

T.C.
MARMARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI
KAMU HUKUKU BİLİM DALI

AVRUPA VERİ KORUMA HUKUKUNA ANAYASAL BİR BAKIŞ

Doktora Tezi

SEZEN KAMA IŞIK

İstanbul, 2019

T.C.
MARMARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI
KAMU HUKUKU BİLİM DALI

AVRUPA VERİ KORUMA HUKUKUNA ANAYASAL BİR BAKIŞ

Doktora Tezi

SEZEN KAMA IŞIK

Danışman: DR. ÖĞR. ÜYESİ OYA BOYAR

İstanbul, 2019

MARMARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜ

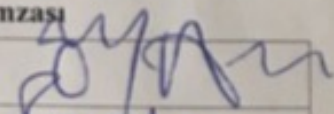
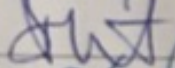
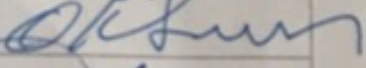
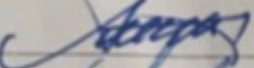
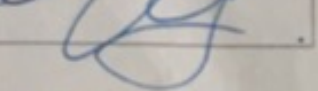
TEZ ONAY BELGESİ

KAMU HUKUKU Anabilim Dalı KAMU HUKUKU Bilim Dalı DOKTORA öğrencisi SEZEN KAMA IŞIK'nın AVRUPA VERİ KORUMA HUKUKUNA ANAYASAL BİR BAKIŞ adlı tez çalışması, Enstitümüz Yönetim Kurulunun 8.08.2019 tarih ve 2019-25/7 sayılı kararıyla oluşturulan jüri tarafından oy birliği / ~~oy çokluğu~~ ile Doktora Tezi olarak kabul edilmiştir.

Tez Savunma Tarihi 27, 09, 2019

Öğretim Üyesi Adı Soyadı

İmzası

1. Tez Danışmanı	Dr. Öğr. Üyesi OYA BOYAR	
2. Jüri Üyesi	Prof. Dr. BİHTERİN DİNÇKOL	
3. Jüri Üyesi	Prof. Dr. OKTAY UYGUN	
4. Jüri Üyesi	Doç. Dr. ABDULLAH SEZER	
5. Jüri Üyesi	Prof. Dr. CİHAN OSMANAĞAOĞLU	

ÖZET

Günümüzde petrolden de değerli görülen verinin hukuki düzenlemelerle korunması oldukça önemlidir. Dışarıdan gelebilecek saldırılara karşı kişinin en temelde mahremiyetini korumak ve varlığını özgürce gerçekleştirebilmesini sağlamak için bu koruma gerekmektedir. Ayrıca son yıllarda Cambridge Analytica gibi skandallar neticesinde görülmüştür ki, kişinin özgür seçim yapabilmesi ve insan onurunun korunması bakımından da verilerinin hukuka uygun olarak korunması ve işlenmesinin temel bir insan hakkı olarak kabul edilmesi ve korunması demokratik bir dünya düzeni için ve otoriterleşme eğilimi karşısında tek geçerli yoldur. Aynı zamanda küreselleşen dünyada verinin hukuka uygun biçimde dolaşımı da artık fazlasıyla önem taşımaktadır.

Avrupa ölçeğinde 1970'lerden beri veriyi korumak adına birçok hukuki düzenleme yapılmıştır. Bu hukuki düzenlemeler incelendiğinde görülmektedir ki, veri koruması ilk başlarda mahremiyet alanında özel yaşamın korunması biçiminde algılanmıştır. Bu koruma bünyesinde doğan kavram zamanla, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilginin korunması ve hukuka uygun işlenmesi anlamına gelerek “Kişisel Verilerin Korunması” biçiminde bağımsız bir temel hak görünümüne evrilmiş ve yeni bir alanın ortaya çıkmasına sebep olmuştur. Son yıllarda ise eskiye nazaran çok daha hızlı gelişen bilişim teknolojilerinin yarattığı tehlikelerden ve özellikle verinin büyük ölçekte işlenmesinin söz konusu olduğu big data, bulut bilişim, blockchain ve nesnelerin interneti gibi yeni sistemler bağlamında Avrupa düzleminde ortak bir koruma, Veri Koruma Reformu ile gerçekleştirilmeye çalışılmaktadır.

Avrupa kıtasında yaklaşık yarım asırlık bir geçmişe sahip olan söz konusu veri koruma hukuku düzenlemelerinin Türkiye'deki yansımasına bakıldığında, her ne kadar başka kanunlarda istisnai olarak bazı düzenlemelere rastlansa da bir Anayasa metninde temel bir hak olarak karşılık bulması yalnızca on yıl kadar geriye götürülebilmektedir. Konuya ilişkin özel bir kanunun kabulü ise ancak üç yıl önce, Avrupa Veri Koruma

Reformu öncesinde geçerli olan Direktif'in eksik biçimde esas alınması ile mümkün olabilmektedir.

İşte bu çalışmada, her geçen gün değişen ve gelişen veri koruma alanının maruz kaldığı tehlikelere karşı, Avrupa Veri Koruma Hukuku ışığında sunulan çözümler incelenecek ve Türkiye'deki anayasal ve konuyu doğrudan düzenleyen kanun ile birlikte gerçekleşen gelişmelerin Avrupa ölçeğinde sunulan çözümler ile uyumu karşılaştırılarak yeterli olup olmadıkları, yeterli değilse hangi değişikliklerin gerektiğine ilişkin tespitlere yer verilecektir.



ABSTRACT

It is important protecting data which is seen more valuable than oil today with legal regulations. This protection is necessary to preserve privacy of a person against attacks from outside and to ensure that a person can be free.

In Europe, there are many legal arrangements have been prepared and accepted to protect data since the 1970s. It can be seen that data protection was initially perceived as the protection of private life in the field of privacy by these legal regulations. This concept has evolved in time to protect personal data by means of protecting all kinds of information relating to a real person by an independent fundamental right. This is because a new field has emerged. In recent years, a common protection in Europe has been implemented through Data Protection Reform from dangers of information technologies that are developing much faster than before.

Data protection law regulations have a half-century history in the European continent. On the other hand, personal data protection has been regulated as a fundamental right in the Constitution of Turkey about ten years ago. The adoption of a specific law on the subject was only possible three years ago. This specific law is based on an incomplete implementation of the 95/46/EC Directive which was valid before the European Data Protection Reform.

Taking everything into account, this study has two main objectives. The first one is to examine the solutions presented in the light of the European Data Protection Law against the dangers of data protection area that is changing and developing day by day. The second one, more importantly, is to compare Turkish constitutional provision, case-law and Data Protection Law with the compliance with European solutions and to understand which changes are necessary for insufficient ones.

İÇİNDEKİLER

KISALTMALAR.....	viii
GİRİŞ.....	1

Birinci Bölüm

İNSAN HAKLARI GENEL KURAMI İŞİĞİNDA

KİŞİSEL VERİLERİN KORUNMASI HAKKI

I. KAVRAMSAL OLARAK İNSAN HAKLARI.....	6
II. TARİHSEL SÜREÇTE İNSAN HAKLARI.....	10
III. İNSAN HAKLARI VE İNSAN ONURU İLİŞKİSİ.....	18
IV. İNSAN HAKLARININ SINIFLANDIRILMASI.....	22
A. JELİNEK ÜÇLÜSÜ: POZİTİF/ NEGATİF/ AKTİF STATÜ HAKLARI	23
B. VASAK'IN HAK KUŞAKLARI.....	25
C. HABERMAS'IN SINIFLAMASI.....	29
V. BİR İNSAN HAKKI OLARAK KİŞİSEL VERİLERİN KORUNMASININ DOĞUŞU	30
A. DÖRDÜNCÜ KUŞAK HAKLAR VE BİLİŞİM TEKNOLOJİSİ	30
B. BİLİŞİM TEKNOLOJİSİ KARŞISINDA ÖZEL YAŞAMIN GİZLİLİĞİ VE KORUNMASI	33
C. KAVRAMIN ORTAYA ÇIKIŞ NOKTASI OLARAK: MAHREMİYET	36
D. MAHREMİYET VE AMERİKAN ANLAYIŞI	39
E. MAHREMİYET VE AVRUPA ANLAYIŞI.....	44
F. MAHREMİYETTEN KİŞİSEL VERİLERİN KORUNMASINA VERİ KORUMA HUKUKUNUN GELİŞİMİ.....	53
G. KİŞİSEL VERİLERİN KORUNMASI KAPSAMINDA BAZI TEMEL KAVRAMLAR	58

İkinci Bölüm

AVRUPA VERİ KORUMA HUKUKU

I. AVRUPA KONSEYİ.....	68

A. 108 SAYILI KİŞİSEL VERİLERİN OTOMATİK İŞLENMESİ SIRASINDA GERÇEK KİŞİLERİN KORUNMASINA İLİŞKİN SÖZLEŞME VE SÖZLEŞME 108+ REVİZYONU	72
B. İNSAN HAKLARI AVRUPA SÖZLEŞMESİ	78
1. İHAM Kararları Bağlamında Mahremiyet Kavramı ve Özel Yaşamın Gizliliği ve Korunması Hakkı.....	79
2. Özel Yaşamın Korunması Hakkı Bağlamında Kişisel Verilerin Korunması..	84
3. Özel Yaşamın Korunması Hakkı Bağlamında Sağlık Verilerinin Korunması	99
II. AVRUPA BİRLİĞİ	103
A. AB TEMEL HAKLAR ŞARTI.....	104
1. Kapsam ve İçerik	105
2. İlgili İçtihat.....	107
B. 95/ 46/ AT SAYILI KİŞİSEL VERİLERİN İŞLENMESİ VE SERBEST DOLAŞIMI BAKIMINDAN BİREYLERİN KORUNMASINA İLİŞKİN AVRUPA PARLAMENTOSU VE AVRUPA KONSEYİ DİREKTİFİ	112
1. Kapsam ve İçerik	115
2. İlgili İçtihat.....	124
C. VERİ KORUMA REFORMUNA GÖTÜREN DİĞER DÜZENLEMELER ..	134
1. 97/66/AT Sayılı Telekomünikasyon Sektöründe Kişisel Verilerin İşlenmesi ve Özel Yaşamın Korunması Direktifi.....	134
3. Avrupa Topluluğu (Amsterdam) Antlaşmasının 286. Maddesi	135
4. 2002/58/AT Sayılı Elektronik İletişimde Kişisel Verilerin İşlenmesi ve Özel Yaşamın Korunması Direktifi	136
5. 45/2001/AT Sayılı Topluluk Kurum ve Organları tarafından Kişisel Verilerin İşlenmesi ve Verilerin Serbest Dolaşımı bakımından Bireylerin Korunması Direktifi.....	137
6. 2006/24/AT Sayılı İletişim Trafik Verilerinin Saklanması Direktifi (Kamu İletişim Ağları veya Kamuya Açık İletişim Servislerinde Üretilen veya İşlenen Verilerin Saklanması Direktifi).....	139
7. Lizbon Anlaşması	140
D. VERİ KORUMA REFORMU	142
1. Genel Veri Koruma Tüzüğü'nün Getirdikleri	145
a) Uygulama Alanı.....	146
b) Kişisel Veri ve Özel Nitelikli Kişisel Veri.....	149
c) Kişisel Verilerin İşlenme Şartları	151
d) Üçüncü Ülkelere Kişisel Veri Aktarımı.....	153

e) Veri Öznesinin Hakları	156
f) Veri Denetleyicisi ve Veri İşleyicisi	159
g) Önleyici Veri Koruma- Denetim ve Yaptırım Sistemi	162
h) Yeni Teknolojiler Bağlamında Veri İşleme	171
2. 95/46/AT Sayılı Direktif ve Genel Veri Koruma Tüzüğü'nün Karşılaştırılması	179
E. VERİ KORUMA REFORMU ÖNCESİ GELİŞMELER İLE REFORMUN ULUSAL HUKUK DÜZENLERİNE ETKİSİ	184

Üçüncü Bölüm

AVRUPA VERİ KORUMA HUKUKUNUN

TÜRK HUKUK SİSTEMİNE ETKİSİ

I. ANAYASAL HÜKÜMLER VE KANUNİ DÜZENLEME	198
A. ANAYASAL DÜZENLEMELER	198
1. Kişisel Verilerin Korunması Hakkı (AY md. 20/3).....	198
2. İlgili Diğer Haklar.....	205
a) İnsan Onuru ve Kişiliğin Serbest Geliştirilmesi Hakkı (Başlangıç ve AY md. 17)	207
b) Özel Yaşamın Gizliliği (AY md. 20).....	212
c) Konut Dokunulmazlığı (AY md. 21).....	213
d) Haberleşme Hürriyeti (AY md. 22)	214
e) Din ve Vicdan Hürriyeti (AY md. 24).....	215
f) Düşünce Hürriyeti (AY md. 25- AY md. 26).....	215
g) Toplantı ve Gösteri Yürüyüşü Düzenleme Hakkı (AY md. 34).....	216
h) Bilgi Edinme Hakkı (AY md. 74).....	217
B. KANUNİ DÜZENLEME	218
1. Uygulama Alanı.....	221
a) Konu Açısından	221
b) Kişi Açısından	225
c) Yer Açısından	229
d) İstisnalar	230
2. Temel İlkeler	239

3. Kişisel Verilerin İşlenme Şartları	245
4. Kişisel Verilerin Aktarımı.....	255
a) Yurt İçinde Üçüncü Kişilere Aktarılması.....	255
b) Yurtdışına Aktarılması	256
5. Veri Öznesinin Hakları (KVKK md. 3- İlgili Kişi).....	259
6. Veri Sorumlusunun Yükümlülükleri	266
7. Denetim ve Yaptırım Sistemi.....	271
a) Bir Denetim Organı Olarak Kişisel Verilerin Korunması Kurulu.....	272
b) Yaptırım Sistemi	282
II. İLGİLİ ANAYASAL İÇTİHAT	287
A. KANUNİLİK VE ÖZELLİKLE VERİ İŞLEMENİN KANUNİLİĞİ	288
B. DEMOKRATİK TOPLUM DÜZENİNDE GEREKLİLİK	301
1. Hakkın Özüne Dokunma Yasağı	304
2. Ölçülülük.....	320
III. AVRUPA VERİ KORUMA HUKUKUNUN ULUSAL HUKUKA	
ETKİLERİNİN DEĞERLENDİRİLMESİ	344
SONUÇ	350
KAYNAKÇA	357

KISALTMALAR

108 Sayılı Sözleşme	Kişisel Verilerin Otomatik İşlenmesi Sirasında Gerçek Kişilerin Korunmasına İlişkin Sözleşme
2006/24/AT Sayılı Direktif	Trafik Verilerinin Saklanması Direktifi (Kamu İletişim Ağları veya Kamuya Açık İletişim Servislerinde Üretilen veya İşlenen Verilerin Saklanması Direktifi)
45/2001 Sayılı Direktif	Topluluk Kurum ve Organları tarafından Kişisel Verilerin İşlenmesi ve Verilerin Serbest Dolaşımı bakımından Bireylerin Korunması Direktifi
95/46/AT Sayılı Direktif	Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi
97/66/AT Sayılı Direktifi	Telekomünikasyon Sektöründe Kişisel Verilerin İşlenmesi ve Özel Yaşamın Korunması Direktifi
AB	Avrupa Birliği
ABA	Avrupa Birliği Antlaşması
ABİA	Avrupa Birliği'nin İşleyişine İlişkin Antlaşma
AK	Avrupa Konseyi
AÜEHFD	Atatürk Üniversitesi Erzincan Hukuk Fakültesi Dergisi
AÜHFD	Ankara Üniversitesi Hukuk Fakültesi Dergisi
AÜSBFD	Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi
AY	Anayasa
AYM	Anayasa Mahkemesi
AYMK	Anayasa Mahkemesi Kararı

B.	Bölüm
Bkz.	Bakınız
C.	Cilt
Çev.	Çeviren
Der.	Derleyen
Diğ.	Diğerleri
E.	Esas sayısı
Ed.	Editör
E.T.	Erişim Tarihi
GVKT	2016/679 Sayılı Genel Veri Koruma Tüzüğü
Haz.	Hazırlayan
İHAM	Avrupa İnsan Hakları Mahkemesi
İHAS	Avrupa İnsan Hakları Sözleşmesi
İHEB	İnsan Hakları Evrensel Beyannamesi
İÜHFM	İstanbul Üniversitesi Hukuk Fakültesi Mecmuası
K.	Karar sayısı
K.T.	Karar tarihi
KVKK	6698 Sayılı Kişisel Verilerin Korunması Kanunu
Md.	Madde
No.	Numara

OECD	Organisation for Economic Co-operation and Development (Ekonomik İşbirliği ve Kalkınma Teşkilatı)
OECD Rehber İlkeleri	Özel Yaşamın Gizliliğinin ve Sınır Ötesi Kişisel Veri Dolaşımının Korunmasına İlişkin OECD Rehber İlkeleri
OJ.	Official Journal of the European Communities (Avrupa Toplulukları Resmi Gazetesi)
Par.	Paragraf
s.	Sayfa
S.	Sayı
ss.	Sayfa Aralığı
TBB	Türkiye Barolar Birliği
vd.	Ve devamı.
Vol.	Volume/ Cilt
Y.	Yıl

GİRİŞ

Teknolojinin gelişmesi insan yaşamına birçok pozitif katkı sağlamakta ve yaşamı kolaylaştırmaktadır. Bununla birlikte birçok negatif etkiye de sahiptir. İşte böyle bir ortamda özellikle bilişim teknolojileri alanındaki gelişmeler, artık petrolden daha değerli olarak nitelenen veri kavramını, teknoloji-hukuk ekseninde önemli bir noktaya koymaktadır.

Yuval Noah Harari'nin çok satan kitabı Homo Deus'ta dile getirdiği üzere, *“Yükselen en ilginç din ne Tanrılara ne de insana hürmet ediyor, sadece veriye tapıyor: Dataizm dini.”*¹ İşte bu denli popülerleşen ve bir yönüyle de giderek acımasız biçimde kullanılan veri kavramı ise teknoloji-insan yarışında insanı önceleyen rolü ile önemini her geçen gün artırmaktadır. Bu bağlamda “veri koruma” tamlamasının seçilmiş olması da doğaldır. Bizi biz yapan ve bizden sadır olduğu belli ya da belirlenebilir olan tüm bilgiler veri kavramı kapsamındadır. Bu bakımdan kişisel veriler aslında insanın varoluşu ve hatta tanımlanışı için bile kullanılır hale gelmiştir. Dolayısıyla verinin korunması aslında en temelde insanın varoluşunun korunması ile eş anlamlı kabul edilebilir. Şöyle ki, kişinin maddi ve manevi varlığını serbestçe geliştirebilmesi için özgür olması gerekmektedir. Ancak kişiye dair bilgilerin herkesçe bilindiği ve kişinin adeta şeffaf olduğu bir toplumda özgürlük alanı kaçınılmaz olarak daralacaktır.

Belirttiğimiz üzere bilişim teknolojilerindeki gelişmeler ve bu bağlamda bilgisayarın artık çok hızlı, kolay ve ucuz biçimde verileri işleyip depolayabilmesi konunun önemini arttırmıştır. Eskiden elle tutulan ve saklanan verilerin çok daha yüksek miktarı yalnızca bir tuşla otomatik biçimde depolanabilmektedir. Ayrıca büyük veri, nesnelerin interneti ve bulut bilişim gibi teknoloji alanında ortaya çıkan yeni oluşumlar veri işleme meselesinin sonuçlarının nerelere varabileceğini tahmin dahi edemememize sebep olmaktadır. Söz gelimi günün birinde sosyal medya uygulamaları üzerinden ya da

¹ Yuval Noah HARARI, *Homo Deus- A Brief History of Tomorrow*, Harper Collins Publishers, 2017, s. 372.

internet alışverişı veya e-devlet gibi uygulamalar üzerinden toplanan verilerimize dayanılarak öldükten sonra dahi sanal bir benzerimizin varlık gösterebilmesi mümkün olabilecektir. İşte bu bakımdan veri koruması artık ilk çıktığı dönemki algılanış biçiminden çok daha farklı bir yere evrilmiş ve konunun önemi daha da artmıştır.

Teknik boyutu oldukça fazla ve disiplinler arası niteliği ağır basan bir konu olan veri koruma alanı, hukuki perspektiften de incelendiğinde birçok hukuk dalı ile doğrudan ilişki halindedir. Dolayısıyla bu çalışma belli sınırlar dahilinde yürütülmüştür. Bu kapsamda çalışmanın temel yaklaşımı, kişinin kendisine ilişkin bilgiler üzerinde kontrolünün sağlanmasının ilk planda bir temel hak ve özgürlük sorunsalı olduğudur. Bu bağlamda bireyin karşılaştığı temel hak ve özgürlük ihlallerine karşı veri koruma sistemi bir güvence oluşturmalıdır.

Son yıllarda Türkiye’de kişisel verilerin korunması konusu hukuk alanında birçok çalışmanın temelini oluşturmuştur. Belirtilmelidir ki, bu konuda akademik anlamda hazırlanan çalışmalar hukukun hemen her alanına ilişkindir. Konu öylesine çok katmanlı bir görünüm arz etmektedir ki, ceza hukukundan idare hukukuna, medeni hukuktan iş hukuku ya da vergi hukukuna dair birçok alana yayılmaktadır. Bu incelemede ise Avrupa Birliği ve Avrupa Konseyi veri koruma hukukunun anayasal açıdan önem taşıyan unsurlarını belirleyerek, Türk anayasal sistemini ne şekilde etkilediğini araştırdık.

Özellikle gerek 2016 yılı ile birlikte Avrupa Veri Koruma Hukuku’nun geçirdiği dönüşüm ve 2010 yılında gerçekleştirilen Anayasa değişikliği ile Türk hukukunda konuya dair ilk defa bir yasal düzenlemenin yapılmış olması, gerekse 2018 ile birlikte Avrupa Veri Koruma Reformu’nun temeli olan Genel Veri Koruma Tüzüğü’nün bütünüyle uygulamaya girmesi ve Türkiye’de Kişisel Verileri Koruma Kurulu’nun giderek artan uygulamacı rolü, konunun ele alınması için elverişli bir ortam yaratmıştır.

Bu çalışma, belli sorulara cevap aramak gayesindedir: i) İnsan hakları genel kuramında dördüncü kuşak hakların ortaya çıkmasına neden olan gelişmeler nelerdir? Bilişim teknolojileri alanında gerçekleşen yenilikler aynı zamanda yeni bir insan hakkının

ortaya çıkışı için insan onuruna yönelik riskler de barındırmakta mıdır? ii) Kişisel verilerin korunmasının temel bir insan hakkı olarak kabulünde başlangıç noktası olan mahremiyet kavramı neden önemlidir ve veri koruma hukukunun gelişimini tarihsel olarak hangi yönlerden etkilemiştir? iii) Avrupa veri koruma hukukunun doğuş ve gelişim aşamaları ile temel hukuki metinleri ne şekilde uygulanmaktadır? Veri Koruma Reformu’nun bir temel hak olan ve Avrupa genelinde çoğunlukla anayasal bir hak olarak kabul edilen kişisel verilerin korunması üzerindeki etkileri nelerdir? iv) Kişisel verilerin korunmasının Türkiye bakımından anayasal bir hak olarak kabulü ve konu hakkındaki Anayasa Mahkemesi içtihadı ne şekilde ortaya çıkmıştır? Kişisel Verilerin Korunması Kanunu’nda yer alan düzenlemeler ve ulusal denetim makamı olan Kişisel Verilerin Korunması Kurumu’nun uygulamaları üzerinde Avrupa Veri Koruma Hukuku’nun etkileri nedir? Ne olmalıdır?

Temelde bu sorulara yanıt arayan çalışmanın, “İnsan Hakları Genel Kuramı Işığında Kişisel Verilerin Korunması Hakkı” başlıklı Birinci Bölümü’nde ilk olarak insan hakları kavramı ve insan haklarının tarihsel süreçteki görünümü ele alınmaktadır. Bunun sebebi, insan haklarının temeli olarak insan onuru kavramının dördüncü kuşak haklar bakımından arz ettiği önemin daha iyi anlaşılabilmesidir. İkinci olarak kişisel verilerin korunmasının bir insan hakkı olarak ele alınması süreci incelenmiştir. Bu noktada bilişim teknolojisinin insan onuruna ilişkin yarattığı tehlikeler karşısında dördüncü kuşak hak kategorisinin oluşumu ve bu tehlikelerin ortadan kaldırılabilmesi için özel yaşamın korunması hakkı içerisinde kişisel verilerin korunmasının ortaya çıkışı açıklanmaya çalışılmıştır. Kişisel verilerin korunması hakkının çıkış noktası olarak kabul edilen mahremiyet konusu da kavramın Avrupa ve Amerikan anlayışları ile birlikte, veri koruma hukukunun doğuşu ve gelişimi sürecine sağladığı katkı bakımından ilgili dönemde hazırlanmış çeşitli rapor ve hukuki metinler incelenerek ele alınmıştır. Bu bölümde son olarak, kişisel verilerin korunması hukukunun temel kavramları incelenmiştir.

Çalışmanın “Avrupa Veri Koruma Hukuku” başlıklı İkinci Bölümünde ise öncelikle Avrupa Veri Koruma Hukuku’nun doğumuna sebep olan etkenler ve buna bağlı olarak ortaya çıkan hukuki metinler ele alınmıştır. Kişisel verilerin korunmasında

uluslararası düzlemde gerek Amerika Birleşik Devletleri gerek de Avrupa ülkeleri tarafından üzerinde uzlaşmış bir metin olan ve ardından gelecek 1981 tarihli 108 Numaralı Kişisel Verilerin Otomatik Olarak İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşme'nin (108 Sayılı Sözleşme) bir bakıma hazırlık çalışmaları gibi de görülebilecek olan 1980 tarihli OECD'nin "Özel Yaşamın Gizliliğinin ve Sınır Ötesi Kişisel Veri Dolaşımının Korunmasına İlişkin Rehber İlkeler"ine (OECD Rehber İlkeler) dair genel bir açıklama yapılmıştır.

Devamında "Avrupa Konseyi" başlığında, bu alanda birinci dalga hukuki düzenleme olarak kabul edilen 108 Sayılı Sözleşme ele alınmıştır. 2018'de 108 Sayılı Sözleşme'yi yenileyen Sözleşme 108+'nın bu noktada getirdiği yenilikler ve Veri Koruma Reformu ile ilişkisi bağlamında incelenmiştir. Avrupa Konseyi'nin yargı organı olan İnsan Hakları Avrupa Mahkemesi'nin konuya yaklaşımı ise İnsan Hakları Avrupa Sözleşmesi'nin 8. maddesinde bulunan özel yaşamın korunması hakkı bakımından 1970'lerden günümüze dek karara bağlamış olduğu bazı temel içtihatları incelenerek sorgulanmıştır.

"Avrupa Birliği" başlığında ise ilk olarak AB Temel Haklar Şartı, kişisel verilerin korunması hakkını bağımsız bir temel hak olarak tanıması kapsamında ve Adalet Divanı'nın konuya ilişkin içtihatları ortaya konulmaya çalışılmıştır. Veri koruma hukukunun ikinci dalga hukuki düzenlemesi olarak kabul edilen 95/ 46/ AT Sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi de Adalet Divanı kararları bakımından incelenmiştir. Divan'ın içtihatları seçilirken kişisel verilerin korunması alanında getirdiği yenilikler ve metinlerin içeriğinin anlaşılmasına yaptığı katkılar dikkate alınmaya çalışılmış ve kararlara Divan'ın geçirdiği tarihsel değişimi de vurgulamak amacıyla kronolojik olarak değinilmiştir. Yine bu bölümde Veri Koruma Reformu'na götüren belli başlı hukuki metinler ele alınmıştır. Avrupa Veri Koruma Hukuku'nun günümüze dek geçirdiği en büyük dönüşümü karşılayan Veri Koruma Reformu başlığında ise Reform'un en temel metni olarak kabul edilen 2016/ 679 Sayılı Genel Veri Koruma Tüzüğü'nün veri koruma alanına getirdikleri detaylı bir biçimde işlenmeye

alışılmış ve kendinden önceki Direktif ile farkları ortaya konulmuştur. Bu bakımdan anılan düzenlemelerin hem Reform öncesi hem de Reform sonrası AB üye ülkelerinin ulusal hukuk düzenlerinde ne gibi değışikliklere yol açtığı açıklanmıştır.

“Avrupa Veri Koruma Hukukunun Türk Hukuk Sistemine Etkisi”nin incelendiğı Üüncü Bölüme gelindiğinde ise öncelikle kişisel verilerin korunması hukukunun doğduğu yer olarak kabul edilen Almanya’dan, Alman Federal Anayasa Mahkemesi’nin nüfus sayım kararı detaylı bir biçimde incelenerek kişisel verilerin korunmasının neden anayasal düzeyde olması gerektiğı açıklanmaya çalışılmıştır. Ardından 2010 yılındaki Anayasa Değışiklikleri ile Türkiye’de bağımsız bir anayasal hak olarak kabul edilen kişisel verilerin korunması(nı isteme) hakkının 1982 Anayasası’nın 20/3. maddesindeki düzenlemesine değinilmiştir. Kişisel verilerin korunmasının her ne kadar bağımsız bir anayasal hak olarak düzenlenişı Avrupa’ya kıyasla nispeten geç bir tarih olsa da bu tarihten önce de kavramın Anayasa’da yer alan bazı temel hak ve özgürlüklerle ilişkilendirilerek korunmaya çalışıldığı görölmüştür. Anayasal görünümü bu biçimde olan hakkın kanunla düzenlenmesi 2016 yılında gerçekleştiğinden, söz konusu gecikmenin olumsuz etkilerinden bahsedilmiştir. 6698 Sayılı Kişisel Verilerin Korunması Kanunu’nun (KVKK) kapsamı ortaya konarken Avrupa Veri Koruma Reformu karşısındaki durumuna ilişkin bir değerlendirme yapılmıştır. Kişisel verilerin korunmasının Türkiye özelinde anayasal ve yasal düzenlemesinin genel itibarıyla bu şekilde ele alınmasının ardından konuya ilişkin Anayasa Mahkemesi içtihadı incelenerek, Avrupa Veri Koruma Hukuku açısından değerlendirilmiştir. Son olarak, kişisel verilerin korunmasına ilişkin anayasal ve yasal mevzuata yönelik değışiklik önerilerinde bulunulmuştur.

