁰⁹ R.G. Sayısı: 24018, R.G. Tarihi: 12.04.2000.

³¹⁰ Bkz. Güvenlik Soruşturması ve Arşiv Araştırması Yönetmeliği m. 11 "a) Kimlik kontrolü, kimlik kayıtlarının doğruluk derecesi, uyrukluğ, geçmişte yabancı bir devletin uyrukluğuna girip girmediği, b) Genel kolluk kuvvetlerinin ve istihbarat birimlerinin arşivlerinde bilgiler bulunup bulunmadığı, adli sicil kaydının ve hakkında arama kaydı veya herhangi bir tahdidin olup olmadığı, c) Terör örgütlerine veya Milli Güvenlik Kurulunca Devletin milli güvenliğine karşı faaliyette bulunduğu karar verilen yapı, oluşum veya gruplara üyeliği, mensubiyeti veya iltisakının bulunup bulunmadığı ve 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanuna ve Atatürk ilke ve inkılaplarına aykırı davranıp davranmadığı, ç) Şeref ve haysiyetini ihlal edecek ve görevine yansıyacak şekilde kumara, uyuşturucuya, içkiye, paraya ve aşırı bir şekilde menfaatine düşkün olup olmadığı, ahlak ve adaba aykırı davranıp davranmadığı, d) Yabancılarla, özellikle hasım ve hasım olması muhtemel Devlet mensupları ve temsilcileriyle ilgili derecesinin iç yüzü ve nedeni" araştırılır.

³¹¹ Küzeci, **a.g.e.**, s. 551.

³¹² M. 10/3 "Onsekiz yaşından küçüklerle ilgili adli sicil ve arşiv kayıtları; ancak soruşturma ve kovuşturma kapsamında değerlendirilmek üzere Cumhuriyet başsavcılıkları, hâkim veya mahkemelerce istenebilir."

Mahkemesi Adalet Komisyonu ile paylaşılmış ve kişinin güvenlik soruşturması olumsuz sonuçlanmıştır³¹³.

Başvuruda, bahsi geçen güvenlik soruşturmasının kanuni dayanağı olarak gösterilen Güvenlik Soruşturması Kanunu'na göre güvenlik soruşturması ve arşiv araştırması sırasında başvurulacak dokümanlar sayılmıştır. Kişinin adli sicil bilgisine de soruşturma kapsamında başvurulurken, bu hususta temel başvuru kaynağı olmasına rağmen Adli Sicil Kanunu'na hiç atıf yapılmamıştır. Üstelik Güvenlik Soruşturması Kanunu'nda pek çok hususun düzenlenmesi bir yönetmeliğe bırakılmış ve güvenlik soruşturmasında toplanan kişisel verilerin süresiz bir biçimde muhafazası öngörülmüştür. AYM, özel yaşama saygı hakkının kanuna dayanma şartı bakımından noksan bulunması nedeniyle bu başvuruda ihlalin bulunduğu sonucuna varmıştır.

Güvenlik soruşturması konulu AYM'ye yapılan bir diğer bireysel başvuruda ise başvuru hakkında 2001 yılında terör örgütüne yardım ve yataklık fiili nedeniyle Adana 1. Devlet Güvenlik Mahkemesi, 4616 sayılı Kanun gereği davanın kesin hükme bağlanmasının ertelenmesine karar vermiştir. 2007 yılında da beş yıllık denetim süresi geçtiğinden kamu davasının ortadan kaldırılmasına karar verilmiştir³¹⁴. Bu karardan sonra da başvurucuya GBT kaydının iptal edildiği bilgisi verilmiştir. Başvurucunun 2012 yılında sözleşmeli ceza infaz kurumu şoförlüğü sınavını kazanması üzerine hakkında güvenlik soruşturması yürütülmüş ve soruşturma olumsuz sonuçlanmıştır. Başvurucu da silinmiş GBT kayıtlarının, yargı kararının ve mahkûmiyet içermeyen sicilinin süresiz olarak saklanmasının AY m. 20'ye aykırı olduğunu ileri sürmüştür³¹⁵. AYM incelemesinde; güvenlik soruşturması ve arşiv araştırmasına konu edilecek bilgi ve belgelerin, bunların elde edilme yöntemlerinin, ilgililerin bu bilgilere itiraz olanaklarının olup olmamasının, bilgilerin hangi hallerde silineceğinin ve ne süre ile muhafaza edileceğinin Güvenlik Soruşturması Kanunu ile düzenlenmediğini belirtmiştir³¹⁶. Bahsi geçen bu hususların bir yönetmelik ile düzenlenmiş olması da

³¹³ *Fatih Saraman* Başvurusu [GK], B. No: 2014/7256, 27.02.2019, para. 14-16 Çevrimiçi <https://www.anayasa.gov.tr/tr/kararlar-bilgi-bankasi/> 29.03.2020.

³¹⁴ *Turgut Duman* Başvurusu, B. No: 2014/15365, 29.05.2019, para. 9 Çevrimiçi <https://www.anayasa.gov.tr/tr/kararlar-bilgi-bankasi/> 29.03.2020.

³¹⁵ *Turgut Duman*, para. 18.

³¹⁶ *Turgut Duman*, para. 84-87.

kanunilik ilkesinin şartlarını sağlamadığından AYM özel yaşama saygı hakkının ihlal edildiği sonucuna varmıştır³¹⁷.

Bireysel başvuruya konu olaylar haricinde AYM, soyut norm denetimi yoluyla yalnız soruşturma ve kovuşturma makamlarının erişebileceği verilere, güvenlik soruşturması ve arşiv araştırması yürüten makamların da erişip erişemeyeceğini değerlendirmiştir. Güvenlik Soruşturması Kanunu'na göre kamu davasının açılmasının ertelenmesi ve hükmün açıklanmasının geri bırakılması kararları da dahil savcılık ve mahkemelerin kararlarını, güvenlik soruşturmaları kapsamında görevli birimler almaya yetkilidir³¹⁸. Ancak Kanunda bu verilerin ne amaçla kullanılacağına yer verilmemiştir. CMK uyarınca özel muameleye tabi olan kamu davasının açılmasının ertelenmesi ve hükmün açıklanmasının geri bırakılması kararlarına yalnızca soruşturma ve kovuşturma makamları, CMK'de belirtilen amaçlarla erişebilmektedir ve bu bilgiler adli sicil kaydında yer almayıp özel bir sisteme kaydedilmektedir³¹⁹. Kararların ne süre ile sınırlı olarak tutulacağı, güvenlik soruşturması ile görevli hangi makamların bu verilere erişebileceği, kişisel verilerin korunmasına dair hangi önlemlerin alınacağı ve veri sahibinin kişisel verilerin korunması hakkına ilişkin denetim yetkisinin bulunup bulunmadığı maddede belirtilmemiştir. Oysaki denetim yetkisinin sağlanabilmesi için veri sahibine veri işlemeye itiraz, sildirme ve düzeltme hakları tanınmış olmalı ve *“gelişigüzel fişlemek ve ‘sakıncalı’ sayılmak son derece kolay ve bunları değiştirebilmek ise hemen hemen imkânsız”* olmamalıdır³²⁰. Öngörülebilirlik ve belirliliğin bu denli sağlanamadığı bu maddeyi AYM iptal etmiştir³²¹.

KVKK m. 28 uyarınca istihbarat faaliyetlerde kullanılan kişisel verilerin korunması KVKK'nin kapsamı dışındadır. Ancak her iki başvuruda da belirtildiği üzere güvenlik soruşturmasına konu edilen kişisel verilerin Yönetmelik ile belirlenmesi, kişisel verilerin korunması hakkına ciddi bir müdahale oluşturmaktadır. AYM her iki başvuruda da değerlendirmesini özel yaşamın gizliliğine saygı hakkı

³¹⁷ Turgut Duman, para. 92.

³¹⁸ Güvenlik Soruşturması Kanunu m. 1/2.

³¹⁹ CMK m. 171/5, 231/13.

³²⁰ Bülent Tanör, **Türkiye'nin İnsan Hakları Sorunu**, 3. Baskı, İstanbul, BDS Yayınları, 1994, s. 36.

³²¹ Bkz. AYM, E. 2018/163, K. 2020/13, 19.02.2020, para. 18 Çevrimiçi <https://www.anayasa.gov.tr/tr/kararlar-bilgi-bankasi/> 29.05.2020

perspektifinden yapmışsa da bu hakka müdahalede kanunilik şartı sağlanmadığından isabetli olarak ihlal olduğuna hükmetmiştir. Nitekim soyut norm denetimi ile DMK m. 48/8 ile memuriyete atanma şartı olarak getirilen güvenlik soruşturması ve arşiv araştırmasını da AYM değerlendirmiştir. AYM değerlendirmesini iki boyutlu yapmıştır ve dayanaklar AY m. 128'e göre memuriyet ve kamu görevliliği atamalarının kanunla düzenlenmesi ve AY m. 20/3'te kişisel verilerin korunması hakkıdır³²². AYM, güvenlik soruşturması ve arşiv araştırması kanun ile memuriyete atanmada temel şartlar arasında sayılmışsa da soruşturma ve araştırmaya konu edilecek kişisel verilerin korunması için herhangi bir güvence sağlanmaması ve kullanılacak kişisel verilerin kanunla düzenlenmemesini AY'ye aykırı bularak DMK m. 48/8'i iptal etmiştir.

³²² Bkz. AYM, E. 2018/73, K. 2019/65, 24.07.2019, para. 163-164 Çevrimiçi <https://www.anayasa.gov.tr/tr/kararlar-bilgi-bankasi/> 29.03.2020.

İKİNCİ BÖLÜM

KOLLUK VE CEZA ADALETİ DİREKTİFİ'NDE YER ALAN SÜJELER

I. VERİ SAHİBİ

A. Tanım

Veri sahibi kimliği belirli veya belirlenebilir gerçek kişidir. Zira Avrupa Konseyi ve Avrupa Birliği düzeyindeki veri koruma düzenlemelerine göre veri sahibi ancak gerçek kişi olabilir¹.

Kolluk ve Ceza Adaleti Direktifi m. 6'da üye devletlerin iç hukuklarında veri sahipleri arasında bir tasnife gidilerek işlenecek kişisel verilerin ayrıma tabi tutulması öngörülmüştür. Haklarında kategorizasyona gidilecek veri sahipleri: bir suç işlediğine veya işlemek üzere olduğuna ilişkin ciddi gerekçe bulunanlar, hükümlüler, bir suçun mağduru ya da mağduru olabileceğine ilişkin kesin gerekçe bulunanlar, tanıklar, suça ilişkin bilgi sağlayabilecek diğer kişiler veya şüpheli, sanık ya da hükümlünün temasının bulunduğu ya da ilgili olduğu kişilerdir.

Bu ayrıma göre veri sahipleri şüpheli, sanık gibi ceza muhakemesinin zorunlu süjeleri olabileceği gibi bilirkişi, tanık gibi görüşü ve bilgisine başvurulacak kişiler de olabilecektir. Ayrımın nedeni WP29'un üye devletlere, şüpheli olmayan kişilerin

¹ AİHM tarafından kişisel verilerin korunması hakkının süjesinin kimler olabileceği *Bernh Larsern Holding ve diğerleri v. Norveç* başvurusunda değerlendirilmiştir. Tüzel kişi olan üç Norveçli şirketin başvurduğu bu davada kişisel verilerin korunması hakkının ihlali özel yaşamın gizliliğine saygı hakkı çerçevesinde değil, konuta saygı hakkı ve haberleşmeye saygı hakkı alt kategorilerinde değerlendirilmiştir. Diğer iki alt kategori bakımından hak süjesi olabilen tüzel kişilerin kişisel verilerin korunması hakkında süje olamaması ise doktrinde eleştirilmiştir. Bkz. Gülay Arslan Öncü, “Özel Yaşama ve Aile Yaşamına Saygı Hakkı”, **Anayasa Mahkemesine Bireysel Başvuru El Kitapları Serisi-8**, 2019, Çevrimiçi https://www.anayasa.gov.tr/media/5604/ozel_yasam_hakki.pdf 30.03.2020, s. 81; Doktrinde tüzel kişiye ait bir veri, gerçek kişinin belirlenmesini mümkün kılıyorsa, tüzel kişiye ait verinin de gerçek kişinin kişisel verilerin korunması hakkından yararlanacağı ifade edilmiştir. Bkz. Zeynel T. Kangal, **Kişisel Verilerin Ceza ve Kabahatler Hukukunda Korunması**, İstanbul, On İki Levha Yayıncılık, 2019, s. 28; Sedat Erdem Aydın, **AİHM İçtihatları Bağlamında Kişisel Verilerin Kaydedilmesi Suçu**, İstanbul, On İki Levha Yayıncılık, 2015, s. 9.

kişisel verilerinin işlenmesinde dikkatli davranılması ve suça karışmayan kişilerin haksız muameleye maruz bırakılmaması için özel şartlar ve güvencelere uyulmasına ilişkin tavsiyesidir². Ayrım, referans kolaylığı sağlayarak verileri sınıflandırmaya hizmet etmektedir. Ancak bu ayrımın, veri sahiplerinin suça ilişkilerine bağlı olarak kişisel verilerine uygulanacak koruma standardının düşmesine yol açabileceğinden endişe edilmiştir³. Kanaatimizce ceza muhakemesinde şüpheli veya sanığın işlemlere katlanma yükümlülüğü mağdur, tanık gibi süjelere göre daha fazladır. Koruma tedbirlerinin uygulanması sırasında da şüpheli veya sanığın ya da hükümlünün bu süreçte gündeme gelen kişisel verilerinin de mağdur veya tanığa göre daha uzun süre saklanması gibi farklı düzeyde kişisel veri korumasına tabi tutulması mümkündür. Bu nedenle şüpheli veya sanık için kişisel verilerin işlenmesinin farklı hukuki düzenlemeye tabi tutulması hukuka uygun olup masumiyet karinesini ihlal etmemektedir.

Kolluk ve Ceza Adaleti Direktifi'ne ilişkin teklif metninde çocuk tanımı yapılmış olsa da yürürlüğe giren metinde çocuk tanımı yer almamış ve veri sahibinin çocuk olması halinde özel düzenlemelere yer verilmemiştir⁴. Oysa GDPR'da bilgi toplumu hizmetlerinden yararlanacak çocuğun kişisel verilerinin işlenmesinde rızasına m. 8'de sayılan şartlarla sonuç bağlanmıştır. Özellikle ceza muhakemesi sürecinde çocukların korunmasına ilişkin daha incelikli haller bulunmakta iken çocukların kişisel verilerinin de bu kapsamda ayrıca korunması, özel işleme şartlarına tabi tutulması kanaatimizce daha isabetli olurdu.

² Salami Emmanuel Akintunde, "The Impact of Directive (EU) 2016/680 on the Processing of Personal Data by Competent Authorities for The Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties and On the Free Movement of Such Data on the Existing Privacy Regime", Çevrimiçi <http://dx.doi.org/10.2139/ssrn.2912449> 10.04.2019, s. 4.

³ Bkz. Murat Volkan Dülger, Onur Özkan, "Adli ve Kolluk Teşkilatında Kişisel Verilerin Korunması: 'Unutulan' Direktifin Kapsamlı ve Karşılaştırmalı Analizi", **CHD**, c. 15, s. 42, 2020, s. 97; Akintunde, **a.g.e.**, s. 4; Lauri J. Pajunoja, "The Data Protection Directive on Police Matters 2016/680 Protects Privacy-The Evolution Of EU's Data Protection Law and Its Compatibility With The Right To Privacy", **University of Helsinki**, Yayımlanmamış Yüksek Lisans Tezi, Helsinki, 2017, s. 58.

⁴ Bilişim ve Teknoloji Hukuku Enstitüsü, **Avrupa Parlamentosu ve Konseyi'nin 2016/680 sayılı ve 27 Nisan 2016 Tarihli Kişisel Verilerin Yetkili Otoritelerce Suçların Önlenmesi, Soruşturulması, Ortaya Çıkarılması veya Kovuşturulması veya Cezaların İnfazı Amacıyla İşlenmesiyle İlgili Gerçek Kişilerin Korunmasına ve Bu Verilerin Serbest Dolaşımına İlişkin ve 2008/977/JHA sayılı Konsey Çerçeve Kararı'nı Yürürlükten Kaldıran Direktif Hakkında Bilgi Notu**, İstanbul Bilgi Üniversitesi, İstanbul, 2019, s. 8.

B. Veri Sahibinin Hakları

Kişisel verilerin korunması ile esas olarak toplama, kayıt, saklama, kullanma ve yok etme gibi tüm veri işleme süreçlerinde, veri sahibinin denetim hakkının sağlanması amaçlanmaktadır⁵. Kolluk ve Ceza Adaleti Direktifi m. 12-18 arasında veri sahibine tanınan haklar sayılmıştır. Ancak veri sahibine tanınan veri koruma düzeyi yalnız Direktif'in bu maddeleri ile sınırlı düşünülmemelidir. Zira Kolluk ve Ceza Adaleti Direktifi m. 1/3'e göre AB üyesi devletler, veri sahibinin hakları bakımından bu Direktif'in öngördüğü korumayı aşar biçimde düzenleme yapabilecektir. Yani Kolluk ve Ceza Adaleti Direktifi, mevcut veri koruma mevzuatından daha üstün bir korumayı da hedeflemiştir⁶.

GDPR'nın veri sorumlusunun yükümlülüklerini artırması sonucu, veri sahibinin veriye erişim hakkı, düzeltme hakkı, itiraz etme haklarına ek olarak unutulma hakkı ve veri taşınabilirliği⁷ hakları getirilmiştir⁸. AB'nin kişisel verilerin korunmasına ilişkin yaklaşımı bireylerin bu hakkından efektif şekilde yararlanması için spesifik haklar ihdas etmeye yöneliktir. Ancak aşağıda inceleneceği üzere veri sahibine tanınan haklar, mutlak haklar değildir. Zira bu haklara GDPR'nın veri korumasındaki gibi başvurulduğunda polis ve ceza adalet faaliyetlerinin işlerliğine ket vurulacaktır⁹. Bu nedenle veri sahibinin haklarının kullanımının sınırlandırılması; kamu yararı, üçüncü

⁵ Elif Küzeci, **Kişisel Verilerin Korunması**, 4. Baskı, İstanbul, On İki Levha Yayıncılık, 2020, s. 14.

⁶ Akıntunde, **a.g.e.**, s. 3; Örneğin Kolluk ve Ceza Adaleti Direktifi bağlamında suçun ortaya çıkarılması amacıyla veri sahibinden DNA örneği alınması için veri sahibinin rızası gerekmemektedir. Ancak Kolluk ve Ceza Adaleti Direktifi resital m. 35'e göre AB üyesi devletler mevzuatlarında DNA örneği alınmasını veri sahibinin rızasına bağlayabilecektir; Korkmaz, **a.g.e.**, s. 242-243. Ancak bu hükmün AB üyesi devletler arasında farklı veri koruma düzeylerine yol açarak Direktifin amaçlarından biri olan AB içinde etkin işbirliği ve veri aktarımını engelleyebileceği ileri sürülmüştür. Bkz. Thomas Marquenie, "The Police and Criminal Justice Authorities Directive: Data Protection Standards and Impact on the Legal Framework", **Computer Law and Security Review**, c. 33, 2017, s. 329.

⁷ Veri taşınabilirliği hakkı (*right to data portability*) GDPR'da işlemenin rızaya dayandığı, otomatik araçlarla gerçekleştirildiği veya sözleşmenin kurulması veya ifası için gerekli olduğu hallerde bu verileri, başka bir veri sorumlusuna aktarma hakkıdır. Direktif bu hakka yer vermediğinden çalışmamızda incelenmemiştir.

⁸ Seçkin Koçer, Avrupa Genel Veri Koruma Tüzüğü Işığında Kişisel Verilerin Korunması Kanununda Verisi İşlenen Kişinin Hakları, **Türk Yargısının Adli ve İdari Kapasitesinin Güçlendirilmesi Projesi Kapsamında Hakim ve Cumhuriyet Savcılarınca Hazırlanan Yüksek Lisans Tezleri**, Ed. Zeliha İnce, Adalet Bakanlığı Avrupa Birliği Genel Müdürlüğü, Ankara, 2018, s. 508.

⁹ Paul De Hert, Vagelis Papakonstantinou, "The New Police and Criminal Justice Data Protection Directive: A First Analysis", **New Journal of European Criminal Law**, c. 7, s. 1, Tilburg, 2016, s. 12.

kişilerin hak ve özgürlükleri, soruşturmanın gizliliğinin korunması nedenlerine dayanabilir. Ancak unutulmamalıdır ki ne olursa olsun bu sınırlamalar hakkın sağladığı korumayı tamamen bertaraf edecek mahiyette olmamalıdır¹⁰.

1. Bilgilendirilme Hakkı

a. Tanım

Bilgilendirilme hakkı¹¹, kişisel verilerin işlenmesinde veri sorumlusuna yüklenen aydınlatma yükümlülüğünün veri sahibine bir hak olarak yansımasıdır. Kişi, ancak kişisel verilerinin işlendiğini ve kendisine hangi hakların tanındığını biliyorsa, haklarını gerçek manası ile kullanabilecektir¹². Kamu kurum ve kuruluşları faaliyette bulunurken pek çok kişisel veri işlemektedirler. Bir hukuk devletinde de veri sahibinin, hangi kamusal makamlar tarafından hangi verisinin işlendiğini bilmeyi talep etmesi, idarenin hesap vermesi ve veri işlemede şeffaflığın sağlanması bakımından gereklidir¹³. Bilgilendirme, veri sorumlusu tarafından haklarını kullanabilmesi için veri sahibine yapılır. Veri sahibine yapılacak bilgilendirme, Kolluk ve Ceza Adaleti Direktifi m. 12/1 uyarınca *anlaşılır, özlü ve kolay erişilebilir* bir formda olmalıdır. Zira bu sayede veri sahibine yapılacak bildirim fiilen bilgilendirilme hakkının gereğini sağlamış olacaktır¹⁴.

Veri sorumlusunun veri sahibinin erişimine sunacağı bilgiler, asgari olarak:

¹⁰ Gülşah Bostancı Bozbayındır, “Avrupa Birliği Ceza Hukuku’nda Polis ve Ceza Adaleti Otoritelerine Yönelik 2018/680 Sayılı Direktif: Kişisel Verilerin Ceza Adalet Mekanizmalarında Korunmasına Getirilen Standartlar ve Direktife Yönelik Eleştiriler”, **GSÜHFD**, c. 17, s. 2, 2018, s. 79.

¹¹ Çalışma kapsamında bilgilendirilme hakkı olarak zikrettiğimiz bu hak, ilk kez OECD’nin 23 Eylül 1980 tarihli Mahremiyetin Korunması ve Kişisel Verilerin Sınır Ötesi Akışına Dair Rehber İlkeleri’nde *bireysel katılım ilkesi* olarak hakkında veri toplanan kişinin veri sorumlusu aracılığıyla veya başka biçimde kendisini ilgilendiren verilerin mevcut olup olmadığını öğrenme ve bu verileri kolayca anlayabileceği biçimde öğrenme olduğu ifade edilmiştir. Bkz. Ahmet Boz, “Kişisel Verilerin Korunması: Türkiye, ABD ve AB Örnekleri”, **Polis Akademisi Güvenlik Bilimleri Enstitüsü**, Yayımlanmamış Yüksek Lisans Tezi, Ankara, 2014, s. 40; Türk hukuku bakımından da bu usuli hak, bilgi edinme hakkı olarak özel yaşama saygı hakkının alt kategorisi olup Anayasa m. 17 ve 20 ile bağlantılı bir haktır. Bkz. Arslan Öncü, “Özel Yaşama ve Aile Yaşamına Saygı Hakkı”, s. 317.

¹² Küzeci, **a.g.e.**, s. 248; Hüseyin Murat Develioğlu, **6698 Sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku**, İstanbul, On İki Levha Yayınları, 2017, s. 83; Ayşe Çiğdem Ayözger, **Kişisel Verilerin Korunması**, İstanbul, Beta Yayıncılık, 2016, s. 44.

¹³ Boz, **a.g.e.**, s. 18.

¹⁴ İbrahim Korkmaz, **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, Güncellenmiş 2. Baskı, Ankara, Seçkin Yayıncılık, 2019, s. 244-245.

- (a) *veri sorumlusunun kimliği ve iletişim bilgisi*
- (b) *varsa veri koruma görevlisinin iletişim bilgisi*
- (c) *kişisel verinin işleme amacı*
- (d) *veri sahibinin kişisel verisine erişim, düzeltme, silinme veya işlemenin sınırlandırılmasını talep hakkıdır*¹⁵.

Bu hakkın kapsamında; GDPR’ın aksine veri sahibine sunulacak ilk bilgiler arasında veri işlemenin hukuki dayanağı ve veri işleme ile hedeflenen meşru menfaat bulunmamaktadır¹⁶. Adli makamların kişisel veri işleme faaliyetleri düşünüldüğünde veri işleme ile hedeflenen meşru menfaat, genellikle kamu güvenliği ve kamu yararına ilişkin olacağından ilk aşamada adli makamların buna ilişkin bilgilendirme yapmasının beklenmemesi kanaatimizce isabetlidir. Ancak her ne olursa olsun veri işlemenin hukuki dayanağı muhakkak veri sahibine bildirilmelidir. Zira veri sahibi bu sayede hukuka aykırı biçimde verisinin işlendiği kanaatindeyse Koluk ve Ceza Adaleti Direktifi’nde öngörülen diğer haklarını kullanabilecektir.

b. Ek Bilgilendirilme Hakkı

Bilgilendirmenin kapsamı, veri işlemenin amacı ve veri sahibinin haklarının hatırlatılması ile sınırlı değildir, veri sahibinin ek bilgilendirilme hakkı da bulunmaktadır. Bu ek bilgilendirilme hakkı:

- (a) *veri işlemenin hukuki dayanağı,*
- (b) *verinin muhafaza süresi, bu süre veri sahibine bildirilemiyorsa sürenin tespitinde başvurulacak ölçütler*
- (c) *verinin yurtdışına aktarımı halinde veri alıcılarının kategorisi*
- (d) *gerekli olması halinde özellikle veri sahibinin bilgisi dışında kişisel verinin toplandığı halde ek diğer bilgilerden oluşmaktadır*¹⁷.

Ek bilgilendirilme hakkının kapsamı (d) bendinden anlaşılacağı üzere sınırlı değildir. Ancak ayrımcılık mahiyetinde olmayan bir profillemeye yapıldığında bu türden

¹⁵ Bkz. Kolluk ve Ceza Adaleti Direktifi m. 13/1.

¹⁶ Dülger, Özkan, **a.g.e.**, s. 109.

¹⁷ Kolluk ve Ceza Adaleti Direktifi m. 13/2.

bir otomatik karar alma mekanizması işleminin gerekçesinin ek bilgilendirilme hakkı kapsamında olmaması eleştirilmiştir¹⁸. Ayrıca kişisel verilerin büyük veri uygulamalarına kaynaklık etmesi halinde bu uygulama da veri sahibinin bilgilendirilme hakkı kapsamındadır. Zira büyük veri doğası gereği pek çok kaynaktan beslenir ve genellikle büyük veriyi oluşturan kişisel veriler, doğrudan veri sahibinden alınan veriler olmayıp başka kanallar aracılığıyla toplanır. Veri sahibinin verilerinin ne amaçla ve nasıl işleneceğini öngörebilmesi bakımından ek bilgilendirme kapsamında veri sahibi bu husustan da haberdar edilmelidir¹⁹.

c. Ek Bilgilendirilme Hakkının Sınırlandırılması

Adli makamların veri işleme faaliyetlerinde bilgilendirilme hakkı mutlak olsaydı; soruşturmanın gizliliği ihlal edilerek kolluk ve ceza adaleti faaliyetleri sekteye uğrayabilecek, istihbarat tehlikeye düşebilecek ve diğer kişilerin özel nitelikli kişisel verilerinin ifşası söz konusu olabilecekti. Bu nedenle bu hakkın bazı hallerde sınırlandırılabilmesi düzenlenmiştir²⁰. Bu türden bir sınırlama yapılması için öncelikle üye devletin iç hukukunda hangi veri işleme kategorilerinin tamamen veya kısmen sınırlamaya konu olabileceği düzenlenmelidir. Üye devletler, iç hukuklarında ek bilgilendirme kapsamında olan verilerin, gerçek kişilerin temel hak ve özgürlükleri ve meşru menfaatleri için demokratik bir toplumda gerekli ve orantılı olması halinde veri

¹⁸ Dülger, Özkan, **a.g.e.**, s. 110.

¹⁹ Şehriban İpek Aşıkoğlu, **Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri**, İstanbul, On İki Levha Yayıncılık, 2018, s. 157.

²⁰ Bostancı Bozbayındır, **a.g.e.**, s.70; David Allen, Evelien van Beek, John Borking, **Practical Guide on the Use of Personal Data in the Police Sector**, Council of Europe, Strasbourg, 2018, s. 6; Kolluk ve Ceza Adaleti Direktifi'nin ihdasından önceki dönemde Başalp'e göre ise suçların önlenmesi gerekçesiyle bilgilendirilme hakkının sınırlandırılmasının genişletici yoruma tabi tutulmamalı, yalnız sınırlamanın zorunlu olması karşısında hukuki düzenlemenin ratio legis'ine uygun şekilde sınırlama yapılmalıdır. Bkz. Nilgün Başalp, **Kişisel Verilerin Korunması ve Saklanması**, Ankara, Yetkin Yayınları, 2004, s. 53; Nitekim AİHM de kişisel verilere ilişkin bilgilendirilme hakkının mutlak olmadığı kanaatindedir. Örneğin *Segerstedt-Wiberg ve diğerleri v. İsveç* (B. No:62332, 06.09.2006) başvurusunda, başvuruçular terörle mücadele kapsamında polis tarafından tutulan kişisel verileri ile ilgili bilgilendirilmemiştir. Ancak "*Ulusal güvenlik ve terörle mücadeleye ilişkin ulusal çıkarların, başvuruçuların Güvenlik Polisi dosyalarında kendileri hakkında tutulan bilgilerin tam kapsamına erişmeye ilişkin çıkarlarının üstünde olduğuna kanaat getirmiştir.*" Akt. Murat Volkan Dülger, **Kişisel Verilerin Korunması Hukuku**, 2. Baskı, İstanbul, Hukuk Akademisi, 2019, s. 72.

sahibine yapılacak bilgilendirmeyi sınırlayacak, engelleyecek veya erteleyecek müdahalelerde bulunabilecektir²¹. Bu müdahalenin amaçları sınırlı sayı prensibince:

- (a) *idari ve adli soruşturma ve kovuşturmaların engellenmesini önlemek,*
- (b) *suçların önlenmesi, ortaya çıkarılması, soruşturulması, kovuşturulması ya da cezanın infazının engellenmesini önlemek,*
- (c) *kamu güvenliğinin korunması*
- (d) *ulusal güvenliğin korunması*
- (e) *üçüncü kişilerin hak ve özgürlüklerinin korunması* olarak sayılmıştır.

Anlaşılaçağı üzere bu amaçlar, Kolluk ve Ceza Adaleti Direktifi'nin ihdas amaçları ile neredeyse birebir örtüşmektedir. Suçların önlenmesi, ceza muhakemesi ve cezaların infazı amacı ile işlenen kişisel verilere sağlanan korumanın aynı gerekçelerle; iç hukukta düzenleme bulunması şartıyla veri sahibine ek bilgi verilmesini sınırlandırması, kanımızca ek bilgilendirilme hakkının sınırlarını veri sahibinin menfaati aleyhine devletlerin takdir yetkisine bırakmaktır²².

2. Erişim Hakkı

a. Tanım

Erişim hakkı bilgilendirilme hakkının tamamlayıcısı olup veri sahibinin; arada herhangi bir adli ya da idari makam olmaksızın makul aralıklarla veri sorumlusuna doğrudan başvurarak²³ kişisel verilerinin işlenip işlenmediğini öğrenmesini, işlenen verilerden hangilerine ilişkin bilgilendirileceğini öğrenmesini ve bunlara erişmesini

²¹ Kolluk ve Ceza Adaleti Direktifi m. 13/3.

²² Kolluk ve Ceza Adaleti Direktifi m. 13/3'teki bu istisnanın veri sahibinin bilgilendirilme hakkını büyük ölçüde kısıtladığına dair bkz. Akıntunde, **a.g.e.**, s. 7; Korkmaz, **a.g.e.**, s. 245.

²³ Kural olarak arada bir makam olmaksızın doğrudan erişim mümkün olmalıdır, ancak doğrudan erişim mümkün olmadığında veri sahibi erişim talebini denetleyici makama iletir. Makam, veri sahibinin kişisel verilerinin işlenmesinin hukuka uyarlığı ile ilgili kontrolleri yapacaktır. Denetleyici makam hangi verilerin açıklanabileceğini, bunun sınırlamalara tabi olup olmadığına dair veri sahibine cevap verecektir. Bkz. Allen, van Beek, Borking, **a.g.e.**, s. 7.

sağlayan bir haktır²⁴. Erişim hakkı, kişisel verinin düzeltilmesi ve silinmesini talep hakkı başta olmak üzere diğer hakların kullanılabilmesi için ön şarttır²⁵.

Veri sahibinin erişim hakkını kullanması halinde kendisine verilecek bilgiler:

- (a) *veri işleminin amaçları ve kanuni dayanağı*
- (b) *ilgili kişisel veri kategorileri*
- (c) *kişisel verilerin sunulduğu veri alıcıları veya alıcı kategorileri, özellikle üçüncü ülkelerdeki veya uluslararası kuruluşlardaki alıcılar*
- (d) *mümkünse, kişisel verilerin saklanacağı öngörülen süre veya mümkün değilse, o dönemi belirlemek için kullanılan kriterler*
- (e) *veri sorumlusuna karşı kullanılacak kişisel verilerin düzeltilmesini veya silinmesini veya veri sahibiyle ilgili kişisel verilerin işlenmesinin kısıtlanmasını talep etme hakkının varlığı*
- (f) *denetim makamına şikâyetle bulunma hakkı ve denetim makamının iletişim bilgileri*
- (g) *işlenmekte olan kişisel verilerin ve bunların kaynağına ilişkin mevcut bilgilerden oluşmaktadır*²⁶.

b. Erişim Hakkının Sınırlandırılması

Erişim hakkı da bilgilendirilme hakkı gibi mutlak olmayan bir haktır. Bilgilendirilme hakkının sınırlandırılması şartları ile aynı olarak erişim hakkına da müdahale edilmesi mümkündür. Ancak veri sahibinin erişim hakkı sınırlandığında veya erişim talebi reddedildiğinde, bu durum veri sahibine gecikmeksizin nedenleri ile birlikte yazılı biçimde bildirilecektir. Söz konusu sınırlama ya da erişim talebinin reddedilmesi nedeninin veri sahibine bildirilmesi, erişim hakkının sınırlandırılma veya reddedilmesi amaçlarına zarar verecekse, bu durumda veri sahibine bu bildirim de yapılmayacaktır. Ancak dikkat edilirse erişim hakkının sınırlandırılması ve erişim talebinin reddine dayanak yapılan idari soruşturmaların ve ceza soruşturmalarının

²⁴ Dülger, Özkan, **a.g.e.**, s. 111; Develioğlu, **a.g.e.**, s. 87; Saadet Yüksel, **Özel Yaşamın Bir Parçası Olarak Telekomünikasyon Yoluyla Yapılan İletişimin Gizliliğine Önleyici Denetimle Müdahale**, İstanbul, Beta Yayıncılık, 2012, s. 118.

²⁵ Allen, van Beek, Borking, **a.g.e.**, s. 6.

²⁶ Kolluk ve Ceza Adaleti Direktifi m. 14/1.

engellenmesini önlemek, kamu güvenliğini sağlamak gibi amaçlara²⁷ dayanarak, bir de veri sahibine yapılacak bildirimin ortadan kaldırılması, veri sahibinin bu hakkını fiilen kullanmasını oldukça güçleştirmektedir. Bu durumda Kolluk ve Ceza Adaleti Direktifi veri sorumlusunun veri sahibine sadece denetim makamına ve yargılama makamına başvurmasına ilişkin bilgi vermesini öngörmektedir.

Veri sahibine kişisel verisinin işlenip işlenmediği konusunda dahi bilgi vermemek; verisi eğer işlenmişse veri sahibinin kişisel verilerin sıhhatini ve kalitesini denetleme imkânını elinden almaktadır ve veri sahibini, kişisel verinin silinmesi ve düzeltilmesini talep haklarından da yoksun bırakmaktadır. Bu doğrultuda AİHM'nin *Leander v. İsveç* kararına değinilmelidir. Karara konu olayda, hakkındaki güvenlik soruşturması nedeniyle İsveçli bir marangoz olan başvurucunun askeri deniz üssü yakınında bulunan müzedeki işine son verilmiştir. Ancak başvurucu kendisine ilişkin güvenlik kayıtlarına, ulusal güvenlik gerekçesiyle ulaşamamaktadır. Başvurucuya ilişkin bilgi, güvenlik güçlerine ve kendisi hakkındaki güvenlik soruşturması için ilgili birime aktarılmıştır. Gizli bir polis sicilinde kişinin özel yaşamına ilişkin verilerinin işlenmesi ve başvurucuya bu kayıtlara dair aksini ispat imkânının verilmemesi m. 8'e bir müdahale olarak değerlendirilmiştir²⁸.

3. Kişisel Verinin Düzeltilmesi ve Silinmesini Talep Hakkı

a. Tanım

²⁷ Bkz. Kolluk ve Ceza Adaleti Direktifi m. 15/1.

²⁸ *Leander v. İsveç*, B. No: 9248/81, 26.03.1987, para. 48 Çevrimiçi <http://hudoc.echr.coe.int/eng?i=001-57519> 27.03.2020. Söz konusu başvuruda AİHM, kişinin bu kayıtlarına erişememesinin, m. 8'in ihlali olduğuna hükmetmemiştir. Ancak başvurucunun devlet koruması altında çocuk olduğu dönemde hakkında tutulan tıbbi kayıt ve polis kayıtlarına erişemediği *Gaskin v. Birleşik Krallık* (B. No. 10454/83, 07.07.1989) başvurusunda Komisyon, durumu *Leander* başvurusundan farklı bir mahiyette görmüştür (para. 39). Zira başvurucu, hakkında tutulan bu kayıtların *Leander* başvurusunun aksine aleyhine kullanıldığını iddia etmemiştir. Başvurucu hakkındaki kayıtlara erişememektedir ve bu nedenle m. 8'in ihlal edildiği iddiasındadır. AİHM de başvurucunun hakkında tutulan kayıtlara ancak kayıt tutan tüm kişilerin rızası ile başvurucunun erişmesine izin veren mevzuatın varlığının m. 8 bakımından devletin pozitif yükümlülüğünü ihlal edip etmediğini değerlendirmiştir (para. 41). AİHM pozitif yükümlülük kapsamında olmasa dahi çocuk bakım hizmetlerinin işleyişi için tutulan kayıtlarda, kamunun menfaati ve hakkında kayıt tutulan bireyin menfaati arasında denge olması gerektiğini belirtmiştir (para. 42-44). AİHM, başvurucunun ancak hakkında tutulan kayıtlara katkı sağlayan kırk altı kişinin tümünün rızası ile erişebilmesini ve rıza verilmemesi halinde otomatik olarak erişememesini m. 8'in ihlali olarak değerlendirmiştir. Zira orantılı bir müdahale değildir, ancak bağımsız bir denetim makamının bulunması halinde m. 8 ihlal edilmemiş olabilirdi (para. 49).

Veri sahibinin menfaatlerinin korunması, kişisel verinin işlenmesi ile sağlanmak istenen amacın gerçekleşmesi, özellikle önleyici kolluk faaliyetleri bakımından kamu düzenine karşı tehditlerin bertaraf edilmesi, ceza muhakemesi bakımından ise maddi gerçeğe ulaşılması için işlenen kişisel verilerin doğru ve güncel olması gerekmektedir. Kişisel verinin silinmesini talep hakkı kişisel verilerle ilgili uluslararası pek çok düzenlemelerde yer almaktadır. Örneğin 2002/58 sayılı Direktif'te kamu haberleşme şebekesi veya kamuya açık olan elektronik haberleşme hizmet sağlayıcılarının işlediği ve sakladığı kullanıcı ve abone bilgilerinin haberleşmenin sağlanması bakımından gerekli olmadığı hallerde silinmesi veya anonimleştirilmesine dair sildirme hakkına ilişkin özel düzenlemeye yer verilmiştir²⁹.

Kişisel verinin silinmesi, verinin veri sorumlusunun hâkimiyet alanından çıkarılmasıdır. Bunun yöntemi de kişisel veriyi ihtiva eden evrakın yok edilmesi, veri taşıyıcı CD, disket gibi aracın yok edilmesi veya veri sahibi ile ilişkilendirilmeyi sağlayan bilgilerin ayrıştırılarak yok edilmesi gibi çok çeşitli biçimlerde olabilir³⁰.

Verinin yanlış veya doğru olması, kişisel veri olma niteliğini etkilememektedir. Belirli veya belirlenebilir bir kişi ile ilişkilendirilebilmesi yeterlidir. Ancak şüphesiz yanlış bir kişisel verinin, veri sahibine zarar verme ihtimali bulunmaktadır ve bu halde de veri sahibi kişisel veri korumasından yararlanmaktadır³¹. Veri sorumlusunun işlediği kişisel verilerin muhtevasının yanlış olması halinde veri sahibinin verinin derhâl düzeltilmesini isteme hakkı bulunmaktadır. Bu hakkın gereği olarak üye devletler veri sahibine; veri sahibinin kişisel verilerin doğruluğu için ek beyanda bulunmasını sağlamak, doğru şekilde verinin eksikliğini tamamlamak ve yanlış hususun düzeltilmesi olanaklarını sağlamakla yükümlüdür³². Ayrıca GDPR'da yer alan yeniliğe paralel olarak veri sorumlusu, kendisine yöneltilen silinme talebini veriyi paylaşmış olduğu üçüncü kişilere de iletmekle yükümlüdür³³.

²⁹ 2002/58 sayılı Direktif m. 6/1.

³⁰ Başalp, **Kişisel Verilerin Korunması ve Saklanması**, s. 50.

³¹ Şeyma Sert, **Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması**, İstanbul, Seçkin Yayıncılık, 2019, s. 27.

³² Dülger, Özkan, **a.g.e.**, s. 112.

³³ Nilgün Başalp, "Avrupa Birliği Veri Koruması Genel Regülasyonu'nun Temel Yenilikleri", **MÜHF-HAD**, c.21, s.1, 2015, s. 93.

b. Silinmeye Alternatif Olarak İşlemenin Sınırlandırılması

Veri işlemenin sınırlandırılmasını talep hakkı, GDPR’da veri sahibinin başlı başına talep edebileceği bir haktır. Kolluk ve Ceza Adaleti Direktifi’nde ise işlemenin sınırlandırılması, başvuru yetkili makamın takdirinde olan ve muhtevası yanlış verinin ortadan kaldırılmasına ilişkin bir alternatiftir³⁴. Veri sahibi tarafından işlenen kişisel verilerin doğru olmadığı iddia edildiğinde ve kişisel verinin sıhhati tespit edilemediğinde veya kişisel verinin delil mahiyetinin bulunması halinde veri sorumlusu veriyi silmek yerine işlenmesini sınırlandırabilecektir.

İşlemenin sınırlandırılması ile sınırlandırılmak üzere bazı kişisel veriler işaretlenir ve bir süre işlenmez. Örneğin veri sahibi, kişisel verinin doğruluğuna itiraz ettiğinde, bu itirazın incelenmesine elverişli bir süre içinde işleme sınırlandırılacaktır veya veri sorumlusunun verilerin işleme amacına gereksiniminin sona ermesi, ancak bir hakkın kullanımı ya da menfaatin devamı için kişisel verinin varlığı gerekliyse, bu durumda işleme sınırlandırılacaktır³⁵.

İşlemenin sınırlandırılması kararı kaldırılırsa veri sahibinin haklarını kullanabilmesi için bu karar da veri sahibine bildirilmelidir. Ayrıca veri sahibi tarafından verinin doğru olmadığı iddiası üzerine verinin sıhhati tespit edilemediği için verinin işlenmesi sınırlandırılmışsa; veri sorumlusu tarafından sınırlandırmanın kaldırılmasından önce veri sahibi bilgilendirilecektir³⁶.

Silinmesi talep edilen verinin ceza muhakemesi sürecinde veya Kolluk ve Ceza Adaleti Direktifi’nin bir başka ihdas amacını sağlayabilmesi için sonraki süreçte kullanılabilme ihtimaline binaen saklanması gerekiyorsa, bu durumda da veri ayrı bir sisteme kaydedilerek verinin işlenmesi sınırlandırılabilir³⁷. Veri işlemenin

³⁴ 95/46 sayılı Direktif m. 12/1-b’de yer alan silinmeye alternatif olarak kişisel verinin engellenmesi hakkına ise Kolluk ve Ceza Adaleti Direktifi’nde yer verilmemiştir. Kişisel verinin engellenmesi halinde veri, veri sorumlusunun hâkimiyet alanında kalırken verilerle ilgili herhangi bir işlem yapılması engellenmektedir. Bkz. Başalp, **Kişisel Verilerin Korunması ve Saklanması**, s. 50. Verinin kalitesinin tartışmalı olduğu olduğu hallerde bu yöntemle veriyi muhafaza etmeye devam etmeye kanaatimizce Kolluk ve Ceza Adaleti Direktifi’nde yer verilmesi gerekirdi.

³⁵ Develioğlu, **a.g.e.**, s. 94.

³⁶ Kolluk ve Ceza Adaleti Direktifi m. 16/3.

³⁷ Dülger, Özkan, **a.g.e.**, s. 113.

sınırlandırılması, silinmesi talep edilen güncel olmayan veya içeriği yanlış olan söz konusu verinin hâlâ veri sorumlusu tarafından tutulacağı ve veri sahibinin haklarını ihlal edeceğinden bahisle eleştirilmiştir³⁸.

c. Kişisel Verinin Düzeltilmesi, Silinmesi veya İşlenmesinin Sınırlandırılması Hakkının Sınırlandırılması

Kişisel verinin düzeltilmesi, silinmesi veya işlenmesinin sınırlandırılmasını talep eden veri sahibinin bu talebinin reddedilmesi halinde, kural olarak veri sahibine ret sebebinin yazılı olarak belirtilmesi gerekmektedir. Ancak bu bilgi verme yükümlülüğü; üye devletin iç hukukunda kanuni düzenleme bulunması, reddin gerçek kişilerin temel hak ve meşru menfaatleri için demokratik bir toplumda gerekli olması halinde Kolluk ve Ceza Adaleti Direktifi m. 16/4 uyarınca kısmen veya tamamen ortadan kalkabilecektir. Kişisel verinin düzeltilmesi, silinmesi veya işlenmenin sınırlandırılması talebinin reddi halinde veri sahibine red sebebinin dahi bildirilmesine olanak sağlamayan bu madde veri korumasını sağlamamaktadır. Bilgilendirilme hakkı ve erişim hakkının sınırlandırılması bahsinde de belirttiğimiz üzere, Kolluk ve Ceza Adaleti Direktifi uyarınca yapılacak veri işleme faaliyetleri suçların önlenmesi, ceza muhakemesi ve cezaların infazı amacıyla gerçekleştirilmektedir. Yine bu amaçlara dayanarak³⁹ Kolluk ve Ceza Adaleti Direktifi'nin sağladığı veri korumasını kısmen veya tamamen kaldırmak izaha muhtaçtır.

d. Unutulma Hakkı ile İlişkisi

Her bireyin, insan onuru⁴⁰ ve kişisel özerklik gereği sınırlarını kendisinin belirlediği ve kendi kontrolünde olan bir alanı bulunmalıdır⁴¹. Bireyin maddi ve

³⁸ Akıntunde, **a.g.e.**, s. 8.

³⁹ Amaçlar için bkz. Kolluk ve Ceza Adaleti Direktifi m. 16/4.

⁴⁰ Birey hakkında söz gelimi sosyal medyada yer alan zarar verici bir verinin onun şeref ve saygınlığını tamamen yok etme potansiyelinin bulunması, unutulma hakkının esasen insan onurunun bir gereği olduğuna işaret etmektedir. Bkz. Aydın Akgül, “Kişisel Verilerin Korunmasında Yeni Bir Hak: ‘Unutulma Hakkı’ ve AB Adalet Divanı’nın ‘Google Kararı’”, **TBB Dergisi**, c. 27, s. 116, 2015, s. 20.

⁴¹ Eren Sözüer, **Unutulma Hakkı İnsan Hakları Hukuku Perspektifinden Bir İnceleme**, İstanbul, On İki Levha Yayıncılık, 2017, s. 11.

manevi varlığını koruyup geliştirebilmesi için geçmişi, geleceğine ket vurmamalıdır. Ancak kişisel verilerin işlendiği ilk andan sonra ileride kullanılabileceği düşüncesi ile ilanihaye tutulması, bireyin maddi ve manevi gelişimini engellemektedir⁴². Unutulma hakkı⁴³, silinmesini talep hakkı ile sıkı bir ilişki içinde olup bireylerin üçüncü kişilerin gözetiminden kurtulmasını sağlayan⁴⁴ ve dijital ortamda bulunan kişisel verilerin belirli bir süreden sonra silinmesini gerektiren ve kişisel verinin geleceğini belirleme hakkının bir görünümüdür⁴⁵. Zira bireyler, geçmişte hukuka uygun bir biçimde işlenmiş verilerine, zamanın geçmesi ile erişimin kaldırılmasını talep edebilmelidirler⁴⁶. Bireyin unutulma hakkı yönünde talepte bulunması üzerine veri sorumlusunun veriyi silme veya yok etme yükümlülüğü bulunmaktadır. Ancak bu kişisel verinin işlenmesinin zorunlu olması, ifade özgürlüğü kapsamında olması, veri işlemede kamu yararının bulunması halinde veri sorumlusunun bu talebi reddetmesi mümkündür⁴⁷.

Unutulma hakkı, teknolojik gelişmeler nedeniyle dijital ortamda işlenen verilerin varlığı da dikkate alınarak bazı yazarlarca analog çağda ve dijital çağda olmak

⁴² Aşıkoğlu, **a.g.e.**, s.178; Ramazan Karabulut, “Kişisel Verilerin Korunması ve Kolluk Hizmetleri”, **Dicle Üniversitesi Sosyal Bilimler Enstitüsü**, Yayınlanmamış Yüksek Lisans Tezi, Diyarbakır, 2014, s. 82; Kişisel verilerin belirli bir süre ile sınırlı olmak üzere tutulması, unutulma hakkının varlığına açıklayan baskın görüşün gerekçesidir. Bir diğer görüş ise kişinin “beyaz sayfa” açmasına olanak sağlanması gerektiğini savunan sosyal perspektifli görüştür. Diğer görüş ise bireyin bu hakkından faydalanarak maddi ve manevi gelişimini sağlaması gerekçesine dayanmaktadır. Murat R. Önok, “Kişisel Verilerin Korunması Bağlamında ‘Unutulma Hakkı’ ve Türkiye Açısından Değerlendirmeler”, **İKÜHFD**, c. 16, s. 1, 2017, s. 160.

⁴³ Kişisel verilerin korunması hakkı bağlamında unutulma hakkı oldukça yeni olsa da kavramsal ve felsefi olarak unutulma hakkı (*right to be forgotten*), bilginin silinmesi hakkı (*right to have information deleted*), bilinmeme hakkı (*right to oblivion*), toplumsal unutkanlık (*social forgetfulness*) biçiminde geçmişe eskiye dayanan bir haktır. Bkz. Tamer Soysal, Unutulma Hakkının Avrupa Birliği’nin Genel Veri Koruma Tüzüğü Çerçevesinde İncelenmesi”, **Uyuşmazlık Mahkemesi Dergisi**, Yıl 7, s. 13, Haziran 2019, s. 349, Önok, **a.g.e.**, s. 165.

⁴⁴ Akgül, “Kişisel Verilerin Korunmasında Yeni Bir Hak: ‘Unutulma Hakkı’ ve AB Adalet Divanı’nın ‘Google Kararı’”, s. 15. *Kangal*’a göre kişisel verinin silinmesini isteme hakkı, unutulma hakkının bir görünümüdür. Kangal, **a.g.e.**, s. 155.

⁴⁵ Ayözger, **a.g.e.**, s. 39-41; Bilginin geleceğini belirleme hakkı (*Informationelle Selbstbestimmung/right to informational self-determination*), Alman Anayasa Mahkemesi’nin Nüfus Sayımı Kararı ile ilk kez zikredilen bu kavram kişisel verilerin tümüyle işlenmesi gizliliğin ihlali olduğu ve bu nedenle özel bir gerekçeye ihtiyaç duyduğu esasına dayanmaktadır. Bkz. Veli Özer Özbek, Koray Doğan, Pınar Bacaksız, **Ceza Muhakemesi Hukuku**, 12. Baskı, Ankara, Seçkin Yayıncılık, 2019, s. 177; Cemil Kaya, **Assessing the Transfer of Personal Data in the European Union in the Light of the Data Protection Directive**, İstanbul, On İki Levha Yayınevi, 2011, s. 14.

⁴⁶ Eren Sözüer, **a.g.e.**, s. 8.

⁴⁷ Akgül, “Kişisel Verilerin Korunmasında Yeni Bir Hak: ‘Unutulma Hakkı’ ve AB Adalet Divanı’nın ‘Google Kararı’”, s. 18.

üzere ikiye ayrılarak incelenmiştir: Analog unutulma hakkı, bireyin resosyalizasyonuna hizmet eden bir hak olup cezası infaz edilmiş hükümlüler başta olmak üzere bireylerin geçmişleri ile yargılanmamalarını ifade etmektedir. Dijital ortamdaki unutulma hakkı ise çevrimiçi unutulma hakkı ve sildirme hakkı ile ilişki içinde incelenmektedir⁴⁸. Çevrimiçi unutulma hakkı, analog unutulma hakkının internetteki görünümü olup birey hakkında yeni yayınlar yapılmasını ve mevcut verilerin sıralı olarak sunulmasını engellemektedir⁴⁹.

Unutulma hakkının, kişisel verinin silinmesini talep hakkı⁵⁰ ile ilişkisine gelindiğinde bu iki hak birbirine bir hayli benzemekle birlikte, çevrimiçi unutulma hakkının konusu aktif biçimde oluşturulan bilgi yani içerik iken; verinin silinmesini talep hakkının konusu ise pasif biçimde dış dünyada tezahür eden veri sahibinin kendisine dair oluşturduğu bilgidir. Çevrimiçi unutulma hakkı, geçmişteki bilginin yayılmasına; verinin silinmesini talep hakkı ise verinin toplanmasına ve işlenmesine ilişkindir. Kullanıldığı takdirde bilginin yayılmasına engel olabilecek çevrimiçi unutulma hakkı, ifade özgürlüğüne müdahale teşkil edebilecekken verinin silinmesini talep hakkı ise tutulan verilere ilişkin olduğundan ifade özgürlüğüne müdahale söz konusu olmayacaktır⁵¹.

⁴⁸ Bkz. Eren Sözüer, **a.g.e.**, s. 23 vd; GDPR ile online ortamda arama motorlarından kişisel veriler içeren arama sonuçlarının çıkarılması hakkını aşar biçimde unutulma hakkının değerlendirilmesi gerektiği ifade edilmiştir. Bkz. Soysal, **a.g.e.**, s. 365; Unutulma hakkının yalnız internetteki verileri kapsadığı görüşü için bkz. Can Yavuz, **İnternetteki Arama Sonuçlarından Kişisel Verilerin Kaldırılması Unutulma Hakkı**, Ankara, Seçkin Yayıncılık, 2016, s. 54.

⁴⁹ Esas olarak çevrimiçi unutulma hakkının analog unutulma hakkından farkı, bireye dair eski haber ve bilgilerin devamlı ve süre sınırı olmaksızın erişilebilir olmasının yarattığı sakıncayı gidermektir. Eren Sözüer, **a.g.e.**, s. 30-31.

⁵⁰ Eren Sözüer'e göre verinin silinmesini sağlama hakkı kişisel verilerin korunması hukukuna özgü bir terminoloji olup sildirme hakkından farklıdır. Verinin silinmesini sağlama hakkı, veri sahibinin kendisine ait verilerin silinmesini talep etmesine hizmet etmektedir. Bkz. Eren Sözüer, **a.g.e.**, s. 35; GDPR öncesi unutulma hakkı, 95/46 sayılı Direktif'te yer almamakta ancak Direktif m. 12'de veri sahibi kişisel verisine erişim hakkından yararlanırken işlenen verisinin eksik, yanlış olması halinde veri sorumlusundan kişisel verisinin düzeltilmesi, silinmesi ve engellenmesi talebinde bulunabilmesi çerçevesinde değerlendirilmekteydi. Bkz. Soysal, **a.g.e.**, s. 364.

⁵¹ Eren Sözüer, **a.g.e.**, s. 40; Unutulma hakkının pozitif boyutunun bireyin geçmişini kontrol etme, kendisine dair belirli hususların geçmişinden silinmesini ve hatırlanmamayı isteme olduğu, negatif boyutunun ise kişinin kendisi hakkındaki verilerin, üçüncü kişilere kullanmamasına veya hatırlanmamasına dair yükümlülük anlamına geldiği ve unutulmayı isteme hakkını içerdiği ifade edilmiştir. Bkz. Akgül, "Kişisel Verilerin Korunmasında Yeni Bir Hak: 'Unutulma Hakkı' ve AB Adalet Divanı'nın 'Google Kararı'", s. 18.

Kişisel verilerin muhtevasının doğru olmaması halinde sildirme ve işlemenin sınırlandırılması alternatifleri haricinde yine de veri kullanılacaksa veri koruma hukukuna göre bu verinin düzeltilmesi gerekmektedir. Bu da veri sahibinin verisinin düzeltilmesini talep hakkı ile mümkün olabilir, ancak unutulma hakkı bu haktan ayrılmaktadır. Unutulma hakkının konusu olan içerik ise hâlihazırda doğru bilgidir, ancak kişinin geleceğine yön verebilecek mahiyette olduğundan “geçmişte kalan bu bilginin unutulması” talep edilmektedir.

GDPR m. 17’de sildirme hakkı, unutulma hakkını kapsar biçimde düzenlenmiştir⁵². Ancak unutulma hakkı ve veri işlemeye itiraz hakkı Kolluk ve Ceza Adaleti Direktifi’nde bulunmamaktadır. Kolluk ve Ceza Adaleti Direktifi’nde yer alan veri silinmesini talep hakkı da unutulma hakkının gereklerini sağlayamamaktadır. Zira unutulma hakkı içeriği doğru ya da yanlış belirli bir zaman sonra verinin ortadan kaldırılmasını hedeflerken⁵³, verinin silinmesini talep hakkı ise hukuka aykırı veri işleme halinde veri sahibinin veri sorumlusundan verinin silinmesini talep etmesini sağlamaktadır. Yani verinin silinmesini talep hakkı, sürelilik ilkesi çerçevesinde verinin gerekli olan süreden fazla işlenmemesi ve saklanmamasını temin etmektedir. Unutulma hakkı ise dar manada en azından kişinin internet üzerindeki verilerinin kaldırılmasını, yok edilmesini temin etmektedir. Unutulma hakkının ileri sürülebileceği kimseler veri sorumlusu ve üçüncü kişilerdir ki genellikle çevrimiçi unutulma hakkı gözetildiğinde arama motorları bu hakkın yükümlüsüdür⁵⁴.

Kolluk ve Ceza Adaleti Direktifi’nde unutulma hakkının bulunmaması, büyük bir eksikliktir ve kişinin özellikle kriminal geçmişinin yaşamını etkilememesi ve insanlar tarafından ayrımcılığa maruz kalmaması için unutulma hakkı temin edilmelidir⁵⁵. Hatta unutulma hakkı yalnız kişinin geçmişinde yer alan ve onu zor

⁵² Soysal, **a.g.e.**, s. 365.

⁵³ Önok, **a.g.e.**, s. 166; Yavuz, **a.g.e.**, s. 54.

⁵⁴ Önok, **a.g.e.**, s. 168; Yavuz, **a.g.e.**, s. 55.

⁵⁵ Ayözger, **a.g.e.**, s. 39; Çalışmamız kapsamında özel kişiler tarafından kolluk ve adli makamların işlediği kişisel verilerin kullanılması yer almamaktadır. Ancak unutulma hakkı en çok da bu hususta, özel kişiler tarafından ceza adalet makamlarının verilerinin kullanılması ve veri sahibinin bir türlü “unutulmaması” nedeniyle gündeme gelmektedir ve kişinin kriminal geçmişi, cezası infaz edilmiş olsa dahi tabiri caizse ayaklarına dolanabilmektedir. İspanya’daki bir olayda “...Gençlik yıllarında kamusal alanda idrarını yaptığı için para cezasına çarptırılmış lise müdürü... üzerinden otuz beş yıldan fazla zaman geçmesine rağmen bu olay, cezanın yayımlanmış olduğu İspanyol resmi gazetesinin internet ortamına aktarılması ile günümüze taşınmıştır. Genel erişime açık bilgilerin [olayda mahkûmiyet]

durumda bırakabilecek bilgiler için değil, genel olarak artık erişilmesini istemediği her türlü veri için söz konusudur⁵⁶. Örneğin cinsel saldırı suçunun mağduru olmuş bir kişinin, mağdur olduğuna dair verinin unutulmasını istemesi gayet olağandır.

Özellikle veri sahibinin işlediği bir suçla ilişkin haberlerin yapılması, kamu yararına hizmet ettiğinden unutulma hakkı, ifade özgürlüğü ve basın özgürlüğü ile yarışmaktadır ve bu durumda şüpheli, sanık, suçtan zarar gören yahut yargılamada başka bir süje olan suçla ilişkili veri sahibinin kişisel verilerinin nasıl korunacağı tartışmalıdır. Unutulma hakkını kullanmak isteyen veri sahibinin, üçüncü kişiler ile ilişkilerinde bu kişilerin meşru menfaati de söz konusu olabilir⁵⁷. Örneğin daha evvel cinsel istismar suçundan mahkûm olmuş ve cezası infaz edilmiş ancak bir kreşte çalışmak için başvuran kişiye dair bu bilginin “unutulmamış” olması üçüncü kişilerin menfaatinedir. Ancak kanaatimizce kişi hakkında yalnız soruşturma yürütülmüş ve kamu davası açılmamışsa bu halde unutulma hakkından yararlanması kabul edilebilirdir.

Unutulma hakkı ve bu hakla yarışan diğer hak ve menfaatler Türk hukukundan birkaç örnek verilerek değerlendirilmelidir. Yargıtay HGK’nın unutulma hakkını ele aldığı bir kararında⁵⁸, cinsel taciz iddiasıyla yürütülen ceza yargılamasında müşteki hükmü temyiz etmiştir. Yargıtay’ın temyiz incelemesi, daha sonra bir ceza hukuku kitabında müştekinin ismi ve karardaki diğer kişilerin isimleri ile birlikte açıkça zikredilmiştir. Bunun üzerine müşteki, kişilik hakkına saldırı olduğu iddiasında bulunmuştur. Ancak davalılar, kitabın geniş kitlelere hitap etmediği ve bilimsel eser mahiyetinde olan kitabın AİHS sisteminde ifade özgürlüğünün uzantısı olarak bilim ve sanat özgürlüğü kapsamında bulunduğunu ileri sürmüşlerdir.

Yargıtay 4. HD, öncelikle adı geçen kitapta davacının adının herhangi bir kodlama olmaksızın yer almasının kitap içeriğine faydasının bulunmadığını belirtmiştir. Ancak bilim özgürlüğünün de sınırsız olmadığı ve kişilik haklarıyla

erişilebilirliğinin artması, bu bilgilerin ifşa olma riskini de artırmaktadır.” Kişi hakkındaki mahkûmiyet kararının aradan geçen otuz beş yıla rağmen “unutulmaması” buna örnektir. Bkz. Eren Sözüer, a.g.e., s. 18.

⁵⁶ Önok, a.g.e., s. 166.

⁵⁷ Önok, a.g.e., s. 166-167.

⁵⁸ Yargıtay HGK, E.2014/56, K.2015/1679, 17.06.2015 Çevrimiçi <http://www.kazanci.com/kho2/ibb/giris.html> 29.03.2020.

yarıştığında somut olaya göre koruma altına alınan diğer hak ve özgürlüğün de öncelenebileceğini belirtmiştir. Oysa bilim özgürlüğü, yani hakkın kullanılması ve iddia edilen haksızlık arasında “mantıki bağ” bulunmalı, yani cinsel taciz mağdurunun isim bilgisinin verilmesi, eserin bilimselliğine katkıda bulunmalıdır. Ancak HD, bu hususu göz ardı etmiştir⁵⁹. Yerel mahkemenin direnmesi üzerine HGK ise kitapta ismi geçen kişi lehine kişilik hakkı ihlal edildiği gerekçesiyle manevi tazminata hükmetmiştir. Kararda çarpıcı nokta, unutulma hakkının kişisel verilerin korunması hakkının esası olduğudur. Zira her iki hakkın temelinde de bireylerin kişisel verileri üzerinde serbestçe tasarruf edebilmesi, geçmişine bağlı kalmaksızın geleceğini dizayn edebilmesi ve kişisel verilerinin aleyhine kullanılmasının engellenmesi bulunmaktadır. Kararda HGK, unutulma hakkının yalnız dijital kişisel veriler için değil, bu hakkın diğer haklarla ilişkisi gözetilerek genel olarak özel yaşamın gizliliğinin korunması için de temin edilmesi gereken bir hak olduğu sonucuna varmıştır⁶⁰.

AYM’nin dijital ortamda unutulma hakkını ele aldığı bir başvuruda⁶¹ da unutulma hakkı ile kamu yararı ve basın özgürlüğü yarışması değerlendirilmiştir. Başvurucunun uyuşturucu kullandığı iddiası ile yargılandığı ceza davasında adli para cezasına mahkûm olmasına ilişkin olay ve 1998-1999 yıllarına ait haberler, bir gazetenin internet arşivinde hala mevcuttur. Başvurucu, internet sitesinde bulunan haberlerin şeref ve haysiyetini ve mahremiyetini zedelediğini iddia ederek içeriğe erişimin kaldırılmasını talep etmiştir, ancak talebi reddedilmiştir. Zira kişinin kimlik bilgisinin internet ortamında hukuka uygun olarak işlenmesi ancak açık rıza veya kanuna dayanma şartı ile mümkündür. Ancak ifade ve basın özgürlüğü kapsamında yapılan bir haber buna istisna olabilir. Geçmişte haber yapılmış ve gerçeğe aykırılığı doğrulanmamış bir habere ve kişisel veriye internet ortamında erişimin engellenmesi,

⁵⁹ Önok, **a.g.e.**, s. 177.

⁶⁰ HGK’nin azınlıkta kalan üyeleri, kitapta yer verilen mahkeme kararındaki ismin kodlanmasına gerek olmadığını, zira yargılamanın aleniliği ilkesi uyarınca hüküm alenen tefhim edilmişken bu kararın kitapta yer almasının özel yaşamın gizliliğini ihlal etmediğini savunmuşsa da çoğunluk, hukuki sorunun mahkeme kararında ismin kodlanmaksızın yer alması olmayıp isme açık halde kitapta yer verilmesinin gerekli olup olmadığına ilişkin olduğunu belirtmiştir.

⁶¹ NBB Başvurusu, B. No: 2013/5653, 03.03.2016 Çevrimiçi <https://www.anayasa.gov.tr/tr/kararlar-bilgi-bankasi/> 29.03.2020.

kişilerin yaptıklarının unutulmasını sağlamaktadır⁶². Günümüzde internetin yaygın kullanımı kişinin geçmişte yaptığı ve hatırlanmasını istemediği hususların karşısına çıkmasını kolaylaştırmış, bu da basın özgürlüğü ve şeref ve haysiyetin korunması hakkı arasındaki dengeyi bozmuştur. Dengenin gözetilmesi ise unutulma hakkının temini ile mümkündür⁶³. Aksi durumda internet aracılığıyla kolayca ulaşılabilen ve uzun süre saklanabilen kişisel veriler, bireylerin ön yargılara maruz kalmasına neden olacak ve manevi varlığını geliştirmesine engel olacaktır⁶⁴. Kararda haber ile kişi arasında ilişki kuran kişisel verinin silinmesi, haberin anonim hale getirilmesi, haber içeriğinin bir kısmına erişimin engellenmesi gibi yöntemler ile unutulma hakkının sağlanabileceği belirtilmiştir⁶⁵. Başvuruya konu haber, aktüel bir olaya ilişkin olmasa da arşivleme, haberlerin saklanması ve erişilebilirliğini sağlamaktadır. Başvurucunun adına yer vermeyerek basın özgürlüğü ve haber alma hakkının sağlanması sonucuna varabilmek de mümkündür. Bu nedenle AYM, hak ihlali bulunduğu karar vermiştir. Ayrıca bu minvalde bir değerlendirme yapılırken başvurucunun siyasi ve medyatik bir figür olup olmadığı, haberin içeriğinin istatistiki ve bilimsel amaçlara hizmet edip etmediği de dikkate alınmalıdır⁶⁶.

Bu hususta karşılaştırmalı hukuktaki düzenlemelerde örneğin İsviçre Federal Mahkemesi kararlarında, ceza yargılamasında yargılanan sanıkların isimlerine haberlerde yer verilmesinin kural olarak yasak olduğu, ancak istisnai bazı hallerde bu yasağın kalkabileceği belirtilmiştir. Bir kere dahi ismin anılması hukuka uygun olsa da sonraki haberlerde kişinin isminin anılmaya devam edilmesi gerekli değildir, zira yaşamın olağan akışı gereği geçen zaman içinde kişinin unutulma hakkı

⁶² NBB, para. 43.

⁶³ NBB, para. 46.

⁶⁴ NBB, para. 47.

⁶⁵ NBB, para. 52.

⁶⁶ AİHM'nin *ML v. Almanya* kararında ünlü bir aktör olan Walter Sedlmayr'ın 1990 yılında cinayet sonucu öldürülmesinin ardından başvuru olan failler Wolfgang Werle ve Manfred Lauber isimli iki kardeş cinayet nedeniyle tutuklanmış ve 2007 ve 2008 yıllarında koşullu salıverilmişlerdir. Ancak başvuru sahiplerinin kendileriyle ilgili haberler gazetelerin internet arşivinde yer almaya devam etmektedir. Başvurucular haberlerin arşivlerden kaldırılması talebinde bulunmuş, ancak kamuoyunun ilgisine mazhar bir cinayetin yeni bir haber olmadığı için ilk bakışta anlaşılması ve potansiyel okuyucuların internet arşivine ulaşmasının engellenmesi için yeterli şartların oluşmadığına karar vermiştir. Nitekim AİHM de başvuru sahiplerinin AİHS m. 8'in ihlali iddiasını adli cezalara ilişkin haberlerin kişinin itibarına zarar verici içeriğine katlanma yükümlülüğü bulunduğunu ve basının kamuoyunda bekçi (watchdog) vazifesi ifa etmekte olup internet arşivlerinin de kamu yararına hizmet ettiğini belirtmiş ve nihayetinde ihlal olmadığına hükmetmiştir. Bkz. Soysal, *a.g.e.*, s. 407.

gözetilmelidir⁶⁷. Federal Mahkeme kararlarında yargılama sona erdiğinde de haberin aktüelitesini yitirmesinden sonra bir kişinin adının ceza yargılaması ile bağlantılı olarak anılmasının yargılamanın aleniliğine dayanmayacağı belirtilmiştir⁶⁸.

4. Anonimlik Hakkı

a. Tanım

Kişisel verinin işlenme amacının ortadan kalkması veya amaca ulaşmak için verinin işlenmesinin gerekli olmaması durumunda kişisel veri yok edilmelidir. Avrupa’da bu yok edilme iki yolla yapılmaktadır: Ya veri ortadan kaldırılır ya da anonimleştirilir⁶⁹. Anonimlik hakkı bir kişi ya da grubun belirli ya da belirlenebilir olmaksızın görüş ve düşüncelerini açıklamasına olanak sağlamaktadır⁷⁰.

Anonimliğin, tam anonimlik (*complete anonymity*) ve maskeleme (*pseudonymity*) olmak üzere iki türü bulunmaktadır⁷¹. Anonim veri, kişisel verinin zıddı olup bir gerçek kişinin belirlenmesi ya da belirlenebilmesine ilişkin bir bilgi taşımayan ya da gerçek kişi ile belirlenebilirlik bakımından ilişkisinin artık mevcut olmadığı veridir. Anonimleştirme teknikleri⁷², bir kişinin adı veya sosyal güvenlik numarası gibi verilerde bulunabilecek doğrudan tanımlayıcıların kaldırılmasıyla sınırlı olmayıp bir bireyin gerçek kimliğine dolaylı olarak ulaşmayı sağlayacak posta kodu gibi ikincil tanımlayıcılar ile de ilgilidir. Bu gibi yarı tanımlayıcıların mutlaka kaldırılması gerekmez, bireylerin tanımlanmaması için veriler dönüştürülebilir⁷³.

⁶⁷ Başalp, “Avrupa Birliği Veri Koruması Genel Regülasyonu’nun Temel Yenilikleri”, s. 94.

⁶⁸ Başalp, “Avrupa Birliği Veri Koruması Genel Regülasyonu’nun Temel Yenilikleri”, s. 95-96; BGE 122 III 449 kararında Federal Mahkeme, geçmişte verilen mahkûmiyet kararının üzerinden 10 yıl geçmesine karşın haberlerde yer almasını değerlendirmiştir ve kişinin topluma tekrar kazandırılması için artık bazı meselelerin unutulması gerektiğini belirtmiştir.

⁶⁹ Küzeci, **a.g.e.**, s. 245-246.

⁷⁰ Küzeci, **a.g.e.**, s. 100.

⁷¹ Küzeci, **a.g.e.**, s. 100; Psödönimleştirme; *Dülger*’e göre takma adlılık veya maskeleme biçimlerinde gerçekleşebilir. Bkz. Dülger, **Kişisel Verilerin Korunması Hukuku**, s. 99.

⁷² Anonimleştirme için ihdas edilmiş projeler de mevcuttur. Örneğin AB tarafından finanse edilen OpenAIRE projesi kapsamında yer alan, kullanımı kolay veri anonimleştirme aracı olan Amnesia (<https://amnesia.openaire.eu>), Gizlilik Korumalı Veri Yayını (PPDP) alanındaki veri anonimleştirme tekniklerini kullanır. Örneğin, k-anonimlik, anonimleştirilmiş verilerdeki her bir kaydın, aynı tanımlayıcılara dayanarak aynı veri kümesindeki diğer k-1 kayıtlardan ayırt edilemeyeceğini garanti eder. Bkz. Rik Crutzen, Gjalt-Jorn Ygram Peters, Christopher Mondschein, “Why and How We Should Care About the General Data Protection Regulation”, **Psychology & Health**, c. 34, s. 11, 2019, s. 1354.

⁷³ Crutzen, Ygram Peters, Mondschein, **a.g.e.**, s. 1354.

Anonimleştirme teknikleri, kişisel verinin mahiyeti dikkate alınarak uygulanmalıdır. Örneğin biyometrik veriler bakımından özel nitelikli verilerin ele geçirilmesini önlemek için biyometrik tanımlayıcıları değiştirme veya çıkarma işlemi olan de-identifikasyon tekniklerinden⁷⁴ yararlanılabilir⁷⁵.

Anonimleştirmeden sonra anonim verinin işlenmesinde veri koruma kuralları uygulanmayacaktır. Ancak maskelenmiş veri (*pseudonymous data*) belirlenebilir bir gerçek kişi ile ilgili veridir⁷⁶. Maskelenen ve ek bir araç ya da bilgi kullanılarak gerçek bir kişiye atfedilebilen bu veri, tanımlanabilir gerçek kişinin kişisel verisidir ve Kolluk ve Ceza Adaleti Direktifi'nin korumasından yararlanır. GDPR gerçek kişiyi tanımlamak için araçların kullanılmasının muhtemel olup olmadığını belirlemede, mevcut teknolojiyi göz önünde bulundurarak kişiyi tespit etmek için gereken zaman, maliyet, işleme ve teknolojik gelişmeler gibi tüm objektif faktörlerin dikkate alınması gerektiğini belirtmiştir⁷⁷.

b. Anonimlik ve Büyük Veri İlişkisi

⁷⁴ Örneğin iptal edilebilir şablon (*cancelable template*), gizlilik sorunlarını, orijinal olanın yerine biyometrik verilerin çarpık bir modelini saklayarak çözer. Bu şablon, kullanıcıların hassas verilerini korumak için orijinal şablonun kasıtlı olarak tekrarlanabilir bir şekilde bozulduğu bir şablon koruma yöntemidir. Herhangi bir nedenden ötürü, orijinal model tehlikeye girerse, bozulma özellikleri değiştirilerek yeni bir farklı bozuk desen üretilebilir. Yalnızca çarpık deseni saklayarak, iptal edilebilir şablon koruma mekanizması kullanıcıların gizliliğini artırır. Biometric Salting ve Dönüştürülemez Dönüşüm (*Non-invertable Transforms*) biçiminde iki türü bulunan bu şablonların ortak özellikleri: çeşitlilik, yeniden kullanılabilirlik, geri dönülemezlik, doğruluk performansdır. Bkz. Cengiz Paşaoğlu, Kayode Hadilou Adje, Orkun Demirtaş, "A Review On Privacy Preserving Biometric Authentication Methods", **Kişisel Verileri Koruma Dergisi**, c. 1, s. 1, 2019, s. 41.

⁷⁵ De-identifikasyon ve anonimleştirme terimleri arasında bazı yazarlarca fark bulunmaktadır. De-identifikasyon kayıtlardan herhangi bir kişisel tanımlayıcı bilgiyi kaldırmak veya gizlemek için geri dönüşümlü bir işlemi ifade etmektedir. Anonimleştirme ise geri dönüşümsüz bir işlemdir. Biyometrik olarak, anonimleştirme (Geri Dönüşümsüz De-identification), tanımlanmış veri setleri ile orijinal veri setleri arasındaki herhangi bir bağlantının veya bağlantıların imhasını içerir. Anonimleştirmeden sonra hassas verilere ulaşmak veya işlemek mümkündür. Bkz. Paşaoğlu, Adje, Demirtaş, **a.g.e.**, s. 41.

⁷⁶ Crutzen, Ygram Peters, Mondschein, **a.g.e.**, s. 1349; Purtova, **a.g.e.**, s. 44.

⁷⁷ GDPR resital m. 26; Bazı yazarlarca bu kriterler yetersiz görülmüş ve gerçek kişinin tespiti, belirli bir ortamda alınması gereken çabalara bağlı olduğundan, maskeleye ve anonimleştirme arasında kesin ve hızlı bir çizgi çekmek için bunun yeterli olmadığı ileri sürülmüştür. Zira bu çizgi teknolojik gelişmelerle zaman içinde değişebilir. Bununla birlikte söz gelimi veri sahibinin adı ve iletişim detaylarının kaldırılması ile (veya sorulmaması), veri setinin anonim hale getirilmediği kanaatindedir. Bkz. Crutzen, Ygram Peters, Mondschein, **a.g.e.**, s. 1350. Sert ise maskeleye ve takma adlılığı anonimleştirme tekniği olarak değerlendirmiştir. Bunların haricinde tekil verilerin kaldırılarak grup halinde veri işleme yani kümeleme ve kaynak verilerin karakterini içeren ancak orijinal değerlerini gizleyen bantlama teknikleri de anonimleştirme tekniği olarak zikredilmiştir. Bkz. Sert, **a.g.e.**, s. 36 dipnot. 81.

Büyük veri, sosyal medya paylaşımları, web sayfaları, giriş-çıkış bilgileri, kamera kayıtları, telekomünikasyon operatörleri gibi farklı kaynaklardan veri grup ve kategorilerinin toplanması ile bir araya gelen veridir⁷⁸. Özellikle akademik çalışmalar, sağlık, sosyal bilimler, ulaşım, enerji alanı, mali alan, e-ticaret, yönetim, mali istihbarat ve suçla mücadele alanlarında büyük veri kullanılmaktadır⁷⁹. Zira kendisini oluşturan her bir kişisel veri haricinde büyük veri uygulamalarına, büyük verinin kullanılacağı sektöre göre değişmekle beraber genel olarak piyasanın gelişmesi, operasyonel çalışmalar, karar alma ve müşteri bağlılığını sağlamak gibi nedenlerle ihtiyaç duyulmaktadır⁸⁰. Genellikle set halinde bulunan veri grupları bir algoritma aracılığıyla eşleştirilerek yeni sonuçlar üretilmektedir⁸¹.

Sosyal medya analizi yoluyla özellikle bilişim suçları ve siber suçların tespitinde büyük veriden yararlanılmaktadır⁸². Suçla mücadele edilmesinde önemli etkileri olan bölgelerin suç haritalarının çıkarılmasında büyük veri gündeme gelmektedir. Özellikle istatistiki veriler elde edilirken kolluk ve adli makamların bilişim sistemlerinden kişisel veriler toplanmaktadır⁸³. Bu halde suç haritasının çıkarılması ve istatistikte kullanılan kişisel verilerin nasıl korunacağı değerlendirilmelidir. Öncelikle belirtilmelidir ki büyük veriye ilişkin bir hüküm Kolluk ve Ceza Adaleti Direktifi'nde bulunmamaktadır. Suç haritalarında kullanılan veriler, istatistik amacıyla kullanıldığından Kolluk ve Ceza Adaleti Direktifi m. 9/2 gereği esasen artık GDPR hükümlerine göre bir koruma gündeme gelmelidir. Ancak suç haritasının çıkarılması ile hedeflenenin de suçların önlenmesi olduğu düşünüldüğünde⁸⁴ bu kez verinin yararlandığı koruma Kolluk ve Ceza Adaleti

⁷⁸ Metin Turan, **Bilişim Hukuku**, Güncellenmiş 3. Baskı, İstanbul, Seçkin Yayıncılık, 2019, s. 254; Mark Latonero, "Big Data Analytics and Human Rights", **Technology and Human Rights Enforcement**, Ed. Molly K. Land, Jay D. Aronson, Pennsylvania, Cambridge University Press, 2018, s. 149; Aşıkoğlu, **a.g.e.**, s. 138.

⁷⁹ Turan, **a.g.e.**, s. 259 vd.

⁸⁰ Aşıkoğlu, **a.g.e.**, s. 140; "Yandex'in sunduğu bir hizmet olan Yandex.Traffic ile şehir içi kaynaklar ve kullanıcılardan toplanan bilgilerle yol ve trafik durumunu gösteren haritalar ve kullanıcılara alternatif yol sunan uygulamaları üretmiştir.... Facebook tarafından tanıtılan DeepFace yazılımı ile bir kişiye ait iki farklı fotoğraf %97.35 başarı oranıyla eşleştirilebilmektedir." Bkz. Aşıkoğlu, **a.g.e.**, s. 143.

⁸¹ Aşıkoğlu, **a.g.e.**, s. 178.

⁸² Turan, **a.g.e.**, s. 259.

⁸³ Ali Rıza Çam, **Adli Bilişim ve Kolluk**, İstanbul, On İki Levha Yayıncılık, 2015, s. 88.

⁸⁴ Nitekim Emniyet Genel Müdürlüğü'nün 2009-2013 arası Stratejik Planı'nda yer alan "Suç analizi suçun oluşmadan önlenmesi, mevcut suçların ve suç eğilimlerinin tespit edilerek bunlara karşı gerekli

Direktifi'ne göre olmalıdır. Kanaatimizce bu halde verinin anonim hale getirilerek suç haritasında kullanılmak üzere işlenmesi gerekmektedir. Bu durumda da kişisel veri artık anonim hale getirildiğinden veri sahibinin GDPR yahut Kolluk ve Ceza Adaleti Direktifi bağlamında korunması gereken bir hukuki değerinden söz edilemeyecektir.

Büyük veri uygulamaları sırasında anonim verilerin kullanıldığı ve bu verilerin kişisel veri mahiyeti olmadığından kişisel veri korumasından yararlanmasının gerekmediği uygulamacılar tarafından iddia edilmektedir. Ancak verinin belirlenebilir olma unsuru bulunduğu sürece bir veri kişisel veridir ve örneğin internete bağlanıldığında kullanılan browserda kullanıcı girişi yapılmamış olsa dahi kullanıcı alışkanlığı ve hareketlerinden kullanıcının, browser tarafından yaklaşık olarak belirlenmesi mümkün olabilmektedir. Bu halde de verinin anonim olduğundan bahsedilememektedir⁸⁵. Ancak büyük veri uygulaması ile sağlanmak istenen amaç, anonim haldeki verilerin işlenmesi ile de sağlanabiliyorsa bu durumda anonimlik tercih edilmelidir⁸⁶.

5. Denetleyici Makama Başvuru Hakkı

Kolluk ve Ceza Adaleti Direktifi'nin veri koruması, veri sahibinin veri sorumlusuna veya denetleyici makamlara başvurmasına cevaz veren iki ayaklı bir korumadır⁸⁷. Veri sahibinin Kolluk ve Ceza Adaleti Direktifi bağlamında tanınan haklarının üye devletçe tanınmaması veya veri sorumlularının yükümlülüklerine aykırı davranması halinde, m. 52'ye göre veri sahibinin yargı makamları haricinde denetleyici makama şikâyetle bulunma hakkı tanınmıştır.

tedbirlerin alınmasını içermektedir. Hangi suçların neden, hangi etkiler altında, hangi bölgede, hangi zaman diliminde, hangi metotla, hangi özelliğe sahip kişiler tarafından işlendiğinin tespit edilmesi neticesinde elde edilecek analizlerle polisin başarısı artacak, personelimizin doğru zamanda, doğru yerde ve doğru sayıda görevlendirilmesi sağlanacaktır.” (akt. Çam, a.g.e., s. 88) ifadelerden suç analizi ve suç haritalarının çıkarılması ile suçların önlenmesi ve suçla mücadele edilmesinin amaçlandığı anlaşılmaktadır.

⁸⁵ Aşıkoğlu, a.g.e., s. 149.

⁸⁶ Aşıkoğlu, a.g.e., s. 176.

⁸⁷ Dülger, Özkan, a.g.e., s. 96.

6. Tazminat Hakkı

Veri sorumlusu yahut yetkili bir diğer makam tarafından hukuka aykırı veri işleme gerçekleşmişse veya üye devletler Kolluk ve Ceza Adaleti Direktifi'nden iç hukuklarına aktardığı hükümlere aykırı bir fiilde bulunmuşsa, bu durumda kişilerin uğradığı maddi ve manevi zarar tazmin edilmelidir⁸⁸.

KVKK uyarınca kişisel verilerin korunması hakkının ihlali halinde kişiler genel hükümlere göre tazminat talebinde bulunabilecektir⁸⁹. Ancak Kolluk ve Ceza Adaleti Direktifi bağlamında gerçekleştirilen veri işleme nedeniyle bu hakkın ihlal edilmesi halinde, söz gelimi kolluk makamından özel hukuk hükümleri çerçevesinde tazminat talebinde bulunulamayacaktır. Zira meri mevzuat gereği idarenin fiillerinden kaynaklanan zararlar adli yargının görev alanına sokulamamaktadır⁹⁰. Önleyici kolluk faaliyetleri bakımından hukuka aykırı bir veri işleme sonucu kişinin tazminat talebi tam yargı davası biçiminde ileri sürülebilecektir.

Ceza muhakemesinde bir koruma tedbirine başvurulurken kişisel verilerin korunması hakkı ihlal edilmiş olan kişi bakımından CMK m. 141 gereği tazminat talebi düşünülebilir. Ancak CMK gereği tazminat talebi ancak yakalama, gözaltı, tutuklama, arama ve elkoymanın söz konusu olduğu hallerde mümkündür. Söz gelimi hukuka aykırı olan fizik kimliğinin tespiti sırasında biyometrik verisi işlenen kişi, CMK uyarınca tazminat talebinde bulunamayacaktır. AY m. 125/son hükmüne göre idarenin hukuka aykırı işlem ve eylemlerine dayanılarak doğan zararın tazmin edilebileceği düşünülebilir. Ancak bu halde de hukuka aykırı işlemi yapan makam yürütmenin içindeki idare değil, yargıdır ve idarenin sorumluluğuna gidilemez. Bu durumda CMK'de yapılacak bir değişiklikle özellikle gizli soruşturmacı görevlendirilmesi gibi modern koruma tedbirleri için m. 141 hükümlerine

⁸⁸ Kolluk ve Ceza Adaleti Direktifi m. 56.

⁸⁹ Bkz. KVKK m. 13/3.

⁹⁰ İdarenin eylem ve işlemlerden kaynaklanan zararların tazmini için açılan davaların idarî yargıya tabi olmasının, "Görev esası izler" ilkesinin bir sonucu olduğuna dair bkz. Kemal Gözler, Gürsel Kaplan, "İdari Eylemlerden Kaynaklanan Zararlara İlişkin Davalar Adli Yargının Görev Alanına Sokulabilir Mi? (HMK m. 3 ve TBK, m. 55/2 Hakkında Eleştiriler)", Çevrimiçi <http://www.idare.gen.tr/gozler-kaplan-hmk-m3.htm> 01.02.2020.

başvurmanın sağlanması önerilmiştir⁹¹. Yargıtay CMUK dönemindeki bir kararında kanunda sınırlı olarak sayılan hallerde tazminat talebinde bulunulabileceğine hükmetmiştir⁹².

Sonuç olarak Türk hukukunda Kolluk ve Ceza Adaleti Direktifi'nin öngördüğü tazminat hakkı, salt kişisel verilerin korunmasına ilişkin mevzuatta yer almamaktadır. Ancak idari kolluk faaliyeti çerçevesinde kişisel veri korumasının ihlal edildiği halde idare hukuku hükümleri gereği tazminat talebinde bulunulabilmektedir. Söz konusu adli makamların hukuka aykırı kişisel veri işlemesi olduğunda ise veri sahibine tanınan tazminat talep hakkı bulunmamaktadır.

II. VERİ SORUMLUSU

A. Tanım ve Türleri

Veri sorumlusu; tek başına veya müşterek biçimde kişisel verilerin işleme amacı ve araçlarını belirleyen yetkili makamdır. Bu belirleme ve karar verme yetkisine sahip kişi tespit edilirken; verinin işleme amacı, işlenecek kişisel veri kategorisi,

⁹¹ Bahri Öztürk, Behiye Eker Kazancı, Sesim Soyer Güleç, **Ceza Muhakemesi Hukukunda Koruma Tedbirleri**, 3. Baskı, Ankara, Seçkin Yayıncılık, 2019, s. 356.

⁹² Bkz. Yargıtay CGK, 31.01.1998, 9-55/ 123; AYM bireysel başvurusuna konu olan bir olayda bir ceza soruşturması kapsamında CMK m. 135 uygulanan şüpheli hakkında verilen kovuşturmayaya yer olmadığı kararı verilmiştir. Başsavcılığın dinleme kayıtlarının imhası kararından itibaren beş ay geçmesine rağmen bu kayıtlar imha edilmemiş, kayıtlar birçok mahkemeye gönderilmiş ve UYAP'a aktarılmıştır. Başvurucu da manevi zarara uğradığından bahisle CMK m. 141/3 uyarınca tazminat talebinde bulunmuş ve talebi reddedilmiştir (para. 11-13). AYM, CMK m.141/3 çerçevesinde ileri sürülen zarar iddialarının her somut olay nazara alınarak değerlendirilmesini ve bu iddiaları değerlendirirken yargı makamlarının yapacakları yorumun etkili başvuru yolunun bulunup bulunmadığı noktasında kilit rol oynadığını belirtmiştir (para. 55). Başvuruya konu olayda derece mahkemeleri somut bir gerekçe sunmaksızın m. 141/3'ün şartlarının oluşmadığını belirtmiştir. Bu nedenle hak ihlali halinde şikayet etkili bir şekilde incelenmemiştir. AYM'ye göre sonuç itibarıyla de özel hayata saygı ve haberleşme hürriyeti çerçevesinde başvurunun zararının tazmini noktasında asgari güvencelere sahip bir etkili hukuk yolu bulunmamaktadır (para. 58). Bkz. Murat Haliç Başvurusu, B. No: 2017/24, 08/07/2020 Çevrimiçi <https://www.anayasa.gov.tr/media/6970/2017-24356.pdf> 21.09.2020. Kanaatimizce burada, iletişimin denetlenmesi çerçevesinde CMK m. 141/3 değerlendirmesi somut olay gözetilerek yapılsa ve tazminata hükmedilmese de bir hak ihlali söz konusu olurdu. Zira mahkemelerin m. 141/3'ü geniş yorumlaması veya somut olay değerlendirilmesi ile aşılamayacak bir durum bulunmaktadır. İletişimin denetlenmesi, teknik araçlarla izleme ve diğer koruma tedbirleri veya delil değerlendirme araçları ile kişisel verilerin korunması hakkına müdahale gerçekleştirmektedir. Tıpkı yakalama, tutuklama ve arama kararlarında olduğu gibi kişisel verilerin korunması hakkının ihlali halinde de şüpheli veya sanığa tazminat olanağı sunulmalıdır.

kimin veri işleyen olması gerektiği, verilerin aktarılıp aktarılmayacağı, aktarım yapılacaksa bunun amacı, veriye erişebilecek kişiler, veri saklama süresi ve veri yok etme süresine karar verme yetkisinin kimde olduğuna bakılmalıdır⁹³. Veri sorumlusu, kişisel verilere ulaşabilir olduğundan ya da hâlihazırda verilere sahip olduğundan değil; verinin işleme amaç ve araçlarını belirleme yetkisine sahip olduğundan veri sorumlusudur⁹⁴. Bu makam, Kolluk ve Ceza Adaleti Direktifi'nin veri işleme amaçlarından olan suçların önlenmesi, soruşturulması, ortaya çıkarılması, kovuşturulması, cezaların infazı ve kamu güvenliğini sağlamakla yetkili kamusal organ veya kamu gücü kullanmakla yetkili kılınmış başka bir organ olabilmektedir⁹⁵.

GDPR ve Kolluk ve Ceza Adaleti Direktifi'nde veri işleme amaç ve araçlarını birden çok gerçek veya tüzel kişinin birlikte belirlemesi mümkündür. Veri sorumlularının birden çok kişi olması halinde, bu kişiler müşterek veri sorumlusudur ve öngörülen yükümlülüklerin yerine getirilmesinden müşterek olarak sorumludurlar.

Birden çok veri sorumlusunun bulunması, veri işleyen ve veri sorumlusu ayrımını derinleştirmeyi gerektirmektedir. ABAD, veri sahibinin daha etkin korumadan yararlanabilmesi için veri sorumlusu tanımını geniş tutma eğilimindedir⁹⁶. Bu hususta Alman Veri Koruma Otoritesi Schleswig-Holstein ve özel bir şirket olan *Wirtschaftsakademie Schleswig-Holstein* arasındaki uyuşmazlığın konu olduğu *Wirtschaftsakademie Schleswig-Holstein* başvurusuna⁹⁷ değinilmelidir. Şirketin Facebook hayran sayfası, sayfayı ziyaret edenlere eğitici hizmetler sunmakta ve Facebook Insights vasıtasıyla bilgisayara çerezler (*cookies*) yerleştirmektedir. Ancak Facebook ya da şirket sayfayı ziyaret edenlerin çerezler vasıtasıyla kişisel verilerinin işleneceğine dair bilgilendirme yapmamıştır. ABAD, *Wirtschaftsakademie*'nin Facebook'un işleyişi bakımından veri sorumlusu olmayacağı ön kabulünde bulundursa da Divan'ın Başsavcısı veri koruma hukukunun gelecekteki uygulaması

⁹³ Dülger, **Kişisel Verilerin Korunması Hukuku**, s. 118-119.

⁹⁴ Develioğlu, **a.g.e.**, s. 42.

⁹⁵ Kolluk ve Ceza Adaleti Direktifi m. 3/7-a.

⁹⁶ Susanna Lindroos-Hovineimo, "Who Controls Our Data? The Legal Reasoning of the European Court of Justice in *Wirtschaftsakademie Schleswig-Holstein* and *Tietosuojaalvautettu v Jehovan Todistajat*", **Information and Communications Technology Law**, c. 28, s. 2, 2019, s. 231.

⁹⁷ *Wirtschaftsakademie Schleswig-Holstein* [BD], B. no: C-210/16, 05.06.2018 Çevrimiçi https://curia.europa.eu/jcms/jcms/Jo1_6308/ 29.03.2020.

için önemli sonuçları olan yorumunda, Facebook ve şirketin müşterek sorumlu olarak kabul edilmesi gerektiğini ileri sürmüştür. Zira şirket, Facebook hayran sayfasının yöneticisidir ve bu yönetici, veri işlemenin araç ve amaçlarını, verilerin Facebook tarafından nasıl işlendiğini belirlemede baskın bir rol oynamaktadır. Ayrıca, Facebook ve Wirtschaftsakademie'nin amaçları bakımından da yakınlık vardır. Wirtschaftsakademie, kişisel verilerin işlenmesini gerektiren istatistiklerin elde edilmesini amaçlarken aynı veri işleme, ağında reklam yayınlatmayı amaçlayan Facebook'un bu amacını gerçekleştirmeye hizmet etmekteydi⁹⁸. Nitekim ABAD de Başsavcı'nın bu görüşüne katılmış ve bir hayran sayfasının yöneticisinin, hizmetlerinden yararlanmak için Facebook tarafından sağlanan bir platformu kullanmasının yöneticiyi kişisel verilerin korunmasını sağlama yükümlülüklerinden muaf tutmadığı sonucuna varmıştır. Ayrıca Facebook'ta barındırılan hayran sayfaları, söz konusu sosyal ağdaki bir kullanıcı hesabı olmadan, Facebook dışındaki kullanıcılar tarafından da ziyaret edilebilmektedir. Bu gibi durumlarda sadece ana sayfayı ziyaret etmek, kişisel verilerinin otomatik işlenmesine yol açacağından hayran sayfası yöneticisinin kişisel verilerin işlenmesi konusundaki sorumluluğu daha da büyük olabilecektir⁹⁹. Bu nedenle ABAD, Facebook ve Wirtschaftsakademie'nin müşterek veri sorumlusu (*joint controllers*) olduğunu ancak müşterek sorumluluğun eşit sorumluluk anlamına gelmediğini belirtmiştir¹⁰⁰. Aksine, müşterek sorumlular kişisel verilerin farklı aşamalarda ve farklı derecelerde işlenmesine katılabileceğinden sorumluluk da buna göre paylaşılmalıdır¹⁰¹.

Nitekim Kolluk ve Ceza Adaleti Direktifi de içtihatla paralel bir hükme yer vermiştir. AB hukuku ya da üye devletin iç hukukunca birden çok veri sorumlusu

⁹⁸ Lindroos-Hovinheimo, **a.g.e.**, s. 231.

⁹⁹ Lindroos-Hovinheimo, **a.g.e.**, s. 232.

¹⁰⁰ Benzer bir tartışma *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW* başvurusunda da mevcuttur. Fashion ID, Facebook'un "Beğen" seçeneğini web sitesine yerleştiren çevrimiçi bir satıcıdır. Bir kullanıcı Fashion ID web sitesini ziyaret ettiğinde, bu kullanıcının IP adresi ve tarayıcı dizesiyle ilgili bilgiler Facebook'a aktarılmaktadır. Bu aktarım, kullanıcının "Beğen" seçeneğini tıklayıp tıklamadığına veya kullanıcının bir Facebook hesabına sahip olup olmamasına bakılmaksızın gerçekleşir. Bu durumda Facebook veya Fashion ID'de hangi tarafın veri sorumlusu olduğu değerlendirilmiştir ve *Wirtschaftsakademie Schleswig-Holstein* içtihadına atıf yapan Başsavcı Bobek, kullanıcılarının kişisel verilerin toplanması ve iletilmesi bakımından Fashion ID'yi sorumlu olarak nitelendirmiştir. Bkz. Lindroos-Hovinheimo, **a.g.e.**, s. 234.

¹⁰¹ Veri işleme faaliyeti sırasında 95/46 sayılı Direktif'in uygulaması devam ettiğinden GDPR m. 26'nın müşterek sorumluluk hükmü uygulanmamıştır. Bkz. Soysal, **a.g.e.**, s. 395.

arasındaki sorumluluk paylaşımı belirlenmedikçe, veri sorumlularının şeffaf bir biçimde kendi aralarında bir sözleşme ile sorumluluğu paylaşmalarına m. 21 olanak tanımıştır. Ancak bu durumda veri sahibinin, haklarını ileri sürebileceği ve kullanabileceği bir veri sorumlusu olan irtibat kişisi üye devlet tarafından belirlenecektir.

B. Türk Hukukunda Veri Sorumlusu Olabilecek Makamlar

Türk hukuku bakımından kimlerin veri sorumlusu olabileceği değerlendirilmelidir. KVKK’de veri sorumlusu *kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi* olarak ifade edilmiştir¹⁰². Doktrinde KVKK’nin veri sorumlusunu tanımlarken yine “sorumlu” ifadesini tercih etmesi, lafzen isabetli bulunmamıştır. Kolluk ve Ceza Adaleti Direktifi’ndeki gibi veri işlemede amaç ve araçları¹⁰³ belirlemeye yetkili olmanın kriter olarak belirlenmesi gerektiği ileri sürülmüştür¹⁰⁴. Veri işleme amaç ve araçlarını belirleme yetkisi; suçların önlenmesi, ceza muhakemesi ve infaz sürecindeki kişisel veriler gözetildiğinde kanundan doğmaktadır.

Suçun önlenmesi ve ceza muhakemesinde faaliyet yürüten kolluk makamları genel-özel kolluk ayrımı¹⁰⁵ veya idari-adli kolluk¹⁰⁶ yapılmaksızın veri sorumlusu olabilmektedir. Ancak bazı hallerde kolluk faaliyeti duruma göre önleyici yahut

¹⁰² KVKK m. 3/1-ı.

¹⁰³ Veri işlemede amaç, verinin kullanım başta olmak üzere işleme amacı iken, veri işlemede araç ise işlemede organizasyonel ve teknik hususları, verileri işlenecek kişi kategorileri ve üçüncü kişilerin erişim olanaklarıdır. Bkz. Mesut Serdar Çekin, **Avrupa Birliği Hukuku ile Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku**, 2. Baskı, İstanbul, On İki Levha Yayınları, 2019, s. 51.

¹⁰⁴ Çekin, **a.g.e.**, s. 50-51.

¹⁰⁵ Kolluk teşkilatı ayrımı 3201 sayılı Emniyet Teşkilatı Kanunu’nda yapılmıştır. M. 3/1 “*Zabıta teşkilatı: Umumi ve hususi olmak üzere iki kısma ayrılır.*

Umumi zabıta: Silahlı bir kuvvet olan (polis) ve (jandarma) dır.

Hususi zabıta: Umumi zabıta haricinde kalan ve mahsus kanunlarına göre teşekkül edip muayyen vazifeleri gören zabıta kuvvetleridir.”

¹⁰⁶ Ayrıma dair detaylı bilgi için bkz. Özge Okay Tekinsoy, “Kolluk”, **İdare Hukuku**, Ed. Turan Yıldırım, Güncelleştirilmiş 7. Baskı, İstanbul, On İki Levha Yayıncılık, 2018, s. 477.

bastırıcı olabileceğinden ayırım güçleşmektedir¹⁰⁷. Görevlerini yerine getirirken kolluk makamları tarafından yürütülen tüm kişisel veri işleme faaliyetlerine Kolluk ve Ceza Adaleti Direktifi uygulanmayacaktır. Zira Kolluk ve Ceza Adaleti Direktifi kapsamındaki veri işleme faaliyetleri, ancak Kolluk ve Ceza Adaleti Direktifi 1. maddesindeki amaçlarla sınırlıdır. Örneğin kamu düzeninin unsurlarından¹⁰⁸ olan kamu sağlığı çerçevesinde koruyucu sağlık hizmeti yürüten kolluk, bu faaliyeti sırasında kişisel veri işlediğinde bu işleme faaliyeti Kolluk ve Ceza Adaleti Direktifi'ne tabi olmamaktadır. Dolayısıyla Kolluk ve Ceza Adaleti Direktifi bağlamında veri sorumlusunu tespit ederken; suçun önlenmesi, soruşturulması, ortaya çıkarılması, kovuşturulması ve cezanın infazı amacıyla faaliyet gösteren bir kolluk makamının varlığı gerekmektedir.

1. Adli-İdari Kolluk

Adli-idari kolluk ayırımı kolluk faaliyetinin amacına göre olup¹⁰⁹ işlevsel yönden bir ayırımdır¹¹⁰. Adli kolluk kamu düzenine aykırı ve suç teşkil eden fiiller ile ilgili fail ve delil araştırması yaparken idari kolluk daha çok kamu düzenini bozan ve suç sayılan fiiller işlenmeden önce bunları önlemek, kamu düzenini sağlamak, korumak ve bozulduğunda geri getirmekle görevlidir¹¹¹. Adli kolluk bastırıcı iken idari kolluk önleyicidir¹¹².

¹⁰⁷ Örneğin bir kimlik kontrolü, bir suç şüphelisinin tespiti için yapıldığında adli kolluk makamının görev alanındayken önleyici bir amaçla yapıldığında idari kolluğun görev alanında olacaktır. Diğer örnekler için bkz. Okay Tekinsoy, **a.g.e.**, s. 479-480.

¹⁰⁸ Toplumsal gelişmeler nedeniyle kamu düzeninin dirlik ve esenlik, sağlık ve güvenlik unsurlarının ötesinde olduğu ve bu çerçevede etik kamu düzeni, spor kamu düzeni, çevre kamu düzeni, ekonomik kamu düzeni gibi kavramlar ileri sürülmüştür. Okay Tekinsoy'a göre, bu kavramlar da kamu düzeninin klasik unsurlarının içinde mevcuttur. Bkz. Okay Tekinsoy, **a.g.e.**, s. 476. Bu tez kapsamında gerek klasik anlamda kamu düzenini sağlamak gerekse de farklı versiyonlarla kamu düzenini sağlamakla yükümlü olan kolluk makamlarının veri işleme faaliyetlerine Kolluk ve Ceza Adaleti Direktifi'nin uygulanıp uygulanmayacağı tespiti yapılırken kriter, ceza hukuku anlamında bir suçla mücadele amacı olacaktır.

¹⁰⁹ Okay Tekinsoy, **a.g.e.**, s. 477.

¹¹⁰ İl Han Özay, **Günlükte Yönetim**, 3. Baskı, İstanbul, Filiz Kitabevi, 2017, s. 727; Metin Günday **İdare Hukuku**, Güncellenmiş ve Gözden Geçirilmiş 10. Baskı, Ankara, İmaj Yayınevi, 2015, s. 290-291, s. 294; Adli kolluk yerine "suç kolluğu" ifadesi için bkz. Özay, **a.g.e.**, s. 725 vd.

¹¹¹ Lütfi Duran, **İdare Hukuku Ders Notları**, İstanbul, Fakülteler Matbaası, 1982, s. 248.

¹¹² Kemal Gözler, **İdare Hukuku**, c. 2, Güncellenmiş 3. Baskı, Bursa, Ekin Yayınevi, 2019, s. 48; Feridun Yenisey, **Kolluk Hukuku**, 2. Baskı, İstanbul, Beta Yayıncılık, 2015, s. 117; Ancak Duran'a göre bu iki kolluk arasındaki fark önleyicilik-bastırıcılık olarak açıklanamaz. Zira idari kolluk da müeyyide uygulama yetkisine sahiptir. Adli kolluk ise cezalandırma yetkisi kullanmayıp yargı

Ülkemizde kamu düzeni ve güvenliğinin korunması ve suç işlenmesinin önlenmesi için idari kolluk yetkilendirilmiştir¹¹³ ve idari kolluk kanunda belirtilen biçimde kişisel veri işleyebilecektir. Ancak idari kolluğun tamamının kişisel veri işleme faaliyetine Kolluk ve Ceza Adaleti Direktifi uygulanmayacaktır. Bu noktada idari kolluğun suçun önlenmesi ile ilgili kişisel veri işleme faaliyetinde bulunması gerekmektedir.

İdari kolluk, genel idari kolluk ve özel idari kolluk olarak ikiye ayrılmaktadır. Özel idari kolluk da imar kolluğu, gayrisihhi müesseseler kolluğu, at yarışları kolluğu gibi farklı hizmet alanlarında faaliyet göstermektedir¹¹⁴. İdari kolluğun suçun önlenmesi amacı faaliyetleri haricinde kişisel veri işleme faaliyetlerine Kolluk ve Ceza Direktifi uygulanmayacaktır. Örneğin Umumi Hıfzıssıhha Kanunu'na göre devletin görevlerinden biri de ülkenin sıhhi şartları ve hastalıklarla mücadele etmektir. Bu amaçla hareket eden idari kolluğun veri işleme faaliyeti Kolluk ve Ceza Adaleti Direktifi'nin konusu ve amaçları arasında değildir, ancak söz gelimi bulaşıcı olan Koronavirüs hastalığı (COVID-19) gerekçesiyle karantinaya alınmış kişilerin kolluk tarafından alınan tedbirlere uymaması TCK m. 195 uyarınca bulaşıcı hastalıklara ilişkin tedbirlere aykırı davranma suçudur. Bu halde idari kolluğun karantinaya alınanların hastalık, isim, soyisim, adres gibi kişisel verilerini işlemesi bu suçun önlenmesi faaliyetidir ve Kolluk ve Ceza Adaleti Direktifi uygulama alanı bulmalıdır.

Ceza muhakemesi aşamasında veri işleme faaliyetleri bir koruma tedbiri, delil elde etme yöntemi veya bir mahkeme kararı yahut hükmünün açıklanması sırasında gündeme gelebilir. Ceza muhakemesinde bu tedbir ve yöntemlere nasıl başvurulacağı esasen CMK'de belirlenmiştir. Bu nedenle ceza muhakemesindeki kolluk ve adli makamdan anlaşılması gerekeni CMK ışığında belirlemekte fayda bulunmaktadır. Ceza muhakemesinde kolluk, CMK m. 164'te belirtilen adli kolluktur. Ancak m. 165 uyarınca durumun gerektirmesi veya savcının talebi ile diğer kolluk birimleri de adli kolluk görevi yürütebilecektir. Bu halde diğer kolluk birimlerinin adli görevleri

makamlarının bu tecziye yetkisini kullanması için yardımcıdır. Esasen her iki kolluğun da bastırıcı niteliği vardır. Bkz. Duran, **a.g.e.**, s. 251.

¹¹³ İdari kolluğa ilişkin bkz. Çam, **a.g.e.**, s. 9; ETK m. 9/A “İdari polis, içtimai ve umumi intizamı temin etmekle mükellef olan kısımdır.”; PVSK m. 1 “Polis, asayiş, amme, şahıs tasarruf emniyetini ve mesken masuniyetini korur. Halkın ırz, can ve malını muhafaza ve ammenin istirahatini temin eder.”

¹¹⁴ Detaylı bilgi için bkz. Okay Tekinsoy, **a.g.e.**, s. 482 vd.

sırasındaki veri işleme faaliyetleri Kolluk ve Ceza Adaleti Direktifi uyarınca yapılmalıdır.

Ceza muhakemesi aşamasında veri işleme faaliyeti yürütebilecek bir diğer makam da şüphesiz adli yargı makamlarıdır. Adli yargı makamlarından anlaşılması gereken ise 5235 sayılı Adli Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanun ikinci bölümde sayılan ceza mahkemeleri ve üçüncü bölümde sayılan Cumhuriyet başsavcılığıdır.

Kolluk ve Ceza Adaleti Direktifi bağlamında veri sorumlusu, kişisel veri işlenmesi amaç ve araçlarına karar veren kişidir. Örneğin CMK m. 81 uyarınca yapılacak fizik kimliğinin tespiti işlemine karar verecek olan kişi Cumhuriyet savcısı olduğundan, bu halde veri sorumlusu bir adli yargı makamı olarak cumhuriyet savcısıdır. CMK m. 75 uyarınca gecikmesinde sakınca bulunan bir hale dayanarak Cumhuriyet savcısı tarafından iç beden muayenesi yapıldığında ise bu muayene sonucunda elde edilen örnekler üzerine moleküler genetik inceleme yapıldığında kişisel veri elde edilmekte yani işlenmektedir¹¹⁵. Gecikmesinde sakınca bulunan halde yapılan iç beden muayenesinde CMK uyarınca yirmi dört saat içinde hakim veya mahkeme onayı gerekmektedir. CMK m. 78 uyarınca moleküler genetik inceleme yapılabilmesi için ise münhasıran hakim kararı gerekmektedir.

Cumhuriyet savcısının kararı yapılan bir iç beden muayenesine hakim veya mahkemenin onay vermesi ve ardından hakim kararı¹¹⁶ ile bilirkişi tarafından moleküler genetik inceleme yapılarak gerçekleşen kişisel veri işleme faaliyetinde veri sorumlusu tespit edilmelidir. Hakim veya mahkemenin onayı üzerine müşterek veri sorumluluğunun gerçekleşip gerçekleşmeyeceği değerlendirilmelidir. Kolluk ve Ceza Adaleti Direktifi m. 21'e göre iki veya daha fazla kişinin müşterek veri sorumlusu olabilmesi için bu kişilerin veri işleme amaç ve araçlarına birlikte karar vermeleri gerekmektedir. Müşterek veri sorumluluğunun pratik sonucu ise veri sahibinin

¹¹⁵ Bkz. CMK m. 80/1.

¹¹⁶ Her ne kadar CMK m. 79/1 uyarınca “78 inci madde uyarınca moleküler genetik incelemeler yapılmasına sadece hâkim karar verebilir.” denmişse de burada mahkeme de moleküler genetik incelemeye karar verebilecektir. Zira 78. madde uyarınca elde edilen bulgunun sanığa ait olup olmayacağına ilişkin de moleküler genetik inceleme yapılabilir. Dolayısıyla kovuşturma evresinde bu kararı verecek olan mahkeme olacaktır.

bilgilendirilme hakkı başta olmak üzere haklarını veri sorumlularına yöneltebilmesidir. Ancak veri sorumluları, AB veya üye devletlerin iç hukukunda bir düzenleme mevcut değilse aralarında yapacakları bir anlaşma ile veri sahibinin irtibat kişisini belirleyerek veri sorumlusu olarak yükümlülüklerini düzenleyebilecektir¹¹⁷. Bu bilgiler ışığında moleküler genetik inceleme sonucu gerçekleşen veri işleme faaliyetinde veri sorumlusu kanaatimizce şüphesiz CMK m. 79 uyarınca hakim veya mahkemedir. İç beden muayenesine karar veren savcı, veri sorumlusu değildir; zira hakim veya mahkeme onayı olmaksızın veri işleme gerçekleşmeyecek ve elde edilen bulgular bir kişiye izafe edilebilir olmayacağından kişisel veri söz konusu olmayacaktır. Savcının iç beden muayenesi kararının ardından moleküler genetik inceleme kararını veren makam yalnız hakim veya mahkemedir. Yani savcı, bu kararı veren merci değildir. Dolayısıyla veri sorumlusu, yalnız hakim veya mahkemedir. Moleküler genetik inceleme kararında belirtilen bilirkişi ise veri işleyendir. CMK veri işleyen olarak bilirkişiye, teknik ve organizasyonel bakımdan yükümlülük de yüklemiştir. Buna göre bilirkişi yasak moleküler genetik incelemelerin yapılmasını ve yetkisiz üçüncü kişilerin bilgi edinmesini önlemekle yükümlüdür¹¹⁸.

Bir başka veri işleme örneği olarak GBT kaydının tutulmasında, veri sorumlusu il emniyet müdürlüğüdür. Kayıtlar, 3152 sayılı Kanun m. 13/e uyarınca İçişleri Bakanlığına bağlı KİHBİ biriminin sisteminde işlenmektedir. Bir suçun işlendiği şüphesinin doğması üzerine kişisel veri işleme, adli kolluğun faaliyet alanında olacaktır. CMK hükümleri uyarınca yetkileri düzenlenen adli kolluk; Emniyet Genel Müdürlüğü, Jandarma Genel Komutanlığı, Sahil Güvenlik Komutanlığı ve Gümrük Muhafaza Genel Müdürlüğünden teşekkül etmektedir¹¹⁹. Bu makamlar veri sorumlusu olabilecektir.

Önleyici kolluk ve bastırıcı kolluğun veri işleme faaliyetinin suç işlenmesinin önlenmesi yahut suçun aydınlatılmasına mı yönelik olduğunun belirsiz olduğu haller olabilir ki bu noktada veri sorumlusunu ve veri ihlali halinde başvurulacak makamı tespit etmek zorlaşır. Örneğin CCTV kamerası ile yapılan izleme ve görüntülerin

¹¹⁷ Kolluk ve Ceza Adaleti Direktifi m. 21/1.

¹¹⁸ CMK m. 79/2.

¹¹⁹ CMK m. 164/1; Adli Kolluk Yönetmeliği m. 3/1.

kaydedilmesinde, suç işlenmesinin önlenmesi mi yahut işlenen suçun faillerini tespit amacının mı ağır bastığı tartışmalı olabilir. Kolluk faaliyetinde önleyici ya da bastırıcı ayırım yapılırken *objektif izleyicinin işlem hakkında edindiği toplum izlenimi* ölçütüne başvurulur¹²⁰. Örneğin Alman hukukunda yapılan değerlendirme sonucunda *çifte karakterli işlem*, önleme ya da adli yetki kurallarından birine uygunsa işlemin hukuka uygun olduğu kabul edilir¹²¹. Suç işlenmesini önleyici kişisel veri işleme faaliyetlerinin hukuka aykırı olduğu iddiasıyla başvurulacak yargı makamı idare mahkemeleri iken kolluğun kişisel veri işlemesi halindeki hukuka aykırılıklarda başvurulacak makam adliye mahkemeleridir¹²².

2. Genel-Özel Kolluk

Güvenlik, dirlik-esenlik ve genel sağlık bakımından toplum düzenini korumakla yükümlü kolluk genel kolluk iken, özel düzenlemelerle farklı personel ve usullerle faaliyet yürüten kolluk ise özel idari kolluk veya hizmet kolluğudur¹²³. Özel idari kolluk ya kamu düzeninin unsurlarından bir veya birkaçı üzerine ya da bu unsurlardan tamamen farklı bir alan veya korunmak istenen değer üzerine daha özel koruma ve müeyyide ihtiyacı nedeniyle faaliyet yürütmektedir¹²⁴.

Genel kolluk İçişleri Bakanlığına bağlıdır ve ülkedeki emniyet ve asayişten Bakan sorumludur¹²⁵. 5442 sayılı İl İdaresi Kanunu m. 11 uyarınca vali il sınırları dâhilinde, m. 32 uyarınca ise kaymakam ilçe sınırları dâhilinde genel ve özel kolluk teşkilatının amiridir. Vali ve kaymakam kamu düzenini koruma yetkilerini emniyet ve jandarma aracılığıyla yürütür. Genel kolluk arasında yer alan polis şehirde, jandarma kırsalda, sahil güvenlik karasularında, gümrük memurları gümrüklerde ve orman muhafaza memurları ormanlarda genel kolluk yetkilerini kullanır¹²⁶. Özel kolluk ise genel kolluk dışında kalan ve özel kanunlarla oluşturulmuş kolluktur¹²⁷. Genel idari

¹²⁰ Yenisey, **Kolluk Hukuku**, s. 131.

¹²¹ Yenisey, **Kolluk Hukuku**, s. 132.

¹²² Yenisey, **Kolluk Hukuku**, s. 128-129.

¹²³ Özay, **a.g.e.**, s. 727.

¹²⁴ Özay, **a.g.e.**, s. 734; Gözler, **a.g.e.**, s. 503.

¹²⁵ 3201 sayılı Emniyet Teşkilatı Kanunu m. 1/1.

¹²⁶ Yenisey, **Kolluk Hukuku**, s. 40.

¹²⁷ 3201 sayılı Kanun m. 3/1.

kolluk haricinde özel idari kolluğa ihtiyaç duyulmasının sebebi özel koruma ihtiyacı ve ihtisaslaşma isteğidir¹²⁸.

7245 sayılı Çarşı ve Mahalle Bekçileri Kanunu uyarınca çarşı ve mahalle bekçileri de genel kolluğa yardımcı bir kolluk türüdür. Kanun’da sayılan görevlerine bakıldığında bunların bir kısmının “bir kimsenin can, mal ve ırzına saldırma ve tehditleri önlemek”¹²⁹ biçiminde suç işlenmesini önlemek, bir kısmının ise “şüphelileri yakalamak”¹³⁰ ceza muhakemesine hizmet etmek amacına yönelik olduğu görülür. Bu iki amaç da Kolluk ve Ceza Adaleti Direktifi’nin kişisel veri işlemesine cevaz verdiğinden çarşı ve mahalle bekçilerinin kişisel veri işlemede veri sorumlusu olabileceği sonucuna varılır. Ancak Kanun çarşı ve mahalle bekçilerine halkın istirahat, sağlık ve selametini sağlamak¹³¹ gibi görevler de yüklediğinden bu görevlerin ifası amacıyla kişisel veri işleme faaliyetleri Kolluk ve Ceza Adaleti Direktifi’nin uygulama alanı dışındadır. Bu halde çarşı ve mahalle bekçileri GDPR uyarınca veri sorumlusu olacaklardır. Özetle idari kolluğun ceza hukuku anlamında suç işlenmesinin önlenmesi amacıyla yetkilerini kullanarak kişisel veri işlemesi halinde kolluk, Kolluk ve Ceza Adaleti Direktifi hükümleri uyarınca veri sorumlusu olabilecektir.

3. Özel Güvenlik Görevlileri

Günümüzde alışveriş merkezleri, spor tesisleri gibi kamuya açık alanlarda güvenlik ihtiyacının genel kolluk ile karşılanması yetersizdir. Bu alanlarda güvenliğe duyulan özel ihtiyaç nedeniyle kolluk hizmetinin dışında özel kişiler aracılığıyla özel güvenlik hizmetleri verilmektedir¹³². Bu güvenlik hizmetinin verilmesi sırasında da en sık olarak korunan alanlar kamera ile izlenmekte ve kişisel veriler işlenmektedir. Yalnız izleme bir kişisel veri işleme faaliyeti olmadığından ve özel güvenliğin hizmet verdiği alanlara girerek kişilerin örtülü rıza gösterdikleri söylenebilir. Ancak özel güvenlik tarafından görüntülerin kayda alınması, kişisel veri işleme faaliyetidir ve özel

¹²⁸ Gözler, **a.g.e.**, s. 530; Yenisey, **Kolluk Hukuku**, s. 62.

¹²⁹ 7245 sayılı Kanun m. 6/1-e.

¹³⁰ 7245 sayılı Kanun m. 8/1-a.

¹³¹ Bkz. 7245 sayılı Kanun m. 5.

¹³² Yenisey, **Kolluk Hukuku**, s. 72.

güvenliğin bu şekilde kişisel veri işleyebileceğine dair 5188 sayılı Özel Güvenlik Hizmetlerine Dair Kanun'da düzenleme yoktur¹³³.

Özel güvenlik hizmetlerinde görev alanların veri sorumlusu olup olamayacağı değerlendirilmelidir. Kolluk ve Ceza Adaleti Direktifi'ne göre işlenen veriler, suçların önlenmesi, ceza muhakemesi ve infaz sürecine ilişkin olduğundan yalnız kolluk ve mahkemeler gibi klasik ceza adalet sistemi süjesi olan ve kamusal güç kullananların veri sorumlusu olduğu düşünülebilir. Oysa Kolluk ve Ceza Adaleti Direktifi'nin "Tanımlar" kısmında veri sorumlusu olan yetkili makam ikiye ayrılarak gruplandırılmıştır ve ilk grupta her ne kadar "kamu otoritesi" olma şartı aranmışsa da ikinci grupta bu şart yer almamaktadır. *AB üyesi devletin kanunları tarafından, kamu güvenliğine yönelik tehditler de dâhil suçların önlenmesi, soruşturulması, ortaya çıkarılması veya kovuşturulması ya da cezaların infazı amacıyla kamu otoritesini ve kamu yetkileri kullanılmak üzere verilen diğer herhangi bir kurum veya kuruluş*¹³⁴ olmak, veri sorumlusu olmak için yeterlidir.

Türk hukukunda güvenlik hizmetleri, *kişi veya kuruluşların talebi üzerine güvenlik hizmeti hizmet sözleşmesi ile istihdam edilen personel tarafından, kurum veya kuruluşlar bünyesindeki özel güvenlik birimleri tarafından veya güvenlik şirketleri tarafından* yürütülmektedir¹³⁵. Türk hukukunda özel güvenlik görevlilerine yetkiler bahşeden kanun, 5188 sayılı Kanun'dur ve bu Kanun, kamu güvenliğini tamamlayıcı mahiyetteki hizmetlerin ifası esaslarını düzenlemektir. Kanaatimizce Kolluk ve Ceza Adaleti Direktifi, kamu güvenliğine yönelik tehditlerin önlenmesi faaliyetinde bulunan kurum ve kuruluşlar bakımından kamu tüzel kişisi olma şartı aramadığından özel güvenlik şirketleri de veri sorumlusu olabilecektir¹³⁶. Örneğin adliyelerde kamu güvenliğini sağlamak amacıyla özel güvenlik görevlileri bulunmaktadır. Avukat girişlerinde barokart okutulmakta ve barokartın okutulmasıyla kişinin fotoğraf, ad, soyad ve avukat, stajyer olduğu bilgisi elektronik tabelalarda görünmektedir. Bu kişisel veriler adliye girişindeki turnikelerde bulunan herkesin görebileceği biçimde

¹³³ Yenisey, **Kolluk Hukuku**, s. 77.

¹³⁴ Kolluk ve Ceza Adaleti Direktifi m. 3/7-b.

¹³⁵ Bkz. 5188 sayılı Kanun m. 3/2.

¹³⁶ Aynı yönde bkz. Baran Kızıllırmak, "Kişisel Verilerin İşlenmesinde Adli ve Önleyici Amaçla Öngörülen İstisnaların Ulusal ve Uluslararası Hukuka Göre Değerlendirilmesi", **Kadir Has Üniversitesi Hukuk Fakültesi Dergisi**, c. 7, s. 2, 2019, s. 243.

işlenmektedir. Dolayısıyla bu veri işleme faaliyeti özel güvenlik tarafından gerçekleşse de Kolluk ve Ceza Adaleti Direktifi kapsamındadır ve Direktif'in gereklerine uygun olmalıdır. Ancak 5188 sayılı Kanun'da özel güvenlik hizmetleri sırasında suçların önlenmesi, ceza muhakemesi veya cezaların infazına dair kişisel veri işleme yetkisi özel güvenlik şirketlerine ve görevlilerine verilmemiştir. Bu nedenle bahsi geçen veri işleme faaliyeti kanuna dayanmadığından hukuka aykırıdır. Güvenliği sağlamak amacıyla kişinin avukat yahut stajyer olup olmadığı bilgisinin yalnızca güvenlik görevlisinin ekranında yansması veya turnikeden okutulması yeterli iken verinin bu şekilde alenileştirilmesi aynı zamanda orantılı ve gerekli de değildir.

C. Veri Sorumlusunun Yükümlülükleri

1. Teknik ve İdari Tedbirler Almak

Teknik ve idari tedbirler, kişisel verilerin korunması ve veri güvenliğinin sağlanması için gereklidir. Verilerin güvenliği ise verilerin kaybedilmesi, yetkisiz kişilerin erişimine açılması, verilerin tahrip edilmesi, değiştirilmesi veya alenileştirilmesi gibi tüm risklere karşı uygun güvenlik önlemlerinin alınarak verilerin korunmasıdır¹³⁷. Verileri korumak için yetkilendirme ve doğrulama mekanizmaları önemlidir ve hassas bilgiler her zaman şifrelenmelidir. Güvenlik seviyesinin uygun olup olmadığını düzenli olarak kontrol etmek için bir denetim rejimi olması en iyi yöntem olarak kabul edilmektedir¹³⁸. Alınacak teknik ve idari tedbirler kişisel verinin mahiyetine uygun olmalıdır. Örneğin biyometrik veriler bakımından şifreleme/kriptolamaya başvurulabilir¹³⁹. Kriptografik yöntemlere başvurulmasıyla da şifreler

¹³⁷ Karabulut, **a.g.e.**, s. 47.

¹³⁸ Allen, van Beek, Borking, **a.g.e.**, s. 16.

¹³⁹ Bkz. Paşaoğlu, Adje, Demirtaş, **a.g.e.**, s. 41. Biyometrik verileri bilgisayarda depolamak için kullanılan biyometrik şifreleme sistemi yaklaşımında biyometrik veri şablonunu korumak için yardımcı verilerden yararlanır. Şifreleme için kullanılan yardımcı verilere, biyometriden bağımsız olması halinde (örneğin, yalnızca bir matematiksel işlev) ve biyometrik şablondan türetilmesi durumunda anahtar oluşturma veya anahtar çıkarma denir. Herhangi bir anahtarlama yapılmadan önce biyometrik veriler dijital görüntü olarak kabul edilir. Daha sonra daha küçük bir boyuta inceltilir ve ikili resme dönüştürülür. Bu işlemlerden sonra, anahtarlama yapılır. Bu anahtar biçimi, sıradan bir şifreleme kombinasyonundan çok daha ileridir, çünkü anahtarlama sonrası elde edilen desen bulanıklaşmıştır. Anahtar çıkarma işleminde, bu bulanıklık, dönüştürüldüğü matematiksel biçimin bilinmesi nedeniyle çözülebilir.

vasıtasıyla muhafaza edilen kişisel verilere, erişime yetkili olan kimseler haricinde ulaşamayacaktır¹⁴⁰.

Kolluk ve Ceza Adaleti Direktifi m. 7/2'ye göre veri sorumluları yanlış, eksik veya güncel olmayan kişisel verilerin iletilmemesini veya erişilebilir olmamasını sağlamak üzere tüm makul tedbirleri almalıdır. Veri sorumlusu, veri aktarımı halinde verinin bu niteliğini kontrol etmekle yükümlüdür. Buna rağmen kişisel veri yanlış, eksik veya güncel olmayan biçimde paylaşılmışsa veri alıcısına bildirimde bulunulmalı ve ayrıca veri sahibinin düzeltme ve sildirme haklarından yararlanabilmesi için bilgilendirme yapılmalıdır. Kolluk ve Ceza Adaleti Direktifi m. 19'a göre veri sorumlusu; işlenen verilerin niteliğini, kapsamını, içeriğini ve amaçlarını, ayrıca gerçek kişilerin hak ve özgürlüklerine ilişkin değişen olasılık ve riskleri göz önünde bulundurarak uygun teknik ve idari tedbirleri almalıdır ve alınan bu tedbirler gözden geçirilip güncellenmelidir.

Kolluk ve Ceza Adaleti Direktifi'nin 29. maddesi kişisel verilerin otomatik yollarla işlenmesi halinde veri sorumlusunu risk değerlendirmesi yapmakla yükümlendirmiş ve bu değerlendirme sonucunda da bazı amaçlara yönelik hangi tedbirlerin alınacağını da saymıştır:

- (a) yetkisiz kişilerin işleme için kullanılan ekipmanlara erişimini reddetmek (ekipman erişim kontrolü)
- (b) veri ortamının yetkisiz okunması, kopyalanması, değiştirilmesi veya kaldırılmasını engellemek (veri medya kontrolü)
- (c) depolanmış kişisel verilere yetkisiz girilmesinin ve saklanan kişisel verilerin yetkisiz kontrolü, değiştirilmesi veya silinmesini önlemek (depolama kontrolü)
- (d) veri iletişim ekipmanı kullanan yetkisiz kişilerce otomatik işlem sistemlerinin kullanılmasını önlemek (kullanıcı kontrolü)

¹⁴⁰ Sevgi Eraslan Türkmen, **Özel Nitelikli Kişisel Verilerin İşlenmesinde Açık Rızanın Aranmadığı Haller**, İstanbul, On İki Levha Yayıncılık, 2019, s. 142.

- (e) *otomatik bir işleme sistemi kullanmaya yetkili kişilerin, yalnızca erişim yetkilerinin kapsadığı kişisel verilere erişebilmelerini sağlamak (veri erişim kontrolü)*
- (f) *veri iletişim ekipmanı kullanılarak kişisel verilerin iletildiği veya iletilebileceği ya da kullanılabilir olabileceğini doğrulamak (iletişim kontrolü)*
- (g) *otomatik işleme sistemlerine hangi kişisel verilerin girildiğini ve kişisel verilerin ne zaman ve kim tarafından girildiğini (giriş kontrolü) doğrulamanın ve tespit etmenin mümkün olduğundan emin olmak*
- (h) *kışisel veri transferleri sırasında veya veri ortamının nakliyesi sırasında (taşıma kontrolü) kişisel bilgilerin yetkisiz okunması, kopyalanması, değıştirilmesi veya silinmesini engellemek*
- (i) *kurulu sistemlerin, kesintiler halinde geri yüklenebileceğinden emin olmak (kurtarma)*
- (j) *sistemin işlevlerini yerine getirdiğinden, işlevlerdeki hataların görüldüğünden (güvenilirlik) ve sistemin hatalı çalışması (bütünlük) nedeniyle saklı kişisel verilerin bozulmamasını sağlamak.*

Kişisel verilerin mahiyetine göre veri sorumlusunun alması gereken teknik ve idari tedbirler de farklılaşabilmelidir. Nitekim doğrudan bir kişinin beyanına dayanan veriler, dolaylı yolla toplanan veriden farklı mahiyettedir. Maddi olgulara dayanan veriler (*hard data*), görüşlere veya kişisel değerlendirmelere dayanan verilerden (*soft data*) farklı olarak değerlendirilmeli¹⁴¹ ve bu verilerin işlenmesinde buna uygun tedbirler alınmalıdır.

a. Nesnelerin İnterneti ve Veri Güvenliğı

İnternet aracılığıyla operasyonel faaliyetlerde kolluk makamlarına gönderilen ya da bu makamlardan alınan kişisel veriler, günümüzde yaygın olan nesnelerin internetine¹⁴² (*Internet of Things/ IoT*) örnektir. Potansiyel güvenlik açıklarına karşı

¹⁴¹ Allen, van Beek, Borking, **a.g.e.**, s. 12.

¹⁴² Bkz. Allen, van Beek, Borking, **a.g.e.**, s. 18; "Fiziksel aygıtların, araçların ("bağı aygıtlar" ve "akıllı aygıtlar" olarak da bilinir), binaların ve bu nesnelerin toplanmasını sağlayan elektronik, yazılım, sensörler, aktüatörler ve ağ bağlantısına sahip diğer öğelerin birbirine bağlanması ve veri değışimi".

IoT, veri güvenliği ve siber saldırılara karşı dayanıklılık sağlamak için veri doğrulama, erişim kontrolü gibi tedbirlerin alınmasını gerektirmektedir. Örneğin potansiyel güvenlik açıkları ışığında, kolluk makamları tarafından kullanılan akıllı gözlükler¹⁴³, doğrudan bir ulusal sabıka kaydı veri tabanına bağlanmamalı ve toplanan verilerin yüksek düzeyde bir güvence altına alınması sağlanmalıdır¹⁴⁴.

b. Büyük Veri Bakımından Alınacak Tedbirler

Büyük veri bakımından veri sorumluları ayrıca idari ve teknik bazı gereklilikleri sağlamalıdır. Veri doğruluğunun, verinin içeriğinin ve alaka düzeyinin doğrulanması, büyük veri kullanan veri sorumlusunun genel kişisel veriye göre sorumluluk düzeyini artırmaktadır. Bu nedenle büyük veri uygulamaları kolluk ve adli makamların faaliyetlerinde kullanıldığında, büyük veri analizinden elde edilen sonuçları tamamlayan soruşturma yöntemleri ile birleştirilecektir.

Bireyleri etkileyen bir karar, yalnızca kişisel verilerin otomatik olarak işlenmesi sonucu alınmamalıdır. Yani yapılacak tahmini bir analizde, analizin ve sonuçların uygunluğunu değerlendirmek için insan müdahalesine de başvurulmalıdır. Ulusal veya uluslararası düzeyde geliştirilen etik kurallar dikkate alınmalıdır. Mevzuatta belirtilen kısıtlamalara ve istisnalara tabi olarak, verilerin gizlilik ve veri koruma ilkelerine uygun olarak nasıl işlendiği açıklanmalı, böylece veri sorumlusu tarafından şeffaflık sağlanmalıdır.

Bir amaç için toplanan veriler başka bir amaç için kullanılıyorsa, veri sorumlusu veri sahiplerini bu sonraki kullanımdan haberdar etmelidir. Büyük veri uygulamalarında karmaşık yöntemler kullanılsa dahi, işlemenin hukuka uygunluğu,

Nesnelerin interneti sayesinde televizyon, buzdolabı gibi cihazların internete bağlanarak veri göndermesi mümkün olduğundan kişisel verilerin korunması daha da zorlaşmaktadır. Bkz. Yavuz, **a.g.e.**, s. 16.

¹⁴³ Örneğin Çin Henan Eyaleti'nin başkenti Çengçou'da polis, GLXSS olarak adlandırılan akıllı gözlük teknolojisini suçluları yakalamak için kullanmaktadır. Demiryolu istasyonlarındaki kalabalıklarda otuz üç şüpheli bu şekilde gözaltına alınmıştır. Google Glass teknolojisine dayanan gözlük, polislerin şüpheli görünen herhangi bir kişinin fotoğrafını çekmesine olanak sağlamaktadır. Fotoğraflar daha sonra polis veri tabanında incelenmekte ve kişinin adı, adresi, sabıka kaydı ve hatta internet geçmişini içeren bilgiler, 0.25 inçlik ekranda görüntülenmek üzere gözlüğe geri gönderilmektedir. Bkz. "Chinese Police Adopt Smart Glass Technology", Springwise, 14.02.2018, Çevrimiçi <https://www.springwise.com/chinese-police-adopt-smart-glass-technology/#:~:text=Using%20facial%20recognition%20technology%2C%20these,technology%20to%20assist%20police%20work.> 22.09.2020.

¹⁴⁴ Allen, van Beek, Borking, **a.g.e.**, s. 10.

sonraki amaçla veri kullanımı da dâhil olmak üzere AİHS m. 8 ile 108 sayılı Sözleşme’de belirtilen şartlara uygunluk gösterilmelidir. İşleme süresince bir veri güvenliği politikası uygulanmalıdır. Veri sorumlusu, kişisel verilerin işlenmesinin, büyük veri uygulamalarının bireyleri etkileyen kararların alınmasında kullanıldığında bu kararlara karşı idari ve adli yargı yoluna başvurabileceği bilgisini veri sahibine sağlamalıdır¹⁴⁵.

2. Logging Kayıtları Tutmak

Logging, elektronik ortamdaki kişisel verilerin belirlenmiş kurallar dâhilinde zaman damgalı ve otomatik olarak işlenmesi olup sistem üzerindeki tüm işlem hareketlerinin kaydının tutulmasına olanak sağlamaktadır¹⁴⁶. Kolluk ve Ceza Adaleti Direktifi uyarınca kayıt tutma yükümlülüğü hem veri sorumlusu hem de veri işleyene yüklenmiştir. Veri sorumlusu ve işleyenlerin her biri, kendi sorumluluk alanındaki tüm veri işleme faaliyeti kategorilerine ilişkin kayıtları ve logging kayıtlarını yazılı olarak ya da dijital ortamda¹⁴⁷ tutmak ve denetleyici makamın talebi üzerine bu kayıtları ibraz edecek biçimde hazır bulundurmakla yükümlüdür¹⁴⁸.

Veri sorumlusunun tutmakla yükümlü bulunduğu kayıtlarda şu bilgiler yer almalıdır:

- (a) *Veri sorumlusunun ve varsa müşterek veri sorumlusunun ve veri koruma görevlisinin kimliği ve iletişim bilgileri*
- (b) *Veri işlemenin amaçları*
- (c) *Üçüncü ülke veya uluslararası kuruluşlar da dâhil verinin aktarıldığı veya aktarılacağı veri alıcısı kategorileri*
- (d) *Veri sahibinin ve kişisel verilerinin tabi olduğu kategorilerin tanımı*
- (e) *Varsa profillemenin kullanım bilgisi*
- (f) *Varsa üçüncü bir ülkeye ve uluslararası kuruluşlara veri aktarımı kategorileri*

¹⁴⁵ Allen, van Beek, Borking, **a.g.e.**, s. 10-11.

¹⁴⁶ Eraslan Türkmen, **a.g.e.**, s. 143.

¹⁴⁷ Dülger, Özkan, **a.g.e.**, s. 118.

¹⁴⁸ Bkz. Kolluk ve Ceza Adaleti Direktifi resital m. 56.

- (g) *Veri aktarımı ve verilerin ne amaçla işlendiği de dâhil olmak üzere veri işleminin hukuki dayanağı*
- (h) *Varsa farklı veri kategorilerinin silinmesi için planlanan süre*
- (i) *Mümkünse m. 29/1 gereği alınan teknik ve idari tedbirlere ilişkin genel bilgiler*

Ancak veri işleyen bakımından tutulması gereken kayıtların muhtevası görece olarak dar olup şu bilgilerden oluşmaktadır:

- (a) *Veri işleyen (/ler) ile bu işleyenlerin hangi veri sorumlusu adına hareket ettikleri ve varsa veri koruma görevlisinin kimliği ve iletişim bilgileri*
- (b) *Her bir veri sorumlusu adına yapılan veri işleme faaliyeti kategorileri*
- (c) *Gereken durumlarda, verilerin veri sorumlusunun talimatı ile bir üçüncü ülke veya uluslararası kuruluşa aktarıldığı bilgisi ve veri alıcısının kimliği*
- (d) *Mümkünse m. 29/1 gereği alınan teknik ve idari tedbirlere ilişkin genel bilgiler.*

Logging, GDPR’da düzenlenmeyen ve veri işleme faaliyetlerinin kötüye kullanılmasının tespitine olanak sağlayan bir kayıt tutma faaliyetidir. Örneğin adli kolluk faaliyeti ile görevli kılınmış bir kolluk görevlisinin soruşturma amacı dışında kendi menfaatine ilişkin kişisel veri toplaması halinde, veri sorumlusu, denetleyici makam veya yargı makamlarının logging kayıtlarından yararlanarak bu kolluk görevlisini tespit etmesi bir hayli kolay olacaktır¹⁴⁹.

Logging kayıtları en azından; kişisel verilerin toplanması, değiştirilmesi, istişare amacıyla verilere başvurulması, aktarım dâhil olmak üzere verinin açıklanması, bir araya getirilmesi ve silinmesinde tutulmalıdır¹⁵⁰. Bu kayıtlar, kişisel verilere istişare ve erişime açma kayıtlarını, bu işlemlerin gerekçelerini, tarihini ve saatini ve mümkünse kişisel verilere başvuran ve erişebilen kişinin kimliğini ve bu kişisel verilerin alıcılarının kimliğini tespit edecek biçimde tutulmalıdır. Logging

¹⁴⁹ Dülger, Özkan, **a.g.e.**, s. 119.

¹⁵⁰ Kolluk ve Ceza Adaleti Direktifi m. 25.

kayıtları sayesinde hangi veri işleme faaliyetinin kim tarafından yapıldığının tespiti olanaklıdır, bu da usulsüz veri işleyenin tespiti bakımından hayati önem taşımaktadır¹⁵¹. Logging kayıtlarının kullanımı; veri işleme faaliyetinin hukuka uygunluğunun tespiti, iç denetim, veri bütünlüğü ve güvenliğinin sağlanması ve ceza muhakemesi işlemleri ile sınırlıdır. Kolluk ve adli makamların veri işleme faaliyetlerinde detaylı bir raporlama yapmaları gerektiğinden bu logging kayıtları aynı zamanda kovuşturma safhasında da kullanılabilecektir¹⁵².

3. Veri İhlal Bildiriminde Bulunmak

a. Bildirimin Denetleyici Makama ve Üye Devletin Veri Sorumlusuna Yapıldığı Haller

Veri ihlal bildirimleri, öncelikle denetleyici makama yapılacaktır. Bildirim veri sorumlusu tarafından ihlalin öğrenilmesinden itibaren gecikmeksizin yetmiş iki saat içinde denetleyici makama yapılmalıdır. Veri işleyenin bulunması halinde genellikle kişisel veri ihlalinin ilk haberdar olacak kişi veri işleyen olduğundan, veri işleyen veri ihlalini öğrenir öğrenmez durumu veri sorumlusuna bildirmelidir¹⁵³. Ancak kişisel veri ihlalinin, bireylerin hak ve özgürlükleri için yüksek bir risk taşıması durumunda veri sahibine de bildirimin yapılması gerekmektedir¹⁵⁴. Ayrıca veri sorumlusunun kişisel verileri başka bir üye devletin veri sorumlusundan alması halinde veya bizzat veri aktarması halinde bu bildirim, makul süre içinde ayrıca o üye devletin veri sorumlusuna da yapılmalıdır¹⁵⁵.

Bildirimin kapsamında aktarılabilecek asgari bilgi içeriği; esas olarak veri ihlalinin mahiyeti, veri sahibi kategorileri ve yaklaşık sayısı, ilgili veri kayıt kategorileri ve yaklaşık sayısı ile birlikte tarifi, veri koruma görevlisi veya başka irtibat kişilerinin ismi ve iletişim bilgileri, kişisel veri ihlalinin olası sonuçlarının tarifi, kişisel veri ihlali

¹⁵¹ Çam, **a.g.e.**, s. 118.

¹⁵² Bilişim ve Teknoloji Hukuku Enstitüsü, **a.g.e.**, s. 10.

¹⁵³ Kolluk ve Ceza Adaleti Direktifi m. 30/1 ve 30/2.

¹⁵⁴ Kolluk ve Ceza Adaleti Direktifi m. 31.

¹⁵⁵ Kolluk ve Ceza Adaleti Direktifi m. 30/6.

karşısında alınan veya alınması teklif edilen olası olumsuz etkileri azaltabilecek tedbirler de dâhil diğer tedbirlerin tarifinden oluşmaktadır¹⁵⁶.

Veri ihlal bildirimi kapsamında yer alan tüm bilgilerin aynı anda temin edilip Kolluk ve Ceza Adaleti Direktifi'nin belirttiği gibi makul süre içinde denetleyici makam veya üye devletin veri sorumlusuna sağlanması veri sorumlusundan beklenmeyecektir. Zira beklenmesi halinde veri sahibinin zarara uğrama riskinin azaltılması veya önlenmesi mümkün olmayabilir. Bu nedenle Kolluk ve Ceza Adaleti Direktifi, bilgilerin gecikmeye mahal vermeden tedrici olarak sağlanmasına olanak tanımıştır¹⁵⁷.

b. Bildirimin Doğrudan Veri Sahibine Yapıldığı Haller

Bazı hallerde kişisel veri ihlali, veri sahibinin hak ve özgürlükleri bakımından o denli yüksek risk taşır ki veri sahibinin kişisel verisi üzerindeki kontrol yetkisini¹⁵⁸ kullanabilmesi için veri sorumlusunun bildirimi doğrudan veri sahibine yapması gerekir. Kolluk ve Ceza Adaleti Direktifi m. 31, buna olanak sağlamakla birlikte açıkça hangi veri ihlallerinin yüksek risk taşıdığını ve doğrudan veri sahibine bildirimi gerektirdiğini belirtmemiştir. Kolluk ve Ceza Adaleti Direktifi, veri sahibinin veri koruma konusunda uzman olmayabileceği gerçeğine binaen bu bildirimin, açık ve net bir üslupla veri ihlalini anlatmasını aramıştır. Buna göre veri koruma yetkilisi veya irtibat kişilerinin ismi ve iletişim bilgileri, kişisel veri ihlalinin olası sonuçlarının tarifi, kişisel veri ihlali karşısında alınan veya alınması teklif edilen olası olumsuz etkileri azaltabilecek tedbirler de dâhil diğer tedbirlerin bildirimde bulunmasını aramıştır.

¹⁵⁶ Kolluk ve Ceza Adaleti Direktifi m. 30/3.

¹⁵⁷ Bkz. Kolluk ve Ceza Adaleti Direktifi m. 30/4.

¹⁵⁸ WP29'a göre kontrol edilebilirlik (*controllability*), bir bilişim sisteminde veri sahibinin kişisel verileri ile ilgili etkili kontrol araçları imkânının bulunmasını gerektirir. Rıza ve itiraz ile ilgili bu türden imkânlar teknolojik araçlarla desteklenmelidir. Akıntunde, **a.g.e.**, s. 8; Birey kontrolü (*individual's control*) için bkz. Jasserand-Breeman, **a.g.e.**, s. 20. GDPR resital m. 7'de gerçek kişilerin kişisel verilerini kontrol edebilecekleri açıkça belirtilmiştir. Direktif'te ise gerçek kişilerin, ayrımcılığa yol açabilecek şekilde profillemeye maruz kaldığında kişisel verileri üzerinde kontrolden mahrum kalacağı resital m. 51'de; kişisel verileri üzerindeki kontrolü kaybetmesi hallerinde veri ihlal bildiriminde bulunulacağı resital m. 61'de belirtilmiştir. Böylece üstü kapalı biçimde de olsa *argumentum a contrario* biçimde Direktif de bireylerin kişisel verileri üzerinde kontrol hakkına sahip olduğunu kabul etmiştir.

Ancak veri ihlal bildirimine ilişkin maddenin lafzından da anlaşılacağı üzere esas olan; denetleyici makama, verilerin başka bir üye devletle paylaşılması halinde ise o devletin veri sorumlusuna bildirimin yapılmasıdır. Bu nedenle Kolluk ve Ceza Adaleti Direktifi yüksek risk içeren halleri açıkça belirtmemişse de doğrudan veri sahibine bildirim yapılmasının gereksiz olduğu hallere yer vermiştir¹⁵⁹. Veri sorumlusu; şifreleme gibi veriye erişim yetkisi olmayanlara veriyi anlaşılabilir kılacak uygun teknolojik ve idari tedbirleri uygulamış, veri sahiplerinin hak ve özgürlüklerine yönelik yüksek riskin ortadan kalkması için gerekli önlemleri almışsa veya veri sahibine yapılacak bildirim orantısız bir çaba gerektirecekse artık veri sahibine doğrudan veri ihlal bildirimi yapılması gerekmemektedir. Orantısızlık; bildirimin yapılması için katlanılacak zorluk ve bildirimin yapılması ile korunan menfaat arasında dengesizlik bulunmasını ifade eder, yani veri sahibine yapılacak bildirimin ciddi bir külfet olması halidir. Bu halde bildirim yapılmayacaksa da veri sahiplerine eşit derecede etkili bir şekilde bilgi verilen kamuya açık bir iletişim veya benzeri bir tedbir bulunmalıdır.

4. Veri Koruma Görevlisi Tayin Etmek

Veri koruma görevlisi, veri işleme faaliyetinin gereklerine uygunluğu gözetken ve veri sorumlusunu bilgilendirip görüş beyan eden uzmandır¹⁶⁰. Kolluk ve Ceza Adaleti Direktifi m. 32 ile veri sorumlusuna veri koruma görevlisi tayin etme yükümlülüğü getirilmiştir.

Veri koruma görevlisi tayin etme yükümlülüğü, 95/46 sayılı Direktif ile ilk kez AB veri koruma mevzuatına girmiştir ve GDPR m. 37’de de bulunmaktadır. Ancak bu yükümlülük, Kolluk ve Ceza Adaleti Direktifi kapsamında ihtiyaridir. Mahkeme ve

¹⁵⁹ Bkz. Kolluk ve Ceza Adaleti Direktifi m. 31/3 “(a) veri sorumlusu uygun teknolojik ve organizasyonel koruma önlemlerini uygulamış ve bu önlemler kişisel veri ihlali nedeniyle etkilenen kişisel verilere, özellikle kişisel verileri şifreleme gibi, erişim yetkisi olmayan herhangi bir kişi için anlaşılabilir hale gelmişse

(b) veri sorumlusu veri sahiplerinin hak ve özgürlükleri için yüksek riskin artık gerçekleşme olasılığını ortadan kaldıran müteakip tedbirler almışsa

(c) bildirim orantısız bir çaba gerektirecekse. Bunun yerine veri sahiplerine eşit derecede etkili bir şekilde bilgi veren kamuya açık iletişim veya benzer bir önlem söz konusu olacaktır.”

¹⁶⁰ Dülger, Özkan, **a.g.e.**, s. 125.

diğer adli makamlar yargısal yükümlölükleri kapsamında hareket ediyorlarsa bu yükümlölükten muaf tutulabilecektir. Veri sorumlusunun veri koruma görevlisi tayin etme yükümlölüğü mevcutken, teklifin aksine Kolluk ve Ceza Adaleti Direktifi'nde veri işleyenin bu yükümlölüğü bulunmamaktadır¹⁶¹.

5. Tasarımdan ve Başlangıçtan İtibaren Veri Koruma Yükümlölüğü

Veri sorumlusu özellikle kişisel verileri depolanması ve verilere erişilmesi için yeni bilgi teknolojileri (*Information Technologies/ IT*) sistemleri kurarken, gizlilik etkileri olan kanunlar, politikalar veya stratejiler geliştirirken ve yeni amaçlar için verileri kullanırken veri koruma girişimi başlatmalıdır¹⁶². Kolluk ve Ceza Adaleti Direktifi, veri işleme faaliyetinin ilk aşamasından başlayarak yani başlangıçtan itibaren (*data protection by default*) ve tasarımdan itibaren veri koruması (*data protection by design*) ilkeleri ile veri sorumlularının sorumluluğunu genişletmiştir¹⁶³.

Kolluk ve Ceza Adaleti Direktifi, tasarımdan itibaren veri korumasının bir örneği olarak teknik ve idari bir tedbir olan psödönimleştirmeyi düzenlemiştir. Psödönimleştirme, Kolluk ve Ceza Adaleti Direktifi'ne göre *ek bilgilerin ayrı olarak tutulması ve teknik ve organizasyonel tedbirlerin alınması ile kişisel verilerin ek bilgi olmaksızın belirli bir veri sahibiyle ilişkilendirilmesinin mümkün olmayacak şekilde işlenmesidir*¹⁶⁴. Bu tedbir, maskeleye yahut takma adlılık biçiminde uygulanabilir¹⁶⁵. Psödönimleştirmeye genellikle şifreleme ile birlikte başvurulur. Verinin tamamen anonim hale getirilmesi amaçlanmadığından öncelikle çift yönlü şifreleme yapılır ve böylece, verinin geri dönüştürülmesi yani kişinin tanınmasına olanak veren biçime gelmesi mümkün olur¹⁶⁶. Örneğin CCTV aracılığıyla kişilerin yüzlerinin bulanıklaştırılarak izlenmesi ve kaydedilmesi psödönimleştirmeye örnek olarak verilebilir. Bu halde bir anonimleştirme söz konusu değildir, zira bulanık hale rağmen

¹⁶¹ Bilişim ve Teknoloji Hukuku Enstitüsü, **a.g.e.**, s. 11.

¹⁶² Allen, van Beek, Borking, **a.g.e.**, s. 16.

¹⁶³ Dülger, Özkan, **a.g.e.**, s. 96.

¹⁶⁴ Kolluk ve Ceza Adaleti Direktifi m. 3/5.

¹⁶⁵ Dülger, **Kişisel Verilerin Korunması Hukuku**, s. 99.

¹⁶⁶ Dülger, **Kişisel Verilerin Korunması Hukuku**, s. 100.

kişilerin eşkâli ve bulanık görüntüdeki kıyafet, boy, kilo analizi ile kişiler tespit edilebilir¹⁶⁷.

Başlangıçtan itibaren veri koruması, kişisel verilerin bireyin müdahalesi olmaksızın belirsiz sayıda gerçek kişi tarafından erişilebilir olmasının engellenmesini amaçlamaktadır. Başlangıçtan itibaren veri koruması, işleme veya sistemin kullanım süresi boyunca veri korumaya ilişkin tehdit analizine dair sıkı testler gerektirmektedir. Tasarımdan itibaren veri koruması ise veri güvenliğinin ayrılmaz bir parçasıdır. Tasarımdan itibaren koruma gereği; yüksek düzeyde veri koruması ve güvenliğini sağlamak ve özellikle veri ihlal olasılığını en aza indirmek için doğrudan veri sistem ve işlemlerine ilişkin teknik ve idari tedbirler alınmalıdır¹⁶⁸. Bu yaklaşım, baştan beri gizliliği ve veri korumaya uyumu teşvik ederek *gizlilikle tasarım* olarak bilinir ve yazılım ve/veya donanım yoluyla sağlanabilir¹⁶⁹.

Veri sahibinin menfaati ve veri sorumlusunun genellikle ekonomik kaygı ve menfaatleri arasında denge kurulmasının sağlanması için tasarımdan itibaren veri koruması, büyük veri uygulamalarının yazılım aşamasında hayati öneme sahiptir. Bu nedenle tarafların menfaatleri arasında makul denge ve her bir somut olay öngörülerek algoritma tasarlanmalıdır¹⁷⁰. Ayrıca Kolluk ve Ceza Adaleti Direktifi; verilerin kötüye kullanımının önlenmesi için erişim kontrolü, şifreleme, denetim kayıtlarının tutulması, veri minimizasyonu, veri saklamanın tasnif dâhilinde yapılması gibi koruma önlemleri alınması da tavsiye etmiştir¹⁷¹.

6. Veri Koruma Etki Değerlendirmesi

Kolluk ve Ceza Adaleti Direktifi m. 27'ye göre veri sorumlusu, veri işleme faaliyetine başlamazdan evvel bu faaliyetin kişisel verilerin korunması üzerindeki etkisine ilişkin değerlendirme yapmalıdır. Yani polis ve ceza adaletinde kişisel verilerin işlenmesinde yeni teknolojiler kullanıldığında, veri koruma risklerini

¹⁶⁷ Dülger, *Kişisel Verilerin Korunması Hukuku*, s. 100.

¹⁶⁸ Allen, van Beek, Borking, *a.g.e.*, s. 16.

¹⁶⁹ Allen, van Beek, Borking, *a.g.e.*, s. 16.

¹⁷⁰ Aşıkoglu, *a.g.e.*, s. 174.

¹⁷¹ Bkz. Kolluk ve Ceza Adaleti Direktifi m. 20/2.

mümkün olan en iyi şekilde azaltmak için bir veri koruma etki değerlendirmesinin yapılması gerekmektedir¹⁷², zira maddenin lafzı da bu değerlendirmenin ihtiyarı olmadığını göstermektedir¹⁷³.

GDPR’da da bulunmakla birlikte veri koruma etki değerlendirmesi özellikle ceza muhakemesi sürecinde özel nitelikli kişisel verilerin işlenmesi söz konusu olduğunda daha da önemli bir fonksiyon icra etmektedir¹⁷⁴. Zira özel nitelikli kişisel verilerin işlenmesinde, diğer kişisel verilere nazaran daha katı bir denetim söz konusu olacaktır¹⁷⁵. Bu durumda da ayrımcılığa maruz kalma, maddi zarara uğrama, meslek sırrının ifşası gibi kişilerin temel hak ve özgürlüklerinin ihlali riskinin bulunması halinde riskin boyutu, veri işlemenin muhtevası ve amaçları gözetilerek belirlenmelidir¹⁷⁶. Etki değerlendirmesi, risklerin ortaya çıktığı anda başlamalıdır. Değerlendirmeye yükümlü makam, veri sorumlusudur. Değerlendirmenin kapsamı Kolluk ve Ceza Adaleti Direktifi m. 27/2’de öngörülen veri işleme faaliyeti, riskin ortadan kaldırılması için alınacak tedbirler ve veri sahiplerinin menfaatlerini gözetecek mekanizmalardan oluşmaktadır.

Yapılan veri koruma etki değerlendirmesine göre daha az müdahale ile verilerin işlenmesindeki amaç gerçekleştirilecek ise bu durumda daha az müdahaleci olan yaklaşıma başvurulmalıdır¹⁷⁷. Veri sorumlusu; ekipman erişim kontrolü, veri medya kontrolü, depolama kontrolü, kullanıcı kontrolü, veri erişim kontrolü, iletişim kontrolü, giriş kontrolü, taşıma kontrolü, kurtarma ve sistem bütünlüğü, güvenilirlik ve bütünlüğü bakımından risk değerlendirmesi yapmalıdır¹⁷⁸.

Kişî hak ve özgürlükleri bakımından ciddi bir risk taşıyan veri işleme faaliyetlerinde veri sorumlusu veya denetleyici makamlarca yapılacak ön denetim

¹⁷² Kolluk ve Ceza Adaleti Direktifi m. 27/1. Örneğin yeni veri madenciliği teknikleri, olası şüphelilerin belirlenmesi için genişletilmiş imkânlar sunabilir. Bunlar mevcut veri koruma kanunlarına uygunluk bakımından ve bireyin hakları ve veri güvenliği dâhil olmak üzere kişisel verilerin korunması için önerilen güvencelerle birlikte dikkatlice değerlendirilmelidir. Bkz. Allen, van Beek, Borking, **a.g.e.**, s. 9.

¹⁷³ De Hert, Papakonstantinou, **a.g.e.**, s. 17.

¹⁷⁴ Dülger, Özkan, **a.g.e.**, s. 120; Develioğlu, **a.g.e.**, s. 112.

¹⁷⁵ Cemil Kaya, “Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi”, **İÜHFİM**, c. 69, s. 1-2, 2011, s. 324.