BİRİNCİ BÖLÜM

İNSAN HAKLARI GENEL KURAMI IŞIĞINDA KİŞİSEL VERİLERİN KORUNMASI HAKKI

İnsan hakları kavramı doğuşundan itibaren zamanın tehditlerine karşı sürekli bir devinim içerisinde olmuştur. Tarihsel süreçte insan haklarının sahneye çıkışlarını esas alan sınıflandırmaya bakıldığında da bu etki fazlasıyla görülür. İnsan onuruna karşı yönelen tehditlere bir cevap niteliği de taşıyan bu sınıflandırmada günümüz teknolojik ve bilimsel gelişmeleri önemli rol oynamaktadır. Bu bakımdan çalışmamızın ilk bölümü, insan hakları genel kuramı bağlamında kişisel verilerin korunmasına giden yolu açıklamak gayretindedir. Öncelikle insan hakları ve bu kavramın tarihsel süreçteki görünümü, Türkiye’yi de değerlendirerek, ele alınacak ve yeni hak kategorilerinin ortaya çıkmasında esas aldığımız ana kavram olan insan onuruna değinilecektir. Bu genel girişin ardından, teknolojik gelişmeler neticesinde dördüncü kuşak hakların doğumundan bahsedilecektir. Özellikle bilişim teknolojilerinin ortaya çıkışı ve gelişmesi ile doğrudan tehdit edilen mahremiyet kavramına gerek Avrupa gerekse Amerika ölçeğinde atfedilen anlam ve değer konu edilerek mahremiyetin korunmasından kişisel verilerin korunmasına evrilen veri koruma hukuku süreci ortaya konulmaya çalışılacaktır. Nihayetinde ise ikinci bölümün daha iyi anlaşılması bakımından teknik bir alan olan kişisel verilerin korunmasına dair bazı temel kavramların genel açıklamaları yapılacaktır.

I. KAVRAMSAL OLARAK İNSAN HAKLARI

Bir hakka dayanan talep, başka ahlaki ve siyasi nedenlere karşı üstünlüğe sahiptir². Bu bakımdan insan hakları öğretisini bütünüyle anlayabilmek, temelde hak kavramını özümsemekle gerçekleşir. Hak, en basit tanımıyla, doğruluk ve yetkidir³.

² Ronald DWORKIN, *Taking Rights Seriously*, Harvard University Press, Massachusetts, 1977, s. 90; Jack DONNELLY, *Teoride ve Uygulamada Evrensel İnsan Hakları*, Çev: Mustafa ERDOĞAN- Levent KORKUT, Yetkin, Ankara. 1995, s. 19.

³ DONNELLY, *Teoride ve Uygulamada Evrensel İnsan Hakları*, s. 19.

Doğruluk boyutuyla hak, bir şeyin doğru, uygun ve yerinde olduğunu belirtmektedir⁴. Yetki boyutuyla ise bir şeyi yapmaya, talep etmeye yetkili olmak anlamına gelmektedir⁵. Başka bir tanımı ile hak, hukuk tarafından sunulan yetkiler içerisinde kişilere tanınmış olan menfaatler olarak ele alınmaktadır⁶. Zaten haklardan söz edildiğinde, yetki anlamı vurgulanmaktadır⁷. Dolayısıyla bu tanımların ortak özelliği, bir hakkın varlığından bahsedebilmek için, yetki ve talep unsurlarının mevcudiyetini gerektirmesidir⁸.

Bir hakka sahip olmak demek, bu hakka dayanan bir talepte ısrara yetkili olmak demektir. Bu bakımdan kişi bir hakka sahip olmadıkça bir faydadan yararlanır, ancak bir şeyi hak (yetki) olarak ileri süremez. Dolayısıyla bir hakka sahip olma, kişi o haktan yararlanamadığı zaman, kişinin hakka sahip olma hali kendi dışındakilerce objektif olarak kabul edilmediğinde anlam kazanır. Bu durum doktrinde “*Hakların Sahiplik Paradoksu*” olarak ele alınmaktadır⁹.

Bir hakkın sahibi olunması çeşitli sebeplere dayanabilmektedir. Bu bağlamda, hakkın kaynağı sözleşme olabilir. Ayrıca hakkın kaynağı, yönetmelik, yasa ya da anayasa gibi hukuk kuralları da olabilmektedir. Bunların dışında bir hakkın kaynağı, o hakkın varlığına ilişkin meşruluk, talebin haklılığı fikridir. Hakkın kaynağı olarak ele alınan bu son unsur, insan hakları fikrinin doğumu açısından özellikle ayrı bir önem taşımaktadır. Bu bakımdan, bir tutum veya davranışın doğruluğu ve başkaları tarafından saygı gösterilmesi zorunluluğu hak kavramını ortaya çıkarmaktadır¹⁰.

Hak kavramının özel bir şekli olarak insan hakları da hak kavramının kaynağını oluşturan ahlaki meşruluk fikrinden doğmaktadır¹¹. Bu bakımdan insan hakları, en üstün

⁴ Ali Fuat BAŞGİL, “Hakkı ve Hukuku Devlet mi Yaratır ve Yapar?”, *Ordinaryüs Prof. Dr. Tahir TANER’e Armağan’dan Ayrı Bası*, İsmail AYGÜN Matbaası, İstanbul, 1956, s. 2.

⁵ DONNELLY, *Teoride ve Uygulamada Evrensel İnsan Hakları*, s. 19.

⁶ Bilge UMAR, *Hukuk Başlangıcı*, Dokuz Eylül Üniversitesi Yayınları, İzmir, 1997, s. 147.

⁷ DONNELLY, *Teoride ve Uygulamada Evrensel İnsan Hakları*, s. 19.

⁸ Nihat BULUT, *Sanayi Devriminden Küreselleşmeye Sosyal Haklar*, XII Levha, İstanbul, 2009, s. 7.

⁹ DONNELLY, *Teoride ve Uygulamada Evrensel İnsan Hakları*, s. 19, 21, 23.

¹⁰ Oktay UYGUN, “İnsan Hakları Kuramı”, *İnsan Hakları*, Ed.: Korkut TANKUTER, Yapı Kredi Yayınları, İstanbul, 2000, s. 13- 14; BULUT, *Sanayi Devriminden Küreselleşmeye Sosyal Haklar*, s. 8.

¹¹ BULUT, *Sanayi Devriminden Küreselleşmeye Sosyal Haklar*, s. 8.

ahlaki haklardır¹². İnsanın insan olmaktan ötürü ve doğuştan sahip olduğu bu haklar¹³, insanın onurunu korumak için devletin mutlak iktidarına bir başkaldırı olarak nitelenebilecektir. Bu bakımdan devletin keyfî müdahalesine karşı ahlaki bir talep olarak doğmuş insan hakları, kural olarak devlet karşısında ileri sürülmeleri sebebiyle siyasi niteliktedir ve devleti bazı davranışları yapmaktan alıkoyar veya bazı davranışları yapmaya zorlar¹⁴. İnsan hakları bu haliyle, siyasal meşruluğun bir ölçütü olarak son çaredir ve esasında var olan hukuki düzleme karşı çıkıp onu değiştirerek, paralel bir hakkın etkin ve sistematik kullanımını yaygınlaştırmayı amaçlamaktadır. Zaten insan haklarının gerçek değeri ve gücü de burada yatmaktadır. Ahlaki bir hak olan insan hakkı, ilerleyen safhalarda hukuk gücüyle desteklenen ve hukuki düzlemde uygulanabilir paralel bir hukuki hakka dönüşmektedir¹⁵.

Ancak insan hakları yerine doktrinde ve bazı belgelerde farklı kavramlarla da karşılaşılmaktadır. Bu bakımdan kamu özgürlükleri, temel haklar, temel hak ve özgürlükler, anayasal haklar ilk planda akla gelmektedir. Kamu özgürlükleri ile devlet tarafından tanınarak pozitif hukuka giren insan hakları kastedilmektedir¹⁶. Daha açık bir söyleyişle kamu özgürlükleri, yürürlükteki hukukça tanınan haklardır. Colliard da kamu özgürlüklerini “...kişilere, devletçe düzenlenen ve korunan bazı haklar...” olarak nitelemiştir. Dolayısıyla bir özgürlük ancak yürürlükte bulunan hukuk tarafından garanti edilmişse kamu özgürlüğü olmaktadır¹⁷. Temel hak ve özgürlükler ile anayasal haklar ifadeleri de doktrinde bu anlamda kullanılabilmektedir¹⁸. Ancak belirtilmelidir ki temel

¹²DONNELLY, *Teoride ve Uygulamada Evrensel İnsan Hakları*, s. 22.

¹³ Jerome J. SHESTACK, “The Philosophical Foundations of Human Rights”, *Human Rights Quarterly*, V. 20, N. 2, Mayıs 1998, s. 203; DONNELLY, *Teoride ve Uygulamada Evrensel İnsan Hakları*, s. 19.

¹⁴ Demelash SHIFERAW, Yonas TESFA, *Human Rights Law*, The Justice and Legal System Research Institute, 2009, s. 2; Mustafa ERDOĞAN, *İnsan Hakları Teorisi ve Hukuku*, Orion Kitabevi, Ankara, 2015, s. 27.

¹⁵ DONNELLY, *Teoride ve Uygulamada Evrensel İnsan Hakları*, s. 24- 26.

¹⁶ Münci KAPANİ, *Kamu Hürriyetleri*, Yetkin Yayınları, Ankara, 2013, s.14; Mehmet AKAD, Bihterin VURAL DİNÇKOL, Nihat BULUT, *Genel Kamu Hukuku*, Der Yayınları, İstanbul, 2018, s. 251- 252.

¹⁷ İlyas DOĞAN, “İnsan Hakları Hukukunun Temel Kavramları ve Özellikleri”, *İnsan Hakları Hukuku*, Ed.: İlyas DOĞAN, Astana Yayınları, Ankara, 2015, s. 44- 45.

¹⁸ Kemal GÖZLER, *Türk Anayasa Hukuku Dersleri*, Ekin Yayınevi, Bursa, 2016, s. 122- 123; ERDOĞAN, *İnsan Hakları Teorisi ve Hukuku*, s. 106.

hak ve özgürlükler, bireylerin yalnızca haklara sahip olmasını değil, ayrıca ödevlerinin de bulunmasını ifade eden bir kavramdır¹⁹. Görüldüğü üzere tüm bunlar arasında önemli farklılıklar bulunmaktadır²⁰. Her ne kadar temel haklar ifadesi, kanunlarla değiştirilemeyecek haklar olarak yorumlandığında hem anayasal sistem tarafından güvence altına alınan, yani bir bakıma hukuk düzenince tanınmış bulunan hakları (kamu özgürlükleri) hem de uluslararası belgelerde düzenlenen hakları ifade etse de içerinden en kapsamlı olanı insan hakları ifadesidir. Bu, insanın sırf insan olmasından kaynaklanan ve hiçbir surette herhangi bir ırksal, dilsel, dini vb. yönelimi barındırmayan bir ifadedir. İlaveten insan hakları kavramı, bir yandan ulusal ve uluslararası alanda oldukça geniş bir haklar bütünü sunarken, diğer yanıyla daha korumacı güvence sistemlerini de barındırmaktadır²¹.

İnsan haklarının başka haklardan ayrılmasını sağlayan spesifik özellikleri bulunmaktadır. Ancak burada belirtilmelidir ki, bu özellikler insan hakkı kavramının temellendirilme biçimine göre değişecektir. Çalışmamızın insan haklarının temelini konumlandırışı bakımından doğal haklar yaklaşımından yola çıkıldığında, insan hakları niteliği gereği evrensel, mutlak, dokunulmaz, devredilmez ve vazgeçilmezdir. İnsan haklarının evrenselliği, zaman ve mekâna bağlı olmaksızın, tüm insanlığı ilgilendiren biçimde dil, din, ırk, toplumsal aidiyet gözetmeksizin herkes tarafından ve dünya ölçeğinde sahip olunmalarını ifade etmektedir²². Özellikle dile getirilmelidir ki, insan haklarının evrensel olma özelliği, çoğulcu bir dünyadaki çeşitli farklılıkların da dikkate alındığı en güncel anlamı ile algılanmalıdır²³. İnsan haklarının mutlaklığı ise, bu hakların hiçbir biçimde kayda ve şarta bağlanmamasını karşılamaktadır. Daha açık bir söyleyişle bu özellik, insan haklarının varlığını toplumsal ödevlerin yerine getirilmesine

¹⁹ DOĞAN, “İnsan Hakları Hukukunun Temel Kavramları ve Özellikleri”, *İnsan Hakları Hukuku*, s. 45.

²⁰ Oktay UYGUN, *1982 Anayasasında Temel Hak ve Özgürlüklerin Genel Rejimi*, Kazancı Yayınları, İstanbul, 1992, s. 3- 4.

²¹ AKAD, VURAL DİNÇKOL, BULUT, *Genel Kamu Hukuku*, s. 251- 252.

²² ERDOĞAN, *İnsan Hakları Teorisi ve Hukuku*, s. 105- 106; BULUT, *Sanayi Devriminden Küreselleşmeye Sosyal Haklar*, s. 10.

²³ Tekin AKILLIOĞLU, *İnsan Hakları: Kavram, Kaynaklar ve Koruma Sistemleri*, İmaj, Ankara, 2010, s. 32.

bağlamamaktadır. İnsan haklarına bütün olarak saygı gösterilmelidir²⁴. İnsan haklarının dokunulmaz oluşuna baktığımızda ise, her ne kadar bazı hakların anayasaya uygun olarak sınırlandırılabilmesi mümkünse de en başta devlet olmak üzere kimsenin belirli bazı mutlak haklara müdahalede bulunamayacağını karşıladığı görülmektedir²⁵. İnsan haklarının devredilmez ve vazgeçilmez olması ise, doğrudan bir insanın kişiliğine bağlı olmasından dolayı bu haklardan herhangi bir biçimde vazgeçilmesinin ya da bir başkasına, bir kuruma devredilmelerinin, hak sahibi tarafından istense dahi, mümkün olmaması halini ifade etmektedir²⁶.

II. TARİHSEL SÜREÇTE İNSAN HAKLARI

İnsan hakları kavramı ve kökenleri, tarihsel süreçte mütemadiyen ilgi çekici bir konu olarak kendini göstermektedir. Felsefi bağlamda ilk çağdan itibaren var olan bu kurum, modern devlet teorisinde Aydınlanma Çağı ile birlikte 17. ve 18. yüzyıllarda siyasi baskıya karşı bir korunma mekanizması olarak ortaya çıkmıştır²⁷. Doğal haklar teorisini 17. yüzyılda geliştiren John Locke, bu kavram kapsamında insan hakları fikrini de ilk dile getiren kişi olarak anılmaktadır. 18. yüzyılda ise Thomas Paine, her insanın doğuştan sahip olduğu ve inkâr edilemeyen hakları bulunduğunu dile getirmiştir²⁸.

Belirtilmelidir ki tarih boyunca ortaya çıkmış ve devamında listeler halinde süregelen insan hakları, aslında belirli alanlarda insan onuruna yönelik ortaya çıkmış standart tehdit ve tehlikelere karşı birer zırhtır. Ne zamanki ortada insan onuruna yönelik

²⁴ ERDOĞAN, *İnsan Hakları Teorisi ve Hukuku*, s. 108.

²⁵ AKILLIOĞLU, *İnsan Hakları: Kavram, Kaynaklar ve Koruma Sistemleri*, s. 21; BULUT, *Sanayi Devriminden Küreselleşmeye Sosyal Haklar*, s. 10.

²⁶ ERDOĞAN, *İnsan Hakları Teorisi ve Hukuku*, s. 111- 112; BULUT, *Sanayi Devriminden Küreselleşmeye Sosyal Haklar*, s. 11.

Bu noktada belirtilmelidir ki, doktrindeki bir görüşe göre insan hakları, bireylerin devlet karşısındaki özgürlük haklarıdır. Bu bakımdan temel bir haktan vazgeçmek, vazgeçme özgürlüğünü kullanmaktır. Zafer GÖREN, *Temel Hak Genel Teorisi*, Dokuz Eylül Üniversitesi Yayını, İzmir, 2000, s. 62.

²⁷ Oktay UYGUN, *Devlet Teorisi*, On İki Levha Yayıncılık, İstanbul, 2014, s. 470; ERDOĞAN, *İnsan Hakları Teorisi ve Hukuku*, s. 24; SHIFERAW, TESFA, *Human Rights Law*, s. 2.

²⁸ ERDOĞAN, *İnsan Hakları Teorisi ve Hukuku*, s. 127.

büyük bir tehlike mevcuttur, işte o noktada insan hakkını tanımak gereği söz konusu olmuştur²⁹.

İnsan hakları her ne kadar modern bir fikir olarak dile getirilse de bu düşünceye götüren ilk hukuki belge Orta Çağ'da İngiltere'de ortaya çıkmıştır³⁰. 1215 tarihli *Magna Carta Libertatum* ile monark ilk kez kendi mutlak ve sınırsız yetkisinden, tebaası lehine bazı haklar bakımından feragat etmiştir³¹. İnsan hakları fikrine ulaşmada yardımcı olan ve Avrupa'da gerçekleşen diğer gelişmelere bakıldığında ise, Macaristan'da 1222 tarihli *Altın Boğa (Golden Bull) Barışı*, Danimarka'da 1282 tarihli *Erik Klippings Anlaşması (håndfæstning)*, Brüksel'de 1356 tarihli *Seviçli Giriş (Joyous Entry) Anlaşması* ve Hollanda'da 1579 tarihli *Utrecht Birliği (Union of Utrecht)* anılmalıdır. Bu belgeler din özgürlüğü gibi spesifik bazı durumlara ilişkin hakları içermekte oldukları için adeta kendi ülkelerinin Magna Cartaları olarak ortaya çıkmışlardır. Fakat tüm bu düzenlemeler, bireysel özgürlük kavramının kapsayıcı felsefi niteliğini haiz değildir ve kişilere kendi mevkii ve statülerine göre haklar tanımışlardır³².

İngiltere'de bu şekilde bir görünüm arz eden insan hakları kavramı, Orta Çağ Avrupası'nda hüküm süren iktidarın, feodal beylikler, krallıklar, kilise gibi kurumlarca bölünmüş bir iktidar olması sebebiyle modern devlette karşılaşacağı kadar büyük bir tehdit altında değildi. Her ne kadar insan onuruna yönelik saldırılar ilgili dönemde de mevcut olsa, insan onuruna karşı en güçlü saldırılar Avrupa'da mutlak monarşilerin ortaya çıktığı ve iktidarın merkezileştiği modern devlette meydana gelmiştir. Orta Çağ Avrupası'nda iktidarın tek elde toplanmış olmaması sebebiyle geniş bir coğrafyada güvenli bir biçimde ticaret yapamayan ve servetini güvence altına alamayan burjuvazi, feodalitenin bölünmüşlüğü ortadan kaldırılana kadar krallara destek olmuştur. Ancak

²⁹ DONNELLY, *Teoride ve Uygulamada Evrensel İnsan Hakları*, s. 36.

³⁰ Daron ACEMOGLU, James A. ROBINSON, *Why Nations Fail – The Origins of Power Prosperity and Poverty*, Profile Books, 2013, s. 185; ERDOĞAN, *İnsan Hakları Teorisi ve Hukuku*, s. 128.

³¹ Sezen KAMA, "Parlamenter Hükümet Sistemi Olarak 'Westminster Modeli' - Britanya Örneği Üzerine Bir Deneme", *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, C. 22, S. 2, s. 179, ss. 161- 201.

³² SHIFERAW, TESFA, *Human Rights Law*, s. 3.

kralların tek ve egemen güç haline gelmesinin ardından bu kez de haklarının güvence altına alınması için krallıklara karşı harekete geçmiş ve anayasa ve haklar bildirisi gibi hareketler sonucu mülkiyet hakkı, düşünce ve inanç özgürlükleri gibi bazı temel haklar ve özgürlüklerin hukuki belgelerde düzenlenmesini sağlamıştır³³.

Bu bağlamda 1628’de İngiliz Haklar Bildirisi (*Petition of Rights*)’nin ilanı ile sebepsiz hapis cezası yasağı, parlamentonun onayı olmaksızın vergi salınım yasağı, askerlerin barış zamanında vatandaşların evlerinde konumlandırılması yasağı gibi mal ve can güvenliğine dokunulmasını engelleyen belli bazı özgürlükler getirilmiş ve monarkın müdahalesi yasaklanmıştır³⁴.

Modern çağda insan hakları teorisi bakımından pratikteki önemli ilk belge ise, otorite ve karar alma yetkisinin artık monarktan parlamentoya resmen geçişini simgeleyen 1688 tarihli Muhteşem Devrim (*Glorious Revolution- Bloodless Revolution*) sonrasında parlamento ile monarkın yeni bir anayasa üzerinde anlaşma sağlayarak 1689 yılında ilan ettiği Haklar Beyannamesi (*Bill of Rights*)’dir³⁵. Haklar Beyannamesi, bir yandan monarkın gücünü kısıtlayıp öte yandan parlamentonun yetkilerini artırmakta ve parlamentodaki ifade özgürlüğünü koruma altına almaktadır³⁶. Ayrıca bu bildiri ile, adil yargılanma ve olağan olmayan cezaya çarptırılma yasağı da doğal haklar olarak nitelendirilmiştir.³⁷

Magna Carta, Haklar Beyannamesi ve onun etkisiyle John Locke tarafından geliştirilen doğal haklar teorisi, Amerika kıtasını önemli ölçüde etkilemiştir³⁸. Bu doğrultuda Haziran 1776 tarihinde “vazgeçilmez haklar” ve “eşit özgürlük” ilkelerine

³³ UYGUN, *Devlet Teorisi*, s. 476- 477.

³⁴ John PATTERSON, *The Bill of Rights Politics Religion and the Quest for Justice*, iUniverse Inc., 2004, s. 23- 24; Bülent YÜCEL, *Parlamente Hükümet Sisteminin Rasyonelleştirilmesi ve Türkiye Örneği*, Adalet Yayınevi, Ankara, 2009, s. 54.

³⁵ ACEMOGLU, ROBINSON, *Why Nations Fail – The Origins of Power Prosperity and Poverty*, s. 191.

³⁶ YÜCEL, *Parlamente Hükümet Sisteminin Rasyonelleştirilmesi ve Türkiye Örneği*, s. 54.

³⁷ ERDOĞAN, *İnsan Hakları Teorisi ve Hukuku*, s. 128.

³⁸ *The Bill of Rights with Writings that Formed Its Foundation*, Applewood Books, 2016, Bedford, s. 6- 7; ERDOĞAN, *İnsan Hakları Teorisi ve Hukuku*, s. 128.

dayanan Virginia Bildirgesi (*Virginia Declaration of Rights*) kabul edilmiştir. Bu bildirmede, yaşam, özgürlük, mülkiyet ve mutluluğu arama hakları vazgeçilmez doğal haklar olarak nitelendirilmişlerdir. Temmuz 1776'da ise Thomas Jefferson tarafından düzenlenen ve on üç Amerikan devleti tarafından oybirliği ile ilan edilen Amerikan Bağımsızlık Bildirgesi (*Declaration of Independence*) de bu haklara yer vermiştir³⁹. Ardından 1791 yılında Amerikan Anayasası'na yapılan ilk değişiklik olan Haklar Beyannamesi (*Bill of Rights*) ifade, basın, toplantı, din, konut dokunulmazlığı, jürili bir mahkeme önünde adil, süratli ve aleni yargılanma, aşırı, olağandışı veya zalimane ceza yasağı gibi hak ve özgürlükleri ele alarak o zamana kadar düzenlenmiş en geniş kapsamlı insan hakları metinlerinden biri olmuştur⁴⁰.

İngiltere ve Amerika'da 17. ve 18. yüzyıllarda meydana gelen bu gelişmeler, 1789 Fransız Devrimi'ne de temel hazırlamıştır. Bu bağlamda insan haklarına ilişkin aynı bakış açısını içeren ve daha önce anılan haklara ilave olarak “güvenlik” ve “baskıya karşı direnme” haklarının da dahil edildiği 1789 İnsan ve Yurttaş Hakları Bildirisi ilan edilmiştir⁴¹.

İngiltere, Amerika ve Fransa'da, yukarıda anılan şekilde söz konusu belgelere kaynaklık eden doğal haklar öğretisi 19. yüzyılla beraber etkisini yitirmeye başlamıştır. Bu dönemde insan hakları anlayışının yerini ulusların hakları almış; Marksist, pragmatist ve pozitivist fikirler daha fazla taraftar bulur hale gelmiştir. 20. yüzyılda ise insan hakları, kanunlar ve anayasalara sistematik olarak girmiştir. Bu dönemde özellikle ekonomik ve sosyal haklar ilk olarak 1917 Meksika Anayasası ve 1919 Weimar Anayasası'nda yer

³⁹ Michael Stokes PAULSEN, Luke PAULSEN, *The Constitution- An Introduction*, Basic Books, New York, 2015, s. 4- 5; *The U.S. Constitution and Other Key American Writings*, Canterbury Classics/ Baker& Taylor Publishing, San Diego, 2015, s. 5- 10.

⁴⁰ Akhil Reed AMAR, *The Bill of Rights- Creation and Reconstruction*, Yale University Press, New Haven& Londra, 1998, s. 21- 45; K. Lee LERNER, Brenda WILMOTH LERNER, Adrienne WILMOTH LERNER (Ed.), *Human and Civil Rights: Essential Primary Sources*, Thomson Gale, Michigan, 2006, s. 6- 9; *The Bill of Rights with Writings that Formed Its Foundation*, Applewood Books, Bedford, 2016, s. 12- 13.

⁴¹ LERNER, WILMOTH LERNER, WILMOTH LERNER (Ed.), *Human and Civil Rights: Essential Primary Sources*, s. 4- 6; ERDOĞAN, *İnsan Hakları Teorisi ve Hukuku*, s. 129.

bulmuş, I. Dünya Savaşı'nın ardından yapılan birçok anayasa da (1920 Estonya Anayasası, 1920 Çekoslovakya Anayasası, 1921 Yugoslavya Anayasası, 1921 Polonya Anayasası ve 1932 Romanya Anayasası) bu haklara geniş biçimde yer vererek aynı yolu takip etmiştir⁴².

“İnsan Hakları” teriminin “Doğal Haklar” kavramı yerine daha geniş bir biçimde kullanılması ise, modern insan hakları öğretisinin de olduğu II. Dünya Savaşı sonrası döneme tekabül etmektedir⁴³. Bu savaşa götüren baskıcı rejimler nedeniyle dünyanın geldiği noktaya bakılarak insan hakları fikrinin yeniden ve şiddetli biçimde kendini göstermesi ise 1948 tarihli İnsan Hakları Evrensel Beyannamesi ile olmuştur.

Ancak bu öğretinin öncüsü olarak 1648 tarihli Westphalia Barışı dile getirilebilir. Ayrıca benzer fikirler, 18. ve 19. yüzyıllarda köle karşıtlığı hareketlerde ve Osmanlı İmparatorluğu'ndaki azınlıkları koruyucu anayasal gelişmelerde de kendini göstermektedir. Bu gelişmelerin devamında hem Avrupa'da hem de Amerika'da bazı girişimler olmuş ve bu girişimler nihai olarak İnsan Hakları Evrensel Beyannamesi metninde vücut bulmuşlardır. İlk olarak 1922 yılında Paris'te Uluslararası İnsan Hakları Federasyonu kurulmuş ve çerçeve bir insan hakları beyannamesi için kampanyalara başlamışlardır. Devamında yine Paris'te bulunan Uluslararası Siyaset Akademisi, New York'taki Uluslararası Hukuk Enstitüsü'nün 1929 tarihli “Uluslararası İnsan Hakları Deklarasyonu”na da temel olacak 1926 tarihli aynı isimli belgeyi yayımlamıştır. 1944 yılında ise Amerikan Hukuku Enstitüsü, “Temel İnsan Hakları Tebliği”ni yayımlamıştır⁴⁴. Tüm bu çalışmalar, Avrupa ve Amerika'da 1948 Deklarasyonu'nu hazırlayacak kamuoyunda büyük yankı uyandırarak anılan belgenin çekirdeğini oluşturmuştur.

⁴² ERDOĞAN, *İnsan Hakları Teorisi ve Hukuku*, s. 130.

⁴³ SHIFERAW, TESFA, *Human Rights Law*, s. 1.

⁴⁴ 1648 Westphalia Barışı'nda Alman Prensligi'nin egemenliğinin, dini toleransın garanti altına alınması sonucunda kısıtlanması söz konusudur.

Charles R. BEITZ, *The Idea of Human Rights*, Oxford University Press, New York, 2009, s. 14- 16.

II. Dünya Savaşı'nın etkileyici bir mirası olarak adlandırılabilir söz konusu insan hakları öğretisi, modern dünyanın bir gerçeği olarak gelişim göstermiştir. Barış zamanının küresel toplumu, insan hakları ile ortak bir değerler dili geliştirmiştir⁴⁵. Yukarıda anılan gelişmeler neticesinde adeta bir haklar, uluslar ve insanlar arasında karşılıklı bağımlılık deklarasyonu olan 1948 tarihli İnsan Hakları Evrensel Beyannamesi ile de ilk bütüncül görünümüne ulaşmıştır. Bu belge başlangıcında, “*İnsanlık ailesinin bütün üyelerinde bulunan onur*”⁴⁶ kavramına yaptığı atıf ile insan haklarının temelini “insan onuru” olduğu görüşüne sahip çıkmakta ve tüm insanların sahip olduğu bu onurun korunması gerekliliğini uluslararası alanda tanınmasını sağlamaktadır⁴⁷.

Türkiye tarihi bakımından ise Tanzimat Dönemi'nin ele alınması, insan hakları fikrinin Osmanlı ve dolayısıyla Türkiye'de hangi surette şekillendiğini ortaya koymak açısından önem taşımaktadır⁴⁸. İlgili dönemin her ne kadar ilk vazifesi varolan tüm kitleleri birarada tutarak devletin dağılmasını engellemek olarak dile getirilse de ikinci önemli vazifesi de bireyin üzerindeki baskıları azaltarak kişilere hukuki olarak korunaklı bir özgürlük alanı yaratmaktır⁴⁹.

Bugünkü anlamı ile insan hakları öğretisinin gelişimi bağlamında Tanzimat Dönemi öncesinde ele alınması gereken metin 1808 tarihli Sened-i İttifak'tır. Söz konusu belge ile Padişah'ın yetkilerine ayanlar lehine bir sınırlama ve ayrıca yoksullar ile halk için bazı güvenceler getirilmiştir. Bu bağlamda doktrinde metnin bazı hükümlerinin kişi

⁴⁵ BEITZ, *The Idea of Human Rights*, s. 1.

⁴⁶ Rona AYBAY, *Açıklamalı İnsan Hakları Evrensel Bildirisi*, TBB, Ankara, 2006, http://tbbyayinlari.barobirlik.org.tr/TBBBooks/insan_haklari_evrensel_bildirisi.pdf, E.T. 28.08.2016.

⁴⁷ BEITZ, *The Idea of Human Rights*, s. 19.