¹⁷⁶ Dülger, Özkan, **a.g.e.**, s. 120-121.

¹⁷⁷ Küzeci, **a.g.e.**, s. 468.

¹⁷⁸ Allen, van Beek, Borking, **a.g.e.**, s. 16.

mahiyetindeki kontrollerle hak ve özgürlüklerin korunmasında ciddi bir adım atılmıştır¹⁷⁹. Yapılacak veri koruma etki değerlendirmesi ile veri sahiplerinin hak ve meşru menfaatleri gözetilecek ve veri işleme faaliyetleri, olası ihlal durumları ve bunlara dair koruma tedbirleri yer alacaktır¹⁸⁰.

7. Denetleyici Makamın Görüşüne Başvurmak

Kolluk ve Ceza Adaleti Direktifi m. 28, veri sorumlusu ve veri işleyenlerin yeni bir dosyalama sisteminin bir parçasını oluşturacak veri işlemeden önce, bazı durumlarda¹⁸¹ denetleyici makamın görüşüne başvurmasını zorunlu tutmuştur. Buna göre;

- (a) *yapılan veri koruma etki değerlendirmesine göre veri sorumlusu tarafından riski hafifletmek için alınması gereken tedbirlerin alınmaması nedeniyle veri işlemenin yüksek bir risk doğuracağına ilişkin işaretler varsa veya*
- (b) *özellikle yeni teknolojilerin, mekanizmaların veya prosedürlerin kullanıldığı veri işlemlerin, veri sahibinin hak ve özgürlükleri için yüksek risk içerdiği durumlarda denetleyici makamın görüşüne başvurulması gerekmektedir.*

Denetleyici makam ve veri sorumlusu arasındaki istişare sürecinde; veri sorumlusunun veri işleme faaliyetini tehlikeye atmamak kaydıyla, gerekçeli görüşünü ve değerlendirmesini sunmak için denetleyici makama yeterli fırsat verilmelidir¹⁸².

Denetleyici makam; veri işlemenin Kolluk ve Ceza Adaleti Direktifi'nin gerekleri ile bağdaşmayacağı görüşündeyse ve veri sorumlusu riski tanımlayamamış veya veri sorumlusunun sunduğu tedbirler yeterli değilse; veri sorumlusu ve veri işleyene görüş talebinden itibaren altı ay içerisinde yazılı olarak bu görüşünü sunacak hatta gerekirse m. 47'deki yetkilerini de kullanabilecektir. Veri işlemenin kompleks

¹⁷⁹ Dülger, Özkan, **a.g.e.**, s. 96.

¹⁸⁰ Bostancı Bozbayındır, **a.g.e.**, s. 82.

¹⁸¹ Örneğin, üye devletler kişisel verilerin korunmasına ilişkin mevzuat hazırlık sürecinde de denetleyici makamın görüşüne başvuracaktır.

¹⁸² Allen, van Beek, Borking, **a.g.e.**, s. 9.

yapıda olması halinde altı aylık bu görüş bildirme süresi, veri sorumlusu ve işleyene gerekçesi de belirtilerek bir aya kadar uzatılabilecektir¹⁸³.

Denetleyici makamın görüşüne başvurma, çoğu zaman veri koruma etki değerlendirmesinin tamamlayıcısıdır, özellikle veri işlemede yeni yöntemlere başvurulduğunda risk değerlendirmesinin ardından istişare de yapılmalıdır. Söz gelimi günümüzde yaygın olan otomatik yüz tanıma sistemlerinin ve biyometrik verilerin otomatik yollarla işlenmesine dayalı diğer sistemlerin bireylerin hak ve özgürlüklerine etkisine ilişkin yapılacak risk analizinin ardından, veri saklama süresi, çapraz eşleşme fonksiyonu, verilerin depolandığı yer, veri sahibinin erişimi gibi hususlarda denetleyici makamla istişare yapılmalıdır¹⁸⁴.

III. VERİ İŞLEYEN

A. Tanım

Veri işleyen; veri sorumlusu adına kişisel veri işleyen gerçek veya tüzel kişi, kamu kuruluşu, ajanı veya başka bir organıdır. Veri işleyeni veri sorumlusundan ayıran, kişisel veri işlemenin teknik gereklilikleri ile ilgilenen bir fonksiyonu olmasıdır. Oysa veri sorumlusu karar veren konumdadır¹⁸⁵. Örneğin ceza muhakemesinde veri işleme kararı veren mahkeme veri sorumlusu iken, işlemeyi yerine getiren görevli polis memuru ise veri işleyendir¹⁸⁶.

Hakim tarafından moleküler genetik inceleme yapılması kararı verildiğinde bu incelemeyi yapacak olanlar; *resmen atanan veya bilirkişilikle ya da soruşturma veya kovuşturmayı yürüten makama mensup olmayan veya bu makamın soruşturma veya kovuşturmayı yürüten dairesinden teşkilat yapısı itibarıyla ve objektif olarak ayrı bir birimine mensup olan görevlilerdir*¹⁸⁷. İncelemeyi yapacak olan bu görevlilere CMK

¹⁸³ Kolluk ve Ceza Adaleti Direktifi m. 28/5.

¹⁸⁴ Allen, van Beek, Borking, **a.g.e.**, s. 10.

¹⁸⁵ Sinem Göçmen Uyarer, **Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması**, İstanbul, Seçkin Yayıncılık, 2019, s. 119.

¹⁸⁶ Muhammet Sefa Mutlu, **Kişisel Verilerin Soruşturma Evresinde İşlenmesi ve İnsan Hakları Kapsamında Korunması**, Ankara, Adalet Yayınevi, 2020, s. 112-113.

¹⁸⁷ CMK m. 79/2.

uyarınca bulgunun sahibi kişinin adı, soyadı, adresi ve doğum tarihi bilgisi verilemeyecek ve özel kod sistemi uygulanacaktır¹⁸⁸. Yani moleküler genetik incelemeyi yapan Adli Tıp Kurumu, yükseköğretim kurum ve birimleri ve diğer kuruluşlar veri işleyendir ve Kolluk ve Ceza Adaleti Direktifi bağlamında veri işleyen, kişisel verilerin korunması için yükümlülükler ve gerekleri yerine getirmekle yükümlüdür. Bunun için gerekli teknik ve idari tedbirleri alabilecek yeterlilikte olmalıdır. Ayrıca veri işleyen idari ve teknik tedbirleri yerine getirirken veri sorumlusunun talimatıyla bağlı olacaktır¹⁸⁹.

B. Veri İşleme

1. Yetkili Makam Tarafından İşleme

İşleme, *kişisel veri ya da veri seti üzerinde gerçekleşen elde etme, kaydetme, düzenleme, yapılandırma, depolama, uyarlama, değiştirme, kullanma, yayınlama, yayma veya başka suretle ulaşılabilir hale getirerek ifşa edilme, sıralama, birleştirme, sınırlama, silme, imha etme, başvurma, erişme ve bunlar gibi otomatik yolla ya da manuel gerçekleştirilen her türlü işlemdir*¹⁹⁰. İşleme fiilleri sınırlı sayı prensibine tabi değildir. Örneğin bilgisayar, akıllı telefon, web kamerası, dashcam veya drone kullanılması, kişisel verilerin akıllı cihazlarla toplanması, bir browserın ön belleği veya bir IT sisteminde saklanması, bilgisayar ekranında gösterilmesi kişisel veri işlemedir¹⁹¹.

Üye devletlerin yetkili olmayan makamları tarafından yapılan veri işleme Kolluk ve Ceza Adaleti Direktifi'ne uygun olmayacaktır. Özel hukuk kişilerinin topladığı kişisel verileri kolluk güçleri ile paylaşması durumunda bu veriler, GDPR'a

¹⁸⁸ Nihal Temizsoy Bayram, "Ceza Muhakemesi Hukukunda Moleküler Genetik İnceleme ve Elde Edilen Verilerin Delil Olarak Kullanılması", **İstanbul Üniversitesi Sosyal Bilimler Enstitüsü**, Yayımlanmamış Yüksek Lisans Tezi, İstanbul, 2018, s. 113.

¹⁸⁹ Dülger, Özkan, **a.g.e.**, s. 116.

¹⁹⁰ Kolluk ve Ceza Adaleti Direktifi m. 3/2.

¹⁹¹ Paul Voigt, Axel von dem Bussche, **The EU General Data Protection Regulation (GDPR) A Practical Guide**, Springer, 2017, s. 10.

tabi olacak ve şartları varsa GDPR m. 23'teki istisnalardan faydalanabilecektir¹⁹². 95/46 sayılı Direktif'te suç, ceza mahkûmiyeti ve güvenlik tedbirlerine ilişkin kişisel verilerin işlenmesi ancak resmi makamların kontrolü altında mümkündür¹⁹³. Ancak ceza mahkûmiyetine ilişkin veriler, banka ve sigorta şirketlerinin menfaatlerinin korunması için istisnai bazı hallerde bu kurumlar tarafından da işlenebilecekti. Zira bu hallerde bu türden kurumların ekonomik menfaatlerinin korunması gerekmektedir. Ancak adli sicil kayıtları bakımından ise mutlak olarak resmi makamca işleme şartı aranmaktaydı¹⁹⁴. Kolluk ve Ceza Adaleti Direktifi'ne göre ise veri işleyen kamu ya da özel hukuk kişisi olabilecektir.

2. Veri Koruma İlkelerine Riayet

a. Hukuka ve Dürüstlük Kurallarına Uygunluk

Tüm AB temel veri koruma düzenlemelerine göre kişisel veriler, hukuka (*lawfully*) ve dürüstlük kuralına uygun (*fairly*) işlenecektir. Hukuka uygunluktan, veri işlemenin normun koruma amacını ortaya koyacak şekilde¹⁹⁵ mevzuatta açık olarak düzenlenmiş olması anlaşılmalıdır. Bu ilkeye göre kişisel verinin işlenmesine izin veren bir kanun hükmü bulunmaması halinde veri işleme yasaktır¹⁹⁶. Nitekim Türk hukukunda da KVKK'nin yürürlüğünden önce kişisel verilerin işlenmesine ilişkin düzenlemelerin kanuna dayanmaması gerekçesiyle pek çok düzenleme AYM tarafından iptal edilmiştir¹⁹⁷.

¹⁹² Catherine Jasserand, "Subsequent Use of GDPR Data For A Law Enforcement Purpose: The Forgotten Principle of Purpose Limitation", **University of Groningen Faculty of Law Research Paper Series**, No.26/2018, EDPL c. 4, s. 2, 2018, s. 3.

¹⁹³ 95/46 sayılı Direktif m. 8/5.

¹⁹⁴ Kaya, "Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi", s. 331.

¹⁹⁵ Dülger, Özkan, **a.g.e.**, s. 100.

¹⁹⁶ Nafiye Yücedağ, "Kişisel Verilerin Korunması Kanunu Kapsamında Genel İlkeler", **Kişisel Verileri Koruma Dergisi**, c. 1, s. 1, 2019, s. 48.

¹⁹⁷ Elektronik haberleşme sektöründe kişisel verilerin işlenmesinde "Kurum, elektronik haberleşme sektörüyle ilgili kişisel verilerin işlenmesi ve gizliliğinin korunmasına yönelik usul ve esasları belirlemeye yetkilidir." şeklinde BTK'ya yetki veren Elektronik Haberleşme Kanunu m. 51'in iptaline ilişkin E. 2013/122, K. 2014/74, 09.04.2014 AYM iptal kararı; 5651 sayılı Kanun m. 3/4'ün "Trafik bilgisi Telekomünikasyon İletişim Başkanlığı tarafından ilgili işletmecilerden temin edilir ve hâkim tarafından karar verilmesi hâlinde ilgili mercilere verilir." hükmünün kişisel verilerin ilgilinin açık rızası veya kanuna dayalı olarak işlenmesine uygun olmadığı gerekçesiyle E. 2014/149, K. 2014/151,

Dürüstlük kuralına uygun biçimde işleme ise veri sorumlularının işleme amacına ulaşırken veri sahibinin menfaat ve makul beklentilerine uygun davranmasını gerektirmektedir¹⁹⁸. Bazı yazarlarca dürüstlük kuralına uygunluğun AB üyesi devletlerin sosyal, kültürel ve ekonomik geçmişleri nedeniyle farklılık gösterebileceği ve bu nedenle müphem olduğu da ifade edilmiştir¹⁹⁹.

GDPR'a göre veri işlemenin temel ilke ve gerekleri; rıza, sözleşmenin yapılması, kanuni yükümlülükle uyumluluk, üstün menfaat, kamu menfaati ve veri sorumlusunun meşru menfaatidir. Kolluk ve Ceza Adaleti Direktifi'nde ise bu ilkelere atıf yapılmamış, kanunilik ilkesini sağlamak için AB üyesi devletlerin iç hukuklarında belirtildiği şekilde veri işleneceği öngörülmüştür²⁰⁰. Ayrıca GDPR hukuka ve dürüstlük kuralına ek olarak şeffaflık (*transparency*) ilkesini aramışsa da Kolluk ve Ceza Adaleti Direktifi'nde bu ilkeye yer verilmemiştir²⁰¹.

Şeffaflık ilkesi ile sağlanmak istenen, veri sahibinin kişisel verisinin kimler tarafından hangi amaç ve şartlarla işlendiğini öğrenmek²⁰² ve veri sorumlusunun meşruiyetini ortaya koymaktır²⁰³. Bu sayede veri sahibi işlemenin varlığından haberdar olarak tam ve doğru şekilde bilgilendirilecektir²⁰⁴. Bu ilkenin bir uzantısı olarak²⁰⁵ Kolluk ve Ceza Adaleti Direktifi'nde mutlak olmasa da veri sahibine

02.10.2014 Çevrimiçi <https://www.anayasa.gov.tr/tr/kararlar-bilgi-bankasi/> 29.03.2020. AYM iptal kararının detaylı analizi için bkz. Göçmen Uyarer, **a.g.e.**, s. 106.

¹⁹⁸ Aşıkoğlu, **a.g.e.**, s. 75; *Yücedağ*'a göre ise dürüstlük kuralına uygun işlemeyen anlaşılması gereken, veri sahibinin çıkar ve makul beklentilerinin dikkate alınması, veri sahibinin hatasından yararlanılmaması, veri sahibinin güveninin kötüye kullanılmamasıdır. Söz gelimi işlemenin dayanağı olarak rıza gösterilmişken esasında rıza değilse ve bu veri sahibine bildirilmemişse veri sahibi rızaya dayalı olarak veri işlendiğinden rızasını geri aldığı anda işlemenin sona ereceği zannıyla hareket edeceğinden bu, dürüst işleme ilkesinin amacına hizmet etmeyecektir. Bkz. *Yücedağ*, **a.g.e.** s. 50

¹⁹⁹ *Yücedağ*, **a.g.e.**, s. 49.

²⁰⁰ De Hert, Papakonstantinou, **a.g.e.**, s. 11.

²⁰¹ *Leiser*'a göre ise bu ilkeye yer verilmiş, ancak devam eden soruşturmanın selameti için sıkı bir şeffaflık aranmamıştır. Bkz. Mark Leiser, "Directive 2016/680 Personal Data in Law Enforcement", Introduction of The Data Protection Reform to The Judicial System Inform, Çevrimiçi <https://www.universiteitleiden.nl/binaries/content/assets/rechtsgeleerdheid/instituut-voor-metajuridica/inform-project/leiser-inform-workshop.pdf> 13.03.2020, s. 8; KVKK'de de kişisel veri işleme ilkeleri arasında şeffaflığa yer verilmemiştir. Ancak *Eraslan Türkmen*, bu ilkenin dürüstlük kuralına uygun veri işleme ilkesi içinde değerlendirilmesi gerektiği kanaatindedir. Bkz. *Eraslan Türkmen*, **a.g.e.**, s. 93.

²⁰² Develioğlu, **a.g.e.**, s. 44.

²⁰³ İkbâl Gür, **Kişisel Verilerin Korunması Hususunda AB ile ABD Arasında Çıkan Uyuşmazlıklar ve Çözüm Yolları**, Ankara, Turhan Kitabevi, 2010, s. 65.

²⁰⁴ *Yücedağ*, **a.g.e.**, s. 49.

²⁰⁵ Dülger, Özkan, **a.g.e.**, s. 100.

bilgilendirilme hakkı ve erişim hakkı tanınmıştır. Şeffaflık ilkesinin tanınmamış olması Kolluk ve Ceza Adaleti Direktifi'nin amaçları da gözetildiğinde isabetlidir, özellikle bir ceza soruşturmasında gizliliğin önemi yadsınamaz ve şeffaflığın sağlanması için soruşturulan şüphelinin kişisel verilerinin işlendiğine dair bilgilendirilmesi, maddi gerçeğe ulaşma amacını zedeleyebilecektir. Nitekim resitalde de bilgilendirilme hakkının, kolluk veya adli yargı makamlarının gizli soruşturma yürütmesi ve kamera kaydı gibi gözetim faaliyetlerini yürütmesine engel olmayacağı belirtilmiştir²⁰⁶.

b. Amaçla Bağlılık

Amaçla bağlılık ilkesi; şeffaflık, hukuki belirlilik ve öngörülebilirliğin veri koruma hukukundaki tezahürü olup²⁰⁷ kişisel verilerin işleme amacının belirli ve açık olmasını ve bu amacın meşru olmasını yani kanuni dayanağının bulunmasını ifade eder. Verinin belirli bir amaçla işlenmesi kişisel verinin ve dolayısıyla veri sahibinin profillenmesinin de önüne geçmektedir²⁰⁸.

Bu ilkenin amacın belirliliği ve uygun kullanım olmak üzere iki boyutu vardır²⁰⁹: Amacın belirliliği, verinin toplandığı ilk anda belirli bir amaca ilişkin işlemenin yapılması iken uygun kullanım, verinin sonraki kullanımı söz konusu olduğunda, başlangıçtaki toplanma amacı ile sonraki kullanım amacının bağdaşır olmasıdır²¹⁰. GDPR'da başlangıçtaki toplama amacı haricinde bir amaçla, eldeki kişisel verinin kullanımı için kural olarak veri sahibinin rızası yeterli görülmüşse de²¹¹ Kolluk ve Ceza Adaleti Direktifi'nde rızaya sonuç bağlanmamıştır. Sonraki kullanıma

²⁰⁶ Kolluk ve Ceza Adaleti Direktifi resital m. 26.

²⁰⁷ Dülger, Özkan, **a.g.e.**, s. 101; Jasserand, **a.g.e.**, s. 5.

²⁰⁸ Çekin, **a.g.e.**, s. 10.

²⁰⁹ Bkz. OECD Gizlilik Rehber İlkeleri para. 9 amacın belirli olması, para. 10 kullanımın sınırlı olması; Jasserand, **a.g.e.**, s. 7.

²¹⁰ Jasserand, **a.g.e.**, s. 7.

²¹¹ Rızanın bulunmaması halinde GDPR m. 6/4'te demokratik bir toplumda gerekli ve ölçülü olması kaydıyla m. 23/1'deki amaçların gözetilerek veri sorumlusunun başlangıçtaki amaçla bağdaşır biçimde verinin sonraki kullanımına izin verilmesinin şartları sayılmıştır. Buna göre kişisel verinin toplanma amacı ve sonraki işleme amacı arasındaki bağlantı, veri sahibi ve sorumlusu arasındaki ilişki gözetilerek kişisel verinin toplandığı bağlam, verinin özellikle hassas veri olup olmadığı ya da ceza mahkûmiyeti ile ilgili olup olmadığına ilişkin doğası, sonraki işlemenin veri sahibi bakımından sonuçları ve kriptolama ya da maskeleye gibi uygun güvencelerin alınıp alınmadığı değerlendirilecektir.

izin veren bir düzenleme esasen amaçla bağlılık ilkesini sınırlayacağından, Avrupa Temel Haklar Şartı m. 52'deki sınırlama şartlarına da uygun olmalıdır²¹².

Kolluk ve Ceza Adaleti Direktifi'ne göre kişisel verinin işlenmesi, suç işlenmesinin önlenmesi, soruşturma, kovuşturma ve cezanın infazı amacına uygun olmalıdır. Amaç belirli, açık ve meşru olmalıdır. Kolluk ve Ceza Adaleti Direktifi'nde kişisel verilerin yeterli, ilgili ve amaca göre aşırı olmayan şekilde işlenmesi gerektiği belirtilmiştir²¹³. Direktif'in bu lafzından anlaşılan da amaç dışında kişisel veri işlemenin mümkün olduğudur²¹⁴. Ancak verilerin daha sonra başka bir amaç için kullanılması gerekiyorsa bunun meşru bir dayanağı bulunmalıdır. Söz gelimi soruşturma aşamasında yapılan bir DNA analizi sonucunun faili tespit etmek dışında bir amaçla kullanılması genetik verinin özel nitelikli veri mahiyeti de gözetildiğinde önemli zararlara yol açabilecektir²¹⁵. Sonraki kullanım kanuni düzenlemeye dayanmıyorsa bu analiz sonucu başka bir amaçla kullanılmamalıdır. Örneğin moleküler genetik inceleme yalnız maddi gerçeğe ulaşma amacına hizmet etmektedir ve bu amacın gerçekleşmesi halinde elde edilen veri, analizin ardından yok edilmelidir. Zira Türk hukukunda DNA bankaları mevcut değildir ve verinin kanuni dayanağı olmayan bir bankada muhafazası sakıncalıdır. Yine amaçla bağlılık ilkesi gereği; analiz sonucu deney veya deneme yapmak için veya fiilen DNA bankası oluşturmak için bu veri kullanılmamalıdır²¹⁶.

Bu ilkeye riayet edilmeksizin yapılan polis ve ceza adaleti faaliyeti kapsamında bir veri işlemenin AİHS m. 8 bağlamında ihlal edildiği iddiasını AİHM, *Liberty ve diğerleri v. Birleşik Krallık* başvurusunda değerlendirmiştir. Savunma Bakanlığının gizli gözetim amaçlarıyla insan hakları örgütlerinin telefon, e-posta ve faks yolu ile gerçekleşen iletişimlerini denetlediği olayda, bir televizyon programının bu durumu

²¹² Jasserand, **a.g.e.**, s. 5.

²¹³ Kolluk ve Ceza Adaleti Direktifi m. 4/1-c. Bu madde ile Kolluk ve Ceza Adaleti Direktifi'nin GDPR'a göre amaca uygun işlemede daha esnek olduğu belirtilmiştir. Baran Kızıllırmak, "Önleyici Amaçla Elde Edilen Verilerin Ceza Muhakemesinde Kullanılabilirliği", **İstanbul Üniversitesi Sosyal Bilimler Enstitüsü**, Yayınlanmamış Yüksek Lisans Tezi, İstanbul, 2018, s. 186.

²¹⁴ Kızıllırmak, "Kişisel Verilerin İşlenmesinde Adli ve Önleyici Amaçla Öngörülen İstisnaların Ulusal ve Uluslararası Hukuka Göre Değerlendirilmesi", s. 232.

²¹⁵ Küzeci, **a.g.e.**, s. 243.

²¹⁶ Öztürk, Eker Kazancı, Soyer Güleç, **a.g.e.**, s. 248.

haber yapması ile insan hakları örgütleri durumdan haberdar olmuştur²¹⁷. Birleşik Krallık'ta iletişimin denetlenmesi, o dönem 1985 tarihli İletişimin Ele Geçirilmesi Kanunu'na dayanarak gerçekleştirilmekteydi. AİHM, iletişimin muhatapların rızası olmaksızın gizlice dinlenmesine olanak tanıyan mevzuatın varlığının; yalnız iletişimi dinlenenler için değil, herkes için gözetleme tehdidi oluşturduğunu belirtmiştir²¹⁸. Zira mevzuatın adli makamlara tanıdığı bu yetki çok geniş kapsamlı olup kişisel veri mahiyetinde olan bu iletişimi denetleme amacı da Kanunda özel olarak belirtilmediğinden AİHM m. 8'in ihlal edildiğine hükmetmiştir²¹⁹.

(1) Verinin Sonraki Kullanımı ve Amaçla Bağlılık

Kişisel verinin toplanma amacı dışında sonraki kullanımı (*subsequent use of personal data*), verinin hâlihazırda mevcut olması ve teknolojik imkânların gelişmesi nedeniyle günümüzde mümkündür²²⁰. Ancak bu sonradan kullanım, verinin geleceğini belirleme hakkı ile ilgilidir ve amaçla bağlılık ilkesi ile arasında denge gözetilmelidir. Bu ilkeye göre belirli bir amaç için toplanan kişisel verinin sonraki kullanımı, uyumlu amaçlar için olmalı ya da farklı bir kanuni dayanağa sahip olmalıdır²²¹. Ancak uyumlu amaç/ uygun kullanımın ne olduğu Kolluk ve Ceza Adaleti Direktifi'nde açıklanmamış, devletlerin iç hukuk düzenlemelerine bırakılmıştır.

GDPR'da da mevcut olan bu ilkeye yüklenen fonksiyon, Kolluk ve Ceza Adaleti Direktifi'nden daha farklıdır. Zira GDPR, sonradan ortaya çıkan ve verilerin işlenme amacına uygun olmayan yeni verilerin işlenmesini sınırlamakta ve kişisel verilerin işlenmesi şartlarının bu yeni veriler bakımından da ayrıca sağlanmasını

²¹⁷ *Liberty ve diğerleri v. Birleşik Krallık*, B. No: 58243/00, 01.10.2008, para. 5 Çevrimiçi <http://hudoc.echr.coe.int/eng?i=001-87207> 13.02.2020.

²¹⁸ *Liberty ve diğerleri v. Birleşik Krallık*, para. 56.

²¹⁹ *Liberty ve diğerleri v. Birleşik Krallık*, para. 69.

²²⁰ Jasserand, **a.g.e.**, s. 2.

²²¹ Jasserand, **a.g.e.**, s. 2; WP29'a göre, uygunluk değerlendirmesi iki farklı yaklaşımla yapılabilir. Katı bir amaca bağlılık gerektiren şekli yaklaşıma göre veri sorumlusu sonraki amaçların, en başta belirtilen amacın bünyesinde olup olmadığını açık ya da örtülü olarak değerlendirmelidir. Esasa ilişkin yaklaşıma göre ise baştaki ve sonraki veri işleme amaçları lafza göre değil, somut olayın koşullarına göre değerlendirme gerektirir. Şekli yaklaşım veri sahibine, yalnız başta belirtilen amaçla veri işlendiğinden daha ciddi bir koruma sağlamaktadır. Ancak WP29 esasa ilişkin yaklaşımı benimsemektedir. Akt. Yücedağ, **a.g.e.**, s. 54 ve s. 57.

aramaktadır²²². Yani bu ilke, yeni veriler için de verilerin korunması amacına hizmet etmektedir. Kişisel verilerin toplanma amacı dışındaki bir amaca yönelik olarak yapılan işleme; veri sahibinin rızası veya üye devlet iç hukuku veya AB hukukuna uygun olarak m. 23'te sayılan meşru menfaatleri korumak amacıyla demokratik bir toplumda gerekli ve ölçülü bir müdahale teşkil etmesi halinde mümkündür²²³. Ancak Kolluk ve Ceza Adaleti Direktifi'nde ise verilerin işlenme amacının yalnız aşırı olmaması (*not excessive*) kriteri benimsenmiştir²²⁴. Bu farklılık, Kolluk ve Ceza Adaleti Direktifi'nin ihdas amacı ve daha geniş biçimde kamu güvenliğinin sağlanması amaçlarıyla açıklanabilir. Söz gelimi başlangıçta verinin toplanma amacı kolluk faaliyeti ile ilgili olmayıp ticari, idari ya da organizasyonel bir amaçtır; ancak sonraki kullanım Kolluk ve Ceza Adaleti Direktifi'nin kapsamına giriyorsa bu durumda kişisel veri, Kolluk ve Ceza Adaleti Direktifi'nin korumasından yararlanacaktır²²⁵.

Kolluk ve Ceza Adaleti Direktifi kapsamında toplanan bir kişisel verinin aynı ya da başka bir veri sorumlusu tarafından başlangıçtaki toplanma amacından farklı bir amaçla işlenmesi mümkündür. Bu durumda sonraki veri işleme faaliyeti, GDPR'a tabi olacaktır²²⁶. Yani sonraki veri işlemenin, AB hukuku ya da iç hukukta veri sorumlusunun sonraki amaçla kişisel veri işlemek üzere yetkilendirilmiş olması veya AB hukuku ya da iç hukuk uyarınca veri işlemenin sonraki amaç için gerekli ve orantılı olması gerekmektedir. Ancak resitalde, başlangıçtaki veri işlemenin Kolluk ve Ceza Adaleti Direktifi kapsamında olup olmadığı belirtilmediğinden bu durum eleştirilmiştir²²⁷.

Verinin sonraki kullanımı, mağdurlar, küçükler veya uluslararası korumaya sahip olanlar gibi savunmasız bireylerle ilgili kişisel verilere ilişkinse, sonraki kullanım gereklilik ve orantılılık ilkelerinin uygulanmasına özel dikkat gösterilerek ek

²²² Dülger, Özkan, **a.g.e.**, s.102; Nitekim WP29 da sonraki işleme için muhakkak ayrı bir hukuka uygunluk sebebini aramaktadır. Bkz. Yücedağ, **a.g.e.**, s. 56.

²²³ GDPR m. 6/4.

²²⁴ Dülger, Özkan, **a.g.e.**, s. 102.

²²⁵ Jasserand, **a.g.e.**, s. 7.

²²⁶ Kolluk ve Ceza Adaleti Direktifi resital m. 12.

²²⁷ Eleştiri için bkz. Jasserand, **a.g.e.**, s. 8.

bakım ve kanuni analizlere tabi tutulmalıdır²²⁸. Veri işleme, insan kaçakçılığı, uyuşturucu madde ticareti, cinsel istismar gibi fail-mağdur arasında gri alanların olabildiği suçlara ilişkin ise sonraki kullanım ve amaçla bağlantı değerlendirilmesi daha incelikli yapılmalıdır. Muhakeme sürecinin başında mağdur olarak değerlendirilen kişilerin bu suçların şüphelisi olması halinde veya mağdurların daha ağır bir suç için korunması menfaati ile daha az ağır suçun kovuşturulması ile sağlanacak menfaat yarıştığında kişisel verilerin sonraki kullanımı gündeme gelebilmektedir. Söz gelimi veri sahibinin vergilendirilmesi amacıyla işlenen kişisel veriler, kanunda açıkça öngörülümüşse sonraki amaç olan kolluk ve adli makamların faaliyetlerinde de kullanılabilir. Suçtan kaynaklanan malvarlığı değerlerini aklama suçuna ilişkin yürütülen soruşturmada, veri sahibinin vergi beyannamelerinin veri sahibi ve aklama fiili arasında bir bağlantı kurmak veya reddetmek için kullanılabileceği öngörülebilir²²⁹.

Türk hukukunda önleme amaçlı iletişimin denetlenmesi tedbirine başvurulduğunda elde edilen kişisel veriler, yalnızca PYSK ve 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanunu'nda (Jandarma Kanunu) belirtilen suçların işlenmesinin önlenmesi amacıyla bağlantı olarak kullanılabilecektir. Bu verilerin hukuk, ceza yargılamasında ve disiplin soruşturmalarında delil olarak kullanılamaması²³⁰ veri işlemenin amaçla bağlantı gereğidir²³¹.

(2) Büyük Veri ve Amaçla Bağlılık

Daha önce belirttiğimiz gibi büyük veriye finansal, akademik, sağlık, ulaşım gibi nedenlerle başvurulmaktadır²³². Söz gelimi akademik bir analiz için oluşturulan büyük veri setinden, büyük veriyi oluşturan verilerin münferiden kolluk ve adli makamların faaliyetlerinde kullanılıp kullanılamayacağı değerlendirilmelidir. Büyük

²²⁸ Allen, van Beek, Borking, **a.g.e.**, s. 4.

²²⁹ Allen, von Beed, Borking, **a.g.e.**, s. 4-5.

²³⁰ Bkz. PYSK ek m. 7/8; 2803 sayılı Jandarma Kanunu ek m. 5/6; 2937 sayılı MİT Kanunu m. 6/6; Yargıtay CGK 17.05.2011, 2011/9-83 2011/95 sayılı kararı.

²³¹ Feridun Yenisey, Ayşe Nuhoğlu, **Ceza Muhakemesi Hukuku**, 7. Baskı, İstanbul, Seçkin Yayıncılık, 2019, s. 284; Necati Meran, **Ceza ve Hukuk Davalarında Yasak Delil İletişimin Denetlenmesi Gizli Soruşturmacı ve Teknik Takibin Hukuki Boyutu**, 3. Baskı, Ankara, Adalet Yayınevi, 2015, s. 13.

²³² Bkz. "Anonimlik ve Büyük Veri İlişkisi" başlıklı bölüm.

veri ve analiz teknolojileri suçların tespitinde yardımcı olabilir, ancak bu türden veri işleme birtakım riskleri de barındırmaktadır.

Bir alan adından gelen veri tabanları; bağlamı değiştiren, yanlış sonuçlara götüren ve geçerli hukuki dayanaktan yoksun biçimde başka bir amaç için kullanılabilir. Bu da veri sahipleri için ciddi sonuçları olan verilerin hukuka aykırı işlenmesine yol açabilir. Profillemeye, kalıp yargıların güçlendirilmesi, damgalanma ve ayrımcılığa yol açabilecek sonuçlara neden olabilir. Veri tabanlarında tutulan kişisel veri miktarının artması, veri güvenliği garanti edilmediğinde ciddi güvenlik açıklarına ve daha sonra veri koruma ihlallerine neden olabilir²³³. Bu kaygılar ışığında, büyük veri uygulamaları Kolluk ve Ceza Adaleti Direktifi'nin veri işleme amaçlarına yönelik ise ve uygulama, idari ve teknik olarak güvenli ise kişisel veri büyük veri uygulamalarında ilk işleme amacından farklı şekilde kullanılabilirdir.

c. Veri Minimizasyonu

Veri minimizasyonundan²³⁴ esas olarak ölçülülük anlaşılmaktadır. Veri minimizasyonu ilkesine göre kişisel veriler, işlendikleri amaçla ilişkili olarak yeterli işlenmelidir²³⁵. Veri işleme faaliyeti gerçekleştirilirken veri sorumlusunda *nice-to-have* anlayışı yerine *need-to-have* anlayışı hâkim olmalıdır²³⁶.

Söz gelimi spor salonunda güvenliğin sağlanması için parmak izi okutulması biyometrik veri işlemedir. Spor salonunun güvenliği kart okutma gibi alternatiflerle sağlanabilecekken biyometrik veri işlenmesi, veri sahibinin haklarına yoğun müdahale teşkil etmektedir²³⁷. Oysa kişisel verinin işlendiği amacın, başka araçlarla yerine getirilmesi mümkün değilse veri işlenmelidir.

²³³ Allen, van Beek, Borking, s. 10.

²³⁴ Veri minimizasyonu yerine “minimumluk ilkesi (principle of minimality)” terimi için bkz. Kaya, “Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi”, s.324. Yazara göre de minimumluktan anlaşılması gereken, toplanan kişisel verilerin toplanma ve işleme amaçları gözetilerek ancak zorunlu miktarda olması gerektiğidir. Nitekim 95/46 sayılı Direktif’te de bu ilke aşırı olmama (not excessive) olarak bulunmaktaydı.

²³⁵ Yücedağ, **a.g.e.**, s. 59.

²³⁶ Crutzen, Ygram Peters, Mondschein, **a.g.e.**, s. 1353.

²³⁷ Yücedağ, **a.g.e.**, s. 59.

Veri minimizasyonu ilkesi dar manada, kişisel verinin saklanması keskin ve belirli bir süre ile sınırlandırılmasını öngörmektedir²³⁸. Geniş manada veri minimizasyonu ise verinin işleme amacı ile ilgilidir. GDPR m. 5/1-c'ye göre veri, işleme amacı ile ilişkili olarak gerekli olanla sınırlı işlenmelidir²³⁹. Ancak Kolluk ve Ceza Adaleti Direktifi veri işlemede “aşırı olmama” ilkesini esas almıştır²⁴⁰. Veri minimizasyonu ilkesine hizmet etmek için teknik imkânlardan da yararlanılarak işlenecek veriler azaltılacağı gibi işlemenin tasarımı aşamasında asgari düzeyde veri işleyecek yöntemler geliştirilmelidir²⁴¹.

d. Güncel Olma İlkesi

Güncel olmayan veya doğru olmayan bir veri, veri sahibinin toplumsal imajını etkilemekte ve bu imaja dayanılarak veri sahibi hakkında karar alınması ve işlem yapılmasına yol açabilmektedir. Bu da veri sahibinin maddi ve manevi varlığını geliştirmesine ket vurmaktadır²⁴². Verilerin şekli bakımından eksik, hatalı işlenmesi veya verinin içeriğinin bizzatı hatalı, eksik olması durumunda bu verilerin güncellenmesi gerekmektedir²⁴³. Zira kişisel verinin işleme süreci boyunca veri, doğru olmalıdır.

Veri sahibi, işleme sırasında kişisel verilerinde meydana gelen değişikliklerin güncellenmesini talep hakkına sahiptir ve veri sorumlusu da verilerin doğruluğunu periyodik olarak gözden geçirmekle yükümlüdür²⁴⁴. Verinin doğruluğu, olgular bakımından ve veri sahibinin profillenerek hakkında bir sonuca varılmasını sağlayan değer yargıları bakımından değerlendirilmelidir²⁴⁵. Güncelliğin sağlanması, kişisel verinin elde edildiği ilk aşamadan itibaren yürütülen ceza soruşturması ve

²³⁸ Soysal, **a.g.e.**, s. 361.

²³⁹ Yücedağ, **a.g.e.**, s. 59.

²⁴⁰ Kolluk ve Ceza Adaleti Direktifi m. 4/1-c.

²⁴¹ Yücedağ, **a.g.e.**, s. 60.

²⁴² Yücedağ, **a.g.e.**, s. 50.

²⁴³ Dülger, Özkan, **a.g.e.**, s. 103.

²⁴⁴ Ayözger, **a.g.e.**, s. 135; Verinin güncel olmasının bütün veri sorumluları bakımından periyodik güncelleme yapmayı gerektirmediği Yücedağ tarafından ileri sürülmüştür. Zira yazar, ancak verinin güncel olmasının veri sahibi üzerinde ağır etki yaratması halinde veri sorumlusunun doğruluk ve güncelliği periyodik olarak kontrol etmesini gerektirdiğini savunmaktadır. Bkz. Yücedağ, **a.g.e.**, s. 51.

²⁴⁵ Yücedağ, **a.g.e.**, s. 51.

kovuşturması boyunca hangi verilerin tutulacağı ve hangilerinin silineceğini değerlendirmek için kapsamlı bir analiz gerekmektedir²⁴⁶.

e. Sürelilik İlkesi

Bir veri tabanına giren ve belirli bir süre ile sınırlı olmaksızın orada tutulan bir kişisel veri sistemde güncelliğini yitirerek veri sahibinin mağduriyetine yol açabilir, bu nedenle kişisel veri belirli bir süre ile sınırlı olarak tutulmalıdır²⁴⁷. Kolluk ve Ceza Adaleti Direktifi'nde teklif metninin aksine saklama ve incelemeye ilişkin süre sınırlarına yer verilmemiş olsa da kişisel verilerin saklanması ve silinmesine ilişkin süre sınırlamalarına taraf devletlerin yer vermesi ve periyodik olarak bu gerekliliğe ilişkin gözden geçirme yükümlülüğünün bulunması gerektiği belirtilmiştir²⁴⁸. Zira kişisel veriler işlendiği amaç ile gereken süreden fazla tutulmamalıdır.

Bu ilkenin bir uzantısı olarak²⁴⁹ süre amaçla bağlı olmalıdır, yani amacın ortadan kalkması ile verinin tutulmasına son verilmelidir. Bu meyanda suç işlenmesinin önlenmesi gerekçesiyle devletin silme ve gözden geçirme yükümlülüğünü yerine getirmesinin beklenip beklenmeyeceğinin değerlendirmesi yapılmalıdır²⁵⁰. Bu hususta WP29 belirli şartlar altında önleyici amaçlarla belirli bir veri imha süresi olmaksızın verinin saklanması mümkün olduğunu belirtmiştir. Ancak bunun için gereklilik ilkesi ihlal edilmemeli ve belirli bir veri sahibine yönelik risk değerlendirme raporlaması yapılmış olmalıdır. Ayrıca WP29'a göre iç hukukta yapılacak düzenlemelerde özel nitelikli ve genel kişisel veri türleri arasındaki mahiyet farkı gözetilerek saklama süresi belirlenmelidir²⁵¹.

Türk hukukunda sürelilik ilkesi ile bağdaşmayan bir düzenlemeye değinilmelidir. PVSK m. 5'te bazı hallerde kişilerin parmak izinin alınabilmesi mümkündür. Alınan parmak izi; veri sahibinin kimlik bilgileri, verinin işlendiği zaman

²⁴⁶ Allen, van Beek, Borking, **a.g.e.**, s. 4.

²⁴⁷ Wayne Madsen, **Handbook of Personal Data Protection**, UK, Macmillan Publishers, 1992, s. 12.

²⁴⁸ Bkz. Kolluk ve Ceza Adaleti Direktifi m. 5; Bilişim ve Teknoloji Hukuku Enstitüsü, **a.g.e.**, s. 9.

²⁴⁹ Bizatihi bu ilkenin de veri minimizasyonunun görünümü olduğuna ilişkin bkz. Yücedağ, **a.g.e.**, s. 60.

²⁵⁰ Dülger, Özkan, **a.g.e.**, s. 103.

²⁵¹ Dülger, Özkan, **a.g.e.**, s. 103.

ve veriyi işleyen kişinin kimliği belirtilmek suretiyle, bu amaca özgü sisteme kaydedilir. Kayıtlı olan parmak izi, kişinin ölümünden itibaren on yıl ve kayıt tarihinden itibaren seksen yıl geçtikten sonra sistemden silinebilir.

PVSK uyarınca gözaltına alınan bir kişinin parmak izinin alınması mümkündür. Kişi hakkında söz gelimi kovuşturmayaya yer olmadığı kararı verilir veya beraat hükmü verilirse CMK m. 81/2²⁵² uyarınca kişisel verisinin yok edilmesi gerekir²⁵³. Ancak PVSK m. 5/10 uyarınca parmak izi alınan bu kişi hakkında yürütülen ceza soruşturması veya kovuşturması sonucundan bağımsız olarak parmak izi AFIS²⁵⁴ denilen sistemde seksen yıl boyunca saklanacaktır. Kolluk birimleri kimlik tespiti veya parmak izi karşılaştırması yapmak için doğrudan bu sistemi kullanabilmektedir²⁵⁵. PVSK'nin bu hükmünün adli kolluk faaliyeti değil, önleyici kolluk faaliyeti olduğu düşünülebilir ve bu nedenle aslında biyometrik veri kaynağı olan parmak izi, önleyici kolluk faaliyeti kapsamında tutulmaya devam etmektedir. Ancak hakkında salt gözaltı kararı verildiği için parmak izi alınan bir kişiden alınan parmak izi ile suç işlemenin önlenmesi faaliyetinin yürütülmesi isabetsizdir, zira kişi hakkında CMK m. 81/2 uyarınca mahkûmiyet hükmü haricinde bir hüküm veya karar verilmiştir.

Ayrıca alınan parmak izinin seksen yıl boyunca tutulmasına izin veren PVSK hükmü, Kolluk ve Ceza Adaleti Direktifi'nde belirtilen sürelilik ilkesi ile bağdaşmamaktadır. Zira Kolluk ve Ceza Adaleti Direktifi verinin muhafazasına ilişkin açık bir süre belirlememişse de insan yaşamının ortalama süresi göz önüne alındığında seksen yıllık tutulma süresinin pratikte sürelilik ilkesine hizmet etmediği açıktır. Zira kişi hakkında mahkûmiyet kararı verilmişse dahi kişinin işlemiş olduğu suç, suçun işleniş biçimi, tekrar suç işleme tehlikesi gözden geçirilmeksizin parmak izinin seksen

²⁵² “Kovuşturmayaya yer olmadığı kararına itiraz süresinin dolması, itirazın reddi, beraat veya ceza verilmesine yer olmadığı kararı verilip kesinleşmesi hâllerinde söz konusu kayıtlar Cumhuriyet savcısının huzurunda derhâl yok edilir ve bu husus tutanağa geçirilir.”

²⁵³ Bu yok etme “Ceza Muhakemesinde Beden Muayenesi, Genetik İncelemeler ve Fizik Kimliğin Tespiti Hakkında Yönetmelik” uyarınca yapılmaktadır.

²⁵⁴ Emniyet Genel Müdürlüğüne ait merkezi sistemli bir veri tabanıdır. Dijital olan bu veri tabanında hâlihazırda mevcut parmak izleri ve soruşturma esnasında elde edilen parmak izleri karşılaştırılarak delilden şüpheli/sanığa ulaşılmaktadır. bkz. Çam, **a.g.e.**, s.91-93.

²⁵⁵ Mehmet Alkan, “Avrupa Konseyi Bakanlar Komitesinin İnsan Hakları ve Terörle Mücadele Hakkındaki İlkeleri ve Türkiye’nin Terörle Mücadele Mevzuatı”, **TBB Dergisi**, c. 29, s. 125, 2016, s. 24.

yıl boyunca saklanması kişisel verilerin korunması hakkının gerekleri ile bağdaşmamaktadır²⁵⁶.

Eleştirimizi teyit edercesine AİHM'nin incelediği *S. ve Marper v. Birleşik Krallık*²⁵⁷ başvurusuna değinilmelidir. Bay S'nin on bir yaşında iken işlemeye teşebbüs ettiği hırsızlık suçu nedeniyle yürütülen soruşturmada DNA ve parmak izi örneği alınmış ve Bay S beraat etmiştir. Bay Marper hakkında yürütülen soruşturma ise partnerine taciz nedeniyle olup DNA ve parmak izi örneği alınmıştır. Bay Marper ve partnerinin uzlaşması üzerine soruşturma sona ermiş, yargılama yapılmamıştır²⁵⁸. Ancak her iki başvuruçunun da parmak izi ve DNA örneği yok edilmemiştir. Zira Birleşik Krallık mevzuatı (PACE 64/1A) kişi beraat etse yahut herhangi bir nedenle yargılama devam etmese de DNA ve hücre örneklerinin süresiz ve sistematik olarak tutulmasına izin vermektedir²⁵⁹.

Başvurucular haklarında biyolojik bilgi taşıyan bu verilerin tutulmasının; özellikle on bir yaşında iken verisi işlenen başvuruçunun bakımından sosyal olarak damgalanmalarına ve psikolojik etkilere yol açacağını ileri sürmüştür²⁶⁰. AİHM kişinin hakkında genetik, biyolojik ve sağlık bilgisi taşıyan DNA verisinin özel nitelikli kişisel veri olduğunu ve bu verinin tutulmasının başlı başına m. 8'e bir müdahale oluşturduğunu belirtmiştir²⁶¹. Parmak izi ise DNA verisi kadar kişinin etnik kökeninden sağlığına kadar bilgi içermese de kişinin belirlenmesine olanak sağladığı için ve objektif ve çürütülemez bilgi içerdiği için bu izin tutulması da m. 8 kapsamında değerlendirilmelidir²⁶².

AİHM verilerin süresiz olarak tutulmasında yarışan kamu menfaati ve başvuruçuların menfaatini tartmıştır. Birleşik Krallık mevzuatında işlenen suçun niteliği ve ağırlığı, şüphelinin yaşı, iddia edilen fiilin sicile işlenen bir suç olup

²⁵⁶ Bayram, **a.g.e.**, s. 37.

²⁵⁷ Kararın detaylı eleştirisi için bkz. R. Barış Erman, "Adli Yargı Sisteminde DNA Örnekleri ve Profilleri– S. ve Marper v. Birleşik Krallık Davası", **Fasikül Hukuk Dergisi**, c. 2, s. 11, 2010, s. 20 vd.

²⁵⁸ *S ve Marper v. Birleşik Krallık* [BD], B. No: 30562/04 ve 30566/04, 04.12.2008, para. 11-12 Çevrimiçi <https://rm.coe.int/168067d21627.03.2020>.

²⁵⁹ *S ve Marper v. Birleşik Krallık*, para. 47.

²⁶⁰ *S ve Marper v. Birleşik Krallık*, para. 60.

²⁶¹ *S ve Marper v. Birleşik Krallık*, para. 73.

²⁶² *S ve Marper v. Birleşik Krallık*, para. 85.

olmadığı, fiilin hapis cezası gerektirip gerektirmediği dikkate alınmaksızın veriler tutulmaktadır. Beraat eden kişinin verisinin yok edilmesi için kişinin önceki tutukluluk süresi, isnat edilen suçun ciddiliği gibi belirli kriterler bulunmamaktadır²⁶³. Ayrıca beraat eden kişinin de verisinin tıpkı mahkûm olan kişinininki gibi tutulması masumiyet karinesine aykırı olup ayrıca kişinin damgalanmasına yol açmaktadır²⁶⁴. Bu nedenlerle AİHM, devletin verilerin tutulmasındaki takdir marjını orantısız kullandığı kanaatine varmış ve m. 8'in ihlal edildiğine hükmetmiştir²⁶⁵.

3. Özel Nitelikli Kişisel Veriler Bakımından Gerekli Güvencenin Bulunması

Kolluk ve Ceza Adaleti Direktifi'nin öngördüğü özel nitelikli kişisel veri kategorisi; GDPR ile paralel olup *ırk, etnik köken, siyasi düşünce, dini, felsefi inanç, sendika üyeliği, biyometrik ve genetik veriler, sağlık verileri, cinsel yaşam veya cinsel yönelime ilişkin verilerden oluşmaktadır*²⁶⁶. Bu verilerin özel nitelikli olarak adlandırılmasının sebebi, kötüye kullanım halinde veri sahibinin ayrımcılığa maruz kalması ve böylece üzerinde doğabilecek zarar ve mağduriyetin daha yüksek olmasıdır²⁶⁷. Özel nitelikli kişisel veriler ancak işlenmesinin mutlak gerekli olduğu haller ile sınırlı olarak işlenebilir.

Özel nitelikli kişisel veriler; AB hukuku yahut üye devlet hukukunun izin verdiği hallerde, veri sahibi yahut üçüncü kişinin hayati önemi haiz menfaatinin bulunduğu hallerde veya veri sahibinin açıkça alenileştirdiği verilerle ilgili işleme hallerinde işlenebilir²⁶⁸. Menfaat değerlendirmesi; verinin özel nitelikte olup olmadığı,

²⁶³ *S ve Marper v. Birleşik Krallık*, para. 119.

²⁶⁴ *S ve Marper v. Birleşik Krallık*, para. 122.

²⁶⁵ *S ve Marper v. Birleşik Krallık*, para. 125.

²⁶⁶ Kolluk ve Ceza Adaleti Direktifi m. 10/1.

²⁶⁷ Dülger, **Kişisel Verilerin Korunması Hukuku**, s. 108; Güray Dağ, "Kişisel Verilerin Ceza Muhakemesi Hukukunda Delil Olarak Kullanılması", **Marmara Üniversitesi Sosyal Bilimler Enstitüsü**, Yayımlanmamış Doktora Tezi, İstanbul, 2011, s. 119; Bu verilerin ifşasının tek sonucu ayrımcılık da değildir. Örneğin bazı hastaneler, ücretsiz tansiyon kontrolü yapmak için alışveriş merkezlerinde sponsor olmaktadır. Daha sonra tıbbi tarama sonuçlarıyla birlikte bireylerin kişisel verilerini derlemekte ve satmaktadırlar. Kontrol yaptıran hastalar da insülin ve hipodermik iğne üreticilerinden doğrudan mailler almaktadır, çünkü tıbbi durumları hastaneler tarafından doğrudan pazarlama firmalarına satılmıştır. Bkz. Madsen, **a.g.e.**, s. 14.

²⁶⁸ Kolluk ve Ceza Adaleti Direktifi m. 10/1.

işlemenin doğuracağı olası zarar, veri sahibinin durumu, çocuk olup olmaması dikkate alınarak yapılmalıdır²⁶⁹.

Özel nitelikli kişisel veriler temel hak ve özgürlüklerinin korunması için güvencelerin sağlanması şartıyla işlenebilir. Güvenceler; teknik bir yapı, ek güvenlik önlemleri, organizasyonel yapının sağlanması, veri elektronik ortamda tutuluyorsa özel kriptografik yöntemler kullanılması, kayıtların loglanması²⁷⁰, veri işleme sürecinde yer alan kişilerin eğitilmesi²⁷¹ biçiminde olabilir. Bu güvenceler, ana çerçevenin farklılaştırılması, farklı veri saklama süreleri gibi çoklu korumanın sağlanması biçiminde veri işleme faaliyeti bakımından her bir verinin özelliği dikkate alınarak yapılmalıdır. Ayrıca gizlilik artırıcı teknolojiler²⁷² (*Privacy-Enhancing Technologies- PETs*) ve veri işlemenin hukuka uygun olup olmadığına dair müteaddit kontroller yapılabilir²⁷³. Genellikle bu, başlangıçtan itibaren ve tasarımdan itibaren veri koruma teknolojileri ile sağlanmaktadır²⁷⁴. Bazı ülke mevzuatlarında da güvence olarak özel nitelikli kişisel veriler işlenmezden evvel ulusal veri koruma makamlarından izin alınması şartı mevcuttur²⁷⁵.

Türkiye’de yayınlandığı dönemde basında geniş yer bulan bir habere bu noktada değinilmelidir. Habere göre İstanbul Emniyet Müdürlüğü İl Sağlık Müdürlüğüne gönderdiği bir yazı ile polikistik over sendromuna sahip ve kürtaj yaptıran otuz ile kırk yaş aralığındaki kadınların listesini tüm kamu, özel ve üniversite hastanelerinden talep etmiştir²⁷⁶. Sağlık verilerini talep gerekçesi ise terör örgütüne

²⁶⁹ Develioğlu, **a.g.e.**, s. 67.

²⁷⁰ Eraslan Türkmen, **a.g.e.**, s. 143; Göçmen Uyarer, **a.g.e.**, s. 134; Her ne kadar Kolluk ve Ceza Adaleti Direktifi bağlamında işlenecek kişisel verilere KVKK hükümleri uygulanmasa da yol gösterici olarak Kişisel Verileri Koruma Kurumunun “*Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler ile ilgili Kişisel Verileri Koruma Kurulunun 31/01/2018 Tarihli ve 2018/10 Sayılı Kararı*” ile veri sorumlusunun özel nitelikli kişisel verilerin korunmasına ilişkin alması gereken önlemler altı madde halinde sayılmıştır. Karar için bkz. Çevrimiçi <https://www.kvkk.gov.tr/Icerik/4110/2018-10 16.02.2020>.

²⁷¹ Eraslan Türkmen, **a.g.e.**, s. 135 vd.

²⁷² “Mahremiyeti teşvik eden teknolojiler” biçimindeki çeviri için bkz. Çekin, **a.g.e.**, s. 12.

²⁷³ Allen, van Beek, Borking, **a.g.e.**, s. 5.

²⁷⁴ Çekin, **a.g.e.**, s. 12.

²⁷⁵ Örneğin Danimarka KVKK m. 50/1’e göre özel nitelikli kişisel verilerin işlenmesi konusunda ön izin vermeye yetkili makam şartı vardır ve bu makam, veri koruma makamıdır. Bkz. Kaya, “Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi”, s. 324.

²⁷⁶ “Emniyet Kürtaj Listesini İstedil!”, Birgün Gazetesi, 09.09.2019, Çevrimiçi <https://www.birgun.net/haber/emniyet-kurtaj-listesini-istedi-267844 16.03.2020>.

üye olma suçu nedeniyle yürütülen bir soruşturmadır. Özel nitelikli kişisel verilerin veri işleme ilkelerine aykırı bir nedenle toplanmak istenmesinin basında eleştirilmesi üzerine İstanbul Cumhuriyet Başsavcılığı açıklama yapmıştır. Açıklamaya göre “yürütülen bir soruşturmada şüpheli hakkında ihbarda bulunan ve açık kimlik ile adres bilgileri bilinmeyen bir şahsın tespiti amacıyla” böyle bir talepte bulunulmuştur²⁷⁷. Açıklamada ihbarda bulunan kişiye ulaşılamadığı, ancak her nasılsa elde edilmiş bilgiye göre kişinin 2017-2019 yılları arasında polikistik over tedavisi gördüğü bilgisi edinilmiştir ve muhbire ulaşabilmek için İstanbul’daki tüm hastanelerden bu şartı sağlayan kişilerin listesi istenmiştir.

Açıklamadan anlaşıldığı kadarıyla İstanbul’daki 30-40 yaş arasında bu hastalığa sahip tüm kadınların sağlık verilerinin toplanma gerekçesi, bir iftira suçunun şüphelisinin bulunmasıdır. Kanaatimizce savcılık, kişisel verilerin soruşturma evresinde KVKK kapsamı dışında bırakılmasından yararlanarak binlerce kişinin verisini toplama yani işleme gayreti içerisinde. Amaçla bağlılık çerçevesinde veri işlenebilmelidir. Burada verilerin toplanması ile amaca ulaşılabileceğini kabul etsek dahi yalnız bir şüpheli haricinde binlerce kişinin verisi hukuka ve dürüstlük kurallarına aykırı olarak işlenecektir ki bu, veri minimizasyonu ilkesi ile de bağdaşmamaktadır. Kanaatimizce bu durumda *Blackstone* formülasyonu ile aynı doğrultuda hareket ederek binlerce masumun kişisel verisi veri koruma ilkelerine aykırı olarak işleneceğine, bir suçlunun yakalanması ve maddi gerçeğe ulaşılması amacı gözden çıkarılmalıdır²⁷⁸.

²⁷⁷ “İstanbul Cumhuriyet Başsavcılığı’ndan ‘Emniyet Kürtaj Listesi İstedi’ Başlıklı Haberlere Dair Açıklama”, Sputnik News Türkiye, 10.09.2019, Çevrimiçi <https://tr.sputniknews.com/turkiye/201909101040137404-istanbul-cumhuriyet-bassavciligindan-emniyet-kurtaj-listesi-istedi-baslikli-haberlere-dair-aciklama/> 16.03.2020.

²⁷⁸ Benzer bir durum, bir dini organizasyon ve gerçek kişilerin başvuru olduğu *Avilkina ve diğerleri v. Rusya* başvurusunda da bulunmaktadır. St. Petersburg’da Yehova Şahitleri İdari Merkezi’nin faaliyetlerine karşı çeşitli makamlara başvurulmuşsa da yürütülen bir ceza kovuşturması bulunmamaktadır. Ancak St. Petersburg Şehir Savcısı, söz konusu organizasyonun faaliyetleri kapsamında soruşturmaya başlamış ve şehirdeki tüm sağlık kurum ve kuruluşlarından kan naklini reddeden Yehova Şahitlerinin listesini istemiştir. Ceza soruşturması, organizasyonun faaliyetlerinin illegal olup olmadığına ilişkindir. Savcı, kan naklini reddedenlerin Yehova Şahidi olduğundan hareketle şehirdeki kan naklini reddeden herkesin kişisel verilerini toplamıştır. Dolayısıyla hakkında soruşturma olmayan kişilerin de verileri işlenmiştir. AİHM bu işlemin demokratik bir toplumda gerekli ve ölçülü olmadığından bahisle m. 8’in ihlal edildiği sonucuna varmıştır. Detaylı bilgi için bkz. Neslihan Can, “Hasta Mahremiyeti Hakkı”, **TBB Dergisi**, c. 32, s. 147, 2020, s. 208-209.

4. Otomatik Karar Alma Mekanizması ve Veri İşleme

Otomatik karar alma mekanizması, hiçbir surette gerçek kişilerin müdahalesi olmaksızın veri işlemeye ilişkin karar alınabilmesini sağlamaktadır²⁷⁹. Veri sorumlusunun tabi olduğu AB'nin veya üye devletlerin iç hukuku tarafından veri sahibinin hak ve özgürlüklerinin korunması için uygun güvencelerin sağlanması, en azından veri sorumlusu tarafından gerçek kişinin müdahalesini elde etme hakkının bulunması halinde otomatik bireysel karar alma mümkündür.

Otomatik karar almaya cevaz veren uygun önlemler Kolluk ve Ceza Adaleti Direktifi'nde açıkça sayılmamıştır. Resitalde, bu türden veri işlenmesi halinde *veri sahibine spesifik bilgi sağlanması, gerçek kişinin müdahalesini elde etme, müdahalenin ardından yapılan değerlendirmeden sonra varılan karara ilişkin açıklama elde etme veya karara itiraz etme olanaklarının bulunması*, önlem olarak zikredilmiştir²⁸⁰. Zira otomatik karar alma mekanizmaları, kişinin “kişisel verisi üzerindeki belirleme hakkı” ve bireysel özerkliğe bir müdahaledir ve bu mekanizmalar aracılığıyla kişinin üzerinde hukuki sonuçlara yol açabilecek iş performansı, kredi konusunda güvenilirliği gibi değerlendirmeler yapılmaktadır²⁸¹.

a. Profillemeye ve Otomatik Karar Alma Mekanizması İlişkisi

Profillemeye, bir gerçek kişinin işyerindeki performansı, ekonomik durumu, sağlığı, kişisel tercihleri, ilgi alanları, güvenilirliği, davranışları, konumu, hareketleri gibi yönlerden analiz edilmesi ya da tahmin edilmesi için kullanılan kişisel verilerinin otomatik olarak işlenmesine ilişkin her tür yöntemdir²⁸².

Otomatik karar alma mekanizmasında insan müdahalesi olmaksızın bir algoritmadan yararlanılarak bir kişisel verinin işlenmesinden üretilen bir sonuç yani çıktı bulunmaktadır. Ancak bu sonuç ya da çıktının profil oluşturması gerekmemektedir. Profillemeye ise genellikle otomatik karar alma mekanizmalarından

²⁷⁹ WP29, “Guidelines on Automated Individual Decision-Making and Profiling for The Purposes of Regulation 2016/679”; Başalp, **Kişisel Verilerin Korunması ve Saklanması**, s. 54.

²⁸⁰ Kolluk ve Ceza Adaleti Direktifi resital m. 38.

²⁸¹ Dağ, **a.g.e.**, s. 122.

²⁸² Bkz. Kolluk ve Ceza Adaleti Direktifi m. 3/4; GDPR m. 4/4.

yararlanılabiliirse de bu elzem değildir. Söz gelimi kamusal alanlarda bulunan kameraların otomatik olarak belirli bir aracın hız sınırını hesaplayarak trafik cezası oluşturmaları, profillemeye gerektirmeyen otomatik karar alma mekanizmasıdır. Öte yandan belirli bir sürücünün alışkanlıklarının belirli süre boyunca izlenerek hız ortalaması, hız sınırı ihlalinin mükerrir olup olmadığı, başka trafik ihlallerinin olup olmadığı incelenerek profillemeye yapılması mümkündür²⁸³.

Profillemeye, genellikle pazarlama ve müşteri yönetim amaçlarıyla kullanılmakta iken polis ve ceza adaleti işlemleri bağlamında profillemeye başvurmak, kötüye kullanımlara yol açabilecektir. Zira bu surette bir karar alma; kişisel verilerin otomatik olarak değerlendirilmesi neticesinde veri sahibi hakkında insan unsuru tarafından bir değerlendirme yapılmaksızın gerçekleşecek ve veri sahibini etkileyecek bir karar alma olacaktır²⁸⁴. Ayrıca bireyin, toplanan verilerinin içeriğinin birileri tarafından denetlendiğini bilmesi, davranışlarında kısıtlamaya ve baskı altında hissetmesine yol açacaktır. Bu da bireyin kişisel verilerini denetleme olanağını ortadan kaldırmaktadır²⁸⁵. Olması gereken bu tür işlemlerin kaldırılması ve kişilerin özelliklerine göre yargılanması olsa da, 2016/681 PNR Direktifi gibi bazı düzenlemelerde kolluk kuvvetlerinin görevlerini yerine getirmesinde, profillemeye yardımcı olabilecektir²⁸⁶.

Kolluk ve Ceza Adaleti Direktifi m. 11'e göre veri işlemeye ilişkin veri sahibine olumsuz hukuki etki yaratacak veya onu önemli ölçüde etkileyecek profillemeye de dâhil otomatik bireysel karar almak yasaktır. Ancak olumsuz hukuki etki ile neyin kast edildiği anlaşılmamaktadır. Zira GDPR'da da buna ilişkin bir tanım bulunmamaktadır²⁸⁷. Kolluk ve Ceza Adaleti Direktifi m. 11/3'e göre gerçek kişiler arasında ayrımcılığa yol açabilecek profillemeye özel nitelikli kişisel veriler bakımından da yasaktır²⁸⁸. Verinin tamamen ırk, etnik köken veya dini aidiyetle ilgili bilgi içermesi

²⁸³ Aşıkoğlu, **a.g.e.**, s. 151.

²⁸⁴ Gür, **a.g.e.**, s. 33.

²⁸⁵ Bayram, **a.g.e.**, s. 5.

²⁸⁶ De Hert, Papakonstantinou, **a.g.e.**, s. 16.

²⁸⁷ Dülger, Özkan, **a.g.e.**, s. 108.

²⁸⁸ Söz gelimi yalnızca dini inançlara dayanan gruplar ve grup üyelerinin bu özel nitelikli kişisel verilerinin profillenmesi ayrımcılığa yol açacağından Direktif'e göre yasaktır. Ancak, belirli bir dini gruba bağlı olası terörist faaliyetlerde bulunan bir grup insan hakkında yürütülen soruşturmada, bu grup üyelerinin ibadet yerleri, din vaizleri, gelenekleri, öğretileri, üyeler ve topluluğun yapısına ilişkin

halinde bu verinin kullanımı veri sahibi bakımından ayrımcılığa yol açacaksa hukuka uygun bir profillemenin varlığından söz edilemez²⁸⁹.

b. Büyük Veri ve Otomatik Karar Alma Mekanizması İlişkisi

Yapay zekâ ve akıllı sistemler kullanılarak kişiler profillenmekte veya otomatik karar alma mekanizmalarına konu olmakta ve böylece büyük veri uygulamaları oluşturulmaktadır²⁹⁰. Büyük veriye ilişkin bir hüküm Kolluk ve Ceza Adaleti Direktifi'nde yer almamaktadır. Kolluk makamlarının büyük veri uygulamalarında; "Profilleme Bağlamında Kişisel Verilerin Otomatik Olarak İşlenmesine Dair Bireylerin Korunmasına İlişkin 2010/35 sayılı Avrupa Konseyi Tavsiye Kararı"²⁹¹ ve "Büyük Veri Dünyasında Kişisel Verilerin İşlenmesine Dair Bireylerin Korunmasına İlişkin Kılavuz"u gözetmesi önerilmiştir²⁹².

Büyük veri uygulamaları ile profillemeye yapıldığından büyük veriye kaynaklık edecek kişisel verinin sahibine asgari biçimde; veri işlemenin bir profillemeye faaliyeti olduğu, profillemenin amacı, sonuçları, profillemeye kullanılan algoritma, kişisel verinin saklanma süresi ve insan unsurunun yer aldığı yeniden değerlendirilebilen otomatik karar alma mekanizmasının bulunduğu hususları kapsamında bilgilendirme yapılmalıdır²⁹³.

Bir sözleşme metninde profillemenin ya da sair otomatik karar alma mekanizmasının kullanıldığı bir büyük veri uygulamasında, bu verilerin ileride kolluk veya adli makamlarla paylaşılabilmesine dair kılavuzun bulunması Kolluk ve Ceza Adaleti Direktifi kapsamında işlemeyi hukuka uygun kılar mı, değerlendirilmelidir. Bu noktada amaçla bağlılık ilkesi de gözetilecektir. Veri sorumlusu, sonradan ortaya çıkan bu kolluk ve ceza adalet faaliyetinde kullanılma amacının veri sahibi bakımından

verilerin işlenmesi maddi gerçeğe ulaşılması için oldukça önemli olup ayrımcılık yasağı nedeniyle yasak olmamalıdır. Bkz. Allen, van Beek, Borking, **a.g.e.**, s. 5.

²⁸⁹ Juraj Sajfert, Teresa Quintel, "Data Protection Directive (EU) 2016/680 For Police and Criminal Justice Authorities", **Cole/Boehm GDPR Commentary**, Edward Elgar Publishing, 2019, s.11, Çevrimiçi https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3285873 04.03.2020.

²⁹⁰ Aşikoğlu, **a.g.e.**, s. 150.

²⁹¹ Tavsiye karar 23.11.2010 tarihinde Bakanlar Komitesi'nin 1099. toplantısında kabul edilmiştir. Çevrimiçi <https://rm.coe.int/16807096c3> 29.09.2019.

²⁹² Allen, van Beek, Borking, **a.g.e.**, s. 10.

²⁹³ Aşikoğlu, **a.g.e.**, s. 161.

doğabilecek sonuçlarına dair bir risk değerlendirmesi yapmalıdır²⁹⁴. Türk hukuku bakımından ise KVKK’de polis ve ceza adalet faaliyetlerinde kişisel verilerin işlenmesine dair hüküm bulunmadığından bu noktada hukuken boşluk bulunmaktadır.

IV. VERİ ALICISI

A. Tanım

Veri alıcısı, kişisel verilerin paylaşıldığı gerçek veya tüzel kişi, kamu kuruluşu, ajanı veya başka bir organ olabilir ve AB üyesi olması gerekmez. Söz gelimi soruşturma makamı, yürütülen bir ceza soruşturmasındaki şüphelinin, yürütülen başka bir soruşturmada da şüpheli olduğuna dair bir belirti varsa örneğin, bir kasten öldürme olayı ile ilgili yürütülen soruşturmada, vergi kaçakçılığı soruşturmasında da şüpheli olan kişinin verilerini aktarabilir²⁹⁵. Bu veri aktarımı yalnız iki kolluk makamı arasında değil, kolluk makamı ve diğer kamu makamları arasında da yapılabilir. Örneğin oturma izni talebinde bulunan bir kişinin talebinin değerlendirilmesi sırasında sabıka kaydının bulunup bulunmadığını doğrulamak için göçmen bürosu ve adli makamlar arasında veri aktarımı gerekmektedir²⁹⁶. Yahut adli makamlardan medyaya bir veri aktarımı gerçekleşebilir. Örneğin polisin, kamuoyunun bilgi edinmesi için medya ile veri paylaşmaya yetkisi varsa, bu veri aktarımının kamu yararı için gerekli olup olmadığı değerlendirilmesi yapılmalıdır²⁹⁷.

B. Veri Aktarımı

Kolluk ve Ceza Adaleti Direktifi’nden önce ceza muhakemesinin yürütülmesi sırasında ulusal devlet otoritelerinin, diğer AB üyesi devletlere ihtiyaç duyduğu kişisel veriler konusunda herhangi bir kanuni düzenleme bulunmamaktaydı. Suçluların iadesi ya da istinabe gibi konularda başvurulmuş klasik yöntemler Adalet Bakanlıkları ve Dış İlişkileri aracılığıyla gündeme gelmekteydi. Bu da bilgi ve kişisel veri talep eden ve

²⁹⁴ Aşıkoğlu, **a.g.e.**, s. 170.

²⁹⁵ Allen, van Beek, Borking, **a.g.e.**, s. 12.

²⁹⁶ Allen, van Beek, Borking, **a.g.e.**, s. 13.

²⁹⁷ Allen, van Beek, Borking, **a.g.e.**, s. 13.

talep edilen devletlerin diplomat ve konsoloslukları arasında gerçekleşmekteydi. 1990 tarihli Schengen Konvansiyonu imzalayan devletler, ağır sınır ötesi suçları cezalandırmak ve mücadele etmek için cezai konularda işbirliği yapmayı taahhüt etmişlerdi²⁹⁸. Bu amaçla Konvansiyon'un 53. maddesinde Adalet Bakanlıkları veya Interpol aracılığıyla talep gönderme ihtimaline hâle getirmeksizin yardım taleplerinin doğrudan adli makamlar arasında olabileceği ve aynı şekilde iade edilebileceği düzenlenmişti.

Europol, Eurojust ve Interpol gibi uluslararası makamlara veri sağlamayı içeren uluslararası yükümlülükler, ikili anlaşmalar ve üye devletler ya da üçüncü ülkeler arasında yapılan karşılıklı adli yardım anlaşmaları gereği kişisel verilerin yurtdışına aktarımı mümkün olmaktadır. Zira AB düzeyinde özgürlük, güvenlik ve adalet konularında üye devletlerin polis ve diğer adli organlarının faaliyetlerinde işbirliği gerekmektedir²⁹⁹.

Kolluk ve Ceza Adaleti Direktifi'nin yürürlüğünden önce Konsey tarafından kolluk güçlerinde bulunan kişisel verilerin sınır ötesi paylaşımına ilişkin Hague Programı yapılmıştır. Program; verinin elde edilebilirliği ilkesi üzerine inşa edilmiştir ve kovuşturma öncesinde yargılamanın icrası için üye devlet kolluk makamının ihtiyacı olan kişisel verinin, bir diğer üye devletin muadil biriminden tedarik edilmesini hedeflemektedir³⁰⁰. Bu amaçla işbirliğini sağlamak için de Prüm Sözleşmesi³⁰¹ imzalanmıştır. *Schengen III* olarak anılan bu Sözleşme ile potansiyel suçlu ve teröristler ile ilgili veriler, DNA örnekleri, parmak izi örnekleri, araç plakaları sirküle etmektedir. Bir devletin tuttuğu kayıtlar, ulusal irtibat merkezi aracılığıyla yabancı ülkedeki verilerle karşılaştırılabilmektedir. Veriler uyduğu takdirde de, talep

²⁹⁸ Y.Y., **Exchange of Information and Data Protection in Cross-Border Criminal Proceedings in Europe**, Ed: Angeles Gutierrez Zarra, Berlin, Springer, 2015, s. 11.

²⁹⁹ Nitekim 1993 tarihli Maastricht Antlaşması ile cezai meselelerde adli işbirliği gereği terörizm olgusu, AB üyesi devletler arasında ortak yarar konusu olmuş ve Europol'ün görev alanına dâhil edilmiştir.

³⁰⁰ Gür, **a.g.e.**, s. 83.

³⁰¹ 27.05.2005 tarihinde Almanya, Avusturya, Belçika, Fransa, İspanya, Lüksemburg ve Hollanda arasında imzalanmış "Terörizm, Sınır Ötesi Suç ve Yasadışı Göç ile Mücadele Amacıyla Sınır Ötesi İşbirliğinin Güçlendirilmesi Hakkında Sözleşme".

eden devlete verinin bulunduğu yer verinin içeriğine yer verilmeksizin bildirilmektedir. Klasik adli yardım yöntemleri ile de veriler aktarılmaktadır³⁰².

Aktarım yapılırken veri aktarımının aciliyeti, varsa veri aktarımına neden olan bir suçun ağırlığı, bunun sınır ötesi karakteri, yürütülen soruşturmanın amacına ilişkin objektif nedenler dikkate alınarak verinin korunmasına ilişkin değerlendirme yapılmalıdır³⁰³. 95/46 sayılı Direktif, AB sınırları dâhilinde faaliyette bulunan kamu ve özel sektörden AB dışında olan ve yetersiz kişisel veri korumasına sahip üçüncü ülkelere veri aktarımı yapılmasına izin vermemiştir. Bu dönemde Komisyon; verinin doğası, işleme amacı, veri alıcısı ülke ve aktarımı yapacak ülkenin hukuk kurallarına göre güvenli olup olmadığına bakarak karar vermektedir³⁰⁴. ABAD, *Schrems Digital Rights İrlanda Ltd.*³⁰⁵ kararında yeterlilik kriterlerini belirlemiştir: Özel yaşamın korunması hakkının korunma düzeyi dikkate alınacak, ayrıca yeterli korumanın sağlanmaması halinde çok sayıda kişi bakımından bir zararın meydana gelip gelmeyeceği, ilgili devletin 108 sayılı Sözleşme'ye taraf olup olmadığı³⁰⁶ ve Sözleşme hükümlerini iç hukukuna aktarıp aktarmadığı gözetilecektir.

Bu meydana belirtilmelidir ki 108 sayılı Sözleşme'ye taraf olmak, tek başına yeterlilik şartını sağlamamaktadır. Zira Sözleşme, taraf devletten taraf olmayan devlete veri aktarımında maddi bakımdan bir koruma öngörmemiştir. Bu da taraf devletin, bir *staging post* olarak veri aktarımında kullanılması riskine yol açabilecektir³⁰⁷. Ayrıca 108 sayılı Sözleşme, veri mahremiyeti ihlali iddialarını inceleyecek bağımsız bir denetleyici makam da içermemektedir. Bu nedenle 108 sayılı Sözleşme'ye taraf olunmasına rağmen, veri alıcısının veri koruma düzeyini değerlendirmek için Avrupa Veri Koruma Otoritesi'nin de görüşüne başvurulabilecektir³⁰⁸.

³⁰² Çam, **a.g.e.**, s. 131; Yenisey, **Kolluk Hukuku**, s. 404.

³⁰³ Allen, van Beek, Borking, **a.g.e.**, s. 14.

³⁰⁴ Gür, **a.g.e.**, s. 42.

³⁰⁵ *Schrems Digital Rights İrlanda Ltd* [BD], B. No: C-362/14, 06.10.2015 Çevrimiçi https://curia.europa.eu/jcms/jcms/j_6/en/ 29.03.2020.

³⁰⁶ Başalp, **Kişisel Verilerin Korunması ve Saklanması**, s. 69.

³⁰⁷ Kaya, **Assessing the Transfer of Personal Data in the European Union in the Light of the Data Protection Directive**, s. 33.

³⁰⁸ Dülger, Özkan, **a.g.e.**, s. 128.

AB ve ABD arasında kişisel veri aktarımı da değerlendirilmelidir. ABD'nin terör saldırılarını önlemek amacıyla iç güvenlik istihbaratı ve kolluk faaliyetlerine ilişkin mevzuatının güncellenmesi sonucu³⁰⁹ AB'den ABD'ye veri aktarımının, kişisel veri korumasını ihlal edebileceği gündeme gelmiştir. AB'den ABD'ye veri aktarımının sağlıklı bir şekilde sürdürülmesi için *Safe Harbour İlkeleri* ihdas edilmiştir. Safe Harbour Lösung Anlaşması ile belirlenen bu ilkeler, 95/46 sayılı Direktif ile getirilen yeterli koruma şartı aranmaksızın veri aktarımını mümkün kılmıştır³¹⁰. ABD'nin merkezi veri koruma düzenlemelerini kabul etmemesi ve yalnız sektörel bazda veri mahremiyeti düzenlemelerine sahip olması nedeniyle AB'deki veri koruma düzeyi sağlanamamıştır³¹¹.

Yukarıda yeterlilik kriterlerinde atıf yaptığımız *Schrems Kararı* ile Safe Harbour'ın geçersiz kılınmasının³¹² ardından uluslararası veri aktarım şartlarına ilişkin yeni mekanizma öngören 29.02.2016 tarihli Privacy Shield Kararı kabul edilmiştir³¹³. Karar yalnız AB'den ABD'ye yapılan veri aktarımlarında uygulanacaktır. Ancak

³⁰⁹ 11 Eylül sonrası ihdas edilen mevzuata USA Patriot Act, gizli izleme otoritelerini mümkün kılan USA Foreign Intelligence Surveillance Act örnek verilebilir.

³¹⁰ Başalp, **Kişisel Verilerin Korunması ve Saklanması**, s. 75; Boz, **a.g.e.**, s. 76.

³¹¹ Zira ABD'de veri bir ekonomik değer olarak nitelendirilip mali olarak önemi haizdir, oysa Avrupa'da kişisel verilerin korunması hakkı bir kişilik hakkıdır. Bu nedenle Avrupa'da kişisel veri koruma düzeyi daha yüksektir. Bkz. Aşıkoğlu, **a.g.e.**, s. 25; Boz, **a.g.e.**, s. 89.

³¹² ABAD, 06.11.2015'te Maximillian Schrems C-362/14 sayılı karar ile Safe Harbour Kararı'nın geçersizliğine hükmetmiştir. Schrems kararına kısaca değinmek gerekirse 2008'den beri Facebook kullanıcısı olan Bay Schrems İrlanda Veri Koruma Komiseri'ne şikâyetle bulunmuştur. Şikâyet gerekçesi, Snowden olayından sonra İrlanda'nın Facebook serverlarının ABD'ye kendi kişisel verilerini aktarmasıdır. Ayrıca bu aktarım AB hukuku anlamında yeterli düzeyde veri korumasını sağlayarak yapılmamıştır. İrlanda Veri Koruma Komiseri, Schrems'in iddialarını kabul etmemiştir, zira veri aktarımı Safe Harbour Anlaşması'na uygundur. Nihayet ABAD Safe Harbour Anlaşması'nın geçersizliğine hükmetmiştir. Zira herhangi bir sınırlama, kategorizasyon, istisna olmaksızın ABD'ye aktarılmakta, veri ABD'ye aktarıldıktan sonra burada FBI tarafından dahi gelişigüzel kullanılabilir, yani ABD'de ulusal güvenlik ve kamu yararı Safe Harbour'ın veri koruma çerçevesinin önüne geçmektedir. Bkz. Valentin M. Pfisterer, "The Right to Privacy- A Fundamental Right in Search of Its Identity: Uncovering the CJEU's Flawed Concept of The Right to Privacy", **German Law Journal**, s. 20, 2019, s. 724-725; Brkan, **a.g.e.**, s. 874-875; Shakila Bu-Pasha, "Cross-Border Issues Under EU Data Protection Law With Regards to Personal Data Protection", **Information and Communication Technology Law**, c. 26, s. 3, 2017, s. 220-221.

³¹³ Pfisterer, **a.g.e.**, s. 723; Aşıkoğlu, **a.g.e.**, s. 56; GDPR ve Kolluk ve Ceza Adaleti Direktifi'nin yürürlüğü ile artık sınır ötesi veri aktarmak ve veri aktarımını kolaylaştırmak için aynı zamanda ABAD'nin de içtihatları dikkate alınmalıdır. Zira pek çok şirket ve devlet, AB ve AB üyesi devletlerle işbirliği yaptığından veri işleme standardını da uyumlaştırmalıdır. Buna "Brüksel Etkisi" denmektedir. Bkz. Cedric Ryngaert, Mistale Taylor, "The GDPR As Global Data Protection Regulation?", **American Journal of International Law**, s. 114, 2020, s. 9; Bart van der Sloot, "Legal Consistency After the General Data Protection Regulation and the Police Directive", **European Journal of Law and Technology**, c. 9, s. 3, 2018; Çevrimiçi https://edps.europa.eu/data-protection/our-work/subjects/police-directive_en 11.03.2020, s.5.

Privacy Shield ile ilgili de veri koruma otoritelerinin endişeleri devam etmektedir. Zira bu düzenleme AB'den ABD'ye aktarılan verilerin üçüncü ülkelere aktarımına da izin vermektedir, üstelik bu halde GDPR'ın 5. bölümündeki veri aktarım kuralları da geçerli olmamaktadır. Privacy Shield'de öngörülen veri koruma ilkeleri ulusal güvenlik, kamu yararı, kolluk faaliyetleri nedeniyle kanun, hükümet tasarrufu ya da içtihatlarla devre dışı kalabilmektedir. Bu nedenle Privacy Shield'in yakın zamanda Avrupa Veri Koruma Reformu ile uyumlu şekilde güncellenmesi beklenmektedir³¹⁴. Nitekim yakın zamanda da ABAD tarafından Privacy Shield'in hükümsüz olduğuna hükmedilmiştir. ABD hukuku, GDPR m. 45 ve Avrupa Birliği Temel Haklar Şartı m. 7, 8 ile 47 eşdeğer anlamda verileri aktarılan veri sahibine yeterli koruma düzeyi sağlayamamaktadır. Zira ulusal mevzuatta öngörülen gerekli sınırlama ve güvenceler ile müdahale halinde efektif yargısal koruma sağlanamamaktadır³¹⁵.

Kişisel verilere ilişkin başta Kolluk ve Ceza Adaleti Direktifi olmak üzere AB'deki düzenlemelerin amacı; kişisel veri akışına ket vurmak değil, bilakis bu akışın veri sahibinin hak ve özgürlüklerini koruyarak kolaylaşmasını sağlamaktır. Bu nedenle verilerin aktarımının mutlak olarak yasaklanması beklenemez. Fakat pek tabidir ki aktarımın yapılacağı ülkede de kişisel verilerin korunur durumda olması ve böylece en azından AB sınırlarında veri cennetlerinin oluşması engellenmelidir. Yanlış bir kişisel veri aktarılmışsa ya da hukuka aykırı olarak aktarılmışsa bu durumda veri alıcısı derhâl bilgilendirilmeli ve kişisel veri, düzeltilmeli, silinmeli yahut 16. madde uyarınca işlenmesi sınırlandırılmalıdır³¹⁶.

1. Veri Aktarımının Şartları

a. Amaç

³¹⁴ Bu-Pasha, **a.g.e.**, s. 224-225.

³¹⁵ *Facebook Ireland and Schrems [BD]*, B. No: C-311/18, 16.07.2020, para. 168 Çevrimiçi <http://curia.europa.eu> 17.07.2020. Örneğin FISA'nın (Foreign Intelligence Surveillance Act/Dış İstihbarat Gözetim Kanunu) 702. Bölümü uyarınca gözetim programları ölçülülük ilkesine uygun güvenceler bulunmamaktadır ve bu, Şart'ın 52/1. maddesi c. 2'ye uygun değildir (para. 178). Ayrıca Privacy Shield'de öngörülen ombudsman mekanizması Şart'ın 47. maddesi uyarınca ABD'ye aktarılan verilerin korunması için yargısal mekanizmaya eşdeğer değildir (para. 197).

³¹⁶ Kolluk ve Ceza Adaleti Direktifi m. 7/3.

Veri aktarımı Kolluk ve Ceza Adaleti Direktifi'nin amaçları doğrultusunda yani suçların önlenmesi, soruşturulması, ortaya çıkarılması, kovuşturulması ve cezaların infazı amacı ile gerçekleşmelidir.

b. Yetkili Makam

Kolluk ve Ceza Adaleti Direktifi kapsamında kişisel verilerin AB üyesi olmayan üçüncü ülkelere ve uluslararası organizasyonlara aktarılması mümkündür. Aktarım, yalnız resmi kanallar aracılığıyla yapılmakta ve AB üyesi devletteki kolluk veya adli makamdan üçüncü bir devletteki kolluk veya adli makama veri aktarılmaktadır³¹⁷. Kişisel verilerin aktarıldığı veri sorumlusunun Kolluk ve Ceza Adaleti Direktifi'ne göre yetkili makam³¹⁸ olması gerekmektedir. Kişisel verilerin kolluk makamı olmayan bir kamu kurumuna uluslararası transferine yalnızca istisnai olarak aktarımın yapılacağı kurum, kuruluş veya makamın görevinin yerine getirilmesi isteniyorsa ve verilerin yetkili bir polis kuruluşuna aktarılmasında etkili bir yolun bulunmadığı münferit olaylarda izin verilebilir³¹⁹.

c. Ön İzin

Veri aktarımını yapacak devlet, transit devlet ise yani başka bir AB üyesi devletten kişisel verinin aktarıldığı devlet ya da erişimine izin verilen devlet ise bu durumda izin prosedürü gündeme gelmektedir. Yani devam eden veri aktarımlarında Kolluk ve Ceza Adaleti Direktifi m. 35/1-c'ye göre ilk aktarımı yapan devletin izni gerekmektedir. Örneğin; Fransa'daki yetkili makamdan ABD'deki yetkili makama aktarılan veriyi, ABD de Brezilya'daki yetkili makama aktarmak isterse bu halde

³¹⁷ Sajfert, Quintel, **a.g.e.**, s. 18.

³¹⁸ Yetkili makamdan anlaşılması gereken, Kolluk ve Ceza Adaleti Direktifi'nin "Tanımlar" bölümünde yer alan kamu güvenliğine yönelik tehditlerin önlenmesi, suçların önlenmesi, soruşturulması, tespit edilmesi veya kovuşturulması veya cezai cezaların infazı için yetkili herhangi bir kamu makamı (m. 3/7-a) ve AB üyesi devletin kanunları tarafından, kamu güvenliğine yönelik tehditler de dâhil suçların önlenmesi, soruşturulması, ortaya çıkarılması veya kovuşturulması ya da cezaların infazı amacıyla kamu otoritesini ve kamu yetkileri kullanılmak üzere verilen diğer herhangi bir kurum veya kuruluştur (m. 3/7-b).

³¹⁹ Allen, van Beek, Borking, **a.g.e.**, s. 14.

Fransa'daki yetkili makamın Brezilya'ya yapılacak veri aktarımına izin vermesi gerekmektedir³²⁰.

Ancak kamu güvenliği veya kamu menfaatini ağır ve ciddi şekilde tehdit eden bir halin bulunması halinde ön izin alınması gerekmemektedir. Aktarım izni aranmayan bir hal, acil durumların varlığı ve veri sahibinin temel menfaatinin korunması gerekliliğinin bulunmasıdır. Ancak bu halde de menfaat ve veri sahibinin hakları arasında denge dikkate alınacak ve durum belgelenecektir³²¹.

d. Yeterli Düzeyde Veri Koruması

(1) Yeterlilik Kriterleri

Kolluk ve Ceza Adaleti Direktifi'ne göre veri aktarımının yapılacağı devlet ya da uluslararası organizasyon veri koruma düzeyi bakımından güvenilir durumda olmalıdır³²². Yeterli düzeyde korunmadan anlaşılması gereken, Avrupa Birliği Temel Haklar Şartı'ndaki temel hak ve özgürlüklerin korunma düzeyi bakımından esasen AB ile eş değer olmaktadır³²³.

Aktarımın yapılacağı kişisel veri, o ülkeden de başka bir ülke ya da organizasyona aktarılacaksa; cezai soruşturma konusu olan fiil, ilk aktarım amacı, sonraki aktarımın yapılacağı devlet veya organizasyonun veri koruma durumu göz önünde bulundurularak aktarıma izin verilecektir. Veri koruma durum ve düzeyi Avrupa Komisyonu'nun hazırladığı listelere dayanılarak tespit edilmektedir. Bu tespit *ad hoc* temele dayanıp³²⁴, dikkate alınan kriterler; devletlerin veri koruma mevzuatları, mahkeme içtihatları, temel hak ve özgürlüklere saygı düzeyi, devletlerin uluslararası

³²⁰ Sajfert, Quintel, **a.g.e.**, s. 18.

³²¹ Bilişim ve Teknoloji Hukuku Enstitüsü, **a.g.e.**, s. 12.

³²² Dülger, Özkan, **a.g.e.**, s. 127; Yeterli düzeyde veri koruması şartı, 95/46 sayılı Direktif'te de bulunmaktaydı, ancak m. 25/2'ye göre yeterlilik değerlendirmesinde kesin standart ve kriterler yoktu. Bu nedenle GDPR ve Kolluk ve Ceza Adaleti Direktifi'nde sınır ötesi veri aktarımlarında kriterlere yer verilmiştir. Bu-Pasha, **a.g.e.**, s. 219.

³²³ Svetlana Yakovleva, "Should Fundamental Rights to Privacy and Data Protection be a Part of the EU's International Trade 'Deals'?", **World Trade Review**, c. 17, s. 3, 2018, s. 486.

³²⁴ Kaya, **Assessing the Transfer of Personal Data in the European Union in the Light of the Data Protection Directive**, s. 23.

düzenlemelere taraf olup olmadıklarıdır³²⁵. Kriterlerin tamamı Kolluk ve Ceza Adaleti Direktifi m. 36/2’de sayılmıştır:

- (a) *hukukun üstünlüğü, insan hakları ve temel hak ve özgürlüklere saygı, kamu güvenliği, savunma, ulusal güvenlik, ceza hukuku ve kamu makamlarının kişisel verilere erişimine ilişkin ilgili mevzuat ve uygulaması, veri koruma kuralları, kişisel verinin üçüncü ülke ya da uluslararası organizasyona aktarımı için uyulması gereken kurallar ve güvenlik önlemleri, verisi aktarılan veri sahibinin hakları ve efektif idari ve adli mekanizmaların olması.*
- (b) *veri sahibinin haklarını kullanması için telkinlerde bulunan ve yardımcı olan, veri koruma kurallarına uygun davranılması için yeterli yetkilerle donatılmış üçüncü ülkedeki veya uluslararası organizasyondaki bir ya da birden çok bağımsız denetleyici makamın varlığı ve etkin işleyişinin olması.*
- (c) *üçüncü ülke ya da uluslararası organizasyonun uluslararası taahhütleri, hukuken bağlayıcı sözleşmeler ve çok taraflı veya bölgesel sistemlerde kişisel verilerin korunmasına ilişkin enstrümanların olması.*

Komisyon, veri koruma yeterlilik düzeyini bu kriterlere göre belirledikten sonra bir uygulama tasarrufu (*implementing act*) ile uluslararası organizasyon ya da üçüncü ülke, üçüncü ülkedeki bir bölge veya birkaç spesifik sektörün bu kriterleri karşıladığına hükmeder. Uygulama tasarrufunda hangi bölge ya da sektöre ilişkin yeterlilik kararı verildiği belirli olmalıdır, denetleyici makam belirtilmelidir ve tasarruf, üçüncü ülke veya uluslararası organizasyondaki ilgili gelişmeleri dikkate alarak en azından dört yılda bir olmak üzere bir gözden geçirme mekanizması sağlamalıdır³²⁶.

Komisyon, üçüncü ülke ya da organizasyonun yeterli korumayı sağlayamadığı kanaatindeyse yeterlilik kararını geriye yürütmeyecek şekilde kaldırabilir, değiştirebilir veya askıya alabilir³²⁷. Komisyon’un yeterlilik kararları ve kaldırma, değiştirme ve askıya alma kararları Avrupa Birliği Resmi Gazetesi’nde yayımlanacaktır³²⁸.

³²⁵ Bilişim ve Teknoloji Hukuku Enstitüsü, **a.g.e.**, s. 12; Allen, van Beek, Borking, **a.g.e.**, s. 14.

³²⁶ Kolluk ve Ceza Adaleti Direktifi m. 36/3.

³²⁷ Kolluk ve Ceza Adaleti Direktifi m. 36/5.

³²⁸ Kolluk ve Ceza Adaleti Direktifi m. 36/8.

(2) Yeterlilik Kararının Aranmadığı Haller

Yeterli veri koruma düzeyinin bulunduğuna ilişkin kararın alınması, veri aktarımında mutlak bir şart değildir. Kolluk ve Ceza Adaleti Direktifi'nin öngördüğü bazı hallerde üçüncü ülke veya organizasyonla bu karar olmaksızın veri aktarımı mümkündür. Bu hallerden ilki, aktarım yapılmak istenen üçüncü devlet ya da organizasyonun kişisel verilerin korunması bakımından uygun güvencelere sahip olduğuna ilişkin bağlayıcı bir belgeye sahip olmasıdır³²⁹. 95/46 sayılı Direktif m. 26/2, bu hükmün muadili mahiyetindedir. 95/46 sayılı Direktif'te veri sorumlusunun, veri sahibinin temel hak ve özgürlüklerinin korunması için yeterli garantiyi göstermesi ve üye devletin transfere onay vermesi halinde veri aktarımına cevaz verilmişti. Ayrıca aranılan garantinin bir sözleşmede yer alması da mümkündür. Kolluk ve Ceza Adaleti Direktifi, 95/46 sayılı Direktif'te düzenlenmesi ihtiyari olarak yer alan garanti sözleşmesini, bağlayıcı bir belge arayarak veri aktarımında veri korumasını bir adım ileri götürmüştür.

Yeterlilik kararının aranmadığı bir diğer hal de veri sorumlusunun aktarıma dair tüm koşulları değerlendirerek veri korunması bakımından uygun güvencenin bulunduğu kanısında olmasıdır³³⁰. Ancak bu durumda dahi öncelikle veri sorumlusu, denetleyici makama aktarıma ilişkin bildirimde bulunmakla yükümlüdür. Veri sorumlusu ayrıca aktarıma ilişkin tarih, saat, aktarım gerekçesi, alıcı makamın ismi ve iletişim bilgilerini belgelemeli ve talep halinde denetleyici makama ibraz etmelidir.

Garanti belgesinin bulunmaması veya veri sorumlusunun uygun güvencelerin bulunduğu kanaatine sahip olmaması halinde de veri aktarımı şu amaçlarla mümkündür³³¹:

- (a) *veri sahibinin veya başka bir kişinin hayati çıkarlarını korumak*
- (b) *veri aktarımını yapacak üye devlette kişisel verilerin aktarımına ilişkin mevzuatın öngördüğü biçimde veri sahibinin meşru menfaatlerini korumak*

³²⁹ Kolluk ve Ceza Adaleti Direktifi m. 37/1-a.

³³⁰ Kolluk ve Ceza Adaleti Direktifi m. 37/1-b.

³³¹ Kolluk ve Ceza Adaleti Direktifi m. 38/1.

- (c) *bir üye devletin veya üçüncü bir ülkenin kamu güvenliği için acil ve ciddi bir tehdidi önlemek*
- (d) *münferit durumlarda, Kolluk ve Ceza Adaleti Direktifi'nin 1. maddesindeki amaçları gerçekleştirmek veya*
- (e) *münferit bir durumda, Kolluk ve Ceza Adaleti Direktifi'nin 1. maddesindeki amaçlarla ilgili yasal talepleri oluşturmak, uygulamak veya savunmak.*

Kolluk ve Ceza Adaleti Direktifi'nin ihdas amacına göre veri aktarımının yapıldığı hallerde, somut olayda veri sorumlusu; kamu yararının sağlanması ile veri sahibinin hak ve özgürlükleri arasında dengesizliğin bulunması halinde veri aktarımının gerçekleşmemesi kararı verebilecektir³³². Yani Kolluk ve Ceza Adaleti Direktifi m. 38/2, veri sahibinin temel hak ve özgürlüklerini kamu yararından önce görmüştür.

95/46 sayılı Direktif'te veri sahibinin önerilen veri aktarımına açık şekilde rızasının olması hali de yeterlilik kararının alınmadığı hallerden biri iken³³³ Kolluk ve Ceza Adaleti Direktifi, rızaya böyle bir hukuki sonuç bağlamamıştır.

2. Veri Aktarımının Doğrudan Veri Alıcısına Yapılması

a. Uluslararası Antlaşma Temeline Dayanmayan Doğrudan Veri Aktarımı

Kural olarak Kolluk ve Ceza Adaleti Direktifi'nin öngördüğü faaliyetler bakımından veri aktarımı öncelikle üçüncü ülke veya uluslararası kuruluştaki veri sorumlusuna aktarılmaktadır. Ancak Kolluk ve Ceza Adaleti Direktifi m. 39/1, yetkili makam tarafından yurtdışındaki bir alıcıya doğrudan aktarım yapılabilmesine de izin vermiştir. Doğrudan aktarım;

- (a) *veri aktarımı, veri aktaran makam tarafından AB veya üye ülke kanunlarının, Kolluk ve Ceza Adaleti Direktifi'nin 1/1. maddesinde belirtilen amaçları yerine getirmesi için muhakkak gerekli ise,*

³³² Dülger, Özkan, **a.g.e.**, s. 129.

³³³ Bkz. 95/46 sayılı Direktif m. 26/1.

- (b) veri aktaran yetkili makam, ilgili veri sahibinin temel hak ve özgürlüklerinin, aktarım gerektiren somut olayda kamu yararından üstün olmadığını tespit etmişse,
- (c) veri aktaran yetkili makam, üçüncü ülkedeki Kolluk ve Ceza Adaleti Direktifi'nin 1. maddesindeki amaçları gerçekleştirmekle yetkili makama zamanında veri aktarımını gerçekleştirmezse aktarım etkisiz ve uygunsuz olacaksa,
- (d) etkisiz veya uygunsuz olmadıkça üçüncü ülkedeki Kolluk ve Ceza Adaleti Direktifi'nin 1. maddesindeki amaçları gerçekleştirmekle yetkili makama gecikmeksizin bildirim yapılmışsa,
- (e) veri aktaran yetkili makam veri alıcısını, ancak veri işlemenin gerekli olması halinde yalnızca belirtilen amaç/amaçlarla veri işleyebileceği konusunda bilgilendirmişse mümkündür³³⁴.

Belirtilmelidir ki bu şartlar kümülatif olarak sağlandığında üçüncü ülkedeki veri alıcısına doğrudan aktarım yapılabilecektir. Veri aktaran yetkili makam, doğrudan aktarımın yapıldığı hususunda da denetleyici makama durumu bildirmekle³³⁵ ve aynı zamanda aktarımı belgelendirmekle yükümlüdür³³⁶.

b. Uluslararası Antlaşma Temeline Dayanan Doğrudan Veri Aktarımı

Cezai meselelerde adli işbirliği ve polis işbirliği alanında AB üyesi devletler ve üçüncü ülkeler arasında yürürlükte olan herhangi bir ikili veya çok taraflı uluslararası antlaşma uyarınca, Kolluk ve Ceza Adaleti Direktifi m. 39/1'de şartlar aranmaksızın veri aktarımı doğrudan veri alıcısına yapılabilecektir. Kolluk ve Ceza Adaleti Direktifi m. 39, Direktif ile gelen bir yenilik olup asimetrik veri aktarımına izin vermektedir.

³³⁴ Kolluk ve Ceza Adaleti Direktifi m. 39/1.

³³⁵ Kolluk ve Ceza Adaleti Direktifi m. 39/3.

³³⁶ Kolluk ve Ceza Adaleti Direktifi m. 39/4.

Genellikle siber suçlar ya da bilişim sistemleri kullanılarak işlenen suçlarda, AB üyesi bir devlette yetkili makam olan kolluk ya da adli makamdaki, üçüncü bir devletteki genellikle hizmet sağlayıcısı olan özel kişiye veri aktarımında asimetrik aktarım gündeme gelmektedir³³⁷. Asimetrik veri aktarımı, suçların önlenmesi, ceza muhakemesi ve cezaların infazı amacının sağlanması için *muhakkak gerekli* olmalıdır. Yani asimetrik aktarıma konu olacak veri salt fişleme veya veri hacmini artırmak için kullanılamaz³³⁸.

Muhakkak gerekli olmaya karar verirken, alıcı makamın faaliyetleri, yetkileri göz önüne alınmalıdır. Ayrıca asimetrik aktarımda ikincilik ilkesi gözetilmelidir. Bu durumlarda üçüncü devletteki yetkili makama yapılacak veri aktarımı güvenli değildir ya da yetkili makam, aktarımlara vaktinde yanıt vermeyen bir durumdadır. Asimetrik aktarıma başvurulmuşsa üçüncü ülkedeki yetkili makam aktarımdan haberdar edilmelidir. Ancak devletin yozlaşmış durumda olması veya fiilen devlet olma niteliğini kaybetmiş olması halinde haberdar etmek gerekmeyecektir³³⁹.

3. Türk Hukukunda Veri Aktarımı

KVKK m. 9'da ilgilinin açık rızası bulunmaksızın kişisel verilerin yurtdışına aktarılamayacağı düzenlenmiştir. Ancak Kolluk ve Ceza Adaleti Direktifi bağlamında işlenen kişisel veriler Türk mevzuatına göre KVKK kapsamında değildir. Adli işbirliği sözleşmeleri ve 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun bağlamında³⁴⁰ özellikle ceza muhakemesi sürecinde kişisel verilerin yurtdışına aktarımı mümkündür.

V. VERİ KORUMA GÖREVLİSİ

Veri sorumlusunun Kolluk ve Ceza Adaleti Direktifi m. 32 uyarınca veri korumada yardımcı olması amacıyla atamakla yükümlü olduğu veri koruma

³³⁷ Sajfert, Quintel, **a.g.e.**, s. 7

³³⁸ Sajfert, Quintel, **a.g.e.**, s. 19.

³³⁹ Sajfert, Quintel, **a.g.e.**, s. 20.

³⁴⁰ 703 sayılı KHK m. 15 ile 5549 sayılı Kanun uyarınca yapılacak uluslararası bilgi değişimine ilişkin 12. madde ilga edilmiştir.

süjesidir³⁴¹. Mahkemeler ve diğer yargı makamları veri koruma görevlisi atama yükümlülüğü altında değildir³⁴². Yüksek nitelikli veri koruma görevlilerinin getirilmesi, daha yüksek derecede veri koruma ve veri koruma kurallarına daha yakın uyuma katkıda bulunurken, mahkemelerin ve diğer adli makamların bu yükümlülüğünden muaf tutulabilmesi, bu süjelere yardım edilmesini engelleyerek potansiyel sorunlu bir durum yaratabilir³⁴³.

Almanya’da özel sektörde otomatik veri işleme sistemleri ve kırktan fazla kişinin çalışması şartıyla şirketler bakımından istisnai olarak, kamu kurumları bakımından ise zorunlu olarak veri koruma görevlisi atanmaktadır³⁴⁴.

Veri koruma görevlisinin yükümlülüklerine aykırılığı halinde hukuki ve cezai sorumluluğu bulunmakla birlikte bu, veri sorumlusunun hukuki ve cezai sorumluluğunu ortadan kaldırmamaktadır³⁴⁵.

VI. DENETLEYİCİ MAKAM

Denetleyici makam, Kolluk ve Ceza Adaleti Direktifi’nin uygulanması ile yükümlü olan bağımsız resmi bir organdır. Bu makamın GDPR uyarınca kurulmuş denetleyici makam olup Kolluk ve Ceza Adaleti Direktifi kapsamında da fonksiyon icra etmesine Kolluk ve Ceza Adaleti Direktifi m. 41/3 uyarınca cevaz verilmiştir. Denetleyici makamın esas fonksiyonu, veri sahiplerinin temel hak ve özgürlüklerinin korunması ve verilerin serbest dolaşımını sağlamaktır. Denetleyici makam; kurumlara ve denetleyicilere tavsiyelerde bulunmak, Direktifin hükümlerini ihlal edenlerin gerekli tüm bilgilerini elde etmek ve veri kontrol faaliyetlerini düzeltmek için etkili danışma, soruşturma ve düzeltici yetkilerle donatılmıştır³⁴⁶. Ancak GDPR’da denetleyici makamın idari para cezası verme yetkisi mevcutken, Kolluk ve Ceza Adaleti Direktifi’nde makama bu yetki tanınmamıştır.

³⁴¹ Marquenie, **a.g.e.**, s. 335.

³⁴² Kolluk ve Ceza Adaleti Direktifi m. 32/1.

³⁴³ Marquenie, **a.g.e.**, s. 335.

³⁴⁴ Aşıkoğlu, **a.g.e.**, s. 71.

³⁴⁵ Aşıkoğlu, **a.g.e.**, s. 72.

³⁴⁶ Marquenie, **a.g.e.**, s. 335.

AB veri koruma modeli genel olarak ilgili üye devletlerin iç hukukunda kişisel verilerin korunması kurallarının uygulanmasıyla görevli bağımsız idari otoritelerin kurulmasını öngörmektedir. Ancak polis ve ceza adaleti bağlamında kişisel verilerin işlenmesinde bağımsız idari otoriteler³⁴⁷ ve mahkemeler başta olmak üzere diğer adli makamlar arasında bu makamların hangisinin faaliyetinin gerektirdiği ihtiyaçların önceleneceği tartışma konusudur.

Veri koruma otoriteleri genellikle geniş kapsamlı olmasa da veri işleme faaliyetlerini denetleme yetkilerini, kendi yetki alanları dâhilinde yürütülen tüm veri işlemlerine ve uygulamalarına uygulamak istemektedir. Öte yandan adli makamlar ise görevlerini yerine getirirken üçüncü şahısların kişisel veri işlemlerini denetlemesinin haksız olduğunu ve bunların gereğinden fazla ölçüde kurumsal bağımsızlıktan yararlandıklarını düşünme eğilimindedir. Bu hususta kilit nokta, veri koruma otoritelerinin yargı makamları ve adli makamlarca yapılan veri işleme faaliyetlerini denetleyip denetleyemeyeceğidir³⁴⁸. Bu anlamda üye devletler, hukuk sistemleri ve tercihlerine göre karar verebilmektedir. Bu meyanda adli makamların adli kapasiteleri dâhilindeki işlemlerinin Kolluk ve Ceza Adaleti Direktifi hükümlerinden etkilenmemesi gerektiği bazı yazarlarca³⁴⁹ iddia edilmişse de kanımızca buna dayanak olarak yazarların gösterdiği Kolluk ve Ceza Adaleti Direktifi'nin 17. maddesi Direktif'in bizatihi ihdas edilme sebebini gereksiz kılmaktadır.

Denetleyici makamların tavsiye verme fonksiyonu bulunmaktadır. Örneğin; veri sorumluları ve veri işleyenler dosyalama sisteminin parçası olan veri işleme faaliyetlerini, veri koruma etki değerlendirmesi sonucunda mevcut risklerin durumunu, veri koruma için ne tür teknolojilerin kullanıldığı ve bu teknolojinin risk durumunu denetleyici makama danışarak yürütmekle yükümlüdürler.

³⁴⁷ Bağımsızlık kavramına farklı açılardan yaklaşılabilir: Kurumsal bağımsızlık, kuvvetler ayrılığı çerçevesinde ayrı bir kuvvet içinde makamın yer alması; işlevsel bağımsızlık, koruma otoritesinin içerik ve kapsam yönünden görevini ifa ederken kimseden emir talimat almamasını; ekonomik bağımsızlık da koruma otoritesinin idari teşkilatta bütçe ve planlama bakımından bağımsız olmasını ifade eder. 95/46 sayılı Direktif'te AB'nin üye devletlerin anayasal sistemlerine müdahale edemeyeceğinden koruma otoritesinin fonksiyonel olarak bağımsız olması gerekmekte, ancak iç hukuktaki yapılanmasına karışılmamıştır. Bkz. Başalp, **Kişisel Verilerin Korunması ve Saklanması**, s. 79-80. Kolluk ve Ceza Adaleti Direktifi'nde de aynı şekilde veri koruma otoritesinin yapılanmasına karışılmamıştır.

³⁴⁸ De Hert, Papakonstantinou, **a.g.e.**, s. 13.

³⁴⁹ De Hert, Papakonstantinou, **a.g.e.**, s. 13.

Kolluk ve Ceza Adaleti Direktifi'nde ayrıca denetleyici makama faaliyetleri hakkında bildirilen ihlal ve uygulanan cezaların listesini içerecek yıllık rapor hazırlama görevi de yüklenmiştir. Denetleyici makam, hazırladığı yıllık faaliyet raporlarını ulusal parlamentoya, hükümete ve iç hukuka göre belirlenen diğer makamlara iletmekle yükümlüdür³⁵⁰. Faaliyet raporları, denetleyici makamın kamuya hesap vererek işlemlerinde şeffaflığı sağlayan ve veri koruma alanında görüşlerini kamuoyuna ifade etmesini sağlayan enstrümanlardır³⁵¹.

Türkiye uygulamasında kişisel verileri koruma görevi yüklenmiş kurum ise Kişisel Verileri Koruma Kurumudur. KVKK ile kurulan Kurum, Kişisel Verileri Koruma Kuruluna veri işleme ilkelerinin uygulanmasında takip ve yönlendirme misyonu yüklemiş ve Kurulun bağımsız olduğunu belirtmiştir³⁵².

VII. AVRUPA VERİ KORUMA KURULU

AB Veri Koruma Reformu ile getirilen bir yenilik de WP29'un yerine AB Veri Koruma Kurulunun kurulmasıdır. 95/46 sayılı Direktif'e dayanarak kurulan WP29 bir danışma mekanizmasıydı ve AB üyesi devletlerin ulusal veri koruma otoritelerine rehberlik etmesi için görüş ve tavsiye yayınlamaktaydı. WP29'un bir diğer yetkisi ise kişisel verilerin sınır ötesine iletilmesi halinde iletilecek üçüncü ülkenin veri koruma düzeyinin yeterli olup olmadığına ilişkin görüş beyan etmektir. GDPR bağlamında ise Veri Koruma Kuruluna esas olarak tutarlılığı sağlayarak merkezi bir rol yüklenmiştir. Ancak Kolluk ve Ceza Adaleti Direktifi uyarınca Kurula böyle bir misyon yüklenmemiştir³⁵³.

³⁵⁰ Kolluk ve Ceza Adaleti Direktifi m. 49/1.

³⁵¹ Başalp, **Kişisel Verilerin Korunması ve Saklanması**, s. 81.

³⁵² Dülger, **Kişisel Verilerin Korunması Hukuku**, s. 29.

³⁵³ Marquenie, **a.g.e.**, s. 336; De Hert, Papakonstantinou, **a.g.e.**, s. 14.

ÜÇÜNCÜ BÖLÜM

KOLLUK VE CEZA ADALETİ DİREKTİFİ'NİN UYGULAMA ALANINDA KİŞİSEL VERİ ELDE ETME YÖNTEMLERİ

I. ÖNLEYİCİ KOLLUK FAALİYETLERİ

A. Kimlik Sorma ve Kimlik Tespiti

Kimlik sorma, yalnız kanunda belirtilen durumlarda başvurulabilen bir kişisel veri toplama yöntemidir¹. Alman hukukunda kontrol noktası olarak düzenlenmiş kamuya açık alanlarda, kimlik tespiti yapılmakta ve kişilerin eşyaları aranmaktadır². Örneğin; Baden Württemberg Polis Kanunu m. 26/1-4 uyarınca polis, failleri ele geçirmek üzere kontrol noktaları oluşturabilmektedir³. Türk hukukunda polisin kontrol noktaları kurma yetkisi bulunmasa da şüpheli olsun olmasın herkese yönelik bir uygulama olduğundan bu, kimlik sormaya benzeyen bir düzenlemedir.

PVSK m. 9 uyarınca önleme aramasına karar verilmiş ve fiilen kontrol noktaları oluşturulmuşsa bu noktalarda kişi veya araçları durdurmak için PVSK m. 4/A uyarınca durdurma nedeni bulunmalıdır⁴. Kimlik sorulan kişinin kimliğini ibraz edememesi, açıklamada bulunmaktan kaçınması veya gerçeğe aykırı beyanda bulunması halinde kişinin kimliğini tespit için kişi polis tarafından tutulur, savcı durumdan haberdar edilir ve kişi kimliği anlaşıncaya kadar gözaltına alınır⁵. Nüfusa

¹ Feridun Yenisey, **Kolluk Hukuku**, 2. Baskı, İstanbul, Beta Yayıncılık, 2015, s. 77; Zeynep Bayram, “Kolluğun Suç Öncesi ve Sonrası Kişisel Veri Toplama Yetkisi”, **Bahçeşehir Üniversitesi Sosyal Bilimler Enstitüsü**, Yayınlanmamış Yüksek Lisans Tezi, İstanbul, 2009, s. 26.

² StPO m. 111; Bu tedbire StPO 129a maddesinde sayılan terör örgütü kurma ve diğer suçlar işlendiğine dair somut vakalara dayalı şüphe olması halinde başvurulmaktadır. Bkz. Yener Ünver, “Federal Almanya’da Terör ve Organize Suçluluk ile İlgili Düzenlemeler”, **Nurullah Kunter’e Armağan**, İstanbul, Beta Yayıncılık, 1998, s. 406-407.

³ Yenisey, **Kolluk Hukuku**, s. 231. StPO m. 111’de de ceza muhakemesi uyarınca kontrol noktaları oluşturulması mümkündür. Ancak ceza muhakemesi çerçevesinde sıkı şekil şartları mevcut olup özellikle terör suçları bakımından uygulanmaktadır. Polis Kanunu’ndaki düzenleme ise suçların işlenmesini önlemeye yöneliktir

⁴ Yenisey, **Kolluk Hukuku**, s. 294.

⁵ PVSK m. 4/A-9.

kayıtlı olmadığı için kimliği tespit edilemeyen kişinin fotoğrafı çekilir ve parmak izi alınarak bunlar kaydedilir⁶.

Öncelikle kimlik sorma ve kimlik tespiti arasındaki ayrıma değinilmelidir. Kimlik tespiti; parmak izinin alınması ya da fotoğraf çekilmesi biçiminde kişinin polis kayıtlarına geçirilmesi⁷ iken kimlik sorma, kayıtlara geçen bir işlem değildir. Kimlik sorulan kişi kimliğini ispata elverişli bir belge göstermekle yükümlüdür⁸. Kimlik tespiti PYSK m. 5, CMK m. 81, 147 ve CGİK m. 21/3'te düzenlenmiştir. Önleyici bir kolluk tedbiri olarak PYSK m. 4 ve 5 uyarınca gerçekleştirilen bu kişisel veri işleme yöntemine ancak polis başvurabilmektedir. Ancak özel güvenlik görevlilerinin de belirli durumlarda kimlik sorma yetkisi vardır. Özel güvenlik; toplantı, konser, spor müsabakası, sahne gösterileri ve benzeri etkinlikler ile cenaze ve düğün törenlerinde ve hava meydanı, liman, gar, istasyon ve terminal gibi toplu ulaşım tesislerinde⁹ kimlik sorabilir.

PYSK uyarınca kolluğa, halk arasında “sanal devriye” olarak bilinen sanal ortamda araştırma yetkisi verilmiş ve sanal ortamda işlenen suçlarda internet abonelerinin kimlik bilgilerine ulaşması mümkün olmuştur. Kolluk bu yetkisini erişim, yer ve hizmet sağlayıcılara kimlik bilgisi talep ederek kullanmaktadır¹⁰. Bu hükmün amacı, sanal ortamda işlenen suçta yetkili Cumhuriyet başsavcılığını tespit etmektir. Ancak savcılığın yetki alanını tespit etmeye ilişkin kurallar hâlihazırda CMK'de bulunmaktadır ve kolluğa sanal ortamda araştırma kimlik tespiti yapma yetkisi veren kural, zorunlu bir toplumsal ihtiyaca karşılık gelmemektedir. İşte bu nedenle AYM, kolluğun sanal ortamda kimlik tespiti yapmasına ilişkin maddeyi iptal etmiştir¹¹.

Bekçilerin kimlik sorma yetkilerinin var olup olmadığı ise son dönemde bir hayli tartışılmıştır. Çarşı ve Mahalle Bekçilerinin Vazifeleri ile İlgili Olarak Riayet Etmeleri Gereken Hususları Gösterir Yönetmelik¹² m. 16/1'de bekçilerin mntıkaları

⁶ PYSK m. 4/A-11.

⁷ Yenisey, **Kolluk Hukuku**, s. 254.

⁸ Yenisey, **Kolluk Hukuku**, s. 249.

⁹ 5188 sayılı Kanun m. 7/1-b ve m. 7/1-f.

¹⁰ PYSK ek m. 6/18.

¹¹ AYM, E. 2018/91, K. 2020/10, 19.02.2020, para. 101 Çevrimiçi <https://www.anayasa.gov.tr/tr/kararlar-bilgi-bankasi/> 29.05.2020.

¹² R.G. Sayısı: 12422, R.G. Tarihi: 10.10.1966.

dâhilindeki şüpheli kişileri takip etme ve hüviyetlerini araştırma yetkisi bulunmaktadır. Ancak bu yetki, yalnız araştırmaktan ibaret olup kanaatimizce bizzat kişiye başvurarak kimliğini sormaya izin veren bir yetki değildir. İzmir 35. Asliye Ceza Mahkemesi de bekçilerin kimlik sorma yetkilerinin bulunmadığı kararını vermiş, ancak Emniyet Genel Müdürlüğü Yönetmelik hükmüne dayanarak bekçilerin kimlik sorma yetkilerinin bulunduğu dair bir basın açıklaması yapmıştır¹³. Yönetmelik hükmünün bekçiye kimlik sorma yetkisi verdiği kabul edilse dahi idare, kanuna dayanmayan bir yetkiyi kullanamayacağından ve mülga 772 sayılı Kanun’da da bekçilere kimlik sorma yetkisi verilmediğinden bekçilerin kimlik sorma yetkisi bulunmamaktadır.

Kimlik sorma yetkisini AY m. 13’e uygun olarak bir kanunla düzenlemek için Çarşı ve Mahalle Bekçileri Kanun Teklifi¹⁴ hazırlanmıştır ve bu teklif kanunlaşmıştır. 7245 sayılı Kanun’un 7. maddesi, çarşı ve mahalle bekçilerin suç ve kabahat faillerinin kimliklerini tespit etmek ile yetkilendirilmesini öngörmektedir. Ancak maddede bekçilerin kimlik tespitini yapacakları bir veri kayıt sistemi olup olmadığı, varsa verilerin bu sistemde tutulma süresi, sisteme erişme yetkisi olan kişiler veya sistemde görülebilecek kişisel veri kategorileri gibi hususlarda herhangi bir düzenlemeye yer verilmemiştir. Bu nedenle hüküm, hukuka uygun bir veri işlemenin gereklerini sağlamamaktadır.

Kolluk görevlileri haricinde 1774 sayılı Kimlik Bildirme Kanunu kapsamında da kimlik tespit etme yetkisi verilmiştir. Kimlik tespitinin muhatabı Kanun’da sayılan özel ya da resmi konaklama, dinlenme, bakım ve tedavi yerleri işletmelerinde geçici ya da sürekli olarak kalan, oturan, çalışan veya araç kiralayan kişilerdir. Bu tesislerin sorumlu işletmecileri; gelen kişilerin kimlik ve geliş- ayrılış kayıtlarını günü gününe tutmak ve genel kolluk makamlarının incelemesine hazır bulundurmakla yükümlüdür. Kayıtlar bilgisayarda güncel olarak tutulacak, genel kolluk makamlarının bilgisayar

¹³ Çevrimiçi <https://www.egm.gov.tr/carsi-ve-mahalle-bekcilerinin-kimlik-sorma-yetkisi-hakinda-basin-aciklamasi> 16.03.2020.

¹⁴ Çevrimiçi <https://www2.tbmm.gov.tr/d27/2/2-2555.pdf> 16.03.2020; Teklifin detaylı analiz ve eleştirisi için bkz. R. Barış Erman, Onur Özcan, Erdi Yetkin, Eşref Barış Börekçi, Saba Ş.T. Üzeltürk, **“Çarşı ve Mahalle Bekçileri Kanunu Teklifi” Hakkında Tespit, Düşünce ve Eleştiriler**, İstanbul, Yeditepe Üniversitesi Yayınevi, 2020.

terminallerine bağlanarak bu tesislerde kalacak kişilerin kişisel verileri işlenecek ve genel kolluk makamlarına anlık olarak bildirilecektir¹⁵.

Kanun'da araç kiralayanlar bakımından da kimlik tespiti nin öngörülmesi, araç kiralama şirketlerinin ticari işlemlerinin kolluk tarafından takibine imkân sağlamaktadır. Her ne kadar çalıntı araçların takibinde kolaylık sağlasa da bunun ticari sırrın korunması ve kişisel verilerin korunması bakımından sakıncalı olduğu doktrinde ifade edilmiştir¹⁶. Ancak kanaatimizce bu verilere yalnız kolluk ulaşabileceğinden ticari sırrın ifşası sakıncası bulunmamaktadır.

Kimlik Bildirme Kanunu gereği bilgisayar terminali aracılığıyla kolluk makamlarına iletilen bu kişisel veriler, şüphesiz Kolluk ve Ceza Adaleti Direktifi'nin korumasından yararlanacaktır. Ayrıca Kanun, bu verilerin talep halinde TÜİK'e verilmesi gerektiğini de düzenlemiştir¹⁷. Bu halde ise TÜİK'in faaliyeti suçların önlenmesi, ceza muhakemesi yahut cezaların infazına ilişkin olmadığından işlenen kişisel veriler GDPR'ın korumasından yararlanacaktır.

B. Parmak İzi ve Fotoğrafların Kaydı

1. Biyometrik Veri İşleme

a. Tanım

Kişiy e PIN kodu sorularak ya da sahip olduğu manyetik kart gibi bir araçtan yararlanılarak kimlik tespiti gerçekleştirilmektedir. Ancak yanlış payının düşürülmesi ve hızlı doğrulamanın yapılması için bu yöntemler haricinde biyometrik yöntemler tercih edilmektedir¹⁸. Biyometrik; biyolojik (anatomik ve fizyolojik) veya davranışsal¹⁹ olarak otomatikleştirilmiş tanıma için kullanılan ölçülebilir bir özellik ve

¹⁵ Bkz. Ek m. 1/2. Özel ve resmi konaklama tesisleri için bu düzenleme 31.10.2016 tarih ve 678 sayılı KHK m. 4 hükmünün 01.02.2018 tarih ve 7071 sayılı Kanun m. 3 ile aynen kabul edilerek kanunlaşmıştır.

¹⁶ Yenisey, **Kolluk Hukuku**, s. 256.

¹⁷ Bkz. 1774 sayılı Kanun m. 2.

¹⁸ Cüneyd Er, **Biyometrik Yöntemler ve Özel Yaşamın Gizliliği Hakkı**, Ankara, Yetkin Yayıncılık, 2007, s. 21 vd.

¹⁹ Davranışsal biyometri, yeterli akıllı cihazlar vasıtasıyla davranış modellerini ölçer. Bireyin araba sürüşü veya yürüme şekli, dudak okuma, oyun stratejisi, biyometrik çizim, akıllı cihaz kullanma,

otomatikleştirilmiş yöntemlerden yararlanarak kişinin tanınması süreci manasına gelmektedir²⁰. Biyometrik sistemlerde genellik, çeşitlilik, süreklilik, toplanabilme, kabul edilebilirlik, sızma, uzayabilirlik özelliklerine sahip veriler, kişinin kimliğini tanıma ve doğrulama fonksiyonuna sahiptir²¹. Tanıma, bireyin bilinen bir nicel özelliğine dayanarak tanınması iken doğrulama ise elde edilmek istenen bir teşhisin onaylanması ya da reddedilmesidir²².

Biyometrik veriler, fiziksel karakteristik olarak parmak izi, retinal örnek, yüz yapısı, ses²³, damar örneği veya davranışsal karakteristik olarak el yazılı imza, spesifik bir konuşma aksanı, yürüyüş gibi her türlü kişisel veridir²⁴. Özellikle parmak izi tanıma teknolojisi olarak optik, silikon, ısı ve ses ötesi teknolojilerden yararlanılmaktadır²⁵.

Biyometrik unsurların ancak belirli (*identified*) ya da belirlenebilir (*identifiable*) bir gerçek kişiye izafe edilebilmesi halinde, bu unsurlar kişisel veridir.

bilgisayar donanımıyla etkileşiminin ölçümü davranışsal biyometrilere aittir. Davranışsal biyometri teknolojileri günümüzde finans, suç profili oluşturma, siber suç soruşturması, sahtekârlık / tehdit tespiti, e-ticaret, metin yazarlığı gibi uygulamalarda güvenliği artırmak için mevcut fiziksel biyometriye ek olarak kullanılmaktadır. Bkz. Cengiz Paşaoğlu, Kayode Hadilou Adje, Orkun Demirtaş, “A Review On Privacy Preserving Biometric Authentication Methods”, **Kişisel Verileri Koruma Dergisi**, c. 1, s. 1, 2019, s. 36-37.

²⁰ Paşaoğlu, Adje, Demirtaş, **a.g.e.**, s. 35-36; Darin R. Walker, “Biometric Technology in Law Enforcement”, **Neurosurgery**, c. 71, s. 2, Ağustos 2012, s. 197.

²¹ Paşaoğlu, Adje, Demirtaş, **a.g.e.**, s. 35.

²² Leyla Keser Berber, Murat Lostar, **Bilişimde Biyometrik Yöntemler**, Ankara, Yetkin Yayınları, 2006, s. 21; Doğrulama bir tarayıcının veri sahibine ait verisinin, daha evvel işlenmiş biyometrik verilerle karşılaştırılması esası hâkimdir. Doğrulamanın tanımadan farkında ise sistemin kullandığı veri tabanında her bir biyometrik veri ve kimlik verisi, kayıtlı bulunan bir kimlik verisine karşılık gelmektedir. Bkz. Er, **a.g.e.**, s. 26-27.

²³ Ses biyometrisi, bir mikrofon ve kayıt cihazı gereken tek şey olduğundan, toplanması en ucuz yöntemlerden biridir. Örneğin bir telefonla uzaktan elde edilebilmektedir. Bununla birlikte, bir kişinin sesini duyduğu gibi mikrofonun konumu, kayıt cihazlarındaki fark, soğuk algınlığı, hastalık, ruh hali ve hatta yaş gibi birçok zorluk nedeniyle kişinin tanımlanmasında zorluklar yaşanmaktadır. Ancak yine de ses uygulanabilir bir biyometrik olma potansiyeline sahiptir. Bkz. Walker, **a.g.e.**, s. 198-199; AİHM, ses kaydı yapılarak bu kaydın bir analiz sürecinin sonunda kişiyi tanımladığını ve bu nedenle AİHS m. 8’in korumasının gündeme geldiğini belirtmiştir. Bkz. *PG ve JH v. Birleşik Krallık*, B. No: 44787, 25.09.2001, para. 59 Çevrimiçi <https://hudoc.echr.coe.int/> 29.03.2020.

²⁴ Murat Volkan Dülger, **Kişisel Verilerin Korunması Hukuku**, 2. Baskı, İstanbul, Hukuk Akademisi, 2019, s. 5; Catherine Jasserand-Breeman, “Reprocessing of Biometric Data for Law Enforcement Purposes: Individuals’ Safeguards Caught at the Interface between the GDPR and the Police Directive?”, **University of Groningen**, Yayınlanmamış Doktora Tezi, Groningen, 2019, s. 50; Keser Berber ve Lostar’a göre ise parmak izi, avuç içi, yüz, iris, retina tanıma vücut özelliğine dayanan biyometrik tanıma yöntemleri iken, konuşma tanıması ise büyük ölçüde davranış özelliklerine dayanan biyometrik tanıma yöntemidir. Davranış modeline dayanan yöntemlerin kopyalanması mümkün olduğundan bu yöntemler, manipülasyona açıktır. Vücut özelliklerine dayanan yöntemler ise güçlü kimlik doğrulaması için daha uygundur. Detaylı bilgi için bkz. Keser Berber, Lostar, **a.g.e.**, s. 33 vd.

²⁵ Er, **a.g.e.**, s. 39 vd.

Söz gelimi, kişinin gözünün, yürüyüşünün görüldüğü herhangi bir fotoğraf peşinen biyometrik veri olamaz, zira GDPR resitalinde de belirtildiği gibi bu görüntünün, kişinin benzersiz şekilde tanınmasına olanak sağlayan bir yöntemle işlenmiş olması gerekmektedir²⁶. Biyometrik olarak bu belirlenebilirlik, tanınabilirlik ise biyometrik özelliklerin numune (*sample*) ya da şablona (*template*) dönüştürülmesi ile mümkündür²⁷. Biyometrik numune, daha önce işlenen ve farklı veri tabanlarında tutulan biyometrik şablonlarla karşılaştırılarak bireyin kimliği tespit edilmektedir. Bu bir *one-to-many* eşleşmesi olup bireyin medeni ya da diğer hukuki kimliğinin oluşturulmasını gerektirmemekte, yalnızca bir örnek ve önceden kaydedilmiş bir şablonun aynı kişiden kaynaklandığını tespit etmektedir²⁸. Parmak izi görüntüsü, yüz imgesi gibi numuneler ve bu numunelerde yer alan bilgiler bir algoritma ile çıkarılır, indirgenir, etiketlere veya sayılara dönüştürülür ve böylece kişisel veri elde edilir²⁹. Yani her halükârda biyometrik özellik bir teknik işleme sürecinden geçerek kişisel veri haline gelmektedir³⁰. GDPR bağlamında kimlik doğrulamada (*authentication*) ise benzersiz şekilde kimlik tespitinin (*unique identification*) zıddı yani *one-to-one* eşleşme söz konusudur. Bireyin biyometrik numunesi, yalnızca akıllı kart, kimlik kartı, pasaport veya tek bir veri tabanı gibi bir cihazda bulunan biyometrik bilgilerle karşılaştırılmaktadır³¹.

Özellikle parmak izi gibi eşsiz (*unique*) olan biyometrik veriler ceza muhakemesinde çok büyük fayda sağladığından yoğun biçimde kullanılmaktadır.

²⁶ Dülger, **Kişisel Verilerin Korunması Hukuku**, s. 112.

²⁷ Jasserand-Breeman, **a.g.e.**, s. 62; Olay yerinde bulunan bir parmak izinin emare niteliğinde olup kişisel veri olmadığı ve bu nedenle toplanıp otomatik sorgulama yapan bir bilişim sistemine kaydının hukuka aykırı olmadığına dair bkz. Hasan Semiz, “Uluslararası Terör Suçları Bakımından Terör Suçlarında Kolluk Yetkileri”, **Harp Akademisi Komutanlığı Stratejik Araştırmalar Enstitüsü**, Yayımlanmamış Yüksek Lisans Tezi, İstanbul, 2007, s. 100.

²⁸ Jasserand-Breeman, **a.g.e.**, s. 69.

²⁹ Dülger, **Kişisel Verilerin Korunması Hukuku**, s. 90; Jasserand-Breeman, **a.g.e.**, s. 66;

³⁰ Ancak buna rağmen, WP29 da dâhil bazı yazarlar, parmak izi, parmak ucu, iris, ses gibi biyometrik numuneleri tanımlamak için ham (*raw*) biyometrik veri ifadesini yanlış kullanmaktadır. Ham verilerin elde edildiği teknik işlemlerin olmaması durumunda, bunlar biyometrik verilerin kapsamı dışında kalmaktadır. Oysa ham veri terimi sadece biyometrik özelliklerin eş anlamlısı olarak kullanılmalıdır. Bkz. Jasserand-Breeman, **a.g.e.**, s. 67.

³¹ Jasserand-Breeman, **a.g.e.**, s. 69; GDPR resital m. 51 “Fotoğrafların işlenmesi sistematik olarak özel nitelikli kişisel verilerin işlenmesi olarak değerlendirilmemelidir. Fotoğraflar, ancak bir gerçek kişinin benzersiz bir şekilde tanımlanmasına veya doğrulanmasına izin veren belirli bir teknik yöntemle işlendiğinde özel nitelikli kişisel veriden söz edilebilir.” Öte yandan GDPR m. 4/14’teki biyometrik veri tanımında; özel teknik işleme ile benzersiz biçimde kişinin tanımlanması şartı aranmıştır. GDPR’ın resital ve ilgili madde metni arasında çelişkinin bulunduğu dair bkz. Jasserand-Breeman, **a.g.e.**, s. 72.

Biyometrik verilerin kolluk faaliyetlerinde kullanılması için de çeşitli standartlar bulunmaktadır. ABD’de federal mahkemeler ve eyalet mahkemelerinin çoğunluğu *Daubert Standardı*’nı kullanmaktadır. Buna göre söz konusu bilimsel sürecin veya metodolojinin geçerliliğinin belirlenmesinde dikkate alınması gereken beş faktör bulunmaktadır: Teori veya tekniğin test edilip edilemeyeceği ve test edilip edilmediği, inceleme ve yayınlanmaya tabi olup olmadığı, bilinen veya potansiyel hata oranı, çalışmasını kontrol eden standartların varlığı ve korunması, ilgili bir bilimsel topluluk içindeki kabul düzeyi³².

Suçun önlenmesi ve kamu güvenliğinin sağlanması amacıyla da biyometrik verilerden yararlanılmaktadır. ABD’de 11 Eylül terör saldırılarından sonra ülkeye giriş ve çıkışlarda parmak iziyle denetim yapma usulü buna örnek olarak gösterilebilir³³. Sadece ABD’de değil, 2001 yılında Hollanda’da da belgede sahteciliğe karşı güvenli bir yapı olacağı düşüncesi ile yeni nesil seyahat belgeleri yürürlüğe girmiştir³⁴. Uluslararası Sivil Havacılık Örgütü de seyahat belgelerine eklenecek yüz tanıma yöntemlerinin arasına biyometrik tanımayı eklemiştir³⁵. Nitekim AB düzeyinde de 13 Aralık 2004 tarihli 2252/2004 sayılı Tüzük³⁶ ile pasaport ve seyahat belgelerinde güvenlik amacıyla biyometrik standartlar belirlenmiştir. Özellikle terör ve sınır ötesi suçlarla mücadelede sınır ötesi işbirliğinin artırılmasına ilişkin 2008/615/JHA ve 2008/616/JHA Konsey Kararı’na atıfta bulunan Prüm Kararları da DNA profilleri, parmak izleri ve araç kayıt verileri gibi kişisel verilerin sınır ötesi dolaşımını ve işbirliğini düzenlemiştir. Kararlara göre, DNA ve parmak izinin aktarımı bir *hit/no-hit* yaklaşımına dayanarak gerçekleşir; bu, AB üyesi bir devlette suç mahallinde bulunan DNA profillerinin veya parmak izlerinin diğer üye devletin veri tabanında bulunan profillerle otomatik olarak karşılaştırılabilmesine olanak sağlamıştır³⁷.

³² Daha az kabul gören bir diğer standart ise *Frye Standardı* olup ABD’de daha az eyalet tarafından uygulanmaktadır. Bu standart ise kullanılan metodolojinin veya sürecin ait olduğu alanda genel kabul görecektir kadar kurulmasını gerektirmektedir. Bkz. Walker, **a.g.e.**, s. 199.

³³ Keser Berber, Lostar, **a.g.e.**, s. 103.

³⁴ Keser Berber, Lostar, **a.g.e.**, s. 110.

³⁵ Keser Berber, Lostar, **a.g.e.**, s. 110.

³⁶ Tüzük metni için bkz. Çevrimiçi <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02004R2252-20090626&from=EN> 17.02.2020.

³⁷ Terör ve Sınır Ötesi Suçlarla Mücadelede Sınır Ötesi İşbirliğinin Arttırılmasına Dair 2008/615/JHA Konsey Kararı Çevrimiçi, https://ec.europa.eu/home-affairs/e-library/glossary/pr%C3%BCm-decisions_en 21.08.2019.

Kamu tüzel kişisi olmayan kurum ve kuruluşlar da biyometrik yöntemleri kullanmaktadır. Bu kişilerin, devlet politikası biçiminde biyometrik takip uygulaması kullandıklarını ilan etmesi gerekmediğinden kullanım istatistiki tespit edilemese de kamudan daha yaygın olarak biyometrik veriler özel sektörde kullanılmaktadır³⁸. Mesai takibi³⁹ ya da spor salonlarına giriş ve çıkışlarda kontrol amacıyla⁴⁰ parmak izi alınması, yüz taraması, retina taraması gibi yöntemlerle biyometrik veriler işlenmektedir. Ancak şüphesiz bu yöntemlere başvurulurken ölçülülük ilkesi gözetilmelidir.

108 sayılı Sözleşme ve 95/46 sayılı Direktif'te biyometrik verilere ilişkin bir düzenleme bulunmamaktadır⁴¹. 2252/2004 sayılı Pasaport Tüzüğü ve EURODAC, VIS, SIS gibi geniş çaplı biyometrik veri tabanlarının kuruluşuna ilişkin düzenlemelerin ihdası üzerine AB düzeyinde biyometrik verilerin işlenmesinin hukuki bir dayanağa bağlanması ihtiyacı belirlemiştir⁴². Zira biyometrik veri, kişinin söz gelimi parmak izi çizgisinden diyabet gibi hastalık riski taşıyıp taşımadığını tespiti elverişli olduğu için bir yandan kişinin sağlıkla ilgili verisi olup öte yandan ırkı ya da etnik kökeninin tespitine olanak sağlayan özel nitelikli veridir.

95/46 sayılı Direktif döneminde biyometrik veri, özel nitelikli veri olarak kabul edilmemişse de bu verinin özel işleme şartlarına tabi olduğu ileri sürülmüştür. Nitekim GDPR'da da biyometrik verinin başlı başına biyometrik veri olduğu için özel nitelikli

³⁸ Er, a.g.e., s. 76.

³⁹ Toptancı halinde çalışan personelin yüz tarama sistemi ile mesai takibi yapılması işleminin hukuka aykırı olduğuna dair bkz. Danıştay 11. Daire, E. 2017/816, K. 2017/4906, 13.06.2017; Konya Eğitim ve Araştırma Hastanesi'nde personelin mesai takibinin kart okutma ile yapılmasından verim alınmayınca imza ve parmak izi taraması ile yapılmasının özel yaşamın gizliliğinin ihlali nedeniyle hukuka aykırı olduğuna dair bkz. Danıştay İdari Dava Daireleri Genel Kurulu, E. 2014/2242, K. 2015/4991, 09.12.2015. Biyometrik verilerin bu gerekçelerle işlenmesi, veri işlemede ölçülülük ilkesine aykırıdır. Mesai takibinin bu yöntemle yapılmasının "biyometrik devlet"e dönüşmeye yol açacağına dair bkz. Aydın Akgül, "Kişisel Verilerin Korunması Bağlamında Biyometrik Yöntemlerin Kullanımı ve Danıştay Yaklaşımı", **TBB Dergisi**, c. 28, s. 118, 2015, s. 211-212.

⁴⁰ Spor salonu hizmetinden faydalanmak için bu yöntemlerle biyometrik verinin işlenmesine rıza gösterme zorunluluğu ölçülülük ilkesi ile bağdaşmamaktadır. Bu işleme son verilmesi için Kişisel Verileri Koruma Kurulunun 25.03.2019 tarihli ve 2019/81 sayılı Karar ve 31/05/2019 tarihli ve 2019/165 sayılı Kararı mevcuttur. Bkz. Çevrimiçi <https://www.kvkk.gov.tr/Icerik/5496/2019-81-165> 28.02.2020.

⁴¹ 108+ Sözleşmesi ile biyometrik veriler özel işleme şartlarına tabi tutulmuştur. Bkz. "108 Sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulmasında Bireylerin Korunmasına Dair Avrupa Konseyi Sözleşmesi (1981) ve 181 Sayılı Ek Protokol" başlıklı bölüm.

⁴² Jasserand-Breeman, a.g.e., s. 59.

veri olduğu ve özel nitelikli verilerin işleme şartlarına tabi olduğu açıkça hükme bağlanmıştır⁴³. Kolluk ve Ceza Adaleti Direktifi de GDPR ile uyumlu olarak biyometrik verileri; *gerçek kişinin kimliğini şüpheye yer bırakmayacak biçimde belirleme veya doğrulamaya imkân veren fiziksel, fizyolojik veya davranışsal özelliklerinin teknik yolla işlenmesi ile elde edilen veriler* olarak tanımlamıştır. Yüz görüntüsü ve daktiloskopik veri biyometrik verilere örnektir ve biyometrik veriler özel işleme şartlarına tabi tutulmuştur⁴⁴.

b. Yüz Tanıma Teknolojisi

Yüz tanıma teknolojisi (*facial recognition technology*)⁴⁵ ile hedeflenen; yüz görüntüsünden bir şablon (*template*) yaratarak bu şablonu, sürücü belgesi, resmi kayıtlar, adli sicil kayıtları, sosyal medya hesapları gibi pek çok yerden toplanan fotoğraflardan oluşan veri tabanında mevcut olan yüz görüntüleri ile karşılaştırmak ve eşleştirmektir (*match*). Yüz tanıma teknolojisi olarak tek çekim, video çekimi, üç boyutlu görüntü, kızılötesi tarama ve ısı yolu yöntemlerinden yararlanılmaktadır⁴⁶.

Yüz tanıma teknolojisi, bir kimsenin kimliğini tespit etmek veya doğrulamak için insan yüzlerinin analizi ile şablon yaratan yazılım uygulamalarını kullanmaktadır. Suçun önlenmesi ve ceza muhakemesi sürecinde güvenlik kamera kayıtlarında tespit edilen kaçak şüpheli ya da sanıkların kimliklerinin tespitinde böyle bir yazılımdan yararlanılması mümkündür⁴⁷.

⁴³ Jasserand-Breeman, **a.g.e.**, s. 74.

⁴⁴ Kolluk ve Ceza Adaleti Direktifi m. 10/1.

⁴⁵ Yüz tanıma teknolojileri ile yüzdeki belirli noktalar ölçülerek benzersiz bir koda sahip şablona dönüştürülmektedir. Benzersiz yüz dokusunu kullanarak 3-D yüz tanıma ve biyometrik yeni teknolojik uygulamalarla birlikte tanıma derecesi artmaktadır. Bkz. Kristin Hamann, Rachel Smith, “Facial Recognition Technology: Where Will It Take Us?”, **American Bar Association**, Çevrimiçi https://www.americanbar.org/groups/criminal_justice/publications/criminal-justice-magazine/2019/spring/facial-recognition-technology/ 30.09.2019, s. 2.

⁴⁶ Er, **a.g.e.**, s. 47 vd.

⁴⁷ Hamann, Smith, **a.g.e.**, s.1; Yüz tanıma teknolojisi Interpol tarafından da kullanılmaktadır. Probe resim sisteme girildiğinde otomatik olarak profil eşleşmesi yapılır ve aday resimler gösterilir. Bunun üzerine Interpol yüz tanıma uzmanları “potansiyel aday”, “aday yok” ve “yetersiz” biçiminde sonuç elde etmektedirler. Bu sonuç sonrasında Interpol bünyesindeki sisteme resim sağlayan ve profil veya eşleşme ile ilgilenebilecek devletlere aktarılmaktadır. Bkz. Interpol, Çevrimiçi <https://www.interpol.int/How-we-work/Forensics/Facial-Recognition> 30.09.2019, s. 2.

Ancak yüz tanıma sistemleri, DNA ve parmak izinin analizinin aksine yaşlanma, plastik cerrahi, kozmetik, fotoğraf kalitesi, uyuşturucu kullanımı, veri sahibinin duruşu gibi değişik faktörlerden etkilenebilmektedir⁴⁸. Ayrıca ABD Teknoloji ve Standartlar Ulusal Enstitüsü (*National Institute of Standards and Technology*) yüz tanıma algoritmalarının kesinliği bakımından yüzden fazla tanıma algoritması üzerinde yaptıkları bir incelemede, çocukların resim eşleşmelerinde hata oranının yüksek olduğunu tespit etmiştir⁴⁹. Zira çocuklar ve ergenlerin kemik elastikiyetleri ve şifitleri daha keskin biçimde değişmektedir⁵⁰. Kanaatimizce yüz tanıma sisteminde verisi işlenen kişilerin çocuk ve ergen olması halinde bu kişilerin görüntüleri kısa sürede değişebileceğinden görüntülerin uzun süreler muhafaza edilmesi gerekmemektedir ve bu görüntüler daha kısa saklama süresine tabi olmalıdır.

2. Türk Hukukunda Durum

Genel sağlık sigortalılarının biyometrik verilerinin işlenebileceğine ilişkin 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu m. 67/3'te bir hüküm bulunmaktadır⁵¹. Bu hüküm dolaylı olarak suçların önlenmesi amacına hizmet

⁴⁸ Interpol, **a.g.e.**, s. 1; New York'ta bir CVS Eczanesinde bira çalan bir kişinin görüntüsü güvenlik kamerasına kaydedilmiştir. New York Polis Departmanı, kişinin görüntüsünü yüz tanıma sistemine yüklemiştir. Ancak sistemde kayıtlı bir yüzle eşleşme yapılamamıştır. Ancak yüz tanıma bölümündeki memur (*Facial Identification Section-FIS*), şüpheliyi ünlü bir oyuncu Woody Harrelson'a benzetip oyuncunun Google resimlerden yüksek kaliteli bir fotoğrafını sisteme yükler ve görüntü, Harrelson'a benzeyen bir kişi ile eşleşir. Bunun üzerine bu kişi, basit hırsızlık suçu isnadı ile tutuklanır. Örnekten anlaşılacağı gibi probe resim olarak, gözetim sisteminden alınmış düşük çözünürlüklü bir fotoğraf, sosyal medyadan alınmış bir fotoğraf, filtreli bir fotoğraf ve hatta şüphelinin ünlü Doppelgänger'i dahi kullanılabilir. Yani probe resim için bir sınır olmayıp bu da veri tabanında kayıtlı olan bir kişinin, kişisel verilerin korunması hakkının ihlali riski bir kenara, haksız yere ceza muhakemesi koruma tedbirlerine maruz kalmasına da yol açabilmektedir. Bkz. Clare Garvie, "Garbage In, Garbage Out. Face Recognition on Flawed Data", Çevrimiçi <https://www.flawedfacedata.com/> 30.09.2019, s. 1-2.

⁴⁹ M.I.T. Medya Laboratuvarı'nda son yapılan araştırmalara göre kadın ve çocuk olmak gibi renk de daha yüksek yanlış eşleşme riskine sebep olabilmektedir. Çocuk ceza adalet sisteminde ise ırka dayalı eşitsizlikler daha da belirginleşmektedir. 2017 yılında ceza yargılamasında bulunan New York'taki siyahi ve Latin gençler çok daha yüksek orandadır. Hatta siyahi gençlerin oranı sayıca on beş kat daha fazladır. Bkz. Joseph Goldstein, Ali Watkins, "She Was Arrested at 14 Then Her Photo Went to a Facial Recognition Database", Çevrimiçi <https://www.nytimes.com/2019/08/01/nyregion/nypd-facial-recognition-children-teenagers.html> 30.09.19, s. 3.

⁵⁰ Goldstein, Watkins, **a.g.e.**, s. 2.

⁵¹ "Ayrıca genel sağlık sigortalısı ve bakmakla yükümlü olduğu kişilerin sağlık hizmetlerinden ve diğer haklardan yararlanabilmeleri için sağlık hizmet sunucularına başvurduklarında acil haller hariç olmak üzere (acil hallerde ise acil halin sona ermesinden sonra); biyometrik yöntemlerle kimlik doğrulamasının yapılması ve/veya nüfus cüzdanı, sürücü belgesi, evlenme cüzdanı, pasaport veya Kurum tarafından verilen resimli sağlık kartı belgelerinden birinin gösterilmesi zorunludur."

etmektedir. Hükümde; işlenen verilerin tutulma süresi, işlemenin kapsamı ve verilerin korunmasına ilişkin usul ve esasların belirlenmemiş olması nedeniyle hükmün Anayasa'ya aykırı olduğu iddiasıyla Danıştay 15. Dairesi tarafından AYM'ye başvurulmuştur⁵². Ancak AYM, bu hükmün sosyal güvenlik ve sağlık sektöründe sahteciliğin önlenmesine ilişkin bir güvenlik tedbiri olduğu kanaatindedir⁵³. AYM çoğunluğu, bu yöntemle elde edilen verilerin sadece sağlık sektöründe kullanılacağına ilişkin bir ön kabulde değerlendirme yapmış, ancak amaçla bağlı veri işlemenin nasıl sağlanacağına dair Kanun'da düzenlemenin bulunmamasını değerlendirmemiştir⁵⁴. Karşı oy gerekçesinde isabetli olarak madde hükmünün; salt kimlik tespitinden ibaret olmayıp kişisel verilerin depolanacağı anlamına geldiği belirtilmiştir. Ancak işlenen bu verilerin ne süre ile saklanacağı, Sosyal Güvenlik Kurumunun bu verileri kimlerle paylaşacağı hususları da Kanun'da düzenlenmemiştir.

Bir diğer önleyici kolluk faaliyeti çerçevesinde biyometrik veri işleme ise PVSK'de düzenlenmiştir. PVSK m. 5 adli veya idari faaliyet ayrımı yapmaksızın hangi durumlarda kişinin parmak izinin alınabileceğini düzenlemiştir⁵⁵. Alınan parmak izi, kişinin kimliği, parmak izi alma işlemini yapan kişinin kimliği ve işlemin zamanı ile birlikte AFIS'ye⁵⁶ kaydedilmektedir. Parmak izinin alındığı sebebe ise

⁵² Danıştay 15. Daire, E. 2014/4562, 11.09.2014 Çevrimiçi <http://www.kazanci.com/kho2/ibb/giris.html> 30.03.2020..

⁵³ AYM, E. 2014/180, K. 2015/30, 19.03.2015 Çevrimiçi <https://www.anayasa.gov.tr/tr/kararlar-bilgi-bankasi/> 29.03.2020.

⁵⁴ AYM'nin bu kararının elektronik haberleşme ve trafik verilerinin işlenmesine ilişkin 5809 sayılı Kanun m. 51'i iptal eden AYM, E. 2013/122, K. 2014/74, 09.04.2014 kararı ile çeliştiği yönünde bkz. Akgül, "Kişisel Verilerin Korunması Bağlamında Biyometrik Yöntemlerin Kullanımı ve Danıştay Yaklaşımı", s. 209.

⁵⁵ PVSK m. 5/1 "Polis;

a) Gönüllü,

b) Her çeşit silah ruhsatı, sürücü belgesi, pasaport veya pasaport yerine geçen belge almak için başvuruda bulunan,

c) Başta polis olmak üzere, genel veya özel kolluk görevlisi ya da özel güvenlik görevlisi olarak istihdam edilen,

ç) Türk vatandaşlığına başvuruda bulunan,

d) Sığınma talebinde bulunan veya gerekli görülmesi halinde, ülkeye giriş yapan sair yabancı,

e) Gözaltına alınan, kişilerin parmak izini alır."

⁵⁶ Erdoğan Tetik, "Kimlik Tespitinde Parmak İzi Arşivlerinin Gerekliği ve Ülkemizdeki Durumun Değerlendirilmesi", **Polis Dergisi**, s.41, 2004, s. 37. Bu sistem dünyada genel olarak kullanılan Otomatik Parmak İzi Tanıma Sistemi'dir (Automated Fingerprint Identification System/ AFIS). Türkiye'de 1997'de Emniyet Genel Müdürlüğü bünyesinde tek parmak ve on parmak izleri tarama veya CCD kamera vasıtasıyla bilgisayar ortamına aktararak işlenmekte ve otomatik olarak eldeki verilerle karşılaştırma yapabilmektedir.

AFIS’de yer verilmez⁵⁷. AFIS’ye kayıta veri işleme sebebinin belirtilmemiş olmasının veri sahibinin lekelenmeme hakkına müdahale teşkil ettiği ileri sürülmüştür⁵⁸. Zira ağır suç işlemiş kişi de gönüllü olan kişi de aynı sisteme kaydedilmektedir. Bu da veri sahipleri arasında kategorizasyona gidilmesini öngören Kolluk ve Ceza Adaleti Direktifi’nin 6. maddesi ile bağdaşmamaktadır ve masumiyet karinesini zedelemektedir. Zira verilere kolluk ve adli makamlar ulaşabilmektedir. Örneğin kolluk kimlik tespiti veya olay yerinden alınan parmak izinin karşılaştırılması için doğrudan AFIS’ye bağlanabilmektedir⁵⁹. Böylece sisteme erişebilen makamlar sistemde verisi işlenen kişinin gözüaltına alınmış ya da hükümlü olduğunu düşünebilmekte ve muamelesi değişebilmektedir.

Maddeye göre parmak izi alınabilecek ilk grup veri sahipleri, gönüllülerdir. Kanun gerekçesine göre gönüllü olmaktan, kişinin baskı altında olmaksızın özgür biçimde ve aydınlatılmış rızasının bulunması gerektiği anlaşılmaktadır⁶⁰. Kanun koyucu, biyometrik veri elde etme yöntemi olan parmak izinin alınmasında gönüllülük esasını kabul etmişse de gönüllü olarak fotoğrafın kaydını kabul etmemiştir⁶¹. Mahiyeti itibariyle daha fazla korunması gereken özel nitelikli verinin işlenmesi için kanun koyucunun rızaya sonuç bağlaması Kolluk ve Ceza Adaleti Direktifi m. 1/3 uyarınca kabul edilebilirdir. Ancak bu halde de verinin işlenmesi için bir gerekçe ve amaç bulunmalıdır. Kişinin salt gönüllü olarak veri işlemeye rıza göstermesi, Kolluk ve Ceza Adaleti Direktifi bağlamında isabetsizdir, zira veri sorumlusu kolluktur ve bireyin kolluk karşısında rızasına sonuç bağlanmamalıdır. Kanaatimizce hem parmak izi hem fotoğraf bakımından da gönüllülük ya da rızaya sonuç bağlanmamalı ve veri işlenmemelidir.

Gönüllü kişinin parmak izi, suçun önlenmesi amacıyla alınmadığı takdirde⁶² artık Kolluk ve Ceza Adaleti Direktifi uygulama alanı bulmayıp GDPR hükümleri

⁵⁷ PVSK m. 5/2.

⁵⁸ Yenisey, **Kolluk Hukuku**, s. 260.

⁵⁹ PVSK m. 5/7.

⁶⁰ Çevrimiçi <https://www.tbmm.gov.tr/sirasayi/donem22/yil01/ss1437m.htm> 03.09.2019.

⁶¹ Bkz. PVSK m. 5/5.

⁶² Emniyet Genel Müdürlüğüne göre gönüllülük esasına dayalı olarak verilen parmak izi; kimlik tespiti, geçmiş durumların belgelendirilmesi, doğal afet durumlarında göçük altında kalan kişilerin kimliğinin tespiti, bu kişilerin ve hafıza kaybı yaşayan kişilerin ailelerine ulaştırılması ve durumdan haberdar edilmesine olanak sağlamaktadır. Bkz. Emniyet Genel Müdürlüğü, “Olay Yeri”, Çevrimiçi

gündeme gelecektir. GDPR veri sahibinin rızasına hukuki sonuç bağlamıştır, ancak buna göre veri sahibi rızasını her zaman geri alabilecektir ve hatta rızayı geri alma, rıza verme kadar da kolay olmalıdır. Söz konusu biyometrik veri, özel nitelikli veri olduğu için veri sahibinin açık rızası gerekmektedir. Açık rıza ise belirli bir konuya ilişkin olma, bilgilendirmeye dayanma ve özgür iradeye dayanma şartlarına tabidir⁶³. Ancak kanımızca PVSK’de gönüllü bir kişiden parmak izi alınmasına cevaz veren bu hüküm, GDPR’ın gereklerine de uygun değildir. Kamu gücü kullanan kolluk makamı karşısında, bireyin özgür iradeye dayanan bir rızasının bulunduğundan söz edilemez, zira gönüllülük esasına göre verilen parmak izinin hangi konu ve amaçla alındığına ilişkin madde bir düzenleme öngörmemiştir ve bu hüküm, veri korumada suistimallere neden olabilecek ve izaha muhtaç bir düzenlemedir⁶⁴.

PVSK’de parmak izinin alınacağı bir diğer hal de durdurulan kişinin kimlik belgesini ibraz etmemesi, kimliğine dair açıklama yapmaktan kaçınması veya gerçeğe aykırı beyanda bulunması üzerine parmak izi alınmasıdır. Bu kişinin, nüfus kayıt sistemine kayıtlı olmadığı anlaşılıyorsa parmak izi ve fotoğrafı tespit edilerek AFIS’ye kaydedilir.

C. Elektronik Gözetim Sistemleri

1. Tanım

Gözetim hakkında veri toplananları etkileme veya idare etme amacıyla tanımlanmış ya da tanımlanmamış herhangi bir kişisel verinin toplanması ve işlenmesi

<https://www.egm.gov.tr/kriminal/olayyeri-sorular> 17.07.2020. Ancak Emniyet Genel Müdürlüğünün gönüllülerden parmak izi alınmasına ilişkin belirttiği haller Kolluk ve Ceza Adaleti Direktifi’nin uygulama alanına girmemektedir ve bu nedenle kolluğa bu halde veri işleme yetkisi veren hüküm isabetsizdir.

⁶³ Dülger, **Kişisel Verilerin Korunması Hukuku**, s. 288.

⁶⁴ Bayram, **a.g.e.**, s. 33; Yazar Danıştay 10. Dairesi’nin, Adli ve Önleme Arama Yönetmeliği m. 8/1-f’nin iptali kararında (E. 2005/6392, K. 2007/948, 13.03.2007) birey ve kolluk arasındaki güç dengesizliğinin rızayı sakatlayabileceğine atıf yaparak parmak izi alınmasında bireylerin rızasının bulunmasının yeterli olmasını, anayasada temel hak ve özgürlüklerin devredilmezliği ve vazgeçilmezliği ile bağdaşır görmemiştir.

olarak tanımlanabilir⁶⁵. Günümüzde kamusal alanlara⁶⁶ elektronik gözetim sistemleri yerleştirilerek insanların suç işlemekten çekinecekleri ve bu sayede suçların önleneceği düşüncesi hâkimdir⁶⁷. Yani gözetim sistemleri önleyici tedbir niteliğindedir⁶⁸. Suçluluğun önlenmesinde etkili olan bu gözetim ve herkesin çipli münhasır bir kimliğe sahip olması CCTV vasıtasıyla sağlanmaktadır⁶⁹. Bu sistemler gözlemleyici ve gerektiğinde müdahaleyi kolaylaştırıcı bir mahiyete sahiptir. Bireylerin CCTV vasıtasıyla izlenmesi, onların her an izlendikleri endişesi ile hareket etmelerine yol açsa da kamusal alanda salt izleme özel yaşamın gizliliğini ihlal değildir⁷⁰. Ancak CCTV kameralarıyla yalnız izleme yapılsa ve görüntüler kayıt altına alınmasa dahi bireylerde kaydedildiklerine dair bir güvensizlik doğacağından sadece izleme de kanun ile düzenlenmelidir⁷¹.

2. Kamusal Alanda Hukuka Uygun Elektronik Gözetim

CCTV araçlarıyla yapılan video kayıtlarında, kişinin tanınabilir olması halinde bu kayıtlar, kişisel veridir ve kayda alınan kişiler başta kişisel verilerin korunması hakkı olmak üzere özel yaşam hakkından yararlanır⁷². Nitekim ABD’de de kişilerin

⁶⁵ David Lyon, **Günlük Yaşamı Kontrol Etmek, Gözetlenen Toplum**, Çev: Gözde Soykan, İstanbul, Kalkedon Yayınları, 2006, s.13-14 (Akt. Dülger, **Kişisel Verilerin Korunması Hukuku**, s. 7).