⁴⁸ Osmanlı Devleti bakımından esas gaye, devletin dağılma ihtimali karşısında mevcut kitleleri yeni ilkeler etrafında toparlamak ve devlet faaliyetlerini bu ilkeler ışığında yürüterek farklı unsurlar arasında düzeni sağlamak olmuştur. Yavuz ABADAN, “Tanzimat Fermanı'nın Tahlili”, *Tanzimat: Değişim Sürecinde Osmanlı İmparatorluğu*, Halil İNALCIK, Mehmet SEYİTDANLIOĞLU, Türkiye İş Bankası Kültür Yayınları, 2014, s. 35, ss. 31- 59.

⁴⁹ ABADAN, “Tanzimat Fermanı'nın Tahlili”, *Tanzimat: Değişim Sürecinde Osmanlı İmparatorluğu*, s. 36.

dokunulmazlığı ve keyfilğin önlenmesi ile suç ve cezada kanunilik ilkesini çağrıştırması bakımından Osmanlı Devleti'nin Magna Cartası olarak kabul edenler mevcuttur⁵⁰.

Tanzimat Dönemi'ne gelindiğinde ise insan hakları kavramına dair ilk ve en önemli gelişme 1839 tarihli Tanzimat Fermanı'dır. Anılan Ferman, bugüne kıyasla çok sınırlı bir şekilde de olsa, bir hak kataloğu barındırmaktadır⁵¹. Genel itibarıyla bu düzenlemeler, can güvenliği, mal ve namus güvenliği, kişi güvenliği, yargılamasız suç ve ceza olmayacağı, mali güce göre vergilendirme ilkesi ve eşitlik ilkesidir⁵². Ayrıca siyaseten katl ve müsadere yöntemleri de kaldırılmıştır. Dolayısıyla bu Ferman doktrinde kimi yazarlar tarafından ilk temel haklar beyannamesi olarak da ele alınmaktadır⁵³. Özellikle söz konusu hakların İmparatorluk'ta yaşayan herkes için geçerli olduğuna dair eşitlik düzenlemesinin, eski İslam geleneklerinden köklü bir ayrılığı ifade ettiği ve insan hakları fikrinin tohumunu oluşturduğu söylenebilir.

Herkes için geçerli olan insan hakları kavramının Osmanlı Devleti'nde ve Tanzimat Dönemi'nde daha vurgulu bir yansıması olarak 1856 tarihli Islahat Fermanı da ele alınmalıdır. Müslümanlar ve gayrimüslimler arasında eşitliği vurgulamak gayesi ile çıkarılan Ferman'da, kamu hizmetlerine alımda ve askerlik hizmetlerinde eşitlik, kanun önünde eşitlik ilkesi, vergide eşitlik, eğitimde eşitlik, gayrimüslimlerin ibadetlerini rahatça yapabilmelerine dair güvence, tutukluluk ve hükümlülük koşullarının iyileştirilmesi, işkence ve eziyete son verilmesi gibi düzenlemeler getirilmiştir. Ancak bu

⁵⁰ Bülent TANÖR, *Osmanlı-Türk Anayasal Gelişmeleri*, YKY, 9. Bası, İstanbul, 2002, s. 59; Niyazi BERKES, *Türkiye'de Çağdaşlaşma*, Haz: Ahmet Kuyaş, YKY Yayınları, 7. Bası, İstanbul, 2004, s. 140; Abdullah SEZER, Emrah KIRIT, Oya BOYAR, *Hukuk Devleti*, Toplumsal Katılım ve Gelişim Vakfı, İstanbul, 2003, s. 66.

⁵¹ ABADAN, "Tanzimat Fermanı'nın Tahlili", *Tanzimat: Değişim Sürecinde Osmanlı İmparatorluğu*, s. 53.

⁵² SEZER, KIRIT, BOYAR, *Hukuk Devleti*, s. 67.

⁵³ Bernard LEWIS, *Modern Türkiye'nin Doğuşu*, Türk Tarih Kurumu, 8. Bası, İstanbul, 2000, s. 107; Coşkun ÜÇÖK, Ahmet MUMCU, Gülnihal BOZKURT, *Türk Hukuk Tarihi*, 14. Bası, Ankara, 2010, s. 331- 332.

kez de gayrimüslimlere yargılama alanında verilen bazı imtiyazlar sebebiyle eşitlik ilkesi Müslümanlar aleyhine sekteye uğramıştır⁵⁴.

Fermanların ardından Osmanlı Devleti'nin ilk Anayasası olan 1876 tarihli Kanun-i Esasi düzenlenmiştir. İnsan hakları fikrinin Türkiye'deki gelişimi açısından hem bir anayasanın yapılması hem de Anayasa'nın 8 ile 26. maddeleri arasında "Temel hak ve hürriyetler" başlıklı bir bölümün bulunması oldukça önem arz etmektedir. Bu bölümde eşitlik ilkesi, kişi dokunulmazlığı, suç ve cezada kanunilik ilkesi, konut dokunulmazlığı, eziyet, işkence ve müsadere ile angarya yasağı, basın özgürlüğü, tabii yargı ve hâkim ilkesi gibi düzenlemeler bulunmaktadır. Ancak Kanun-i Esasi'de ayrıca padişahın sürgün yetkisi bulunması, bu hakların anlamını sorgulatmış ve hatta kişi güvenliği bakımından Tanzimat Fermanı'nın bile daha ileride olduğu gibi yorumlara sebebiyet vermiştir⁵⁵. Kanun-i Esasi'de yapılan 1909 Değişiklikleri bağlamında padişahın söz konusu sürgün yetkisinin kaldırılması, kişi hak ve özgürlüklerinin Osmanlı Devleti'ndeki gelişimi açısından en önemli düzenlemesidir⁵⁶. Toplantı ve dernek kurma özgürlüğü de bu Değişiklikler ile getirilmiştir. Bu bakımdan 1909 Değişiklikleri ile 1876 Kanun-i Esasi temel hak ve özgürlükler bakımından daha anlamlı bir seviyeye ulaşmıştır⁵⁷.

Osmanlı Devleti ve dolayısıyla Türkiye bakımından insan haklarının tarihsel gelişimine bakıldığında 19. yüzyıl sonrasında Tanzimat Dönemi ile temel hak ve özgürlüklerin düzenlenme çabaları karşımıza çıkmaktaysa da çağdaşı devletlerde insan hakları kavramının gelişim sürecine bakıldığında bir parça daha geride kaldığı söylenebilecektir.

⁵⁴ ÜÇÖK, MUMCU, BOZKURT, *Türk Hukuk Tarihi*, s. 335.

⁵⁵ LEWIS, *Modern Türkiye'nin Doğuşu*, s. 166; ÜÇÖK, MUMCU, BOZKURT, *Türk Hukuk Tarihi*, s. 340.

⁵⁶ SEZER, KIRIT, BOYAR, *Hukuk Devleti*, s. 71.

⁵⁷ Ahmet MUMCU, Elif KÜZECİ, *İnsan Hakları ve Kamu Özgürlükleri*, Turhan Kitabevi, 5. Bası, Ankara, 2011, s. 175.

III. İNSAN HAKLARI VE İNSAN ONURU İLİŞKİSİ

Temel hak ve özgürlüklerin, belli bir ekonomik sınıfın (burjuvazi) mücadelesi neticesinde, belli bir ırk (beyaz ırk) ve cinsiyetin (erkek) mücadelesi şeklinde ortaya çıkarak oldukça geniş kitlelerce kabul edilmesinin sebebi, burjuvazinin bu savaşta yalnız kalmamak adına, sınıfsal ifadelerden uzak, tüm insanları içine alan evrensel bir söylemi esas almasında gizlidir⁵⁸. Bu haklardan bazı insanların yararlanabilmesini istemek, onları tüm insanlar için talep edilebilir hale getirmekle mümkün olmuştur⁵⁹. Bu bakımdan insan haklarının gerçek anlamda “evrensel” olabilmesi gerekmektedir. Bu ise, söz konusu hakların meşruiyetinin tüm insanların sahip oldukları özelliklerden kaynaklandığı ve akıl ve vicdan sahibi insanların ahlaki olarak eşit olduğu varsayımı ile mümkün olabilmektedir⁶⁰. Daha açık bir ifadeyle, insanlar arası farklılıklar ne olursa olsun, insani değerleri bakımından eşit olduklarını kabul ederiz⁶¹.

Ahlaki olarak eşitlik temelinde birleşen insan haklarının kaynağı, insan doğası ve insanlık kavramlarıdır⁶². Kaynağını insan doğasında bulan insan hakları, insanın değerini,

⁵⁸ UYGUN, *Devlet Teorisi*, s. 477- 478; Oktay UYGUN, “Çağımızın İnsan Onuruna Yönelttiği Tehditler Karşısında İnsan Haklarının Önemi”, *Kamu Hukuku İncelemeleri- İnsan Hakları, Demokrasi, Hukuk Devleti ve Egemenlik*, Oniki Levha Yayıncılık, İstanbul, 2013, s. 50, ss. 45- 83; Harovon SENER, “From the Limited to the Universal Concept of Human Rights: Two Periods of Human Rights”, *Human Rights and Cultural Diversity*, Keip Publishing, 1993, s. 47- 100.

⁵⁹ Belirtilmelidir ki, insan haklarının herkes için talep edilebilir olması fikri, öncelikle bireyin devlete karşı ileri sürebileceği taleplerin doğumuna sebep olmuştur. Bu ise, insan hakları ile korunan durumlarda bireyin devlete karşı önceliği olduğu liberal öğretiye dayanmaktadır. DONNELLY, *Teoride ve Uygulamada Evrensel İnsan Hakları*, s. 79. Ancak herkes için geçerli oldukları varsayımına dayanan insan hakları anlayışının bir yönü ile sürekli genişleyen insan hakları listeleri yaratıyor oluşunun belirsizliklere de yol açıyor olması bazı yazarlarca eleştirilen bir noktadır. Bkz. Harun TEPE, “İnsan Hakları: Kavram, Kapsam, Ölçüt”, *Disiplinlerarası Yaklaşımla İnsan Hakları*, Ed. Selda ÇAĞLAR, Beta, İstanbul, 2010, s. 4, ss. 1- 32.

⁶⁰ AKAD, VURAL DİNÇKOL, BULUT, *Genel Kamu Hukuku*, s. 254; SHESTACK, “The Philosophical Foundations of Human Rights”, s. 204.

⁶¹ Norman P. BARRY, *Modern Siyaset Teorisi*, Çev: Mustafa ERDOĞAN- Yusuf ŞAHİN, Liberte, Ankara, 2003, s. 262.

⁶² DONNELLY, *Teoride ve Uygulamada Evrensel İnsan Hakları*, s. 27.

daha açık bir ifadeyle insan onurunu korumak gayesini taşımaktadır⁶³. Detaylı bir ifadeyle, devletin mutlak iktidarı karşısında korunması gereken kişi hakları biçiminde doğan ve devletin söz konusu iktidarının, kişiye onurlu bir hayat sunulması için sınırlandırılması sonucunu doğuran insan hakları öğretisi, “*insan onuru*”nu korumak ilkesi üzerine inşa edilmiştir⁶⁴. İnsan hakları öğretilerinde insan haklarına sahip olmak, insan olmakla birdir⁶⁵. Bu bakımdan insan hakları, hiçbir ayırım olmaksızın, insanın yalnızca insan olmasından kaynaklı olarak, insan onurunun bir gereği olan haklardır. Bu bağlamda yöneldikleri amaç vesilesiyle, insan onurunu koruyan tüm hakların insan hakları olarak kabul edileceği dile getirilmektedir⁶⁶.

İnsan onuru kavramının felsefi açıdan temellendirilmesinde Kant’ın anlayışına değinmek insan onuru ve insan hakları ilişkisini anlamak bakımından önem taşımaktadır. Kant’a göre insan, ahlaki seçimler yapabilmesi ile diğer tüm canlılardan farklılık göstermektedir. İnsanın ahlaki seçimler yapabilmesi tüm insanlar için ortak bir özelliktir ve bu bakımdan insanları eşitler. İnsan Hakları Evrensel Bildirgesi’de 1. maddesinde, “*Bütün insanlar özgür, onur ve haklar bakımından eşit doğarlar. Akıl ve vicdana sahiptirler, birbirlerine karşı kardeşlik anlayışıyla davranmalıdırlar.*” derken Kant’ın söz ettiği ahlaki seçimler yapabilme özelliğini akıl ve vicdan sahibi olmak ile ilişkilendirmiştir⁶⁷. İnsan haklarına ilişkin başka bazı uluslararası belgelerde de “insan onuru” kavramı önemli bir yere sahiptir. Söz gelimi, gerek Medeni ve Siyasi Haklara İlişkin Uluslararası Sözleşmesi (1966), gerekse Ekonomik Sosyal ve Kültürel Haklara

⁶³ UYGUN, “Çağımızın İnsan Onuruna Yöneltiltiği Tehditler Karşısında İnsan Haklarının Önemi”, s. 46.

⁶⁴ Mehmet Merdan HEKİMOĞLU, “İnsan Haklarının Temelini Oluşturan ‘İnsan Onuru’ Kavramının Anayasal Boyutları: Federal Almanya Örneği”, *Kazancı Hakemli Hukuk Dergisi*, N: 71- 72, s. 102, 103; ERDOĞAN, Mustafa *İnsan Hakları Teorisi ve Hukuku*, Orion Kitabevi, Ankara, 2015, s. 56; UYGUN, *Devlet Teorisi*, s. 471.

⁶⁵ DONNELLY, *Teoride ve Uygulamada Evrensel İnsan Hakları*, s. 29.

⁶⁶ Oktay UYGUN, *Türkiye’de Demokrasi ve İnsan Hakları*, TODAİE İnsan Hakları Araştırma ve Derleme Merkezi, Ankara, 1996, s. 6; UYGUN, “Çağımızın İnsan Onuruna Yöneltiltiği Tehditler Karşısında İnsan Haklarının Önemi”, s. 46, ss. 45- 83; BULUT, *Sanayi Devriminden Küreselleşmeye Sosyal Haklar*, s. 11; AKILLIOĞLU, *İnsan Hakları: Kavram, Kaynaklar ve Koruma Sistemleri*, s. 6.

⁶⁷ UYGUN, “Çağımızın İnsan Onuruna Yöneltiltiği Tehditler Karşısında İnsan Haklarının Önemi”, s. 47-48.

İlişkin Uluslararası Sözleşme (1966) insan haklarının “...insanın doğuştan sahip olduğu insanlık onurundan türediğini kabul...” etmektedir⁶⁸.

Türk Dil Kurumu’na göre “onur” kelimesinin iki anlamı bulunmaktadır. Bunlardan ilki; “insanın kendine karşı duyduğu saygı, şeref, öz saygı, haysiyet, izzetinefis” tir. Onur kelimesinin ikinci anlamı ise; “başkalarının gösterdiği saygının dayandığı kişisel değer, şeref, itibar” dır⁶⁹. Buradan hareketle, insan hakları teorisinin evrenselliğinin anahtarı olan insan onuru da sübjektif ve objektif anlamları haiz bir kavram olarak karşımıza çıkmaktadır. Buna göre insan onuru, bir kimsenin hem kendisine verdiği hem de toplumun ona atfettiği değer olmakla birlikte ayrıca genel, soyut ve etik bir değerdir. Ancak insan hakları teorisinde esas olan insanın içinden, sırf insan olmasından gelen bir değer olan insan onurudur. İnsanın öz benliğinde yer alan onurun sağlanması insan hakları ile mümkün olabilecektir, çünkü bu haklar olmaksızın insana özgü değerli bir hayat sürdürülemez⁷⁰.

Bunun yanı sıra insan onuru, devletin hem negatif hem de pozitif tutumlarını gerektiren iki boyutlu bir kavramdır. Devletin negatif tutumunu gerektiren birinci boyut, bireyin devlete karşı korunmasını gerektirmektedir. Bu doğrultuda devletin insanı nesne yerine koymadan, aşağılayıcı cezalar vermeden ve insana küçük düşürücü muamele yapmadan, vücut bütünlüğüne ve kişisel dünyasına saygı göstermesi gerekmektedir. Bu fikir ise, hukuk devleti prensibinin ve bu bağlamda kişisel hakların doğumuna sebep olmuştur⁷¹.

Ancak zamanla, temelinde insan onurunu korumayı amaçlayan hukuk devleti ilkesi ve kişisel hakların insan onurunu korumak için yeterli olmadığı görülmüştür.

⁶⁸ DONNELLY, *Teoride ve Uygulamada Evrensel İnsan Hakları*, s. 74.

⁶⁹ Türk Dil Kurumu, *Güncel Türkçe Sözlük*, http://www.tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.57f2de20d49305.41451640, E.T. 03.10.2016.

⁷⁰ AKAD, VURAL DİNÇKOL, BULUT, *Genel Kamu Hukuku*, s. 254; AKILLIOĞLU, *İnsan Hakları: Kavram, Kaynaklar ve Koruma Sistemleri*, s. 5; DONNELLY, *Teoride ve Uygulamada Evrensel İnsan Hakları*, s. 28- 29.

⁷¹ BULUT, *Sanayi Devriminden Küreselleşmeye Sosyal Haklar*, s. 1.

Özellikle Sanayi Devrimi sonrası insanın adeta bir nesne olarak muamele görmesine bu kavramlar engel olamamıştır. İşte bu durumun yarattığı ortama ilişkin çözüm arayışları, devletin bireyi koruması gerektiği fikrini içeren sosyal devlet kavramının ortaya çıkışını ve sosyal hakların insan onurunu korumaya destekleyici gücünün fark edilmesini sağlamıştır⁷².

Bu bağlamda insan onuru kavramının anayasal sistemlerde temel bir hak ölçütüne dönüşmesi gerçekleşmiştir. İnsan onuru her ne kadar eski çağlardan beri var olan bir görüş olsa da anayasa, yasa ve hukuki belgelerde yer alması ancak 20. yüzyılda mümkün olabilmıştır. 1949 Bonn Anayasası, insan onurunu ele alması bakımından kendinden sonraki tüm hukuki metinlere bir temel oluşturmuştur. Bu bağlamda insan onuru kavramının Alman hukukundan kaynaklı olarak yayılım göstermesi aslında tesadüfi bir durum da değildir. Weimar Cumhuriyeti dönemi uygulamaları ile Nazi Dönemi ve ilgili dönemdeki insanlık dışı uygulamalar düşünüldüğünde Alman değer anlayışının insanın zincirlenmemiş tutkularından korku sonucu oluştuğu söylenebilecektir⁷³.

İnsan onurunun insan haklarının temelini oluşturduğu fikri doktrinde genel kabul görse de bunun aksini ileri sürenler de bulunmaktadır. Söz gelimi Van Dun’a göre insan onuru kavramı, insan haklarının neler olduklarını ve içeriklerinde nelerin yer aldığını ortaya koymamaktadır. İnsan haklarının objektif olarak içeriğinin ortaya konmaması sebebiyle ise insan onuru belirsiz bir hale gelmektedir⁷⁴.

⁷² DOĞAN, “İnsan Hakları Hukukunun Temel Kavramları ve Özellikleri”, *İnsan Hakları Hukuku*, s. 47; BULUT, *Sanayi Devriminden Küreselleşmeye Sosyal Haklar*, s. 1- 2.

⁷³ Edward J. EBERLE, “Human Dignity, Privacy and Personality in German and American Constitutional Law”, *Utah Law Review*, No:4, Y: 1997, s. 1053, ss. 963- 1056; DOĞAN, “İnsan Hakları Hukukunun Temel Kavramları ve Özellikleri”, *İnsan Hakları Hukuku*, s. 46- 48.

1919 Weimar Anayasası m. 151/1: “*Ekonomik yaşam, herkese onurlu bir yaşam sağlamak amacıyla adalet ilkelerine dayalı olarak organize edilmelidir.*”

Weimar Constitution, http://www.zum.de/psm/weimar/weimar_vve.php , E.T. 18.10.2016.

⁷⁴ Frank VAN DUN, “Human Dignity: Reason or Desire? Natural Rights versus Human Rights”, *Journal of Libertarian Studies*, C: 15, N: 4, s.14.

Genel olarak insan haklarının temel insani gereksinimlere denk düřtüğü dile getirilmektedir⁷⁵. Ancak hořa giden ve insanın çıkarına yönelik her řey, insan haklarının üstünlüğü ve ahlaki olarak bağlayıcılığını zayıflatabileceğı için, insan hakkı olarak nitelenemeyecektir⁷⁶. Özü itibarıyla ahlaki iddia ve talepler olan insan haklarının öğretilindeki temel sorulardan biri de neden bazı gereksinimler “hak” olarak görülürken, diğelerinin bu kavrama dahil olamadıklarıdır. Bunun anlamı, ilk olarak ortaya bir ihtiyacın çıkması ve devamında bunun bir hak talebi olarak gündeme gelmesidir⁷⁷. Söz gelimi ortada kişisel verilere ve mahremiyete yönelik tehdit ve saldırı var olduğunda bu kavramın korunmasına dair bir ihtiyaç doğar ve kişisel verilerin korunmasına ilişkin bir hakkın ortaya çıkışı gerçekleşir. Dolayısıyla insan haklarını ulusal ya da uluslararası belgeler yaratmaz. Bu gibi hukuki düzenlemeler yalnızca insanların sahip oldukları hakları tanımakla görevlidirler⁷⁸.

Fakat bu çıkarım her durum için geçerli olmayacaktır. Her gereksinimin bir hakkı karşılamadığı ya da tam tersi her hakkın bir gereksinime denk düşmediğı durumlar da mevcuttur. İnsan hakları öğretiline dinamizm katan en mühim özellik olarak karşımıza çıkan durum da henüz ihtiyaç duyulmamış; ancak yakın gelecekte doğabilecek bir gereksinim ve/ veya hak kategorileridir⁷⁹.

IV. İNSAN HAKLARININ SINIFLANDIRILMASI

Tarihsel süreçte insan onuruna yönelik tehditler sürekli farklılaştığından her dönemde yeni insan hakları ortaya çıkmaktadır⁸⁰. Bu ise, insan hakları öğretisinin daha kolay anlaşılmasını sağlamak için insan haklarının kategorik olarak incelenmesini gerektirmiştir. Ancak bu durum insan haklarının kendi içinde bir önem sırasına sahip

⁷⁵ UYGUN, *Devlet Teorisi*, s. 485; DONNELLY, *Teoride ve Uygulamada Evrensel İnsan Hakları*, s. 27 vd.

⁷⁶ ERDOĞAN, *İnsan Hakları Teorisi ve Hukuku*, s. 25.

⁷⁷ UYGUN, *Devlet Teorisi*, s. 486.

⁷⁸ ERDOĞAN, *İnsan Hakları Teorisi ve Hukuku*, s. 26.

⁷⁹ UYGUN, *Devlet Teorisi*, s. 486.

⁸⁰ UYGUN, “Çağımızın İnsan Onuruna Yönelttiğı Tehditler Karşısında İnsan Haklarının Önemi”, s. 51.

olduğu anlamına gelmemektedir. İnsan hakları ne şekilde sınıflandırılırsa sınıflandırılsın, bir bütündürler ve aralarında asla bir hiyerarşi bulunmamaktadır. Bir hakkın yokluğu diğer hakları da olumsuz etkiler⁸¹. Aralarından bazılarını çıkarmak ya da kategoriler arası önem düzeylerinin farklı olduklarını iddia etmek insan hakları öğretisine zarar verir. Bu bakımdan esas olan, hak kategorileri arasında ayrımcılık yapmaksızın, genel olarak insan haklarını korunma mekanizmalarını güçlendirmek olmalıdır. Bu durum ise, insan haklarının belirli kategorilere ayrılamayacağı anlamına gelmemelidir. Fakat bu ayrımların hangi kıstaslara dayanılarak yapılacağı sorusu belirsizlik taşımaktadır. Bu bakımdan doktrinde farklı ölçütlere dayanılarak çeşitli ayrımlar yapılmıştır⁸².

Ayrıca belirtilmelidir ki, özellikle toplumsal değişimler ve günümüz teknolojik, bilimsel gelişmeleri yeni insan hakkı kategorileri ortaya çıkarmakta ve bu durum farklı sınıflandırmaların da yakın gelecekte muhtemel olacağını göstermektedir. İşte bu nedenlerle, insan hakları tarihsel süreç içerisinde hukuki kaynağına veya ortaya çıkış dönemine göre belirli sınıflandırmalara tabi tutulabilmektedir.

A. JELLİNEK ÜÇLÜSÜ: POZİTİF/ NEGATİF/ AKTİF STATÜ HAKLARI

Georg Jellinek, insan haklarını bireylerin devletten beklentileri ve devlet karşısındaki konumuna göre üç farklı sınıfa ayırmıştır. Bu ayırım, insan hakları öğretisine önemli katkısının yanı sıra, öğretim kolaylığı bakımından da önem taşıyan bir sınıflandırmadır. Jellinek'e göre insan hakları, pozitif (olumlu) statü, negatif (olumsuz) statü ve aktif statü hakları olarak ayrılmaktadır⁸³. Pozitif ve negatif statü hakları, devletin insan haklarına müdahil olup olmama haline göre belirlenmekte iken, aktif statü hakları bunlardan farklı bir özellik arz etmektedir⁸⁴.

⁸¹ UYGUN, *Devlet Teorisi*, s. 499.

⁸² BULUT, *Sanayi Devriminden Küreselleşmeye Sosyal Haklar*, s. 3.

⁸³ DOĞAN, "İnsan Hakları Hukukunun Temel Kavramları ve Özellikleri", *İnsan Hakları Hukuku*, s. 55.

⁸⁴ Matthias KLATT, "Positive Rights: Who decides? Judicial Review in Balance", *International Journal of Constitutional Law*, Vol. 13, No: 2, Y: 2015, s. 355, ss. 354- 382.

İlk olarak vatandaşların devletten bazı edimleri yerine getirmesini beklediği grup pozitif statü haklarını oluşturmaktadır. Bireylerin yararlanırken devletin müdahalede bulunamayacağı hak grubu ise negatif statü haklarıdır. Detaylı bir anlatımla, negatif statü hakları, ifade özgürlüğü, konut dokunulmazlığı ya da din ve vicdan hürriyeti gibi, devlet tarafından dokunulamayacak özel alanının sınırlarını çizen hak ve hürriyetlerdir⁸⁵. Negatif statü haklarının en önemli özelliği, devletin müdahalesine karşı yargısal bağlamda bir talep hakkının doğmasını sağlamalarıdır. Şöyle ki, devlet karışmama yükümlülüğünü ihlal ettiği takdirde birey dava edebilme hakkına sahiptir. Pozitif statü hakları ise, eğitimin sağlanması, çevrenin korunması ya da çalışma hakkının mümkün kılınması gibi hakları içeren ve devletin yerine getirmesinin zorunlu addedildiği hakları içermektedir. Bu haklar devlete sosyal alanda birtakım ödevler yüklemektedir. Bunun sebebi ise, sanayileşme ile birlikte anayasal sistemlerde yer almaya başlamalarıdır⁸⁶. Bir başka ifade ile sosyal haklar da denilen pozitif statü hakları ise, devletin ekonomik gücü ile yakından ilgili olmaları dolayısıyla, negatif statü haklarına kıyasen ulusal ve uluslararası yargı bakımından dava edilebilirliği daha yeni ve zorlu bir hak kategorisini oluşturmaktadır⁸⁷.

Jellinek bu iki ayrıma ayrıca, aktif statü haklarını da eklemektedir. Buna göre bireylerin devlet yönetimine katılmalarını sağlayan haklara da aktif statü hakları denilmektedir. Bu bakımdan bu haklara “katılma hakları” da denir. Söz gelimi, seçme ve seçilme hakkı, dilekçe hakkı, kamu hizmetine girme hakkı gibi haklar aktif statü

⁸⁵ Münici KAPANİ, *Kamu Hürriyetleri*, Ankara Üniversitesi Hukuk Fakültesi Yayını, Ankara, 1981, s. 6.

⁸⁶ A. Şeref GÖZÜBÜYÜK, *Anayasa Hukuku*, Turhan Kitabevi, Ankara, 1998, s. 166- 167; DOĞAN, “İnsan Hakları Hukukunun Temel Kavramları ve Özellikleri”, *İnsan Hakları Hukuku*, s. 55.

⁸⁷ KLATT, “Positive Rights: Who decides? Judicial Review in Balance”, s. 355- 356.

Bu bakımdan uluslararası düzlemde önem taşıyan bir yenilik dile getirilmelidir. Buna göre, Ekonomik, Sosyal ve Kültürel Haklara İlişkin Sözleşme’nin İhtiyari Protokolü 2008 yılında kabul edilmiş ve 5 Mayıs 2013’te yürürlüğe girmiştir. İnsan hakları koruma mekanizması bakımından hayati önem taşıyan bu değişiklik sayesinde ekonomik, sosyal ve kültürel haklara dair ihlal iddiaları artık dava edilebilir hale gelmiştir. Irene BIGLINO, Christophe GOLAY, *The Optional Protocol to the International Covenant on Economic, Social and Cultural Rights*, Academy in-Brief, No: 2, Geneva Academy of International Humanitarian Law and Human Rights, Geneva, 2013, s. 3- 6, <http://www.geneva-academy.ch/docs/publications/The%20optional%20protocol%20In%20brief%202.pdf>, E.T. 31.10.2016.

haklarındandır. Bu noktada belirtilmelidir ki, aktif statü hakları da devlete olumlu veya olumsuz edim yükleyebilir⁸⁸.

B. VASAK'IN HAK KUŞAKLARI

İnsan hakları öğretisinde “Hak Kuşakları” olarak kabul gören söz konusu ayırım, 1979’da Karel Vasak tarafından yapılmıştır⁸⁹. Temelinde insan haklarını, tarihsel süreçte ortaya çıkış dönemlerine göre ayıran bu yapılanma (şimdilik) dört kuşak hak kategorisini vurgulamaktadır. Doktrinde bu sınıflandırmanın kabulünün temel olarak üç nedene dayandığı belirtilmektedir⁹⁰. Buna göre bu sınıflandırma, yukarıda da belirtildiği üzere, insan hakları öğretisinin tarihsel gelişimini yansıtmaktadır. Bu bağlamda hakların doğduğu ortamın ve sebeplerin anlaşılmasına yardımcı olur. Son olarak ise, hakların niteliklerine ilişkin başka ayrımlarla da kısmen örtüşebilmektedir.

Birinci kuşak haklar olarak isimlendirilen ilk grup, Amerikan ve Fransız Devrimleri ile kabul görmeye başlayan ve özgürlük kavramını esas alan medeni ve siyasi haklardır⁹¹. Buradaki temel özellik, kişinin belli bazı haklarına devlet ve toplum tarafından müdahale edilememesidir. Bu bakımdan pozitif bir karakterden ziyade, negatif bir nitelik gösterirler⁹². Bazı yazarlar, bunların tamamının tek bir hak olarak, “özgürlük hakkı” biçiminde bir adlandırmayla ele alınabileceğini düşünmüşlerdir. Birinci kuşak hakların oldukça cezbedici dünyası, zamanla bu haklardan yalnızca belli bir kesimin yararlanması (burjuvazi) ve insanların büyük çoğunluğunun yoksulluk nedeniyle bu

⁸⁸ GÖZÜBÜYÜK, *Anayasa Hukuku*, s. 151; Kemal GÖZLER, *Türk Anayasa Hukuku*, Ekin Yayınevi, Bursa, 2000, s. 210-211; DOĞAN, “İnsan Hakları Hukukunun Temel Kavramları ve Özellikleri”, *İnsan Hakları Hukuku*, s. 55.

⁸⁹ Karel VASAK, *Human Rights: A Thirty-Year Struggle: the Sustained Efforts to give Force of law to the Universal Declaration of Human Rights*, United Nations Educational, Scientific, and Cultural Organization, November 1977, s. 29.

⁹⁰ UYGUN, *Devlet Teorisi*, s. 493.

⁹¹ Lindsey REID, “The Generations of Human Rights”, *The University of Alabama at Birmingham Institute for Human Rights Blog*, <https://cas.uab.edu/humanrights/2019/01/14/the-generations-of-human-rights/> , E.T. 18.05.2019; UYGUN, *Devlet Teorisi*, s. 494; DOĞAN, “İnsan Hakları Hukukunun Temel Kavramları ve Özellikleri”, *İnsan Hakları Hukuku*, s. 57.

⁹² AKAD, VURAL DİNÇKOL, BULUT, *Genel Kamu Hukuku*, s. 287.

haklardan yararlanamaması durumunu doğurmuştur. Oysa insan hakları tarih sahnesine ilk çıktığında herkes için doğuştan geçerli oldukları fikrini getirmişti⁹³. Bu nedenle 19. yüzyılda Sanayi Devrimi'nin tarih sahnesinde yer bulması nedeniyle çekiciliğini yitirmiştir⁹⁴.

Her ne kadar tüm insanlar için oldukları söylense de asgari yaşam standartlarına sahip olamayan insanlar için birinci kuşak haklar bir miktar lüks kalmaktaydı⁹⁵. Bu nedenle insan hakları artık sadece bir özgürlük olarak değil, aynı zamanda devletten bir hizmet isteme yetkisi veren haklar olarak görülmeye başlanmıştır⁹⁶. Böylece eşitlik kavramını esas alan ikinci kuşak haklar doğmuştur⁹⁷. Bu haklar devlete bir kamu hizmeti tesis ve temini görevini yüklemektedir. Bu bakımdan devlet mali kaynaklarını kullanmalıdır. Ayrıca birinci kuşak hakların lokomotifi, belirtildiği üzere, burjuvazi iken; bu hak kategorisinin lokomotifi işçi sınıfı olmuştur. Söz konusu kategori, yoksul kimselerin insan haklarından tam olarak yararlandırılmasını amaçlamıştır⁹⁸. Bu durum, 1948 tarihli İnsan Hakları Evrensel Beyannamesi ve devamında 1966 tarihli BM İkiz Paktları ile de kayıt altına alınmıştır. Dolayısıyla anılan her iki hak kategorisi de insan onurunun korunması için geniş kitlelerce kabul gören ve artık herkesçe başvurulanan bir yol göstericidirler⁹⁹.

Bu konsensüs ortamına karşın, her iki hak kategorisine de bazı eleştiriler yöneltilmektedir. Öncelikle birinci kuşak haklar için her ne kadar devletin negatif bir tutum sergileyerek sağlanacakları dile getirilmişse de son yıllarda bazı hallerde devletin pozitif bir ediminin gerekeceği haller olduğu da gerek doktrinde gerek İnsan Hakları

⁹³ UYGUN, “Çağımızın İnsan Onuruna Yönelttiği Tehditler Karşısında İnsan Haklarının Önemi”, s. 52.

⁹⁴ Andrew VINCENT, *The Politics of Human Rights*, Oxford University Press, 2010, s. 132- 134.

⁹⁵ KAPANİ, *Kamu Hürriyetleri*, s. 51.

⁹⁶ UYGUN, “Çağımızın İnsan Onuruna Yönelttiği Tehditler Karşısında İnsan Haklarının Önemi”, s. 52.

⁹⁷ Lindsey REID, “The Generations of Human Rights”, *The University of Alabama at Birmingham Institute for Human Rights Blog*, <https://cas.uab.edu/humanrights/2019/01/14/the-generations-of-human-rights/> , E.T. 18.05.2019.

⁹⁸ AKAD, VURAL DİNÇKOL, BULUT, *Genel Kamu Hukuku*, s. 287.

⁹⁹ UYGUN, *Devlet Teorisi*, s. 496- 497.

Avrupa Mahkemesi içtihatlarında belirtilmektedir¹⁰⁰. İkinci kuşak haklarla ilgili temel tartışmalar ise dört ana başlıkta toplanılabilir. Öncelikle bir kısım yazar, insan haklarının yalnızca devletin negatif edimini gerektirmesi fikrinden yola çıkarak, devletin pozitif edimini gerektiren ikinci kuşak hakların insan hakkı olmadığını ileri sürmektedir. İkinci eleştiri noktası, ikinci kuşak hakların uygulanabilmelerinin ekonomik şartlara bağlı olmaları nedeniyle hak değil, arzulanabilir hedef olarak adlandırılabilirlerdir¹⁰¹. Bir diğer husus ise, birinci kuşak hakların ikinci kuşak haklardan üstün olduğu iddiasıdır¹⁰². Son olarak bir kısım düşünür, ikinci kuşak haklarla birinci kuşak hakların bağdaşmadığını ve ikinci kuşak hakların birinci kuşak hakları tahrip ettiğini iddia etmektedir¹⁰³.

Bu genel eleştirilerle birlikte¹⁰⁴, ilk planda insan haklarına dair kuşaklandırmanın yukarıda anılan iki türden oluştuğu kabul edilmekteyken, değişen tarihsel, ekonomik ve teknolojik koşulların etkisiyle insan onuruna yönelik tehditler değişmiş¹⁰⁵ ve sayılarak tüketilmeyen insan hakları artmıştır. Bu bağlamda İkinci Dünya Savaşı sonrası Westfalya

¹⁰⁰ Devletin pozitif yükümlülükleri için bkz. Oya BOYAR, “Devletin Pozitif Yükümlülükleri ve Dolaylı Yatay Etki”, *İnsan Hakları Avrupa Sözleşmesi ve Anayasa*, Ed. Sibel İNCEOĞLU, Avrupa Konseyi, Ankara, 2013, s. 53 v.d.

Kaldı ki Harris, O’Boyle & Warbrick, İHAM’ın ve doktrinin yapmış olduğu negatif- pozitif yükümlülük ayrımının yerine insan haklarına saygı (respect), koruma (protect) ve insan haklarını yerine getirme (fulfil) biçimindeki ayrımın daha anlamlı olduğunu dile getirmektedirler. David HARRIS, Michael O’BOYLE & Warbrick, *Law of the European Convention on Human Rights*, Oxford University Press, 2009, s. 21- 23.

¹⁰¹ VINCENT, *The Politics of Human Rights*, s. 150; UYGUN, *Devlet Teorisi*, s. 534.

¹⁰² Özellikle Cranston’a bakılacak olursa, klasik hakların evrensel, mutlak ve üstün olduğu belirtilirken, iktisadi ve sosyal hakların farklı bir mantıksal kategoriye ait oldukları vurgulanmaktadır. DONNELLY, *Teoride ve Uygulamada Evrensel İnsan Hakları*, s. 41- 44. Bu doğrultuda günümüze yakın bir düşünür olarak; Friedrich HAYEK, *Kanun Yasama Faaliyeti ve Özgürlük: Sosyal Adalet Serabı*, Çev: Mustafa ERDOĞAN, Türkiye İş Bankası Yayınları, İstanbul, 1995, s. 145.

¹⁰³ DONNELLY, *Teoride ve Uygulamada Evrensel İnsan Hakları*, s. 83.

¹⁰⁴ İkinci kuşak haklar bakımından dile getirilen bu temel eleştiriler dışında belirtilmesi gereken önemli bir husus, günümüzde sosyal hakların esasen küreselleşme nedeniyle tehlike altında oldukları iddiasıdır çünkü son yıllarda küreselleşme, ulus devletin sosyal amaçlı politikalar izlemesine engel olan bir süreç olarak karşımıza çıkmaktadır. AKAD, VURAL DİNÇKOL, BULUT, *Genel Kamu Hukuku*, s. 218- 219; Detaylı bir analiz için bkz. Selda ÇAĞLAR, *Küreselleşme Sürecinde Sosyal Hakları Yeniden Düşünmek*, *Maltepe Üniversitesi Hukuk Fakültesi Dergisi*, Vol. 1, Y: 2010, Maltepe Üniversitesi Yayınları, İstanbul, s. 211- 226.

¹⁰⁵ Teknolojinin hukuk ile etkileşimi ve teknoloji kullanımının hukukta yarattığı olumlu ve olumsuz dönüşüm için bkz. Abdullah DİNÇKOL, “Teknoloji ve Hukuk”, *Hukuk Felsefesi ve Sosyolojisi Arkivi*, S. 19, İstanbul Barosu Yayınları, 2010, s. 263- 278, ss. 248- 279.

modeli egemenlik anlayışının insan hakları lehine zayıflaması, uluslararası siyasi düzeni etkileyerek dayanışma kavramını temel alan grup hakları fikrini ortaya çıkarmış ve Birleşmiş Milletler düzleminde insan hakları olarak tanınmışlardır¹⁰⁶. Söz konusu bu haklar bilimsel ve teknik ilerlemelerin yarattığı çevre kirliliği, nükleer silahlar, ülkeler ve bölgeler arasında çok büyük farklılıklar arz eden gelişmişlik düzeyleri dayanışma hakları denilen üçüncü kuşak hakları ortaya çıkarmıştır¹⁰⁷.

Dayanışma hakları olarak da isimlendirilen üçüncü kuşak haklar, kolektif nitelikli haklardır. Bu hakların öznesi yalnızca bireyler değil, kolektif niteliği dolayısıyla topluluklar da olmaktadır¹⁰⁸. Bu hakların temel amacı insancıl bir toplum yaratma düşüncesidir. Bu bağlamda söz konusu hakların gerçekleşmesi yalnızca devletin görevi değildir. Ayrıca toplumda yaşayan herkesin kolektif katılımı gerekmektedir¹⁰⁹. Anılan grup, barış hakkı, su hakkı, gelişme hakkı veya çevre hakkı biçiminde oldukça geniş bir yelpazede yapılanmış ve dini, etnik, kültürel grupların talepleri ile de gerçekleşmiştir. Ayrıca kişiler, gruplar, devletler ve hatta sınıflar arasında bir dayanışmayı gerektirmektedir. Bu bakımdan “Dayanışma Hakları” olarak da isimlendirilirler¹¹⁰. Üçüncü kuşak hakların en önemli sorunu ise, henüz iyi bir biçimde formüle edilmemiş olmalarıdır¹¹¹. Daha açık bir ifade ile, bu hakların insan hakkı olup olmadıkları

¹⁰⁶ Lindsey REID, “The Generations of Human Rights”, *The University of Alabama at Birmingham Institute for Human Rights Blog*, <https://cas.uab.edu/humanrights/2019/01/14/the-generations-of-human-rights/> , E.T. 18.05.2019; UYGUN, *Devlet Teorisi*, s. 550.

¹⁰⁷ UYGUN, “Çağımızın İnsan Onuruna Yöneltiltiği Tehditler Karşısında İnsan Haklarının Önemi”, s. 53-54.

¹⁰⁸ Birinci ve ikinci kuşak haklara bakıldığında içlerinde kolektif boyutu olan haklar mevcuttur. Söz gelimi birinci kuşak haklardan olan dernek kurma hakkı ile toplantı ve gösteri yürüyüşü düzenleme özgürlüğü kullanımları bakımından kolektiftirler. İlâveten ikinci kuşak haklardan çalışma hakkı, eğitim hakkı gibi haklar gerçekleştirilmeleri bakımından kolektif özellik gösterirler. UYGUN, *Devlet Teorisi*, s. 552.

¹⁰⁹ AKAD, VURAL DİNÇKOL, BULUT, *Genel Kamu Hukuku*, s. 288.

¹¹⁰ Christian TOMUSCHAT, *Human Rights: Between Idealism and Realism*, Oxford University Press, 2008, s. 54.

¹¹¹ Üçüncü kuşak haklara ilişkin özellikle hakkın öznesi hususunda bazı eleştiriler yükselmektedir. Buna göre, üçüncü kuşak hakların öznesi olarak insan değil de gruplar, halklar gibi kolektif varlıkların hakları olarak nitelendirilmesinde insan hakları teorisinde oldukça keskin bir zemin kaymasına sebep olabileceği kaygısı vurgulanmıştır. Dolayısıyla kolektif varlıkların hakları insan hakkı olarak nitelendirilmemelidir. DONNELLY, *Teoride ve Uygulamada Evrensel İnsan Hakları*, s. 155.

konusunda bir birlik bulunmamakta ve tam olarak hangi hakların bu kategoriye girdiği belirlenmemektedir¹¹².

Vasak'ın ortaya attığı hak kuşaklarının bu incelemesinden anlaşılmaktadır ki, insan onuruna karşı oluşan tehditler her dönemde farklılık göstermektedir. Bu nedenle üçüncü kuşak haklar bir “son durak” olmamıştır ve hak kuşaklarının devamı olarak dördüncü ve hatta beşinci kuşak haklardan giderek daha yüksek sesle söz edilmektedir¹¹³. Bu bağlamda Kant'ın dile getirdiği ahlaki seçimler yapabilme kapasitesine sahip akıllı ve vicdanlı insanın maruz kaldığı tehditler her devirde farklılık arz etmektedir. Dolayısıyla ortaya çıkan önemli tehditlere karşı yeni hakların formüle edilmesi gayreti dördüncü ve hatta beşinci kuşak haklardan söz edilmesine sebep olmaktadır¹¹⁴.

C. HABERMAS'IN SINIFLAMASI

Günümüzde ise Jürgen Habermas insan haklarını, bireysel özgürlük hakları, hukuki ve siyasi katılım hakları ile sosyal katılım hakları olarak üçe ayırmaktadır¹¹⁵.

Devletin bireylere ve bireylerin birbirine karşı saygı gösterme yükümlülüğünün bulunduğu haklar, bireysel özgürlük haklarını oluşturur. Bunlardan bazıları, özel yaşamın gizliliği hakkı, kölelik yasağı, toplantı ve gösteri yürüyüşü hakkı gibi haklar iken; ayrıca masumiyet karinesi, düşünce ve inanç özgürlüğü, mülkiyet hakkı gibi Fransız İnsan ve Yurttaş Hakları Bildirgesi'nde yer alan haklar da bu kapsamdadır. Hukuki ve siyasi katılım hakları ise, yargılamanın aleniliği, seçme ve seçilme hakkı, topluca düşünce açıklama hakkı gibi hakları içerir. Bir bakıma sosyal haklar da denen sosyal katılım

¹¹² UYGUN, *Devlet Teorisi*, s. 497; Bülent ALGAN, “Rethinking ‘Third Generation’ Human Rights”, *Ankara Law Review*, Vol. 1, No: 1, Y. 2004, s. 126- 150, ss. 121- 155.

¹¹³ UYGUN, *Devlet Teorisi*, s. 499; Dördüncü kuşak haklar için bkz. V. A. Başlığı.

¹¹⁴ UYGUN, “Çağımızın İnsan Onuruna Yöneltiltiği Tehditler Karşısında İnsan Haklarının Önemi”, s. 51.

¹¹⁵ “Jürgen HABERMAS”, *Internet Encyclopedia of Philosophy*, <https://www.iep.utm.edu/habermas/>, E.T. 21.05.2019.

hakları ise, sosyal güvenlik hakkı, çalışma hakkı, eğitim hakkı, konut hakkı gibi haklardan meydana gelmektedir¹¹⁶.

V. BİR İNSAN HAKKI OLARAK KİŞİSEL VERİLERİN KORUNMASININ DOĞUŞU

İnsan haklarının sahneye çıkışlarını esas alan sınıflandırma insan onuruna karşı yönelen tehditlere bir cevap niteliğindedir. Dördüncü kuşak haklar da bu sınıflandırmada günümüz teknolojik ve bilimsel gelişmelerinden etkilenecek şekilde ortaya çıkmıştır. Söz konusu bilişim teknolojilerinin ortaya çıkışı ve gelişmesi sonucu ilk planda mahremiyet kavramı doğrudan tehdide maruz kalmış ve mahremiyetin korunması gereği fikri doğmuştur. Bu bakımdan çalışmamızın bu başlığında, dördüncü kuşak hakların bilişim teknolojileri ile ilişkisi ortaya konulduktan sonra, mahremiyet kavramının gerek Avrupa gerekse Amerika ölçeğinde tarihsel süreçteki anlayışları incelenecektir. Bu vesile ile mahremiyetin korunmasından kişisel verilerin korunmasına evrilen veri koruma hukuku sürecinin doğuşu ortaya konulmaya çalışılacaktır.

A. DÖRDÜNCÜ KUŞAK HAKLAR VE BİLİŞİM TEKNOLOJİSİ

Yukarıdaki başlıkta Vasak'ın 1979 yılında gerçekleştirdiği üçlü kuşak ayrımını ele alınmıştır. Genel itibarıyla tarihsel sürecin ön plana çıktığı kuşaklar arası sınıflama, doktrinde oldukça benimsenmiş görünmektedir. Bu doğrultuda zamanla insan onuruna karşı yönelen tehditler çeşitlenmiş ve 21. yüzyıla birlikte başka hak talepleri ortaya çıkmıştır. Yeni haklar için hem zamansal hem de niteliksel olarak ilk üç kuşak harici bir nitelermeye ihtiyaç duyulmuş ve dördüncü kuşak hak kategorisi doğmuştur. Bazı yazarları

¹¹⁶ David INGRAM, "Of Sweatshops and Subsistence: Habermas on Human Rights", *Ethics & Global Politics*, Vol. 2, No: 3, Y: 2009, s. 200, ss. 193, 217; DOĞAN, "İnsan Hakları Hukukunun Temel Kavramları ve Özellikleri", *İnsan Hakları Hukuku*, s. 59.

bir kenara bırakarak¹¹⁷ genel kabule göre “şimdilik” son denilebilecek bir kategori olarak dördüncü kuşak haklardan söz edilmektedir.

İnsanın varoluşu, 20 ve 21. yüzyıllarda teknolojik ve bilimsel gelişmelerin ulaştığı düzey nedeniyle hem bir atılım sürecinde hem de büyük bir risk altındadır¹¹⁸. Özellikle biyoteknolojik gelişmelerin insan doğasına ilişkin ulaştığı nokta ve bilişim teknolojisinin insanın özel yaşamına dahli düşünüldüğünde, insan onuru bugüne dek karşılaşmadığı ve ulaşacağı boyutları da öngörülemeyen bir tehditle karşı karşıya kalmıştır¹¹⁹. İşte bilim ve teknolojinin yarattığı tehlikeler neticesinde zarar görme ihtimali olan insan onurunun korunması için ortaya çıkan haklar dördüncü kuşak haklar olarak adlandırılmaktadır¹²⁰.

Dördüncü kuşak hakların neler olduğu kesin bir biçimde belli olmasa da bazı yazarlarca, farklı olma hakkı, biyoetik haklar, siber uzay hakkı, ayırım yapılmaksızın tüm yurttaşları temsil eden demokratik bir siyasal rejimde yaşama hakkı, su hakkı dile getirilmiştir¹²¹. Bunlar dışında, BM Konvansiyonu’nun 1989’da çocuk hakları arasına aldığı; ihmal, kıyım, sömürü ve ayrımcılığa karşı koruma hakkı, zorunlu ve bedelsiz eğitim hakkı, akıl ve fizik sağlığı hakkı, oyun hakkı, engelli çocukların özel eğitimden yararlanma hakkı gibi haklar da dördüncü kuşak insan hakları arasında sayılmıştır¹²².

Her ne kadar yukarıda belirtilen haklar çeşitli yazarlarca dördüncü kuşak haklar arasında sayılıyor olsa da bu kategorinin şimdiye dek çerçevesi belirlenmiş örnekleri

¹¹⁷ Kimi yazarlar halklar, etnik gruplar veya azınlıkların haklarını kolektif haklar olarak üçüncü kuşak haklar olarak, hayvan haklarını dördüncü kuşak haklar olarak, çevre hakkını da beşinci kuşak hak olarak nitilemektedir. Bkz. VINCENT, *The Politics of Human Rights*, s. 139- 143, 147.

¹¹⁸ DİNÇKOL, “Teknoloji ve Hukuk”, *Hukuk Felsefesi ve Sosyolojisi Arkivi*, s. 263- 278; Özellikle küreselleşme sürecinde ortaya çıkan yeni olgular ve insan hakları anlayışı için bkz. Abdullah DİNÇKOL, “Küreselleşme ve İnsan Hakları”, *Doç. Dr. Mehmet SOMER’e Armağan*, Marmara Üniversitesi Hukuk Fakültesi Yayını, 2006, s. 884, 897, 905, ss. 879- 919.

¹¹⁹ UYGUN, *Devlet Teorisi*, s. 558 vd.

¹²⁰ AKAD, VURAL DİNÇKOL, BULUT, *Genel Kamu Hukuku*, s. 288; UYGUN, “Çağımızın İnsan Onuruna Yöneltiltiği Tehditler Karşısında İnsan Haklarının Önemi”, s. 71.

¹²¹ İlker GÜNDÜZÖZ, “Yeni Kuşak İnsan Hakları Çerçevesinde Türkiye’de Mülki İdare Amirliğine Analitik Bir Yaklaşım”, *İnsan Hakları Yıllığı*, C.: 33, Y: 2015, ss. 19- 33, s. 25.

¹²² Can HAMAMCI, “Üçüncü Kuşak İnsan Hakları”, *Yeni Kuşak İnsan Hakları*, Ed. Ertan Kırılcım Akkoyunlu, TODAİE Yayın No: 371, 2013, ss.1-237, s. 53.

olarak, bilimin kötüye kullanılmaması hakkı bağlamında kişisel bütünlük hakkı ve tezimizin konusunu oluşturan kişisel verilerin korunması hakkı sayılmaktadır¹²³.

Özel yaşamın gizliliği denen kavram 1970’li yıllara dek kişiye, geçerli bir neden olmaksızın, kendisi ile ilgili birçok bilgiyi (ad, adres, yaş, cinsel yönelim, malvarlığı, adli sicil kaydı, parmak izi vb.) açıklamama imkânı ve hakkı vermektedir. Ancak bu yıllarla birlikte teknolojik gelişmelerin hızı öyle bir noktaya geldi ki, artık tüm bu bilgiler kamu ya da özel bir şirkete ait olan veri bankalarında tutulmaya başlanmıştır. Hatta zamanla internetin ve sosyal medyanın cazibesine kapılan insanoğlu, mobil iletişim araçları ya da bilgisayarlar vasıtasıyla çoğu zaman farkında olmaksızın bu bilgileri kendisi vermiş ve artan bir ivme ile vermeye devam etmektedir. Bu bağlamda yeni iletişim teknikleri mahremiyeti oldukça risk altına sokmaktadır. Belki de yakın bir gelecekte insanlar özellikle sosyal medyanın da etkisi ile değişen algıları sebebiyle iletişimin gizliliğinin özel yaşam kavramı içerisinde değerlendirmeyecektir¹²⁴.

Doğaldır ki bu durum, önceleri daha geniş bir biçimde ele alınan mahremiyet kavramının dönüşümüne de sebep olmaktadır. Özellikle internet ve sosyal medya kullanımı ile mahrem algısı değişmiş ve özel yaşamın gizliliği hakkının koruduğu alan daralmıştır. Ayrıca hukuk sistemleri de kişilerin internette bıraktıkları izlerin takibini şimdilik hak ihlali olarak görmemektedir. İnternet ortamındaki hareketlerin rıza dışında izlenmesinin hak ihlali olarak görüldüğü ihtimalde dahi, özellikle failin belirlenmesinin çok güç olması, durumu daha da zorlaştırmaktadır¹²⁵. Bu noktada temel bir insan hakkı olan özel yaşamın gizliliğinin sürdürülmesi ve insan onurunun korunması oldukça zorlaşmıştır. Dolayısıyla bilişim teknolojisinin insan onurunu tehlikeye düşüren bu güncel ve her gün daha şiddetli tehdidine karşılık, özel yaşamın gizliliği hakkının korunması için etkili denetim mekanizmalarının oluşturulması meselenin odak noktasını teşkil etmiştir. Fakat artık insanın doğmadan önce ve ölümünden sonra dahi izlenebiliyor

¹²³ UYGUN, *Devlet Teorisi*, s. 498- 499, 568- 571.

¹²⁴ UYGUN, “Çağımızın İnsan Onuruna Yöneltili Tehditler Karşısında İnsan Haklarının Önemi”, s. 64-65.

¹²⁵ UYGUN, *Devlet Teorisi*, s. 567.

ve kiři ile ilgili birçok verinin kayıtlanabiliyor olması sebebiyle önemi daha iyi anlaşılmıř ve yalnızca özel yařamın gizlilięi veya dięer bařka haklar baęlamında korunmasının yeterli olmayacaęı ortaya çıkmıřtır.

Tam da bu noktada, biliřim teknolojisinin ulařtıęı düzey dolayısıyla kiřinin özel yařamını korumanın bu karmařıklıęı karřısında kiřiye ait verilerin kayıtlanması, saklanması ve en önemlisi korunması için dördüncü kuřak haklardan olan kiřisel verilerin korunması hakkı karřımıza çıkmaktadır.

B. BİLİřİM TEKNOLOJİSİ KARřISINDA ÖZEL YAřAMIN GİZLİLİęİ VE KORUNMASI

Samuel D. Warren ve Louis D. Brandeis tarafından ilk defa 1890 yılında adlandırılan özel yařamın gizlilięi hakkı “yalnız bırakılma hakkı” olarak ele alınmıřtır¹²⁶. Bu hakkın temelinde kiřinin kendi ile ilgili bilgileri bařkaları ile paylařma yetkisinin kendinde olması kastedilmektedir. Dolayısıyla kiřisel verilerin korunması kavramının özel yařamın içinde doęup gelişmesi kesinlikle bir tesadüf deęildir.

Genel olarak kiřiye dair verilerin korunması denildięinde önceleri özel yařamın gizlilięi ve korunması hakkı akla gelmekteydi. Bunun en önde gelen sebebi, kavramın oldukça geniř ve kapsayıcı bir biçimde ortaya çıkmıř olmasıdır. Fakat özel yařam kavramının bu denli geniř olması, onu “kapsamlı bir tanım yapmaya elveriřsiz” kılmıřtır¹²⁷.

Özel yařama dair bir tanım yapmanın zorluęu sebebiyle kavram genel olarak iç içe geçmiř çemberlere benzetilerek anlatılmaya çalıřılmıřtır¹²⁸. Söz konusu çemberler, kamuya açık yařam alanı olan “Genel Yařam Alanı”, belirli kimselerle ve belirli

¹²⁶ Samuel WARREN, Louis BRANDEIS, “The Right to Privacy”, Harvard Law Review, Vol. 4, No: 5, Y. 1890, s. 214, ss. 193- 220.

¹²⁷ *Bensaid v. United Kingdom*, Par. 47, Application No: 44599/98, 06.05.2011, <http://hudoc.echr.coe.int/eng?i=001-59206>, E.T. 29.09.2017.

¹²⁸ Elif KÜZECİ, *Kiřisel Verilerin Korunması*, Gözden Geçirilmiş ve Yenilenmiş 2. Baskı, Turhan Kitabevi, 2018, s. 74.

ölçülerde paylaşılan “Kişinin Özel Yaşam Alanı” ve kişinin yalnızca kendine saklamak istediği alan olan “Sır Alanı”dır¹²⁹. Bu bağlamda doktrinde özel yaşamı,

“kişinin mutlak olarak gizli tuttuğu yaşam parçaları ile herkesin bilmesini uygun bulmadığı, yalnız kendi seçeceği kişilerle, belirlediği ölçü ve biçimde paylaşacağı yaşam parçalarının birlikte oluşturdukları yaşam alanı”

şeklinde tanımlama çabaları da mevcut olmuştur¹³⁰.

İnsan Hakları Avrupa Mahkemesi’ne göre özel yaşam kavramını tanımlama çabası gereksiz ve imkânsızdır¹³¹. Ancak bir fikir edinebilmek adına kapsamına giren bazı örneklerden yola çıkılabilir. Söz gelimi kişinin giyinme tarzı, cinsel yönelimi, doğum kontrolü, konutunun dokunulmazlığı, iletişimin denetlenmesi gibi pek çok husus özel yaşam bağlamında ele alınmaktadır¹³². Bu durum aslında kişisel verilerin korunması hususu bakımından da Mahkeme’ye geniş bir hareket alanı tanımıştır. İHAS’ın hazırlandığı esnada henüz mevcut olmayan ve teknolojik gelişmeler ışığında bir risk unsuru oluşturan DNA profilleri, kişiye ait verilerin kayıt altına alınması, bunlara yetkisiz kişilerin erişimi ya da gereken sürede imha edilmemeleri gibi kişisel verilerin korunması hakkı kapsamında değerlendirilen tüm durumlar, Sözleşme’nin güncel gelişmelerin ışığında değerlendirilmesi ilkesi ile de oldukça geniş bir biçimde ele alınan özel yaşamın gizliliği hakkı kapsamında değerlendirmektedir¹³³.

1950’de imzalanıp 1953’te yürürlüğe giren İHAS için durum böyle olmakla birlikte, 2000 yılında onaylanan Avrupa Birliği Temel Haklar Şartı’nda md. 7 “Özel ve

¹²⁹ Alan F. WESTIN, *Privacy and Freedom*, Atheneum, New York, 1970, s. 33 vd.

¹³⁰ Oya ARASLI, *Özel Yaşamın Gizliliği Hakkı ve T.C. Anayasasında Düzenlenişi*, Ankara, 1979, (Yayımlanmamış Doçentlik Tezi), s. 4.

¹³¹ *Niemietz v. Germany*, Par. 29, Application No: 13710/88, 16.12.992, <http://hudoc.echr.coe.int/eng?i=001-57887>, E.T. 29.09.2017.

¹³² Sultan ÜZELTÜRK, *1982 Anayasası ve İnsan Hakları Avrupa Sözleşmesine Göre Özel Hayatın Gizliliği Hakkı*, Beta, İstanbul, 2004, s. 3-5.

¹³³ İnsan Hakları Avrupa Mahkemesi ve kişisel verilerin korunması ilişkisi için bkz. II. Bölüm, B. 3. Başlığı.