⁶⁶ Hubmann’ın meşhur “yaşam alanı teorisi”ne göre yaşam alanı; giz alanı, özel alan ve kamusal alandan oluşmaktadır. Giz alanı kişinin yalnız en güvendikleri ile paylaştığı alanı olup dışarıya kapalıdır, özel alan kişinin giz alanına dâhil olmayan ancak sıkı ilişki içinde olduğu aile, arkadaş gibi çevresi ile paylaştığı alanı ve kamusal/kamuya açık alan ise kişinin başkalarının bilmesinden rahatsız olmadığı alandır. Bkz. Sinan Bayındır, Özge Apiş, Oğuz Ersöz, **Kitle İletişim Hukuku**, İstanbul, On İki Levha Yayıncılık, 2018, s.62 vd; Akyürek, **a.g.e.**, s. 25 vd; Tahmazoğlu Üzeltürk, **a.g.e.**, s. 100.

⁶⁷ Veli Özer Özbek, Koray Doğan, Pınar Bacaksız, **Ceza Muhakemesi Hukuku**, 12. Baskı, Ankara, Seçkin Yayıncılık, 2019, s. 176; Ramazan Karabulut, “Kişisel Verilerin Korunması ve Kolluk Hizmetleri”, **Dicle Üniversitesi Sosyal Bilimler Enstitüsü**, Yayımlanmamış Yüksek Lisans Tezi, Diyarbakır, 2014, s. 94; Bayram, **a.g.e.**, s. 31; Thomas Würtenberger, “**Tehlike Kavramı**” ve **Alman Uygulaması Ekseninde Kolluk Hukuku**, Çev. Feridun Yenisey, Ankara, Asayiş Dairesi Başkanlığı, 2008, s. 36; İktidarın gözetlemeye başvurma gerekçesi olarak bilgi edinmek ve gözetleme sayesinde kurallara uyan bireyler yetiştirmeyi ve Panopticon modelindeki gibi tabiri caizse bireyleri terbiye etmeyi hedeflediği ileri sürülmüştür. Gözetim ve iktidar ilişkisine felsefi bir bakış için bkz. Hakan Karakehya, “Gözetim ve Suçla Mücadele”, **AÜHFĐ**, c.58, s.2, Ankara, 2009, s. 334 vd.

⁶⁸ Halid Özkan, “Mobese İzleme ve Kayıtlarının Ceza Muhakemesi Hukuku Açısından Değerlendirilmesi”, **CHĐ**, c. 11, s. 30, 2016, s. 66.

⁶⁹ Elif Küzeci, **Kişisel Verilerin Korunması**, 4. Baskı, İstanbul, On İki Levha Yayıncılık, 2020, s. 45.

⁷⁰ *P.G. ve J.H. v. Birleşik Krallık*, B. No: 44787/98, 25.12.2001, para. 57; *Perry v. Birleşik Krallık*, para. 38 Çevrimiçi <https://hudoc.echr.coe.int/> 29.03.2020.

⁷¹ Halid Özkan, **a.g.e.**, s. 70; Yenisey, **Kolluk Hukuku**, s. 358; Feridun Yenisey, “Aleni Alanların Video Kamera ile Denetlenmesi”, Çevrimiçi http://www.cagipolisi.com.tr/eski_sitemiz/120/8-9.htm 11.03.2020.

⁷² Dülger, **Kişisel Verilerin Korunması Hukuku**, s. 90

sokaklardaki güvenlik kameralarıyla izlenmesinin ardından bunun özel yaşama müdahale mahiyetinde olduğuna ilişkin tartışmalarda, kişilerin kamusal alanlarda, kalabalıklarda tanınmazlık hakkının (*right to public anonymity*) bulunduğu sonucuna varılmıştır, yani kişilerin kamusal alanda tanınmama, fark edilmeme hakkı olmalıdır⁷³.

CCTV araçlarıyla yürütülen gözetim faaliyeti, kamuya açık alanlarda yapılmalıdır. Kamuya açık alanın fiziksel ve mekânsal olarak kapalı veya açık olması ya da mülkiyetinin kamu ya da özel hukuk tüzel kişisine ait olması arasında fark bulunmamaktadır. Kamuya açık alana girişin, ücret ödemek ya da rezervasyon yaptırmak gibi herkes için aynı kurallara tabi tutulması halinde bu alanda yapılan gözetim de kamuya açık alanda yapılmış olur⁷⁴. Yapılacak gözetim, kamu tüzel kişisi tarafından önleyici amaçla yapılmalıdır⁷⁵.

Avusturya Veri Koruma Kanunu'ndaki (*Datenschutzgesetz*) açık düzenleme gereği CCTV sistemlerinin izleme ve kayıt faaliyetlerinde bulunması mümkündür. Kayıt, bireylerin yaşamsal menfaatlerinin korunması amacını sağlıyorsa, kamusal açıdan gözetilmesi gereken bir davranışın kayıt altına alındığı bireylerce biliniyorsa ve ilgisinin bu yönde açık rızası varsa kamusal alanda gözetleme yapılabilir⁷⁶. Almanya'da da Federal Veri Koruma Kanunu (*Bundesdatenschutzgesetz*) federe düzenlemeler haricinde CCTV görüntülerinin işlenmesi için geçerli ek kurallar içermektedir ve Alman veri koruma otoriteleri 2014 yılında CCTV kullanımı ile ilgili kılavuzlar yayımlamıştır⁷⁷.

Birleşik Krallık'ta kamusal alanda gözetleme yapan ve gözetlenen kişilerin biyometrik verilerini çıkaran yüz tanıma teknolojilerinden (*Live Facial Recognition-LFR*) yararlanan Metropolitan Polis Teşkilatı'na (*MET*) da değinilmelidir. Canlı yüz, yüz tanıma kameraları ile direkt sistemin veri tabanına aktarılmaktadır. Veri tabanı,

⁷³ Dönmezer, Bayraktar, **a.g.e.**, s. 350; Buket Abanoz, "Kamusal Alanda Kameralı Gözetlemenin Suçun Önlenmesindeki Etkisi ve Elde Edilen Delillerin Hukuka Uygunluğu Sorunu", **İstanbul Üniversitesi Sosyal Bilimler Enstitüsü**, Yayınlanmamış Yüksek Lisans Tezi, İstanbul, 2015, s. 107 vd.

⁷⁴ Tevfik Sönmez Küçük, "Kişisel Verilerin Korunması Hakkı Çerçevesinde Kamuya Açık Alanların Kamu Tüzel Kişileri Tarafından Video Kamera Aracılığı İle Önleyici Amaçla İzlenmesi", **YÜHFD**, c. 15, s. 1, 2018, s. 68-69.

⁷⁵ Küçük, **a.g.e.**, s. 69.

⁷⁶ § 50a Akt. Özbek, Doğan, Bacaksız, **a.g.e.**, s. 184.

⁷⁷ Bart Custers, Alan M. Sears, Francien Dechesne, Ilina Georgieva, Tommaso Tani, Simone van der Hof, **EU Personal Data Protection in Policy and Practice**, The Hague, Springer, 2019, s. 63.

kolluk ve ceza mahkemeleri tarafından aranan kişilerin bulunduğu gözleme listesini (*watch list*) içermektedir⁷⁸. MET'in kullandığı yüz tanıma sistemi, gözleme listesindeki kişilerin görüntülerini; yüzün yapısı, gözler, burun, çene, ağız ve bunlar arasındaki mesafeyi ölçerek analiz eden NEC'in *NeoFace* teknolojisini kullanmaktadır. Sistem yüzü tespit ettiğinde dijital bir versiyonunu yaratmakta ve gözleme listesinde aramaktadır. Bunun üzerine yüz tanıma uzmanına uyarı göndermektedir. Ancak LFR sistemi yalnız gözleme listesine uyan yüz görüntülerini otuz gün boyunca tutmakta ve gözleme listesindeki diğer tüm verileri ve kaydettiği görüntüleri silmektedir⁷⁹.

Kişilerin salt kamusal alana girmekle birlikte CCTV ile izlenmeye ve kişisel verilerinin işlenmesine rıza gösterdikleri kabul edilemez, zira aksi kamusal alanda bulunan herkesin kamusal figür olmasına yol açar⁸⁰. AİHM'ye göre kişilerin kimliklerinden bağımsız olarak kamusal alanda izlenmesi ancak bunun kaydedilmemesi özel yaşamın gizliliğine aykırı değildir⁸¹. Ancak AİHM, kamusal alanda özel yaşamın gizliliğinden yararlanmak için makul beklenti doktrininden hareket etmektedir. Makul beklentiden anlaşılması gereken içinse *Halford v. Birleşik Krallık* başvurusuna değinilmelidir. Bu başvuruda polis memuru olan başvuru, kendi kullanımına tahsis edilen işyerindeki ofis telefonundan yaptığı özel telefon görüşmelerinin dinlenmesi üzerine özel yaşamın gizliliği hakkının ihlal edildiği iddiasındadır⁸². AİHM telefon görüşmelerinin dinlendiğine dair bilgilendirilmeyen başvuru, mahremiyet hususunda makul beklentisi (*reasonable expectation of*

⁷⁸ Bkz. Metropolitan Police, Çevrimiçi <https://www.met.police.uk/live-facial-recognition-trial/> 30.09.2019, s. 1.

⁷⁹ Metropolitan Police, **a.g.e.**, s. 2.

⁸⁰ Küçük, **a.g.e.**, s. 57.

⁸¹ Hatta AİHK, *Friedl v. Avusturya* başvurusunda bir gösteride polis tarafından fotoğrafları çekilen ve muhafaza edilen bireyin özel yaşamının m. 8 kapsamında ihlal edilmediği kanaatindedir. Zira fotoğraf çekilmesi biçimindeki müdahale bir kamusal etkinlikte olup kişinin söz gelimi evinde değildir ve kişinin özel yaşamının iç çemberinde (*inner circle*) değildir. Akt. Tzarou, **a.g.e.**, s. 45; Ancak kararda Hükümet tarafından gösterilen teminatlar da önemli olmuştur. Zira Hükümet; gösteride elde edilen fotoğrafların hiçbir isim yazılmadan kişilerin kimliğini tespit etmeye yönelik herhangi bir adım atılmadığını belirtmiştir. Akt. Kilkely, **a.g.e.**, s. 59-60; Rooy'a göre de konutu dışına çıkan bir kişi kamusal yaşama dâhil olarak hareketlerinin herkesçe görülebileceğinin bilincindedir ve bu esnada bir iletişim aracında kendisinin belirmesi, o kişinin özel yaşamına bir müdahale teşkil etmemektedir. Akt. Dönmezer, Bayraktar, **a.g.e.**, s. 349.

⁸² *Halford v. Birleşik Krallık*, B. No: 20605/92, 25.06.1997, para. 41 Çevrimiçi <https://hudoc.echr.coe.int/> 29.03.2020.

privacy) olduğunu belirtmiştir⁸³. AİHM, özel yaşamın gizliliğine saygı hakkı ile bireylerin kişisel gelişimi ve dış dünya ile ilişkilerini geliştirmelerini hedeflemektedir. Kişilerin gözetlenmesi ya da iletişiminin denetlenmesi hali de bu nedenle kanunda düzenlenmeli ve düzenleme belirli bir kalitede olmalıdır. Zira bu hallerde kamu denetimi azdır ve bu gözetleme ve dinleme gücünün kötüye kullanılması riski fazladır⁸⁴. Böylece kamusal alan da olsa bireyin diğer kişilerle etkileşim halinde olması hali, özel yaşamın korumasından yararlanmalıdır⁸⁵. Belirtilmelidir ki kişinin kamusal alanda bulunması, görüntülerin gizli olmadığından bahisle peşinen hukuka uygun olmaz. Zira buradaki ölçüt, kişinin görüntüsünün yani kişisel verisinin sistematik biçimde belirli bir amaçla işlenip işlenmediğidir⁸⁶. Kamuya açık alanda alınan bu görüntüler sistematik ve sürekli olarak kaydedildiğinde ise artık özel yaşama bir müdahale söz konusudur⁸⁷.

Toplantı ve gösteri yürüyüşleri, konser, spor müsabakası gibi insanların toplu olarak bir arada bulunduğu faaliyetlerde katılımın resmi makamlarca kayıt altına alınacağı herkesçe bilinmektedir. Bu kayıt altına alma; suç işlenmesi halinde failin tespit edilmesine olanak sağlamakla birlikte⁸⁸ katılımının kayıt altına alınacağını bilmek, özellikle onur yürüyüşü gibi ayrımcılığa maruz kalma riski taşıyan etkinliklerde katılımcıların özel yaşamın gizliliği hakkı haricinde toplantı ve gösteri yürüyüşü hakkını kullanmaktan da imtina etmesine yol açabilmektedir⁸⁹. Gözetime

⁸³ *Halford v. Birleşik Krallık*, para. 45.

⁸⁴ *Halford v. Birleşik Krallık*, para. 49.

⁸⁵ ABD’de ise ABD Anayasası 4. Amendment ile dolaylı olarak mahremiyet hakkı tanınmıştır ve bu hak, yalnız devlet organlarına karşı ileri sürülebilmektedir. Kamusal yaşamda kolayca fark edilebilir bir faaliyet, nesneler ve banka kayıtları gibi üçüncü kişilerin kontrolünü gerektiren durumlarda, AİHS’nin öngördüğü korumanın aksine mahremiyet hakkı korumasından yararlanılamamaktadır. Örneğin *Olmstead v. ABD* kararında ABD Yüksek Mahkemesi, davacıların konutlarının dinlenmesini, konutlarına eşya ve belgelerinin aranması için fiziksel olarak girilmediğine dayanarak 4. Amendment’in ihlal edilmediğine hükmetmiştir. Ancak Mahkeme’nin yaklaşımı zamanla ve teknolojik ilerlemeler ile değişmiştir. Örneğin *Kyllo v. ABD* kararında ısı görüntüleme sisteminden yararlanılarak bir eve fiziksel olarak girilme de evde uyuşturucu madde yetiştirildiği tespiti edilmiştir. Mahkeme makul bir mahremiyet beklentisinden hareketle bu cihazın kullanılmasını 4. Amendment’in ihlali olarak değerlendirmiştir. Bkz. Yüksel, **a.g.e.**, s. 10-11, s.49; Gür, **a.g.e.**, s. 108-109.

⁸⁶ Dülger, **Kişisel Verilerin Korunması Hukuku**, s. 63.

⁸⁷ *Peck v. Birleşik Krallık*, B. No: 44647/98, 28.04.2003, para. 59 Çevrimiçi <https://hudoc.echr.coe.int/> 29.03.2020.

⁸⁸ Son dönemde basına da yansımış bir olay olarak Freddie Gray’in ölümünün ardından Baltimore’da polis müdahalesi, kargaşa ve ayaklanmalar sırasında protestocular genel gözetleme monitörlerden yüz tanıma uygulaması sayesinde tespit edilmiş ve yakalanarak tutuklanmışlardır. Bkz. Hamann, Smith, **a.g.e.**, s. 3.

⁸⁹ Küzeci, **a.g.e.**, s. 77; Küçük, **a.g.e.**, s. 55

yönelik kaydetme gibi bu türden uygulamalar, toplumun güvenlik ihtiyacını karşılarsa da kaydedilen bu verilerin ne amaçla kullanıldığı da önem arz etmektedir⁹⁰.

Elektronik gözetim araçlarıyla izleme yalnız toplantı ve gösteri yürüyüşleri, spor müsabakaları veya trafikte değil, okullarda da gerçekleşmektedir. Bu tür yerlerde elektronik gözetim faaliyetleri de kanunda öngörülmüş olmalıdır. AİHM'nin *Antović ve Mirković v. Karadağ* kararına konu olayda bir üniversite dekanı fakültedeki yedi amfiye güvenliği sağlamak için kamera yerleştirmiş ve video ile kaydedilen verilere yalnız kendisinin erişebildiğini ve verilerin bir yıl süre ile tutulacağı hususunu fakültede çalışan profesörlere bildirmiştir⁹¹. Karadağ Kişisel Verilerin Korunması Kanunu m. 35 kamu kurumlarının binalarına girişte video gözetimi yapılabilmesini; m. 36 ise kişi veya mülklerin güvenliğini sağlamak veya gizli verilerin korunmasını sağlamak için başka hiçbir yol mümkün değilse, resmi veya ticari tesislerde video gözetiminin gerçekleştirilmesini öngörmektedir⁹². Fakültede ders veren iki profesörün başvuru olduğu kararda, AİHM amfilerde ders veren başvuru sahiplerinin iş ortamlarında video gözetimine tabi olarak özel yaşamlarına müdahale edildiği sonucuna varmıştır. Zira video gözetimi kamu binasına girişte değil, amfide yapıldığından m. 35'e uygun değildir. Kamu binasının içinde yapılmasına izin veren m. 36 için ise kişi veya mülkün korunmasını gerektiren herhangi bir neden veya delil bulunmayıp yalnız soyut olarak güvenlik ihtiyacı öne sürülmüştür. Bu nedenle AİHM, özel yaşamın gizliliğinin ihlal edildiği sonucuna varmıştır⁹³.

3. Türk Hukukunda Durum

a. Mobil Elektronik Sistem Entegrasyonu (MOBESE)

(1) Mevcut Uygulama

⁹⁰ Küzeci, **a.g.e.**, s. 92.

⁹¹ *Antović ve Mirković v. Karadağ*, B. No: 70838/13, 28.02.2018, para. 6-7 Çevrimiçi <https://hudoc.echr.coe.int/> 29.03.2020.

⁹² *Antović ve Mirković v. Karadağ*, para. 26-27.

⁹³ *Antović ve Mirković v. Karadağ*, para. 58-59.

MOBESE, Emniyet Genel Müdürlüğünün Stratejik Planı doğrultusunda *asayışı sağlamak, kent güvenliğine yönelik tehditleri önceden algılamak, suç ve suçlularla hızlı ve etkin mücadele edilmesini sağlamak amacıyla*⁹⁴ herhangi bir kanuni düzenlemeye dayanmaksızın oluşturulan bir şehir izleme sistemidir⁹⁵. Coğrafi bilgi sistemleri ve bilgi yönetim sistemleri ile entegre biçimde işleyen MOBESE, Emniyet Genel Müdürlüğü araçları için tasarlanmış ve GPRS teknolojisini kullanan bir yazılımdır. Taşıtların plakalarını okuyup sahibi ile bağlantı kurabilmekte ve trafik akışı, büyükşehirlerin anayolları, meydanlar, şehir giriş çıkışı gibi kritik noktalarda gözetleme yapmaktadır⁹⁶. Bu türden kritik noktalarda bulunduğundan suçun önlenmesi, suç sonrası delil tespiti, faillerin tespiti ve yakalanması, çalıntı araçların bulunması, şüpheli paket tespiti, trafik kazası tespitlerinde de işlevseldir⁹⁷. Yani MOBESE ile kentsel güvenlik hakkı sağlanmaya çalışılmaktadır⁹⁸. Ancak MOBESE kameraları yalnız izleme yapmayıp verileri özel kodlarla kaydetmektedir⁹⁹.

Günümüzde mobil izlemenin ötesine geçmiş olan MOBESE, *optik ve teknik araçların kullanılması suretiyle veri toplanması* işlevi görmektedir¹⁰⁰. Toplanan verilerden ceza muhakemesinde de yararlanılmaktadır¹⁰¹. Veri toplama işlevi ile

⁹⁴ Emniyet Genel Müdürlüğü Stratejik Plan 2009-2013 (akt. Çam, **a.g.e.**, s. 97).

⁹⁵ Küzeci, **a.g.e.**, s. 508; Sabire Sanem Yılmaz, “Video Gözetimi, Yapay Zeka ve Kişisel Verilerin Korunması Hakkı” Çevrimiçi <https://www.hukukihaber.net/video-gozetimi-yapay-zeka-ve-kisisel-verilerin-korunmasi-hakki-makale,7001.html> 10.11.2019 ; Özbek, Doğan, Bacaksız, **a.g.e.**, s. 173; Yenisey, **Kolluk Hukuku**, s. 351.

⁹⁶ Özbek, Doğan, Bacaksız, **a.g.e.**, s. 174.

⁹⁷ Özbek, Doğan, Bacaksız, **a.g.e.**, s. 174; R. Cengiz Derdiman, Nihal Tataroğlu, “Devlet Gözetimi ile İnsan Haklarının Uyumlaştırılması Sorunu ve Çözüm Önerileri”, **İÜHFD**, c. 7, s. 1, 2016, s. 256.

⁹⁸ Derdiman, Tataroğlu, **a.g.e.**, s. 269.

⁹⁹ Küçük, **a.g.e.**, s. 73.

¹⁰⁰ Özbek, Doğan, Bacaksız, **a.g.e.**, s. 175; Halid Özkan, **a.g.e.**, s. 65.

¹⁰¹ Örneğin bkz. Yargıtay 2. CD, E. 2019/12748, K. 2019/19640 “*Olay tarihinde katılan ...'a ait motosikletin park halinde bulunduğu sırada saat 00.00 ile 08.00 arasında çalındığı, 05/09/2014 tarihli bilirkişi raporuna göre, olay yerine yakın MOBESE görüntülerinin incelenmesi sonucu motosikletin olay yerine bir başka motosikletle gelen bir kişi tarafından çalındığı, ikinci motosikletin çalınan motosiklet ile birlikte hareket ettiği, renginin siyah olma ihtimali yüksek bir araç tarafından da bu motosikletlerin sürekli takip edildiği, 26/05/2011 tarihli tutanağa göre katılana ait motosikleti kullanan kişinin üzerindeki siyah-gri renkli motosiklet sürücüsü montunun üzerinde “...” ibaresinin yazılı olduğu, sanıklardan ...'nın evinde yapılan aramada, motosikleti çalan sürücüsünün üzerindeki montun aynısının ele geçirildiği, sanık ...'nın olayın sıcağı sıcağına soruşturma aşamasında müdafii huzurunda alınan 26.05.2011 tarihli ifadesinde, MOBESE görüntülerindeki motosikleti çalan şahıslardan birinin ... olduğunu teşhis ettiği...*”; Yargıtay 23. CD, E. 2015/14246, K. 2015/6548 “*Sanık F. K.'ın suç tarihinde şikâyetçi M. A.'a ait olup, ayakkabı boyacılığında kullanılan ve adı geçen şikâyetçi tarafından A.... İli, M... İlçesi, K... Ö... Caddesinde bulunan K... Otelinin önünde muhafaza edilen boya sandığına tiner döküp yakmak suretiyle zarar verdiğinin iddia edildiği somut olayda; Sanık savunmasına, şikâyetçi beyanına, tanık anlatımına, mobese izleme ve kamera izleme tutanaklarına,*

birlikte MOBESE, kişisel verilerin korunması hakkına müdahale teşkil ettiğinden bir kanuni düzenlemeye dayanmalı ve bu düzenleme de AY m. 13'ün gereklerine uygun olmalıdır¹⁰². Yani elektronik gözetlemeye ilişkin kanun, yayımlanarak bireyler tarafından ulaşılabilir olmalı, yeterince açık ve anlaşılır ifadelerle izlemenin şartları ve bireylerin haklarını bilmesi bakımından öngörülebilir olmalıdır¹⁰³. Zira bir hukuk devletinde bireylerin, idarenin hangi şartlarda kendi kişisel verilerini taşıyan görüntü ve sesleri izleyip kaydedeceğini bilmesi gerekmektedir¹⁰⁴. İdarenin yetkisinin kanuna dayanması anayasal bir zorunluluktur¹⁰⁵.

MOBESE yoluyla izleme ve görüntülerin kayda alınmasının dahası ceza muhakemesinde bu kayıtların kullanılmasının bir kanuni dayanağı bulunmamaktadır. Üstelik MOBESE yoluyla veri işlemlere KVKK m. 28/1-ç uyarınca KVKK de uygulanamamaktadır. PYSK ve Jandarma Kanunu'nda polis ve jandarmaya hakim kararı ile teknik araçla izleme yapma yetkisi verilmişse de bu yetki, yalnız maddede sayılan suçların önlenmesi bakımındandır. Oysa MOBESE ile yapılan izlemeler sınırlı sayıda belirli suçların değil, genel olarak suçların önlenmesi ve kişilerde suç işlememe için çekince uyandırma amacıyladır. Valiliklerce yayımlanan genelgeler ile kamu ve özel kuruluşlarda kamera kullanılması yükümlülüğü karşısında 5442 sayılı İl İdaresi Kanunu çerçevesinde de bir değerlendirme yapılmalıdır. Kanun m. 11/A ve m. 32/B uyarınca vali ve kaymakam suç işlenmesini önlemek için her türlü tedbiri almaya yetkilidir. Ancak maddelerde video gözetim sistemi ile kişisel veri işleme yetkisi,

01/10/2010 tarihli ekspertiz raporu ile Adli Tıp Kurumu Fizik İhtisas Dairesi Başkanlığı Ses ve Görüntü İnceleme Şubesinin 15/07/2011 tarihli uzmanlık raporu içeriğine ve tüm dosya kapsamına göre; sanığın üzerine atılı "nitelikli mala zarar verme" suçundan mahkûmiyetine yönelik kabulde herhangi bir isabetsizlik görülmemiş"; Yargıtay 4. CD, E. 2015/17224, K. 2019/16889 "Sanıkların aşamalarda, katılanların kalabalık bir şekilde ellerindeki sopalarla kendilerine saldırdıklarını beyan etmeleri ve dosya içinde bulunan mobese kamerasındaki görüntüleri içerir CD üzerinde yapılan bilirkişi incelemesi sonucu hazırlanan rapordaki görüntülerde, ikisinin elinde sopa olan dört kişinin yürüdüğü belirlenmesi karşısında, olayın çıkışı ve gelişimi üzerinde durularak, sanıklar hakkında haksız tahrik ve meşru savunma hükümlerinin uygulanıp uygulanmayacağı değerlendirilmemesi, Kanuna aykırı, sanıklar ... ve ...'un temyiz nedenleri yerinde görüldüğünden, hükümlerin bozulmasına". Çevrimiçi <http://www.kazanci.com/kho2/ibb/giris.html> 02.01.2020.

¹⁰² Örneğin İtalyan Ceza Kanunu m. 615'e göre kamera sistemleri; kayıtlarını yalnız yakın zaman dilimlerini tutacak şekilde ayarlayarak, hedefin farklı şekilde elde edilemeyeceği durumlar ile sınırlanarak kullanılması gerektiğini düzenlemiştir. Türk hukukunda da yapılacak bu minvalde bir düzenleme ölçülülük ilkesine hizmet edecektir. Bkz. Yılmaz, **a.g.e.**

¹⁰³ Kathleen M. Burch, "Protecting Privacy in the Digital Age: Europe and The United States", **Prof. Dr. Feridun Yenisey'e Armağan**, c. 2, İstanbul, Beta Yayıncılık, 2014, s. 1717.

¹⁰⁴ Özbek, Doğan, Bacaksız, **a.g.e.**, s. 175.

¹⁰⁵ AY m. 8, m. 123.

verilerin arşivlenme ve kullanılma usulü gibi hususlar açıkça belirtilmediğinden¹⁰⁶ idare, kanunda yer almayan bir yetkiyi kullanamaz. İl İdaresi Kanunu'nda MOBESE'ye ilişkin en yakın düzenleme m. 11/H'dir. Bu düzenlemeye göre vali, *“kamu düzeni ve güvenliği ile kişilerin can ve mal emniyetinin korunması, suç işlenmesinin önlenmesi, trafik güvenliği ve kontrolünün sağlanması amacıyla meydan, karayolları, cadde, sokak ve park gibi kamuya açık alanlarda kurulacak sistemlerin yerlerinin tespiti, kurulumu ve altyapı faaliyetlerini”* koordine edebilir. Ancak bu hükümde elektronik gözetim sistemlerinin veri işleyip işlemeyeceğinden dahi bahsedilmemiştir¹⁰⁷. Sonuç olarak MOBESE yoluyla elektronik gözetleme herhangi bir kanuni düzenlemeye dayanmamaktadır. Kanuni bir düzenleme olmaksızın bu denli büyük bir hukuka aykırılığın nasıl süregeldiği ise izaha muhtaçtır.

Kanuni düzenleme bulunmadan meşru savunma ve zorunluluk hali gibi ceza hukuku müesseselerine başvurularak ceza muhakemesinde MOBESE kayıtlarından yararlanılması isabetli değildir. Zira MOBESE kameraları suç işlenmeden önce belirli alanlara yerleştirilmiştir, yani aktüel bir saldırı bulunmazdan evvel kameralar izleme ve kayıt yaptığından meşru savunmaya başvurulamaz. Önleyici meşru savunmadan¹⁰⁸ yararlanabilmek için ise saldırı ile eş zamanlı harekete geçen bir izleme ve kayıt faaliyetinin olması gerekir ki bu da MOBESE'de mevcut değildir¹⁰⁹. Dolayısıyla ceza muhakemesinde MOBESE kayıtlarından yararlanılması kanuni dayanağa sahip değildir ve AY m. 38/6 uyarınca bu kayıtlar delil olarak değerlendirilmemelidir. Aksi kişisel verilerin korunması hakkı ve adil yargılanma hakkının da ihlaline yol açacaktır¹¹⁰. AİHM kararlarında hukuka aykırı delille kişinin mahkûm edilmesi bazı

¹⁰⁶ Küçük, **a.g.e.**, s. 74; Derdiman, Tataroğlu, **a.g.e.**, s. 263.

¹⁰⁷ Küçük, **a.g.e.**, s. 75.

¹⁰⁸ “Offendicula”. Saldırının gerçekleştiği anda önleyici nitelikteki araç, savunma pozisyonu almaktadır. Bkz. Hakan Hakeri, Recep Gülşen, “Offendicula ve Yeni Ceza Kanunu”, **AÜEHFD**, c. 9, s. 1-2, 2005, s. 52-53.

¹⁰⁹ Halid Özkan, **a.g.e.**, s. 71; MOBESE kayıtlarının ilgilinin kamusal alana girmekle rızası, meşru savunma ve PVSK ek m. 7/6 kapsamında kanun hükmünü icra hukuka uygunluk nedenlerinden yararlanıp yararlanamayacağına ilişkin değerlendirme için bkz. Abanoz, **a.g.e.**, s. 110 vd.

¹¹⁰ Esasında AİHM, yargılamanın bir bütün olarak hakkaniyete uygun yürütülmesi halinde delil iç hukuka uygun olarak elde edilmemişse de adil yargılanma hakkının ihlal edilmediği kanaatindedir. AİHM'ye göre delil doğru sınanmış, çelişmeli yargılama yapılmış, sanığa delile karşı koyma imkânı verilmişse muhakeme hakkaniyete uygun yürütülmüştür. Detaylı bilgi için bkz. Mehmet Maden, “Anayasa Mahkemesine Bireysel Başvuru Bakımından Adil Yargılanma Hakkı Çerçevesinde Delil Yasakları”, **Anayasa Yargısı**, s. 32, 2016, s. 213; Murat Volkan Dülger, **Ceza Muhakemesi**

hallerde adil yargılanma hakkını ihlal etmemektedir. Hukuka aykırı bulgunun tek delil veya esas delil olup olmaması AİHM'nin değerlendirmesinde önem taşımaktadır¹¹¹.

(2) Olması Gereken Uygulama

Yapılacak kanuni düzenleme; MOBESE sistemlerinin nerede kurulacağı, kullanılacak araçların özellikleri, kayıt yapılıp yapılmayacağı ve yapılacaksa kayıtların saklama süresini belirlemelidir¹¹². Kanuni düzenlemede gözetimi yapacak personel, verilerin muhafaza edileceği veri tabanına erişebilecek kişiler gösterilmelidir ve bu kişiler münhasıran kolluk güçleri arasından seçilmeli, özel hukuk kişileri olmamalıdır¹¹³.

Alman Kuzey Ren Vestfalya Polis Kanunu'nda tedbirin uygulanacağı yerin suç bakımından anlam ifade eden bir yer olması aranmıştır¹¹⁴. Yani suçluluğun çok yaygın olduğu bir bölgede kamera gözetim sistemi kurulması anlaşılabilirse de suç işleme ihtimalinin düşük olduğu bir mahalde bu gözetim sistemi kurulmamalıdır¹¹⁵. Ayrıca periyodik kontrollerle de suçluluğun olmadığı ya da azaldığının anlaşıldığı mahalde gözetim faaliyeti azaltılmalıdır. Suçların önlenmesi amacıyla yürütülen gözetim faaliyeti ölçülü olmalıdır, yani suçların önlenmesi için bölgeyi ışıklandırmak, güvenlik personeline başvurmak gibi yapısal tedbirler yeterli olabilecekse gözetim sistemine başvurulmamalıdır¹¹⁶. Kameraların yerleştirildiği bölgeler, kişilerin özel yaşam beklentilerinin bulunmadığı yerler olmalıdır ve kamera kişi hareket ettikçe onu takip

Hukukunda Dışlama Kuralı ve Hukuka Aykırı Delillerin Uzak Etkisi (Zehirli Ağacın Meyvesi Öğretisi), Ankara, Seçkin Yayıncılık, 2014, s. 103-105.

¹¹¹ Maden, **a.g.e.**, s. 214. Örneğin bkz. *Khan v. Birleşik Krallık*, para. 37; *Mialhe v. Fransa*, para. 44-46.

¹¹² Özbek, Doğan, Bacaksız, **a.g.e.**, s. 178; Söz gelimi Alman NRW Polis Kanunu m. 15a/2'ye göre izleme suretiyle yapılacak kayıt en fazla on dört gün süre ile saklanabilmektedir. Bkz. Özbek, Doğan, Bacaksız, **a.g.e.**, s. 180.

¹¹³ Derdman, Tataroğlu, **a.g.e.**, s. 278.

¹¹⁴ Özbek, Doğan, Bacaksız, **a.g.e.**, s. 181; Bu hususu *Özkan*, üstün bir kamu yararının varlığı halinde yapılacak gözetlemenin “ciddi ve önemli gerekçeler” ile yapılması biçiminde ifade etmiştir. Bkz. Halid Özkan, **a.g.e.**, s. 73.

¹¹⁵ Württenberger, **a.g.e.**, s. 36; Örneğin Mannheim Yüksek İdare Mahkemesi, suçların yoğun olduğu yerleri belirleme bakımından Baden-Württemberg Polis Kanunu m. 26'daki tehlikeli yerleri kriter olarak ele almıştır. Suçların hazırlandığı ve işlendiği yerler, aleni yerler bu kapsamdadır. Ayrıca bölgedeki diğer yerlerle kıyaslandığında orada daha fazla suç işleniyor olmalıdır. Külli olarak tüm bölge kamera sistemi ile gözetlenmemelidir. Bkz. Yenisey, **Kolluk Hukuku**, s. 357-358.

¹¹⁶ Küçük, **a.g.e.**, s. 76.

eder vaziyette olmamalıdır¹¹⁷. Kamera yapacağı izlemeyi yönünü değiştirmeden ve yakın çekim yapmadan gerçekleştirmelidir¹¹⁸. Görüntülerin izlenmesi yeterli ise bu durumda görüntüler kaydedilmemelidir.

MOBESE kameralarının yerleştirildiği yerlerde uyarıcı işaretler bulunması gerekir ki görüntüleri izlenen ve kaydedilen kişi bu sayede uyarılabilsin¹¹⁹. Gözetlemenin ayrıntıları, kamera sayısı gibi teknik hususların gözetlenecek kişilere bildirilmesi gerekme de fark edilebilir bir şekilde kişilere izlendikleri bilgisi açık şekilde sunulmalıdır¹²⁰. Ayrıca veri sorumlusu olan kamu tüzel kişisi de belirtilmelidir, bu sayede veri sahibi, kişisel verisinin korunmasına ilişkin taleplerini bu kişiye yöneltebilecektir¹²¹. Monitörler, herkesçe ulaşılabilir biçimde olmamalı¹²² ve görüntüler anlık olarak ya da sonrasında nakledilmemeli, yayınlanmamalıdır¹²³. Ancak kamu yararı ve kamunun ilgisini çekebilen haber değeri olan bir görüntü bulanıklaştırarak kişinin tanınmasına engel olan biçimde yayınlanabilmelidir. Eğer gizli olarak gözetleme yapılacaksa da gizlilik gerekçeleri de kanunda açıkça gösterilmelidir¹²⁴.

Kamusal alanlar harici özel kişilerin mülklerinde izleme ve kayıt altına alma faaliyetinin diğer kişiler bakımından bilinir olması gerekir, bu nedenle uyarıcı levhalar bu yerlere de konulmalıdır¹²⁵. Özel kişiler tarafından CCTV yoluyla gerçekleşen veri işleme faaliyetine GDPR uygulanacaktır, zira Kolluk ve Ceza Adaleti Direktifi bağlamında yetkili makam bulunmamaktadır¹²⁶. Ayrıca özel kişiler tarafından yapılan CCTV izleme ve kayıtlarında, kameranın konulduğu alandaki tüm kişilerin rızasının

¹¹⁷ Yenisey, **Kolluk Hukuku**, s. 352.

¹¹⁸ Özbek, Doğan, Bacaksız, **a.g.e.**, s. 181; Halid Özkan, **a.g.e.**, s. 77.

¹¹⁹ Özbek, Doğan, Bacaksız, **a.g.e.**, s. 176; Yılmaz, **a.g.e.**

¹²⁰ Bkz. *López Ribalda ve diğerleri v. İspanya* [BD], B. No: 1874/13 ve 8567/13, 17.10.2019, para. 116 Çevrimiçi <https://hudoc.echr.coe.int/> 29.03.2020.

¹²¹ Küçük, **a.g.e.**, s. 78.

¹²² Yılmaz, bu hususta şehrin panoramik görüntüsünü büyük ekranlarda herkesin izleyeceği biçimde ortama monitör kuran belediyelerin KVKK'ye muhalefet ettiğini belirtmiştir. Bkz. Yılmaz, **a.g.e.**

¹²³ Halid Özkan, **a.g.e.**, s. 77.

¹²⁴ Özbek, Doğan, Bacaksız, **a.g.e.**, s. 180.

¹²⁵ Özbek, Doğan, Bacaksız, **a.g.e.**, s. 183.

¹²⁶ Leiser, **a.g.e.**, s. 7.

olması gerekmekte olup izlemeyi yapacak kişinin bu izleme ile doğrudan bir hukuki menfaati bulunmalıdır¹²⁷.

b. Araç Plakasının Okunması

Araç plakasının okunması, elektronik şekilde geçen araçların plaka tanıma sistemlerinin sabit bir kamera ile izlenmesi ve otomatik biçimde kaydedilmesidir. Bu yöntemle pek çok plaka toplanmakta ve plaka sorgulaması ile trafik kurallarını ihlal edenlerden suç işleyenlere kadar pek çok kişi tespit edilebilmektedir¹²⁸. Örneğin; Trafik Bilgi Sistemi'nde GPRS ve GPS teknolojilerinden yararlanarak trafik ekipleri, kişisel veri olan kişinin kullandığı aracın plakasını okuyarak takip etmektedirler¹²⁹. Bu gözetleme, yalnız trafik ihlallerinin hangi durumlar olduğunu ve sadece bu durumları kaydeden ve trafik ihlalinde bulunmamış araçların görüntülerini silen yapay zekâ teknolojilerinden yararlanılarak yapılmalıdır¹³⁰. Belirtelim ki Türk hukukunda bu tedbir de kanuni bir dayanağı olmaksızın uygulanmaktadır¹³¹.

c. Çocuk Bakım Kuruluşlarında Güvenlik Kamerası Uygulaması

Güvenlik kamerası uygulamasına ilişkin uygulamada mevcut tek norm, Çocuk Bakım Kuruluşlarında Güvenlik Kamerası Sistemi Kurulumu ve Kullanımı Hakkında Genelge'dir¹³². Genelgede kamera gözetimi ile amacın *özel yaşama müdahale etme olmayıp daha güvenli bir ortamda çocuk bakım hizmeti sunma, olumsuz olayların önlenmesi ve olası risklerin bertaraf edilmesi* olduğu belirtilmiştir. Bu amaçların sağlanması için çocuk evleri sitesi, çocuk yuvası, yetiştirme yurdundaki bina giriş ve

¹²⁷ Halid Özkan, **a.g.e.**, s. 92-93.

¹²⁸ Halid Özkan, **a.g.e.**, s. 86; Yenisey, **Kolluk Hukuku**, s. 330.

¹²⁹ Bayram, **a.g.e.**, s. 30.

¹³⁰ Yılmaz, **a.g.e.**

¹³¹ Buna karşın Almanya Baden-Württemberg Polis Kanunu §22a'da plaka tanıma programları da açık şekilde düzenlenmiştir. Ancak Avusturya'da bu tür bir kullanıma izin verilmemektedir. Bkz. Özbek, Doğan, Bacaksız, **a.g.e.**, s. 185-187; Baran Kızıllırmak, "Önleyici Amaçla Elde Edilen Verilerin Ceza Muhakemesinde Kullanılabilirliği", **İstanbul Üniversitesi Sosyal Bilimler Enstitüsü**, Yayınlanmamış Yüksek Lisans Tezi, İstanbul, 2018, s. 156.

¹³² 13.10.2016 tarih ve 92131503-010.06.01-E.106499 sayılı Genelge. Çevrimiçi <https://www.ailevecalisma.gov.tr/uploads/chgm/uploads/pages/genelgeler/2016-05-cocuk-bakim-kuruluslarinda-guvenlik-kamerasi-sistemi-kurulumu-ve-kullanimi-hakkinda.pdf> 10.11.2019.

çıkış kapıları, kuruluş bahçesi ile çocuk evlerinde evin daire giriş kapısı gibi ortak alanlara güvenlik kamerası takılması öngörülmüştür.

Genelge; hatalı olarak ortak alanlarda hukuken korunacak bir gizlilik ve mahremiyet bulunmadığından bahisle bu alanlarda herkes tarafından bilinen ve görülebilir kamera sistemlerinin kurulmasında, herhangi bir hak ihlalinin olmadığını belirtmiştir. Oysa daha önce de belirttiğimiz gibi güvenlik kamerası, CCTV, MOBESE, adı her ne olursa olsun bu görüntüleme cihazları ile yapılan izleme ve kaydetmenin yaşamın gizli alanı ve özel alanına müdahale etmemesi halinde, bunların peşinen hukuka uygun olduğundan bahsedilemez. Zira kişisel verilerin hukuka aykırı olarak işlenmesi ile bu uygulamalar, günümüzde başlı başına bir hak olan kişisel verilerin korunması hakkına müdahale oluşturmaktadır. Nitekim bahsi geçen güvenlik kamerası ile izlemenin dayanağı genelgedir ve AY m. 13 gereği temel hak ve özgürlüklere müdahale ancak kanunla mümkündür. Dolayısıyla güvenlik kamerası uygulaması, kişisel verilerin hukuka aykırı işlenmesidir¹³³.

Genelge'ye göre güvenlik kamerası kayıtları, önleyici tedbir mahiyetinin haricinde ceza muhakemesinde delil olarak da kullanılabilecektir. Ancak kanuni düzenleme olmaksızın hukuka aykırı olarak yapılan güvenlik kamerası kaydının, AY m. 38/6 karşısında ceza muhakemesinde nasıl delil olarak kullanılacağı izaha muhtaçtır. Genelge'ye göre kamera kaydı ile elde edilen görüntüler, CD/DVD ortamına yüklenerek ilgili adli ve idari makamlara tutanak ile teslim edilecektir, ancak ilgili makamdan ne anlaşılabileceği da belirtilmemiştir. Kişisel verilerin paylaşılacağı makamın dahi açıkça belirtilmemiş olması da izaha muhtaçtır.

Ayrıca son olarak Genelge'de kayıtların altı aylık sürelerle elektronik ortamda arşivleneceği düzenlenmişse de silme ve anonim hale getirme yöntemleri gibi hiçbir yöntemden bahsedilmemiş olması, CCTV sistemlerine dair tek hukuki düzenlemenin, kılavuz niteliğinin dahi olmadığını göstermektedir¹³⁴.

¹³³ Veri güvenliği ve uyarının bulunmaması halinde gündeme gelen aydınlatma yükümlülüğünün ihlali gibi hallerin hukuka uygun işleme ilkesi altında incelenmemesi gerektiği görüşü için bkz. Nafiye Yücedağ, "Kişisel Verilerin Korunması Kanunu Kapsamında Genel İlkeler", **Kişisel Verileri Koruma Dergisi**, c. 1, s. 1, 2019, s. 48. Zira yazara göre hukuka uygun işleme ilkesinden anlaşılması gereken, yalnız veri işlemenin kanun hükmüne dayanıp dayanmadığıdır.

¹³⁴ Yılmaz, **a.g.e.**

D. Telekomünikasyon Yoluyla İletişimin Denetlenmesi

1. AİHM ve ABAD'nin Yaklaşımı

Interception kavramıyla AİHM kararlarında kendine yer bulan iletişimin denetlenmesi, iletişimin taraflarının rızası olmaksızın kapsamı hakkında bilgi toplanmasıdır¹³⁵. Suç işlenmesinin önlenmesi, işlenmiş veya işlenmekte olan bir suçta delil elde etmek veya istihbarat amacıyla, gizli kalması beklenen telekomünikasyon yoluyla iletişim denetlenebilmektedir¹³⁶. Devlet bireysel haberleşme gizliliğine saygı duymak ve ihlal etmemekle yükümlüdür¹³⁷. Telefon görüşmeleri başta olmak üzere telekomünikasyon yoluyla iletişimin kolluk ve adli makamlarca denetlenmesi, özel yaşama saygı hakkı ve bu hakkın alt kategorisi olan haberleşmeye saygı hakkı kapsamında bir müdahaledir¹³⁸.

Fransa'da önleyici kolluk tedbiri olarak başbakanın kararı ile ulusal güvenlik, bilimsel ve ekonomik kaynakların korunması, terörizm ve organize suçluluğun önlenmesi ile ilgili bilgi toplamak amacıyla iletişim denetlenebilmektedir. Ancak bu denetlemenin fişleme amacıyla yapılması yasaktır¹³⁹. İletişimin denetlenmesi kararı prosedürel kurallara ve mahremiyet hakkına uygunluğu denetlemek üzere bağımsız idari otorite olan Güvenlik Müdahalelerinin Kontrolü Ulusal Komisyonu'na

¹³⁵ Bkz. *Malone v. Birleşik Krallık*, B. No: 8691/79, 02.08.1984, para. 19 Çevrimiçi <https://hudoc.echr.coe.int/> 29.03.2020.

¹³⁶ Nur Centel, "5271 Sayılı Ceza Muhakemesi Kanunu'na Göre Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi", Prof. Dr. Köksal Bayraktar'a Armağan c. 1, **GSÜHFD**, 2011, s. 162; Örneğin Fransa'da alt sınırı iki yıl hapis cezası gerektiren ciddi suçlarda (*crime ve délit*) hakim kararıyla ceza yargılaması sırasında iletişim dinlenip kaydedilebileceği gibi kamu güvenliğinin sağlanması için idari olarak da (*interceptions de sécurité*) denetlenmektedir. Bkz. Francesca Galli, "The Interception of Communication in France and Italy – What Relevance For The Development of English Law?", **The International Journal of Human Rights**, c. 20, s. 5, UK, 2016, s. 667.

¹³⁷ Galli, **a.g.e.**, s.667; Adem Sözüer, "Türkiye'de Karşılaştırmalı Hukukta Telefon, Teleks, Faks ve Benzeri Araçlarla Yapılan Özel Haberleşmenin Bir Ceza Yargılaması Önlemi Olarak Denetlenmesi", **İÜHFM**, c. 55, s. 3, 1997, s. 71.

¹³⁸ A. Şeref Gözübüyük, Feyyaz Gölcüklü, **Avrupa İnsan Hakları Sözleşmesi ve Uygulaması**, 11. Bası, Ankara, Turhan Kitabevi, 2016, s. 360; Gülay Arslan Öncü, "Özel Yaşama ve Aile Yaşamına Saygı Hakkı", **İnsan Hakları Avrupa Sözleşmesi ve Anayasa Mahkemesine Bireysel Başvuru Kapsamında Bir İnceleme**, Ed. Sibel İncoğlu, 3. Baskı, İstanbul, Beta Yayıncılık, 2013. s. 321. AİHS'nin Fransızca ve İngilizce metninde yer alan *correspondence* kavramından anlaşılması gereken yalnız yazışma olmayıp mektup, telefon, telsiz gibi kişiler arasında iletişim vasıtası olan her çeşit yol haberleşme manasına gelmektedir.

¹³⁹ Galli, **a.g.e.**, s. 669.

(*Commission Nationale de Contrôle des Interceptions de Sécurité-CNCIS*) gönderilmektedir. Tedbire başvurma gerekçesi olarak ulusal güvenliğin belirsiz bir kavram oluşu, kanunun tedbirin yenilenmesi için üst sınırı belirlememiş olması, önleyici amaçla iletişimin denetlenmesi yargılamada delil olarak kullanılamasa da kayıtların tutulması bu müessesenin eleştirilebilir yönleridir¹⁴⁰. İtalya’da da iletişimin denetlenmesine, *post delictum* ve terörizm ile organize suçluluğun önlenmesinde önleyici tedbir olarak başvurulmaktadır. Ancak İtalya’da da önleyici tedbir olarak iletişim denetlendiğinde yenileme süresinin üst sınırı bulunmamaktadır. Bu tedbir sonucunda elde edilen kayıtlar ceza muhakemesinde kullanılamazsa da savcının soruşturmaya başlaması için başlangıç şüphesi teşkil etmektedir¹⁴¹.

İletişimin denetlenmesi şartları AİHM tarafından *Malone v. Birleşik Krallık* kararında belirlenmiştir. Başvurucu Bay Malone, suç eşyasını bulundurma suçu nedeniyle yargılanıp beraat ettikten sonra telefonları Metropolitan Polis Teşkilatı’na dinlenmiş, kaydedilmiş ve *metering* uygulanmıştır¹⁴². AİHM’nin değerlendirmesine göre iletişimin denetlenmesi konusunda kolluk ve adli makamlara yetki veren bir iç hukuk kuralı olmalıdır. Bu kural keyfilikten uzak olmalı ve kişilerin m. 8/1 çerçevesinde haklarını korumak için garanti sunmalı, kanunda kamu makamlarına verilen takdir yetkisinin sınırları iyi çizilmiş olmalı ve bu yetkiyi kötüye kullanmaya karşı yeterli garantiler bulunmalıdır¹⁴³. Metering ise telefon abonesinin, hizmete ilişkin şikâyetlerini veya olası suiistimallerini doğru şekilde inceleme ve araştırma için kullanılmaktadır. Ancak metering kayıtları kişinin hangi numaraları çevirdiğine, iletişimine dair bütüncül bilgi taşımaktadır ve abonenin rızası olmaksızın bu bilgilerin polise verilmesi m. 8 uyarınca bir müdahaledir¹⁴⁴.

¹⁴⁰ Galli, **a.g.e.**, s. 671.

¹⁴¹ Galli, **a.g.e.**, s. 673.

¹⁴² *Malone v. Birleşik Krallık*, para. 62; *Metering* bir telefonda hangi numaraların arandığı, aramanın süresi ve saatini kaydeden bir araçla iletişimin denetlenmesidir. Detaylı bilgi için bkz. Saadet Yüksel, **Özel Yaşamın Bir Parçası Olarak Telekomünikasyon Yoluyla Yapılan İletişimin Gizliliğine Önleyici Denetimle Müdahale**, İstanbul, Beta Yayıncılık, 2012, s. 150-151.

¹⁴³ *Malone v. Birleşik Krallık*, para. 70 vd.; Detaylı değerlendirme için bkz. Sözüer, “Türkiye’de Karşılaştırmalı Hukukta Telefon, Teleks, Faks ve Benzeri Araçlarla Yapılan Özel Haberleşmenin Bir Ceza Yargılaması Önlemi Olarak Denetlenmesi”, s. 74-75.

¹⁴⁴ *Malone v. Birleşik Krallık*, para. 84.

*Digital Rights Ireland Ltd.*¹⁴⁵ kararında ABAD, terör ve organize suçlarla mücadelede ve ceza muhakemesinde 2006/24 sayılı Direktif uyarınca kullanılabilecek kişisel verileri değerlendirmiştir. Direktif'e göre internet sağlayıcıları kişilerin kimliği ve internete erişim bilgilerini iletişimin gerçekleştiği tarihten itibaren altı aydan iki yıla kadar saklayabilir.

Başvuru, bir kolektif dava mahiyetinde olup Avusturya'da 2006/24 sayılı AB Direktifi'ne uyum kapsamında ihdas edilen Telekomünikasyon Kanunu ile kişisel verinin korunması hakkının ihlali iddiasına ilişkindir¹⁴⁶. Bahsi geçen Kanun, telefon, mobil telefon, internet erişimi, internet e-posta vasıtasıyla gerçekleşen tüm iletişim yollarını ve bunun süjesi tüm kayıtlı kullanıcı ve aboneleri kapsamaktadır. Bu düzenleme; internetten yararlanacak kişiler ve genel ya da özel nitelikli veriler arasında herhangi bir ayırım gözetmemektedir. Yani istisna veya güvenceye tabi olmaksızın yetkililerin kullanıcılar ile ilgili verileri araştırması ve bu verilerin içeriği hakkında bilgi edinmesi, kullanıcı olan veri sahiplerinin özel yaşam ile meslek sırları hakkında¹⁴⁷ bilgi edinilmesine yol açmakta ve veri sahiplerini bunların kötüye kullanılması riskine maruz bırakmaktadır¹⁴⁸. Ayrıca altı aydan iki yıla kadar saklanacak veriler arasında ilgilerine göre bir süre sınırı olmayıp bu otoritelerin takdirine bırakılmıştır.

2006/24 sayılı Direktif'in amacı; organize suç ve teröre karşı mücadele başta olmak üzere suçların önlenmesi, kamu güvenliği ve etkinliğinin sağlanmasıdır. Bu genel amaçlara dayanarak modern diğer araştırma teknikleri varken otomatik olarak 2006/24 sayılı Direktif ile belirlenen veri saklama süresi orantılılık şartını tek başına sağlamamaktadır¹⁴⁹. ABAD, Direktif'i AB Temel Haklar Şartı'nın özel ve aile

¹⁴⁵ Büyük Daire'nin 08.04.2014 tarihli hükmünde, Avusturya'da *Digital Rights Ireland Ltd.* (C-293/12) ve Bay Landesregierung, Bay Seitlinger, Bay Tschohl ve diğer 11.128 başvuru tarafından yapılan (C-594/12) başvurular birleştirilmiştir. Başvurucular, Federal Kanun'a (*Bundesgesetz*) 2006/24 sayılı AB Direktifi gereği ek yapılan Telekomünikasyon Kanunu (*Telekommunikationsgesetz*) 102a paragrafının temel hak ve özgürlüklerini ihlal ettiği iddiasına dayanmaktadır.

¹⁴⁶ *Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl ve diğerleri*, para. 19.

¹⁴⁷ *Digital Rights Ireland Ltd.*, para. 58.

¹⁴⁸ *Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl ve diğerleri*, para. 20.

¹⁴⁹ *Digital Rights Ireland Ltd.*, para. 51.

yaşamına saygı, kişisel verilerin korunması hakkı ve ifade ve haber alma özgürlüğü maddeleriyle bağdaşmadığını ileri sürerek hükümsüz olarak yorumlamıştır¹⁵⁰.

2. Türk Hukukunda Durum

PVSK ek m. 7/2 ve Jandarma Kanunu ek m. 5/1 uyarınca polisin ve jandarmanın; telekomünikasyon yoluyla iletişimin tespiti, dinlenmesi, sinyal bilgilerinin değerlendirilmesi ve kayda alınması yetkisi mevcuttur. Ayrıca telekomünikasyon yoluyla yapılan iletişim veya internet bağlantı adresleri ve internet kaynakları arasındaki veri trafiği ile iletilen veriler tespit edilebilir, dinlenebilir, sinyal bilgileri değerlendirilebilir, kayda alınabilir. Telekomünikasyon, Ceza Muhakemesi Kanununda Öngörülen Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmelik'te *işaret, sembol, ses ve görüntü ile elektrik sinyallerine dönüştürülebilen her türlü verinin; kablo, telsiz, optik, elektrik, manyetik, elektromanyetik, elektro kimyasal, elektro mekanik ve diğer iletim sistemleri vasıtasıyla iletilmesi, gönderilmesi ve alınması* olarak tanımlanmıştır¹⁵¹. İletişimin kayda alınması uygun bir teknik araçla eş zamanlı olarak konuşmanın kaydedilmesidir, konuşma el yazısı ile not edildiğinde bu iletişimin kaydedilmesi olmayacaktır¹⁵². Nitekim Kolluk ve Ceza Adaleti Direktifi bağlamında değerlendirme yapılabilmesi için de iletişimin kaydedilmesi suretiyle veri işlemenin kısmen veya tamamen otomatik araçlarla işlenmesi veya veri kayıt sisteminin parçası olması gerekmektedir. Sinyal bilgilerinin değerlendirilmesi ise iletişim içeriğine herhangi bir müdahale söz konusu olmaksızın sinyal verilerinin iletişim sistemlerinde bıraktıkları izlerin tespiti ve bunlardan bir sonuca varılmasıdır¹⁵³.

¹⁵⁰ *Digital Rights Ireland Ltd.*, para. 73.

¹⁵¹ 26434 sayılı RG'de 14.02.2007'de yayımlanan bu Yönetmelik (İletişimin Denetlenmesi Yönetmeliği), CMK kapsamındaki koruma tedbirlerinde Adalet Bakanlığının düzenleme yetkisinin olmadığı ve yargılama usulünde idarenin yasamanın fonksiyonunu gasp ettiği gerekçesiyle Danıştay Onuncu Dairesi'nin 09.03.2017 tarihli ve E. 2012/1001, K. 2017/1361 sayılı kararı ile iptal edilmiştir.

¹⁵² Yüksel, **a.g.e.**, s. 155; Ersan Şen, **Türk Hukukunda Telefon Dinleme, Gizli Soruşturmacı, X Muhbir**, 5. Baskı, Ankara, Seçkin Yayıncılık, 2011, s. 84.

¹⁵³ İletişimin Denetlenmesi Yönetmeliği m. 4/1.

Öncelikle polise ve jandarmaya tanınan bu yetkinin istihbarat faaliyeti çerçevesinde mi önleyici kolluk faaliyeti çerçevesinde mi olduğu tespit edilmelidir. Zira suçu önleyici bir faaliyet olarak bu yetki kullanılıyorsa, bu yetkilerin kullanılması sonucu elde edilen kişisel verilerin korunması için Kolluk ve Ceza Adaleti Direktifi uygulanacaktır. Ancak Türkiye’de meri hukuk bakımından önleyici kolluk ya da istihbarat faaliyetleri gereği işlenen kişisel veriler korunaksızdır. Zira KVKK m. 28/1-ç gereği ulusal güvenlik ve suçların önlenmesi gereği veri işlemler KVKK hükümlerine tabi değildir¹⁵⁴.

a. İletişimin Denetlenmesinde Önleyici Kolluk ve İstihbari Kolluk Faaliyeti Ayrımı

Türkiye’de istihbarat faaliyetleri; MİT Kanunu’na dayanmaktadır ve MİT, Emniyet Genel Müdürlüğü ve Jandarma Genel Komutanlığı tarafından yürütülmektedir. Emniyet ve jandarma birimleri tarafından yürütülen istihbarat faaliyeti suçun önlenmesi amacıyla iken, MİT tarafından yürütülen istihbarat faaliyeti ise iç ve dış güvenliğin sağlanmasına yönelik olup daha geniş çaplıdır¹⁵⁵.

PVSK’da emniyet birimlerine devlet güvenliği, Anayasal düzen ve genel güvenlik konularında önleyici ve koruyucu tedbirler alma, emniyet ve asayiş

¹⁵⁴ Bu hüküm kişisel verileri bir hayli korumasız bırakmaktadır. Nitekim bu, kanun koyucu tarafından da görülmüştür ki MİT Kanunu uyarınca Güvenlik ve İstihbarat Komisyonu’na güvenlik ve istihbarat hizmetleri sırasında elde edilen kişisel verilerin güvenliğini ve bireyin hak ve özgürlüklerini koruyucu öneriler geliştirmek görevi yüklenmiştir. Bkz. MİT Kanunu m. 2/4-d; Maddenin AY’ye aykırı olduğu iddia edilmişse de AYM aykırılık iddiasını reddetmiştir. AYM değerlendirmesinde 108 sayılı Sözleşme m. 9’u emsal göstererek devletin güvenliği, kamu güvenliği, suçla mücadelede kişisel verilerin kullanılması durumunda bu hakka sınırlandırmanın mümkün olduğunu belirtmiştir. AYM; kamu güvenliği, milli güvenlik, kamu düzeni gibi kavramların belirsiz ve soyut olmasının; kuralın belirsiz ve soyut olduğu anlamına gelmediğini vurgulamış ve bu durumun kanun yapma tekniğinden kaynaklandığını belirtmiştir. Detaylı değerlendirme için bkz. Bahri Öztürk, Elif Altınok Çalışkan, “Kişisel Verilerin Korunması Kanunu Hakkında Genel Değerlendirmeler ve Anayasaya Aykırılık Sorunu”, **Fasikül Hukuk Dergisi**, c. 10, s. 100, 2018, s. 288-290; Bu faaliyetler çerçevesinde işlenen kişisel verilerin KVKK’nin uygulama alanında bulunmaması AB İlerleme Raporları’nda da eleştirilmiştir. Bkz. AB-Türkiye İlerleme Raporu 2016, Çevrimiçi https://www.ab.gov.tr/files/ceb/Progress_Reports/2016_ilerleme_raporu_tr.pdf 16.03.2020, s. 78; AB-Türkiye İlerleme Raporu 2018, Çevrimiçi https://www.ab.gov.tr/siteimages/pub/komisyon_ulke_raporlari/2018_turkiye_raporu_tr.pdf 16.03.2020, s. 44; AB-Türkiye İlerleme Raporu 2019, Çevrimiçi https://www.ab.gov.tr/siteimages/birimler/kpb/2019_trkiye_raporu-tr.pdf 16.03.2020, s. 35.

¹⁵⁵ Zülküf Bayındır, “Özel Yaşamın Korunması Çerçevesinde İstihbarat Faaliyetleri”, **Bahçeşehir Üniversitesi Sosyal Bilimler Enstitüsü**, Yayımlanmamış Yüksek Lisans Tezi, İstanbul, 2016, s. 64.

sağlamak üzere istihbarat faaliyetlerinde bulunma yetkisi verilmiştir¹⁵⁶. Jandarmaya tanınan istihbarat faaliyetlerinde bulunma yetkisi ise Jandarma Kanunu'na dayanmaktadır. Jandarma; emniyet ve asayiş, kamu düzeni, kaçakçılığı men, takip ve tahkik, suç işlenmesini önlemek için ceza ve infaz kurumları ve tutukevlerinin dış korumalarını yapmak gibi belirli alanda görevlerini yerine getirmek üzere istihbarat faaliyetlerinde bulunabilecektir. Yani jandarmanın istihbarat faaliyet alanı emniyet birimlerinden daha sınırlıdır¹⁵⁷.

İstihbarat faaliyeti gereği iletişimin denetlenmesi, adli ve önleme amaçlı iletişimin denetlenmesinden daha esnek şartlara sahiptir. Ancak istihbarat gereği denetlemede de önlenmesi amaçlanan suçlar sınırlı sayı prensibince belirlenmiştir. İstihbarat faaliyeti gereği iletişimin denetlenmesine; katalog suçların işlenmesi bakımından kuvvetli şüphe ve klasik bilgi toplama araçlarının yeterli olup olmadığına dair bir değerlendirme yapılmaksızın başvurulabilecektir. Doktrinde isabetli olarak klasik suç önleme yöntemlerinin olayda uygulanmasının yetersiz kalacağına ilişkin yapılacak bir değerlendirmenin ardından ikincil olarak istihbarat gereği iletişimin denetlenmesine başvurulması gerektiği ileri sürülmüştür¹⁵⁸.

PSVK gereği, yalnız örgüt faaliyeti çerçevesinde işlenen uyuşturucu veya uyarıcı madde imal ve ticareti suçu, haksız ekonomik çıkar sağlamak amacıyla kurulmuş bir örgütün faaliyeti çerçevesinde cebir ve tehdit uygulanarak işlenen suçlar ve TCK'de sayılan devletin güvenliğine karşı suçlardan bazılarının önlenmesi amacıyla iletişim denetlenebilecektir. Böyle bir hüküm, kapsamın sınırlandırılması bakımından isabetlidir. Ancak PVSK, bu tedbirin uygulanacağı kişiler bakımından herhangi bir sınırlama yapmamıştır. Bu demektir ki herkes bu tedbirlerin muhatabı olup herkesin kişisel verileri işlenebilecektir. En azından tanıklıktan çekinebilecek kişiler arasında ve kişi ve müdafî olabilecek avukat arasındaki iletişim denetlenmemelidir¹⁵⁹.

¹⁵⁶ PVSK ek m. 7.

¹⁵⁷ Bayındır, **a.g.e.**, s. 84.

¹⁵⁸ Bkz. Fatih Birtok, "İstihbarat Amacıyla İletişim Özgürlüğüne Müdahale Edilmesi ve Müdahaleden Elde Edilen Materyallerin Delil Olarak Kabul Edilebilirliği", **CHD**, c. 6, s. 16, Ağustos 2011, s. 111.

¹⁵⁹ Yüksel, **a.g.e.**, s. 166; *Birtok*'e göre henüz bir suç şüphesi olmaksızın başvurulmuş bu istihbari tedbirlerde CMK'nin aksine şüpheli/sanık gibi bir ayırım yapılmadığından potansiyel olarak herkesin muhatap olması isabetlidir. Birtok, **a.g.e.**, s. 112.

PVSK uyarınca tedbirin sona ermesi halinde dinlemenin içeriğine ilişkin kayıtlar en geç on gün içinde yok edilecektir¹⁶⁰. Ancak maddede sona eren tedbire ilişkin tedbirin uygulandığı kişiye bildirim yapılacağına dair bir düzenleme bulunmamaktadır. Bu da hukuka aykırı bir dinleme halinde kişinin idari bir işlem olan dinlemeye karşı kanuni haklarını kullanmasına engel olmakta ve Anayasa m. 125 ile bağdaşmamaktadır. Ayrıca bilgilendirilme hakkının öngörüldüğü Kolluk ve Ceza Adaleti Direktifi'nin gerekleri ile de bağdaşmamaktadır. Oysa adli amaçlı iletişimin denetlenmesinde CMK m. 137/3 ve 4 gereği veri sahibine bildirim yapılmaktadır. Kanaatimizce CMK'de veri sahibine tanınan bu hak, PVSK gereği yapılan dinlemenin muhatabına da tanınmalıdır. Bu bildirimin yapılmasının PVSK'deki önleyici dinlemenin amacı ile bağdaşmadığı ve tedbirin amacını tehlikeye düşürebileceği düşünülebilir. Ancak buna her somut olay nezdinde değerlendirme yapılarak karar verilmelidir. Oysa mevcut düzenlemeye göre amaçla bağdaşıp bağdaşmadığı gözetilmeksizin bildirim yapılmamaktadır¹⁶¹.

İletişimin denetlenmesi tedbiri üç ay için başvurulabilecek bir tedbir olup üçer ayı geçmeyecek şekilde en fazla üç defa uzatılabilecekken, terör örgütünün faaliyeti çerçevesinde devam eden tehlikelere ilişkin olarak uzatma kararı müteaddit defalar verilebilecektir¹⁶². Yani terör örgütü faaliyeti çerçevesinde devam eden tehlike gerekçesine dayanarak bir üst sınıra tabi olmaksızın devamlı iletişimin denetlenebileceğine izin veren bu hüküm oldukça sakıncalıdır¹⁶³.

b. Kaybolan Çocukların Bulunması Amacıyla İletişimin Denetlenmesi

PVSK m. 13/A'ya göre kaybolan çocukların bulunması amacıyla polis; sulh ceza hakiminin kararı veya gecikmesinde sakınca bulunan hallerde mülki idari amirin yazılı ya da sözlü emriyle kayıp çocuk ya da çocuğun kullandığı ancak başkasına ait

¹⁶⁰ PVSK ek m. 7/2.

¹⁶¹ *Klass ve diğerleri v. Almanya* kararında da AİHM, iletişimin denetlenmesi tedbirinden sonra kişilerin bilgilendirilmesinin gerekip gerekmediğini her bir somut olay bakımından değerlendirmek gerektiğini ve bazı durumlarda bu bilgilendirmenin yapılmamış olmasının ihlal olarak değerlendirmemiştir. Bkz. Birtek, **a.g.e.**, s. 122.

¹⁶² PVSK ek m. 7/4.

¹⁶³ Birtek, **a.g.e.**, s. 116.

olan her türlü banka hesap hareketlerini değerlendirme, telekomünikasyon yoluyla iletişimi denetleme veya sinyal bilgilerini değerlendirme yetkisine sahiptir¹⁶⁴. Bu hüküm her ne kadar veri sahibinin kişisel verilerinin korunması hakkına müdahale teşkil etse de veri sahibine Kolluk ve Ceza Adaleti Direktifi uyarınca bilgilendirme, erişme gibi haklar tanınması halinde hukuka uygundur. Zira üstün bir menfaat olarak kayıp çocuğun bulunması amaçlanmaktadır.

E. Teknik Araçlarla İzleme

PVSK ek m. 7/6 ve Jandarma Kanunu ek m. 5/5'e göre maddede belirtilen katalog suçların önlenmesi amacıyla polisin ve jandarmanın teknik araçla izleme yetkisi bulunmaktadır. Ancak her iki düzenlemelerde de izleme haricinde kayıt yapılacağı öngörülmemiştir, dolayısıyla polis ve jandarma önleyici amaçla yalnız izleme yapabilecektir, kayıt yapamayacaktır¹⁶⁵. Bu tedbir bakımından herhangi bir süre sınırı ya da tedbir sona erdikten sonra kişinin bilgilendirilip bilgilendirilmeyeceği öngörülmemiştir. Bu türden bir hükmün olmaması, veri sahibinin bilgilendirilme hakkı ve hukuka aykırı şekilde bu tedbire başvurulmuşsa diğer haklarını kullanmasına engel teşkil etmektedir. Ayrıca bir üst süre olmaksızın kişinin izlenebilmesine izin veren mevzuat, kişisel verilerin korunması ve özel yaşamın gizliliğine saygı hakkına ölçüsüz bir müdahaledir¹⁶⁶.

F. Banka Hesaplarının İncelenmesi

*M.N. ve diğerleri v. San Marino*¹⁶⁷ başvurusunda AİHM, özel nitelikli veri olup olmadığı ayrımı aramaksızın bankacılık belgelerinin kişisel veri olduğuna hükmetmiştir. Almanya'da Kredi Bankacılık Kanunu (*Kreditwesengesetz*) 24c hükmü ile terörizmle bağlantılı para hareketleri hakkında yapılacak banka denetim faaliyeti

¹⁶⁴ Bu hüküm, 06.01.2017 tarihli Resmi Gazete'de yayımlanan 680 sayılı KHK m. 26 ile PVSK'ye eklenmiştir.

¹⁶⁵ Şen, **a.g.e.**, s. 80.

¹⁶⁶ Bu nedenle *Özbek/Doğan/Bacaksız* önleme amaçlı dinlemeye ilişkin sürenin kıyasen önleme amaçlı teknik araçla izlemeye de uygulanması gerektiğini savunmuştur. Bkz. *Özbek, Doğan, Bacaksız, a.g.e.*, s. 169.

¹⁶⁷ *M.N. ve diğerleri v. San Marino*, B. No: 28005/12, 26.04.2012, Çevrimiçi <https://hudoc.echr.coe.int/> 29.03.2020.

ile banka hesaplarına ilişkin kayıtların otomatik olarak Alman Federal Finansal Hizmetler Kurumuna iletilmesi sağlanmıştır. Ayrıca Swift verilerinin kolluk ve adli makamlarla paylaşılması da özellikle ekonomik suçların önlenmesi amacıyla hizmet etmektedir. Bu amaçla örneğin; ABD Hazine Departmanı Swift'ten¹⁶⁸ iki yüz kırk bir veri kabul etmiş ve bu verileri CIA, FBI ve diğer devlet kurumlarının erişebildiği veri tabanında toplamıştır. WP29, 10/2006 sayılı Karar'ında Swift'i veri sorumlusu olarak nitelendirmiştir. Bu niteliği dolayısıyla normal güvenli mesaj hizmeti sunan ve talep edilen verileri işleyen Swift, verilerin ABD'ye aktarımından 95/46 sayılı Direktif hükümlerine göre sorumlu tutulmuştur¹⁶⁹.

II. CEZA MUHAKEMESİ İŞLEMLERİ

A. Fizik Kimliğinin Tespiti

Fizik kimliği tespit edilirken kişinin biyometrik verileri ve/veya fotoğraflarından yararlanılmaktadır. Kolluk ve Ceza Adaleti Direktifi uyarınca önleyici kolluk faaliyetleri sırasında işlenecek veriler ile ceza muhakemesi sırasında işlenecek kişisel veriler aynı korumadan yararlandığından önceki bölüme atıf yapmakla yetinmekteyiz¹⁷⁰.

Fizik kimliğinin tespiti, CMK m. 81'e göre üst sınırı iki yıl veya daha fazla olan suçlarda şüpheli veya sanığın tespiti amacıyla başvurulmuş bir yöntemdir. Kişinin kimliğinin belirlenebilmesi için fotoğrafı çekilebilir, parmak izi alınabilir veya ses ve görüntüleri kaydedilebilir. Doktrinde kovuşturmayla yer olmadığı kararı ile beraat ve ceza verilmesine yer olmadığı kararının kesinleşmesi hallerinde fizik kimliğinin tespiti sonuçlarının yok edilmesi ve CMK m. 80/2 moleküler genetik inceleme sonuçlarının yok edilmesi hükümlerinin hatalı olduğu ileri sürülmüştür. Bu görüşe göre sonradan

¹⁶⁸ Swift, finans kurumları (banka, komisyoncu, yatırım danışmanı firmalar vs.) arasında iki yüzden fazla ülkede güvenli mesaj hizmeti sunan Belçikalı bir şirkettir.

¹⁶⁹ İkbal Gür, **Kişisel Verilerin Korunması Hususunda AB ile ABD Arasında Çıkan Uyuşmazlıklar ve Çözüm Yolları**, Ankara, Turhan Kitabevi, 2010, s. 260.

¹⁷⁰ Bkz. "Biyometrik Veri İşleme" başlıklı bölüm.

inceleme gerekebileceğinden verilerin yok edilmesi yerine saklanması gerekir¹⁷¹. Ancak hakkında yürütülen ceza muhakemesi sona eren ve suçu işlemediği anlaşılan kişinin verilerinin tutulmaya devam etmesi kanaatimizce artık amaçla bağlılığa hizmet etmediğinden isabetsiz olacaktır, mevcut düzenleme veri koruma hukuku gereklerine daha uygundur.

B. Genel Bilgi Toplama (GBT)

1. Tanım

GBT sistemi, hakkında yakalama, tutuklama, yurt dışına çıkma yasağı olan veya yakalanmışsa da hakkında kovuşturma yürütülen kişilerin kaydının tutulduğu sistemdir¹⁷². GBT sorgusu PVSK m. 4/A uyarınca yapılmaktadır. Kayıtlar; 29.03.2005 tarihli Kaçakçılık, İstihbarat, Harekât ve Bilgi Toplama Yönergesi uyarınca İçişleri Bakanlığına bağlı KİHBİ Daire Başkanlığı tarafından tutulmaktadır. Yönerge'nin dayanağı 3152 sayılı İçişleri Bakanlığı Teşkilat ve Görevleri Hakkında Kanun m. 13/1-c ve m. 33, PVSK ek m. 7 ve Jandarma Teşkilatı Görev ve Yetkileri Yönetmeliği m. 42/1-f bendi olarak belirtilmiştir. Ancak Yönerge *hizmete özel gizlilik derecesi* taşıdığı için Resmi Gazete'de yayımlanmamıştır¹⁷³. GBT kaydı tutma yetkisi, KİHBİ Daire Başkanlığına *suç işleyip ele geçmeyen kişilerin, çalınan veya kaybedilen motorlu taşıtların, ateşli silahların, kimliği ispata yarayan her türlü belgelerin kayıtlarını tutarak güvenlik kuvvetlerine bildirmek, görevli kuruluşlarla ilgili koordinasyon sağlamak* ¹⁷⁴ amacıyla, yani suç işleyip ele geçirilemeyen kişilerin kaydedilmesi amacıyla verilmiştir¹⁷⁵.

GBT kayıtları; kolluk güçlerinin yürüttüğü suçlulukla mücadelede, silah ruhsatı, sürücü belgesi ve pasaport işlemleri, kamu hizmetlerinden menin takibinde,

¹⁷¹ Yener Ünver, Hakan Hakeri, **Ceza Muhakemesi Hukuku**, c. 1, 15. Baskı, Ankara, Adalet Yayınevi, 2019, s. 608.

¹⁷² İbrahim Çiçek, "GBT (Genel Bilgi Toplama) Kayıtlarının Silinmesi", **Terazi Hukuk Dergisi**, c. 8, s. 88, 2013, s. 45.

¹⁷³ Yönerge yayımlanmadığı için bu bilgiler, Çiçek, **a.g.e.**, s. 45 ve *E.Ç.A. Başvurusu* [GK], B. No: 2014/5671, 07.06.2018, para. 22'den alınmıştır (Çevrimiçi <https://www.anayasa.gov.tr/tr/kararlar-bilgi-bankasi/> 29.03.2020).

¹⁷⁴ Bkz. 3152 sayılı Kanun m. 13/1-c.

¹⁷⁵ *E.Ç.A.*, Hasan Tahsin Gökcan ve Yusuf Şevki Hakyemez'in Karşı Oyu, para. 8.

Güvenlik Soruşturması Kanunu ile Güvenlik Soruşturması ve Arşiv Araştırması Yönetmeliği uyarınca güvenlik soruşturması ve arşiv araştırmasında kullanılmaktadır¹⁷⁶.

GBT sisteminde kişiler hakkında bilgi formları düzenlenmektedir. Sistemde yakalama emri, tutuklama kararı, Yönerge m. 9/b kapsamındaki suçlarda yakalama kararı yerine getirilmişse de kişinin kaydı, belirli hakları kullanmaktan yoksun bırakılan kişilerin kaydı, çalınan, kaybedilen araç kayıtları, asker kaçağı ve bakaya kaydı yer alır. GBT sisteminde yer alan bu veriler güncel olmalıdır ve güncel olmayan veriler silinmelidir. GBT kaydı tutulan kişi de kesinleşmiş mahkeme hükmü veya kovuşturmayaya yer olmadığı kararı ile KİHBİ Daire Başkanlığına dilekçe ile başvurarak kaydının silinmesini talep edebilecektir¹⁷⁷.

Kişinin GBT kaydına konu olan yakalama emri veya tutuklama kararı, KİHBİ Yönergesi m. 9/b kapsamında olan suçlardan dolayı ise kayıt silinmemektedir. Bu kapsamdaki suçla ilgili kişi hakkında tutuklama kararının kaldırılması veya yakalama emrinin iptali kaydın muhafazasına engel değildir. Yönerge m. 9/b kapsamındaki suçları işleyenler hakkında verilen beraat, ceza verilmesine yer olmadığı ve düşme kararının kesinleşmesi halinde kişi hakkında tutulan bilgi formu iptal edilir¹⁷⁸. Kişinin bu kapsamdaki suçlar nedeniyle hükümlü olması halinde ise bilgi formu ancak ölüm veya gaiplik kararı üzerine iptal edilir¹⁷⁹. Ancak hakkında kayıt tutulan kişi, kayda konu suçu işlediği anda on sekiz yaşından küçükse ve yargılama sonunda mahkûm olmuşsa beş yıl boyunca m. 9/b kapsamındaki suçlardan birini işlemediğinde kaydı silinebilir.

GBT kaydı, Yönerge m. 9/b kapsamında olmayan suçlardan dolayı tutulmuş ise kişinin yakalanması ile kayıt iptal edilir¹⁸⁰. Hakkında kovuşturmayaya yer olmadığı kararı verilen veya yargılama sonunda beraat kararı verilen kişinin kaydı, savcılık ve mahkemenin KİHBİ sistemindeki formu doldurup kolluk makamlarına havale etmesi

¹⁷⁶ E.Ç.A., para. 23.

¹⁷⁷ Çiçek, a.g.e., s. 46.

¹⁷⁸ Çiçek, a.g.e., s. 46.

¹⁷⁹ Çiçek, a.g.e., s. 46.