Aile Yaşamına Saygı” Hakkını düzenlerken md. 8 “Kişisel Bilgilerin Korunması” Hakkını ayrı bir düzenleme olarak ele almıştır¹³⁴.

Zamanla güncel teknolojik gelişmeler sebebiyle özel yaşamın gizliliğinin korunması hakkının içinde yeşerip gelişen kişisel verilerin korunmasının münhasır bir hak kategorisi olarak düzenlenmesi, dünya genelinde birçok anayasal düzenlemede de karşımıza çıkmaktadır¹³⁵. Yakın tarihli olanlardan söz gelimi, 2008 tarihli Hollanda Anayasası’nın 10. maddesinin ilk fıkrası her ne kadar özel yaşama saygı hakkını içeriyor olsa da ikinci ve üçüncü fıkralarında bağımsız bir hak olarak kişisel verilerin korunması hakkı düzenlenmektedir¹³⁶. 2005 Değişiklikleri ile Portekiz Anayasası’nın “Bilgi Edinme Hakkı” yan başlık ve “Bilgisayarların Kullanımı” başlıklı 35. maddesine bakıldığında, kişisel veri kavramının hem otomatik hem de manuel biçimde tutulan dosyalarca korunmasını düzenlediği görülmektedir¹³⁷. 1982 tarihli Türkiye Cumhuriyeti Anayasası da 2010 yılında gerçekleştirilen değişiklik neticesinde, Hollanda Anayasası’na benzer bir biçimde kişisel verilerin korunması hakkını, özel yaşamın gizliliği başlıklı 20. maddenin 3. fıkrasında ayrı bir hak olarak ele almıştır. Bu düzenlemeye göre;

“Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir.

Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme

¹³⁴ Charter of Fundamental Rights of The European Union, (2000/C 364/01), 18.10.2000, http://www.europarl.europa.eu/charter/pdf/text_en.pdf, E.T. 10.03.2018.

¹³⁵ Arjantin Federal Anayasası Bölüm 43, http://www.wipo.int/wipolex/en/text.jsp?file_id=282508, E.T. 12.03.2018; İspanya Anayasası Md. 18/4, http://www.congreso.es/portal/page/portal/Congreso/Congreso/Hist_Normas/Norm/const_espa_texto_ingles_0.pdf, E.T. 15.03.2018; Portekiz Anayasası Md. 35, <http://www.en.parlamento.pt/Legislation/CRP/Constitution7th.pdf>, E.T. 15.03.2018; Rusya Federasyonu Anayasası md. 24/1, <http://www.constitution.ru/en/10003000-03.htm>, E.T. 15.03.2018; Ukrayna Anayasası Md. 32/2, https://www.justice.gov/sites/default/files/eoir/legacy/2013/11/08/constitution_14.pdf, E.T. 15.03.2018.

¹³⁶ Hollanda Anayasası Md. 10, <https://www.government.nl/documents/regulations/2012/10/18/the-constitution-of-the-kingdom-of-the-netherlands-2008>, E.T. 12.03.2018.

¹³⁷ Portekiz Anayasası Md. 35, https://www.constituteproject.org/constitution/Portugal_2005.pdf, E.T. 17.05.2019.

ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar.

Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.”

Tüm bu örnekler göstermektedir ki, kişisel verilerin korunması özel yaşamın gizliliği hakkının içerisinde vücut bulmakla beraber zamanla bağımsız bir hak olarak kendini göstermektedir. Bu bakımdan Adalet Divanı ve İnsan Hakları Avrupa Mahkemesi’nin kararlarının yer aldığı İkinci Bölüm, özellikle Avrupa Veri Koruma Hukuku’nun gelişiminde özel yaşamın gizliliği içerisinde doğup gelişen bu hakkın nasıl ayrı bir hak kategorisi oluşturduğunu ele alacaktır.

C. KAVRAMIN ORTAYA ÇIKIŞ NOKTASI OLARAK: MAHREMİYET

Mahremiyet kavramı, kişisel verilerin korunması fikrinin oluşumunun çıkış noktası olarak ele alınmaktadır. Fakat kavramın tanımına ilişkin doktrinde birçok görüş ortaya atılmıştır.

“Mahremiyet” fikrinin birden fazla yönü vardır. Öncelikle belirtmelidir ki, mahremiyet (privacy)¹³⁸, Latince “privatus” kelimesinden türemiştir. Ayrıca yine bu kökenden gelen “privatum” kelimesi de ev gibi özel varlıkları içeren bir anlamı karşılamaktadır. Bu bağlamda mahremiyet, kamusal olanın (public) karşıtı, bireyin ve hatta kamu yaşamından çekilmiş olan basit bir vatandaşın talebi olarak ele alınmıştır¹³⁹.

Yukarıda belirtildiği üzere mahremiyet ilk planda halka, kamuya açık olmayan anlamındadır. Bu bakımdan mahremiyet, kamu ile ilgili olmayan, söz gelimi aile yaşamı ya da ev gibi unsurları içermektedir. Yine bu doğrultuda mahremiyet kapalı, gizli,

¹³⁸ İngilizce’de mahremiyet anlamına gelen “privacy” kelimesinin 16. Yüzyıl öncesinde nadiren kullanıldığı belirtilmektedir. Gloria Gonzales FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Law, Governance and Technology Series 16, Springer International Publishing, 2014, s. 22.

¹³⁹ Ferdinand David SCHOEMAN, *Privacy and Social Freedom*, Cambridge University Press, 2008, s. 116.

mühürlü, erişilemeyen, özel bir alanı simgelemektedir. Buna göre doktrinde her ne kadar özel ile kamusal ayrımının sınırları keskin biçimde belirlenemese de bu iki düzlem arasında mutlaka bir ayrım olması gerektiği belirtilmiştir¹⁴⁰. Fakat Nissenbaum gibi bazı yazarlar, kamusal düzlemde dahi belli bir mahremiyetin korunması gerektiğini ileri sürmüşlerdir¹⁴¹. Öte yandan Gavison’a göre mahremiyet, bireye erişime ilişkin bir sınırlamadır¹⁴². Bireysel mahremiyet olarak düşünüldüğünde ise kişinin istediği biçimde yaşayabileceğinin kabulü anlamında özel yaşamına saygı duyulması, başkaları tarafından kontrol edilememesi, yabancılaştırılmaması şeklinde tanımlanmaktadır¹⁴³. Dolayısıyla mahremiyet, özgürlük ile doğrudan ilgilidir. Doktrinde Sofsky gibi bazı yazarlar mahremiyetin, kişisel özgürlüğün kalesi olduğunu dile getirmektedir¹⁴⁴. İlaveten mahremiyet, erken dönem Hristiyanlığı ile oluşturulmaya çalışılan, Orta Çağ boyunca gelişmeye başlayan, Aydınlanma Çağı’nda daha da yer eden ve modern anayasacılıkla ilerleme kaydeden birey kavramının inşasının sonucu olarak bireysellikle de doğrudan bağlantılıdır¹⁴⁵.

Yukarıda genel itibarıyla ele alınan düşüncelerin aksine, doktrinde bir kısım yazar da mahremiyet kavramını, kamuya ait olanın tam karşıtı biçiminde ele almanın doğru olmadığını belirtmektedirler. Çünkü söz konusu kamuya ait olan- mahrem ayrımı, özellikle kadınlar bakımından yıkıcı sonuçlara yol açabilecek, kişiyi kamusal yaşamdan dışlayıcı sonuçlar doğurabilecektir. Bu yazarlara göre insanın ihtiyacı “mahrem bir yaşam”dan ziyade kendi dilediği biçimde yaşamaktır¹⁴⁶.

¹⁴⁰ Peter BLUME, *Protection of Informational Privacy*, International Specialized Book Service Incorporated, DJOF Publishing, 2002, s. 1.

¹⁴¹ Helen NISSENBAUM, *Privacy in Context: Technology, Policy and the Integrity of Social Life*, Stanford University Press, 2010, s. 217.

¹⁴² Ruth GAVISON, “Privacy and the Limits of Law”, *The Yale Law Journal*, Vol. 89, No: 3, ss. 421- 471, s. 428.

¹⁴³ FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, s. 22.

¹⁴⁴ Wolfgang SOFSKY, *Privacy: A Manifesto*, Princeton University Press, 2008, s. 30.

¹⁴⁵ Lee A. BYGRAVE, *Data Protection Law: Approaching its Rationale, Logic and Limits*, Kluwer Law International, 2002, s.133.

¹⁴⁶ Colin J. BENNETT, Charles D. RAAB, *The Governance of Privacy: Policy Instruments in Global Perspective*, The MIT Press, 2006, s. 21.

Mahremiyet kavramı, insan onuru ile de ilgilidir. Bireyin kendini özgür bir biçimde geliştirebilmesi, doğasına içkin olan bir özelliğidir. Bu nedenle insan onuru, kişinin kendi kaderini tayin edebilmesi, kendi geleceğini belirlemesi kabulünü de içermektedir. Kaldı ki bireysellik de kişiliğin tam anlamıyla gelişimi ile tanımlanmaktadır. Netice olarak da mahremiyet, kişiliğin bütünüyle gelişimine olanak tanımaktadır. Bu bağlamda çalışmamızın konusu ile de doğrudan ilgili olması sebebiyle mutlaka belirtilmelidir ki mahremiyet, kişisel bilgiler üzerinde kontrolü sağlar¹⁴⁷.

“Özel Yaşamın Korunması/ Mahremiyet Hakkı”nın karşılaştırmalı anayasa hukukunda tanınması ise, konut dokunulmazlığı, iletişimin gizliliği gibi kavramların ortaya çıkmasını takip eden, nispeten geç bir gelişme olmuştur. Fakat tanınması ile birlikte, bir şemsiye hak olarak ele alınmıştır¹⁴⁸.

Mahremiyet denildiğinde ele alınması gereken bir diğer önemli kavram da mahrem alan, özel alan, sosyal alan veya kamusal alan gibi kullanımları bulunan “alan” kavramıdır. Söz konusu ifade, 1950’lerde Alman anayasa hukuku içtihatlarında “Alanlar Teorisi”yle ortaya çıkmış; insan onurunun dokunulmazlığı ve kişiliğin serbest biçimde geliştirilmesi düzenlemeleri ile birlikte okunması gereken kişilik hakkı içinde gelişim göstermiştir¹⁴⁹. Buna göre Alman Federal Anayasa Mahkemesi, farklı mahremiyet seviyelerini betimleyen, iç içe geçmiş bir alan silsilesi olduğunu varsaymıştır: Sosyal alan, özel alan, mahrem alan¹⁵⁰. Mahkeme her ne kadar 1983 yılında bu teoriyi terk etse de hem Alman hem de diğer doktrinlerde oldukça belirgin bir iz bırakmıştır. Örneğin, Hollanda Anayasası’nda “Kişisel Yaşam Alanına Saygı Gösterme Hakkı” (right to

¹⁴⁷ FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, s. 23, 27.

¹⁴⁸ Daniel J. SOLOVE, “A Taxonomy of Privacy”, *University of Pennsylvania Law Review*, Vol. 154, No: 3, 2006, ss. 477- 564, s. 486.

¹⁴⁹ 1949 tarihli Federal Almanya Cumhuriyeti Anayasası md. 1 ve 2, <http://www.adalet.gov.tr/duyurular/2011/eylul/anayasalar/ulkeana/pdf/08-ALMANYA%20209-276.pdf> , E.T. 21.11.2016.

¹⁵⁰ Robert ALEX, *A Theory of Constitutional Rights*, Oxford University Press, 2010, s. 223, 236.

respect for their personal sphere of life/ recht op eerbiediging van zijn persoonlijke levenssfeer) yer almaktadır¹⁵¹.

D. MAHREMİYET VE AMERİKAN ANLAYIŞI

Mahremiyet kavramının Anglo-Amerikan hukuk terminolojisine girişı, 1890 yılında Harvard Law Review’de yayımlanan ve Samuel D. Warren ve Louis Brandeis’e ait olan “Mahremiyet Hakkı” isimli makale ile olmuştur.

Bu makalede Amerikan mahremiyet hakkı, 19. yüzyılda İngiliz hukukunda yer alan “mahremiyet” konseptine dayandırılmıştır. Ayrıca yazarlara göre anılan kavram, kişilerin mahremiyeti ile ilgili vakıaların şayet kişinin onayı olmaksızın veya kamusal olarak zaten daha evvelden bilinmedikçe yayımlanmasını yasaklayan 11 Mayıs 1868 tarihli Fransız Basın Kanunu’nda da yer almaktadır. Warren ve Brandeis’e göre mahremiyet hakkı, kişinin yalnız bırakılması hakkı biçiminde formüle edilmektedir¹⁵².

Amerika’da mahremiyetin korunması yalnızca haksız fiil hukuku bağlamında değil, bireylerin devlete karşı korunmasını sağlamak için anayasa hukukunda da gelişim göstermiştir. Amerikan Anayasası’nda mahremiyet ya da özel yaşam hakkı bulunmamaktadır. Fakat ifade, inanç ve dernek hürriyetine ilişkin İlk Değişiklik (The First Amendment), askerlerin barış zamanında ev sahibinin rızası olmaksızın ve savaş zamanında kanuna aykırı olarak bir eve yerleştirilmeyeceklerine dair Üçüncü Değişiklik (The Third Amendment), kişilerin, üstlerinin, evlerinin, belgelerinin ve eşyalarının gereksiz aranmayacağı ve el konulmayacağına dair Dördüncü Değişiklik (The Fourth Amendment) ve kişinin kendisini suçlandıramayacağına ilişkin Beşinci Değişiklik (The

¹⁵¹ FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, s. 26.

¹⁵² WARREN, BRANDEIS, “The Right to Privacy”, s. 214.

Warren ve Brandeis’in kült haline gelmiş makalelerinin ardından, mahremiyetin Amerikan haksız fiil hukukunda ne şekilde vücut bulduğunu 1960 yılında Amerikalı bir diğer akademisyen William L. Prosser ele almıştır. William L. PROSSER, “Privacy”, *California Law Review*, Vol. 48, Y: 1960, No: 3, ss. 383-423.

Fifth Amendment) gibi birçok maddenin¹⁵³ yargı kararlarındaki yorumlaması ile mahremiyetin birçok boyutunun korunduğu belirtilmektedir¹⁵⁴. Keza Amerikan Yüksek Mahkemesi 1965 yılında, doğum kontrol haplarının kullanım yasağının evliliğe dair mahremiyet hakkını ihlal ettiğine karar verdiği *Griswold- Connecticut* davasında, Amerikan Haklar Bildirgesi'nin geniş bir biçimde yorumlanması neticesi bireylerin anayasal bir hak olarak mahremiyet hakkına sahip olduklarını açık bir şekilde belirtmiştir¹⁵⁵.

Mahremiyet kavramının bilgisayarlarla bağlantısı ise, 1950'lerde Amerikan pazarında ortaya çıkan elektronik veri işleme makinelerinin görünümünden sonra, 1960'larla birlikte olmuştur¹⁵⁶. İlk kez 1961 yılında veri işleme sistemleri üreten Kaliforniyalı bir şirketin sahibi olan Bernard S. Benson, bilgisayarların farkına varılmaksızın kişiler hakkında oldukça fazla veriyi saklama imkanına sahip olduğunu ve bu nedenle yakın bir gelecekte, kişilerin mahremiyetinin bilgisayarları kontrol eden kişilerin insafına bırakılmasının söz konusu olacağını dile getirmiştir¹⁵⁷. Ardından 1964 yılında Amerikalı yazar Vance Packard ise ortaya çıkan bu yeni teknolojilerin yalnızca kişilerin mahremiyet hakkını değil; başkalarından farklı olma hakkı, kefareh hakkı veya yeniden başlama hakkı gibi bazı başka hakları da tehlikeye atacağını savunmuştur¹⁵⁸.

1960'larla birlikte mahremiyet ve teknoloji çatışması, pilli mikrofonlar, portatif kayıt aletleri, tek bir hat ile kullanımı mümkün olan telefonlar ve yüksek çözünürlüklü kameralar gibi verilerin kayıt altına alınmasını sağlayan cihazların ortaya çıkışı ile gittikçe şiddetlendi. 1962 yılında New York Barosu Hukuk ve Bilim Birliği Özel

¹⁵³ *The U.S. Constitution and Other Key American Writings*, Canterbury Classics/ Baker& Taylor Publishing, 2015, San Diego, s. 111- 113

¹⁵⁴ Daniel J. SOLOVE, Marc ROTENBERG, Paul M. SCHWARTZ, *Information Privacy Law*, New York, 2006, s. 33- 34.

¹⁵⁵ *Griswold v. Connecticut*, 381 U.S. 479 (1965), <https://supreme.justia.com/cases/federal/us/381/479/> , E.T. 21.11.2016; SOLOVE, ROTENBERG, SCHWARTZ, *Information Privacy Law*, s. 34.

¹⁵⁶ Alan F. WESTIN, Michael A. BAKER, *Databanks in Free Society: Computers, Recordkeeping and Privacy*, Quadrangle Books, New York, 1972, s. 12.

¹⁵⁷ United Press International (UPI), "Electronic Brain: 'Peril' to Liberty", *Sarasota Journal*, 17.04.1961, s. 8.

¹⁵⁸ Vance PACKARD, *The Naked Society*, Penguin Books, Harmondsworth, 1971, s. 23- 24.

Komitesi, teknolojik kayıtlama sistemlerinin kişisel mahremiyete nasıl zarar verdiğine dair resmi bir araştırma yapmaya karar verdi ve bu araştırmayı Kolombiya Üniversitesi'nde Kamu Hukuku Profesörü olan ve yıllardır telefon dinleme ve mahremiyet konusunda çalışan Alan F. Westin'e teslim etti. Bu araştırmanın ortaya çıkması ile birlikte Amerika'nın genelinde mahremiyet konusuna ilişkin tartışmalar fazlasıyla arttı. 1965 yılında ise, mahremiyet ve bilgisayar çatışması konusu Kongre'nin özel bir alt komitesi tarafından ele alınarak devlet nezdinde resmi bir karşılık bulmuş oldu. Bunun ardından, çok büyük miktarda bilgilerin bilinmeyen amaçlarla kolaylıkla saklanıp erişilebilir kılınması bilgisi medyada olağanüstü bir tepki yarattı. Bu gelişmeler, 1966'da anılan alt komite tarafından gerçekleştirilen ve federal bilgi bankaları hakkında olan görüşmelerin "Bilgisayar ve Mahremiyet" başlığı altında gerçekleştirilmesine sebep olmuştur¹⁵⁹. 1962'de New York Barosu Hukuk ve Bilim Birliği Özel Komitesi tarafından başlatılan araştırma 1967 yılında Alan F. Westin'in yazarı olduğu "*Mahremiyet ve Özgürlük*" adlı kitabın yayımlanması ile kamuya paylaşıldı. Bu kitap ile mahremiyet kavramına yeni bir tanım yapıldı. Buna göre; mahremiyet, bireylerin, grupların veya kurumların kendileri hakkında bir bilgiyi ne zaman, nasıl ve ne ölçüde başkaları ile paylaşabileceklerine ilişkin bir kavramdır. Westin'e göre, mahremiyetin en temel özelliği, sonraları veri koruma hukuku bakımından oldukça önem taşıyacak olan, bireylerin kendileri ile ilgili bilgi üzerinde kontrolüdür¹⁶⁰ ve mahremiyetin bilgisayar teknolojisi bakımından sağlanması özgür bir toplum bakımından hayati önem taşımaktadır¹⁶¹.

Yukarıda anılan gelişmelerin neticesinde Amerikan kanun koyucusu harekete geçti ve 1970 yılında Amerikan Kongresi, Kredi Raporlama Ajansları tarafından edinilen

¹⁵⁹ WESTIN, *Privacy and Freedom*, s. 312- 319.

¹⁶⁰ WESTIN, *Privacy and Freedom*, s. 7- 8.

Mahremiyet tanımının bu yeni yüzü, sonradan gelen yazarlar tarafından "bilginin mahremiyeti" (privacy of information), "bilgi gizliliği" (information privacy), "bilgilendirme mahremiyeti" (informational privacy) şeklinde de tanımlanmıştır. Beate RÖSSLER, "Privacies: An Overview", *Privacies*, Ed.: Beate RÖSSLER, Stanford University Press, 2014, ss. 1- 18, s.4; Richard C. TURKINGTON, Anita L. ALLEN, *Privacy Law: Cases and Materials*, St. Paul West Group, 1999, s. 75.

¹⁶¹ WESTIN, *Privacy and Freedom*, s. 67.

kişisel bilgilerin yanlış kullanıma karşı korunması amacıyla gerektiğinde kişilerin kendileri hakkındaki bilgileri değiştirebilmelerine de olanak veren “*Adil Kredi Raporlama Yasası*”nı kabul etti¹⁶².

1971 yılında ise, Arthur R. Miller, “Mahremiyete Saldırı” adlı eserinde, Westin’in mahremiyet anlayışına, bilgisayar ve mahremiyet ilişkisi bakımından yeni bir bakış açısı sunmuştur. Bu bağlamda Miller’a göre, bilgisayarlarla mahremiyetin esas çatıştığı nokta, bireye ilişkin bilginin bir kez depolandığında artık bireyin bu bilgi üzerindeki kontrol yetkisini kaybettiği hususudur. Bu sebeple Miller, bireylerin kendilerine dair veriler üzerindeki kontrollerini devletlerin yararına yitirdiklerini ve devletlerin kendi nezdinde bilgi sistemleri kurmaları gerektiği üzerinde durmuştur¹⁶³.

1972 yılında Amerikan Sağlık, Eğitim ve Refah Departmanı, otomatik şekilde veri işleyen bilgisayar sistemlerinin zararlı sonuçlarını araştırması ve bu sonuçlardan bireylerin korunması için gerekli olan tavsiyeleri sunması için Otomatik İşlenen Kişisel Veri Sistemlerine İlişkin Danışma Komitesi’ni kurmuştur¹⁶⁴. Anılan Komite’nin hazırlamış olduğu rapor hem Amerika’da hem Avrupa’da otomatik işlem yapan kişisel veri sistemlerine dair ortaya çıkan yenilikleri ele almaktadır. Buna göre özellikle 1970 yılında Alman federe devleti olan Hessen’deki “*Veri Koruma Kanunu*” ve 1973 yılında ortaya çıkmış İsveç “*Veri Kanunu*” incelenmiş ve Fransa ile Birleşik Krallık’ta konu ile ilgili yapılan tartışmalar dile getirilmiştir. Ancak bu raporla ortaya konan birkaç önemli husus bulunmaktadır. Öncelikle rapor, kişisel verilerin otomatik olarak işlenmesi bağlamında kişisel veriyi tanımlamaktadır. Metinde birçok defa geçen bu kavram, “kişi hakkında olan tüm veriler”in, “kişiyi ayırt edici biçimde ortaya koyan tüm bilgiler”in “kişisel veri” olduğunu belirtmektedir. Ayrıca bu raporla birlikte, kişinin kendisi

¹⁶² Fair Credit Reporting Act, <https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/fair-credit-reporting-act>, E.T. 27.11.2016.

¹⁶³ Arthur R. MILLER, *The Assault on Privacy: Computers, Data Bank and Dossiers*, University of Michigan Press, 1971, s. 24, 40- 42.

¹⁶⁴ U.S. Department of Health, Education and Welfare, “Records, Computers and the Rights of Citizens”, Report of the Secretary’s Advisory Committee on Automated Personal Data Systems, DHEW Publication NO. (OS) 73- 94, July 1973, <https://www.justice.gov/opcl/docs/rec-com-rights.pdf>, E.T. 27.11.2016.

hakkında hangi bilgilerin kayıtlandığını ve bu bilginin nasıl kullanılacağını bilmesi hakkı, gerektiğinde bu bilgilerin düzeltilebileceği hususları gibi, veri koruma bakımından temel olan ilkeler ortaya çıkmıştır. Raporun vardığı ana sonuç ise, ajanslar, devlet kurumları vb. tarafından otomatik biçimde veri işleyen tüm sistemlere ve işlediği kişisel verilere ilişkin Adil Bilgi Uygulamaları Yasası'nın (Code of Fair Information Practice) çıkarılmasının zorunlu olduğudur¹⁶⁵.

1974 yılının başında Başkan Richard Nixon, yıl sonuna gelmeden tüm Amerikalıların kişisel mahremiyet haklarının korunması ve tanımlanması için tarihi bir adım atacağını belirtmiştir¹⁶⁶. Bu doğrultuda aynı yıl şubat ayında, Beyaz Saray Mahremiyet Hakkı Komitesi'nin kurulmasını sağlamıştır. Fakat bu sürecin devamında Watergate Skandalı'nın patlak vermesi sonucunda Ağustos 1974 tarihinde Nixon istifa etmiş ve yerine Gerald Ford başkan olarak geçmiştir¹⁶⁷. Her ne kadar bu olaylar yaşanıyor olsa da nihayetinde 31 Aralık 1974 tarihinde Amerikan Mahremiyet Yasası çıkarılmış; yürürlük tarihi olarak da 27 Eylül 1975 belirlenmiştir. Bu yasanın temel amacı, kişi hakkında elde edilmiş tüm bilgilerin (yalnızca bilgisayarla işlenmiş olanlar değil) suiistimaline karşı bireyleri korumak ve bu bilgilere kişilerin erişimini sağlamaktır¹⁶⁸. Mahremiyet Yasası'nın hükümlerinin uygulanmasını gözlemlemek için “Federal Mahremiyet Kurulu” (Federal Privacy Board) adında ad-hoc bir kurul oluşturulması beklenmekteydi. Ancak bu yasa ile yalnızca Mahremiyet Koruması Çalışma Komisyonu (Privacy Protection Study Commission) kurulmuştur¹⁶⁹. Bu yasanın yürürlüğe girmesi ile Amerikan Yüksek Mahkemesi Anayasa ile korunan mahremiyet alanını genişletmiştir.

¹⁶⁵ U.S. Department of Health, Education and Welfare, “Records, Computers and the Rights of Citizens”, Report of the Secretary’s Advisory Committee on Automated Personal Data Systems, DHEW Publication NO. (OS) 73- 94, July 1973, <https://www.justice.gov/opcl/docs/rec-com-rights.pdf>, E.T. 27.11.2016, s. 33-77, 168- 174, 136- 138.

¹⁶⁶ Richard NIXON, “Address on the State of the Union Delivered Before a Joint Session of the Congress”, 30.01.1974, <http://www.presidency.ucsb.edu/ws/?pid=4327>, E.T. 05.12.2016.

¹⁶⁷ “Watergate Scandal”, *Encyclopedia Britannica*, <https://global.britannica.com/event/Watergate-Scandal>, E.T. 05.12.2016.

¹⁶⁸ Privacy Act of 1974, <https://www.justice.gov/opcl/privacy-act-1974>, E.T. 05.12.2016.

¹⁶⁹ Marc ROTENBERG, *The Privacy Law Sourcebook 2001: United States Law International Law and Recent Developments*, Electronic Privacy Information Center, Washington, 2001, s.39.

Bu bağlamda ilgili dönemde Yüksek Mahkeme'nin önüne gelen *Whalen- Roe* kararına bakmak gerekmektedir. Söz konusu olayda New York Eyaleti'nde bazı uyarıcı-uyuşturucu özellikli ilaçların bulunduğu 2 Numaralı İlaç Çizelgesi denen listedeki ilaçların bir doktor tarafından hastasına yazılması halinde, ilacı yazan doktorun adı, hastanın adı, yaşı, adresi, ilacın dozu gibi bilgilerin raporlanması ve saklanması kuralına ilişkin bir yasa mevcuttur. Mahkeme burada mahremiyete dair korunması gereken iki farklı menfaat tespit etmiştir. Bunlardan biri, kişisel konuların ifşasının kontrol edilebilmesindeki menfaattir. Bir diğeri ise, belirli kişisel kararların devlet müdahalesi olmaksızın verilebilmesindeki menfaattir. Karardaki çoğunluk görüşü her ne kadar böyle bir analiz yapsa ve devletin vatandaşların kişisel bilgilerini depolaması hallerindeki kaygılara hak verse de somut olay bağlamında Anayasa'ya aykırılık tespit etmemiştir¹⁷⁰.

E. MAHREMİYET VE AVRUPA ANLAYIŞI

Mahremiyet ve yeniden tanımlanması ile bilgisayarla ilişkisi Amerika'da böyle gelişmekte iken, Avrupa bu konuda hem ulusal hem de uluslararası düzeyde çözüm arayışına girdi.

İngilizce olarak "Right to Privacy" olarak ifade edilen mahremiyet hakkı, Anglo-Sakson hukukunda bu biçimde ifade edilmekte iken, Kara Avrupası'na geçildiğinde, "Kişilik Hakları- Rights of the Personality" biçiminde bir karşılık bulmaktadır¹⁷¹.

¹⁷⁰ Anılan kararda çoğunluk görüşüne farklı bir gerekçe ile katılan Yargıç Brennan'ın bazı tespitleri de mahremiyet algısı için sonraki süreçte önemli olmuştur. Brennan'a göre, Devlet'in toplayacağı bilgi türü ve toplanma biçiminde bazı sınırlar olmalıdır. Bilgisayarlarla büyük miktarda verilerin toplanabilmesinin giderek kolaylaştığı bir dünyada bu tür verilerin yanlış kullanılma ihtimali de artmaktadır. Bu nedenle Yargıç Brennan gelecekteki şartlar düşünüldüğünde, mahremiyet yasasına teknoloji ile ilgili kısıtlamalar getirilebileceği ihtimalinin de göz önünde bulundurulması gerektiğini dile getirmiştir. *Whalen v. Roe*, 429 U.S. 589 (1977), <https://supreme.justia.com/cases/federal/us/429/589/case.html> , E.T. 17.05.2019; SOLOVE, ROTENBERG, SCHWARTZ, *Information Privacy Law*, s. 34.

¹⁷¹ Stig STRÖMHOLM, *Right of Privacy and Rights of the Personality- A Comparative Survey*, Working Paper prepared for the Nordic Conference on Privacy, International Commission of Jurists, Stockholm, May 1967, s. 25- 26.

Kavramsal olarak bu farklılaşmaya bir de mahremiyet hakkının içeriği ve tanımlanmasına ilişkin tartışmalar eklenmiştir¹⁷².

Bu bağlamda öncelikle 1948 tarihli İnsan Hakları Evrensel Beyannamesi (İHEB) ele alınabilir. Anılan düzenlemenin 12. maddesine göre;

“Hiç kimse özel yaşamı, ailesi, meskeni veya yazışması hususlarında keyfi karışmalara, şeref ve şöhretine karşı tecavüzlere maruz bırakılamaz.

*Herkesin bu karışma ve tecavüzlere karşı kanun ile korunmaya hakkı vardır.”*¹⁷³

Görüldüğü üzere ilgili madde 1948 yılında bir mahremiyet- özel yaşam hakkından söz etmiş ve içeriğine ilişkin ipucu (aile, mesken, haberleşme gibi.) vermiş; fakat bu kavramların hiçbirini tanımlamamıştır¹⁷⁴. 1966 yılında İkiz Paktlar’ın kabul edilmesi ile, Medeni ve Siyasal Haklara İlişkin Uluslararası Sözleşme’nin 17. maddesi de,

“Hiç kimsenin özel ve aile yaşamına, konutuna veya haberleşmesine keyfi veya hukuka aykırı olarak müdahale edilemez; onuru veya itibarı hukuka aykırı saldırılara maruz bırakılamaz.

Herkes bu tür saldırılara veya müdahalelere karşı hukuk tarafından korunma hakkına sahiptir.”

diyerek İHEB’e benzer bir düzenleme yapmış ve fakat mahremiyeti yine tanımlamamıştır¹⁷⁵.

¹⁷² Söz konusu tartışmalar için bkz; Gülay ARSLAN ÖNCÜ, *Avrupa İnsan Hakları Sözleşmesinde Özel Yaşamın Korunması Hakkı*, Beta, 2011.

¹⁷³ Resmî Gazete, 27.05.1949, Sayı: 7217, <http://www.resmigazete.gov.tr/arsiv/7217.pdf>, E.T. 05.12.2016.

¹⁷⁴ FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, s. 37.

¹⁷⁵ Resmî Gazete, 18.06.2003, Sayı: 25142, <http://www.resmigazete.gov.tr/eskiler/2003/06/20030618.htm#3>, E.T. 05.12.2016.

1950 tarihli İnsan Hakları Avrupa Sözleşmesi (İHAS) ise, yukarıda anılan sözleşmelerden farklı bir ifade şeklini benimsemiş ve “mahremiyet”ten söz etmemiştir. Bunun yerine 8. maddesinde;

“Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.

Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir.”¹⁷⁶

İlgili maddeden de görüleceği üzere İHAS mahremiyet yerine, “özel yaşama saygı” ifadesini kullanmaktadır. Her ne kadar İHAS içtihatları ile özel yaşam düzenlemesi, ilerideki bölümlerde anlatılacağı üzere, Avrupa’da mahremiyet algısının genişleme ve gelişmesini sağlayacak olsa da başlarda böyle değildi.

1948’den itibaren Avrupa ekseninde ortaya çıkan düzenlemelerdeki mahremiyet algısı yukarıda belirtildiği gibi daha yüzeysel bir görünüm arz etmekteydi. Fakat 1960’ların sonuna gelindiğinde bir sivil toplum kuruluşu olarak adlandırılabilen Uluslararası Hukukçular Komisyonu mahremiyet kavramı ve güvencelerinin daha derinlikli bir biçimde araştırılması için lokomotif görevi gördü ve 1967 yılında Nordik Konferansı’na ev sahipliği yaptı¹⁷⁷. Bu konferansın en önemli çıktısı olarak, “Mahremiyet Hakkı”nın tanımlanmış olması gösterilebilir. Bu tanıma göre;

¹⁷⁶ Resmî Gazete, 19.03.1954, Sayı: 8662, <http://www.resmigazete.gov.tr/arsiv/8662.pdf>, E.T. 05.12.2016.

¹⁷⁷ International Commission of Jurists, “The Protection of Privacy”, *UNESCO International Social Science Journal*, Vol. XXIV, No: 3, 1972, s. 448.

*“Mahremiyet Hakkı, kişinin kendi yaşamını, minimum ölçüde müdahalede bulunularak, sürdürmesi için yalnız bırakılma/ kalma hakkıdır.”*¹⁷⁸

Tanım daha detaylı olarak bakıldığında, söz konusu yalnız bırakılma hakkının, “mahremiyet, aile ve ev yaşamı” ile şöhret ve onura karşı yapılan saldırılara; ayrıca özel yaşama dair utanç verici ya da ilgisiz gerçeklerin ifşasına karşı koruma sağlaması gerektiği vurgulanmaktadır¹⁷⁹. Fakat anılan konferansın sonuç bildirgesine bakıldığında bilgisayarlara ilişkin özel bir gönderme bulunmadığı görülmektedir¹⁸⁰.

Bu eksiklik, 1970 yılında Uluslararası Hukukçular Komisyonu’nun Britanya ayağı olan Justice olarak adlandırılan bölümü tarafından tamamlandı. Justice, “Mahremiyet ve Hukuk” başlığını taşıyan bir rapor hazırladı ve içerisine “Bilgisayarlar ve Mahremiyet” başlığını taşıyan bir bölüm ekledi. Bu rapora göre mahremiyet kavramı, her ne kadar içeriğinin belirlenmesi çok zor olsa da mutlaka tanımlanmalıdır¹⁸¹. Bu amaç doğrultusunda mahremiyetin, hangi hususların mahremiyet ihlali oluşturduğunu belirterek tanımlanması yoluna gidilmiştir¹⁸². Bu ise, hem Warren ve Brandeis’in kült

¹⁷⁸ International Commission of Jurists, “Right to Privacy: Conclusions of the Nordic Conference”, Cenevre, Mayıs 1967, s. 2, <http://www.icj.org/wp-content/uploads/2013/06/Right-to-privacy-seminar-report-conclusions-1967-eng.pdf>, E.T. 11.12.2016.

¹⁷⁹ Andrew T. KEYTON, “Defamation and Privacy in an Era of ‘More Speech’”, *Comperative Defamation and Privacy Law*, Ed. Andrew T. KEYTON, Cambridge University Press, 2016, s. 6.

¹⁸⁰ International Commission of Jurists, “Right to Privacy: Conclusions of the Nordic Conference”, Cenevre, Mayıs 1967, <http://www.icj.org/wp-content/uploads/2013/06/Right-to-privacy-seminar-report-conclusions-1967-eng.pdf>, E.T. 11.12.2016.

¹⁸¹ Eleni KOSTA, *Consent in European Data Protection Law*, Martinus Nijhoff Publishers, Leiden- Boston, 2013, s. 56- 57.

¹⁸² “Mahremiyet hakkı, herhangi bir kişinin kendisine, evine, ailesine, başkalarıyla olan ilişkilerine ve iletişimine, mülküne ve ticari meselelerine yapılan saldırılara karşı korunma hakkı anlamına gelir. Ayrıca; a) casusluk, gözetleme, izleme, sürekli rahatsız etme yoluyla saldırı,

b) konuşulanların izinsiz dinlenmesi veya kaydedilmesi;

c) görsel imajların yetkisiz şekilde elde edilmesi,

d) belgelerin yetkisiz okunması veya kopyalanması,

e) kişinin kendisine sıkıntı, rahatsızlık veya utanç verici olması için hesaplanan gizli bilgiler veya gerçekler (adını, kimliğini v.b. içeren) yetkisiz kullanımı veya ifşa edilmesi veya onun yanlış değerlendirilmesine (‘false light’) sebep olma

(‘false light’ kavramı en geniş anlamı ile, birini yanlış lanse ederek kişinin mahremiyetinin ihlali neticesinde doğan bir haksız fiildir. Wex Legal Dictionary/ Encyclopedia, Legal Information Institute,

makalelerinde, hem de Nordik Konferans'ın sonuç raporunda tanımlanan mahremiyet hakkından farklılık yaratmıştır¹⁸³. Tüm bu özellikleri ile rapor, taslak bir "Mahremiyet Hakkı Yasası" da içermektedir¹⁸⁴.

Bu raporun ardından, Uluslararası Hukukçular Komisyonu 1972 yılında UNESCO için, "Mahremiyetin Yasal Koruması: 10 Ülkeye İlişkin Karşılaştırmalı Araştırma" isimli çalışmayı, özellikle yukarıda değinilen Justice Raporu'na dayanarak hazırlamıştır. İlgili düzenlemenin mahremiyet ve kişisel veri alanındaki belki de en değerli katkısı, mahremiyetin teknolojik gelişmelerden kaynaklı değişen anlamı için bilgisayarlaşma neticesinde elde edilen kişisel bilgilerin mahremiyetin korunması için büyük bir tehdit oluşturduğu ve mahremiyetin, daha somut bir ifade ile kişisel verilerin korunmasının en nihai amaç olması gerektiğini belirtmesidir¹⁸⁵.

Avrupa hukuk düzleminde mahremiyet kavramı genel görünümü ile yukarıda anlatıldığı gibi bir ortaya çıkış ve gelişim gösterirken ulusal bazda da çeşitli ülkelerde değişimler yaşanmaktaydı.

Warren ve Brandeis mahremiyet hakkının köklerinin İngiliz ve Fransız hukukunda bulunduğunu belirtmekteydi. Her ne kadar böyle demişlerse de İngiliz hukukunda mahremiyet kavramına ilk kez 1849 tarihli *Prince Albert- Strange*¹⁸⁶ kararında rastlanmaktadır¹⁸⁷. Olay, Kraliçe Victoria ve Prens Albert'in kara kalem hobilerini bakır levhalara gravür olarak bastırmak istemeleri neticesinde ortaya çıkmıştır.

Cornell Law School, https://www.law.cornell.edu/wex/false_light, E.T. 12.12.2016.)

f) *adının, kimliğinin veya benzerliğinin başkasının kazanımı için yetkisiz olarak tahsis edilmesi.*"

International Commission of Jurists, Committee on Privacy and JUSTICE (The British Section of ICJ), "Privacy and the Law", Stevens& Sons Ltd., Londra, 1970, s. 5.

¹⁸³ KOSTA, *Consent in European Data Protection Law*, s. 58.

¹⁸⁴ International Commission of Jurists, Committee on Privacy and JUSTICE (The British Section of ICJ), *Privacy and the Law*, Stevens& Sons Ltd., Londra, 1970, s. 27.

¹⁸⁵ International Commission of Jurists, UNESCO International Social Science Journal, *The Protection of Privacy*, Vol. XXIV, No: 3, 1972, s. 417, 420.

¹⁸⁶ *Prince Albert v. Strange*, High Court of Chancery, (1849) 1 Mac & G 25, [1849] EWHC Ch J20, 41 ER 1171, (1849) 18 LJ Ch 120, <http://www.bailii.org/ew/cases/EWHC/Ch/1849/J20.html>, E.T. 19.12.2016.

¹⁸⁷ International Commission of Jurists, "The Protection of Privacy", *UNESCO International Social Science Journal*, Vol. XXIV, No: 3, 1972, s. 457- 458.

Kraliçe ve Prens tasarladıkları bu gravürlerden yakınları ve ailelerine vermek için bazı kara kalem çalışmaları hazırlamışlardır. Bu çalışmalardan birini (bir eğlence esnasında Kraliçe'nin hayat arkadaşı olan Prens Albert'i gösteren resmi) arkadaşları olan John Brown isimli bir yazara vermiş ya da göstermişlerdir ve neticesinde bu resmin bir kopyası oluşturulmuştur. Bu kopyalar sonrasında Kraliçe ve Prens'e geri verilmiştir. Ancak Brown'ın bir çalışanı olan Middleton, bazı ekstra kopyalar bastırmıştır. Ardından bu kopyaları yayımlaması için yayıncı Jasper Tomsett Judge'a satmıştır. Yayıncı Judge bu kara kalemlerin gravürlerinin halka açık bir sergide gösterilmesini önermiş ve matbaacı William Strange tarafından basılan kopyalardan bir katalog hazırlatmıştır. Neticesinde Prens Albert, gravürleri basan William Strange ve bunları yayımlayan yayıncı Jasper Tomsett Judge'ı dava etmiştir. Burada yargıç Knight Bruce ve Lord Cottenham, kişinin rızası olmaksızın kendi eğlenceleri için yapılmış olan çizimlerin, Kraliçe'nin Windsor'daki evinde ve ayrıca kilitli olarak muhafaza ediliyor olmaları sebebiyle mahremiyet taşıdığını, davalıların eline ise gizlice geçmiş olduklarını belirtmişlerdir. Bu davada mahremiyet, mülkiyetin bir türü olarak görülerek gravürlerin basılması durdurulmuş ve davalıların tazminat ödemesine karar verilmiştir¹⁸⁸.

Bu karardan sonraki yıllarda mahremiyet kavramının durumu, Britanya her ne kadar İHEB ve İHAS'a taraf da olsa, Uluslararası Hukukçular Birliği olan Justice'in 1970 yılında mahremiyet hakkını tanımış olduğu raporuna dek çok kapsamlı bir gelişim gösterememiştir¹⁸⁹. Bu bağlamda elbette 1961 yılından itibaren Lord Mancroft'un "Mahremiyet Hakkı Yasa Tasarısı" gibi bazı girişimler yadsınamaz¹⁹⁰. Ancak mahremiyetin bilgisayarlaşma süreci neticesinde yaratabileceği tehlikeler, Sör Kenneth Younger'ın başkanlığındaki Mahremiyet Komitesi'nin 1972 yılında yayımladığı ve

¹⁸⁸ Ursula SMARTT, *Media and Entertainment Law*, Routledge, London & New York, 2011, s. 31- 32.

¹⁸⁹ FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, s. 42.

¹⁹⁰ Diğer bazı hukuki girişimler, 1967 tarihli Telefon Dinleme Yasa Tasarısı (*Telephone Monitoring Bill*), 1968 tarihli Endüstriyel Bilgi Yasa Tasarısı (*Industrial Information Bill*), 1968 tarihli Özel Dedektiflerin Tescili Yasa Tasarısı (*Bill for the Registration of Private Detectives*), 1969 tarihli Veri İzleme Yasa Tasarısı (*Data Surveillance Bill*) ve 1969 tarihli Kişisel Kayıtlar (Bilgisayarlar) Yasa Tasarısıdır (*Personal Records-Computers- Bill*).

International Commission of Jurists, "The Protection of Privacy", *UNESCO International Social Science Journal*, Vol. XXIV, No: 3, 1972, s. 459- 460.

“Younger Raporu” olarak da anılan nihai raporun, özellikle özel sektörün bilgisayarlar aracılığıyla veri işleme sürecini ele almasıyla dikkatleri üzerine çekmiştir¹⁹¹. Devamında 1975 yılında Birleşik Krallık hükümeti “Bilgisayarlar ve Mahremiyet” ile “Bilgisayarlar: Mahremiyet için Emniyet Tedbirleri” başlığını taşıyan iki adet Beyaz Rapor (White Paper) hazırlamıştır. Bu iki hükümet raporu sonrasında yasal bir mevzuat gerekliliği hasıl olması ve kamu sektöründe bilgisayar kullanımının da artışı neticesinde ayrıca bir “Veri Koruma Komitesi” kurulmuş ve başkanlığına Sör Norman Lindop getirilmiştir. Bu komite de 1978 yılında “Lindop Raporu” olarak anılan çalışmasını yayımlamış ve Younger Raporu’ndan farklı olarak, bilgisayar yolu ile elde edilen kişisel verilerin korunması için bir veri koruma otoritesi oluşturulmasını ve bunun için gereken yasal düzenlemenin hazırlanmasını tavsiye etmiştir. Fakat Mayıs 1979’da Margaret Thatcher’ın Muhafazakâr Parti hükümetinin başa gelmesi ile veri koruma meselesine dair ilk yasal düzenlemenin kabul edilmesi 1984 yılına dek ertelenmiştir¹⁹².

Her ne kadar mahremiyet ve veri işleme konularına dair ilk düzenlemeler yukarıda belirtildiği şekilde olsa da mahremiyet kavramının diğer Avrupa ülkelerindeki gelişimi de pek farklılık göstermemiştir. İlk olarak Hollanda’ya baktığımızda, 1971 yılında Mahremiyet ve Kişisel Siciller Komitesi’nin kurulduğu göze çarpmaktadır. Bu komite 1974’te bir Geçici Rapor hazırlamış ve bu raporda, kişilerin mahremiyetinin korunması için kamu ve özel sektörü kapsayan bir veri koruma kanunu hazırlanması gerektiğini belirtmiştir¹⁹³. Anayasal düzlemde ise veri bankaları ve veri işleme gibi tekniklerle birlikte dijitalleşen dünyayı dikkate alarak, 1983 yılında Hollanda Anayasası’nın 10. maddesinde yer alan “Kişisel Yaşam Alanına Saygı Hakkı”nda bir değişikliğe gidilerek kişisel verilerin kayıtlanması ve dağıtımına ilişkin korumayı maddeye eklemiştir¹⁹⁴.

¹⁹¹ Adam P. WARREN, James DEARNLY, “Data Protection Legislation in the United Kingdom: From Development to Statute 1969-84”, *Information Communication and Society*, Vol. 8 (2), 2005, s. 241- 242, ss. 238 – 263.

¹⁹² Colin J. BENNETT, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*, Cornell University Press, Ithaca & London, 1992, s. 87- 89.

¹⁹³ FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, s. 45.

¹⁹⁴ Gert- Jan LEENKNEGT, “The Protection of Fundamental Rights in Digital Age”, *Electronic Journal of Comparative Law*, Netherlands Comparative Law Association, Vol. 6, 4.12.2002, s. 340.

Fransa'ya bakıldığında ise, 1849 tarihli *Prens Albert- Strange* kararından yaklaşık on yıl sonra mahremiyet kavramının *Felix- O'Connell* kararında ele alındığı görülmektedir. Bu davanın konusunu, ünlü bir aktristin ölüm döşeginde iken kardeşi tarafından, kendilerine anı olarak kalması için çektiirdiği fotoğrafların daha sonra çizimlerinin yapılarak satışa çıkarılması oluşturmaktadır. Seine Hukuk Mahkemesi tarafından görülen davada, Rachel Felix'in ünlü bir kişi olmasına rağmen bu denli mahrem bir fotoğrafının çoğaltılması ve yayınlanması için ailesinin rızası olması gerektiğine, çünkü davacının fotoğraftaki hakkının mutlak bir hak olduğuna karar verilmiştir¹⁹⁵. Her ne kadar bu kararda açık bir biçimde "mahremiyet hakkı- right to privacy" yer almasa da bu karardan 9 yıl sonra 1867'de *Dumas- Liébert* Kararı'nda anılan haktan açıkça söz edilmiştir. Söz konusu olayda Dumas, genç Amerikalı aktris Adah Menken ile birlikte gömlekli bir pozunu içeren fotoğrafların Le Figaro'da yayınlanması neticesinde alaycı yorumlara ve fotoğrafçının vitrininde yer alması sebebiyle halkın eğlenmesine yol açtığı gerekçesi ile fotoğrafların yayımı ve gösterimini önlemek için Mahkeme'ye başvurmuştur. Bir önceki davadaki Sarah Felix'in aksine Dumas, fotoğrafçı Liébert ile bir anlaşma yaparak fotoğrafları kullanmasına ilişkin şartlar koymamıştı ve ayrıca Liébert fotoğrafları almak için bir ödeme yapmıştı. Ancak Mahkeme genel ahlak uyarınca, mahremiyet hakkının kalıcı olarak bir başkasına devri için mutlaka resmi bir anlaşma yapılmasını gerektiğine hükmetmiştir. Sonuç olarak Dumas fotoğrafların parasını fotoğrafçıya ödemeyi teklif ettiğinden Mahkeme, miktarı 100 Frangı olarak belirlemiş ve Liébert'e kalan fotoğrafları satmamasını ve yayınlamamasını emretmiştir¹⁹⁶.

Mahremiyet kavramının Fransa'daki gelişimi açısından Fransız Anayasa Konseyi'nin bu kararlardan yaklaşık 100 yıl sonra 1971 yılında, 1789 Fransız İnsan ve Yurttaş Hakları Bildirgesi'ni de anayasaya yerleşik kamu özgürlükleri arasında ele alması

¹⁹⁵ *Felix c. O'Connell*, Seine Hukuk Mahkemesi, 16.6.1858, aktaran: Megan RICHARDSON, *The Right to Privacy Origins and Influence of Nineteenth- Century Idea*, Cambridge University Press, 2017, s. 64- 67; Huw BEVERLEY- SMITH, Ansgar OHLY, Agnes LUCAS- SCHLOETTER, *Privacy, Property and Personality- Civil Law Perspectives on Commercial Appropriation*, Cambridge University Press, New York, 2005, s. 147.

¹⁹⁶ RICHARDSON, *The Right to Privacy Origins and Influence of Nineteenth- Century Idea*, s. 67.

önem taşımaktadır. Böylece Bildirge'nin 2. maddesinde yer alan “bireysel özgürlük”, bireyin mahremiyetini de koruyan bir düzenleme olarak değerlendirilmeye başlamıştır¹⁹⁷.

Veri koruma hukukunun ortaya kalıcı bir biçimde çıkış yılları olan 70'lerde Fransız hukuku da yeni teknolojiler ve özellikle bilgisayarların kamu özgürlükleri ile ilişkisini de incelemeye başlar. Bu geniş perspektif, 1974 yılında İHAS'a taraf olunmasıyla 8. madde bağlamında da desteğini bulur¹⁹⁸.

Mahremiyet kavramının Avrupa'daki ortaya çıkış serüveninde ilginç bir örnek olarak İsveç'e de değinmek gerekmektedir. Kamu sektörünün bilgisayarlaşması 1960'ların başlarına tekabül etmektedir. Bu dönemle birlikte nüfusun önemli bir kısmı, toplanan bilgilerin otomatik olarak işlenmesi sürecine tabi tutulduğunu fark ederek endişe duymaya başlar. Devamında ise İsveç hükümeti, bilgisayarlı veri saklama konusuna ilişkin resmi bir komisyon görevlendirir. Anılan Resmî Belgelerin Aleniyet ve Gizliliği Parlamenter Komisyonu, 1972 yılında bilgisayarlı veri saklama konusunda bir rapor yayımlar. Bu raporun ismi, İngilizce konuşulan çevrelerde “Bilgisayarlar ve Mahremiyet” (Computers and Privacy) olarak bilinmeye başlar; ancak raporun orijinal ismi “Data och integritet” biçimindedir ve bu raporla ortaya çıkmaktadır ki, İsveç dilinde “mahremiyet” anlamına gelen “privacy” kelimesi yoktur ve bu kelimeye en yakın anlamda olabilecek kelime “integritet” (personal integrity), kişisel bütünlük anlamına da gelmektedir¹⁹⁹. Veri korumasına dair İsveç anlayışı, bugün dahi veri işleme düzenlemesini kişisel bütünlüğün korunması bağlamında değerlendirmektedir²⁰⁰.

¹⁹⁷ FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, s. 47.

¹⁹⁸ Chart of Signatures and Ratifications of Treaty 005- *Convention for the Protection of Human Rights and Fundamental Freedoms*, Status as of 30/05/2017, <http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005/signatures> , E.T. 30.05.2017.

¹⁹⁹ David H. FLAHERTY, *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada and the United States*, University of North Carolina Press, 1989, s. 104- 105.

²⁰⁰ BYGRAVE, *Data Protection Law: Approaching its Rationale, Logic and Limits*, s. 322.

F. MAHREMİYETTEN KİŞİSEL VERİLERİN KORUNMASINA VERİ KORUMA HUKUKUNUN GELİŞİMİ

Kişisel verilerin korunması esasında kişisel verilerin işlenmesi ile ilgili bir dizi fikri içeren bir terimdir ve ilk ortaya çıktığı zaman doktrinde çoğu zaman mahremiyet kavramı ile anılmıştır. Bu bağlamda söz konusu kavram ile gerçekten ne ifade edildiğini anlamak ve zamanla nasıl bağımsız hale geldiğini görmek önemlidir.

Veri özneleri çoğu zaman verilerinin işlenmesini engelleyemezler. Veri denetleyicileri de çoklukla başkalarına ait verileri işleyebilirler. Daha açık bir ifadeyle, veri korumanın anlamı veri işlemenin yasak olması değil, hukuk dışı ve orantısız veri işlemenin yasak olmasıdır. Dolayısıyla veri koruma düzenlemelerinin esas amacı, kişilerin verilerini haksız bir şekilde toplama, saklama, kullanma ve kişisel detayların yayılmasını engellemektir. Bu ise, mahremiyetin korunmasının temel amaçlarından biri olan özel yaşama ilişkin haksız müdahalelerin engellenmesi ile birebir aynı amaca hizmet etmektedir²⁰¹.

Kişisel verilerin korunması, sürekli değişen ve büyüyen bir süreç olarak karşımıza çıkmaktadır. Teknolojik gelişmelerle birlikte yeni zorlukların ortaya çıkması sürekli olarak yeni kural ve ilkeleri gerektirmektedir. Dolayısıyla veri koruma kavramının altında yatan ana unsurun yalnızca mahremiyet olduğunu söylemek ilk başlarda mümkünse de günümüzde çok daha kapsamlı bir hale evrilmiştir. Yukarıda belirtildiği üzere doktrinde veri korumanın yalnız bırakılma hakkından başlayıp bilgilerin geleceğini belirleme ve özel yaşamın korunmasına dek süregelen birçok gerekçesi olduğu görülmektedir. Ayrıca

²⁰¹ Paul DE HERT, Serge GUTWIRTH, “Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalisation in Action”, *Reinventing Data Protection*, Serge GUTWIRTH, Yves POULLET, Paul DE HERT, Cecile DE TERWANGNE, Sjaak NOUWT (Ed.), Springer, 2009, s. 3, ss. 3- 44.

kişisel verilerin korunması kavramı otonomi, güçler ayrılığı, demokrasi, çoğulculuk gibi birçok konu ile de ilişkilidir²⁰².

Doktrinde çoklukla veri koruma hukukunun temeli olarak ele alınan mahremiyet ve kavramın veri koruma alanındaki yansıması 1970’lerden önce genel itibarıyla yukarıdaki biçimde bir gelişim göstermiştir. Bu noktada kişisel verilerin korunması adına dünyadaki düzenlemelerde üç farklı yönelim görüldüğü belirtilmelidir. Bunlardan ilki, genel itibarıyla Avrupa veri koruma hukukunda olan kişisel verinin korunması hakkında genel bir veri koruma kanunu çıkartmaktır. İkinci örnek ise daha ziyade Amerika’da görülen, farklı sektörlerle yönelik özel hayatın gizliliğine ilişkin kanuni düzenlemeler yapmaktır. Son olarak üçüncü yol ise Brezilya, Peru, Arjantin gibi Latin Amerika ülkelerinde görülen ve “*Habeas data*” biçiminde adlandırılan bir anayasal hak olan bireysel bir şikâyet yoludur²⁰³. Anılan bu üç yöntemin ilki olarak 1970’lerle birlikte artık Avrupa ülkelerinde verilerin otomatik işlenmesi meselesi için gerek anayasal düzeyde gerekse özel düzeyde düzenlemelere gidilmiştir. Bu düzenlemelerde ise, kişisel verilerin korunması artık ayrı bir temel hak kategorisi olarak ortaya çıkmaktadır.

1970’ten 1981 yılındaki Avrupa Konseyi Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi’ne (108 Sayılı Sözleşme) dek olan dönemde bireylere ilişkin veri işleme konusu mahremiyet kavramından bağımsızlaşarak ayrı bir alan oluşturmuştur. Bu dönemde farklı Avrupa ülkeleri, çeşitli yasal düzenlemeler ile veri işleme sürecini düzenleme altına almıştır. Bu doğrultuda

²⁰² Paul DE HERT, Serge GUTWIRTH, “Privacy, Data Protection and Law Enforcement- Opacity of the Individual and Transparency of Power”, *Privacy and the Criminal Law*, Erik CLAES, Anthony DUFF, Serge GUTWIRTH (Ed.), Antwerp/Oxford, Intersentia, 2006, s. 61–104.

²⁰³ “*Habeas Data*” kavramının terminolojik içerik ve tarihsel kökenleri ile Latin ülkelerinde anayasal hakların bireysel başvuru yolu ile korunması modeli hakkında detaylı bir çalışma için bkz. Sibel İNCEOĞLU, *Anayasa Mahkemesi’ne Bireysel Başvuru- Türkiye ve Latin Modelleri*, On İki Levha Yayıncılık, İstanbul, 2017, s. 4-6; Cemil KAYA, *İdare Hukukunda Bilgi Edinme Hakkı*, Seçkin Yayıncılık, Ankara, 2005, s. 97.

Alman Eyaleti Hessen, İsveç, Almanya ve Fransa, bireylere ilişkin veri işlenmesine dair Avrupa'daki ilk spesifik yasal düzenlemeleri gerçekleştirmiştir²⁰⁴.

“Veri Koruması” adını içeren ilk yasal düzenleme, Ekim 1970 tarihinde Almanya'nın Hessen Eyaleti'nde düzenlenmiştir. Anılan düzenlemenin tam adı, Hessen Eyaleti Veri Koruma Kanunu'dur²⁰⁵. Her ne kadar bazı başka eyaletlerin çeşitli yasal düzenlemelerinde, bireylerin haklarını korumak adına veri işleme sürecine dair kurallar bulunmuş olsa da bu düzenlemenin özelliği, devletin bünyesinde saklanan devlete dair dosyalardaki bilgilerin kullanımı ve bunların korunmasına dair emniyet tedbirlerini ele alan ayrı ve genel bir veri koruma kanunu olmasıdır²⁰⁶.

Hessen Eyaleti Veri Koruma Kanunu'nda kullanılan “Veri Koruma (Datenschutz)” kavramı, İngilizce'de yer alan “Data Protection” kavramından alıntılanmış ve daha sonra tüm Avrupa dillerine yayılmıştır. Bu adlandırmanın temelinde her ne kadar verilmiş, paylaşılmış herhangi bir bilgi parçası anlamına gelen Latince “datum” kelimesinden türetilmiş “data” sözcüğü kullanılsa da bu sözcük zamanla teknolojik gelişmelerdeki ivme sebebiyle, yalnızca bilgisayarlar tarafından işletilen bilgi anlamına gelmekte ve böylece özel bir nitelemeyi karşılamaktadır²⁰⁷.

Avrupa'da eyalet bazında Hessen ilk örnek olarak karşımıza çıkmaktaysa da ilk ulusal veri koruma kanunu İsveç'te görülmektedir²⁰⁸. 11 Mayıs 1973 tarihli İsveç Veri Kanunu, 1972 yılında Resmî Belgelerin Aleniyet ve Gizliliği Parlamenter Komisyonu tarafından bilgisayarlı veri saklama konusunda yayımlanan “Bilgisayarlar ve Mahremiyet” (Computers and Privacy) isimli raporun doğurduğu bir sonuç olarak

²⁰⁴ FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, s. 55- 56.

²⁰⁵ Hessen Eyaleti'ne özgü anılan düzenlemenin Almanca ismi; “Hessische Datenschutzgesetz”dir.

Douwe KORFF, *Comparative Study on Different Approaches to New Privacy Challenges in Particular in the light of Technological Developments*, Country Studies: Germany, European Commission, 2010, s. 2.

²⁰⁶ Frits W. HONDIUS, *Emerging Data Protection in Europe*, North Holland Publishing Company, 1975, s. 35.