¹⁸⁰ Çiçek, a.g.e., s. 45.

ile silinmektedir¹⁸¹. Dolayısıyla yargı makamları ve kolluk arasında GBT kaydının silinmesi ve verinin güncel olarak tutulması için koordinasyon sağlanmalıdır. Örneğin; Danıştay kararına konu olan bir olayda kişinin hakkında verilen hükmün kesinleşmiş ve infaz edilmiş olmasına rağmen GBT sistemindeki yakalama emrine ilişkin kaydı silinmediği için kişi pek çok defa gözaltına alınmıştır ve sürücü ehliyeti alamamaktadır. Danıştay, yakalama emrinin geri alınmaması ve infaz edilen hapis cezasının emniyet birimlerine bildirilmemiş olması biçimindeki emniyet ile savcılık arasındaki koordinasyonsuzluğu sebebiyle idarenin sorumluluğu olduğuna hükmetmiştir¹⁸².

2. Hukuka Uygunluk Değerlendirmesi

Kanaatimizce GBT kayıtlarının tutulması kanunilik ilkesinin gereklerini sağlamadığından hukuka aykırıdır. Zira Yönerge'ye dayanak olarak gösterilen 3152 sayılı Kanun'un ilgili hükümleri ilga edilmiştir. PVSK ek m. 7'de polisin bilgi toplama yetkisi mevcut olsa da GBT sistemi ile kişisel veri işleme söz konusu olduğundan, veri işlemenin usul, esasları, verilerin tutulma süresi ve hukuka aykırı veri işleme halinde veri sahibinin hakları ve başvuracağı makamlar maddede belirtilmemiştir. GBT sisteminin düzenlendiği yegâne hukuki düzenleme olan Yönerge ise Resmi Gazete'de yayımlanmadığından ulaşılabilir değildir. Dolayısıyla GBT kaydı ile kişisel veri işleme hukuka aykırı olup kişisel verilerin korunması hakkını ihlal etmektedir.

AYM kararına konu bir başvuruda, 1989 yılında işlediği hırsızlık suçları nedeniyle 1990 yılında hakkında adli para cezasına hükmedilen başvurucunun adli sicil kaydı silinmiştir. Ancak GBT kaydı hala GBT sisteminde tutulmaktadır. Başvurucu uzun yıllar geçmesine rağmen kaydın silinmemesinin, polis kontrollerinde kendisine tutumun değişmesine yol açtığını ve özel yaşama saygı hakkının ihlal edildiğini ileri sürmüştür¹⁸³. AYM; kanunilik, meşru amaç ve demokratik toplumda

¹⁸¹ Çiçek, **a.g.e.**, s. 46.

¹⁸² Danıştay 10. Daire E. 2007/1376 K. 2007/4756, 17.10.2007 Çevrimiçi <http://www.kazanci.com/kho2/ibb/giris.html> 30.03.2020. İdarenin elindeki kişisel verileri güncellememesi ve silinmesi gereken veriyi silmemesi hizmet kusurudur. Bkz. Halil Altındağ, "Kişisel Verilerin Korunması Bağlamında İdarenin Sorumluluğu", **İKÜHFD**, c. 18, s. 2, 2019, s. 393.

¹⁸³ E.Ç.A., para. 37.

gerekli ve ölçülü olma cihetinden yaptığı incelemede GBT kaydının bu kadar uzun süre tutulmasının özel yaşama saygı hakkını ihlal etmediği sonucuna varmıştır. Oysa yukarıda belirttiğimiz gibi, GBT sistemi ile veri işleme kanuna dayanmayan bir idari faaliyet olup kişisel verilerin korunmasına aykırıdır. Ancak AYM, bu değerlendirmeyi yapmayıp *Bülent Kaya* başvurusuna atıf yapmakla yetinmiştir¹⁸⁴. Ancak karşı oyda belirtildiği üzere; kişinin bu denli hassas verisinin, veri işlemeye neden olan hırsızlığın üzerinden yirmi beş yıl gibi bir zaman geçmiş olmasına rağmen hâlâ olağan bir trafik kontrolünde karşısına çıkması ölçülü değildir. Verilerin saklanma süresi, silinme şartları ve bu verileri inceleyebilecek kişiler açık ve öngörülebilir düzenlemeye dayanmamaktadır¹⁸⁵. Kararda yer almasa da kanaatimizce unutulma hakkı perspektifinden de başvuru değerlendirilmelidir. Zira kişi hakkında adli sicil kaydı dahi silinebilirken GBT kayıtlarının silinmemesi unutulma hakkı ile bağdaşmamaktadır. GBT kaydına konu suç nedeniyle kişi adli para cezasına mahkûm edilmiş ve cezanın infazı üzerinden yirmi beş yıl geçmiştir, ancak kayıtlar tutulmaya devam etmektedir.

¹⁸⁴ E.Ç.A., para. 49; *Bülent Kaya* başvurusunda (B. No: 2013/2941, 11.05.2016) başvuru hakkında Van Ağır Ceza Mahkemesi'nde derdest ceza yargılaması bulunmaktadır. Van Devlet Güvenlik Mahkemesi Cumhuriyet Savcılığınca terör örgütüne yardım ve yataklık etme suçu kapsamında yürütülen soruşturmada KİHBİ Bilgi Toplama Yönergesi'ne göre başvurucuya ilişkin bilgi formu düzenlenip GBT kapsamına alınmıştır. Başvurucu ise GBT sisteminde yer alan kişisel verilerinin silinmesini idareden talep etmiş; ancak idare, söz konusu derdest yargılamaya ilişkin verinin Bilgi Toplama Yönergesi m. 9/b kapsamındaki suçlarla ilgili olduğu ve bu kaydın ancak başvurucağının beraati veya dava zamanaşımının tamamlanması ile silinebileceği gerekçesiyle bu talebi reddetmiştir. Başvurucu hakkında tanzim edilen bu formun ne kadar süre ile tutulacağı ve silineceğine ilişkin bir hüküm bulunmamaktadır. Bu nedenle başvurucağı özel yaşamın gizliliği hakkının ihlal edildiğini ileri sürmüştür.

AYM'ye göre PVS ek m. 7'ye göre istihbarat faaliyetlerinin gereği olarak bilgi toplama, yetkili mercilerle bilgileri paylaşma mümkündür. Dolayısıyla kanunilik şartı sağlanmıştır. Meşru amaç bakımından kamu düzeni ve kamu güvenliğinin sağlanması da mevcuttur. AYM, başvuruda belirli suçlar bakımından yapılan derdest yargılamaya ilişkin bilginin GBT sistemine kaydı ve bunun paylaşılmasını kamu düzeni ve güvenliği bakımından elzem görmüş ve güvenlik soruşturmaları başta olmak üzere kullanım amaçlarına da bakıldığında özel yaşamın gizliliği hakkının ihlali mahiyetinde bulmamıştır. Ancak kanaatimizce karara ilişkin karşı oyda da (Bkz. *Bülent Kaya*, Engin Yıldırım'ın Karşı Oyu, para. 13) belirtildiği gibi AİHS sisteminde müdahalenin öngörülebilir olma şartı bulunmaktadır. Ancak Yönerge hizmet gerekçe gösterilerek yayımlanmamıştır, dolayısıyla verilerin ne süre için tutulacağı, kullanılacağı, kimler tarafından verilere erişilebileceği öngörülebilir değildir. E.Ç.A. ve *Bülent Kaya* başvuruları hakkında detaylı inceleme için bkz. Naciye Betül Haliloğlu, "Yargılamaya ve Mahkûmiyete İlişkin Verilerin Genel Bilgi Toplama (GBT) Sisteminde Tutulması: Anayasa Mahkemesinin Bülent Kaya ve E.Ç.A. Kararlarının Avrupa İnsan Hakları Mahkemesi İçtihatları Işığında Değerlendirilmesi", *Anayasa Yargısı*, c. 36, s. 2, 2019, s. 356 vd.

¹⁸⁵ E.Ç.A., Osman Ali Feyyaz Paksüt ve Muammer Topal'ın Karşıoyu, para. 3; Hasan Tahsin Gökcan ve Yusuf Şevki Hakyemez'in Karşı Oyu, para. 7-9.

Kamu Denetçiliği Kurumuna yapılan bir başvuruda da başvuru hakkında, 6136 sayılı Kanun uyarınca ruhsatsız ateşli silahlarla mermileri satın alma veya taşıma veya bulundurma suçundan adli para cezasına hükmedilmiştir. Cezanın infazından on yıl sonra adli sicil kaydı silinmesine rağmen başvuru kişinin GBT kaydı silinmemiştir. Başvuru kişisi yaşadığı yer olan Diyarbakır'da terör olayları nedeniyle yapılan GBT araştırmalarında kaydı görüldüğü için potansiyel suçlu olarak damgalandığını belirtmiş ve GBT kaydı yapılmasının herhangi bir kanuni dayanağı olmadığını vurgulamıştır¹⁸⁶. Kamu Denetçiliği Kurumu kararında İçişleri Bakanlığına GBT kayıtlarının tutulacağı süre, kullanımı ve üçüncü kişilerin bu kayıtlara erişimi konusunda kanun düzeyinde mevzuat çalışması yapılmasını tavsiye etmiştir¹⁸⁷.

Kamu Denetçiliği Kurumu GBT kayıt işleminin özel yaşam kapsamında kanuna uygun bir müdahale olup olmadığına dair değerlendirmesinde AİHM'nin *Shimovolos v. Rusya* kararına da değinmiştir. Bu karara konu olayda Gözetim Veri Tabanı'nda kaydı bulunan başvuru kişisi, seyahatlerine ilişkin verilerin polis tarafından toplanmasının özel yaşamın gizliliğini ihlal ettiğini ileri sürmüştür. Zira Gözetim Veri Tabanı gizlilik gerekçesiyle yayımlanmamış bir bakanlık talimatı ile oluşturulmuştur¹⁸⁸. AİHM'nin bu kararında esnek olan ve bağlayıcı etkisi bulunmayan idari nitelikteki düzenlemelerin kamuya açık olmaması halinde, ulaşılabilir ve öngörülebilir bir hukuki düzenlemeden bahsedilemeyeceği belirtilmiştir¹⁸⁹. Bu nedenle Mahkeme, kişilerin Gözetim Veri Tabanı'na kaydının özel yaşamın gizliliğini ihlal ettiğine hükmetmiştir.

Sonuç olarak ilgili AYM ve AİHM kararları ışığında gizlilik gerekçesiyle yayımlanmamış bir yönergeye dayanarak GBT kaydının tutulması, kişisel verilerin korunması hakkına ciddi anlamda bir müdahale teşkil etmektedir. Veri işlemeye neden olan tutuklama kararı veya yakalama emri ortadan kalkmasına rağmen kaydın

¹⁸⁶ Kamu Denetçiliği Kurumu, B. No: 2017/9518, 29.01.2018, para. 1, Çevrimiçi <https://www.ombudsman.gov.tr/wp-content/uploads/2018/03/2017-9518-Ba%C5%9Fvuran%C4%B1n-GBT-kayd%C4%B1n%C4%B1n-silinmesi-talebi-hakk%C4%B1nda.pdf> 23.03.2020.

¹⁸⁷ Kamu Denetçiliği Kurumu, "Karar".

¹⁸⁸ *Shimovolos v. Rusya*, B. No: 30194/09, 28.11.2011, para. 60 Çevrimiçi <https://hudoc.echr.coe.int/> 29.03.2020.

¹⁸⁹ *Shimovolos v. Rusya*, para. 69-70.

tutulmaya devam etmesi, veri işlemede amaçla bağlılık ilkesi ile bağdaşmamaktadır. Ayrıca hükümlü kişi hakkında arşiv kaydı dahi Adli Sicil Kanunu m. 12'ye göre belirli bir süre ile sınırlı olarak tutulurken GBT kaydının kişinin ölümüne kadar tutulması izaha muhtaç olup sürelilik ilkesi ile de bağdaşmamaktadır¹⁹⁰.

C. Beden Muayenesi, Vücuttan Örnek Alınması ve Moleküler Genetik İnceleme

1. Tanım

Olay yeri inceleme veya beden muayenesinin ardından vücuttan alınan örnekler moleküler genetik incelemeye tabi tutulmaktadır¹⁹¹. Genetik inceleme kişinin genetik özelliklerinin belirlenmesine hizmet eden bir yöntemdir¹⁹². Suçla mücadele ve adli tıpta bireylerin teşhisine olanak tanıyan bir yöntem olarak genellikle DNA parmak izi yöntemine başvurulmaktadır. Kan hücresi ve cilt yüzeyindeki hücreler hariç saç teli, tükürük gibi değişmez ve kişisel olan DNA örnekleri toplanmaktadır. DNA ise kan, kıl, tükürük, mukoza akıntısı, ter, meni, idrar, doku parçası, kemik doku, kepek ve deri döküntüleri gibi parçalarda bulunmaktadır¹⁹³. DNA bilgileri taşıyan bu maddeler ile de biyometrik özellik işlenmektedir¹⁹⁴.

DNA verisinin işlenmesine dair ABD'de FBI'nın biyometrik çabalarından biri olan Kombine DNA İndeks Sistemi'ne (CODIS) değinilmelidir. CODIS 1990 yılında tanıtılan ve eyalet, yerli ve yabancı laboratuvarlara DNA örneklerinde yardımcı olmak için kullanılan bir yazılım eşleştirme programıdır. Bir teknisyen CODIS kullanarak, bir ceza soruşturmasıyla birlikte toplanan DNA örneklerini alır ve örnekleri işleme için onaylı bir laboratuvara sunar. Hükümlü ve şüpheli/ sanıklar birden fazla devletin veri tabanından aranabilir. CODIS yazılımının kendisi DNA profilleri içermez. Yazılım,

¹⁹⁰ AYM, E. 2008/44, K.2011/21, 02.01.2011 tarihli iptal kararındaki anlayış gereği GBT kaydının tutulmasının Anayasa'ya aykırı olduğuna dair bkz. Çiçek, **a.g.e.**, s. 47.

¹⁹¹ Ünver, Hakeri, **a.g.e.**, s. 619.

¹⁹² Veli Özer Özbek, "Tıp Ceza Hukukunda DNA İncelemesi", **V. Türk-Alman Tıp Hukuku Sempozyumu**, Ankara, TBB Yayını, 2008, s. 1076.

¹⁹³ Nihal Temizsoy Bayram, "Ceza Muhakemesi Hukukunda Moleküler Genetik İnceleme ve Elde Edilen Verilerin Delil Olarak Kullanılması", **İstanbul Üniversitesi Sosyal Bilimler Enstitüsü**, Yayımlanmamış Yüksek Lisans Tezi, İstanbul, 2018, s. 93.

¹⁹⁴ Keser Berber, Lostar, **a.g.e.**, s. 78.

durum veri tabanlarını eşleşmelerde arama ve eşleşmeyi geri göndermenin ya da kaynak kuruma göndermenin bir yoludur. DNA'nın işlenmesi için ortaya çıkan bir teknoloji de Hızlı DNA (R-DNA) olarak bilinir. R-DNA'nın amacı, iki saatlik toplama içerisinde bir DNA profilinin oluşturulmasıdır. R-DNA, bir laboratuvarın sınırları dışındaki DNA örneklerinin basit ve karmaşık bir şekilde işlenmesini sağlamaktadır¹⁹⁵.

Moleküler genetik inceleme sonucu yapılan kimliklendirme işlemi ile âdeta bireyin *moleküler biyolojik vesikalık resmi* çekilmektedir¹⁹⁶. Ancak belirtilmelidir ki insan bedeninden elde edilen dokular, kişisel veri olmayıp bu doku ve parçaların belirli bir analize tabi tutulması sonucu elde edilen bilgiler kişisel veridir¹⁹⁷. Kolluk ve Ceza Adaleti Direktifi m. 3/12 genetik verileri, *gerçek bir kişinin fizyolojisi veya sağlığı hakkında benzersiz bilgi veren ve özellikle söz konusu gerçek kişiden gelen bir biyolojik örneğin analizinden kaynaklanan, gerçek bir kişinin kalıtsal veya edinilmiş genetik özellikleri ile ilgili kişisel veriler* şeklinde tanımlamıştır¹⁹⁸. Genetik veriler Kolluk ve Ceza Adaleti Direktifi m. 10'a göre özel nitelikli kişisel veridir. Hatta genetik özgücülük (*genetic exceptionalism*) anlayışı¹⁹⁹ gereği genetik veriler, kalıtsal veri içerip kişinin ailevi ilişkileri hakkında da bilgi taşıdığından ve değişmez mahiyette olduğundan özel nitelikli veriler içerisinde de daha incelikli bir korumayı hak etmektedirler.

2. DNA Verilerinden Ceza Muhakemesinde Yararlanılması

Genetik bilgi taşıyan DNA verilerinin işlenmesi, suçların aydınlatılmasına hizmet etmekte iken aynı zamanda verisi işlenen veri sahibinin kişisel verilerinin

¹⁹⁵ Walker, **a.g.e.**, s. 198.

¹⁹⁶ Gülsün Ayhan Aygörmöz Uğurlubay, "Almanya, İsviçre ve Avusturya Hukuku Bağlamında Türk Ceza Muhakemesi Hukukunda Adli DNA Analizleri", **CHKD**, c. 5, s. 2, 2017, s. 50.

¹⁹⁷ Jasserand-Breeman, **a.g.e.**, s. 49; Aygörmöz Uğurlubay, **a.g.e.**, s. 52.

¹⁹⁸ Tanım, GDPR m. 4/13 ile birebir aynıdır. GDPR ve Kolluk ve Ceza Adaleti Direktifi'nin yürürlüğünden evvel genetik veriler özel nitelikli kişisel veri olarak açıkça sayılmasa da kişinin kalıtım ve sağlık durumuna ilişkin bilgi ihtiva ettiğinden özel nitelikli veri olarak değerlendirilmekteydi. Bkz. Temizsoy Bayram, **a.g.e.**, s. 12; Başalp, **Kişisel Verilerin Korunması ve Saklanması**, s. 42.

¹⁹⁹ Genetik özgücülük için bkz. Rahime Erbaş, "The Tension between Genome Privacy and Criminal Justice in the Wake of DNA Databases", **CHKD**, c. 5, s. 2, 2017, s. 167-168; Koen Bruynseels, Jeroen van den Hoven, "How to Do Things with Personal Big Biodata", **Social Dimensions of Privacy Interdisciplinary Perspectives**, Ed.Beate Roessler, Dorota Mokrosinska, UK, Cambridge, 2015, s. 125.

korunması hakkına da bir müdahale oluşturmaktadır. Suçun aydınlatılması ile sağlanması hedeflenen kamu yararı ve bireyin özel yararı arasındaki denge orantılılık ilkesi ile sağlanmaya çalışılmaktadır. Buna göre DNA verileri belirli bir süre ile sınırlı olarak tutulmalı ve bu süre işlenen suçun niteliği gözetilerek belirlenmelidir²⁰⁰.

Birleşik Krallık'ta PACE'in yürürlükte olduğu dönemde DNA örnekleri ancak ciddi suçlarda şüpheli olanlardan alınabilmekteydi. Ancak 2003 tarihli Ceza Adaleti Kanunu'na göre DNA örnekleri; kişinin rızası olup olmadığına, mahkûm olup olmadığına ve örneklerin soruşturma için tutulmasında yarar olup olmadığına bakılmaksızın süresiz olarak saklanmaktadır²⁰¹. Nitekim AİHM, *S ve Marper v. Birleşik Krallık*²⁰² başvurusunda sanıkların hücre ve DNA örneklerinin beraat etmelerine rağmen süresiz olarak tutulmasının AİHS m. 8'in ihlali olduğuna hükmetmiştir. Birleşik Krallık'ın bu gerekçeyle pek çok ihlalle karşı karşıya kalması üzerine 2012 tarihli POFA'da DNA örneği ve parmak izinin ancak mahkûmiyet halinde süresiz olarak saklanması mümkün olduğu öngörülmüştür. Mahkûmiyet hali haricinde DNA örneği ve parmak izinin muhafaza süresi, kişinin mahkûm olup olmaması, işlenen suçun niteliği ve kişinin yaşına göre değişmektedir²⁰³. Ancak *Gaughran v. Birleşik Krallık* başvurusunda 2008 yılında aşırı alkollü iken araç sürme nedeniyle (hapis cezası gerektiren bir suç) başvurusunun ehliyetine elkonulmuş ve başvuru elli İngiliz Sterlini ile cezalandırılmıştır²⁰⁴. Başvurucudan DNA örneği, parmak izi alınmış ve fotoğrafları çekilmiştir. DNA örneği 2015 yılında yok edilmişse de Kuzey İrlanda Polis Servisi tarafından DNA profili, parmak izi ve fotoğraflar tutulmaya devam edilmektedir²⁰⁵. AİHM detaylı incelemesine geçmeden önce Avrupa Konseyi üyesi devletlerin DNA verilerini saklama durumlarını incelemiştir²⁰⁶ ve takdir marjı bakımından bir değerlendirme yapmıştır.

²⁰⁰ Erbaş, **a.g.e.**, s. 171-172.

²⁰¹ Namık Kemal Topçu, **İngiliz Ceza Muhakemesi Hukukunda Soruşturma Evresi**, Ankara, Adalet Yayınevi, 2018, s. 104-105; Atak, **a.g.e.**, s. 119.

²⁰² Detaylı analiz için bkz. "Sürelilik İlkesi" başlıklı bölüm.

²⁰³ Topçu, **a.g.e.**, s. 105.

²⁰⁴ *Gaughran v. Birleşik Krallık*, B. No: 45245/15, 13.02.2020, para. 7, Çevrimiçi <https://hudoc.echr.coe.int/> 29.03.2020.

²⁰⁵ *Gaughran v. Birleşik Krallık*, para. 9.

²⁰⁶ Cünha (*minor criminal offence*) nedeniyle mahkûmiyetten ötürü verilerin süresiz olarak muhafaza edildiği dört Konsey üyesi devlet (Kıbrıs, İrlanda, Kuzey Makedonya ve Karadağ) vardır. Avusturya, Belçika, Fransa, Hollanda gibi yirmi devlette DNA örnekleri belirli bir süre ile muhafaza edilmektedir.

Hükümet takdir marjının geniş olmasını şu gerekçelere dayandırmıştır: Öncelikle taraf devletler arasında hükümlülerin biyometrik veri ve fotoğraflarının tutulmasına ilişkin bir konsensüs bulunmamaktadır. Hatta bazı taraf devletlerde de hükümlünün bu verilerinin süresiz ya da çok uzun süre tutulması mümkündür. Kuzey İrlanda’da yalnız hapis cezasını gerektiren bir suçtan hüküm giyen kişilerin verileri tutulmakta ve istatistiklere göre suç işleyen kişilerin tekrar suç işleme oranlarının yüksek olması nedeniyle verilerin tutulması, suçların önlenmesi amacına da hizmet etmektedir²⁰⁷.

AİHM parmak izi ve fotoğrafların kişinin ölümüne kadar tutulmasının belirsiz bir muhafaza olduğu kanaatindedir. Yüz tanıma sistemleri, face mapping gibi yüz analizinde yeni teknolojik olanaklar kişisel veriler bakımından risk yaratmaktadır, bu risk nedeniyle verilerin belirli muhafaza süresine tabi olması gerekmektedir²⁰⁸. DNA verisi bakımından ise durum daha da incelikli değerlendirme gerektirmektedir, zira veri sahibinin ölümünden sonra tutulan DNA verisi kalıtsal bilgi taşıdığı için veri sahibinin ailesini de etkileyebilecektir. Dolayısıyla kişinin ölümüne bağlı bir veri muhafaza süresi kabul edilemezdir²⁰⁹. Hükümet’in verilerin tutulmasının suçun önlenmesi amacına hizmet ettiğine ilişkin argümanı da veri tutmanın kapsamını aşırı ölçüde genişletir mahiyette bir yorum olacaktır, öyle ki bu yorum suçların önlenmesi için nüfusun tamamından veri toplanmasına eş değerdir²¹⁰. AİHM m. 8’in ihlal edildiğine hükmederken devletlerin iç hukuk düzenlemelerinde veri muhafaza süresine ilişkin dikkate almaları gereken birtakım kriterleri belirlemiştir. Buna göre suçun ağırlığı, verinin daha uzun süre tutulması için bir gereklilik, bu gerekliliğin

Ancak Belçika ve Litvanya’da kabahatler için DNA örnekleri muhafaza edilmemektedir. Yedi devletin (Bosna-Hersek, Danimarka, Finlandiya, Moldova Cumhuriyeti, Hollanda, Norveç ve İsviçre) hüküm giymiş kişinin ölüm tarihiyle bağlantılı olarak (genel veya daha ciddi suçlar için) belirli bir muhafaza süresi vardır. Hollanda’nın mevzuatı, ciddi suçlar için en çok ölüm tarihinden itibaren yirmi yıl ve daha az ciddi suçlar için daha kısa muhafaza süreleri belirtir. Üç devletin ise (Çek Cumhuriyeti, Almanya ve Malta) belirli muhafaza süreleri yoktur, ancak muhafaza konusunda çeşitli önemli sınırlamalar vardır ve uzun süreli muhafaza için temel gerekliliklerin karşılanıp karşılanmadığını belirlemek için periyodik değerlendirmeler yapılmaktadır. Bkz. *Gaughran v. Birleşik Krallık*, para. 53.

²⁰⁷ *Gaughran v. Birleşik Krallık*, para. 62.

²⁰⁸ *Gaughran v. Birleşik Krallık*, para. 70.

²⁰⁹ *Gaughran v. Birleşik Krallık*, para. 81.

²¹⁰ *Gaughran v. Birleşik Krallık*, para. 89.

gözden geçirilmesi ve yarışan bireysel ve kamusal menfaat arasındaki denge gözetilmelidir²¹¹.

3. Türk Hukukunda Durum

Türk hukukunda beden muayenesi, vücuttan örnek alınması²¹² ve moleküler genetik incelemenin²¹³ hukuki niteliği tartışmalıdır. Beden muayenesi ve vücuttan örnek alınmasında amaç, delil elde etmek iken moleküler genetik incelemede amaç, elde edilen deliller üzerinde karşılaştırma yapmaktır²¹⁴. CMK hükümleri uyarınca şüpheli, sanık yahut üçüncü kişinin vücutundan alınan doku üzerinde yapılan DNA inceleme sonuçları, kişisel veridir²¹⁵. Kişisel verinin elde edilebilmesi için öncelikle beden muayenesi yahut olay yeri incelemeye konu bir biyolojik parçanın elde edilmesi gerekmekte, sonrasında bu parça moleküler genetik incelemeye tabi tutulmaktadır. Bu nedenle beden muayenesi ve moleküler genetik incelemeyi külli olarak anlatmayı tercih etmekteyiz.

Moleküler genetik inceleme, özel genetik karakterler hakkında açıklama içermeyen kromozom bölgesi ile sınırlı olarak yapılır. Analiz için bilirkişiye gönderilen bulgular, rapor hazırlandıktan sonra imha edilir ve bu husus raporda belirtilir²¹⁶. Elde edilen kişisel veriler, CMK m. 80/2'ye göre kovuşturmaya yer olmadığı kararının kesinleşmesi, beraat ve ceza verilmesine yer olmadığı kararının

²¹¹ *Gaughran v. Birleşik Krallık*, para. 96.

²¹² Beden muayenesi ve vücuttan örnek alınmasının temel hak ve özgürlüklere müdahale özelliği gözetilerek bir koruma tedbiri olduğuna ilişkin bkz. Esra Alan, “Ceza Muhakemesinde Beden Muayenesi ve Vücuttan Örnek Alınması”, *Uğur Alacakaptan’a Armağan*, c. 1, İstanbul, İstanbul Bilgi Üniversitesi Yayınları, 2008, s. 48; Delil elde etme yöntemi olduğuna ilişkin ise bkz. Ünver, Hakeri, *a.g.e.*, s. 595; Hem koruma tedbiri hem bilirkişi incelemesi olduğuna dair bkz. Bahri Öztürk, Behiye Eker Kazancı, Sesim Soyer Güleç, *Ceza Muhakemesi Hukukunda Koruma Tedbirleri*, Ankara, Seçkin Yayıncılık, 2019, s. 218; Faruk Turhan, “Ceza Muhakemesinde Beden Muayenesi ve Tıp Hukuku (Özellikle AİHM Kararları Işığında Şüpheli veya Sanığın Zorla Muayenesi Konusunun Değerlendirilmesi)”, *V. Türk-Alman Tıp Hukuku Sempozyumu*, Ankara, TBB Yayını, 2008, s. 1026.

²¹³ Moleküler genetik incelemenin bağımsız bir tedbir değil; hakim bakımından keşif, analizi yapacak uzman tarafından ise bilirkişi incelemesi olduğuna dair bkz. Özbek, *a.g.e.*, s. 1088; Bilirkişi incelemesi yani delil değerlendirme aracı olduğuna ilişkin bkz. Temizsoy Bayram, *a.g.e.*, s. 76-77.

²¹⁴ Öztürk, Eker Kazancı, Soyer Güleç, *a.g.e.*, s. 215.

²¹⁵ CMK m. 80/1; Aygörmez Ugurlubay, *a.g.e.*, s.58; Handan Yokuş Sevik, “Tıp Ceza Hukukunda Kişisel Verilerin Açıklanması”, *V. Türk-Alman Tıp Hukuku Sempozyumu*, Ankara, TBB Yayını, 2008, s. 797.

²¹⁶ Mehmet Alkan, “Avrupa Konseyi Bakanlar Komitesinin İnsan Hakları ve Terörle Mücadele Hakkındaki İlkeleri ve Türkiye’nin Terörle Mücadele Mevzuatı”, *TBB Dergisi*, c. 29, s. 125, 2016, s. 26.

kesinleşmesi üzerine derhâl yok edilir. Mahkûmiyet halinde verinin yok edileceğine ilişkin bir düzenleme CMK ve Ceza Muhakemesinde Beden Muayenesi, Genetik İncelemeler ve Fizik Kimliğin Tespiti Hakkında Yönetmelik'te²¹⁷ bulunmamaktadır, bu nedenle bu verilerin arşivleneceği düşünülebilir. Ancak doktrinde bu halin de CMK'de düzenlenmiş olması gerektiği ileri sürülmüştür²¹⁸. Ayrıca DNA veri bankası bulunmazken muhafaza süresi ve şekli belirtilmeyen verinin nasıl muhafaza edileceği de anlaşılamamaktadır.

Beden muayenesi ve vücuttan örnek alınması şüpheli, sanık veya CMK m. 76'nın kenar başlığı uyarınca üçüncü kişi üzerinde yapılır. Ancak maddede kenar başlığının aksine yalnız mağdur üzerinde yapılacağı öngörülmüştür. Yönetmelik m. 8'e göre ise diğer kişilerin vücutundan da örnek alınabileceği düzenlenmiştir. Ancak diğer kişilerin kim olduğu belirtilmemiştir. Kanunun sınırını aşan²¹⁹ ve veri sahibinin niteliği ve kimliğini böylesine belirsizleştiren Yönetmelik hükmü kişisel verilerin korunması bakımından sakıncalıdır.

Beden muayenesi ve vücuttan örnek alınmasına ancak hakim, gecikmesinde sakınca bulunan hallerde ise savcı kararı ile başvurulabilir. Ancak savcının kararı, hakimin onayına tabidir. Hakimin kararı onaylamadığı halde, bu materyallerin delil olarak kullanılamayacağı düzenlenmiştir²²⁰. Bunların yok edilip edilmeyeceğine ilişkin bir düzenleme ise CMK'de bulunmamaktadır. Vücuttan örnek almaya delil elde etme amacıyla başvurulduğuna göre delil olarak kullanılmayacak bu materyallerin şüphesiz yok edilmesi gerekmektedir. Nitekim Yönetmelik m. 6/1'e göre Cumhuriyet savcısının huzurunda ve uygun göreceği usullerle şüpheli veya sanıktan alınan materyal derhâl yok edilecektir. Ancak Yönetmelik'te diğer kişilerin vücutundan alınan materyalin yok edilip edilmeyeceğine ilişkin bir düzenleme bulunmamaktadır ve bu ciddi bir eksikliktir.

²¹⁷ R.G. Sayısı: 25832, R.G. Tarihi: 01.06.2005.

²¹⁸ Öztürk, Eker Kazancı, Soyer Güleç, **a.g.e.**, s. 253; Özbek, **a.g.e.**, s. 1115.

²¹⁹ Ünver, Hakeri, **a.g.e.**, s. 609; Atalay'a göre ise moleküler genetik inceleme; şüpheli ve sanık haricinde tanık, mağdur ve diğer kişilere ilişkin de olabilecektir. Ayşe Özge Atalay, "Ceza Muhakemesi Hukukunda Moleküler Genetik İncelemelerin Özel Nitelikli Kişisel Verilerin Korunması Açısından Değerlendirilmesi", **CHKD**, c. 7, s. 2, 2019, s. 140.

²²⁰ CMK m. 75/1, 76/1.

CMK hükümlerince yapılan beden muayenesinden elde edilen örneklerde başka amaçla inceleme yapılamamaktadır. Bazı yazarlarca başka inceleme yapılması mümkün olsaydı, yapılan inceleme sonucu elde edilen kişisel verilerin ileride işlenebilecek suçlarda karşılaştırma yapılarak maddi gerçeğin aydınlatılmasına yardımcı olacağı ifade edilmiştir²²¹. Ancak bu türden bir düzenleme, ceza muhakemesi amaçlarından uzaklaşarak fiilen DNA veri bankasının ihdasını ve veri madenciliği tehlikesini gündeme getirebilecektir. Örneğin; son dönemlerdeki bilimsel gelişmelerle Adli Tıp Kurumunun dahi dâhil olduğu bazı bölgelerdeki kanalizasyon ve atıklardan kişilerin idrar, tırnak, saç gibi örnekleri alınıp incelenerek uyuşturucu madde kullanımı tespit edilmeye ve bölgesel suç haritaları çıkarılmaya çalışılmaktadır²²². Ancak bu uygulamanın herhangi bir kanuni dayanağı bulunmamaktadır, zira beden muayenesi ve vücuttan örnek almaya önleyici amaçla²²³ ya da kişinin ileride suç işleyebileceğinden bahisle başvurulamaz²²⁴. Ayrıca CMK m. 78/1'de soybağının tespiti için de moleküler genetik inceleme yapılacağı belirtilmişse de bu inceleme, bir suçla ilgili olması halinde yapılacaktır²²⁵. Yani salt hukuk mahkemesini ilgilendiren bir hususta CMK m. 78/1 hükümlerine göre moleküler genetik inceleme yapılmayacak ve sonuç hukuk muhakemesinde kullanılamayacakken²²⁶, fail ve mağdur arasında altsoy-üstsoy ilişkisini tespit veya çocuğun soybağını değiştirme suçunun oluşup oluşmadığını tespit için m. 78/1 hükmü gündeme gelecektir.

Yönetmelik'e göre, kişinin vücut yüzeyinde bulunan ancak biyolojik olmayan materyaller ve vücut yüzeyinde bulunup da kişiye ait olmadığı açıkça belli olan elbise, kıl, tüy gibi örneklerin alınması ve olay yeri inceleme uzmanlarınca incelenmesinde CMK hükümleri uyarınca karar alınması gerekmemektedir²²⁷. Ancak başkası üzerinde bulunan kıl örneğinin alınarak uzmanlarca yapılan değerlendirme sonucu bir başka kişi

²²¹ Bkz. Semiz, **a.g.e.**, s. 82.

²²² Çevrimiçi <https://tr.sputniknews.com/turkiye/201803201032712064-akdag-kanalizasyon-suyunda-uyusturucu-takibi-yapacagiz/> 11.03.2020.

²²³ Çiğdem Adar Özdemir, **Nemo Tenetur İlkesi Bağlamında Beden Muayenesi ve Vücuttan Örnek Alınması**, İstanbul, Seçkin Yayıncılık, 2020, s. 111.

²²⁴ Turhan, **a.g.e.**, s. 1032.

²²⁵ Atalay, **a.g.e.**, s. 142.

²²⁶ Öztürk, Eker Kazancı, Soyer Güleç, **a.g.e.**, s.237.

²²⁷ Yönetmelik m. 23; Yönetmelik'in böyle bir hüküm getirmesinin nedeni, bu materyallerin Adli ve Önleme Aramaları Yönetmeliği m. 9 uyarınca olay yeri incelemeye tabi tutulmaya çalışılmasıdır. Bkz. Turhan, **a.g.e.**, s. 1032; Hükmün somut ve anlaşılır biçimde CMK'de düzenlenmesi gerektiğine ilişkin bkz. Alan, **a.g.e.**, s. 47.

ile ilişkilendirilebilir olması halinde, bu materyal sonucunda bir kişisel veri işlenmektedir ve bu inceleme, Yönetmelik gereği CMK'ye tabi değildir. Dolayısıyla kişisel verilerin işlenmesinde kanunilik ilkesine uyulmayan sonuçlara yol açan bu hüküm isabetsizdir.

DNA veri bankası kurulmasına ilişkin Türkiye'de 2000'lerin başında çalışmalar yapılmışsa da bu çalışmalar, Türkiye Milli DNA Veri Bankası Kanunu Tasarısı'nın ötesine geçememiştir²²⁸. Nitekim Tasarı'nın da başlı başına sakıncalı hükümleri mevcuttu. Tasarı'nın 5. maddesine göre suç sebebiyle olay yerinden, kimliği tespit edilemeyen kişi ve ölülerden, görevleri sebebiyle hayati risk taşıyanlardan ve gönüllülerden biyolojik materyal alınması mümkündü. 8. maddeye göre de mahkeme, hakim veya savcının veri bankasından ceza muhakemesinden maddi gerçeğe ulaşabilmek için DNA profil karşılaştırması talep etmesi mümkündü. Ayrıca alıcı ülkede yeterli düzeyde veri korumasının bulunması halinde DNA örneklerinin yurtdışına aktarılması da mümkündü. Tasarı uzun yıllardır kanunlaşmadığından üzerinde detaylı incelemeler yapmaya gerek duymamaktayız. Ancak *gönüllülük* esasına dayanarak ceza muhakemesinde kullanılabilecek özel nitelikli genetik verinin işlenmesi başlı başına sakıncalıdır ve Kolluk ve Ceza Adaleti Direktifi hükümleri ile de bağdaşmamaktadır. Meri mevzuat bakımından moleküler genetik incelemeye ancak soybağının veya elde edilen bulgunun şüpheli veya sanığa ya da mağdura ait olup olmadığının tespiti için başvurulabilecektir²²⁹.

D. Adli Bilişim

1. Tanım

Potansiyel delillerin elde edilebilmesi amacıyla bilgisayarda inceleme ve analiz metotlarından yararlanılmakta²³⁰ ve bilgisayar sistem analizlerinden yararlanılarak şüpheli ve sanıklar tespit edilebilmektedir. *Elektronik bir araç tarafından iletilen veya*

²²⁸ Tasarının tam metni için bkz. Çevrimiçi http://www.ttb.org.tr/haberarsiv_goster.php?Guid=665acfee-9232-11e7-b66d-1540034f819c 13.03.2020.

²²⁹ CMK m. 78/1.

²³⁰ Leyla Keser Berber, **Adli Bilişim (Computer Forensic)**, Ankara, Yetkin Yayınları, 2004, s. 39.

*bu araçlar üzerine kaydedilmiş ve soruşturma açısından değeri olan bilgi veya veriler elektronik delillerdir*²³¹. Elektronik delillerden ceza muhakemesinde yararlanılabilmesi için toplama, inceleme, analiz ve belge hazırlamadan oluşan adli bilişim prosedürüne başvurmak gerekmektedir²³².

Adli bilişimde en yaygın yöntemlerden biri şüpheli sayısını en aza indirmeyi amaçlayan bilgisayar sistem analizi olarak trol ağı yöntemidir²³³. Bir bilgisayar sistemine kayıtlı olan verilerin karşılaştırılması ve analizi ile şüphelinin tespitine olanak tanıyan bilgisayar sistemleri bulunmaktadır. Şüpheli veya üçüncü kişilerin aranması, sorgusu, gizli soruşturmacı yahut teknik araçla yapılan dinlemelerde elde edilen veriler veya sigorta şirketleri, sosyal kurumlar, kamu kurumları gibi kurumlardan elde edilen veriler sisteme yüklenerek bağlantı kurulmaya çalışılmakta ve bir şüpheli profili oluşturulmaktadır²³⁴. Boy, kilo, göz rengi, medeni durum gibi çok çeşitli fiziksel ya da diğer özellikleri benzer olan kişilerin incelenerek olası failin tespiti yapılmakta ve şüpheli sayısı azaltılmaktadır²³⁵. Şüpheli ile kriminojen özellikleri benzeyen kişilerin “trol ağına takılması” ile aslında yalnız şüpheli değil, pek çok kişi hakkında araştırma yapılmaktadır²³⁶.

Özellikleri karşılaştırılan kişilerin kişisel verilerinin sisteme kaydı ile o kişiler şüpheli olmamaktadır. Buna rağmen suçsuz yahut kendisinden şüphelenilmeyen kişilerin de verileri bu yöntemde kullanıldığından bu, veri koruma hukuku bakımından sakıncalı bir düzenlemedir. Bu sakıncaların bertaraf edilmesi için doktrinde olumlu ve olumsuz trol ağı metodu ayrımı yapılarak; bu, şüpheliler hakkında uygulandığında olumlu trol ağı, şüpheli olmayanlar hakkında uygulandığında ise olumsuz trol ağı metodu olmaktadır ve böylece şüpheli olmayanların ayrılmasına çalışılmaktadır²³⁷.

²³¹ Keser Berber, **a.g.e.**, s. 44.

²³² Keser Berber, **a.g.e.**, s. 45.

²³³ Ünver, “Federal Almanya’da Terör ve Organize Suçluluk ile İlgili Düzenlemeler”, s. 408-409; 1970-80’lerde başvuru trol ağı metodu verilerin korunması bakımından endişe doğurmuşsa da terör örgütlerinin takibinde yalnız maddi gerçeğin ortaya çıkarılması bakımından değil, tehlikelerin önlenmesi bakımından da bu metod işlevsel olmuştur.

²³⁴ Ünver, “Federal Almanya’da Terör ve Organize Suçluluk ile İlgili Düzenlemeler”, s. 408.

²³⁵ Bayram, **a.g.e.**, s. 59.

²³⁶ Yenisey, **Kolluk Hukuku**, s. 334.

²³⁷ Ünver, “Federal Almanya’da Terör ve Organize Suçluluk ile İlgili Düzenlemeler”, s. 409.

Alman hukukunda bu ynteme, diğr yollarla maddi gerçeğe ulařma ve faili tespit etmenin daha az bařarı řansı olacağı ve daha zor olacağı durumlarda yalnızca StPO 163d'nin saydığı terr rgt oluřturmak, silahlı soygun ve ateřli silahlar ile uyuruřturucu madde suçlarında uygulanmasına izin verilmiřtir²³⁸. Failin sahip olduėu ve belirli nemli zellikleri gsteren kiřisel veriler, řpheli olmayan kiřileri dıřlamak veya soruřturmayla ilgili diğr kiřileri tespit etmek iin otomatik olarak sisteme kayıtlı diğr verilerle eřleřtirilebilmektedir. Bu tedbire bařvurulması iin hakim, gecikmesinde sakınca bulunan hallerde hakim onayına sunulmak ve  gn iinde onayın alınması řartıyla savcının kararı gerekmektedir. Verileri depolayan veri sorumluları, bunları kolluk glerine iletmekte ve savcılığın talebi zerine, veri sorumluları karřılařtırmayı yapan makama yardım etmektedir. Veri karřılařtırmasında kullanılan ancak faile ait olmadığı anlařılan veriler, alındıkları kuruma derhl iade edilirler ve ceza muhakemesinde kullanılmayan veriler silinir²³⁹. Ayrıca trol ağı yntemi uygulanarak bilgileri bilgisayara kaydedilen kimselerin haklarında ek arařtırma yapılmıř ve řpheli statsne girmemiřlerse bu kiřilere haklarında trol ağı yntemine bařvurulduėuna dair bilgi verilir. Bilgilendirmenin istisnası soruřturmanın amacının tehlikeye dřrlmesidir²⁴⁰.

Bir diğr sistem analizi de bilgisayar eřleřtirmedir (*computer matching*). Bu yntem ile resmi ve zel kurumların bilgisayar sistemlerinde kayıtlı olan veriler karřılařtırılarak fail ve failin yařayıřı hakkında bilgi toplanarak toplanan verilerden faile ulařılmaya alıřılmaktadır²⁴¹. Sz gelimi kamu kurumları, vergi dairesi, hastane, yurt gibi kurumların bilgisayar sistemine kayıtlı verilerden olası failin kiřisel verilerinin karřılařtırılması ile maddi gerçeğe ulařılmaya alıřıldığından kayıtların doėru tasnif edilerek tutulması nemlidir²⁴².

2. Trk Hukukunda Adli Biliřim Uygulamaları

²³⁸ Yenisey, **Kolluk Hukuku**, s. 335.

²³⁹ Yenisey, **Kolluk Hukuku**, s. 336; nver, "Federal Almanya'da Terr ve Organize Sululuk ile İlgili Dzenlemeler", s. 408-409.

²⁴⁰ Yenisey, **Kolluk Hukuku**, s. 337.

²⁴¹ Bayram, **a.g.e.**, s. 60.

²⁴² nver, "Federal Almanya'da Terr ve Organize Sululuk ile İlgili Dzenlemeler", s. 407.

a. UYAP Bilişim Sistemi

UYAP yargı birimleri arasında yargısal ve idari işleyişte kullanılan bir bilişim otomasyon sistemidir²⁴³. Adalet Bakanlığı Bilgi İşlem Daire Başkanlığının çalışmaları ile bu sisteme yeni alt uygulamalar eklenmektedir. Sistemin amacı, adli makamların emniyet teşkilatı ve yüksek yargı organları arasındaki faaliyetleri arasında koordinasyonun sağlanmasıdır. Mernis²⁴⁴ ve Polnet ile de entegre halde işleyen bu sistem ile yargı hizmetleri daha hızlı ve şeffaf biçimde yürütülebilecektir²⁴⁵.

(1) UYAP Kolluk Bilişim Sistemi

UYAP kolluk bilişim sistemi; CMK uyarınca kolluk, adli kolluk görevini ifa eden orman kolluğu ve çocuk izleme merkezlerinin yürüttüğü soruşturma işlemlerinde fezleke hazırlanması, taraf ifadelerini alınması gibi süreçlerde kullanılan bilişim sistemidir. Bu sistem üzerinden kişilerin kollukça alınan ifadesi, adresi, SGK bilgisi, vatandaşlık kimlik numarası, ikamet bilgisi gibi kişisel verilerine erişilebilmektedir²⁴⁶.

(2) Mobil Arananlar Bilgi Sistemi

Mobil Arananlar Bilgi Sistemi, kolluğun yakalama ve tutuklama kararlarına yapacakları çevrimiçi sorgulama ile anında ulaşarak bu kararları yerine getirmelerine olanak sağlayan bir sistemdir²⁴⁷. Hakkında yakalama ve tutuklama kararı bulunan kişilerin verileri sistemde yer almaktadır.

(3) SEGBİS

²⁴³ Çevrimiçi <https://www.uyap.gov.tr/Tarihce> 05.02.2020; Ceza Muhakemesinde Ses ve Görüntü Bilişim Sisteminin Kullanılması Hakkında Yönetmelik m. 3/e “UYAP Bilişim Sistemi: Adalet hizmetlerinin elektronik ortamda yürütülmesi amacıyla oluşturulan bilişim sistemini” ifade eder.

²⁴⁴ Cahit Çelik, “UYAP’ın Temel Sistemi ve Güvenlik”, **Bilişim Hukuku**, Ed. Mete Tevetoğlu, İstanbul, Kadir Has Üniversitesi Yayınları, 2006, s. 152.

²⁴⁵ Mesut Orta, “UYAP Sistemi ve Temel Özellikleri”, **Bilişim Hukuku**, Ed. Mete Tevetoğlu, İstanbul, Kadir Has Üniversitesi Yayınları, 2006, s. 147.

²⁴⁶ Ali Rıza Çam, **Adli Bilişim ve Kolluk**, İstanbul, On İki Levha Yayıncılık, 2015, s. 73-74.

²⁴⁷ Çevrimiçi <https://www.uyap.gov.tr/Projeler> 05.02.2020.

SEGBİS'ten yararlanılarak CMK uyarınca şüpheli, sanık, tanık, bilirkişilerin dinlenmesi, ifade alma ve sorgu işlemleri sırasında görüntülü ve sesli olarak kayıt yapılabilmektedir²⁴⁸. SEGBİS'e ilişkin CMK'nin muhtelif hükümlerinde kişisel verilerin korunmasına özen gösterilmeye çalışıldığı anlaşılmaktadır. Örneğin; *duruşmaya getirilmeden dinlenen tanığın bu yolla elde edilen ses ve görüntü kaydı sadece ceza muhakemesinde kullanılır*²⁴⁹ hükmü amaçla bağlılık ilkesi ile bağdaşmaktadır. TCK m. 102/2'nin mağdurunun beyan ve görüntülerinin ancak rızası ile kayda alınmasına izin veren CMK m. 236/6 hükmü de Kolluk ve Ceza Adaleti Direktifi'nin öngördüğü korumanın ötesinde bir veri koruması sağlamaktadır. Ancak SEGBİS kayıtların muhafaza süresinin kanun koyucu tarafından öngörülmemiş olması ciddi bir eksikliktir²⁵⁰.

b. Polnet

Emniyet Genel Müdürlüğü bünyesindeki hizmetlerin elektronik ortamda sunulmasını sağlayan bir sistemdir. Ulusal ve uluslararası veri tabanları ile de entegre halde işlemesi Polnet'in etkili olmasını sağlamıştır²⁵¹. Bünyesinde bulunan *Tahdit Programı* ile Türkiye'ye giriş ve çıkış yapan kişilerin, *Yabancılar Programı* ile ülkeye meşru-gayrimeşru yollardan giren kişilerin, *Sürücü Ceza Programı* ile ülkede trafik cezası alan sürücülerin, *GBT Programı* ile herhangi bir suretle suça karışan kişilerin, *Gözetli İşlemleri Programı* ile de gözetli altına alınan kişiler ve serbest bırakılanlar hakkındaki kayıtların yapıldığı ve bu kişilerin kişisel verilerinin işlendiği bir sistemdir²⁵². Polnet aracılığıyla delil, parmak izi, balistik inceleme raporları, DNA, doku, kan analizlerinin ve benzeri gerekli dokümanların kısa süre içinde elektronik ortamda sirkülasyonunun sağlanması şüphesiz kolluk makamları için büyük bir

²⁴⁸ Bkz. CMK m. 52, 58, 180, 196, 219. Bazı hallerde SEGBİS'e başvurulması m. 52/3 "*Tanıkların dinlenmesi sırasındaki görüntü veya sesler kayda alınabilir.*" denilmek suretiyle ihtiyari iken bazı hallerde ise CMK m. 236/5 "*Türk Ceza Kanununun 103 üncü maddesinin ikinci fıkrasında düzenlenen suçlardan mağdur olan çocukların soruşturma evresindeki beyanları, bunlara yönelik hizmet veren merkezlerde Cumhuriyet savcısının nezaretinde uzmanlar aracılığıyla alınır. Mağdur çocuğun beyan ve görüntüleri kayda alınır*" gibi zorunludur.

²⁴⁹ CMK m. 52/4

²⁵⁰ Ses ve kayıtların yok edilme usulü bakımından "Ceza Muhakemesinde Ses ve Görüntü Bilişim Sisteminin Kullanılması Hakkında Yönetmelik" de herhangi bir hüküm içermemektedir.

²⁵¹ Çam, **a.g.e.**, s. 93.

²⁵² Çam, **a.g.e.**, s. 95-96.

kolaylıktır²⁵³ ve maddi gerçeğe daha kısa sürede ulaşılmasına hizmet etmektedir. Ancak özel nitelikli de dâhil her neviden kişisel veriye erişmeye olanak sağlayan bu sistem kişisel verilerin korunması hakkına da risk teşkil etmektedir ve teknik altyapısının iyi sağlanması gerekmektedir²⁵⁴.

c. Jandarma Entegre Muhabere ve Bilgi Sistemi (JEMUS)

Jandarma birimleri arasında *telli sistem sayesinde; kaliteli ses haberleşmesi elektronik posta alışverişi, dosya paylaşımı, intranet erişimi, emniyetli ve süratli veri aktarımı, suç ve suçlu sorgulaması ve sistemlerin merkezden yönetimi*²⁵⁵ gibi işlemlerin elektronik ortamda yürütülmesine olanak sağlayan bir bilişim sistemidir. JEMUS bünyesindeki Coğrafi Bilgi Sistemi'nden yararlanarak bir harita üzerinde, gerçekleşen olayların coğrafi konumları ve suç bilgileri gösterilmekte iken Araç Takip Uygulaması ile de Jandarma Genel Komutanlığı'na bağlı araçlar kriptolu biçimde takip edilmektedir²⁵⁶. JEMUS aracılığıyla adli kolluk görevi yürüten jandarmanın bir soruşturma çerçevesinde ihtiyaç duyduğu parmak izi de dâhil kişisel verilere erişim mümkündür²⁵⁷.

d. Balistika

TÜBİTAK Uzay'ın geliştirdiği bu sistem ile balistik iz ve görüntüler analiz edilip eşleştirilebilmektedir. Balistika, silah kovan ve çekirdekleri üzerinde yapılan üç boyutlu incelemeler ile silahlar ve olayların oluş sıklıkları ve daha da önemlisi bunları kişilerle ilişkilendirmeye olanak sağlayan veri tabanına sahip bir sistemdir²⁵⁸. Bir

²⁵³ Çam, **a.g.e.**, s. 97.

²⁵⁴ *Memurlar.net* isimli internet sitesinin 25.05.2009 tarihli “Pol-Net'te keyfi sorgulama!” başlıklı haberi de bu endişeyi haklı çıkarmaktadır. Emniyet içindeki on altı farklı birimin herhangi bir gerekçe belirtmesine gerek olmaksızın kamusal bir figürü elli altı kez sorgulaması Polnet'e tüm emniyet personelinin ulaşmasını tartışmaya açmıştır. Sistem, erişim sağlayan personelin log kayıtlarını tutsa da kullanıcı girişi yapmaksızın da sisteme girilebilmesi hesap verilebilirliğe de gölge düşürmüştür. Çevrimiçi <https://www.memurlar.net/haber/140285/pol-net-te-keyfi-sorgulama.html> 05.02.2020.

²⁵⁵ Çevrimiçi <http://www.islem.com.tr/uploads/proje/JEMUS.pdf> 06.02.2020.

²⁵⁶ Çevrimiçi <http://www.islem.com.tr/uploads/proje/JEMUS.pdf> 06.02.2020.

²⁵⁷ Çam, **a.g.e.**, s. 100.

²⁵⁸ Çevrimiçi <https://uzay.tubitak.gov.tr/tr/urunlerimiz/balistika-0> 06.02.2020.

gerçek kişi ile ilişkilendirme sağlayan bu sistem aynı zamanda kişisel veri işleyen bir veri tabanıdır.

E. Arama ve Elkoyma

1. CMK’de Yer Alan Arama ve Elkoyma Tedbirleri

CMK uyarınca şüpheli, sanığın üstünde, eşyasında, konutunda yapılacak arama ve elkoymalarda kişisel veriler ele geçirilebilir. Arama ve elkoymanın uygulanması sırasında işlenen kişisel verilerin korunmasına ilişkin CMK özel bir koruma öngörmemektedir. Yalnız CMK m. 130/2 gereği elkonulan şeyin avukat ve müvekkili arasındaki mesleki ilişkiye dair olması halinde elkoymanın sona ermesi ve bu işlem ile ilgili tutanakların yok edilmesi hükmü, avukat ve müvekkilin mesleki ilişkisinde gündeme gelen kişisel verilerin korunmasına hizmet edebilecek bir hükümdür.

MİT Kanunu ek m. 1 uyarınca MİT’in uhdesindeki istihbarat bilgi ve belgelerinin adli mercilerce kullanılması bazı istisnai suçların muhakemesi hariç mümkün değildir. Maddede “*adli mercilerce istenemez*” hükmü ile mahkeme veya savcılık bu bilgi ve belgelere ulaşamayacaktır ve bu hüküm dolaylı olarak MİT bünyesindeki kişisel verilerin korunmasına hizmet etmektedir. Anlaşılacağı üzere arama ve elkoymaya ilişkin kişisel verilerin korunmasına dair bir hüküm CMK’de bulunmamaktadır.

Arama ve elkoymanın özel bir türü olan bilgisayarlarda, bilgisayar kütükleri ve programlarında arama, kopyalama ve elkoymada ise işlenen kişisel verilerin korunması daha da önemlidir. Zira bu halde bilgisayar verileri kopyalanmak, yedeklenmek, çözülmek suretiyle işlenmektedir. *Bilgisayar sisteminin bir işlevini yerine getirmesini mümkün kılan bir programı da kapsayan olguların, bilginin veya kavramların bir bilgisayar sisteminde işlenmeye uygun haldeki her türlü temsili bilgisayar verisidir*²⁵⁹. Bu verilerin arasında kişinin fotoğrafları, sağlık kayıtları gibi

²⁵⁹ Avrupa Siber Suçlar Sözleşmesi m. 1/b. Doktrinde bilgisayar verisi yerine daha üst bir kavram olarak elektronik olarak işlenmiş ve saklanmış verilerin tercih edilmesi gerektiği ileri sürülmüştür. Bkz. Veli Özer Özbek, “Elektronik Ortamda Saklı Bulunan Verilerin Ceza Muhakemesinde Delil Niteliği ve Değerlendirilmesi”, *İÜHFİM*, c. 59, s. 1-2, 2001, s. 183.

kişisel verilerinin de bulunması muhtemeldir. İşlenen verilerin ne süre ile tutulacağı, kişinin beraat etmesi halinde yok edilip edilmeyeceğine ilişkin bir hüküm CMK’de bulunmamaktadır. CMK m. 134/1’de yalnız Cumhuriyet savcısı kararı ile bu tedbire başvurulduğunda, hakim kararı onaylamamışsa kopyalar ve çözümlerin imha edileceği düzenlenmiştir. Oysa beraat ve kovuşturmayaya yer olmadığı kararının kesinleşmesi hallerinde de yok edilmelidir²⁶⁰.

CMK m. 134’teki bu tedbire başvurulduğunda bilgisayar program ve kütüklerinde değişiklik yapıldığına ilişkin iddiaların önüne geçmek için yedekleme yapılmalıdır ve kişisel verilere zarar verilmemelidir²⁶¹. Örneğin bir bilgisayarın hard diski alındığında önce hash değeri alınarak tutanak tutulmalı, şüpheli veya müdafinin yanında imaj alınmalı ve yedekleme yapılmalıdır²⁶². Bu sayede veri bütünlüğü sağlanarak kişisel verilerin dezenforme edilmesinin önüne geçilebilecektir.

2. IP Adresi

Bilgisayar, bilgisayar kütükleri ve programlarında arama, kopyalama ve elkoyma tedbirine genellikle bir IP adresine ulaşılmasının ardından başvurulmaktadır. Bu nedenle IP adreslerine de bu başlık altında değinmeyi uygun bulduk. IP adresi, internet ağına bağlanan bilgisayara her bağlandığında verilen adrestir ve her bağlantıda farklı bir adres verildiğinden tek bir IP adresi ile kullanıcı belirlenemediğinden IP adresinin kişisel veri olup olmadığı tartışılmıştır²⁶³. Her bağlantıda IP adresinin son numarası değişmektedir, ancak numara değişse bile log kayıtlarından hangi tarih ve saatte IP adresinin hangi telefon numarasına tahsis edildiği saklanmaktadır²⁶⁴, bu da kişinin belirlenebilirliğine hizmet ettiğinden IP adresi de kişisel veridir.

²⁶⁰ Öztürk, Eker Kazancı, Soyer Güleç, **a.g.e.**, s. 206-207.

²⁶¹ Öztürk, Eker Kazancı, Soyer Güleç, **a.g.e.**, s.205. Nitekim 6526 sayılı Kanun ile getirilen değişiklikle CMK m. 134/4 gereği bu yedekten bir kopyanın şüpheli veya müdafie verilmesi zorunlu hale getirilmiştir.

²⁶² Muharrem Özen, Gürkan Özocak, “Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK M. 134)”, **Ankara Barosu Dergisi**, 2015/1, s. 68.

²⁶³ Güçlü Akyürek, **Özel Hayatın Gizliliğini İhlal Suçu**, Güncellenmiş ve Genişletilmiş 2. Baskı, Ankara, Seçkin Yayıncılık, 2014, s. 68.

²⁶⁴ Murat Volkan Dülger, Gözde Madoğlu, “Bilişim Suçları, Soruşturma ve Kovuşturma Yöntemleri ile İnternet İletişim Hukuku (Uygulama Rehberi)”, **Türk Ceza Adalet Sisteminin Geliştirilmesi Avrupa Birliği/ Avrupa Konseyi Ortak Programı**, Ankara, Şen Matbaa, 2014, s. 110.

ABAD, dinamik IP adreslerinin kişisel veri olduğuna hükmetmiştir²⁶⁵. Başvuruya konu olayda başvuru, Almanya'nın pek çok kurumunun internet siteleri aracılığıyla kişilerin internet kullanımlarına dair kayıt ve IP adreslerini internet erişimi kesildikten sonra da belirli bir süre saklanmasına karşı dava açmıştır. ABAD'ye göre üçüncü kişilerden alınacak ek bilgiler ile IP adreslerinin birleştirilmesi ve erişilebilir üçüncü kişilerin kim olduğuna ilişkin makul ihtimaller çerçevesinde değerlendirme yapılmalıdır. ABAD, makul imkânların bulunması halinde internet erişim sağlayıcısının gereken ek bilgilerin talebi üzerine IP adresi ile kişinin belirlenebileceği ve belirlenebilirliği sağlayan bu verinin veri sorumlusunda bulunması gerekmediğini belirtmiştir²⁶⁶.

*Benedik v. Slovenya*²⁶⁷ başvurusunda da başvuru hakkında çocuk pornografisi suçu nedeniyle yürütülen soruşturmada, mahkeme kararı olmaksızın internet servis sağlayıcısından IP adresi ve adres bilgileri temin edilmiştir. Slovenya Ceza Muhakemesi Kanunu m. 149b/1'e göre elektronik haberleşme ağını kullanan kişiler hakkında yürütülen soruşturma kapsamında suç işlendiğine dair makul şüphenin mevcut olması halinde, operatörden kullanıcıya dair sayı, tür, tarih, süre, zaman, miktar bilgileri hakim kararı ile temin edilebilmektedir. Kanun m. 149b/3'e göre ise takibi şikâyeteye bağlı olmayan bir suça ilişkin yürütülen soruşturmada suçun işlendiğine dair makul şüphe mevcutsa polisin suçu ortaya çıkarmak için operatöründen failin bilgisini yazılı olarak talep edebilmesi mümkündür. Başvuru

²⁶⁵ Dinamik IP adresi, servis sağlayıcının o an için boş olan IP adresini kullanıcıya ataması nedeniyle zaman ve oturuma göre değişirken statik IP adresi ise sistem yöneticisi tarafından tanımlanan ve değişmeyen adrestir. Bkz. Dülger, Madoğlu, **a.g.e.**, s. 25; Belirlenebilirliğe dair önemli bir karar olarak Bkz. *Patrick Breyer v. Bundesrepublik Deutschland*, B. No: C-582/14, 14.10.2016, Çevrimiçi https://curia.europa.eu/jcms/jcms/j_6/en/ 29.03.2020; Belirlenebilirlik WP29'a göre doğrudan ve dolaylı belirlenebilirlik olarak ayrılabilir. Doğrudan belirli/ belirlenebilir olmak en çok kişinin ismi ile tanınması olarak örneklendirilebilir, dolaylı belirlenebilirlik ise kişinin belirlenmesini sağlayan benzersiz olmayan tanımlayıcıların benzersiz biçimde kombinasyonları ile dolaylı olarak tanımlanabilmesidir. Ayrıca WP29, belirlenebilirliğin tamamen hipotetik ihtimalini (hypothetical possibility), oldukça muhtemel olma (reasonably likely) standardını taşımadığını belirtmiştir. Bunun yerine belirlenebilirlik maliyeti, işlemenin sarfiyatı ya da zımni amacı, mahremiyet yükümlülüğünün ihlali gibi idari işlevsizlik riskleri, teknik başarısızlıklar, işlemenin gerçekleştiği andaki teknolojinin durumu, gelecekteki olası teknolojik ilerlemeler, anonimliği sağlayacak tedbirleri göz önüne alarak belirlenebilir olma ihtimalini değerlendirmeyi önermiştir. Bkz. Nadezhda Purtova, "The Law of Everything: Broad Concept of Personal Data and Future of EU Data Protection Law", **Law, Innovation and Technology**, c. 10, s. 1, 2018, s. 47.

²⁶⁶ Şehriban İpek Aşıkoğlu, **Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri**, İstanbul, On İki Levha Yayıncılık, 2018, s. 19.

²⁶⁷ *Benedik v. Slovenya*, B. No: 62357/14, 24.04.2018, Çevrimiçi <https://hudoc.echr.coe.int/> 29.03.2020.

da tespiti yapılan bu IP adresinin, bilgisayar her açıldığında yeniden belirlenen dinamik IP adresi olduğundan bahisle trafik verisi olarak değerlendirilmesi gerektiğini ileri sürmüştür ki trafik verileri de kişisel veridir. AİHM de ABAD'nin IP adresinin internet kullanıcılarının tam olarak tespitini sağlayan kişisel veri olduğu kararına²⁶⁸ atıf yapmış ve Slovenya Ceza Muhakemesi Kanunu m. 149b/3'ün dinamik IP adreslerinin temini için değil, yalnız elektronik iletişim aracı sahibi veya kullanıcısı hakkında bilgi talebine ilişkin olduğuna hükmetmiştir. Bu durumda da hakim kararı olmaksızın dinamik IP adresinin temini AİHS m. 8'in ihlaline yol açmıştır²⁶⁹.

Ancak bazı hallerde IP adresinin paylaşılması kişisel verilerin korunması ve özel yaşamın gizliliğinin ihlali mahiyetinde olmayabilir. *K.U. v. Finlandiya* başvurusuna konu olayda başvurusunun on iki yaşındayken kişisel bilgileri ve telefon numarası internette bir flört sitesinde paylaşarak cinsel ilişki aradığına dair reklam verilmiştir²⁷⁰. Başvurucu, e-mail aldığı bu reklamdan haberi olmuştur ve kolluk makamına başvurmuştur. Kolluğun talebine rağmen internet servis sağlayıcısı, internet kullanıcısının dinamik IP adresini kanunda belirtilen iletişim güvenliğine dayanarak paylaşmamıştır²⁷¹. Başvurucu da maddi ve manevi bütünlüğünün ihlal edildiğini ve iç hukukta failin tespit edilmemesi nedeniyle özel yaşama saygı hakkının ihlal edildiğini iddia etmiştir. AİHM, Bakanlar Komitesi'nin 95 (13) sayılı Tavsiye Kararı'na değinmiştir. Karar'ın 12. maddesine göre yetkili soruşturma makamı tarafından istendiğinde, kamu veya özel ağlar aracılığıyla telekomünikasyon hizmetleri sunan hizmet sağlayıcılarına kullanıcıyı tanımlamak ve vermek için özel yükümlülükler uygulanmalıdır. AİHM, ifade özgürlüğünün ve iletişimin gizliliğinin telekomünikasyon ve internet hizmetlerinin öncelikli amaçlarından olduğunu ancak bunların etkili bir ceza soruşturmasının yürütülmesi amacı karşısında mutlak olmadığını vurgulamıştır. IP adresinin paylaşılmamasının da başvurusunun maddi ve manevi bütünlüğünü ihlal ettiği sonucuna varmıştır²⁷². AİHM'ye göre söz konusu olay

²⁶⁸ Bkz. *Scarlet Extended*, B. No: C-70/10, 24.11.2011 Çevrimiçi https://curia.europa.eu/jcms/jcms/j_6/en/ 29.03.2020.

²⁶⁹ Tamer Soysal, "Unutulma Hakkının Avrupa Birliği'nin Genel Veri Koruma Tüzüğü Çerçevesinde İncelenmesi", *Uyuşmazlık Mahkemesi Dergisi*, Yıl 7, s. 13, Haziran 2019, s. 346-347.

²⁷⁰ *K.U. v. Finlandiya*, para. 7.

²⁷¹ *K.U. v. Finlandiya*, para. 9.

²⁷² *K.U. v. Finlandiya*, para. 49.

iç hukukta “kasten yanlış beyan (malicious misrepresentation)” olarak nitelendirilmişse de on iki yaşındaki bir çocuğun durumu gözetildiğinde bu, maddi ve manevi bütünlüğüne ciddi bir müdahaledir²⁷³ ve devletin bu müdahale karşısında sorumluyu tespiti olanak vermeyen mevzuatı, özel yaşamın korunması konusunda pozitif yükümlülüğünü ihlal ettiğini göstermektedir.

Dünyada çocuk pornografisi izleyenlerin IP adreslerinden tespit edilerek pedofili haritası çıkaran “pedomap.live” isimli sitenin Türkiye’de bir ilde emniyet güçleri ile anlaşma yaptığı son dönemde gündeme gelmiştir²⁷⁴. Site, çocuk pornografisine ilişkin içeriklerini izlemiş/indirmiş kullanıcıların IP adreslerini maskeleyerek yayınlamakta ve kolluk güçlerine site ile işbirliği yapmayı tavsiye etmektedir²⁷⁵. Site VPN ve TOR’dan arındırılmış IP adresi sunduğunu belirtmektedir, ancak sitenin kullanıcıların kişisel verisi olan IP adreslerini nasıl temin ettiğine ilişkin bir bilgi bulunmamaktadır. IP adreslerinin hukuka uygun olarak elde edilmesi ve işlenmiş olması halinde, kolluk güçlerinin de özel kişilerce işlenmiş bu kişisel verilerden Kolluk ve Ceza Adaleti Direktifi uyarınca yararlanması kanaatimizce mümkündür ve çocuk pornografisi ile mücadelede ileri bir adımdır.

F. Özel Soruşturma Yöntemleri

Avrupa ve ABD’de terörle mücadele başta olmak üzere ulusal güvenlik ve kamu güvenliğini sağlama lehine yapılan düzenlemeler ile kolluğun kişisel verilerin

²⁷³ K.U. v. Finlandiya, para. 41.

²⁷⁴ “Çocuk Pornosu İzleyenleri Tespit Eden Sistem Türkiye’de”, Cumhuriyet Gazetesi, 14.07.2020, Çevrimiçi <https://www.cumhuriyet.com.tr/haber/cocuk-pornosu-izleyenleri-tespit-eden-sistem-turkiyede-1751575> 20.07.2020.

²⁷⁵ Çevrimiçi <https://pedomap.live/about> 20.07.2020; Özel kişilerce çocuk pornografisi ve pedofili ile mücadele yakın tarihte Birleşik Krallık’taki bir ceza yargılamasına da konu olmuştur. Pedofili avcılarının denilen bir grup (Groom Resisters Scotland) bir internet sitesinde on üç yaşındaki bir çocukmuş gibi bir yetişkin olan Sutherland ile yazışmıştır ve Sutherland’dan gelen cinsel görüntü ve yazışmalar üzerine grup, yazışma ve görüntüleri polisle paylaşmıştır. Yargılanan ve mahkum edilen Sutherland, AİHS m. 8 kapsamında özel yaşamın gizliliğine saygı hakkının ihlal edildiğini iddia ederek temyiz başvurmıştır. Temyiz Mahkemesi, delilleri kolluk makamına sunan kişilerin özel kişiler olduğu ve Sutherland ve bu kişiler arasındaki iletişimde Sutherland’ın makul gizlilik beklentisi olmadığını belirtmiştir. Zira Sutherland rızaen Grindr ve Whatsapp üzerinden cinsel amaçla çocuk olarak bildiği kişi ile konuşmuştur (para. 23). Sutherland’ın çocuk olarak bildiği kişi ile konuşmalarının niteliği ve m. 8 bağlamında makul gizlilik beklentisinin olmadığı gözetilerek bu konuşmaların kolluk makamları ile paylaşılması m. 8’in ihlali olarak nitelendirilmemiştir ve temyiz başvurusu reddedilmiştir. Sutherland v Her Majesty’s Advocate (Scotland), 15.07.2020, Çevrimiçi <https://www.supremecourt.uk/cases/docs/uksc-2020-0022-judgment.pdf> 20.07.2020.

korunması ve özel yaşama müdahale teşkil eden yetkileri artırılmıştır²⁷⁶. Günümüzde kolluğun önleyici ya da bastırıcı faaliyetleri sırasında bilgisayar ya da diğer teknolojik araçlar ile elde ettiği kişisel veriler, suç işlenmesinin önlenmesi ya da işlenen bir suçta maddi gerçeğin ortaya çıkarılması için kullanılmaktadır. AİHM de organize suçlar ve terör suçları başta olmak üzere suçlulukla mücadelede istisnai koşullarla mektup, posta, telekomünikasyon üzerinde izleme yetkisi veren kanunların demokratik bir toplumda gerekli olduğunu kabul etmiştir²⁷⁷. Bu türden özel soruşturma yöntemlerine, kolluğun tehlikeyi önleme amacıyla veya ceza muhakemesindeki adli yetkileri kapsamında başvurması mümkündür. Bu yöntemlere hangi amaçla başvurulduğunu tespit *eşik teorisi* uygulanır ve yapılan işlemin ağırlık noktasının suç işlenmesinin önlenmesi yahut suçun aydınlatılması olduğu tespit edilir²⁷⁸. Özel soruşturma yöntemleri, gizli olarak uygulandığı için keyfi uygulama riski de bir hayli yüksektir²⁷⁹.

1970’li yıllarda ortaya çıkan organize suçluluk²⁸⁰ ile suçun yapısı, kapsamı, suç işleme yöntemleri ve organize yapı profesyonel bir görünüme bürünmüştür. Ceza muhakemesindeki klasik koruma tedbirleri ile organize suçlulukla mücadele de bir hayli zorlaşmıştır²⁸¹. Zira suç örgütleri içlerine sızılmasını önleyici tedbirlere başvurmakta ve adliye, basın ve siyasi organlar üzerinde baskı kurmaya çalışmaktadır. Organize suçlulukta failleri ve delil elde etmeyi güçleştiren engelleri aşmak için ceza

²⁷⁶ Anglo Amerikan ve Kıta Avrupası’nda, ceza adalet sistemindeki modellerden kişi hak ve özgürlüklerini önceleyen *due process modeli* ve kolluk faaliyetlerinin işlerliğini sağlamak için güvenlik ihtiyaçlarını önceleyen *crime control modeli* arasında bir denge sağlanmaya çalışılmaktadır. Ancak terör ve örgütlü suçlulukla mücadele için kolluğun yetkilerinin artırılması eğilimi yükseliştir ve bunu, devletlerin ceza hukukunun “güvenlik hukuku”na evrilmesi olarak yorumlamak da mümkündür. Bkz. Bayram, **a.g.e.**, s. 1-3.

²⁷⁷ *Klass ve diğerleri v. Almanya*, B. No: 5029/71, 06.09.1978, para. 48 Çevrimiçi <https://hudoc.echr.coe.int/> 29.03.2020; Küzeci, **a.g.e.**, s. 161; Bayram, **a.g.e.**, s. 2; Benzer yönde bkz. Renzo Orlandi, “Telekomünikasyon Yoluyla İletişimin Önleme ve Adli Amaçlı Denetlenmesi-Özel Yaşamın Gizli Alanı, Teknik Araçla İzleme, Online Arama ve Kendi Kişisel Bilgileri Üzerinde Karar Verebilme Hakkı”, Çev. Ali Kemal Yıldız, **Dünyada ve Türkiye’de Ceza Hukuku Reformları Kongresi**, c. 1, Ed. Adem Sözüer, İstanbul, On İki Levha Yayıncılık, 2013, s. 139.

²⁷⁸ Yenisey, **Kolluk Hukuku**, s. 326.

²⁷⁹ Ursula Kilkely, “Özel Yaşama ve Aile Yaşamına Saygı Gösterilmesi Hakkı”, **İnsan Hakları El Kitapları No.1**, Almanya, Avrupa Konseyi, 2001, s. 48.

²⁸⁰ 1970’li yıllarda sınırötesi organize suçluluk, uyuşturucu trafiği, yasadışı göç ve terör suçluluğunun yaygın olmasının nedeni olarak 1957 tarihli Roma Antlaşması’nın Avrupa Topluluğu dâhilinde serbest dolaşım noktasında yarattığı özgürlük alanı olduğuna dair bkz. Ertan Beşe, **Terörizm, Avrupa Birliği ve İnsan Hakları**, İstanbul, Seçkin Yayıncılık, 2002, s. 69.

²⁸¹ Gottfried Plagemann, “Alman Hukuku’nda Gizli Soruşturmacının Kullanılması ve Gizli Soruşturmacının Yetkileri”, **CHKD**, c. 2, s. 1-2, 2014, s. 160; Ünver, “Federal Almanya’da Terör ve Organize Suçluluk ile İlgili Düzenlemeler”, s. 388.

muhakemesi hukukunda bilgisayar analizi, teknik araçla takip, iletişimin denetlenmesi gibi yöntemlere başvurulmuştur²⁸². Organize suçlulukla mücadelede örgüt bağlantılarını tespit edebilmek için para hareketlerinin takibi ve hatta uçak yolcu listelerinin incelenmesi gibi kişisel verilerin de incelenmesi gerekir²⁸³. Ancak şüphesiz ki teknolojik olanaklardan yararlanarak önleyici tedbirler ve koruma tedbirlerine başvurulduğunda bu, adil yargılanma hakkı²⁸⁴, özel yaşamın gizliliğine saygı hakkı ve kişisel verilerin korunması hakkı başta olmak üzere temel hak ve özgürlüklere müdahale mahiyetindedir.

Doktrinde bir görüşe göre gizli soruşturma yöntemleri de dâhil devletin tüm bilgi toplama faaliyetleri kişilerin temel hak ve özgürlüklerine müdahale teşkil ettiği için kanunla düzenlenmelidir. Diğer görüşe göre devletin tüm bilgi toplama faaliyetleri temel haklara müdahale olmayıp gizli soruşturma yöntemleri kullanılarak şüphelinin aldatılması hali, kişinin *bilgi alışverişi faaliyetlerini serbestçe belirleme hakkına* müdahaledir ve bu nedenle gizli soruşturma yöntemlerinin kanunla düzenlenmesi yeterlidir. Alman yüksek mahkemelerinin içtihatlarında da yer almış bir diğer görüşe göre ise devletin iç güvenliği ve ceza adaletinin sağlanması için gizli soruşturma yöntemlerine başvurmak gerekmektedir ve bu, temel hak ve özgürlükleri ihlal etmediğinden kanunla düzenleme gerekmemektedir²⁸⁵.

Gizli soruşturma yöntemlerinin ceza muhakemesinde kullanılması ve bu yöntemler sonucu elde edilen kişisel veri işleme faaliyetleri, temel hak ve özgürlüklere müdahaledir ve kanunla düzenlenmesi gerekir. Nitekim Almanya’da da Federal Anayasa Mahkemesi’nin kişisel verilere ilişkin meşhur Nüfus Sayımı Kararı gözetilerek²⁸⁶ anayasaya aykırılık iddiası ile karşılaşmamak için 1992 tarihli Yasadışı Uyuşturucu Madde Ticareti ve Organize Suçluluğun Diğer Görünüş Şekilleri ile

²⁸² Adem Sözüer, “Organize Suçlulukla İlgili Kovuşturma Yöntemleri (İletişimin Dinlenmesi)”, **Legal Hukuk Dergisi**, c. 1/B, s. 10, İstanbul, 2003, s. 2495-2496.

²⁸³ Yenisey, **Kolluk Hukuku**, s. 2.

²⁸⁴ Organize suçluluktaki artışın buna uygun tedbirler alınmayı gerektirmesine rağmen adil yargılanma hakkının yine de ön planda olması gerektiğine ilişkin bkz. Volkan Aslan, “Avrupa İnsan Hakları Mahkemesi Kararlarında Ajan Provokatör ve Adil Yargılanma Hakkı”, **Hukukçular Arası Makale Yarışması**, Ed., Türkiye Barolar Birliği, Ankara, TBB Yayınları, 2014, s. 30.

²⁸⁵ Sözüer, “Organize Suçlulukla İlgili Kovuşturma Yöntemleri (İletişimin Dinlenmesi)”, s. 2497.

²⁸⁶ Kararın detaylı analizi için bkz. Dülger, **Kişisel Verilerin Korunması Hukuku**, s. 22-23.

Mücadele Edilmesine İlişkin Kanun ile organize suçlulukla mücadelede yeni araştırma yöntemlerine başvurulacağı düzenlenmiştir²⁸⁷.