²⁰⁷ HONDIUS, *Emerging Data Protection in Europe*, s. 84- 85.

²⁰⁸ Hans Peter GASSMANN, *30 Years After: The Impact of the OECD Privacy Guidelines, Joint Roundtable of the Committee for Information, Computer and Communications Policy (ICCP), and its Working Party on Information Security and Privacy (WPISP)*, 10.03.2010, s. 2.

karşımıza çıkmaktadır. İsveç'in bu alanda ilk ulusal düzenlemeyi gerçekleştirmesi şaşırtıcı olmamıştır; çünkü anılan ülke geleneksel olarak açıklık ve kamusal erişim ilkelerine olağanüstü bir önem atfetmekte ve 1766 tarihli Basın Özgürlüğü Kanunu'ndan beri resmî belgelere kamunun erişimini garanti etmektedir. Ayrıca 1940'lı yıllardan itibaren kamusal alanda bilgisayarlaşmanın etkisiyle kişisel kimlik numarası gibi sistemleri uygulamaya koymuş bulunmaktadır²⁰⁹. Adı geçen kanunun en önemli özelliği, Veri İnceleme Kurulu adı altında bir kurul oluşturarak kişisel verilerin merkezi kaydının tutulması fikrinin tüm Avrupa Ekonomik Topluluğu (AET) bünyesinde yerleşmesini sağlamak olmuştur²¹⁰.

Avrupa Topluluğu (AT)²¹¹ bünyesinde ilk ulusal düzenlemeyi gerçekleştiren ülke ise Almanya olmuştur²¹². Ocak 1977 tarihinde ilk Federal Veri Koruma Kanunu uygulamaya konulmuştur. Federal Kanun, Hessen Eyaleti Veri Koruma Kanunu'ndan yaklaşık 7 yıl sonra yapılabilmektedir²¹³. Bu kanuna göre, kişisel verinin işlenmesi yalnızca iki şartta mümkün olmaktadır; ilgili kanun yahut başka bir kanun tarafından izin verilmiş olması veya ilgili kişinin rızasının bulunması halleri²¹⁴. Almanya'yı takiben Fransa, Ocak 1978'de Bilgi Teknolojileri, Veri Dosyaları ve Kamu Özgürlükleri Hakkında Kanun'u yürürlüğe koymuştur. Bu kanunun en önemli özelliği, daha sonra uzun bir süre veri koruma hukukunun mihenk taşı olacak olan 95/46/EC sayılı Avrupa Birliği (AB) Direktifi'ne ilham kaynağı olmasıdır²¹⁵.

²⁰⁹ Jonathan STEELE, "Data Protection: An Opening Door? The Relationship Between Accessibility and Privacy in Sweden in an EU Perspective", *Liverpool Law Review* 24, s. 19-20, ss. 19-39.

²¹⁰ FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, s. 59.

²¹¹ 2007 yılında imzalanan ve 2009 yılında yürürlüğe giren Lizbon Antlaşması ile Avrupa Topluluğu'nu kuran Antlaşmanın adı "Avrupa Birliği'nin İşleyişi Hakkında Antlaşma" olarak değiştirildi. Alexander H. TURK, "Lawmaking after Lisbon", *EU Law After Lisbon*, Ed. Andrea BIONDI, Piet EECKHOUT, Stefanie RIPLEY, Oxford University Press, 2012, s. 62- 63, ss. 62- 84.

²¹² J. Lee RICCARDI, "The German Data Protection Act of 1977: Protecting the Right to Privacy?", *Boston College International and Comparative Law Review*, Vol. 6, Issue: 1, 12.01.1983, s. 244, ss. 243- 271.

²¹³ Philippa WEBB, "A Comparative Analysis of Data Protection Laws in Australia and Germany", *Journal of Information, Law and Technology*, Y. 2003, Issue: 2, s. 11, ss. 2-26.

²¹⁴ RICCARDI, "The German Data Protection Act of 1977: Protecting the Right to Privacy?", s. 248.

²¹⁵ Nicole ATWILL, "Online Privacy Law: France", Library of Congress, June 2012, <http://www.loc.gov/law/help/online-privacy-law/2012/france.php>, E.T. 06.09.2017.

İlk yasal düzenlemeler genel hatlarıyla bu şekilde görünmekteyse de 1970’li yıllar başka birçok Avrupa ülkesinde veri koruması hakkında spesifik belgelerin ortaya çıktığı yıllar olmuştur. 1978 yılında Danimarka, benzer iki adet kanun düzenlemiştir; Özel Kayıtlar Kanunu ve Kamu Otoriteleri Kayıtları Kanunu. Bu iki kanun, kamu ve özel sektörün elindeki veri bankalarının yönetilmesi ile ilgilidir. Yine aynı yıl Norveç de Veri Kayıtları Kanunu altında bir düzenleme yapmıştır²¹⁶.

Spesifik yasal düzenlemelerin yanında bazı Avrupa ülkeleri, daha farklı bir yol izleyerek, veri işleme ve koruma sürecini anayasal düzenlemelerle teminat alma yoluna gitmiştir. Bunlardan ilki, 1976 tarihli Portekiz Anayasası’dır. Anılan Anayasa’nın 35. maddesinin başlığı “Veri İşlemenin Kullanımı”dır²¹⁷. Genel itibarıyla, tüm vatandaşların kendileri ile ilgili veri bankalarına erişim ve düzeltme hakkına sahip oldukları düzenlenmiştir. Ayrıca verinin tanımlanamaz hali istisna olmak üzere, kişinin siyasi fikri, dini inancı ya da özel yaşamı hakkında olması halinde veri işlenmesi yasaklanmıştır²¹⁸. 1978 yılına gelindiğinde ise Portekiz Anayasası’ndan etkilenen İspanyol Anayasası’nın 18. maddesinin 4. fıkrası ile karşılaşmaktayız. Hükme göre, vatandaşın onuru ile kişisel ve aile mahremiyet haklarının tam olarak kullanılmasını garanti etmek için bilgi teknolojilerinin kullanımı yasa ile sınırlandırılacaktır²¹⁹.

1978 yılında Avusturya, Kişisel Verilerin Korunmasına Dair Federal Kanun’u yürürlüğe koymuştur. Bu kanun, yukarıda anılan gerek ulusal ve spesifik düzenlemelerden gerekse anayasal hükümlerden farklı olarak, ilk bölümünde yer alan

²¹⁶ Albert J. MARCELLA, Carol STUCKI, *Privacy Handbook- Guidelines, Exposures, Policy Implementation and International Issues*, John Wiley & Sons Inc., 2003, s. 88; Peter BLUME, *Nordic Studies in Information Technology and Law*, Kluwer Law and Taxation Publishers, 1991, s. 2, 25.

²¹⁷ Eduardo SOARES, *Online Privacy Law: Portugal Country Report*, Library of Congress, June 2012, https://www.loc.gov/law/help/online-privacy-law/2012/portugal.php#_ftn6, E.T. 07.09.2017.

²¹⁸ Constitution of the Portuguese Republic 1976- 7th Revision 2005, <http://www.en.parlamento.pt/Legislation/CRP/Constitution7th.pdf>, E.T. 07.09.2017.

²¹⁹ Graciela RODRIGUEZ-FERRAND, *Online Privacy Law: Spain Country Report*, Library of Congress, June 2012, <https://www.loc.gov/law/help/online-privacy-law/2012/spain.php>, E.T. 18.05.2019.

“Veri Koruma Hakkı”nı anayasal koruma altına almıştır²²⁰. Bunun sebebi Avusturya anayasa hukukuna göre, anayasal değerde olan yasal düzenlemelerde yer alan tüm bireysel haklara anayasal koruma sağlanmasıdır²²¹. Bu bağlamda Avusturya bizatihi ve açıkça “Veri Koruma” kavramını anayasal koruma altına alan ilk ülke olmuştur²²².

1970’lerde veri işleme ve koruma sürecinin yasal düzenlemelerle ele alınması ile başlayan bu süreç, 1980’lerde konu ile ilgili uluslararası düzenlemelerin ortaya çıkışı ile devam etmiştir. Bu noktada günümüze dek değişen ve gelişen Avrupa Veri Koruma Hukuku’nun uluslararası düzenlemelere dair tarihçesine detaylı olarak girmeden evvel, tüm bu sürecin üç dalga halinde adlandırılmasına değinmek gerekmektedir. Buna göre 1970’lerde Almanya’nın Hessen Eyaleti’nin Veri Koruma Kanunu ile başlayan ve 1995 tarihli 95/46/AT Sayılı Direktif’e dek olan dönem, bireylere ilişkin veri işleme konusunun mahremiyet kavramından bağımsızlaşarak ayrı bir alan oluşturması hasebiyle veri koruma alanındaki yasal gelişmelerde “Birinci Dalga” olarak anılmaktadır. 95/46/AT Sayılı Direktif ise, kişisel verilerin işlenmesine ilişkin kuralların gelişiminde oldukça önem arz etmesi ve verilerin her tür ticarete entegrasyonunu sağlaması dolayısıyla veri koruma hukukundaki yasal süreçte “İkinci Dalga”yı başlatmaktadır. “Üçüncü Dalga” ise gelişen bilişim teknolojilerinin etkisi ile artık yeknesak kuralları karşılayan Genel Veri Koruma Tüzüğü’nün ortaya çıkışı ile olmuştur²²³.

G. KİŞİSEL VERİLERİN KORUNMASI KAPSAMINDA BAZI TEMEL KAVRAMLAR

Avrupa Veri Koruma Hukukunun uygulamadaki yansımasına yönelmeden önce bazı temel kavramların açıklanması, konunun anlaşılması için önem taşımaktadır. Alanın

²²⁰ Andreas LEHNER, “The Protection of Personal Data by the Austrian Constitutional Court”, *ICL Journal- Vienna Journal on International Constitutional Law*, Vol. 2, Issue: 3, 2017, s. 196- 198, <https://doi.org/10.1515/icl-2008-0304>, E.T. 07.09.2017.

²²¹ Lucas PRAKKE, Constantijn A. J. M. KORTMANN, *Constitutional Law of 15 EU Member States*, Kluwer Law International, 2005, s. 67- 68.

²²² FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, s. 71.

²²³ Andrew CHARLESWORTH, “CCTV, the GDPR and the Third Wave of Data Protection”, *The Watching The Watchers, A Cloudview White Paper*, 2017, s. 4-6, ss. 1- 20.

Türkiye’de çok da eski tarihlere gitmemesi sebebiyle birçok kavramın orijinal dili olan İngilizce’den Türkçe’ye aktarılmasında yeknesak bir kabul yoktur. Ayrıca konunun teknoloji ile ayrılmaz ilişkisi dolayısıyla pek çok teknik terim mevcuttur ve her geçen gün yenisi ortaya çıkabilmektedir. Dolayısıyla burada açıklanacak kavramlar sınırlı sayıda değildir ve yalnızca çalışma kapsamında en çok bahis konusu edilenlere yönelik olacaktır.

Açıklamalara, çalışma konusu kapsamında en çok dile getirilen kavram olan “kişisel veri” ile başlamak gerekmektedir. Fakat önce kısaca da olsa kişisel veri ifadesinde geçen bir unsur olarak “veri” kavramına bakılacaktır. Öncelikle belirtilmelidir ki, doktrinde enformasyon ve bilgi kavramları ile veri kavramının birbirlerinden farklı olduğu ve muadil biçimde kullanılmamaları gerektiğini dile getiren bazı yazarlar mevcuttur²²⁴. Bu konuda çalışmamızda takip edeceğimiz usulü belirtmeden önce “veri” kavramının tanımını yapmamız gerekmektedir. Buna göre veri, bilginin bilgisayarlarca kullanılabilir ve işlenebilir sayısal birimlerde gösterilmiş halini karşılamaktadır²²⁵. Ancak bu tanımda yalnızca bilgisayar verisi ele alınmaktadır. Bu durum ise doktrinde eleştirilmekte ve şayet bu şekliyle kabul edilirse konunun koruma alanının oldukça daralacağı, haklı olarak belirtilmektedir²²⁶. Oysa konunun kapsamı gereği çalışmamızda veri kavramı hem bilgisayar verisi hem elektronik ortamda tutulan veri hem de elektronik ortam dışı tutulan veriyi karşılamaktadır.

“Kişisel veri”, belirli ya da belirlenebilir nitelikteki bir kişiye ilişkin her türlü bilgidir²²⁷. Bu tanım gerek ulusal gerekse uluslararası birçok metinde yer almaktadır²²⁸.

²²⁴ Anthony LIEW, “Understanding Data, Information, Knowledge and Their Inter-Relationships”, *Journal of Knowledge Management Practice*, C. 8, No: 2, June 2007.

²²⁵ Mehmet Bedii KAYA, *Teknik ve Hukuki Boyutlarıyla İnternete Erişimin Engellenmesi*, On İki Levha Yayıncılık, İstanbul, 2010, s. 5.

²²⁶ KÜZECİ, *Kişisel Verilerin Korunması*, s. 10; Murat Volkan DÜLGER, *Bilişim Suçları ve İnternet İletişim Hukuku*, Seçkin Yayıncılık, Ankara, 2014, s. 74- 75.

²²⁷ Christopher MILLARD, W. Kuan HON, “Defining ‘Personal Data’ in E-Social Science”, *Information, Communication and Society*, Vol. 15, No:1, February 2012, s. 68- 69, ss. 66- 84.

²²⁸ Kişisel veri kavramının en güncel ulusal tanımına baktığımızda, 6698 Sayılı Kişisel Verilerin Korunması Kanunu’nun 3. maddesine göre, “Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi” tanımının kabul edildiği görülmektedir. Ulusalüstü alanda ise Avrupa Komisyonu’nun 2016/679 Sayılı Genel Veri Koruma Tüzüğü’nün 4. Maddesine göre kişisel veri, “belirli veya belirlenebilir bir gerçek kişiye

Bu bağlamda 95/46/AT Sayılı Direktif'in 29. maddesi uyarınca kurulan Çalışma Gurubu, kişisel veri kavramının içeriğinin belirlenmesi için 20 Haziran 2007'de 4/2007 Sayılı Görüş'ünü açıklamıştır²²⁹. Buna göre kişisel veri kavramı söz konusu tanımda görüleceği üzere, mümkün olduğunca geniş tutulmuştur. Burada önem arzeden husus, bilginin belirli ya da belirlenebilir nitelikteki bir kişi ile ilişkilendirilebilir olmasıdır.

Kişi ile ilgili "her türlü bilgi" kavramın kapsamındadır. Şöyle ki, bu bilgi objektif ya da sübjektif olabilir. Hatta doğru ya da kanıtlanmış bilgi olması da gerekli değildir. Söz gelimi, "Bay A iyi bir çalışandır." ya da "Bay A'nın sağlık raporlarına bakıldığında yakında ölmeyeceği tahmin edilmektedir." gibi bilgiler bu bağlamda değerlendirilebilecektir. Bilginin "kişi ile ilgili olması" da kavram bakımından önemli bir noktadır. Örneğin bir evin maddi değeri tek başına kişisel veri teşkil etmezken, vergi yükümlülüğünü belirlemek için evin malikinin kimliği ile ilişki kurulduğunda bu artık kişisel veri teşkil edecektir. Bir başka örnek olarak bir aracın servis kayıtları, plakası ile ve oradan da aracın sahibi ile ilişki kurulması bakımından kişisel veri teşkil edebilecektir. Kavrama ilişkin önem arzeden bir diğer husus da bilginin "belirli ya da belirlenebilir" nitelikteki bir kişiye ilişkin olmasıdır. Bilginin doğrudan (isim yolu ile) ya da dolaylı (telefon numarası ya da kimlik numarası gibi yollarla) olarak kişi ile ilişkilendirilebilir olması halleri bu bağlamda düşünülmelidir. Ayrıca bazı belirlenebilir bilgiler başka hiçbir ilave bilgiye ihtiyaç olmaksızın kişi ile ilişkilendirilebilirken (örneğin Türkiye Cumhuriyeti'nin kurucusu gibi) bazı bilgiler için ek başka bazı bilgilerin

ilişkin her türlü bilgidir ('veri öznesi'); tanımlanmış bir gerçek kişi özellikle bir isim, kimlik numarası, konum verileri, çevrim içi tanımlayıcı ya da söz konusu gerçek kişinin fiziksel, fizyolojik, genetik, ruhsal, ekonomik, kültürel veya toplumsal kimliğine özgü bir ya da daha fazla sayıda faktöre atıfta bulunularak doğrudan veya dolaylı olarak tanımlanabilen bir kişidir." Görüleceği üzere Tüzük aynı tanımı, biraz daha detaylı açıklayarak kabul etmiştir. Bunlar dışında, Avrupa Birliği'nin 95/46/AT Sayılı Direktifi'nin 2. maddesi, Avrupa Konseyi'nin 108 Sayılı Sözleşmesi'nin 2. maddesi ve OECD'nin 1980 yılında yayınlanan Rehber İlkeleri'nin 1. Maddesi de kişisel veri kavramını bu biçimde tanımlamıştır.

²²⁹ Article 29 Data Protection Working Party, Opinion 4/2007 on the Concept of Personal Data, 20.06.2007, 01248/07/EN WP136, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf, E.T. 17.05.2019.

kombinasyonuna ihtiyaç duyulabilir. Neticesinde önemli olan kişinin belirlenebilirliğinin sağlanmasıdır.

Kişisel veri genel itibarıyla bu şekilde ele alınmaktadır. Bazı kişisel veri türleri ise, ulusal ve uluslararası metinlerde çok daha özel nitelikli bir koruma gerektirdiklerinden bahisle “hassas veri”, “özel nitelikli veri” şekillerinde adlandırılmaktadır²³⁰. İlk defa 1981 yılındaki Avrupa Konseyi Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi’nin 6. maddesi ile veri koruma hukuku alanında ilave bir korumaya alınan “hassas veri”, ırk, etnik köken, siyasi görüş, dini veya felsefi inanç, sendika veya dernek üyeliği, genetik veriler, biyometrik veriler, sağlık verileri, cinsel yaşam veya cinsel eğilime dair verileri içermektedir²³¹. Görüleceği üzere bu verilerin kişinin temel hak ve özgürlükleri ile oldukça yakın bir ilişkisi mevcuttur. 6698 Sayılı KVKK’nın Gerekçesi’nde de belirtildiği üzere, bu verilerin açıklanması ile kişi ayrımcılığa maruz kalabilecek veya zarar görebilecektir²³². Bu bakımdan hassas veriler, kişisel veri korumasında daha yüksek bir korumayı öngören özel bir kategoriye temsil etmektedirler²³³.

²³⁰ Hassas veri kavramının güncel ulusal tanımına bakacak olursak, 6698 Sayılı KVKK’nın “Özel nitelikli kişisel verilerin işlenme şartları” başlıklı 6/1. maddesine göre, “*Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir.*” 2016/679 Sayılı GVKT’nin “Özel kategorilerdeki kişisel verilerin işlenmesi” başlıklı 9/1. Maddesine göre ise, “*İrk veya etnik köken, siyasi görüşler, dini veya felsefi inançlar ya da sendika üyeliğinin ifşa edildiği kişisel verilerin işlenmesi ve bir gerçek kişinin kimlik teşhisinin yapılması amacıyla genetik veriler ile biyometrik verilerin, sağlık ile ilgili verilerin veya bir gerçek kişinin cinsel yaşamı veya cinsel eğilimine ilişkin verilerin işlenmesi yasaktır.*” denilerek kavramın tanımı, temel kuralın açıklanması ile ortaya konulmuştur. Burada yalnızca metinlerin tanımlamalarına değinilmekle yetinilecektir. KVKK ve GVKT’nin tanımsal farklılıklarına ilişkin hem KVKK’nın ele alındığı bölümde hem de konu ile ilgili olarak Türk Anayasa Mahkemesi’nin içtihatlarının ele alındığı bölümlerde çeşitli açıklamalar yapılmıştır.

²³¹ Rebecca WONG, “Data Protection Online: Alternative Approaches to Sensitive Data?”, *Journal of International Commercial Law and Technology*, Vol. 2, No:1, 2007, s. 10, ss. 9- 16.

²³² Aydın AKGÜL, *Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması*, Beta, 2014, s. 18.

²³³ BYGRAVE, *Data Protection Law: Approaching its Rationale, Logic and Limits*, s. 68.

Kişisel verilerin korunması kapsamında ele alınması gereken bir diğer kavram ise, “kişisel verilerin işlenmesi (*processing*)”dır²³⁴. Tüm veri koruma hukuku, veri işlenmesinin hukuka uygun olup olmadığı üzerinde yükselmektedir. Bu bakımdan kavramın en genel biçimi ile tanımlanması faydalı olacaktır. Kişisel verilerin işlenmesi, verilerin otomatik olan ya da olmayan yollarla elde edilmesi, toplanması, saklanması, kayıt altına alınması, muhafaza edilmesi, değiştirilmesi, silinmesi, yok edilmesi, yeniden düzenlenmesi, başka bir biçimde elde edilebilir hale getirilmesi, aktarılması, işaretlenmesi, sınıflandırılması, kullanımının engellenmesi, açıklanması “gibi” tüm iş ve işlemler bütününe karşılamaktadır²³⁵. Bu genel tanımda bulunan “gibi” ifadesi oldukça önemlidir, çünkü özellikle teknolojinin gelişmesi ile veri işleme metodları da çeşitlenebilecektir. Dolayısıyla kavramın tanımını kadük bırakmamak için çoğu ulusal ve uluslararası metin bu yolu takip etmektedir.

Kişisel verilerin korunması alanında önem taşıyan bir başka kavram da “veri öznesi (*data subject*)”dır. En genel şekliyle, kişisel verilerin korumasının konusu olan kişi olarak adlandırılan veri öznesi, ilgili kişi olarak da anılmaktadır²³⁶. Verilerin nitelediği esas kişi olan veri öznesi, GVKT’nin de benimsediği deyimdir. Öte yandan KVKK ilgili kişi deyimini benimsemiştir. Avrupa Veri Koruma Denetçisi Veri Koruma

Her ne kadar birçok ulusal ve uluslararası metin belirtildiği üzere hassas veriler için özel bir koruma öngörse de Avrupa Veri Koruma Hukuku bağlamında OECD Rehber İlkeleri bu tür verilere yönelik özel bir koruma biçimi öngörmemiştir. KÜZECİ, *Kişisel Verilerin Korunması*, s. 250.

²³⁴ Kişisel verilerin işlenmesi kavramının ulusal alanda güncel tanımına bakacak olursak KVKK’nın 3/1. maddesine göre, “*Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem*” veri işlemeyi oluşturur. GVKT’nin 4. maddesinde yer alan “işleme” kavramının tanımı da açıklanan tanımlarla yaklaşık olarak aynıdır.

²³⁵ “What constitutes data processing?”, *Reform of EU Data Protection Rules*, European Commission, https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-constitutes-data-processing_en , E.T. 17.05.2019.

²³⁶ KÜZECİ, *Kişisel Verilerin Korunması*, s. 15.

Sözlüğü’nde yer alan bir diğer tanıma göre veri öznesi, kişisel verileri toplanan, tutulan ve işlenen kişidir²³⁷.

Kişisel verilerin korunması alanında veri öznesinin kişisel verilerinin işlenmesi sürecine dahil olan bir başka aktör de “veri denetleyicisi (*data controller*)”dir. Türkçe metinlerde “veri sorumlusu” olarak da ifade edilen kavrama göre, “verilerin işlenmesinin amaç ve araçlarına karar veren kişi ya da kişilerdir²³⁸. Bu noktada ele alınması gereken bir diğer kavram da, veri denetleyicisi ile oldukça ilişkili olan “veri işleyicisi (*data processor*)”dir. Veri işlemede amaç ve araçlara karar veren kişi ya da kişiler veri denetleyicisi olsa da gerçek işlemeyi veri denetleyicisi adına yapan başka bir gerçek veya tüzel kişi, kamu otoritesi, ajans veya başka bir kurum da bulunabilir. Bu kişi ya da kişilere “veri işleyicisi” denilmektedir. Denetleyici, verinin işlenmesinin hukuka uygunluğundan, verilerin korunmasından ve veri öznelerinin haklarına saygı duymaktan sorumludur. İşleyici ise yalnızca denetleyicinin talimatları ile bağlı ve onun adına davranmaktadır. Söz gelimi bir üniversite binasına girerken giriş-çıkışları kayıt altına alan özel güvenlik şirketi, kişilerin bilgilerini kendi amaçları için değil, söz konusu üniversite adına işlemektedir²³⁹.

²³⁷ “Data Subject”, *European Data Protection Supervisor, Data Protection, Glossary*, https://edps.europa.eu/data-protection/data-protection/glossary_en, E.T. 17.05.2019.

²³⁸ “Data Controller”, *European Data Protection Supervisor, Data Protection, Glossary*, https://edps.europa.eu/data-protection/data-protection/glossary_en, E.T. 17.05.2019.

²³⁹ “Processor”, *European Data Protection Supervisor, Data Protection, Glossary*, https://edps.europa.eu/data-protection/data-protection/glossary_en, E.T. 17.05.2019.

İKİNCİ BÖLÜM

AVRUPA VERİ KORUMA HUKUKU

Çalışmamızın İkinci Bölümünde öncelikle Avrupa Veri Koruma Hukuku’nu doğuran etkenler ve hukuki düzenlemeler ortaya konulacaktır. Bu bakımdan bu alanda birinci dalga yasal düzenleme olarak adlandırılan 108 Numaralı Kişisel Verilerin Otomatik Olarak İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşme’nin bir bakıma hazırlık çalışmaları gibi de görülebilecek olan OECD’nin Rehber İlkeleri’ne dair yapılacak açıklamanın ardından Avrupa Konseyi kapsamındaki çalışmalar ele alınacaktır. Bu noktada İnsan Hakları Avrupa Mahkemesi’nin konuya ilişkin içtihatlarının üzerinde durularak Mahkeme’nin kişisel verilerin korunması alanında ne gibi bir bakış açısına sahip olduğu belirlenecektir. Avrupa Birliği’ne gelindiğinde ise gerek AB Temel Haklar Şartı gerekse Avrupa Veri Koruma Hukuku’nun ikinci dalga yasal düzenlemesi olan 95/46/AT Sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi, Adalet Divanı’nın bu metinlere dair bazı içtihatları ile ortaya konulmaya çalışılacaktır. İlgili düzenlemeler sonrası Veri Koruma Reformu’na götüren hukuki metinlerin incelenmesinin devamında ise Reform’un temel metni olarak düşünülebilecek 2016/679 Sayılı Genel Veri Koruma Tüzüğü, getirdiği tüm yeniliklerle ele alınacak ve en nihayetinde 95/46/AT Sayılı Direktif ile karşılaştırılarak bu iki düzenlemenin üye ülkelerin ulusal hukuk düzenlerinde ne gibi metinlerle karşılama bulduğu belirtilecektir.

Bilgilerin işlenmesi hususu, 1970’lerin sonuna gelindiğinde birçok kuruluş ve kişinin ilgisini çekmiş ve bu konuda uluslararası düzenlemelerin oluşturulmasına sebep olmuştur. Bu durumdan dolayı iki temel uluslararası düzenleme ortaya çıkmıştır: OECD’nin 1980 tarihli “Özel Yaşamın Gizliliğinin ve Sınır Ötesi Kişisel Veri Dolaşımının Korunmasına İlişkin Rehber İlkeler”i (*OECD Rehber İlkeleri*) ile Avrupa Konseyi’nin 1981 tarihli ve 108 sayılı “Kişisel Verilerin Otomatik Olarak İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşme”si (108 sayılı Sözleşme).

1948 yılında kurulan ve Avrupa Ekonomik İşbirliği Topluluğu olarak bilinen OEEC'nin devamı sayılan ve genel olarak OECD olarak bilinen, Ekonomik İşbirliği ve Kalkınma Örgütü 30 Eylül 1961 tarihinde, ekonomik kalkınma ve dünya ticaretini desteklemek amacıyla kurulmuştur. İlk planda 18 ülkenin üyeliği ile başlayan süreç, günümüzde dünyanın dört bir yanından 35 ülke ile yola devam etmektedir. OECD'nin resmi dilleri İngilizce ve Fransızca olup merkezi Paris'tedir²⁴⁰.

OECD veri korumasına ilişkin olarak 1980 yılında, uluslararası düzlemde bu alana yönelik ilk düzenlemeleri içeren “Özel Yaşamın Gizliliğinin ve Sınır Ötesi Kişisel Veri Dolaşımının Korunmasına İlişkin Rehber İlkeler”i yayımlamıştır. Bu düzenlemenin önemli özelliklerinden biri, gerek Amerika Birleşik Devletleri gerek de Avrupa ülkeleri tarafından üzerinde uzlaşmış bir metin olmasıdır²⁴¹.

OECD'nin bilgisayarlaşma meselesine yönelmeye başlaması, 1968 yılındaki “OECD Ülkelerinde Bilim” isimli Bakanlar Toplantısı'nın “Teknolojideki Boşluklar” konusunu ele alması ile olmuştur²⁴². Devamında OECD Bilim Politikası Komitesi, konunun daha detaylı araştırılması için “Bilgisayar Kullanım Grubu (Computer Utilisation Group)” adı altında bir çalışma grubu oluşturmuştur²⁴³. 1971 yılına gelindiğinde, OECD Bilişim Çalışmaları Serisi bağlamında, “Kamu Yönetiminde Bilgisayarlı Veri Bankaları”, “Veri Koruma ve Mahremiyet Konularında Politika

²⁴⁰ Warren CHRISTOPHER, *In the Stream of History- Shaping Foreign Policy for a New Era*, Stanford University Press, 1998, s. 165.

²⁴¹ Michael KIRBY, “The History, Achievement and Future of the 1980 OECD Guidelines on Privacy”, *International Data Privacy Law*, Vol. 1, No: 1, Y.: 2011, ss. 6- 14, s. 6; Working Party for Information Security and Privacy (WPISP), *The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines*, Directorate for Science, Technology and Industry– Committee for Information, Computer and Communications Policy, 06.04.2011, s. 12, <http://www.oecd-ilibrary.org/docserver/download/5kgf09z90c31en.pdf?expires=1516186345&id=id&accname=guest&checksum=DCF492E917A83B087F7FCAE3125E7D32F>, E.T. 16.09.2017,

²⁴² “The Third Ministerial Meeting on Science at OECD”, March 1968, *The OECD Observer*, No: 33, April 1968, s. 15- 17.

²⁴³ KIRBY, “The History, Achievement and Future of the 1980 OECD Guidelines on Privacy”, s. 7; HONDIUS, *Emerging Data Protection in Europe*, s. 57- 58.

Sorunları” ve “Dijital Bilgi ve Mahremiyet Problemi” gibi raporlar yayımlanmıştır²⁴⁴. Açıktır ki, OECD veri koruma meselesini gittikçe odak noktasına taşımıştır.