Türkiye’de 4422 sayılı Çıkar Amaçlı Suç Örgütleriyle Mücadele Kanunu’nda ilk kez gizli soruşturmacı ve teknik araçla takip özel koruma tedbirleri olarak düzenlenmiş ve Türk Ceza Hukuku Reformu’nun bir sonucu olarak telekomünikasyon yoluyla iletişimin tespiti, teknik araçla izleme ve gizli soruşturmacı görevlendirilmesi olarak özel soruşturma yöntemleri CMK’de yer almıştır²⁸⁸.

Avrupa Konseyi Bakanlar Komitesi’nin İnsan Hakları ve Terörle Mücadelede Rehber İlkeleri’ne²⁸⁹ göre AB Konseyi üye devletleri, ülkelerinde güvenliği sağlamak için bulundukları faaliyetlerde kişisel verilerin toplanması ve özel yaşamın gizliliğine saygının sağlanması için ilkeleri gözeterek hareket etmelidir. 5. ilke terörizmle mücadele bağlamında, kişisel verilerin devlet güvenliği alanındaki herhangi bir yetkili otorite tarafından toplanması ve işlenmesinde, özel olarak bu tür toplama ve işlemenin; uygun iç hukuk hükümlerine tabi olması, toplama ve işlemenin öngörülen amaçla orantılı olması ve bağımsız bir otoritenin denetimine tabi olması gerektiğini belirtmiştir. 6. ilkeye göre ise terörizmle mücadelede kullanılan ve mahremiyete müdahale teşkil eden özellikle üst araması, konutta arama, telefon dinleme, yazışmanın denetimi ve gizli ajan kullanımı gibi önlemler hukuka uygun olmalı ve hukukilik denetiminin mahkemelerce yapılması mümkün olmalıdır.

²⁸⁷ Ünver, “Federal Almanya’da Terör ve Organize Suçluluk ile İlgili Düzenlemeler”, s. 402; Ayrıca Alman CMK’de 110a, b ve c maddelerinde tanım, başvurma şartları ve yetkileri ile gizli soruşturmacı kanun düzeyinde kanuni dayanağa kavuşmuştur. Plagemann, **a.g.e.**, s. 163.

²⁸⁸ Öztürk/Eker Kazancı/Soyer Güleç bu tedbirleri, “Modern Koruma Tedbirleri” olarak değerlendirmektedir. Bkz. Öztürk, Eker Kazancı, Soyer Güleç, **a.g.e.**, s. 213; Telekomünikasyon yoluyla iletişimin tespiti ve teknik araçla izlemeyi “Elektronik Takip İşlemleri” olarak sistematize eden eser için bkz. Çam, **a.g.e.**, s. 40.

²⁸⁹ “Guidelines on Human Rights and The Fight Against Terrorism”, 11.07.2002 tarihli Bakanlar Komitesi’nin 804. toplantısında bu ilkeler kabul edilmiştir.

Bakanlar Komitesi'nin 2017 (6) sayılı Tavsiye Kararı'na²⁹⁰ göre terör eylemleri gibi ciddi suçlarda özel soruşturma teknikleri²⁹¹ kullanılabilir. Özel soruşturma teknikleri kullanılarak varılan sonuç, daha az müdahale gerektiren bir yöntemle sağlanamayacaksa özel soruşturma tekniğinin kullanımı ölçülüdür. Söz gelimi yürütülen soruşturmada iki şüpheli arasındaki bağ, soruşturmanın etkinliğini tehlikeye atmaksızın sorgu, tanık beyanları, arama kayıtlarına başvurulması ile tespit edilebiliyorsa telefon dinleme gibi daha fazla müdahaleci tekniklere başvurulmamalıdır²⁹². Bu önlemler özellikle gizli uygulandıkları için nitelik ve uygulanmaları gereği şüpheli ve sanık harici üçüncü kişilerin de kişisel verilerinin korunması hakkına müdahale oluşturmaktadır ve sınırlamalara gidilmelidir²⁹³.

1. Telekomünikasyon Yoluyla İletişimin Denetlenmesi

a. İletişimin Denetlenmesi Şartları

Telekomünikasyon yoluyla iletişimin tespitine ceza muhakemesinde başvurulabilmesi için birtakım şartlar gerekmektedir. Öncelikle kanunda bir suç kataloğu olmalı ya da fiil belirli bir ağırlıkta olmalıdır. Zira bu tedbir bireysel iletişim vasıtalarına müdahale gerektirmekte ve her suç bakımından bu tedbire başvurulması haberleşme özgürlüğüne ciddi müdahale oluşturmaktadır²⁹⁴. Bu suçların belirlenmesinde karşılaştırmalı hukukta; suç kataloğu, tedbirin uygulanacağı suçlar bakımından mutlak cezalandırılabilirlik sınırı ve suçun ağırlığı olmak üzere üç yöntem

²⁹⁰ 05.07.2017 tarihli Bakanlar Komitesi kararıdır. Recommendation CM/Rec(2017)6 of the Committee of Ministers to member States on "special investigation techniques" in relation to serious crimes including acts of terrorism; Bu karardan önce de terör suçları dâhil ağır suçlara yönelik bir diğer karar Bakanlar Komitesi'nin 2005 (10) sayılı Tavsiye Kararı'dır. Bu karardaki özel soruşturma tekniklerinin detaylı değerlendirmesi için bkz. Begüm Bulak Uygun, "Avrupa İnsan Hakları Mahkemesi'nin Son Dönemdeki İçtihatları Işığında İletişimin Adli ve Önleme Amaçlı Olarak Denetlenmesi ve Özel Hayata Müdahale", *YÜHFD*, c. 13, s. 2, 2017, s. 144 vd.

²⁹¹ Bkz. Allen, van Beek, Borking, *a.g.e.*, s. 18 "Yetkili makamlarca, ciddi suçları önlemek, tespit etmek, soruşturmak, kovuşturmak ve bastırmak amacıyla, hedef kişileri uyarmayacak şekilde bilgi toplamayı amaçlayan ceza soruşturmaları bağlamında uygulanan teknikler."

²⁹² Allen, van Beek, Borking, *a.g.e.*, s. 9.

²⁹³ Ünver, "Federal Almanya'da Terör ve Organize Suçluluk ile İlgili Düzenlemeler", s. 437.

²⁹⁴ Sözüer, "Organize Suçlulukla İlgili Kovuşturma Yöntemleri (İletişimin Dinlenmesi)", s. 2501.

kullanılmaktadır²⁹⁵. Ayrıca tedbiri öngören kanunda, koruma tedbirlerinin süreli olmasından hareketle azami bir süre sınırı bulunmalıdır.

Özellikle çocuk pornografisi ve terör suçlarıyla mücadelede internet üzerindeki materyalleri tespit etmek için soruşturma faaliyetlerinde telekomünikasyon yoluyla iletişimin denetlenmesi tedbirine sıklıkla başvurulmaktadır²⁹⁶. Alman Anayasa Mahkemesi, ceza muhakemesinde telekomünikasyon hareketliliğine ilişkin kişisel verilerin kullanılmasına dair bir kararında kanun koyucunun dikkat etmesi gereken hususları saymıştır. Buna göre kanun koyucu, verilerin güvenliğini sağlamalı ve detaylı organize ve teknik düzenlemelere yer vermelidir. Zira bu veriler özel telekomünikasyon hizmeti sağlayıcıları tarafından depolanmaktadır ve veri hırsızlığı veya ekonomik casusluk faaliyetlerine konu olabilirler²⁹⁷. Verilerin kullanımının tabi olduğu koşullar belirlenmelidir. Örneğin; her suç bakımından değil, yalnız ağır bir suçun varlığı halinde yetkili makamlar hizmet sağlayıcılarından bu verileri talep edebilmelidir. Verilerin yok edilmesi halinde de bu husus bir tutanağa bağlanmalıdır. Adli makamlardan istihbarat makamlarına bu telekomünikasyon verileri aktarıldığında, istihbarat makamı görevini yerine getirebilmek için bu verileri doğrudan hizmet sağlayıcısından istemeye yetkili olmalıdır²⁹⁸. Mahkemenin aradığı bir diğer şart da şeffaflıktır. Buna göre telekomünikasyon verileri yetkili makamlarca kullanıldığında veri sahibi bu hususa dair bilgilendirilmelidir. Bildirimin yapılmasının soruşturmanın amacını tehlikeye düşürmesi halinde istisnai olarak bildirimden sarfınazar edilebilir. Ancak bu halde de hakim hukuka uyarlık olup olmadığını takip etmelidir. Son olarak da kişisel verilerin bu tedbir gereği kaydedildiği hallerde veri sahibine etkili bir hukuki koruma sağlanmalıdır. Etkili hukuki korumayı gerçekleştirecek kanuni düzenlemeler, ceza muhakemesinde delil değerlendirme

²⁹⁵ Sözüer, “Organize Suçlulukla İlgili Kovuşturma Yöntemleri (İletişimin Dinlenmesi)”, s. 2504; Örneğin Polonya Ceza Muhakemesi Kanunu m. 237’de adam öldürme, insan ticareti, yağma, casusluk gibi kanunun belirttiği suç kataloğunda yer alan suçlarda iletişimin denetlenmesine başvurulmaktadır. Fransa Ceza Muhakemesi Kanunu m. 100’e göre de tedbir konusu suçun iki yıl veya daha fazla ceza gerektiren bir suç olması gerekmektedir. Bkz. Güray Dağ, “Kişisel Verilerin Ceza Muhakemesi Hukukunda Delil Olarak Kullanılması”, **Marmara Üniversitesi Sosyal Bilimler Enstitüsü**, Yayınlanmamış Doktora Tezi, İstanbul, 2011, s. 128.

²⁹⁶ Mark A. Zöller, “Telekomünikasyon Verilerinin Depolanarak Kaydedilmesi (Alman) Uygulaması ve Yanlış Uygulaması”, Çev. Hakan Karakehya, **Dünyada ve Türkiye’de Ceza Hukuku Reformları Kongresi**, c. 1, Ed. Adem Sözüer, İstanbul, On İki Levha Yayıncılık, 2013, s. 166.

²⁹⁷ Zöller, **a.g.e.**, s. 171-172.

²⁹⁸ Zöller, **a.g.e.**, s. 172.

yasağı ve özel hukukta veri sahibinin kişilik hakkının ihlalinin doğan zararın tazmini biçiminde olabilir²⁹⁹.

Gizli telefon dinlemelerini m. 8 altında değerlendiren AİHM, *Klass ve diğerleri v. Almanya* başvurusunda değerlendirme yapmıştır³⁰⁰. Başvuruya konu olayda Mektup, Posta ve Telekomünikasyonun Gizliliğinin Sınırlandırılması Kanunu'nun AİHS'ye aykırı olduğu ileri sürülmüştür. Başvurucular bu Kanun'un uygulanması ile mevcut bir zarara uğramamışlardır. Ancak başvurucular; telefon görüşmelerinin denetlenmesi ve kişiler hakkında önlem alabilme yetkisini getiren ve bu uygulamaya karşı da hak arama yöntemi öngörmeyen bu Kanun'un salt mevcut olmasıyla potansiyel mağdur olduklarını iddia etmişlerdir. AİHM de haberleşmenin gizli denetlenmesine izin veren mevzuatın varlığının m. 8'e müdahale olduğunu ve başvurucuların potansiyel mağdur olduğunu kabul etmiştir³⁰¹. AİHM *Uzun v. Almanya* başvurusunda ise bu tedbire başvurulmasına olanak sağlayan kanunun içermesi gereken hususları saymıştır. Buna göre suçların niteliği, iletişimi denetleme sorumlularının tanımı, denetimin süresi, elde edilen verilerin incelenmesi, kullanılması ve saklanması için izlenecek prosedür, veriler diğer taraflara iletilirken alınacak önlemler ve elde edilen verilerin silinebileceği veya kayıtların imha edilebildiği durumlar kanunda düzenlenmiş olmalıdır³⁰².

b. Trafik Verisi

Trafik verisi, elektronik iletişim ağları üzerinden iletişimin sağlanması ve bu amaçla faturalandırma için işlenen, iletişimin başlangıç ve hedefe varma noktasını,

²⁹⁹ Zöller, **a.g.e.**, s. 172-173.

³⁰⁰ Telefon görüşmelerinin dinlenmesi ve kaydı, posta gönderilerinin açılması ve okunmasının haberleşmenin gizliliğine ve özel yaşama müdahale olduğuna dair diğer örnekler için bkz. Gözübüyük, **Gölcüklü, a.g.e.**, s. 354.

³⁰¹ Küzeci, **a.g.e.**, s.158; Gizli dinlemenin zorlayıcı bir toplumsal ihtiyaç sonucu olması halinde kamu makamları buna başvurabilecektir. Ancak bireylerin hangi koşul ve durumda dinlenebilecekleri öngörülebilir olmalıdır. Bu hususta asgari güvenceler *Klass ve diğerleri v. Almanya* kararında AİHM tarafından sayılmıştır. Buna göre denetleme kararı alınmasına yol açan suçların niteliği, telefonları dinlenecek kişi kategorilerinin belirlenmesi, dinleme süresine getirilebilecek sınır, elde edilen bilginin diğer kişilere aktarılmasında alınacak önlemler, kayıtların silinme, yok edilme koşullarının kanunda açıkça yer alması gerekmektedir. Akt. bkz. Arslan Öncü, "Özel Yaşama ve Aile Yaşamına Saygı Hakkı", s. 324.

³⁰² *Uzun v. Almanya*, B. No: 35623, 02.12.2010, para. 65; Aynı yönde bkz. *Roman Zakharov v. Rusya* [BD], B. No: 47143/06, 04.12.2015, para. 231 Çevrimiçi <https://hudoc.echr.coe.int/> 29.03.2020.

yolu, saati, süresini gösteren veridir³⁰³. İletişimin başlangıç noktası, iletişimin tanımlanmasını sağlayacak bir telefon numarası, IP adresi yahut benzeri bilgi olabilir³⁰⁴. Konum verisi ise, elektronik iletişim hizmeti kullanıcılarının yararlandığı iletişim aracının coğrafi pozisyonunu belirleyen veridir³⁰⁵. Trafik internet verisi aracılığıyla internet ortamındaki erişimin tarafları, erişimin süresi, veri miktarı ve bağlantı noktaları tespit edilmektedir³⁰⁶. 95/46 sayılı Direktif'te açıkça sayılmamış olsa da gerçek kişilere dair konum verisi³⁰⁷ Kolluk ve Ceza Adaleti Direktifi kapsamında kişisel veridir. Zira kullanıcı veya abonenin iletişiminden ve konumundan yararlanarak kimliği belirlenebiliyor ise trafik ve konum verisi kişisel veridir³⁰⁸. Bir verinin hem trafik verisi hem de konum verisi olması halinde, özel düzenleme olarak trafik verisi korumasından yararlanması gerektiği belirtilmiştir. Zira 2002/58 sayılı Direktif, özellikle trafik verisi haricinde olan konum verilerine ilişkin düzenleme öngörmüştür³⁰⁹. Ancak Kolluk ve Ceza Adaleti Direktifi'nde böyle bir ayırım yer almadığından kişisel veri mahiyetinde olması halinde trafik ve konum verisi de aynı kişisel verilerin korunması hakkından yararlanacaktır.

Avrupa Konseyi, Avrupa'da yükselen terörizm sonucu yayımladığı Terörle Mücadele Deklarasyonu³¹⁰ ile üye devletlere, hizmet sağlayıcıları tarafından

³⁰³ Avrupa Konseyi Siber Suçlar Sözleşmesi m. 1/d; 2002/58 sayılı Direktif m. 2/b; Trafik verisi için “İnternet ortamında gerçekleştirilen her türlü erişime ilişkin kütük bilgisi” biçiminde tanım için bkz. Durmuş Tezcan, Mustafa Ruhan Erdem, R. Murat Önok, **Teorik ve Pratik Ceza Özel Hukuku**, Güncellenmiş 17. Baskı, Ankara, Seçkin Yayıncılık, 2019, s. 653.

³⁰⁴ Serap Keskin, “Avrupa Konseyi Siber Suçlar Sözleşmesinde Ceza Muhakemesine İlişkin Hükümlerin Değerlendirilmesi”, **İÜHF**, c. 59, s. 1-2, 2001, s. 173.

³⁰⁵ Gür, **a.g.e.**, s. 79.

³⁰⁶ Servet Yetim, “5651 Sayılı Yasa Kapsamında Tutulan İnternet Trafik Bilgilerinin Özel Yaşam ve Yaşamın Gizliliği Kapsamında Değerlendirilmesi”, **Terazi Hukuk Dergisi**, c. 4, s. 36, 2009, s. 56.

³⁰⁷ Konum verisi haricinde gerçek kişilere ait çevrimiçi tanımlayıcılar da kişisel veridir, bu da Direktif'in küresel teknolojik ilerlemelere uygun bir mantaliteyle hazırlandığını göstermektedir. Bkz. Salami Emmanuel Akintunde, “The Impact of Directive (EU) 2016/680 on the Processing of Personal Data by Competent Authorities for The Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties and On the Free Movement of Such Data on the Existing Privacy Regime”, Çevrimiçi <http://dx.doi.org/10.2139/ssrn.2912449> 10.04.2019, s. 4.

³⁰⁸ Ancak çağrı yapan bir telefon kulübesinin konum verisi, kişisel veri niteliğinde değil, yalnız trafik ve konum verisidir. Bkz. Ayşe Çiğdem Ayözger, **Kişisel Verilerin Korunması**, İstanbul, Beta Yayıncılık, 2016, s. 149.

³⁰⁹ Türk hukukunda ise Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik'te 2013 yılında yapılan değişiklikle konum verisi (m. 3/j) ve trafik verisi (m. 3/p) ayrı tanımlanmış ve bu veriler bakımından ayrı işleme şartları (m. 8 ve 11) öngörülmüştür. (R.G. Sayısı: 28363, R.G. Tarihi: 24.07.2012).

³¹⁰ Deklarasyon, 25.03.2004 tarihinde Avrupa Konseyi (European Council) tarafından ilan edilmiştir.

haberleşme trafik verilerinin tutulmasına ilişkin kurallar oluşturmasını önermiştir. Ceza muhakemesinde trafik ve konum verilerinin önemi göz önüne alındığında, iletişim hizmetlerinin temini sırasında işlenen verilerin, halka açık elektronik iletişim hizmet sağlayıcısı veya kamu iletişim hizmet sağlayıcısı tarafından muhafaza edilmesi gerekmektedir³¹¹.

Mobil telefon yoluyla gerçekleşen iletişimde hizmet sağlayıcısı, mobil telefon kullanıcısının iletişiminin tarih ve yerini, telefonun ne zaman nerede olduğunu tespit edebilmektedir. Bu nedenle mobil telefon kullanıcılarının, hizmet sağlayıcısının sahip olduğu bu bilgileri kimlerle paylaştığını ve bu bilgilerin ne amaçla kullandığını bilmesi gerekmektedir³¹². 2002/58 sayılı Direktif'e göre kullanıcı ve kayıtlı abonelerin iletişiminin iki ya da daha fazla coğrafi nokta arasında olması halinde, bu noktaların başlangıç, devam ve bitiş tarihlerinin tespitinde trafik verilerinden yararlanmak mümkündür³¹³. Mülga 2006/24 sayılı Direktif'te de veri sorumlusunun yetkisi trafik ve konum verilerini tespit ile sınırlı olup iletişim içeriğinin tespiti yetkisi bulunmamaktadır.

Akıllı telefon kullanımındaki artış ve konum belirleme uygulamaları ile kişilerin konumlarının hukuka uygun şekilde tespit edilmesi ve işlenmesine ilişkin rızalarının nasıl sağlanacağı tartışma konusu olmuştur. Hukuka uygun işlemeyi sağlamak için akıllı telefon ve diğer bilgisayar aygıtı gibi elektronik haberleşme cihazlarının konum verilerinin işlenmesinin kapalı olması, ancak kullanıcı ya da abonenin aktif hareketi, tercihi ile konum verisinin açılması gerektiği ileri sürülmüştür³¹⁴.

c. Türk Hukukunda Durum

CMK m. 135'e göre iletişimin tespiti kapsamında; iletişimin dinlenmesi, kayda alınması ve sinyal bilgilerinin değerlendirilmesi yer almaktadır. İletişimin dinlenmesinden anlaşılabilecek olan telli, telsiz telefon veya internet aracılığıyla yapılan

³¹¹ Bkz. *Digital Rights Ireland*, para. 11.

³¹² Küzeci, **a.g.e.**, s. 43.

³¹³ Ayrıca roaming halinde kullanıcının hangi noktada kimlerle elektronik yollarla iletişim kurduğu ve iletişim süresinin tespitinde de trafik verilerinden yararlanılabilmektedir. Bkz. Ayözger, **a.g.e.**, s. 148.

³¹⁴ Ayözger, **a.g.e.**, s. 158.

görüşmelerin öğrenilmesidir³¹⁵. İletişimin kayda alınması, bu görüşmelerdeki ses, görüntü ya da elektronik posta yoluyla yapılan iletişim içeriğinin kaydedilmesidir. Dinlemenin fonksiyonel olabilmesi yani ceza muhakemesinde delil olarak kullanılabilmesi için kayda alınması gerekmektedir³¹⁶. Sinyal bilgisinin değerlendirilmesi; bir şebekede haberleşmenin iletilmesi veya faturalama amacıyla işlenen, telefon görüşmeleri, içerik bilgisi ve faturalandırma bilgilerinin öğrenilmesidir³¹⁷. Mobil telefonun yerinin tespiti ise şüpheli veya sanığın ele geçirilmesi için mağdur veya üçüncü kişiye ait mobil telefonun izlemeye alınmasıdır³¹⁸.

Erişim sağlayıcı ve yer sağlayıcı, trafik verilerini 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'a göre tutmakla yükümlüdür. Trafik verilerinin tutulma amacı; gelişen bilişim teknolojilerinden yararlanan suç ve suçlunun, çocuk, aile ve gençler başta olmak üzere topluma karşı işleyeceği suçlarda önleyici tedbirler alabilmektir³¹⁹. Erişim sağlayıcıları, *“Sağladığı hizmetlere ilişkin, yönetmelikte belirtilen trafik bilgilerini altı aydan az ve iki yıldan fazla olmamak üzere yönetmelikte belirlenecek süre kadar saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla”* yükümlüdür³²⁰. Ancak Kanun'un kişinin suç işlemiş olması veya suçun önlenmesi gibi bir amaç yahut kritere dayanmaksızın trafik verilerini sağlama yükümlülüğü öngörmesi eleştirilmiştir³²¹. Ayrıca düzenleme ile amaç trafik verilerinin tutulmasıdır, ancak trafik verileri yanında birincil kişisel veriler de tutulmaktadır ve verileri bu süre zarfında muhafaza etmekle yükümlü, yer ve erişim sağlayıcısı gibi özel hukuk tüzel kişileridir. En azından birincil nitelikli kişisel verilerin, özel hukuk kişisi hariç bir merkezi sistemde kodlanmış olarak tutulması

³¹⁵ Centel, **a.g.e.**, s. 175.

³¹⁶ Centel, **a.g.e.**, s. 175.

³¹⁷ Centel, **a.g.e.**, s. 175.

³¹⁸ Centel, **a.g.e.**, s. 176.

³¹⁹ Yetim, **a.g.e.**, s. 58.

³²⁰ 5651 sayılı Kanun m. 5/3.

³²¹ Tezcan, Erdem, Önok, **a.g.e.**, s. 653.

önerilmiştir. Ceza muhakemesinde bu verilerden yararlanılması gerektiğinde de yetkili makamlar kodları çözerek kişiye ulaşabilecektir³²².

Bilişim suçları ya da bilişim sistemlerinden yararlanılarak işlenen suçların soruşturulmasında IP adresi ve trafik verilerinden yararlanmak için adli makamlar yer sağlayıcılardan talepte bulunmaktadır. Facebook, Twitter gibi firmalar, adli makamların bu talebini ancak adli yardım yoluyla firma merkezinin bulunduğu devlete yapılan bir talebin ardından yerine getirmektedirler. Bazı hallerde ise doğrudan firmaların Türkiye'deki temsilciliklerine başvurulduğunda IP adresi ve trafik verisi verilmektedir. Örneğin Microsoft'un Türkiye'deki temsilciliği içeriğin tespitine ilişkin talepler hariç bu yolu izlemektedir. Ya da Facebook intihara teşebbüs, kayıpların bulunması ve cinsel istismar hallerinde belirli şartlarla IP adresi ve trafik verisini doğrudan paylaşmaktadır³²³.

Telekomünikasyon yoluyla iletişimin denetlenmesi tedbirinin uygulanması ile kişisel verilerin ceza muhakemesinde kullanılmasında hakim kararı gerekmektedir. Örneğin; *Figuerido Teixeira v. Andorra* başvurusunda ön ödemeli bir hat kullanıcısı olan başvurucunun iki telefon hattına gelen ve giden aramalar, arama listesindeki kişiler ve numaralarının Andorra Telekom'dan hakim kararıyla talep edilmesinin özel yaşamın gizliliğini ihlal edip etmediği değerlendirilmiştir. Verilerin saklanması ve aktarılması kararının soruşturma hakim tarafından verilmesi halinde kamu makamının yetki sınırları açıkça ilgili kanunda belirtildiğinden AİHM müdahaleyi ihlal mahiyetinde bulmamıştır³²⁴.

CMK m. 137/3'e göre telekomünikasyon yoluyla iletişimin tespiti kararı verildiğinde kişi hakkında kovuşturmayaya yer olmadığı kararı verilmişse veya gecikmesinde sakınca bulunan hale dayanılarak savcı kararı ile bu tedbire başvurulmuş ve hakim onayı alınamamışsa savcı tarafından tedbire son verilecek ve kayıtlar en geç on gün içerisinde yok edilecektir. Yok etme için kovuşturmayaya yer olmadığı kararının kesinleşmesi beklenmelidir³²⁵. İletişimin denetlenmesi mahiyeti itibarıyla gizli bir

³²² Yetim, **a.g.e.**, s. 61.

³²³ Dülger, Modoğlu, **a.g.e.**, s. 162-163.

³²⁴ *Figuerido Teixeira v. Andorra*, B. No: 72384/14, 08.02.2017, para. 43 (Akt. Bulak Uygun, **a.g.e.**, s.152).

³²⁵ Centel, **a.g.e.**, s. 182.

tedbir olduğundan belirli bir sürenin sonunda kişiye bilgi verilmesi tedbirin amacına hizmet etmektedir. Hakkında tedbir uygulanan kişiye soruşturma evresinin bitiminde bilgi verilmesinin AY m. 36 hak arama özgürlüğü ve m. 40 yetkili makama başvuru imkânına ket vurduğu doktrinde ileri sürülmüştür³²⁶. Ancak bu görüşe göre gizliliğe tedbir süresince riayet etmek yeterli olup tedbir sona erdikten sonra bu tedbirden yarar da elde edilmişse ilgilinin haberdar edilmesi gerekmektedir. Kişinin haklarını kullanması için soruşturma evresinin sonuna kadar beklemesi gerekmemelidir.

Maddede kişinin beraat etmesi halinde tedbire ilişkin kayıtların yok edilip edilmeyeceği düzenlemesine yer verilmemiştir. Doktrinde kanun koyucunun bu hususu unuttuğu ileri sürülmüşse de³²⁷ kanaatimizce unutma söz konusu değildir. Kanun koyucu bilinçli olarak yalnız soruşturma evresinde CMK m. 135 kayıtlarının yok edilmesini öngörmüştür, zira maddede yalnız savcının yetkisine yer verilmiştir. Ancak beraat halinde tedbir sonucu elde edilen kişisel verilere yönelik bir korumaya yer verilmemesi eksiklik³²⁸, en azından CMK m. 81/2 hükmü minvalinde bir düzenlemeye yer verilmelidir.

Telekomünikasyon yoluyla iletişimin denetlenmesi sonucunda kişi hakkında kayıtların yok edileceği CMK m. 137/3'te düzenlenmişse de bu tedbirin muhatabı olup da kişisel verileri işlenmiş veri sahibine tazminat olanağı tanınmamıştır³²⁹. Zira CMK m. 141/1'de yalnız belirli koruma tedbirleri için tazminat öngörülmüştür. Ancak CMK m. 141/3 hükmüne dayanarak kişi hakkında hakim veya savcının kişisel kusuru veya haksız fiili ile hukuka aykırı bir şekilde iletişimin denetlenmesi kararı vermesi halinde

³²⁶ Handan Yokuş Sevrük, "Postada El Koyma ve Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi", **TBB Dergisi**, c. 20, s. 69, 2007, s. 116.

³²⁷ Bkz. Dağ, **a.g.e.**, s. 197.

³²⁸ Centel, **a.g.e.**, s. 182.

³²⁹ Yokuş Sevrük, "Postada El Koyma ve Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi", s. 116-117.

kişisel verileri işlendiği için tazminat talebinde bulunabilmelidir³³⁰. Ayrıca etkili başvuru hakkının da sağlanabilmesi için CMK m. 141/3 geniş yorumlanmalıdır³³¹.

2. Gizli Gözetleme ve Teknik Araçla Takip

Almanya’da önemli bir suçun işlendiğine dair yeterli şüphenin bulunması halinde bir kişinin kimlik bilgisi ve aracının plaka numarası takibe alınarak kişi kontrol noktalarından geçtiğinde bu kaydedilmekte ve bir süre sonra gizli gözetleme ile elde edilen veriler bir araya getirilerek kişinin davranış tarzı belirlenmektedir³³². Bu koruma tedbirinin amacı, yerel veya federal polis kurumunda bireylerle ilgili belirli bir sisteme kaydedilen verilerden hareketle suç işleyen kişinin hareket planının ortaya konmasıdır³³³. Gizli gözetleme sırasında üçüncü kişilerin kişisel verileri de işlenebilmektedir. Zira belirli şartlarla fail ile ilişkisi olduğundan bahisle şüphelenilen

³³⁰ Bakırköy 11. Ağır Ceza Mahkemesi E. 2016/59, K. 2017/349, T. 13/12/2017 “... İstanbul Cumhuriyet Başsavcılığının ... soruşturma sayılı evrakın incelenmesinde: Davacının İstanbul Emniyet Müdürlüğü Terörle Mücadele Şube Müdürlüğüne yürütülen soruşturma sırasında teknik takip altında tutulduğu, telefonlarının dinlendiği, hakkında iletişim tespit kararları verildiği ve bu kararların bir çok kez uzatıldığı, İstanbul Cumhuriyet Başsavcılığının ... evrakında verilen 02/11/2015 tarihli ... kovuşturmaya yer olmadığına dair karar verildiği anlaşılmış, böylece hakkında haksız yere koruma ve denetim tedbirlerinin uygulandığı, KYOK kararı verildikten sonra davacı hakkında yapılan dinleme kayıtlarının, teknik takip kayıtlarının uyap sistemine yüklenerek 24 farklı dosyaya girdiği, davacı hakkında haksız dinleme sonucunda elde edilen dinleme kayıtlarının hukuka aykırı olarak elde tutulduğu ve yok edilmediği, bu sebeple davacının CMK’nın 141/3. maddedeki şartların gerçekleştiği anlaşılmakla haksız koruma ve denetim tedbirlerine maruz kalan davacının zenginleşmeye yol açmayacak şekilde iletişimin tespiti, dinlenmesi ve kayda alınması ile teknik takip tedbirine başvurulmasından dolayı meydana gelen mağduriyetinin giderilmesi için 1.500 TL manevi tazminatın 02/02/2016 tarihinden itibaren işleyecek yasal faizi ile birlikte haksız dinleme sonucunda elde edilen dinleme kayıtlarının hukuka aykırı olarak elde tutulmasından ve yok edilmemiş olmasından dolayı meydana gelen mağduriyetinin giderilmesi için 1.500 TL manevi tazminatın 10/05/2016 tarihinden itibaren işleyecek yasal faizi ile davalı hazineden alınarak davacıya ... verilmesine hükmedilmesi gerekmektedir.”

³³¹ Nitekim Yargıtay da CMK m. 141/3’ü bir kararında geniş yorumlamıştır. Bkz. Yargıtay 12. CD, E. 2015/13049, K. 2015/17584 “...Tüm bu açıklamalar ışığında davacının iddiaları değerlendirildiğinde, iddianamede mağdur olarak gösterilen davacı hakkında tutulan işleme kayıtlarının iddianamede aynen yer alması, içeriğiyle ilgili hiçbir değerlendirme yapılmaksızın ve değer yargısında bulunulmaksızın CMK’nın 141/3. fıkrası uyarınca tazminatı gerektirmektedir. Zira sanıklara isnat edilen suç gözetildiğinde, bu kayıtların iddianamede aynen yer alması gerekmediği gibi, aynen yer almasında kamusal bir yarar da bulunmamaktadır. Yargılama faaliyetinden kaynaklanan ve emredici veya yasaklayıcı bir norm bulunmaması nedeniyle, kişisel kusur veya haksız fiil kapsamında değerlendirilemeyecek bu özensiz davranış nedeniyle doğan zararın giderilmesinde, Devletin kusursuz sorumluluğu söz konusu olup, yapılan soruşturma ve kovuşturmalarda oluşan bu tür zararların tazminat hukukunun genel ilkeleri çerçevesinde Devlet tarafından karşılanması gerekmektedir.”

³³² Ünver, “Federal Almanya’da Terör ve Organize Suçluluk ile İlgili Düzenlemeler”, s. 410.

³³³ Ünver, “Federal Almanya’da Terör ve Organize Suçluluk ile İlgili Düzenlemeler”, s. 411.

kişiler ve bu kişilerle ilişkiye geçmek isteyen kişiler hakkında da gizli gözetleme uygulanabilmektedir³³⁴.

AIHM kişilerin özellikle GPS yoluyla gizli gözetlenmesi ve bu yolla kişisel veri işlenmesi hallerini, AIHS m. 8 kapsamında değerlendirmektedir³³⁵. Daha önce değindiğimiz *Uzun v. Almanya* kararına konu olan olayda başvuru, Kuzey Ren-Vestfalya Anayasayı Koruma Departmanı tarafından terör suçlarına katıldığı iddiasıyla video kameralarla izlenmektedir. Ayrıca Federal Ceza Soruşturması Ofisi, başvurucaunun da içinde bulunduđu bir başka kişinin arabasına da bir GPS alıcısı kurmuştur. Böylece başvurucaunun GPS aracılığıyla izlenmesi yoluyla, soruşturma makamları, yaklaşık üç ay boyunca, kişinin kamusal alandaki yerini ve hareketlerini belirleyen verileri sistematik olarak toplamış ve kaydetmiştir.

AIHM, GPS alıcısı ile kişinin izlenmesi ve kişisel verilerinin kaydedilmesinin, söz gelimi telekomünikasyon yoluyla iletişimin denetlenmesinden daha az müdahaleci olduğunu belirtmiştir³³⁶. Bu nedenle GPS ile izlemede kriterler, telekomünikasyon yoluyla iletişimin denetlenmesinde aranan kriterler kadar katı uygulanmayacaktır³³⁷. Ayrıca AIHM kişinin teknik araçlarla gözetlenmesi tedbirinden anlaşıması gerekenin, şüphelinin yerini tespiti elverişli tüm araçlar olduğunu ve GPS yoluyla gözetimin de bu araçlardan olduğunu kabul etmiştir³³⁸. Yani kanunda lafzen açıkça GPS yoluyla izlemenin düzenlenmesi gerekmemektedir. Gözetim belirli bir süre ile sınırlı olmalıdır. Sadece belirli bir ağırlığa sahip suçtan şüphelenilen bir kişiye veya çok sınırlı durumlarda sanıkla temas ettiğinden şüphelenilen üçüncü bir kişiye karşı ve sanığın

³³⁴ Ünver, “Federal Almanya’da Terör ve Organize Suçluluk ile İlgili Düzenlemeler”, s. 410.

³³⁵ ABD’de de durumun dolaylı olarak mahremiyet kapsamında değerlendirildiği söylenebilir. *ABD v. Jones* kararında ABD Yüksek Mahkemesi makul şüpheye dayanan bir arama kararı olmaksızın Bay Jones’un aracına polis tarafından GPS alıcısı yerleştirilmesi ile ABD Anayasası 4. Amendment’ın ihlal edildiği sonucuna varmıştır. Mahkeme, *Katz v. ABD* başvurusunda geliştirdiği iki yönlü bir gizlilik ölçütü olan makul mahremiyet beklentisinden yararlanmıştır. Değerlendirmenin ilk yönü öznel ve bireyin gerçek bir gizlilik beklentisi sergilemesini gerektirir. İkinci yön ise nesneldir ve toplumun gizlilik beklentisini makul olarak tanımasını gerektirir. Bkz. Burch, **a.g.e.**, s. 1715 ve 1722; Esasında 4. Amendment mahremiyet hakkını tanımamaktadır. Ceza soruşturma ve kovuşturmalarda hukuka aykırı aramalara karşı bir koruma sağlamaktadır. Ancak düzenleme geniş yorumlanarak söz gelimi gizli dinlemeler de kapsama alınmaktadır. Bkz. Akyürek, **a.g.e.**, s. 139-140.

³³⁶ *Uzun v. Almanya*, para. 72.

³³⁷ Telekomünikasyon yoluyla iletişime müdahale konusundaki kriterler için bkz. “Telekomünikasyon Yoluyla İletişimin Tespiti” başlıklı bölüm.

³³⁸ *Uzun v. Almanya*, para. 69.

bulunduğu yeri tespit etmenin başka yollarının muhtemel olmaması halinde üçüncü kişinin aracına GPS aracı takılması iç hukukta öngörülmemiştir³³⁹.

Teknik araçla izlemede, kişinin bulunduğu ortamdaki konuşmaları akustik ve optik araçlarla kayda alınmak suretiyle başta kişisel verilerin korunması hakkı olmak üzere haberleşme özgürlüğü ve özel yaşamın gizliliğine müdahale edilmektedir³⁴⁰. Teknik araçla izleme tedbiri ile elde edilen delillerin ceza kovuşturmasında gerekli olmaması halinde derhâl Cumhuriyet savcısının gözetiminde yok edileceği düzenlenmiştir³⁴¹. Ancak düzenleme, CMK m. 135/3 ile kıyaslandığında oldukça belirsiz ve yetersizdir. Zira teknik araçla izleme tedbirinde elde edilen kişisel veriler, kovuşturmaya yer olmadığı kararının verilmesi üzerine yok edilip de bu karara itiraz halinde iddianame düzenlenmişse yok edilen verilerin nasıl kullanılabileceği anlaşılamamaktadır. Yahut verinin ceza kovuşturmasında gerekli olup olmadığına kovuşturmanın en başında, hüküm veya kanun yolunda yani hangi aşamada karar verileceği belirsizdir³⁴².

MOBESE izleme ve kayıtları ceza muhakemesinde de kullanılmaktadır, ancak biz bunun hukuka aykırı olduğunu daha önce ifade etmiştik. Elektronik gözetim ve teknik araçla takibin farklarına kısaca değinmek bu noktada yeterli olacaktır. Teknik araçla takip gizli bir koruma tedbiri olup bu tedbire ancak kanunda belirtilen katalog suçlarda başvurulabilmektedir. Oysa MOBESE kayıtlarının ceza muhakemesinde kullanılacağı suçlar sınırlı sayıda değildir, nitekim bu hususta kanuni düzenleme dahi bulunmamaktadır. Ayrıca teknik araçla takibe belirli bir şüpheli veya sanık hakkında başvurulurken, MOBESE izleme ve kayıtları genel ve tesadüfidir³⁴³.

3. Gizli Soruşturmacı Görevlendirilmesi

³³⁹ *Uzun v. Almanya*, para. 70.

³⁴⁰ Adem Kartal, “Teknik Araçlarla İzleme ve Elde Edilen Delillerin Değerlendirilmesi”, **Terazi Hukuk Dergisi**, c. 9, s. 98, 2014, s. 15.

³⁴¹ CMK m. 140/4.

³⁴² Benzer endişeler için bkz. Kartal, **a.g.e.**, s. 20.

³⁴³ Halid Özkan, **a.g.e.**, s. 71.

Gizli soruşturmacı; muhbir, güvenilir kişi³⁴⁴, ajan provokatör³⁴⁵ gibi kavramlardan farklıdır³⁴⁶. Ayrıca gizli soruşturmacı haricinde de soruşturmaya gizlice katılan birtakım kimselerin yetkileri de diğer mevzuatta düzenlenmektedir. Örneğin Alman hukukunda eyalet polis kanunlarında ve istihbarat hizmetlerine ilişkin kanunlarda düzenlenmeler bulunmaktadır³⁴⁷. Ancak CMK m. 139’da düzenlenen gizli soruşturmacı görevlendirilmesi halinde bu kişinin işlediği kişisel verilerin korunmasına ilişkin açık bir düzenleme bulunmamaktadır. CMK m. 139/6’nın zımni olarak kişisel verileri koruduğu düşünülmelidir. Zira gizli soruşturmacının elde ettiği kişisel veriler ancak görevlendirildiği ceza soruşturması ile ilgili olarak kullanılabilir. Suçla bağlantılı olmayan kişisel veriler ise yok edilecektir. Bu hükme göre; gizli soruşturmacı ancak m. 139/7’de belirtilen suçlarla sınırlı olarak görevlendirilebileceğinden bu katalog haricindeki suçlarla ilgili kişisel veriler işlenmemeli, işlenmişse derhâl yok edilmelidir.

³⁴⁴ Resmi görevi olmayan ve herhangi bir adli kolluk görevlisi olmayan güvenilir kişi (*V-Mann/V-Person/Trusted person*) Alman hukukunda başka insanların bilgisi olmaksızın polisle işbirliği yapan kişidir. Bazı hallerde bu kişiden, Memur Olmayan Kişilerin Resmen Görevlendirme Kanunu’na (Gesetz über die förmliche Verpflichtung nichtbeamteter Personen) göre yükümlülüklerini özenli bir şekilde yerine getireceklerine dair taahhütname alınabilir. StPO bakımından ise güvenilir kişi tanıklara ilişkin düzenlemelere tabidir. Ancak güvenilir kişi ve kişisel veri toplamasına ilişkin eyalet bazlı kanuni düzenlemeler mevcuttur. Örneğin; Aşağı Saksonya Kamu Güvenliği ve Düzeni Hakkında Kanun (Niedersächsisches Gesetz über die öffentliche Sicherheit und Ordnung) § 36’da üçüncü kişilerce bilinmeyen güvenilir kişinin ve kişisel verilerin toplanmasına ilişkin düzenlemeye yer vermiştir. Buna göre güvenilir kişi, polisin kullanması gereken araç ve yöntemleri kullanarak kişisel veri toplayamaz. Güvenilir kişi, özel yaşamın giz alanındaki verilerden haberdar olursa bu veriler kaydedilemez, değiştirilemez veya kullanılamaz. Kaydedilmişse bile ilgili kayıtlar derhâl silinmeli ve silindiği belgelenmelidir. Detaylı bilgi için bkz. Plagemann, **a.g.e.**, s. 164.

³⁴⁵ İngiliz hukukunda ise bu kavramlar arasında dörtlü bir ayrım yapılmaktadır: Yalnız suç işlenmesini gözleyip herhangi bir rolü olmayan casus (*spy*), failin emirlerine uyarak suç işlenmesine iştirak eden işbirlikçi (*collaborator*), faili suç işlemeye teşvik eden teşvikçi (*tempter*) ve aktif çabası ile faili yakalamak için ona suç işleme kararı aldırان ajan provokatör. Bu dört grup da failin yakalaması amacı ile delil toplamaktadır. Bkz. Hakan Hakeri, **Ceza Hukuku Genel Hükümler**, 22. Baskı, Ankara, Adalet Yayınevi, 2019, s. 586; AİHM kararlarında teşvik sonucu işlenen suç sonucunda kişi hakkında verilen mahkûmiyet hükmünün adil yargılanma hakkını ihlal ettiğine dair başvurularda kışkırtan kişi her kararda ajan provokatör terimi ile ifade edilmemektedir. Bazı kararlarda ajan provokatör, bazılarında tuzak, çoğu zaman da *incitement* (kışkırtma/ tahrik) biçiminde ifade tercih edilmektedir. Detaylı bilgi için bkz. Aslan, **a.g.e.**, s. 29.

³⁴⁶ Ünver, “Federal Almanya’da Terör ve Organize Suçluluk ile İlgili Düzenlemeler”, s. 412; AİHM uygulamasında da faaliyet olarak bir ayrıma gidilerek ajan provokatörler, gizli soruşturmacıdan (*undercover agent*) ayrılmaktadır. Zira gizli soruşturmacı, kimliğini gizleyerek suça katılırken suç işlenmesini teşvik etmemektedir. Oysa ajan provokatör, başka türlü suç işlemeyecek kişiyi suç işlemeye teşvik etmektedir. Bkz. Aslan, **a.g.e.**, s. 28.

³⁴⁷ Plagemann, **a.g.e.**, s. 163.

Gizli soruşturmacının görevlendirildiği suçlarla ilgili soruşturmada elde edilen kişisel veri, soruşturma ya da kovuşturmada kullanılmayacak bir veri ise, söz gelimi silahlı örgüt üyelerinin sağlık verileri ya da cinsel yaşamlarına dair verileri muhakeme konusu suçla bağlantılı değilse yok edilmelidir. Gizli soruşturmacının elde ettiği kişisel veriler, soruşturmacının görevlendirildiği suç haricinde başka bir suçun işlendiğine dair delil niteliğindeyse de bu suçlarla ilgili kullanılamayacaktır. Zira CMK m. 139'da, m. 138 minvalinde bir tesadüfi delil düzenlemesine yer verilmemiştir³⁴⁸. Ancak bu halde şöyle bir tartışma yürütülebilir: Silahlı örgüt üyesi olan kişilerden birinin AIDS olduğu bilgisi bir sağlık verisidir ve yürütülmekte olan silahlı örgüt soruşturması ile bir bağlantısı bulunmamaktadır, dolayısıyla yok edilmesi gerekmektedir. Ancak AIDS olan silahlı örgüt üyesinin, işlediği bir cinsel saldırı suçu sonucu bu hastalığı kaptığı bilgisi de yürütülmekte olan soruşturma harici bir başka suçun işlendiğine işarettir. Bu halde kamu görevlisi olan gizli soruşturmacının, TCK m. 279 uyarınca suçu bildirme yükümlülüğü bulunmaktadır ve yetkili makamlarla bu kişisel veriyi paylaşmalıdır.

Madde, kişisel verinin suçla bağlantılı olup olmadığına kimin karar vereceğine dair bir düzenleme yapmamış, yani bu türden kişisel verilerin yok edilme safhasını belirtmemiştir. Kanaatimizce gizli soruşturmacı, soruşturma evresinde başvurulabilecek bir tedbir olduğundan bu evrenin amiri olan savcı, verinin suçla bağlantılı olmadığı tespitini yaptıktan sonra veriyi yok etmelidir. Zira suçla bağlantılı olmayan verilerin, kovuşturma dosyasına girmesi halinde gizlilik ilkesi sona ereceğinden suçla bağlantılı olmayan bu veri sahibinin, kişisel verilerinin korunması hakkı ciddi şekilde zedelenecektir.

Son olarak gizli soruşturmacının delil toplayabileceği süre ve dolayısıyla veri işleyebileceği süre kanunda belirtilmemiştir. Bazı yazarlar gizli soruşturmacı soruşturmada görevlendirilse de kovuşturmada da görevinin devam edebileceğini savunsa da³⁴⁹ kanunilik ilkesinden hareketle biz bu görüşe iştirak etmiyoruz. Gizli

³⁴⁸ Gizli soruşturmacının elde ettiği, yürütülen soruşturma haricindeki kişisel verilerin tesadüfi delil olarak kullanılmasına ilişkin maddede bir düzenleme yapılması gerektiğine dair bkz. Yener Ünver, "Kişisel Verilerin Korunması", **GSÜHFD**, c. 7, s. 1, İstanbul, 2008, s. 192.

³⁴⁹ Öztürk, Eker Kazancı, Soyer Güleç, **a.g.e.**, s. 313.

soruşturmacı yalnız soruşturma aşamasında görevli olabilir ve dolayısıyla veri işleyebilir. Veri işlemede sürelilik ilkesi de ancak bu yorumla sağlanabilecektir.

G. Mahkeme Tutanakları ve Kararları

Kolluk ve Ceza Adaleti Direktifi m. 18 kişisel verilerin bir mahkeme kararında veya cezai soruşturma ve kovuşturma sırasında tutulan bir kayıt veya dosyada yer alması durumunda; veri sahibinin bilgilendirilme, erişim, düzeltme veya silinmeyi talep hakkının üye devletlerin iç hukuklarına göre sağlanacağını düzenlemiştir. Dolayısıyla bu durum, AB hukukunun değil, iç hukukun uygulama alanındadır.

Mahkeme tutanaklarında yargılama süreçlerinin kişisel verilerinin yer alması yargılamanın doğasının bir gereğidir. Örneğin CMK m. 209'a göre delil olarak kullanılacak belge ve yazılar haricinde sanığın kişisel ve ekonomik duruma ilişkin bilgi ve belgeler de duruşmada anlatılacak yani kişisel veriler yargılamanın gereği olarak ifşa edilecektir. Ancak bu halde yalnız yargılama ile ilgili kişisel veriler işlenmelidir. Örneğin CMUK'ta tanığa sorulacak sorular arasında dininin de yer alması³⁵⁰ ve bunun kayıtlara geçmesi yargılamanın bir gereği değildir. Bu hüküm Anayasa'ya aykırılık iddiasıyla AYM'nin önüne gelmiştir. Tanık kendisine sorulan sorulara cevap vermekle yükümlü olup dininin sorulması halinde buna da cevap vermeye zorlanmaktadır, bu ise din ve vicdan özgürlüğü ile bağdaşmamaktadır ve AYM bu hükmü iptal etmiştir³⁵¹. AYM'nin bu değerlendirmeyi yaptığı dönemde kişisel verilerin korunması hakkı, Anayasal düzeyde bir hak olmadığından bu çerçevede bir değerlendirme yapılmamıştır. Ancak özel nitelikli veri kategorisinde yer alan kişinin mensup olduğu dine ilişkin bilginin mahkeme tutanağı ile işlenmesi şüphesiz kişisel verilerin korunması hakkına da müdahaledir³⁵². AYM kararına konu bir diğer olayda da örgütlü suçluluk faaliyetleri nedeniyle yürütülen bir ceza kovuşturmasında, dosyaya MİT'in bir istihbarat raporu da konulmuştur. Raporda, yürütülen yargılama ile bir ilgisi bulunmayan avukat olan başvurucunun kişisel

³⁵⁰ Bkz. m. 61 “Şahide şahadetinden evvel adı, sanı, yaşı, işi, dini ve ikametgâhı sorulur. İktiza ederse şahadetine ne dereceye kadar itimat edilebileceği hakkında hakimi tenvir edecek hallere mütaallik ve hele maznun veya mağdur ile münasebetlerine dair sualler sorulur.”

³⁵¹ AYM, E. 1995/25, K. 1996/5, 02.02.1996 Çevrimiçi <https://www.anayasa.gov.tr/tr/kararlar-bilgi-bankasi/> 29.03.2020.

³⁵² Dağ, a.g.e., s. 90.

bilgilerine ve örgüt üst yönetimi ve cezaevinde bulunan üyeleri arasında kuryelik yapabileceğine dair hakkında birtakım değerlendirmelere yer verilmiştir³⁵³. AYM, hakkında bir suç isnadı bulunmamasına rağmen başvurusunun mesleki yaşamını etkileyebilecek bu değerlendirmelerin dava dosyasına konulmak suretiyle alenileştirilmesini ihlal mahiyetinde bulmuştur³⁵⁴.

AIHM kararına konu olan *Panteleyenکو v. Ukrayna* başvurusunda ise yerel mahkeme, başvurusunun ruh haleti ve tedavisine ilişkin psikiyatri hastanesinden bilgi talep etmiş ve gelen gizli bilgiyi tarafların ve diğer kişilerin bulunduğu duruşma sırasında paylaşmıştır³⁵⁵. AIHM, paylaşılan bu sağlık verisinin yargılama için gereksiz olduğundan bahisle ifşasını m. 8'in ihlali mahiyetinde bulmuştur³⁵⁶.

III. CEZALARIN İNFAZI

A. Adli Sicil Kaydının Tutulması

1. Türk Hukukunda Durum

Adli sicil kayıtları, Adli Sicil ve İstatistik Genel Müdürlüğünce merkezi adli sicilde tutulmaktadır. Adli Sicil Kanunu m. 9'a göre adli sicil kayıtları silindiğinde bu husus arşiv kaydına alınmaktadır. Kişinin ölümü halinde ise adli sicil bilgileri tamamen silinmektedir. Adli sicil ve arşiv bilgilerinin silinmesi³⁵⁷, bu kayıtlarda

³⁵³ *Ercan Kanar* Başvurusu, B. No: 2013/533, 09.01.2014, para. 59 Çevrimiçi <https://www.anayasa.gov.tr/tr/kararlar-bilgi-bankasi/> 29.03.2020.

³⁵⁴ *Ercan Kanar*, para. 60-61.

³⁵⁵ *Panteleyenکو v. Ukrayna*, B. No: 11901/02, 12.02.2001, para. 57 Çevrimiçi <https://hudoc.echr.coe.int/> 29.03.2020; Meme küçültme operasyonu geçiren başvurusunun hatalı tıbbi uygulama iddiasıyla açtığı tazminat davasında da benzer yönde bir iddia yer almaktadır. Başvurusunun üst bedeninde bulunan deformasyonlara ilişkin fotoğraflar dava dosyasında sunulmuş ve gizlilik talep edilmiştir. Ancak gerekçesiz biçimde gizlilik talebi reddedilmiştir (para. 68). Üstelik dava yedi yıldır derdesttir, AYM gerekçesiz bir biçimde başvurusunun mahremiyetinin ihlal edilerek aleni yargılama yapılmasında özel hayatın gizliliğinin ihlal edildiğine karar vermiştir (para. 69). Bkz. *B.K. Başvurusu*, B. No: 2014/14189, 25.10.2017 Çevrimiçi <https://www.anayasa.gov.tr/tr/kararlar-bilgi-bankasi/> 29.03.2020. Söz konusu kararda, *Panteleyenکو* kararının aksine, başvurusunun fotoğraflarının yargılama ile ilgisi bulunmaktadır, ancak çıplak beden bölgesinin aleni yargılamada ifşa edilmesi, üstelik davanın yedi yıl boyunca sürmesi şüphesiz özel hayatın gizliliği ve kişisel verilerin korunması hakkı ile bağdaşmamaktadır.

³⁵⁶ *Panteleyenکو v. Ukrayna*, para. 61.

³⁵⁷ Bkz. 5352 sayılı Kanun m. 12.

sorgulama yapabilecek kişilerin³⁵⁸ kanunla belirlenmesi, adli sicil ve arşiv kayıtları özel nitelikli kişisel veri³⁵⁹ olduğundan isabetlidir.

Adli sicil kayıtlarının belirli bir süre sonra silinmesini talep hakkı ve unutulma hakkı, failin resosyalizasyonu ve ıslahına olanak sağlamaktadır. Adli sicil kaydı ve mahkeme kararlarının bilinmesinde kamunun yararı bulunmaktadır ve veri sahibi söz gelimi unutulma hakkını kullanarak bu resmi kayıtlara erişimin kaldırılmasını talep ettiğinde devletin negatif yükümlülüğü gereği erişimi kaldırması gerekecektir. Ancak kamu yararı öncelenecekse de verinin gizliliğine ilişkin uygun önlemler alınmalıdır³⁶⁰. GDPR m. 17/3-b'ye göre AB üyesi devletlerin ulusal hukuklarınca veya AB hukukuna göre kişisel verilerin işlenmesine dair kanuni bir yükümlülük mevcutsa bu durumda adli sicil kaydının silinme ya da unutulmaya konu olmaması hukuka uygundur³⁶¹.

AYM ceza mahkûmiyetine ilişkin arşiv kaydının, kişinin ölümü ve herhalde kaydın girildiği tarihten itibaren seksen yıl sonra silinebileceğine ilişkin Adli Sicil Kanunu m. 12/1'i iptal etmiştir. Zira suç ve cezaların nitelikleri veya ağırlıkları dikkate alınmadan tüm suçlara ilişkin arşiv kayıtlarının aynı ve bu denli uzun süre tutulması bu sürenin arşiv kaydına alınmayı gerekli kılan amaçla orantılı ve makul değildir³⁶². İptal kararında unutulma hakkına yer verilmemiş, kişinin maddi ve manevi varlığını geliştirme ve hükümlülerin ıslahı gerekçesine dayanılmıştır. İptal kararı üzerine 6290 sayılı Kanun ile Adli Sicil Kanunu'nda değişiklik yapılmış ve arşiv kaydının silinmesinde AY m. 76/2'deki yüz kısaltıcı suçlar ile TCK dışındaki hak yoksunluğuna neden olan suçlar kategorisi oluşturularak süreler belirlenmiş ve kişisel verilerin işlenmesinde sürelilik ilkesine uygun düzenleme yapılmıştır.

Adli sicil kaydı ve arşiv kayıtları gizlidir. Adli Sicil Kanunu m. 7'ye göre adli sicil kayıtlarının kullanım amacı belirtilerek kimlere verilebileceği sayılmıştır. M. 9'da da hangi hallerde kayıtların silineceği ve arşive kaldırılacağı düzenlenmiştir. Arşiv

³⁵⁸ Bkz. 5352 sayılı Kanun m. 13.

³⁵⁹ Nitekim AİHM de *M.M. v. Birleşik Krallık* başvurusunda kişinin ceza mahkûmiyeti ve adli sicil kayıtlarının bu mahiyette olduğuna karar vermiştir. Bkz. *M.M. v. Birleşik Krallık*, B. No: 24029/07, 13.11.2012, para. 200 Çevrimiçi <https://hudoc.echr.coe.int/> 29.03.2020.

³⁶⁰ Eren Sözüer, **a.g.e.**, s. 76.

³⁶¹ Soysal, **a.g.e.**, s. 403.

³⁶² AYM, E. 2008/44, K. 2011/21, 20.01.2011 Çevrimiçi <https://www.anayasa.gov.tr/tr/kararlar-bilgi-bankasi/> 29.03.2020.

kaydı ve sicil kayıtlarının gizliliği kişilerin lekelenmeme hakkı ve cezanın ıslah amacının gerçekleşmesi için de gereklidir. Adli Sicil Kanunu’nda on sekiz yaşını tamamlamamış çocukların adli sicil kayıtlarının sınırlı sayıda kimse ile paylaşılmasına dair hüküm bulunması³⁶³, kanun koyucunun unutulma hakkı bakımından pozitif yükümlülüğünü yerine getirdiğini göstermektedir. Zira özellikle çocuklar başta olmak üzere bireylerin geçmişlerinin etkisinden kurtulması için resmi mahiyetteki kayıtlar buna uygun olarak silinmeli ya da erişimi sınırlandırılabilirdir³⁶⁴. *Aycaguer v. Fransa*³⁶⁵ başvurusunda AİHM, özel nitelikli veri olan mahkûmiyete ilişkin verilerinin, mahkûmların işledikleri suçun niteliğine göre bir ayırım olmaksızın aynı saklama süresine tabi tutulmasını ve adli sicil kaydının silinmesini sağlamak için hukuki bir yolun bulunmamasını m. 8’in ihlali olarak nitelemiştir³⁶⁶.

CMK’de maslahata uygunluk ilkesi gereği savcı kamu davası açmada takdir yetkisini kullanmakta yahut bazı durumlarda açık hükmün varlığı sebebiyle kamu davasının açılmasının ertelenmesi gündeme gelmektedir. Ayrıca onarıcı adalet gereği hükmün açıklanmasının geri bırakılması kararı verilebilmektedir. Bu iki halde de kanun koyucu bu kararların bunlara mahsus bir sisteme kaydını öngörmüş ve bu kayıtların ancak belirli amaçlar dâhilinde kullanılabileceğini düzenlemiştir³⁶⁷. Maddelerde sınırlı sayıda kimse olarak mahkeme, hakim ve Cumhuriyet savcısının soruşturma ve kovuşturma dâhilinde kayıtlara ulaşmasına olanak tanınmıştır.

Son olarak kişisel verilerin hukuka aykırı olarak kaydedilmesi suçunun daha fazla cezayı gerektiren nitelikli hali olarak düzenlenen TCK m. 135/2’de kişinin ceza mahkûmiyeti ve güvenlik tedbirlerine yer verilmemesi eleştirilmelidir. Zira KVKK m. 6’ya göre kişinin ceza mahkûmiyeti ve güvenlik tedbirlerine ilişkin verileri, GDPR’da da olduğu gibi özel nitelikli kişisel verilerdir. Dolayısıyla bu veriler daha nitelikli bir

³⁶³ M. 10/3 “On sekiz yaşından küçüklerle ilgili adli sicil ve arşiv kayıtları; ancak soruşturma ve kovuşturma kapsamında değerlendirilmek üzere Cumhuriyet başsavcılıkları, hâkim veya mahkemelerce istenebilir.”

³⁶⁴ Eren Sözüer, **a.g.e.**, s. 24; Alman Federal Anayasa Mahkemesi *Lebach* kararında suçu infaz edilmiş ya da infazı tamamlanmak üzere olan bireyin menfaatinin, kamunun bilgilendirilmesi menfaati ile yarıştığını ve bu suç hakkında tekrar yayın yapılmasının onun resosyalizasyonuna engel olduğu kanısındadır. Bkz. Eren Sözüer, **a.g.e.**, s. 26.

³⁶⁵ *Aycaguer v. Fransa*, B. No: 8806/12, 22.06.2017, Çevrimiçi <https://hudoc.echr.coe.int/> 29.03.2020.

³⁶⁶ Arslan Öncü, **Anayasa Mahkemesine Bireysel Başvuru El Kitapları Serisi-8**, s. 85.

³⁶⁷ Bkz. CMK m. 231/13; CMK m. 171/5.

korumayı hak etmektedir ve ceza siyaseti bakımından da caydırıcılığın sağlanması için bu verilerin kaydedilmesi daha fazla cezayı gerektirmektedir.

2. Sicil Bilgilerinin Kamuya Açıklanması

ABD’de bazı eyaletlerde cinsel suçlardan mahkûm olan kişilerin adresleri ve bilgileri sicile kaydedilmekte ve kamuya açıklanmaktadır. Bunda amaç, mağdurların kendileri ve çocuklarını cinsel suçlardan hüküm giymiş kimselerden korumalarını sağlamaktır. Örneğin New Jersey’de 1994 tarihli Sicile Kayıt ve Toplumun Bilgilendirilmesi Kanunu uyarınca cinsel suç failleri bir sicile kaydedilmekte ve suçluların tekrar suç işlemeleri riski üzerine toplum bilgilendirilmektedir. Kişinin itiyadi suçlu olup olmadığına göre yapılan değerlendirmede bazen mağdur ile ailesi ve kolluk güçleri bazen de okullar, dini organizasyon ve gençlik organizasyonları dahi bilgilendirilmektedir³⁶⁸. Federal Megan Kanunu uyarınca sicile kaydedilen kişilerin bilgileri ve parmak izleri FBI’ya dahi gönderilmektedir. Sicile kayıt kural olarak on yıl ile sınırlıyken kişinin cinsel şiddet içeren bir suçtan bir veya birkaç kez veya bunun ağırlaşmış halinden mahkûm olması ya da cinsel şiddet saldırganı olarak saptanmış olması halinde, kişi süresiz olarak sicile kayıtlı olacaktır³⁶⁹. Kanun’a göre eyalet kanunlarının izin verdiği bir amaçla bu bilgiler kamuya açıklanabilecektir³⁷⁰.

Kanaatimizce cinsel suç faillerinin damgalanmasına yol açan ve ıslah edilmesine kesinlikle hizmet etmeyen bu düzenleme, kişisel verilerin korunması hakkı ve daha özel olarak unutulma hakkı ile bağdaşmamaktadır. Örneğin herhangi bir isim ya da posta kodu yazarak ABD Adalet Bakanlığının *Dru Sjodin National Sex Offender Public Website* isimli internet sitesinden³⁷¹ cinsel suçlardan hüküm giymiş kişilerin

³⁶⁸ Selman Dursun, “Megan Kanunu (ABD’de Cinsel Suç Faillerinin Sicile Kaydı ve Sicil Bilgilerinin Kamuya Açıklanması)”, **AÜEHFD**, c. 8, s. 1-2, 2004, s. 238 vd.

³⁶⁹ Dursun, “Megan Kanunu (ABD’de Cinsel Suç Faillerinin Sicile Kaydı ve Sicil Bilgilerinin Kamuya Açıklanması)”, s. 243-244.

³⁷⁰ Dursun, “Megan Kanunu (ABD’de Cinsel Suç Faillerinin Sicile Kaydı ve Sicil Bilgilerinin Kamuya Açıklanması)”, s. 245.

³⁷¹ Çevrimiçi <https://www.nsopw.gov/en/Search/Results> 23.03.2020; Bu internet sitesi, 2003 yılında Dju Sjodin isimli bir üniversite öğrencisinin cinsel saldırıya uğrayıp öldürülmesi üzerine 2005 yılında Adalet Bakanlığı tarafından kurulmuştur. 2005 yılında ise Adam Walsh Çocuk Koruma ve Güvenliği Kanunu çıkarılarak sicile kayıt konusunda eyaletin takdir yetkisine bırakılan hususlar, bildirim zorunlu hale getirilerek genişletilmiştir. Bkz. Selman Dursun, “Özellikle Mağduru Çocuk Olan Mükerrir Cinsel Suç Faillerine Karşı Toplumun Korunması Bağlamında Megan Kanunu Hakkında Soru ve Cevaplar”, **CHKD**, c. 2, s. 1-2, 2014, s. 236-237.

adı, diğer adı, soyadı, fotoğrafı, yaşı, mesleği, iş adresi ve ikamet adresine dünyanın her yerinden ulaşmak olanaklıdır.

Bu uygulama kişinin cezası infaz edildikten sonra kendisine yeni bir yaşam kurmasına da imkân vermemekte ve kişinin maddi ve manevi olarak kendini geliştirme hakkına ket vurmaktadır. Üstelik bu durum, internet sitesinden alınan adres bilgisi ile hükümlüye zarar verilmesine yani yaşam hakkının ihlaline dahi yol açabilecektir. Böylesi bir düzenlemenin Türkiye’de olmaması isabetlidir.

Fransa’da da 2004 yılından beri cinsel istismardan mahkûm olan kimseler, Fransa Adalet Bakanlığı bünyesinde tutulan cinsel suçlar veri tabanına kaydedilmektedir. Veri tabanına kaydetme ile hedeflenen cinsel suçların tekerrürünün önlenmesidir³⁷². Kaydedilen kimseler adres değişikliklerini on beş gün içinde bildirmekle yükümlü olup kayıtlar işlenen suçun cezasının on yıl veya daha kısa bir hapis cezası olması halinde yirmi yıl, on yıldan daha uzun olması halinde ise otuz yıl boyunca tutulmaktadır³⁷³. ABD’deki münferit eyaletlerdekinin aksine bu sicil kamuya açık değildir. Bu uygulamanın AİHS m. 8’e uygunluğu AİHM tarafından değerlendirilmiştir. AİHM, sicilin herkese açık olmaması, kanunda belirtilen ve sır saklama yükümlülüğü bulunan yetkililerin ancak sicil bilgilerine erişebilmesi, verilerin yirmi-otuz yıllık sürelerle tabi olarak tutulması ve savcı, özgürlükler hakimi ve soruşturma bölümü başkanına başvuru ile bilgilerin silinmesinin mümkün olması gerçeği karşısında; Fransa Ceza Kanunu ile düzenlenen sicile kaydın, m. 8 ile uyumlu güvencelere sahip olduğunu belirtmiştir³⁷⁴. Kanaatimizce de bu karar isabetlidir, zira ABD’nin aksine Fransa’daki düzenlemede cinsel suçlara ilişkin tutulan bu sicil kamuya açık değildir ve suçun tekerrürü halinde daha evvel adres bildiriminde bulunmakla yükümlü olan failin daha kolay ele geçirilmesine imkân sağlamaktadır. Ayrıca devletin cinsel suçlarla mücadele yöntemi takdir marjı kapsamında olup,

³⁷² Terry Thomas, **The Registration and Monitoring of Sex Offenders: A Comparative Study**, London, Routledge, 2011, s. 83.

³⁷³ FIJAIS (Fichier Des Auteurs D’infractions Sexuelles ou Violentes) isimli bu veri tabanına kaydetme uygulaması 2004-2204 sayılı Kanun ile Fransa Ceza Kanunu m. 706 ve devamında düzenlenmiştir. Detaylı bilgi için bkz. Thomas, **a.g.e.**, s. 83-84.

³⁷⁴ *Gardel v. Fransa*, B. No: 16428/05, 17.03.2010, para. 54 Çevrimiçi <https://hudoc.echr.coe.int/> 29.03.2020.

hükümlünün kişisel verilerin korunması hakkına müdahalesi hukuka uygun ve süreli veri tutulması söz konusu olduğu için de ölçülüdür.

B. Parmak İzi Alınması

Ceza infaz kurumlarında fiziksel erişimleri denetlemek için biyometrik cihazlar vasıtasıyla infaz kurumu çalışanları, tutuklu ve hükümlüler ve kuruma gelen ziyaretçilerin biyometrik verileri işlenmektedir³⁷⁵. Kuruma gelen hükümlülerin tanısı için ilk etapta alınan parmak izleri, CGİK m. 21/3 uyarınca AFIS'ye kaydedilir. Kanun parmak izi alınmasının tanıya yönelik olduğunu belirtse de burada amaç hükümlünün kişisel verilerinin depolanmasıdır³⁷⁶. Zira yalnız parmak izi hükümlünün tanısına yetebilecek iken Kanun hükümlünün fotoğraflarının da çekilmesini dahası kan grubunun, ölçülerinin ve vücudunun dış özelliklerinin de belirlenmesini öngörmüştür. Sağlık verisi olan kan grubunun hükümlünün tanınmasına nasıl hizmet ettiği ise anlaşılmamaktadır.

Kanun, bu kayıtların Kanun'da yer alan zorunlu haller dışında kimse ile paylaşılamayacağını belirtmiştir ki bu da CGİK'nin biyometrik veriler için öngördüğü tek korumadır. AFIS'de gönüllü, gözaltına alınan, emniyet mensubu gibi kişilerin de kaydı bulunmaktadır ve CGİK'nin öngördüğü haller dışında paylaşılamayacak hükümlünün parmak izinin AFIS'de ayrı bir bölümde mi saklanacağı, bu amaca bağlı kullanımın nasıl sağlanacağı düzenlenmemiştir. Ayrıca kişinin infaz kurumundan ayrılması halinde verinin silinip silinmeyeceği ya da ne süre ile sınırlı tutulacağı düzenlenmemiştir.

C. Elektronik İzleme

1. Tanım

³⁷⁵ Er, **a.g.e.**, s. 32.

³⁷⁶ Veli Özer Özbek, **İnfaz Hukuku**, Geliştirilmiş ve Güncellenmiş 11. Baskı, Ankara, Seçkin Yayıncılık, 2019, s. 128.

Elektronik izleme³⁷⁷, şüpheli, sanık veya hükümlünün belirli bir yerde bulunma zorunluluğunun bulunduğu hallerde, bu zorunluluğun gereklerine uyulup uyulmadığının takibine hizmet eden bir yöntemdir. Elektronik izleme, özellikle hükümlülerin toplumla bağlarının kopmaması ve cezaların ıslah amacına hizmet eden hükümlünün koşullu salıverilmesinde, bazı seçenek yaptırımların infazında, cinsel suçlardan mahkûm olanların mağdurdan ve çocuklardan uzak durması gibi müesseselerin takibinde oldukça işlevseldir³⁷⁸.

Elektronik izlemeye ilişkin 2014/4 sayılı Avrupa Konseyi Bakanlar Komitesinin Üye Devletlere Elektronik İzleme Konusunda Tavsiye Kararı'nda³⁷⁹ elektronik izlemeye başvurulabilecek haller³⁸⁰ ve kişisel verilerin korunmasına ilişkin hükümler yer almaktadır. Zira elektronik olarak izlenen kişinin konum bilgisi de onun kişisel verisi olup korunmaya muhtaçtır. Tavsiye Karar uyarınca üye devletler;

29. *Elektronik izleme kullanımı sırasında toplanan veriler, verilerin depolanması, kullanılması ve paylaşılması ile ilgili uluslararası standartlara dayanan özel düzenlemelere tabi olacaktır.*

30. *Bu tür verilerin cezai soruşturmalar ve kovuşturmalar çerçevesinde kullanılmasına ve paylaşılmasına kesin olarak dikkat edilmelidir.*

³⁷⁷ Terimsel olarak "Alman hukukunda elektronik izleme 'elektronische überwachung', elektronik kelepçe 'elektronische fußfessel' olarak; Avusturya Ceza İnfaz Kanunu'nda elektronik izleme 'elektronischen Aufsicht', Anglosakson hukukunda ise 'Tackling the rag' olarak kullanılmaktadır." Soner Hamza Çetin, **Türk Ceza Hukuku'nda Elektronik İzleme**, Ankara, Adalet Yayınevi, 2020, s. 34.

³⁷⁸ Çetin, **a.g.e.**, s.23; Göksu Işık, "Elektronik İzleme", **Terazi Hukuk Dergisi**, c. 13, s. 142, 2018, s. 33; Nilay Pekel Uludağlı, "Hükümlülerin Denetiminde ve Topluma Kazandırılmasında Yeni Bir Yöntem Olarak Elektronik İzleme", **AÜHFD**, c. 61, s. 4, Ankara, 2012, s. 1340.

³⁷⁹ "Recommendation CM/Rec(2014)4 of the Committee of Ministers to Member States on Electronic Monitoring". Tavsiye kararın tam metni için bkz. Çevrimiçi <https://pjp.eu.int/documents/41781569/42171329/CMRec+%282014%29+4+on+electronic+monitoring.pdf/c9756d5b-be0e-4c72-b085-745c9199bef4> (06.02.2020).

³⁸⁰ Bu hallere "II. Tanımlar" başlığı altında yer verilmiştir:

"- yargılama öncesi ceza yargılama aşamasında;
- hapis cezasını erteleme veya infaz etme koşulu olarak;
- toplum içinde cezai yaptırım veya tedbirin uygulanmasını denetlemenin bağımsız bir yolu olarak;
- diğer denetimli serbestlik müdahaleleri ile birlikte;
- cezaevinde olanlar için tahliye öncesi tedbir olarak;
- cezaevinden koşullu salıverilme çerçevesinde;
- cezaevinden serbest bırakıldıktan sonra belirli suçlu türleri için yoğun bir rehberlik ve denetim tedbiri olarak;
- cezaevindeki ve / veya açık cezaevindeki suçluların iç hareketlerini izlemenin bir yolu olarak;
- belirli suç mağdurlarını bireysel şüphelilerden veya suçlulardan korumak için bir araç olarak"

elektronik izlemeye başvurulabilir.

31. *Bu tür verilerin dikkatsiz veya kasıtlı olarak kötüye kullanılması veya kullanılması durumunda etkili bir yaptırım sistemi uygulanacaktır.*
32. *Elektronik izleme ekipmanı sağlayan veya elektronik izleme kapsamındaki kişileri denetlemekten sorumlu özel kuruluşlar, ellerindeki verilerin işlenmesine ilişkin aynı kural ve düzenlemelere tabidir.*

Elektronik izlemede en çok kullanılan yöntemler, radyo frekansı (RF) yöntemi ve GPS yöntemidir³⁸¹. İlk nesil yöntem olan RF yöntemi, söz gelimi evinde izlenen kişinin evinden ayrılması halinde radyo frekansı kesildiği için bulunduğu yeri tespit edememekte, yalnız bulunması gereken yerden ayrıldığına ilişkin tespit yapabilmektedir. GPS yöntemi ise kişinin bulunması gereken yerden ayrılması halinde de takibi olanaklı kılıp ayrıca tam olarak kişinin bulunduğu yeri tespit etmektedir³⁸². İlk nesil sistem yöntemin kişisel verilerin korunması noktasında daha az müdahaleci olduğu anlaşılmaktadır. Bu yöntemler haricinde, elektronik izlenenin kimlik doğrulaması için özellikle biyometrik yöntemlerle yüz tanıma sistemlerinden de yararlanılmaktadır³⁸³. Bir diğer yöntemde ise kişi, önceden belirlenen zamanda telefonla aranır ve sorulan sorulara cevap vermesi ile ses doğrulaması yapılır³⁸⁴.

2. Türk Hukukunda Elektronik İzleme

Türkiye’de elektronik izlemeye ilk kez 2012 yılında bir Avrupa Birliği Projesi’nin³⁸⁵ AB tarafından uygun bulunması ile başvurulmuştur. 5402 sayılı Denetimli Serbestlik Hizmetleri Kanunu m. 15/A’ya göre “*Şüpheli, sanık ve hükümlülerin toplum içinde izlenmesi, gözetimi ve denetimi elektronik cihazların kullanılması suretiyle de yerine getirilebilir*” denilmek suretiyle ihtiyari olarak Türk

³⁸¹ Çetin, **a.g.e.**, s. 27; Pekel Uludağlı, **a.g.e.**, s. 1342; Bir diğer ayrım ise teknik açıdan aktif ve pasif sistem ayrımıdır. Aktif sistemde kişinin el veya ayak bileklerine alet yerleştirilerek kişinin konutundan sinyal alınmaktayken pasif sistemde ise iki yöntem bulunmaktadır. Bunlardan ilkinde kişinin el veya ayak bileklerine yerleştirilen elektronik kelepçe belirli numaralar göndermekte ve ilgili, bu numaraları merkezi bilgisayara iletmektedir. Diğer yöntem ise ses doğrulama esasına dayanmakta ve ilgilinin sesi kaydedilmekte ve bilgisayar kişinin aranması sırasındaki ses ve kayıtlı sesi karşılaştırarak elektronik izleme yapmaktadır. Ayrımın detayları için bkz. Işık, **a.g.e.**, s. 37; Ziya Koç, “Elektronik İzleme ile Hapis Cezasının Konutta Çektirilmesi”, **Ankara Barosu Dergisi**, s. 2, Ankara, 2013, s. 184.

³⁸² Çetin, **a.g.e.**, s. 98-99.

³⁸³ Çetin, **a.g.e.**, s. 102.

³⁸⁴ Çetin, **a.g.e.**, s. 114.

³⁸⁵ “Elektronik İzleme Sistemine Geçişte Denetimli Serbestlik Hizmetlerinin Kurumsal Kapasitesinin Güçlendirilmesi Avrupa Birliği Eşleştirme Projesi”.

hukukunda elektronik izlemeye başvurulabileceği düzenlenmiştir. Maddenin devamında izlemede elektronik cihazların kullanılması, şüpheli, sanık ve hükümlünün rızasına bağlanmıştır³⁸⁶. İzleme, gözetim ve denetime ilişkin esas ve usuller de Denetimli Serbestlik Hizmetleri Yönetmeliği'nde³⁸⁷ düzenlenmiştir.

Yönetmelik'e göre elektronik izlemenin hukuki mahiyeti, ceza muhakemesinde kararların infazında kullanılan bir yöntem olmasıdır³⁸⁸. Bu yöntemden; *belirli yerlere gitmekten yasaklanma* gibi güvenlik tedbirlerinde, *konutunu terk etmemek* gibi adli kontrol kararlarında, hükmün açıklanmasının geri bırakılması kararında yer alan belirli yükümlülüklerin takibinde, bazı suç faillerine verilen *mağdurun oturduğu ve çalıştığı yerleşim bölgesinde ikamet etmekten yasaklanma* gibi özel infaz rejimi ve denetimli serbestlik tedbirinde ve 6284 sayılı Ailenin Korunması ve Kadına Karşı Şiddetin Önlenmesine Dair Kanun uyarınca verilen tedbir kararının uygulanmasında yararlanılabilir³⁸⁹.

Belirtilmelidir ki elektronik izlemeye yalnız 5402 sayılı Kanun ve 6284 sayılı Kanun'da yer verildiğinden ancak bu sınırlar dâhilinde başvurulabilir. Söz gelimi kamu güvenliği, suçun önlenmesi gibi bir amaçla elektronik izlemeye başvurulamaz³⁹⁰. Ayrıca kanunun öngördüğü bağlam ile sınırlı olarak bu kişiler izlenebilecektir. 2014/4 sayılı Tavsiye Karar uyarınca hükümlü ve tutukluların infaz kurumu içinde izlenmesi olanaklıysa da Türk hukukunda buna dair bir kanun hükmü olmadığından bu alanlarda izleme yapılamayacak³⁹¹ ve kişisel veriler işlenemeyecektir.

6284 sayılı Kanun gereği uygulanacak tedbirde elektronik izlemeye başvurulduğunda kişisel verilerin korunması anlamında sakınca bulunmamaktadır.

³⁸⁶ Belirtelim ki yetkili makamın kararı haricinde elektronik cihazla takip edilecek kişinin rızasına sonuç bağlanması veri işleme bakımından Kolluk ve Ceza Adaleti Direktifi m. 1/3 uyarınca devletin daha yüksek bir koruma sağladığını göstermektedir.

³⁸⁷ R.G. Sayısı: 28578, R.G. Tarihi: 05.03.2013.

³⁸⁸ Bkz. Denetimli Serbestlik Hizmetleri Yönetmeliği m. 101/1 "*Elektronik izleme; şüpheli, sanık veya hükümlülerin elektronik yöntem ve araçlar ile toplum içinde izlenmesini, gözetim ve denetim altında tutulmasını sağlayan, mağdurun ve toplumun korunmasını destekleyen kararların infaz edilmesinde kullanılan bir yöntemdir.*"

³⁸⁹ Elektronik izlemeye başvurulabilen tüm hallerin listesi için bkz. Çetin, **a.g.e.**, s. 25.

³⁹⁰ Çetin, **a.g.e.**, s. 57.

³⁹¹ Çetin, **a.g.e.**, s. 59.

Zira elektronik izlemeye başvurulduğunda kişilerin ses ve görüntüleri dinlenememekte, izlenememekte ve kayda alınmamaktadır³⁹².

Türkiye’de elektronik izlemede kullanılan yöntem karma olup hem GPS hem de RF yönteminden yararlanılmaktadır³⁹³. Türk hukukunda elektronik izlemeye yalnız yetişkinler için başvurulabilmektedir³⁹⁴. Elektronik izleme; hüküm, adli kontrol kararı ya da denetimli serbestlik süresince başvuru olan bir yöntem ise de izleme kayıtlarının tutulup tutulmayacağına ilişkin hükme yer verilmemiş olması nedeniyle kanaatimizce kayıt yapılamayacaktır. Yapılan izleme anlık olmak zorundadır. Ayrıca izleme sürecini yürütecek olan bir komisyonun olması ve izlemenin elektronik yapılmasından ziyade insan unsuruna yer verilerek insan tarafından yapılması gerektiği ileri sürülmektedir³⁹⁵.

Elektronik İzleme Merkezi görevlilerince izlenen kişilere ilişkin rapor tutulduğunda bu rapor, kişisel veriler ihtiva ettiğinden Kolluk ve Ceza Adaleti Direktifi hükümleri cezaların infazı sırasında elde edilen bu kişisel veriler bakımından da uygulanacaktır. Kanun ve Yönetmelik’e göre Elektronik İzleme Merkezi görevlileri, gizliliğe uygun davranmakla yükümlüdürler³⁹⁶. Ancak Yönetmelik “*Bu bilgiler Kanunun veya bu Yönetmeliğin zorunlu kıldığı haller dışında hiçbir kurum ve kişiye verilemez*”³⁹⁷ hükmü ile âdeta Kanun’un gizlilik ilkesini esnetmiştir.

Elektronik izlemeye başvuru olan hallerden hapis cezasının konutta çektirilmesinde, kişinin kadın mahkûm veya altmış beş yaşını bitirmiş mahkûm olması durumunda altı ay veya daha az süreli hapis cezası konutta infaz edilebilecektir. Bu hüküm, kadının ailenin temelini oluşturduğundan bahisle³⁹⁸ kadına imtiyaz sağlamışsa da kanaatimizce konutta ceza infazında kadın-erkek ayrımı gözetilmesi eşitliğe

³⁹² 6284 sayılı Kanun m. 12/1 “*Bu Kanun hükümlerine göre verilen tedbir kararlarının uygulanmasında hâkim kararı ile teknik araç ve yöntemler kullanılabilir. Ancak, bu suretle, kişilerin ses ve görüntülerini dinlenemez, izlenemez ve kayda alınmaz.*”

³⁹³ Çetin, **a.g.e.**, s. 108.

³⁹⁴ Çetin, **a.g.e.**, s. 248.

³⁹⁵ Işık, **a.g.e.**, s. 43.

³⁹⁶ 5402 sayılı Kanun m. 4/1-b “*Gizlilik: Bu Kanunun uygulanmasında görev alanlar; suçtan zarar gören, şüpheli veya sanık, hükümlü ya da bunların ailesi hakkında öğrenmiş olduğu bilgilerin gizliliğini korumak zorundadır. Bu bilgiler kanunun zorunlu kıldığı haller dışında hiçbir kurum ve kişiye verilemez.*”

³⁹⁷ Denetimli Serbestlik Hizmetleri Yönetmeliği m. 5/1-b.

³⁹⁸ Koç, **a.g.e.**, s. 203.

aykırıdır ve bu hükmün sonucu olarak altı ay hapis cezasına mahkûm olmuş iki bireyden yalnız kadın olanın cezası, konutta infaz edilecek ve kişisel verileri de izlemenin konusu olacaktır. Kolluk ve Ceza Adaleti Direktifi m. 6 her ne kadar veri sahipleri arasında ayırım yapılarak verilerin işlenmesini öngörmüşse de bu ayırım; şüpheli, sanık, tanık ve yargılamanın diğer süjeleri arasında bir ayırım olup ayrımcılık yapılmasını hedeflememektedir. Dolayısıyla kadın ve erkek arasında bu türden bir infaz rejimi ayrımcılığının sonucu olarak kişisel veri işlenmesinde de ayrımcılık söz konusu olmaktadır ve bu eşitlik ilkesi ile bağdaşmamaktadır³⁹⁹.

D. Hükümlünün İletişiminin Denetlenmesi

Hükümlülerin mektuplaşması ve telefonla görüşmeleri, aileleri başta olmak üzere dış dünya ile ilişki kurmalarına olanak sağlamakta ve böylece cezaların ıslah amacına hizmet etmektedir. Aynı zamanda bu olanaklardan yararlanan hükümlü hakkında denetim yapılarak kişisel veri toplanmaktadır. İspanya, Danimarka, Slovenya’da mektupların denetlendiği esnada hükümlü de hazır bulundurulmakta, Belçika’da cezaevi müdürü tarafından denetleme yapılmakta iken İtalya’da ise mektup denetimi hakim veya savcı kararı ile yapılmaktadır⁴⁰⁰.

CGİK m. 66/1’e göre hükümlülerin telefon görüşmeleri dinlenmekte ve ceza infaz kurumu idaresince kayıt altına alınmaktadır. Ancak bu kayıtların ne kadar süre ile tutulacağı, kimlerin bu kayıtlara erişebileceği, telefon görüşmesi hükümlü ve avukatı arasında gerçekleşiyorsa kaydedilip kaydedilmeyeceği gibi hususlar düzenlenmemiştir.

CGİK m. 68 uyarınca hükümlülerin alıcı ve gönderici olduğu mektuplar, suç işlenmesinin önlenmesi ve infaz güvenliğinin sağlanması amacıyla denetlenmekte ve cezaevi idaresince oluşturulan bir okuma komisyonunca okunmaktadır. Son yıllarda cezaevi nüfusunun artması üzerine, Adalet Bakanlığı Ceza ve Tevkifevleri Genel Müdürlüğü’nün bir yazısı ile mektupların taranıp UYAP’a kaydedilmesi şeklinde idari bir uygulamaya başlanmıştır. Bu uygulamanın AY m. 20’ye aykırı olduğu iddiasıyla

³⁹⁹ Özbek, **İnfaz Hukuku**, s. 111.

⁴⁰⁰ Bülent Altınsoy, “Avrupa İnsan Hakları Mahkemesi Kararları Işığında Mahkûmların Özel Hayatı”, **TBB Dergisi**, c. 27, s. 115, Ankara, 2014, s. 47.

AYM'ye birkaç bireysel başvuruda bulunulmuştur. AYM, mektuplarda kişiyi belirlenebilir kılan yazının ve ad soyadın kişisel veri olduğunu ve kişisel verilerin korunmasından yararlanması gerektiğini belirtmiştir⁴⁰¹. AYM, mektupların okunması ve denetlenmesinin, CGİK m. 68'te öngörülmesi ve infaz işlemlerinde UYAP'ın kullanılması nedeniyle kanuna uygun olduğu kanaatindedir⁴⁰². Zira AYM'ye göre kişisel verinin UYAP'a kaydına ilişkin detayların tamamının, kanunla düzenlenmesi mümkün olmayıp düzenleyici işleme bırakılması isabetlidir⁴⁰³. Ancak AYM kararına katılmak mümkün değildir. Müdahalenin kanuna uygun olabilmesi için kanunun öngörülebilir, ulaşılabilir olmasının yanında kişisel verilerin korunması için güvenceler de içermesi gerekmektedir. Oysa mektupların UYAP'ta ne kadar süre ile tutulacağı, kimlerin bu mektuplara erişebileceği ne kanunda ne de bahsi geçen yazıda düzenlenmiştir. Dolayısıyla bu idari uygulamanın hukuka uygun olduğunu söylemek oldukça güçtür⁴⁰⁴.

Hükümlünün savunma hakkının temini için avukatı ile de görüşmesi mümkündür. Ancak CGİK m. 59/5'te belirtilen suçlardan mahkûm olan kişinin avukatı ile görüşmesinin toplum ve kurumun güvenliğini tehdit etmesi halinde hakim kararı ile avukat ve hükümlünün görüşmeleri üç ay süre ile teknik cihazla sesli veya görüntülü olarak kaydedilebilecektir. Bu kayıtların tutulma süresi, kimlerin bu kayıtlara erişebileceğine ilişkin bir düzenleme bulunmamaktadır.

E. Seyirden Yasaklanma

Spor müsabakalarını seyirden yasaklanma 6222 sayılı Sporda Şiddet ve Düzensizliğin Önlenmesi Kanunu m. 18 uyarınca öngörülmüş bir güvenlik tedbiri aynı zamanda bir koruma tedbiridir⁴⁰⁵. İki halde de hakkında tedbir uygulanan kişinin

⁴⁰¹ *Kemal Karanfil* Başvurusu, B. No: 2017/24776, 24.05.2018, para. 46 Çevrimiçi <https://kararlarbilgibankasi.anayasa.gov.tr/> 29.03.2020.

⁴⁰² *Kemal Karanfil*, para. 63-64; Aynı yönde bkz. *Bekir Demirci* Başvurusu, B. No: 2017/37143, 11.03.2020, para. 38.

⁴⁰³ *Kemal Karanfil*, para. 66.

⁴⁰⁴ *Kemal Karanfil* başvurusunda Engin Yıldırım'ın karşı oyunda ise bu uygulamanın, belirtilen gerekçelerle ölçüsüz olduğu öne sürülmüştür. Bkz. *Kemal Karanfil*, Engin Yıldırım'ın Karşı Oyu, para. 9.

⁴⁰⁵ Seyirden yasaklanmanın önleyici tedbir, koruma tedbiri, adli kontrol benzeri kurum ve nihayet güvenlik tedbiri olduğuna dair bkz. Bahri Öztürk, "Sporda Şiddet ve Düzensizliğin Önlenmesine Çare

bilgileri Emniyet Genel Müdürlüğü Merkezi Spor Güvenlik Birimi bünyesinde tutulan elektronik bilgi bankasına kaydedilmektedir. Bilgi bankasına federasyonlar ve spor kulüpleri erişebilmektedir⁴⁰⁶. Aynı zamanda bu kişiye dair bilgiler, ilgili spor kulübü ve yurt dışında yapılan bir müsabaka ise o ülkedeki yetkili makama bildirilecektir. Ancak kişisel verilerin yurtdışına aktarımına izin veren bu hüküm veri sahibine hiçbir koruma sağlamamaktadır. Yetkili makamın yeterli veri koruma düzeyine sahip olup olmadığı değerlendirmesi yapılmaksızın veri makama aktarılacaktır. Ayrıca verinin aktarılması halinde veri sahibine bildirim yapıp yapılmayacağı da belirtilmemiştir.

Kanunda elektronik bilgi bankasında yer alacak veriler sayılmamış, seyirden yasaklanmaya ilişkin bazı hususlar Sporda Şiddet ve Düzensizliğin Önlenmesine Dair Kanunun Uygulanmasına İlişkin Yönetmelik'te⁴⁰⁷ düzenlenmiştir. Kanunda yer almazken Yönetmelik m. 7/1-c'ye göre kişinin fotoğrafı da kaydedilecek veriler arasında sayılmıştır. Ayrıca ne Kanun ne Yönetmelik'te ne kadar süre ile bu verilerin tutulacağına yer verilmiştir.

Güvenlik tedbiri olarak düzenlenen seyirden yasaklanmanın infazına, hükmün kesinleşmesi ile başlanacak ve cezanın infazının sona ermesinden itibaren bir yıl geçmesi ile son verilecektir. Ceza verilmesine yer olmadığı kararı verilmişse de bunun kesinleşmesinden itibaren bir yıl geçmesi ile seyirden yasaklanma son bulacaktır. Bu bir yıllık süreler, kişi hakkında ikinci kez seyirden yasaklanma yaptırımına karar verilmesi halinde üç yıl; üçüncü kez karar verilmesi halinde ise beş yıl olarak uygulanacaktır. Güvenlik tedbiri olan seyirden yasaklanma adli sicile kaydedilmektedir⁴⁰⁸. Ancak maddede kişinin verilerinin veri bankasından ne zaman silineceği düzenlenmemiştir. Kanaatimizce Kanun üst had olarak beş yıl süre ile tedbirin uygulanmasını öngördüğü için veriler en fazla beş yıl süre ile tutulmalıdır.

Koruma tedbiri olarak seyirden yasaklanma ise 6222 sayılı Kanun m. 18'de belirtilen suçlar için soruşturma başlatılması halinde uygulanmaktadır. Tedbir savcı veya mahkeme tarafından kaldırılabilmesi gibi kovuşturmayaya yer olmadığı kararı

Olarak Seyirden Yasaklanma", **Sporda Şiddet ve Düzensizliğin Önlenmesi Kanunu**, Ed. Cumhuriyet Şahin, İzzet Özgenç, İlhan Üzülmüş, Ankara, Seçkin Yayıncılık, 2012, s. 36.

⁴⁰⁶ 6222 sayılı Kanun m. 18/4.

⁴⁰⁷ R.G. Sayısı: 28505 R.G. Tarihi: 22.12.2012.

⁴⁰⁸ 6222 sayılı Kanun m. 18/1.

verilmesi, sanığın beraat etmesi veya hakkında düşme kararı verilmesi hallerinde de ortadan kalkar⁴⁰⁹ ve bu hususlar elektronik bilgi bankasına kaydedilir. Ancak Kanun tedbirin sona ermesine rağmen kişinin bilgilerinin veri bankasından silinmesini öngörmemiştir. Bir tedbirin adli kontrol müessesesi benzeri bir gereği olarak⁴¹⁰ kişi, taraftarı olduğu takımın müsabakasının yurt içinde yapılması halinde müsabakanın başladığı saatte ve bundan bir saat sonra kolluğa başvuracaktır ve kolluk bu işlemlerin takibi için biyometrik yöntemler kullanabilecektir⁴¹¹. Biyometrik yöntemler tanınabilirliğe en iyi hizmet eden yöntemlerden olduğu için bu düzenleme holiganlıkla mücadelede uygun bir tedbirdir. Ancak bu verilerin nasıl işleneceği, nereye kaydedileceği, verilerin ne süre ile muhafaza edileceği yine maddede düzenlenmemiştir.

Önleyici kolluk faaliyeti gereği de kişi seyirden yasaklanabilir⁴¹². Alkol ya da uyuşturucu madde etkisi altında olan kişinin spor müsabakasının tertip edildiği alana girmesi ve dışarı çıkmamada ısrarcı olması halinde kişi bir yıl boyunca seyirden yasaklanabilir. Bu tedbir uygulandığında kişinin verileri bilgi bankasına kesinlikle kaydedilmeyecektir, zira m. 18/4'te yalnız koruma tedbiri ve güvenlik tedbiri ifadesi yer almaktadır.

⁴⁰⁹ 6222 sayılı Kanun m. 18/5.

⁴¹⁰ Adli kontrol benzeri müessese görüşü için bkz. Öztürk, **a.g.e.**, s. 43; Yusuf Yaşar, "6222 Sayılı Sporda Şiddet ve Düzensizliğin Önlenmesine Dair Kanun'un 18'inci Maddesinde Yer Alan 'Seyirden Yasaklanma' ile 'Seyirden Yasaklama' Tedbirleri", **MÜHF- HAD**, c. 19, s. 1, 2013, s. 32.

⁴¹¹ 6222 sayılı Kanun m. 18/8.

⁴¹² 6222 sayılı Kanun m. 18/7; Bu maddeyi önleyici tedbir olarak tasnif eden eser için bkz. Öztürk, **a.g.e.**, s. 36; idari yaptırım olarak tasnif eden eser için bkz. Yaşar, **a.g.e.**, s. 27.

SONUÇ

Kişisel verilerin korunması ulusalüstü hukukta görece olarak yeni bir haktır ve AİHS'nin öngördüğü koruma sisteminde özel yaşamın gizliliğine saygı hakkı bünyesinde değerlendirilmektedir. Türk hukukunda kişisel verilerin kanun düzeyinde korunması ise ilk kez KVKK'nin yürürlüğü ile sağlanmıştır. Ancak veri işlemeye konu olan veriler; suçların önlenmesi, ceza muhakemesi, cezaların infazı ve devletin istihbarat faaliyetleri gereği işlenen veriler olduğunda KVKK hükümleri uygulanmamaktadır. Bu da bu alanlarda kişisel verilerin yalnızca PVSİ, CMK ve diğer mevzuat uyarınca korunmasına neden olmaktadır. Ancak belirtilen mevzuatta da kişisel verilerin korunmasına dair düzenlemeler bir hayli sınırlıdır. Hakim, mahkeme veya savcı kararı olduğunda veri işleme kendiliğinden hukuka uygun olmaktadır. Örneğin yürütülen bir ceza soruşturması gereği savcıların “İstanbul’da otuz kırk yaş arasında polikistik over sendromuna sahip” tüm kadınların hasta kayıtlarına ulaşması mümkündür.

Avrupa Birliği'nin kişisel veriler alanındaki düzenlemelerine bakıldığında hemen hepsinin kişisel verilerin korunması ve serbest veri aktarımına ilişkin standardizasyon yaratma çabası içinde olduğu anlaşılmaktadır. Ancak söz konusu kişisel verilerin bir suçla ilgili olarak işlenmesi olduğunda, Avrupa Birliği düzeyinde standart yakalanamamış ve veri koruması ulusal hukuk düzenlemelerine bırakılmıştır. Avrupa Birliği'nde kişisel verilerin korunması düzenlemeleri, 2016 yılındaki Veri Koruma Reformu'nun ardından hız kazanmıştır. Avrupa Konseyi ve Avrupa Birliği düzeyindeki veri koruma düzenlemelerinde kapsam dışı bırakılan suçların önlenmesi, ceza muhakemesi ve cezaların infazı sırasındaki veri işleme faaliyetleri ilk kez Kolluk ve Ceza Adaleti Direktifi ile kendilerine korunaklı bir alan bulmuşlardır. Nitekim tezimizin ana eksenı de Kolluk ve Ceza Adaleti Direktifi üzerine kurulmuştur. Kolluk ve Ceza Adaleti Direktifi, genel ve özellikle ticari kişisel verilerin korunmasını düzenleyen GDPR'ın gölgesinde kalmakla birlikte esasen GDPR ile paralel bir koruma sağlamaktadır. Ancak Kolluk ve Ceza Adaleti Direktifi işlemeye konu olan verilerin mahiyeti gereği bilgilendirme hakkı, erişim hakkı ve diğer haklar bakımından

daha derinlikli sınırlamalara yer vermekte ve veri sahibinin rızasına hukuki sonuç bağlamamaktadır.

Kolluk ve Ceza Adaleti Direktifi'nin kanaatimizce en önemli eksikliği, ulusal güvenlik ve istihbarat faaliyetleri gereği işlenen verilerin korunmasını kapsam dışı bırakmış olmasıdır. Üstelik Direktif, kamu güvenliği ve ulusal güvenlik arasındaki ayrıma yer vermemiş ve kamu güvenliği gereği işlenen verileri Kolluk ve Ceza Adaleti Direktifi hükümlerine tabi tutmuştur. Bu hüküm, ulusal güvenlik ve temel hak ve özgürlükler yarışmasında yine güvenlik lehine hakkın feda edilmesinin bir görünümünü oluşturmaktadır.

Türk hukukunda da ulusal güvenlik gereği işlenen verilerin korunmaması kişilerin mağduriyetine yol açmaktadır. Ulusal güvenlik nedeniyle kişisel verilerin işlenmesinde AB hukuku ve Türk hukukunun aksine AİHM ve AYM daha incelmış bir adalet anlayışının yansıması olarak, bu veri işleme faaliyetlerini de özel yaşamın gizliliği koruması çerçevesinde değerlendirmektedir. Bu türden veri işleme faaliyetleri özel yaşamın gizliliğine bir müdahaledir ve bu müdahale hukuka uygunluk, gereklilik ve orantılılık şartlarını sağlamalıdır. Türk hukukunda bu verilerin korunması için yapılması gereken, istihbarat gereği veri işleme ve suçların önlenmesi gereği veri işlemleri keskin bir şekilde ayırmaktır. Suçların önlenmesi amacıyla işlenen veriler, PVSK'ye hüküm eklenerek ya da münferit bir kanun ile korunmalıdır. Önleyici kolluk tedbiri olarak başvuru ile iletişimin denetlenmesinde söz konusu terör suçları olduğunda iletişim süresiz şekilde denetlenebilmektedir ki bu da süresiz şekilde veri işlemek demektir. Bu düzenlemeye son verilmeli, ancak suç işlendiğine ilişkin basit bir şüphe varsa CMK hükümleri gündeme gelmeli ve iletişim denetlenmelidir. Ayrıca önleyici amaçla başvuru ile iletişimin denetlenmesi tedbiri sona erdiğinde iletişimi denetlenen ve bu suretle kişisel verileri işlenen veri sahibine bilgilendirme yapılmalıdır.

Son dönemlerde ulusal güvenlik nedeniyle veri işlemlere en güncel örnek güvenlik soruşturmalarıdır. Ancak güvenlik soruşturması sırasında veri işleme bir yönetmeliğe dayandığı için kişisel verilerin korunması hakkı ihlal edilmektedir. Nitekim AYM de bu gerekçeyle güvenlik soruşturmaları gereği kişisel veri işlemler

ile ilgili hak ihlali kararları vermiş ve soyut norm denetimi yoluyla kamu görevine girişte güvenlik soruşturmasının uygulanmasını iptal etmiştir. Güvenlik soruşturmalarına ilişkin yapılacak olası bir kanuni düzenlemede; soruşturmaya konu veriler, bu verilere erişecek kolluk veya diğer makamlar, verilerin tutulacağı süre açıkça kanunda gösterilmelidir.

Ceza muhakemesi hukukunda bazı koruma tedbirlerine hukuka aykırı başvurulduğunda bireylere tazminat hakkı tanınmıştır. Ancak bu hak, özellikle kişi özgürlüğünü ihlal etmiş koruma tedbirleri için tanınmış olup özel yaşamın gizliliğini ve kişisel verilerin korunmasını ihlal eden tedbirler için öngörülmemiştir ki bu bir eksikliktir.

Biyometrik veriler suçların önlenmesi, ceza muhakemesi, cezaların infazında ve hatta spor salonlarında, mesai takiplerinde dahi kullanılmaktadır. Ancak biyometrik veri işlemeye konu olan parmak izlerinin ne süre ile muhafaza edileceğine dair düzenlemeler veri işleme ilkeleri ile bağdaşmamaktadır. İlgili kısımlarda belirttiğimiz üzere söz gelimi gözaltına alınan kişinin parmak izi, ceza yargılamasında mahkûm olmasa dahi AFIS'ye kaydedilmesinden itibaren seksen yıl ve kişinin ölümünden sonra on yıl kadar tutulmaya devam etmektedir. Bu hüküm, verinin amaçla bağlı işlenmesi, süreli olarak işlenmesi ilkesi ve masumiyet karinesi ile bağdaşmamaktadır. Zira AFIS'de hükümlü kişinin verileri de gönüllü olarak parmak izi işlenen kişinin verileri de yer almaktadır. Oysa ilgili AİHM kararlarında belirttiğimiz üzere verinin muhafaza süresi; isnat edilen suçun niteliği ve ciddiyeti, veri sahibinin yaşı gibi hususlar gözetilerek belirlenmelidir. Hatta kişinin mahkûm olduğu bir suçun muhakemesi sırasında parmak izi alınmış olsa dahi bu biyometrik veriler belirli bir süre ile sınırlı olarak tutulmalıdır.

Türk hukukunda suçların önlenmesi amacıyla başvuru alan elektronik gözetim herhangi bir kanuni dayanağa sahip değildir. İnsanlarda izlendikleri korkusunu uyandırarak suç işlemeyi caydırma amacıyla hemen her yere yerleştirilen MOBESE kameralarından; yalnız suçların önlenmesinde değil, işlenen suçun aydınlatılmasında da yararlanılmaktadır. Amaç her ne kadar suç işlenmesinin önlenmesi ve suçların aydınlatılması sayesinde kamunun menfaatinin sağlanması olsa da MOBESE

kameraları ile izlenme ve kaydedilme bireylerin kişisel verilerinin korunması hakkına bir müdahaledir. Bu müdahale kanuna dayanmalıdır, oysa meri mevzuatta bir düzenleme bulunmamaktadır ve bu nedenle hukuka aykırı kayıtlardan ceza muhakemesinde yararlanılmamalıdır. MOBESE ile izleme ve kaydetme faaliyetlerini düzenleyecek olası bir kanuni düzenlemede; verilerin tutulma süresi, bu verilerin tutulacağı veri tabanına erişme yetkisi olan makam ve kişiler yer almalıdır. Ceza muhakemesinde kullanılan kayıtlarda, suçla ilgisi olmayan kişilerin yüzleri bulanıklaştırılmalı ve görüntü anonim hale getirilmelidir. MOBESE kameraları suç ve suçluluk olgusunun fazla olduğu yerlere kurulmalıdır ve ayrıca suçluluk oranları belirli periyotlarla gözden geçirilerek kameranın gereksiz olması halinde izleme ve kayıt işlemi sona ermelidir.

GBT uygulamasının herhangi bir kanuni dayanağı bulunmamaktadır, daha da vahimi adli sicil kaydı dahi silinebilirken GBT kayıtları belirli suçlar söz konusu olduğunda silinmemektedir ve bu durum, kişinin yaşamı boyunca GBT kontrolünde damgalanmasına neden olmaktadır. İlgili AYM ve AİHM kararları da göz önüne alındığında, gizlilik gerekçesi ile yayımlanmayan bir yönergeye dayanarak bireylerin kişisel verilerinin ilanihaye tutulması uygulamasına derhâl son verilmelidir.

Son olarak belirtilmelidir ki Kolluk ve Ceza Adaleti Direktifi'nin sağladığı kişisel veri koruması Türk hukuku için erişilmesi gereken bir nokta ya da hedef değildir. Zira başta ulusal güvenlik gerekçesiyle veri işlemler olmak üzere Direktif yeterli düzeyde veri koruması sağlamamaktadır. Ancak kişisel verilerin PVSİ, CMK, Adli Sicil Kanunu'ndaki dağınık sınırlı sayıda hüküm ile korunması da yetersizdir. Veri sahibinin yaşı, isnat edilen suçun niteliği, suçun işlenmiş olması halinde veri sahibi failin mahkûm olup olmadığı, veri sahibinin muhakemedeki hangi süje olduğu gibi hususlar gözetilerek veri sahibinin bilgilendirilme, veriye erişme ve özellikle tazminat olmak üzere haklarının yer aldığı bir veri koruma kanunu ihdas edilmelidir. Özellikle bilişim teknolojilerinden yararlanılarak işlenen suçların muhakemesinde yabancı bir devlet veya organizasyondan aktarılabilecek veya bu devlet veya organizasyona aktarılabilecek verilerin aktarımı ve korunması da kanunda düzenlenmelidir. Zira bu veriler, yalnız adli yardım antlaşmalarının öngördüğü koruma ve aktarım şartlarına bırakılamayacak kadar önemlidir.

KAYNAKÇA

- Abanoz, Buket : “Kamusal Alanda Kameralı Gözetlemenin Suçun Önlenmesindeki Etkisi ve Elde Edilen Delillerin Hukuka Uygunluğu Sorunu”, **İstanbul Üniversitesi Sosyal Bilimler Enstitüsü**, Yayınlanmamış Yüksek Lisans Tezi, İstanbul, 2015.
- Adar Özdemir, : **Nemo Tenetur İlkesi Bağlamında Beden Muayenesi ve Çiğdem Vücuttan Örnek Alınması**, İstanbul, Seçkin Yayıncılık, 2020.
- Akgül, Aydın : “Kişisel Verilerin Korunması Bağlamında Biyometrik Yöntemlerin Kullanımı ve Danıştay Yaklaşımı”, **TBB Dergisi**, c. 28, s. 118, 2015, ss. 199-222.
- Akgül, Aydın : “Kişisel Verilerin Korunmasında Yeni Bir Hak: ‘Unutulma Hakkı’ ve AB Adalet Divanı’nın ‘Google Kararı’”, **TBB Dergisi**, c. 27, s. 116, 2015, ss. 11-38.
- Akıntunde, Salami : “The Impact of Directive (EU) 2016/680 on the Processing Emmanuel of Personal Data by Competent Authorities for The Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties and On the Free Movement of Such Data on the Existing Privacy Regime”, Çevrimiçi <http://dx.doi.org/10.2139/ssrn.2912449> 10.04.2019.
- Akyürek, Güçlü : **Özel Hayatın Gizliliğini İhlal Suçu**, Güncellenmiş ve Genişletilmiş 2. Baskı, Ankara, Seçkin Yayıncılık, 2014.

- Alan, Esra : “Ceza Muhakemesinde Beden Muayenesi ve Vücuttan Örnek Alınması”, **Uğur Alacakaptan’a Armağan**, c. 1, İstanbul, İstanbul Bilgi Üniversitesi Yayınları, 2008, ss. 45-58.
- Alkan, Mehmet : “Avrupa Konseyi Bakanlar Komitesinin İnsan Hakları ve Terörle Mücadele Hakkındaki İlkeleri ve Türkiye’nin Terörle Mücadele Mevzuatı”, **TBB Dergisi**, c. 29, s. 125, 2016, ss. 9-38.
- Allen, David, van Beek, Evelien, Borking, John : **Practical Guide on the Use of Personal Data in the Police Sector**, Council of Europe, Strasbourg, 2018.
- Altındağ, Halil : “Kişisel Verilerin Korunması Bağlamında İdarenin Sorumluluğu”, **İKÜHFD**, c. 18, s. 2, 2019, ss. 387-401.
- Altınsoy, Bülent : “Avrupa İnsan Hakları Mahkemesi Kararları Işığında Mahkûmların Özel Hayatı”, **TBB Dergisi**, c. 27, s. 115, Ankara, 2014, ss. 37-60.
- Arslan Öncü, Gülay : **Özel Yaşamın Korunması Hakkı**, İstanbul, Beta Yayıncılık, 2011.
- Arslan Öncü, Gülay : “Özel Yaşama ve Aile Yaşamına Saygı Hakkı”, **İnsan Hakları Avrupa Sözleşmesi ve Anayasa Mahkemesine Bireysel Başvuru Kapsamında Bir İnceleme**, Ed. Sibel İncoğlu, 3. Baskı, İstanbul, Beta Yayıncılık, 2013.
- Arslan Öncü, Gülay : “Özel Yaşama ve Aile Yaşamına Saygı Hakkı”, **Anayasa Mahkemesine Bireysel Başvuru El Kitapları Serisi-8**,

2019

Çevrimiçi

https://www.anayasa.gov.tr/media/5604/ozel_yasam_hakki.pdf 30.03.2020.

Aslan, Volkan : “Avrupa İnsan Hakları Mahkemesi Kararlarında Ajan Provokatör ve Adil Yargılanma Hakkı”, **Hukukçular Arası Makale Yarışması**, Ed., Türkiye Barolar Birliği, Ankara, Türkiye Barolar Birliği Yayınları, 2014, ss. 25-37.

Aşıkoğlu, Şehriban İpek : **Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri**, İstanbul, On İki Levha Yayıncılık, 2018.

Atak, Songül : “Avrupa Konseyi’nin Kişisel Veriler Açısından Sağladığı Temel Güvenceler”, **TBB Dergisi**, c. 22, s. 87, 2010, ss. 90-120.

Atalay, Ayşe Özge : “Ceza Muhakemesi Hukukunda Moleküler Genetik İncelemelerin Özel Nitelikli Kişisel Verilerin Korunması Açısından Değerlendirilmesi”, **CHKD**, c. 7, s. 2, 2019, ss. 127-184.

Avrupa Birliği Başkanlığı : “AB-Türkiye İlerleme Raporu 2015”, Çevrimiçi https://www.ab.gov.tr/files/000files/2015/11/2015_turkiye_raporu.pdf 08.01.2020.

Avrupa Birliği Başkanlığı : “AB-Türkiye İlerleme Raporu 2016”, Çevrimiçi https://www.ab.gov.tr/files/ceb/Progress_Reports/2016_ilerleme_raporu_tr.pdf 16.03.2020.

Avrupa Birliği : “AB-Türkiye İlerleme Raporu 2018”, Çevrimiçi Başkanlığı https://www.ab.gov.tr/siteimages/pub/komisyon_ulke_raporlari/2018_turkiye_raporu_tr.pdf 16.03.2020.

Avrupa Birliği : “AB-Türkiye İlerleme Raporu 2019”, Çevrimiçi Başkanlığı https://www.ab.gov.tr/siteimages/birimler/kpb/2019_trkiye_raporu-tr.pdf 16.03.2020.

Avrupa Komisyonu : “A New Era for Data Protection in the EU What Changes After May 2018”, Çevrimiçi https://ec.europa.eu/info/sites/info/files/data-protection-factsheet-changes_en.pdf 19.03.2020.

Aydın, Sedat Erdem : **AİHM İçtihatları Bağlamında Kişisel Verilerin Kaydedilmesi Suçu**, İstanbul, On İki Levha Yayıncılık, 2015.

Aygörmez Uğurlubay, Gülsün Ayhan : “Almanya, İsviçre ve Avusturya Hukuku Bağlamında Türk Ceza Muhakemesi Hukukunda Adli DNA Analizleri”, **CHKD**, c. 5, s. 2, 2017, ss. 29-87.

Ayözger, Ayşe : **Kişisel Verilerin Korunması**, İstanbul, Beta Yayıncılık, Çiğdem 2016.

Başalp, Nilgün : “Avrupa Birliği Veri Koruması Genel Regülasyonu’nun Temel Yenilikleri”, **MÜHF-HAD**, c. 21, s. 1, 2015, ss. 77-106.

Başalp, Nilgün : **Kişisel Verilerin Korunması ve Saklanması**, Ankara, Yetkin Yayınları, 2004.

- Baştürk, Ömer Özmen : **Milli İstihbarat Teşkilatı'na Ait Bilgi, Belge ve Kimliklere Karşı Suçlar**, Ankara, Adalet Yayınevi, 2019.
- Bayındır, Sinan, Apiş, Özge, Ersöz, Oğuz : **Kitle İletişim Hukuku**, İstanbul, On İki Levha Yayıncılık, 2018.
- Bayındır, Zülküf : “Özel Yaşamın Korunması Çerçevesinde İstihbarat Faaliyetleri”, **Bahçeşehir Üniversitesi Sosyal Bilimler Enstitüsü**, Yayımlanmamış Yüksek Lisans Tezi, İstanbul, 2016.
- Bayram, Zeynep : “Kolluğun Suç Öncesi ve Sonrası Kişisel Veri Toplama Yetkisi”, **Bahçeşehir Üniversitesi Sosyal Bilimler Enstitüsü**, Yayımlanmamış Yüksek Lisans Tezi, İstanbul, 2009.
- Beşe, Ertan : **Terörizm, Avrupa Birliği ve İnsan Hakları**, İstanbul, Seçkin Yayıncılık, 2002.
- Bignami, Francesca : “Protecting Privacy Against the Police in the European Union: The Data Retention Directive”, **Duke Law School Faculty Scholarship Series**, paper 76, 2007, Çevrimiçi http://lsr.nellco.org/duke_fs/76 23.03.2020.
- Birtek, Fatih : “İstihbarat Amacıyla İletişim Özgürlüğüne Müdahale Edilmesi ve Müdahaleden Elde Edilen Materyallerin Delil Olarak Kabul Edilebilirliği”, **CHD**, c. 6, s. 16, Ağustos 2011, ss. 100-148.
- Bostancı Bozbayındır, Gülşah : “Avrupa Birliği Ceza Hukuku’nda Polis ve Ceza Adaleti Otoritelerine Yönelik 2018/680 Sayılı Direktif: Kişisel

Verilerin Ceza Adalet Mekanizmalarında Korunmasına Getirilen Standartlar ve Direktife Yönelik Eleştiriler”, **GSÜHFD**, c. 17, s. 2, 2018, ss. 51-104.

Bozkurt, Enver, Köktaş, Arif : **Avrupa Birliği Hukuku**, Güncellenmiş 7. Baskı, Ankara, Legem Yayıncılık, 2018.

Boz, Ahmet : “Kişisel Verilerin Korunması: Türkiye, ABD ve AB Örnekleri”, **Polis Akademisi Güvenlik Bilimleri Enstitüsü**, Yayımlanmamış Yüksek Lisans Tezi, Ankara, 2014.

Brkan, Maja : “The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU’s Constitutional Reasoning”, **German Law Journal**, s. 20, 2019, ss. 864-883.

Bruynseels, Koen, van den Hoven, Jeroen : “How to Do Things with Personal Big Biodata”, **Social Dimensions of Privacy Interdisciplinary Perspectives**, Ed. Beate Roessler, Dorota Mokrosinska, UK, Cambridge, 2015.

Bulak Uygun, Begüm : “Avrupa İnsan Hakları Mahkemesi’nin Son Dönemdeki İçtihatları Işığında İletişimin Adli ve Önleme Amaçlı Olarak Denetlenmesi ve Özel Hayata Müdahale”, **YÜHFD**, c. 13, s. 2, İstanbul, 2017, ss. 139-154.

Burch, Kathleen M. : “Protecting Privacy in the Digital Age: Europe and The United States”, **Prof. Dr. Feridun Yenisey’e Armağan**, c. 2, İstanbul, Beta Yayıncılık, 2014, ss. 1713-1731.

Bu-Pasha, Shakila : “Cross-Border Issues Under EU Data Protection Law With Regards to Personal Data Protection”, **Information and**

Communication Technology Law, c. 26, s. 3, 2017, ss. 213-228.

Can, Neslihan : “Hasta Mahremiyeti Hakkı”, **TBB Dergisi**, s. 147, 2020, ss. 183-219.

Can, Neslihan : “Tıp Hukuku Bağlamında Çocuk Hastanın Mahremiyet Hakkı”, **3. Uluslararası Tıp Hukuku Kongresi Bildirileri Kitabı**, Ed. Hakan Hakeri, Cahid Doğan, Ankara, Adalet Yayınevi, 2019, ss. 1139-1144.

Centel, Nur : “5271 Sayılı Ceza Muhakemesi Kanunu’na Göre Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi”, **GSÜHFD**, c. 9, s. 1, 2011, ss. 161-192.

Craig, Paul, de Burca, Grainne : **EU Law Text Cases and Materials**, 5. Baskı, New York, Oxford University Press, 2011.

Crutzen, Rik, Ygram : “Why and How We Should Care About the General Data Protection Regulation”, **Psychology & Health**, c. 34, s. 11, 2019, ss. 1347-1357.

Peters, Gjalt-Jorn, Mondschein, Christopher

Cumhuriyet Gazetesi : “Çocuk Pornosu İzleyenleri Tespit Eden Sistem Türkiye’de”, Cumhuriyet Gazetesi, 14.07.2020, Çevrimiçi <https://www.cumhuriyet.com.tr/haber/cocuk-pornosu-izleyenleri-tespit-eden-sistem-turkiyede-1751575> 20.07.2020.

Custers, Bart, Sears, Alan M., : **EU Personal Data Protection in Policy and Practice**, The Hague, Springer, 2019.

Dechesne, Francien,
Georgieva, Ilina
Tani, Tommaso, van
der Hof, Simone

Çam, Ali Rıza : **Adli Bilişim ve Kolluk**, İstanbul, On İki Levha Yayıncılık, 2015.

Çekin, Mesut Serdar : **Avrupa Birliği Hukuku ile Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku**, 2. Baskı, İstanbul, On İki Levha Yayıncılık, 2019.

Çelik, Cahit : “UYAP’ın Temel Sistemi ve Güvenlik”, **Bilişim Hukuku**, Ed. Mete Tevetoğlu, İstanbul, Kadir Has Üniversitesi Yayınları, 2006, ss. 152-155.

Çetin, Soner Hamza : **Türk Ceza Hukuku’nda Elektronik İzleme**, Ankara, Adalet Yayınevi, 2020.

Çiçek, İbrahim : “GBT (Genel Bilgi Toplama) Kayıtlarının Silinmesi”, **Terazi Hukuk Dergisi**, c. 8, s. 88, 2013, ss. 44-48.

Dağ, Güray : “Kişisel Verilerin Ceza Muhakemesi Hukukunda Delil Olarak Kullanılması”, **Marmara Üniversitesi Sosyal Bilimler Enstitüsü**, Yayımlanmamış Doktora Tezi, İstanbul, 2011.

De Hert, Paul, Papakonstantinou, Vagelis : “The New Police and Criminal Justice Data Protection Directive: A First Analysis”, **New Journal of European Criminal Law**, c. 7, s. 1, Tilburg, 2016, ss. 7-19.

Derdiman, R. Cengiz, : “Devlet Gözetimi ile İnsan Haklarının Uyumlaştırılması
Tataroğlu, Nihal Sorunu ve Çözüm Önerileri”, **İÜHFD**, c. 7, s. 1, 2016, ss.
247-293.

Develioğlu, Hüseyin : **6698 Sayılı Kişisel Verilerin Korunması Kanunu ile
Murat Karşılaştırmalı Olarak Avrupa Birliği Genel Veri
Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması
Hukuku**, İstanbul, On İki Levha Yayınları, 2017.

Doğru, Osman : İnsan Hakları Avrupa Mahkemesi Kararlarının İç Hukuklara
Etkileri, Çevrimiçi
<https://www.anayasa.gov.tr/media/4671/dogru.pdf>
08.01.2020.

Dönmezer, Sulhi, : **Basın Hukuku**, Genişletilmiş 6. Baskı, İstanbul, Beta
Bayraktar, Köksal Yayıncılık, 2016.

Drăgoianu, Sergiu, : “Romania Transposes Directive (EU) 2016/680”, Çevrimiçi
Alexie, Daniel [https://www.lexology.com/library/detail.aspx?g=719b914a-
d5af-478b-a5a6-2b96c2b01ec3](https://www.lexology.com/library/detail.aspx?g=719b914a-d5af-478b-a5a6-2b96c2b01ec3) 30.03.2020.

Duran, Lütfi : **İdare Hukuku Ders Notları**, İstanbul, Fakülteler Matbaası,
1982.

Dursun, Selman : “Megan Kanunu (ABD’de Cinsel Suç Faillerinin Sicile
Kaydı ve Sicil Bilgilerinin Kamuya Açıklanması)”,
AÜEHFD, c. 8, s. 1-2, 2004, ss. 233-262.

Dursun, Selman : “Özellikle Mağduru Çocuk Olan Mükerrir Cinsel Suç
Faillerine Karşı Toplumun Korunması Bağlamında Megan

Kanunu Hakkında Soru ve Cevaplar”, **CHKD**, c. 2, s. 1-2, 2014, ss. 235-240.

Dülger, Murat : “Bilişim Suçları, Soruşturma ve Kovuşturma Yöntemleri ile
Volkan, Modoğlu, İnternet İletişim Hukuku (Uygulama Rehberi)”, **Türk Ceza
Gözde Adalet Sisteminin Geliştirilmesi Avrupa Birliği/ Avrupa
Konseyi Ortak Programı**, Ankara, Şen Matbaa, 2014.

Dülger, Murat : “Adli ve Kolluk Teşkilatında Kişisel Verilerin Korunması:
Volkan, Özkan, Onur ‘Unutulan’ Direktifin Kapsamlı ve Karşılaştırmalı Analizi”,
CHD, c. 15, s. 42, 2020, ss. 85-149.

Dülger, Murat Volkan : **Ceza Muhakemesi Hukukunda Dışlama Kuralı ve
Hukuka Aykırı Delillerin Uzak Etkisi (Zehirli Ağacın
Meyvesi Öğretisi)**, Ankara, Seçkin Yayıncılık, 2014.

Dülger, Murat Volkan : **Kişisel Verilerin Korunması Hukuku**, 2. Baskı, İstanbul,
Hukuk Akademisi, 2019.

Emniyet Genel : “Çarşı ve Mahalle Bekçilerinin Kimlik Sorma Yetkisi
Müdürlüğü Hakkında Basın Açıklaması”, Çevrimiçi
[https://www.egm.gov.tr/carsi-ve-mahalle-bekcilerinin-
kimlik-sorma-yetkisi-hakkinda-basin-aciklamasi](https://www.egm.gov.tr/carsi-ve-mahalle-bekcilerinin-kimlik-sorma-yetkisi-hakkinda-basin-aciklamasi)
16.03.2020.

Emniyet Genel : “Olay Yeri”, Çevrimiçi
Müdürlüğü <https://www.egm.gov.tr/kriminal/olayyeri-sorular>
17.07.2020.

- Eraslan Türkmen, : **Özel Nitelikli Kişisel Verilerin İşlenmesinde Açık Rızanın Aranmadığı Haller**, İstanbul, On İki Levha Yayıncılık, 2019.
- Erbaş, Rahime : “The Tension Between Genome Privacy and Criminal Justice in the wake of DNA Databases”, **CHKD**, c. 5, s. 2, 2017, ss. 163-178.
- Erman, R. Barış, : **“Çarşı ve Mahalle Bekçileri Kanunu Teklifi” Hakkında Özman, Onur, Yetkin, Tespit, Düşünce ve Eleştiriler**, İstanbul, Yeditepe Erdi, Börekçi, Eşref Üniversitesi Yayınevi, 2020.
- Barış, Üzeltürk, Saba Ş.T.
- Erman, R. Barış : “Adli Yargı Sisteminde DNA Örnekleri ve Profilleri– S. ve Marper v. Birleşik Krallık Davası”, **Fasikül Hukuk Dergisi**, c. 2, s. 11, 2010, ss. 20-23.
- Er, Cüneyd : **Biyometrik Yöntemler ve Özel Yaşamın Gizliliği Hakkı**, Ankara, Yetkin Yayıncılık, 2007.
- European Commission : “Access Rights and Data Protection”, Çevrimiçi <https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system/access-rights-and-data-protection> 06.02.2020.
- European Commission : “Visa Information System”, Çevrimiçi https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/visa-information-system_en 06.02.2020.

- Europol : “Crime Areas and Trends”, Çevrimiçi <https://www.europol.europa.eu/crime-areas-and-trends/crime-areas> 06.02.2020.
- Galli, Francesca : “The Interception of Communication in France and Italy – What Relevance For The Development of English Law?”, **The International Journal of Human Rights**, c. 20, s. 5, UK, 2016, ss. 666-683.
- Garvie, Clare : “Garbage In, Garbage Out. Face Recognition on Flawed Data”, Çevrimiçi <https://www.flawedfacedata.com/> 30.09.2019.
- Goldstein, Joseph, : “She Was Arrested at 14 Then Her Photo Went to a Facial
Watkins, Ali Recognition Database”, Çevrimiçi <https://www.nytimes.com/2019/08/01/nyregion/nypd-facial-recognition-children-teenagers.html> 30.09.2019.
- Göçmen Uyarer, : **Kişisel Verilerin Korunması Kanunu ve Türk Ceza
Sinem Kanunu Kapsamında Kişisel Verilerin Korunması**, İstanbul, Seçkin Yayıncılık, 2019.
- Göçmen, İlke : **Avrupa Birliği Hukukunda Direktiflerin Bireyler
Arasındaki İlişkilere Etkileri**, Ankara, Yetkin Yayınları, 2008.
- Gözler, Kemal, : “İdari Eylemlerden Kaynaklanan Zararlara İlişkin Davalar
Kaplan, Gürsel Adli Yargının Görev Alanına Sokulabilir Mi? (HMK m.3 ve TBK, m.55/2 Hakkında Eleştiriler)”, Çevrimiçi <http://www.idare.gen.tr/gozler-kaplan-hmk-m3.htm> 01.02.2020.

- Gözler, Kemal : **İdare Hukuku**, c. 2, Güncellenmiş 3. Baskı, Bursa, Ekin Yayınevi, 2019.
- Gözübüyük, A. Şeref, Gölcüklü, Feyyaz : **Avrupa İnsan Hakları Sözleşmesi ve Uygulaması**, 11. Bası, Ankara, Turhan Kitabevi, 2016.
- Gültekin Varkonyi, Gizem : “Yolcu İsim Kayıtlarının Terörle Mücadele Kapsamında Yurt Dışına Yasal Aktarımı: Avrupa Birliği Uygulamaları ve Türkiye”, **TBB Dergisi**, c. 30, s. 132, 2017, ss. 339-382.
- Günday, Metin : **İdare Hukuku**, Güncellenmiş ve Gözden Geçirilmiş 10. Baskı, Ankara, İmaj Yayınevi, 2015.
- Güneş, Ahmet M. : **Avrupa Birliği Hukukuna Giriş**, 2. Baskı, İstanbul, On İki Levha Yayıncılık, 2016.
- Gür, İkbâl : **Kişisel Verilerin Korunması Hususunda AB ile ABD Arasında Çıkan Uyuşmazlıklar ve Çözüm Yolları**, Ankara, Turhan Kitabevi, 2010.
- Hakeri, Hakan, Gülşen, Recep : “Offendicula ve Yeni Ceza Kanunu”, **AÜEHFD**, c. 9, s. 1-2, 2005, ss. 41-71.
- Hakeri, Hakan : **Ceza Hukuku Genel Hükümler**, 22. Baskı, Ankara, Adalet Yayınevi, 2019.
- Haliloğlu, Naciye Betül : “Yargılamaya ve Mahkûmiyete İlişkin Verilerin Genel Bilgi Toplama (GBT) Sisteminde Tutulması: Anayasa Mahkemesinin Bülent Kaya ve E.Ç.A. Kararlarının Avrupa

İnsan Hakları Mahkemesi İçtihatları Işığında Değerlendirilmesi”, **Anayasa Yargısı**, c. 36, s. 2, 2019, ss. 349-400.

Hamann, Kristine, : “Facial Recognition Technology: Where Will It Take Us?”,
Smith, Rachel **American Bar Association**, Çevrimiçi
https://www.americanbar.org/groups/criminal_justice/publications/criminal-justice-magazine/2019/spring/facial-recognition-technology/ 30.09.2019.

Interpol : Çevrimiçi <https://www.interpol.int/How-we-work/Forensics/Facial-Recognition> 30.09.2019.

Işık, Göksu : “Elektronik İzleme”, **Terazi Hukuk Dergisi**, c. 13, s. 142, 2018, ss. 32-44.

İstanbul Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü : Avrupa Parlamentosu ve Konseyi’nin 2016/680 Sayılı ve 27 Nisan 2016 Tarihli Kişisel Verilerin Yetkili Otoritelerce Suçların Önlenmesi, Soruşturulması, Ortaya Çıkarılması veya Kovuşturulması ve Cezaların İnfazı Amacıyla İşlenmesiyle İlgili Gerçek Kişilerin Korunmasına ve Bu Verilerin Serbest Dolaşımına İlişkin ve 2008/977/JHA Sayılı Konsey Çerçeve Kararı’nı Yürürlükten Kaldıran Direktif Hakkında Bilgi Notu, Çevrimiçi <https://www.mbkaya.com/hukuk/law-enforcement-directive-bilgi-notu.pdf> 12.12.2019.

Jasserand-Breeman, Catherine : “Reprocessing of Biometric Data for Law Enforcement Purposes: Individuals’ Safeguards Caught at the Interface Between the GDPR and the Police Directive?”, **University of**

Groningen, Yayınlanmamış Doktora Tezi, Groningen, 2019.

Jasserand, Catherine : “Subsequent Use of GDPR Data For A Law Enforcement Purpose: The Forgotten Principle of Purpose Limitation”, **University of Groningen Faculty of Law Research Paper Series No.26/2018**, EDPL c. 4, s. 2, 2018.

Kangal, Zeynel T. : **Kişisel Verilerin Ceza ve Kabahatler Hukukunda Korunması**, İstanbul, On İki Levha Yayıncılık, 2019.

Karabulut, Ramazan : “Kişisel Verilerin Korunması ve Kolluk Hizmetleri”, **Dicle Üniversitesi Sosyal Bilimler Enstitüsü**, Yayınlanmamış Yüksek Lisans Tezi, Diyarbakır, 2014.

Karakehya, Hakan : “Gözetim ve Suçla Mücadele”, **AÜHFD**, c. 58, s. 2, Ankara, 2009, ss. 319-357.

Kartal, Adem : “Teknik Araçlarla İzleme ve Elde Edilen Delillerin Değerlendirilmesi”, **Terazi Hukuk Dergisi**, c. 9, s. 98, 2014, ss. 14-24.

Kaya, Cemil : **Assessing the Transfer of Personal Data in the European Union in the Light of the Data Protection Directive**, İstanbul, On İki Levha Yayıncılık, 2011.

Kaya, Cemil : “Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi”, **İÜHFM**, c. 69, s. 1-2, 2011, ss. 317-334.

- Keser Berber, Leyla, : **Bilişimde Biyometrik Yöntemler**, Ankara, Yetkin
Lostar, Murat Yayınları, 2006.
- Keser Berber, Leyla : **Adli Bilişim (Computer Forensic)**, Ankara, Yetkin
Yayınları, 2004.
- Keskin, Serap : “Avrupa Konseyi Siber Suçlar Sözleşmesinde Ceza
Muhakemesine İlişkin Hükümlerin Değerlendirilmesi”,
İÜHFM, c. 59, s. 1-2, 2001, ss. 155-180.
- Ketizmen, Muammer : **Türk Ceza Hukukunda Bilişim Suçları**, Ankara, Adalet
Yayınevi, 2008.
- Kılınç, Doğan: “Anayasal Bir Hak Olarak Kişisel Verilerin Korunması”,
AÜHFD, c. 61, s. 3, 2012, ss. 1089-1169.
- Kızılırmak, Baran : “Kişisel Verilerin İşlenmesinde Adli ve Önleyici Amaçla
Öngörülen İstisnaların Ulusal ve Uluslararası Hukuka Göre
Değerlendirilmesi”, **Kadir Has Üniversitesi Hukuk
Fakültesi Dergisi**, c. 7, s. 2, 2019, ss. 225-261.
- Kızılırmak, Baran : “Önleyici Amaçla Elde Edilen Verilerin Ceza
Muhakemesinde Kullanılabilirliği”, **İstanbul Üniversitesi
Sosyal Bilimler Enstitüsü**, Yayınlanmamış Yüksek Lisans
Tezi, İstanbul, 2018.
- Kilkely, Ursula : “Özel Yaşama ve Aile Yaşamına Saygı Gösterilmesi
Hakkı”, **İnsan Hakları El Kitapları No.1**, Almanya, Avrupa
Konseyi, 2001.

Kişisel Verileri : **Kişisel Verilerin Korunması Kanununa İlişkin**
Koruma Kurumu **Uygulama Rehberi**, Ankara, KVKK Yayınları, 2018,
Çevrimiçi <https://www.kvkk.gov.tr/Icerik/4197/Kisisel-Verilerin-Korunmasi-Kanununa-Iliskin-Uygulama-Rehberi>
16.03.2020.

Kişisel Verileri : “Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri
Koruma Kurumu Sorumlularınca Alınması Gereken Yeterli Önlemler ile ilgili
Kişisel Verileri Koruma Kurulunun 31/01/2018 Tarihli ve
2018/10 Sayılı Kararı”, Çevrimiçi
<https://www.kvkk.gov.tr/Icerik/4110/2018-10> 16.02.2020.

Koçer, Seçkin : “Avrupa Genel Veri Koruma Tüzüğü Işığında Kişisel
Verilerin Korunması Kanununda Verisi İşlenen Kişinin
Hakları”, **Türk Yargısının Adli ve İdari Kapasitesinin
Güçlendirilmesi Projesi Kapsamında Hakim ve
Cumhuriyet Savcılarınca Hazırlanan Yüksek Lisans
Tezleri**, Ed. Zeliha İnce, Adalet Bakanlığı Avrupa Birliği
Genel Müdürlüğü, Ankara, 2018.

Koç, Ziya : “Elektronik İzleme ile Hapis Cezasının Konutta
Çektirilmesi”, **Ankara Barosu Dergisi**, s. 2, Ankara, 2013,
ss. 173-220.

Kokott, Juliane, : “The Distinction Between Privacy and Data Protection in
Sobotta, Christoph the Jurisprudence of the CJEU and the ECtHR”,
International Data Privacy Law, c. 3, s. 4, 2013, ss. 222-
228.

Korkmaz, İbrahim : **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**,
Güncellenmiş 2. Baskı, Ankara, Seçkin Yayıncılık, 2019.

- Köktaş, Arif : “Özgürlük, Güvenlik ve Adalet Alanı”, **Avrupa Birliği**, Ed. Belgin Akçay, İlke Göçmen, Gözden Geçirilmiş ve Güncellenmiş 3. Baskı, Ankara, Seçkin Yayıncılık, 2016.
- Kuloğlu, Gökhan : **İç Güvenlik İstihbaratı ve Kolluk**, İstanbul, Beta Yayınevi, 2015.
- Küçük, Tevfik : “Kişisel Verilerin Korunması Hakkı Çerçevesinde Kamuya Açık Alanların Kamu Tüzel Kişileri Tarafından Video Kamera Aracılığı İle Önleyici Amaçla İzlenmesi”, **YÜHFD**, c. 15, s. 1, 2018, ss. 49-87.
- Küzeci, Elif : **Kişisel Verilerin Korunması**, 4. Baskı, İstanbul, On İki Levha Yayıncılık, 2020.
- Latonero, Mark : “Big Data Analytics and Human Rights”, **Technology and Human Rights Enforcement**, Ed. Molly K. Land, Jay D. Aronson, Pennsylvania, Cambridge University Press, 2018.
- Leiser, Mark : “Directive 2016/680 Personal Data in Law Enforcement”, **Introduction of The Data Protection Reform to The Judicial System Inform**, Çevrimiçi <https://www.universiteitleiden.nl/binaries/content/assets/rec htsgelerdheid/instituut-voor-metajuridica/inform-project/leiser-inform-workshop.pdf> 13.03.2020.
- Lindroos-Hovinheimo, Susanna : “Who Controls Our Data? The Legal Reasoning of the European Court of Justice in *Wirtschaftsakademie Schleswig-Holstein* and *Tietosuojaalvautettu v Jehovan*

Todistajat”, **Information and Communications Technology Law**, c. 28, s. 2, 2019, ss. 225-238.

Lyon, David : **Günlük Yaşamı Kontrol Etmek, Gözetlenen Toplum**, Çev: Gözde Soykan, İstanbul, Kalkedon Yayınları, 2006.

Maden, Mehmet : “Anayasa Mahkemesine Bireysel Başvuru Bakımından Adil Yargılanma Hakkı Çerçevesinde Delil Yasakları”, **Anayasa Yargısı**, s. 32, 2016, ss. 207-234.

Madsen, Wayne : **Handbook of Personal Data Protection**, UK, Macmillan Publishers, 1992.

Mahmutoğlu, Fatih : “Ceza ve Ceza Yargılama Hukukunda Özel Yaşam”, **Özel Yaşamın Gizliliği Paneli**, Ankara, TBB Yayınları, 2009, ss. 100-110.

Marquenie, Thomas : “The Police and Criminal Justice Authorities Directive: Data Protection Standards and Impact on the Legal Framework”, **Computer Law and Security Review**, c. 33, 2017, ss. 324-340.

Meran, Necati : **Ceza ve Hukuk Davalarında Yasak Delil İletişimin Denetlenmesi Gizli Soruşturmacı ve Teknik Takibin Hukuki Boyutu**, 3. Baskı, Ankara, Adalet Yayınevi, 2015.

Mutlu, Muhammet : **Kişisel Verilerin Soruşturma Evresinde İşlenmesi ve İnsan Hakları Kapsamında Korunması**, Ankara, Adalet Yayınevi, 2020.

- Okay Tekinsoy, Özge : “Kolluk”, **İdare Hukuku**, Ed. Turan Yıldırım, Güncelleştirilmiş 7. Baskı, İstanbul, On İki Levha Yayıncılık, 2018, ss. 469-531.
- Orlandi, Renzo : “Telekomünikasyon Yoluyla İletişimin Önleme ve Adli Amaçlı Denetlenmesi-Özel Yaşamın Gizli Alanı, Teknik Araçla İzleme, Online Arama ve Kendi Kişisel Bilgileri Üzerinde Karar Verebilme Hakkı”, Çev. Ali Kemal Yıldız, **Dünyada ve Türkiye’de Ceza Hukuku Reformları Kongresi**, c. 1, Ed. Adem Sözüer, İstanbul, On İki Levha Yayıncılık, 2013, ss. 140-148.
- Orta, Mesut : “UYAP Sistemi ve Temel Özellikleri”, **Bilişim Hukuku**, Ed. Mete Tevetoğlu, İstanbul, Kadir Has Üniversitesi Yayınları, 2006, ss. 147-151.
- Önok, Murat : “Kişisel Verilerin Korunması Bağlamında ‘Unutulma Hakkı’ ve Türkiye Açısından Değerlendirmeler”, **İKÜHFD**, c. 16, s. 1, 2017, ss. 155-188.
- Özay, İl Han : **Günışığında Yönetim**, 3. Baskı, İstanbul, Filiz Kitabevi, 2017.
- Özbek, Veli Özer, Doğan, Koray, Bacaksız, Pınar : **Ceza Muhakemesi Hukuku**, 12. Baskı, Ankara, Seçkin Yayıncılık, 2019.
- Özbek, Veli Özer : “Elektronik Ortamda Saklı Bulunan Verilerin Ceza Muhakemesinde Delil Niteliği ve Değerlendirilmesi”, **İÜHFM**, c. 59, s. 1-2, 2001, ss. 181-202.

- Özbek, Veli Özer : **İnfaz Hukuku**, Geliştirilmiş ve Güncellenmiş 11. Baskı, Ankara, Seçkin Yayıncılık, 2019.
- Özbek, Veli Özer : “Tıp Ceza Hukukunda DNA İncelemesi”, **V. Türk-Alman Tıp Hukuku Sempozyumu**, Ankara, TBB Yayını, 2008, ss.1076-1133.
- Özen, Muharrem, Özocak, Gürkan : “Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK M. 134)”, **Ankara Barosu Dergisi**, 2015/1, ss. 43-77.
- Özkan, Halid : “Mobese İzleme ve Kayıtlarının Ceza Muhakemesi Hukuku Açısından Değerlendirilmesi”, **CHD**, c. 11, s. 30, 2016, ss. 63-103.
- Özkan, Işıl : **Avrupa Birliği Kamu Hukuku**, Ankara, Seçkin Yayıncılık, 2011.
- Öztürk, Bahri, Altınok Çalışkan, Elif : “Kişisel Verilerin Korunması Kanunu Hakkında Genel Değerlendirmeler ve Anayasaya Aykırılık Sorunu”, **Fasikül Hukuk Dergisi**, c. 10, s. 100, 2018, ss. 277-336.
- Öztürk, Bahri, Eker Kazancı, Behiye, Soyer Güleç, Sesim : **Ceza Muhakemesi Hukukunda Koruma Tedbirleri**, 3. Baskı, Ankara, Seçkin Yayıncılık, 2019.
- Öztürk, Bahri : “Sporda Şiddet ve Düzensizliğin Önlenmesine Çare Olarak Seyirden Yasaklanma”, **Sporda Şiddet ve Düzensizliğin Önlenmesi Kanunu**, Ed. Cumhur Şahin, İzzet Özgenç, İlhan Üzülmöz, Ankara, Seçkin Yayıncılık, 2012, ss. 33-46.

- Pajunoja, Lauri J. : “The Data Protection Directive on Police Matters 2016/680 Protects Privacy-The Evolution Of EU’s Data Protection Law and Its Compatibility With The Right To Privacy”, **University of Helsinki**, Yayınlanmamış Yüksek Lisans Tezi, Helsinki, 2017.
- Paşaoğlu, Cengiz, : “A Review On Privacy Preserving Biometric Authentication
Adje, Kayode Methods”, **Kişisel Verileri Koruma Dergisi**, c. 1, s. 1, 2019,
Hadilou, Demirtaş, ss. 34-46.
Orkun
- Pekel Uludağlı, Nilay : “Hükümlülerin Denetiminde ve Topluma
Kazandırılmasında Yeni Bir Yöntem Olarak Elektronik
İzleme”, **AÜHFD**, c. 61, s. 4, Ankara, 2012, ss. 1337-1368.
- Pfisterer, Valentin M. : “The Right to Privacy- A Fundamental Right in Search of
Its Identity: Uncovering the CJEU’s Flawed Concept of The
Right to Privacy”, **German Law Journal**, s. 20, 2019, ss.
722-733.
- Plagemann, Gottfried : “Alman Hukuku’nda Gizli Soruşturmacının Kullanılması ve
Gizli Soruşturmacının Yetkileri”, **CHKD**, c. 2, s.1-2, 2014,
ss. 157-187.
- Purtova, Nadezhda : “The Law of Everything. Broad Concept of Personal Data
and Future of EU Data Protection Law”, **Law, Innovation
and Technology**, c. 10, s. 1, 2018, ss. 40-81.
- Ryngaert, Cedric, : “The GDPR As Global Data Protection Regulation?”,
Taylor, Mistale **American Journal Of International Law**, s. 114, 2020, ss.
5-9.

Sajfert, Juraj, Quintel, Teresa : “Data Protection Directive (EU) 2016/680 For Police and Criminal Justice Authorities”, **Cole/Boehm GDPR Commentary**, Edward Elgar Publishing, 2019, Çevrimiçi https://papers.ssrn.com/sol3/papers.cfm?abstract_id=328587 3 04.03.2020.

Semiz, Hasan : “Uluslararası Terör Suçları Bakımından Terör Suçlarında Kolluk Yetkileri”, **Harp Akademisi Komutanlığı Stratejik Araştırmalar Enstitüsü**, Yayımlanmamış Yüksek Lisans Tezi, İstanbul, 2007.

Sert, Şeyma : **Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması**, İstanbul, Seçkin Yayıncılık, 2019.

Skendzic, Aleksandar, Kovacic, Bozidar, Tijan, Edvard : “General Data Protection Regulation- Protection Of Personal Data In An Organisation”, **41st International Convention on Information and Communication Technology, Electronics and Microelectronics**, Opatija, 2018, ss. 1370-1375.

Sondergaard, Peter : “Big Data Fades to the Algorithm Economy”, Çevrimiçi <https://www.forbes.com/sites/gartnergroup/2015/08/14/big-data-fades-to-the-algorithm-economy/#69161c9851a3> 22.10.2019.

Soysal, Tamer : “Unutulma Hakkının Avrupa Birliği’nin Genel Veri Koruma Tüzüğü Çerçevesinde İncelenmesi”, **Uyuşmazlık Mahkemesi Dergisi**, Yıl 7, s. 13, Haziran 2019, ss. 339-422.

- Sözüer, Adem : “Organize Suçlulukla İlgili Kovuşturma Yöntemleri (İletişimin Dinlenmesi)”, **Legal Hukuk Dergisi**, c. 1/B, s. 10, İstanbul, 2003, ss. 2495-2512.
- Sözüer, Adem : “Türkiye’de Karşılaştırmalı Hukukta Telefon, Teleks, Faks ve Benzeri Araçlarla Yapılan Özel Haberleşmenin Bir Ceza Yargılaması Önlemi Olarak Denetlenmesi”, **İÜHFM**, İstanbul, c. 55, s. 3, 1997, ss. 65-110.
- Sözüer, Eren : **Unutulma Hakkı İnsan Hakları Hukuku Perspektifinden Bir İnceleme**, İstanbul, On İki Levha Yayıncılık, 2017.
- Springwise : “Chinese Police Adopt Smart Glass Technology”, Springwise, 14.02.2018, Çevrimiçi <https://www.springwise.com/chinese-police-adopt-smart-glass-technology/#:~:text=Using%20facial%20recognition%20technology%2C%20these,technology%20to%20assist%20police%20work.22.09.2020>.
- Sputnik News : “İstanbul Cumhuriyet Başsavcılığı’ndan 'Emniyet Kürtaj Listesi İstedi' Başlıklı Haberlere Dair Açıklama”, Sputnik News Türkiye, 10.09.2019, Çevrimiçi <https://tr.sputniknews.com/turkiye/201909101040137404-istanbul-cumhuriyet-bassavciligindan-emniyet-kurtaj-listesi-istedi-baslikli-haberlere-dair-aciklama/> 16.03.2020.
- Sputnik News : “Akdağ: Kanalizasyon Suyunda Uyuşturucu Takibi Yapacağız”, Çevrimiçi <https://tr.sputniknews.com/turkiye/201803201032712064->

akdag-kanalizasyon-suyunda-uyusturucu-takibi-yapacagiz/
11.03.2020.

Şahin, Uğur : “Emniyet Kürtaj Listesini İstedi!”, Birgün Gazetesi,
09.09.2019, Çevrimiçi
<https://www.birgun.net/haber/emniyet-kurtaj-listesini-istedi-267844> 16.03.2020.

Şen, Ersan : **Türk Hukukunda Telefon Dinleme, Gizli Soruşturmacı, X Muhbir**, 5. Baskı, Ankara, Seçkin Yayıncılık, 2011.

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

Tahmazoğlu Üzeltürk, Sultan : “Özel Hayatın Korunmasına İlişkin Başlıca Sorunlar”, **GSÜHFD**, c. 7, s. 1, İstanbul, 2008, s. 95-129.

Tanör, Bülent : **Türkiye’nin İnsan Hakları Sorunu**, 3. Baskı, İstanbul, BDS Yayınları, 1994.

Temizsoy Bayram, Nihal : “Ceza Muhakemesi Hukukunda Moleküler Genetik İnceleme ve Elde Edilen Verilerin Delil Olarak Kullanılması”, **İstanbul Üniversitesi Sosyal Bilimler Enstitüsü**, Yayımlanmamış Yüksek Lisans Tezi, İstanbul, 2018.

Tetik, Erdoğan : “Kimlik Tespitinde Parmak İzi Arşivlerinin Gerekliliği ve Ülkemizdeki Durumun Değerlendirilmesi”, **Polis Dergisi**, s. 41, 2004.

- Tezcan, Durmuş, : **Teorik ve Pratik Ceza Özel Hukuku**, Güncellenmiş 17. Baskı, Ankara, Seçkin Yayıncılık, 2019.
- Erdem, Mustafa
- Ruhan, Önok, R. Murat
- Tezcan, Durmuş : “Özel Hayat Açısından Kişisel Verilerin Korunması”, **İKÜHFD**, c. 16, s. 1, 2017, ss. 17-25.
- The Metropolitan Police : Çevrimiçi <https://www.met.police.uk/live-facial-recognition-trial/> 30.09.2019.
- Thomas, Terry : **The Registration and Monitoring of Sex Offenders: A Comparative Study**, London, Routledge, 2011.
- Topçu, Namık Kemal : **İngiliz Ceza Muhakemesi Hukukunda Soruşturma Evresi**, Ankara, Adalet Yayınevi, 2018.
- Turan, Metin : **Bilişim Hukuku**, Güncellenmiş 3. Baskı, İstanbul, Seçkin Yayıncılık, 2019.
- Turhan, Faruk : “Ceza Muhakemesinde Beden Muayenesi ve Tıp Hukuku (Özellikle AİHM Kararları Işığında Şüpheli veya Sanığın Zorla Muayenesi Konusunun Değerlendirilmesi)”, **V. Türk-Alman Tıp Hukuku Sempozyumu**, Ankara, TBB Yayını, 2008, ss. 1025-1076.
- Tzanou, Maria : **The Fundamental Right to Data Protection**, Oregon, Hart Publishing, 2017.
- Ünver, Yener, Hakeri, Hakan : **Ceza Muhakemesi Hukuku**, c.1, 15. Baskı, Ankara, Adalet Yayınevi, 2019.

- Ünver, Yener : “Federal Almanya’da Terör ve Organize Suçluluk ile İlgili Düzenlemeler”, **Nurullah Kunter’e Armağan**, İstanbul, Beta Yayıncılık, 1998.
- Ünver, Yener : “Kişisel Verilerin Korunması”, **GSÜHFD**, c. 7, s. 1, İstanbul, 2008, ss. 163-196.
- van der Sloot, Bart : “Legal Consistency After the General Data Protection Regulation and the Police Directive”, **European Journal of Law and Technology**, c. 9, s. 3, 2018 ss. 1-18.
- Voigt, Paul : **The EU General Data Protection Regulation (GDPR) A Practical Guide**, Springer, 2017.
- von dem Bussche, Axel
- Walker, Darin R. : “Biometric Technology in Law Enforcement”, **Neurosurgery**, c. 71, s. 2, Ağustos 2012, ss. 197–200.
- Würtenberger, Thomas : “**Tehlike Kavramı**” ve **Alman Uygulaması Ekseninde Kolluk Hukuku**, Çev. Feridun Yenisey, Ankara, Asayiş Dairesi Başkanlığı, 2008.
- Yakovleva, Svetlana : “Should Fundamental Rights to Privacy and Data Protection Be A Part of the EU’s International Trade ‘Deals’?”, **World Trade Review**, c. 17, s. 3, 2018, ss. 477-508.
- Yaşar, Yusuf : “6222 Sayılı Sporda Şiddet ve Düzensizliğin Önlenmesine Dair Kanun’un 18’inci Maddesinde Yer Alan ‘Seyirden Yasaklanma’ ile ‘Seyirden Yasaklama’ Tedbirleri”, **MÜHF-HAD**, c. 19, s. 1, 2013, ss. 3-38.

- Yavuz, Can : **İnternetteki Arama Sonuçlarından Kişisel Verilerin Kaldırılması Unutulma Hakkı**, Ankara, Seçkin Yayıncılık, 2016.
- Yenisey, Feridun, Nuhoğlu, Ayşe : **Ceza Muhakemesi Hukuku**, 7. Baskı, İstanbul, Seçkin Yayıncılık, 2019.
- Yenisey, Feridun : “Aleni Alanların Video Kamera ile Denetlenmesi”, Çevrimiçi
http://www.caginpolicisi.com.tr/eski_sitemiz/120/8-9.htm
11.03.2020.
- Yenisey, Feridun : “Ön Alan Araştırmaları”, **Dünyada ve Türkiye’de Ceza Hukuku Reformları Kongresi**, c. 1, Ed. Adem Sözüer, İstanbul, On İki Levha Yayıncılık, 2013, ss. 91-98.
- Yenisey, Feridun : **Kolluk Hukuku**, 2. Baskı, İstanbul, Beta Yayıncılık, 2015.
- Yetim, Servet : “5651 Sayılı Yasa Kapsamında Tutulan İnternet Trafik Bilgilerinin Özel Yaşam ve Yaşamın Gizliliği Kapsamında Değerlendirilmesi”, **Terazi Hukuk Dergisi**, c. 4, s. 36, 2009, ss. 55-63.
- Yılmaz, Sabire Sanem : “Video Gözetimi, Yapay Zekâ ve Kişisel Verilerin Korunması Hakkı”, Çevrimiçi
<https://www.hukukihaber.net/video-gozetimi-yapay-zeka-ve-kisisel-verilerin-korunmasi-hakki-makale,7001.html>
10.11.2019.

- Yokuş Sevük, Handan : **Türk Ceza Hukuku Özel Hükümler**, Genişletilmiş ve Gözden Geçirilmiş 2. Baskı, Ankara, Adalet Yayınevi, 2019.
- Yokuş Sevük, Handan : “Postada El Koyma ve Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi”, **TBB Dergisi**, c. 20, s. 69, 2007, ss. 97-124.
- Yokuş Sevük, Handan : “Tıp Ceza Hukukunda Kişisel Verilerin Açıklanması”, **V. Türk-Alman Tıp Hukuku Sempozyumu**, Ankara, Türkiye Barolar Birliği Yayını, 2008.
- Yücedağ, Nafiye : “Kişisel Verilerin Korunması Kanunu Kapsamında Genel İlkeler”, **Kişisel Verileri Koruma Dergisi**, c. 1, s. 1, 2019, ss. 47-63.
- Yüksel, Saadet : **Özel Yaşamın Bir Parçası Olarak Telekomünikasyon Yoluyla Yapılan İletişimin Gizliliğine Önleyici Denetimle Müdahale**, İstanbul, Beta Yayıncılık, 2012.
- Y.Y. : **Exchange of Information and Data Protection in Cross-Border Criminal Proceedings in Europe**, Ed: Angeles Gutierrez Zarra, Berlin, Springer, 2015.
- Zöller, Mark A. : “Telekomünikasyon Verilerinin Depolanarak Kaydedilmesi (Alman) Uygulaması ve Yanlış Uygulaması”, Çev. Hakan Karakehya, **Dünyada ve Türkiye’de Ceza Hukuku Reformları Kongresi**, c. 1, Ed. Adem Sözüer, İstanbul, On İki Levha Yayıncılık, 2013, ss. 165-178.

DiĞER KAYNAKLAR

Çevrimiçi <https://www.ab.gov.tr/files/pub/antlasmalar.pdf>
18.02.2020.

Çevrimiçi <https://www.anayasa.gov.tr/tr/kararlar-bilgi-bankasi/> 29.03.2020.

Çevrimiçi <https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=16641&lang%20=en>
04.03.2020.

Çevrimiçi https://curia.europa.eu/jcms/jcms/j_6/en/
29.03.2020.

Çevrimiçi <http://curia.europa.eu/juris/document/document.jsf?text=&docid=183140&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=491722> 23.03.2020.

Çevrimiçi <http://ekutup.dpt.gov.tr/ab/sozluk.pdf> 02.09.2019.

Çevrimiçi <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32006R1987&from=EN> 06.02.2020.

Çevrimiçi <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32007D0533&from=EN> 06.02.2020.

Çevrimiçi <https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:32006L0024> 08.02.2020.

Çevrimiçi <https://eur-lex.europa.eu/summary/glossary/europol.html> 14.02.2020.

Çevrimiçi <https://hudoc.echr.coe.int/> 27.03.2020.

Çevrimiçi <http://www.islem.com.tr/uploads/proje/JEMUS.pdf> 06.02.2020.

Çevrimiçi <http://www.kazanci.com/kho2/ibb/giris.html> 29.03.2020.

Çevrimiçi <https://www.memurlar.net/haber/140285/pol-net-te-keyfi-sorgulama.html> 05.02.2020.

Çevrimiçi <https://www.nsopw.gov/en/Search/Results> 23.03.2020.

Çevrimiçi <https://www.netherlandsworldwide.nl/living-working/applying-for-consular-declarations/certificate-of-conduct-vog> 13.03.2020.

Çevrimiçi <https://www.ombudsman.gov.tr/wp-content/uploads/2018/03/2017-9518-Ba%C5%9Fvuran%C4%B1n-GBT-kayd%C4%B1n%C4%B1n-silinmesi-talebi-hakk%C4%B1nda.pdf> 23.03.2020.

Çevrimiçi <https://pedomap.live/about> 20.07.2020.

Çevrimiçi

<https://pjpeu.coe.int/documents/41781569/42171329/CMRec+%282014%29+4+on+electronic+monitoring.pdf/c9756d5b-be0e-4c72-b085-745c9199bef4> 06.02.2020.

Çevrimiçi

http://www.sbb.gov.tr/wp-content/uploads/2018/11/Avrupa_Birligi_Temel_Haklar_Sarti%E2%80%8B.pdf 05.03.2020.

Çevrimiçi

<https://www.supremecourt.uk/cases/docs/uksc-2020-0022-judgment.pdf> 20.07.2020.

Çevrimiçi

http://www.ttb.org.tr/haberarsiv_goster.php?Guid=665acfee-9232-11e7-b66d-1540034f819c 13.03.2020.

Çevrimiçi

<https://uzay.tubitak.gov.tr/tr/urunlerimiz/balistika-0> 06.02.2020.

Çevrimiçi

<https://www.uyap.gov.tr/Tarihce> 05.02.2020.

Çevrimiçi

<https://www2.tbmm.gov.tr/d27/2/2-2555.pdf> 16.03.2020.