Meseleye artan ilgi sonucu OECD 1972 yılında, “Veri Bankası Paneli” adı altında bir kurul oluşturmuştur. Bu kurul 1974 yılında, “Veri Koruma ve Mahremiyet Konularında Politika Sorunlarına Dair OECD Semineri”ni düzenlemiştir. Bu toplantıda, “Kişisel Tanımlayıcı ve Mahremiyet”, “Vatandaşların Kendilerine Dair Dosyalara Erişim Hakkı” ve “Sınır Ötesi Veri Dolaşımı için Kurallar” başlıklı oturumlar söz konusuydu²⁴⁵. Bir süre sonra, sonuncu başlık OECD’nin veri koruma konusuna dair odak noktasını oluşturacaktı²⁴⁶.

OECD’nin birincil amaçlarından biri, dünya ticaretinin artmasını desteklemektir. Bu bağlamda ilgili kuruluş, ulusal düzenlemelerin bilginin serbest dolaşımını engelleyici sınırlar oluşturabileceği ve bu durumun büyümeyi engelleyeceği konusunda endişeler taşımaktaydı²⁴⁷. Bu sebeple, belirlenen bir ülkeden diğerine yasal olarak veri aktarma imkânı anlamına gelen sınır ötesi veri dolaşımı kavramı²⁴⁸, giderek OECD’nin ana gündemini oluşturmaya başlamıştır.

²⁴⁴ Working Party for Information Security and Privacy (WPISP), *The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines*, Directorate for Science, Technology and Industry – Committee for Information, Computer and Communications Policy, 06.04.2011, <http://www.oecd-ilibrary.org/docserver/download/5kgf09z90c31en.pdf?expires=1516186345&id=id&accname=guest&checksum=DCF492E917A83B087FFCAE3125E7D32F>, E.T. 16.09.2017, s. 9.

²⁴⁵ KIRBY, “The History, Achievement and Future of the 1980 OECD Guidelines on Privacy”, s. 7; Working Party for Information Security and Privacy (WPISP), *The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines*, Directorate for Science, Technology and Industry – Committee for Information, Computer and Communications Policy, 06.04.2011, <http://www.oecd-ilibrary.org/docserver/download/5kgf09z90c31en.pdf?expires=1516186345&id=id&accname=guest&checksum=DCF492E917A83B087FFCAE3125E7D32F>, E.T. 16.09.2017, s. 9.

²⁴⁶ GASSMANN, *30 Years After: The Impact of the OECD Privacy Guidelines*, s.1.

²⁴⁷ Working Party for Information Security and Privacy (WPISP), *The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines*, Directorate for Science, Technology and Industry – Committee for Information, Computer and Communications Policy, 06.04.2011, <http://www.oecd-ilibrary.org/docserver/download/5kgf09z90c31en.pdf?expires=1516186345&id=id&accname=guest&checksum=DCF492E917A83B087FFCAE3125E7D32F>, E.T. 16.09.2017 s. 10.

²⁴⁸ Christopher KUNER, *Regulation of Transborder Data Flows Under Data Protection and Privacy Law: Past, Present and Future*, OECD Digital Economy Papers No: 187, OECD Publishing, 2011, s. 14.

1977 yılında OECD Veri Bankası Paneli isimli kurul, “Sınır Ötesi Veri Dolaşımı ve Mahremiyetin Korunması Sempozyumu” adı altında bir etkinlik düzenlemiştir. Bu etkinliğin en önemli özelliği, sınır ötesi veri dolaşımındaki ulusal çıkar ve bunun ekonomik değerine vurgu yapılmış olmasıdır. Ayrıca bu etkinlikle birlikte Veri Bankası Paneli kurulunu dağıtılmış ve yerine OECD Uzman Grubu oluşturulmuştur²⁴⁹.

1978 yılına gelindiğinde OECD Uzman Grubu’nun tek bir gayesi bulunmaktaydı; Sınır ötesi kişisel verilerin dolaşımı ve mahremiyetin korunması hakkında rehber ilkeleri oluşturabilmek²⁵⁰. Nihayetinde Eylül 1980’de OECD, Özel Yaşamın Gizliliğinin ve Sınır Ötesi Kişisel Veri Dolaşımının Korunmasına İlişkin Rehber İlkeler Hakkında Öneri’yi kabul etmiştir²⁵¹. OECD Rehber İlkeleri, her ne kadar dünya çapında oldukça ses getirse de tavsiye kararı olmaları sebebiyle üye ülkeleri bağlayıcı değildir. Dolayısıyla üye ülkeler bu ilkeleri iç hukuk düzlemlerine taşıyıp taşımamakta özgürdürler. Anılan ilkeler, kişisel veriler bağlamında mahremiyet ve bireysel özgürlükleri korumayı amaçlamaktadır²⁵². Ayrıca ulusal mevzuatlarda “sınır ötesi kişisel verilerin serbest dolaşımını” engelleyen herhangi bir farklılıktan kaçınarak, kişisel verilerin sınır ötesi akışlarının da korunması istenmektedir. Bu bağlamda birazdan aşağıda anılacak olan ilkeler, veri korumasına dair minimum şartları ortaya koymaktadır²⁵³.

²⁴⁹ Working Party for Information Security and Privacy (WPISP), *The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines*, Directorate for Science, Technology and Industry – Committee for Information, Computer and Communications Policy, 06.04.2011, <http://www.oecd-ilibrary.org/docserver/download/5kgf09z90c31en.pdf?expires=1516186345&id=id&accname=guest&checksum=DCF492E917A83B087FFCAE3125E7D32F>, E.T. 16.09.2017, s. 10.

²⁵⁰ KIRBY, “The History, Achievement and Future of the 1980 OECD Guidelines on Privacy”, s. 8; James MICHAEL, *Privacy and Human Rights: An International and Comparative Study with Special Reference to Developments in Information Technology*, UNESCO, 1994, s. 34- 35.

²⁵¹ *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 23 Eylül 1980, <https://www.oecd.org/internet/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsofPersonalData.htm>, E.T. 16.09.2017. İlgili İlkeler 2013 tarihinde revize edilmiştir.

²⁵² FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, s. 79.

²⁵³ *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 23 Eylül 1980, <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsOfPersonalData.htm>, E.T. 16.09.2017.

OECD Rehber İlkeleri bağlamında üye ülkelerde kişisel verinin işlenmesi süreci sekiz adet temel ilkeye dayanmaktadır. Buna göre;

- Madde 7: (Veri) Toplamanın Sınırlanması İlkesi,
- Madde 8: Veri Kalitesi İlkesi²⁵⁴,
- Madde 9: Amacın Belirli Olması İlkesi,
- Madde 10: Kullanımın Sınırlı Olması İlkesi,
- Madde 11: Güvenlik Önlemleri İlkesi²⁵⁵,
- Madde 12: Açıklık İlkesi,
- Madde 13: Bireysel Katılım İlkesi,
- Madde 14: Hesap Verilebilirlik İlkesi.

OECD Rehber İlkeleri'nin oluşturulmasının ardından, OECD veri koruma alanında aktif rol oynamaya devam etmiştir. Söz gelimi, 11 Nisan 1985 tarihinde "Sınır Ötesi Veri Dolaşımına Dair Deklarasyon"u kabul etmiştir²⁵⁶. Fakat OECD Rehber İlkeleri'nin ardından, Avrupa ölçeğinde çok daha ses getirici bir etki taşıyacak ve hukuki açıdan bağlayıcı olan bir düzenleme, Avrupa Konseyi tarafından hazırlanmaktaydı. Dolayısıyla OECD Rehber İlkeleri, Avrupa Konseyi'nin konuya ilişkin düzenlemeleri açısından hazırlık çalışması gibi de okunabilecektir.

I. AVRUPA KONSEYİ

İkinci Dünya Savaşı sonrası ürünlerinden olan Avrupa Konseyi, 1949 yılında Avrupa ölçeğinde ortak demokrasi anlayışını geliştirmeyi hedefleyen ve 10 Avrupa ülkesi tarafından kurulan uluslararası bir organizasyondur. Günümüzde 47 ülkeden oluşan bu

²⁵⁴ Verilerin belirli bir niteliği karşılamaını ifade etmektedir. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 23 Eylül 1980, <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprivacyandtransborderflowsofpersonaldata.htm> , E.T. 16.09.2017.

²⁵⁵ Veri güvenliği hususunu ifade etmektedir. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 23 Eylül 1980, <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprivacyandtransborderflowsofpersonaldata.htm> , E.T. 16.09.2017.

²⁵⁶ FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, s. 80.

kuruluş Strazburg’da bulunmakta ve resmi dil olarak İngilizce ve Fransızca’yı kabul etmektedir²⁵⁷.

Avrupa Konseyi, bazı hukuksal çalışmalar yürüterek çeşitli hukuki metinlerin kabulünü bölgesel ölçekte sağlamak ve böylece temel amaçlarından biri olan insan haklarını korumaktadır²⁵⁸. Bu doğrultuda Avrupa Konseyi’nin veri koruma alanına dair dolaylı ilk çalışması 3 Eylül 1953 tarihinde yürürlüğe giren İnsan Hakları Avrupa Sözleşmesi’dir²⁵⁹. Ancak Konsey 70’lerin başında İHAS’ın 8. maddesinin özellikle bilişim teknolojilerinde yaşanan gelişmeler bakımından sınırlı kaldığı sonucuna varmıştır²⁶⁰. Bunun devamında daha spesifik düzenlemelere gidilmiş ve 1968 yılında 509 Numaralı İnsan Hakları ve Modern Bilimsel ve Teknolojik Gelişmeler Hakkında Tavsiye Kararı²⁶¹, 1973 yılında 22 Numaralı Özel Sektördeki Elektronik Veri Bankalarında Gerçek Kişilerin Mahremiyetinin Korunması Kararı²⁶² ile 1974 yılında 29 Numaralı Kamu Sektöründeki Elektronik Veri Bankalarında Gerçek Kişilerin Mahremiyetinin

²⁵⁷ Desmond DINAN, *Europe Recast: A History of European Union*, Lynne Rienner Publishers, 2014, s.5-7, 11-13; Olivier DE SCHUTTER, *International Human Rights Law*, Cambridge University Press, 2010, 21; “Founding Fathers”, “Our Member States”, “Headquarters and Offices”, <https://www.coe.int/en/web/about-us/> , E.T. 19.09.2017.

Kurucu ülkeler; Belçika, Birleşik Krallık, Danimarka, Fransa, Hollanda, İrlanda, İsveç, İtalya, Lüksemburg ve Norveç’tir. Bu ülkelere kısa bir süre sonra Türkiye’de dahil olmuştur.

“Council of Europe”, <https://www.britannica.com/topic/Council-of-Europe> , E.T. 19.09.2017.

²⁵⁸ Manfred NOWAK, *Introduction to the International Human Rights Regime*, The Raoul Wallenberg Institute Human Rights Library, Vol. 14, Brill- Martinus Nijhoff Publishers, 2003, 168 vd.; “Values: Human Rights, Democracy, Rule of Law”, <https://www.coe.int/en/web/about-us/values> , E.T. 19.09.2017.

²⁵⁹ Anılan Sözleşme’nin tam adı: The Convention for the Protection of Human Rights and Fundamental Freedoms- İnsan Hakları ve Temel Özgürlüklerin Korunmasına İlişkin Sözleşme’dir.

“European Convention on Human Rights”, <http://www.echr.coe.int/pages/home.aspx?p=basictexts> , E.T. 19.09.2017.

²⁶⁰ DE HERT, GUTWIRTH, “Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action”, *Reinventing Data Protection*, s. 5.

²⁶¹ Recommendation 509 (1968) Human Rights and Modern Scientific and Technological Developments, <http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=14546&lang=en> , E.T. 19.09.2017.

²⁶² Resolution 73 (22) on the Protection of the Privacy of Individuals vis-a-vis Electronic Data Banks in the Private Sector <https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=589402&SecMode=1&DocId=646994&Usage=2> , E.T. 19.09.2017.

Korunması Kararı²⁶³ ortaya çıkmıştır. 1981 yılında ise Avrupa Konseyi bireylerin temel hak ve özgürlüklerinin, özellikle de mahremiyet haklarının kişisel verilerin işlenmesiyle ilgili olarak korunması amacıyla ayrı bir Veri Koruma Sözleşmesi düzenlemiştir. Avrupa Konseyi'nin kişisel verilerin korunmasına dair ilk bağlayıcı hukuki düzenlemesi olan söz konusu 108 Sayılı Sözleşme 1 Ekim 1985 tarihine gelindiğinde yürürlüğe girmiştir²⁶⁴. Dolayısıyla görülmektedir ki artık veri koruma, mahremiyetin korunmasından çok daha geniş ve spesifik bir hal almaktadır²⁶⁵.

Avrupa Konseyi, bilgisayarlaşmanın getirdiği teknolojik değişimler ve veri koruma konularının önemini özellikle 1960'lı yıllar ile birlikte anlamaya başlamıştır. Bu doğrultuda 1968 yılında 509 Numaralı İnsan Hakları ve Modern Bilimsel ve Teknolojik Gelişmeler Hakkında Tavsiye Kararı'nı yayımlamıştır. Bu karara göre, modern bilimsel ve teknolojik yöntemler, başta mahremiyet hakkı olmak üzere tüm hak ve özgürlüklere yönelik tehdit oluşturmaktadır²⁶⁶.

Bu kararın devamında İnsan Hakları Uzmanları Komitesi kurulmuştur²⁶⁷. Anılan komite, 509 Numaralı Karar'da bahis konusu edilen tüm teknolojik gelişmelerin kontrol altında olduğunu; fakat bu kararda söz konusu edilmeyen bir kavramın ciddi sorunlar doğuracağını dile getirmiştir: Bilgisayarlar²⁶⁸. Bu sebeple Avrupa Konseyi 1970'lerin başıyla birlikte, kişilerin mahremiyetlerinin korunması meselesini yeniden ele alarak, bu

²⁶³ Resolution 74 (29) on the Protection of the Privacy of Individuals vis-a-vis Electronic Data Banks in the Public Sector, <https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=590512&SecMode=1&DocId=649498&Usage=2>, Erişim Tarihi: 19.09.2017.

²⁶⁴ Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108>, E.T. 19.09.2017.

²⁶⁵ DE HERT, GUTWIRTH, "Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action", *Reinventing Data Protection*, s. 6.

²⁶⁶ Recommendation 509 (1968) Human Rights and Modern Scientific and Technological Developments, Par. 8, <http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=14546&lang=en>, E.T. 19.09.2017.

²⁶⁷ FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, s. 84.

²⁶⁸ Frits W. HONDIUS, *The Council of Europe's Work in the area of Computers and Privacy*, Discussion Paper on the Use of Data Processing, Parliamentary Assembly of the Council of Europe, 18- 19 May 1978, s.2.

defa bilgisayarların doğurduğu bilgi ve veri mahremiyeti konularına yönelmeyi amaçlamıştır²⁶⁹.

509 Numaralı Tavsiye Kararı'nın ardından Avrupa Konseyi, teknik cihazlar tarafından mahremiyete müdahalelere karşı vatandaşın korunması konusuna daha fazla yönelerek bu alanda yeni adımlar atmıştır. Bu bağlamda, 1973 yılında 22 Numaralı Özel Sektördeki Elektronik Veri Bankalarında Gerçek Kişilerin Mahremiyetinin Korunması İlke Kararı yayımlanmıştır. Bu karar üye ülkelere, özel sektörde bulunan elektronik veri bankalarında saklanan kişisel bilgilere ilişkin uygulanacak olan on adet temel ilkeyi ortaya koymakta ve buna göre etkili adımlar atılmasını tavsiye etmektedir. 22 Numaralı İlke Kararı'na göre bu on temel ilke şunlardır: Saklanan verinin belli bir kalitede olması, verinin edinilmesinin bir amacı olması, verinin hangi yollarla edinilebileceği, hangi verinin hangi sürede saklanabileceği, veriye erişim için yetkili merci, verinin ilgili olduğu kişinin bilgilendirilmesi, saklanan verinin düzeltilmesi veya ortadan kaldırılması, kötüye kullanımların önüne geçilmesi, veriye erişim ve istatistiki veriler²⁷⁰. Ayrıca bu kararda “bilgi” ve “veri” kavramları birbirlerinin yerine kullanılarak, “*Kişilerin mahrem alanına dair bilgiler kaydedilemez ve hiçbir durumda yayılamaz.*” denilmiştir. Dolayısıyla görülebileceği üzere, “özel yaşamın mahrem alanı” (*intimate private life*) kavramına da üstü örtülü bir biçimde değinilmiştir²⁷¹.

Özel sektördeki veri bankalarının durumunun belirlenmesinin ardından, aynı durumun kamu sektöründeki yansıması olarak 1974 yılında 29 Numaralı Kamu Sektöründeki Elektronik Veri Bankalarında Gerçek Kişilerin Mahremiyetinin Korunması İlke Kararı düzenlenmiştir. Bu kararda da tıpkı 22 Numaralı Karar'da olduğu gibi bazı temel ilkeler ortaya konulmuştur. Buna göre, kamunun belirli zaman aralıklarında kamu sektöründe veri bankalarının kurulumu, yönetimi ve geliştirilmesi hakkında

²⁶⁹ FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, s. 84.

²⁷⁰ Resolution 73 (22) on the Protection of the Privacy of Individuals vis-a-vis Electronic Data Banks in the Private Sector, <https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=589402&SecMode=1&DocId=646994&Usage=2>, E.T. 20.09.2017.

²⁷¹ FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, s. 85.

bilgilendirilmesi, saklanan verinin belirli bir kalitede olması, ilgisiz, uygunsuz ve belirsiz verilerin silinmesi, hangi verinin hangi sürede saklanabileceği, verinin ilgili olduğu kişinin bilgilendirilmesi, kötüye kullanımların önüne geçilmesi, verinin erişilmesi için yetkili merci ve istatistiki verilerin akıbeti hususları ele alınmıştır²⁷². Görüleceği üzere kamu sektöründeki bu temel ilkeler, özel sektördeki temel ilkelerle oldukça örtüşmektedir.

Bu düzenlemeler neticesinde 1974'ün sonuna doğru gelindiğinde “veri koruma” ifadesi artık bilgisayarlarla kayıt altına alınmış bilgilere de karşı bireylerin korunmasını karşılayan yeni bir kavramı işaret etmekteydi²⁷³.

A. 108 SAYILI KİŞİSEL VERİLERİN OTOMATİK İŞLENMESİ SİRASINDA GERÇEK KİŞİLERİN KORUNMASINA İLİŞKİN SÖZLEŞME VE SÖZLEŞME 108+ REVİZYONU

Yukarıda anılan düzenlemelerin ardından 1976 yılında, Avrupa Hukuki İş Birliği Komitesi'nin denetimi altında olan Veri Koruma Uzmanları Komitesi kurulmuştur. Bu komitenin kurulma amacı, veri işleme süreci ile ilişkili olarak mahremiyetin korunmasına dair bir sözleşme hazırlamaktır²⁷⁴.

Söz konusu sözleşmenin önemli özelliklerinden biri, hazırlanırken yalnızca Avrupa'nın değil, Avrupa dışındaki OECD gözlemci ülkeleri olan Avustralya, Birleşik Devletler, Japonya ve Kanada'nın da düşünülerek hazırlanmış olmasıdır. Zaten anılan belgenin isminin “Avrupa Sözleşmesi” değil de yalnızca “Sözleşme” olarak belirlenmesi de bilinçli bir tercih olarak karşımıza çıkmaktadır²⁷⁵.

²⁷² Resolution 74 (29) on the Protection of the Privacy of Individuals vis-a-vis Electronic Data Banks in the Public Sector, <https://wed.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=590512&SecMode=1&DocId=649498&Usage=2> , Erişim Tarihi: 20.09.2017.

²⁷³ HONDIUS, *The Council of Europe's Work in the area of Computers and Privacy*, s. 3.

²⁷⁴ HONDIUS, *The Council of Europe's Work in the area of Computers and Privacy*, s.8.

²⁷⁵ Explanatory Report to the Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, par. 24, <https://rm.coe.int/16800ca434> , E.T. 21.09.2017.

108 Sayılı Kişisel Verilerin Otomatik İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşme'nin temel gayesi, genel bir ifade ile taraf ülkelerin sınırları dâhilinde kişilerin temel hak ve özgürlüklerini korumaktır. Spesifik olarak ise, kişisel verilerin otomatik işlenmesi bağlamında mahremiyet hakkının korunmasını sağlamaktır²⁷⁶. Dolayısıyla 108 Sayılı Sözleşme Avrupa tarihinde, içerisinde “veri koruma” kavramının geçtiği ve uluslararası bağlayıcılığı olan ilk düzenlemedir²⁷⁷. Ayrıca, İHAS'ın 8. maddesinde öngörüldüğü gibi anlaşılan “özel yaşamın gizliliği hakkı” ile “veri koruma”nın özel bir bağlantısını ifade etmektedir²⁷⁸. Ancak burada önemle belirtilmelidir ki daha 1970'lerde Avrupa Konseyi, İHAS'ın 8. maddesinin özel yaşam kavramının belirsizliği sebebiyle özellikle bilişim teknolojileri alanındaki yeni gelişmeler karşısında oldukça sınırlı kaldığını belirterek bu alanda spesifik bir hukuki düzenleme olan ve veri işleme konusunda bireylerin temel haklarını korumak amacını güden 108 Sayılı Sözleşme'yi yapmıştır²⁷⁹.

108 Sayılı Sözleşme'nin amacı veri koruma olsa da bünyesinde “Sınır Ötesi Veri Dolaşımı”na dair birçok düzenleme barındırmakta ve genel olarak kişisel verilerin dolaşımına dair herhangi bir kısıtlamayı yasaklamaktadır²⁸⁰. Ayrıca daha evvelki

²⁷⁶ Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, Article 1, <https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37> , E.T. 21.09.2017.

²⁷⁷ Antonella GALETTA, Paul DE HERT, “A European Perspective on Data Protection and Access Rights”, *Increasing Resilience in Surveillance Societies (IRISS) Project*, Vrije Universiteit Brussels-Belgium, 2014, <http://irissproject.eu/wp-content/uploads/2014/06/European-level-legal-analysisFinal1.pdf>, E.T. 03.09.2018.

²⁷⁸ Explanatory Report to the Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, par. 19, <https://rm.coe.int/16800ca434> , E.T. 21.09.2017.

²⁷⁹ DE HERT, GUTWIRTH, “Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action”, s. 6.

²⁸⁰ Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, Article 12, <https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37> , E.T. 21.09.2017.

düzenlemelerin aksine 108 Sayılı Sözleşme hem kamu hem de özel sektörde işlenen kişisel verilerin korunmasını ele almaktadır²⁸¹.

108 Sayılı Sözleşme, OECD Rehber İlkeleri ile benzer şekilde bazı genel ilkeleri ortaya koymuştur. Bu bakımdan Avrupa’da kendinden sonra düzenlenen tüm yasal düzenlemelere de temel teşkil etmiştir ve günümüzde tüm AB üyeleri ilgili sözleşmenin tarafıdır²⁸².

Kişisel verilerin korunması hakkı bakımından öncelikle belirtilmelidir ki, bu hak Avrupa Konseyi tarafından düşünülmüş ve 108 Sayılı Sözleşme ile özel yaşamın korunması hakkı gibi temel hak ve özgürlüklerin adeta bir parçası olarak ele alınmıştır²⁸³. Kişisel verilerin işlenmesi, bireylerin hak ve özgürlüklerinin korunmasını sağlamak amacıyla 108 Sayılı Sözleşme ile geliştirilmiştir²⁸⁴. Bunun dışında Sözleşme’nin genel ilkelerine bakılacak olursa;

- *Verilerin belirli bir nitelikte olması (Md. 5)*: Otomatik olarak işlenecek verilerin meşru ve yasal yollardan elde edilme ve işlenmesi, belirli ve meşru amaçlar için tutulması ve bu amaçlar harici kullanılamaması; yalnızca ilgili ve

²⁸¹ Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, Article 3, <https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37> , E.T. 21.09.2017.

²⁸² Thomas ZERDICK, “European Aspects of Data Protection: What Rights for the Citizen?”, *Legal Issues of Economic Integration*, Vol. 22, Issue: 2, s. 80- 83.

108 Sayılı Sözleşme’nin ardından, 1984 yılında Birleşik Krallık, Veri Koruma Kanunu’nu yürürlüğe koymuştur. Devamında 1988 yılında hem Sözleşme hem de Birleşik Krallık’ın etkisiyle İrlanda kendi Veri Koruma Kanunu’nu düzenlemiştir. Aynı yıl Finlandiya da son İskandinav ülkesi olarak, kendi Kişisel Veri Dosyası Kanunu’nu uygulamaya koymuştur. Hollanda ise, 1985 tarihli kişisel yaşam alanına saygı anayasal hakkı ile ilişkilendirdiği kanunu 1989 yılında yasalaştırmıştır. Son olarak Belçika, 108 Sayılı Sözleşme’yi her ne kadar 1982 yılında imzalamış olsa da 1993 yılında onaylamasının da etkisi ile, 1992 yılında kişisel verilerin korunmasına dair kanunu düzenlemiştir.

²⁸³ Bu durum daha sonra AB Temel Haklar şartı ile değişecektir. Bkz. DE HERT, GUTWIRTH, “Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action”, s. 7.

²⁸⁴ Peter HUSTINX, "EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation", *Collected Courses of the European University Institute's Academy of European Law*, 24th Session on European Union Law, 1-12 July 2013, s. 17, https://edps.europa.eu/data-protection/our-work/publications/speeches-articles/eu-data-protection-law-review-directive_en , E.T. 04.11.2018.

gerektiği kadar verinin tutulması, verilerin doğru ve güncel olması, gerekli olandan uzun süre saklanmaması gerekmektedir.

- *Hassas verilerin özel olarak korunması (Md. 6)*: Hassas veriler muhatap devletin ulusal hukukunda uygun güvenceler sağlanmadıkça işlenemez.
- *Veri güvenliği (Md. 7)*: Verilere yetkisiz biçimde erişim engellenmeli, verilerin değiştirilmesi ya da ortadan kaldırılması önlenmelidir.
- *İlgili kişinin bilgi alma, verilere ulaşma ve gerektiğinde onları düzeltme hakkı (Md. 8)*: İlgili kişi kendisine dair otomatik işlenmiş verileri hakkında gerektiğinde bilgi alabilecektir. Verileri hukuka aykırı olarak işlenmişse bu verileri sildirtebilecek, yanlış olanları düzeltebilecek ve bu talepleri karşılanmazsa gereken hukuki yollara başvurabilecektir.

108 Sayılı Sözleşme ayrıca uluslararası alanda kişisel verilerin serbestçe dolaşması ilkesini kabul etmektedir; fakat devletler iki istisnai durumda bu veri aktarımını yasaklayabilecektir: Belirli veri kategorileri için özel bir koruma getirilmiş olması ve aktarımın yapılacağı devlette eşdeğer bir korumanın bulunmaması ile aktarımın Sözleşme’ye taraf olmayan üçüncü bir devlet aracılığı ile yapılacak olması halleridir (Md. 12). Bunun yanında 108 Sayılı Sözleşme, hükümlerin yorumlanması ve yerinde uygulanmaları amacıyla tarafların temsilcilerinden oluşan bir Danışma Komitesi kurmuştur²⁸⁵.

Taraf ülkelerin kendi hukuk sistemlerini bu Sözleşme’ye göre adapte etmelerini arayan 108 Sayılı Sözleşme, 1 Ekim 1985 tarihinde yürürlüğe girmiştir²⁸⁶. 108 Sayılı Sözleşme’nin yürürlüğe girmesi ile İHAS’a bir hüküm konulmasına gerek görülmemiştir²⁸⁷. Anılan Sözleşme, 1999 yılına gelindiğinde Avrupa Topluluğu’na da

²⁸⁵ GALETTA, DE HERT, “A European Perspective on Data Protection and Access Rights”, <http://irissproject.eu/wp-content/uploads/2014/06/European-level-legal-analysis-Final1.pdf> , E.T. 03.09.2018.

²⁸⁶ Details of Treaty No.108- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108> , E.T. 27.09.2017.

²⁸⁷ FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, s. 91.

açılacak şekilde değişikliğe uğramıştır. 2001 yılında ise Sözleşme sistemini Avrupa Topluluğu'na yaklaştıran Ek Protokol imzaya açılmıştır²⁸⁸. 2011 yılında 108 Sayılı Sözleşme yeniden değerlendirilme aşamasındadır ve bu aşamada “Kişisel Verilerin Korunması Hakkı”na açıkça atıfta bulunma ihtimali tartışılmıştır. 2016 yılında ise, 108 Sayılı Sözleşme'nin yenilenme sürecinin ikinci aşaması başlatılmıştır. Böylece Sözleşme'de yer alan düzenlemelerin, tavsiye ve yönergeler yoluyla daha detaylı sektörel metinlerle tamamlanacak ilkesel maddeler haline gelmeleri sağlanmakta ve AB yasal çerçevesiyle tutarlılık ve uyum sağlanması amaçlanmaktadır. Nihayetinde ise Sözleşme'nin evrensel açıdan bir standart oluşturduğunu belirten bir taslak ortaya çıkmıştır²⁸⁹.

Nihayetinde AB Genel Veri Koruma Tüzüğü'nün yürürlüğe girmesinin ardından 18 Mayıs 2018'de Avrupa Konseyi Bakanlar Komitesi, Avrupa Konseyi'nin 108 Sayılı Sözleşmesi'ni yenileyen Protokol'ü (Sözleşme 108+) kabul etmiştir²⁹⁰. Sözleşme 108+'nın yürürlüğe girmesi ise iki durumda gerçekleşecektir: Mevcut tüm tarafların (53 ülke) Sözleşme 108+'ı kabulü halinde veya imzaya açılmasından beş yıl sonra toplamda 38 taraf ülkenin Sözleşme 108+'ı kabul etmesi sonucunda Sözleşme 108+ yürürlüğe girecektir²⁹¹.

Sözleşme 108+ ile bilişim teknolojilerindeki gelişmeler dikkate alınarak daha güçlü bir veri koruma sistemi yaratılmıştır. Bu bakımdan Sözleşme 108+, GVKT'de yer alan en önemli yenilikleri tanımaktadır²⁹². Sözleşme'nin amacında insan onuru ve

²⁸⁸ Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding Supervisory Authorities and Transborder Data Flows, <https://rm.coe.int/1680080626>, E.T. 27.09.2017.

²⁸⁹ “Modernisation of the Data Protection ‘Convention 108’” <http://www.coe.int/en/web/portal/28-january-data-protection-day-factsheet>, E.T. 27.09.2017.

²⁹⁰ Convention 108+, Convention for the protection of individuals with regard to the processing of personal data, 18.05.2018, <https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1>, E.T. 18.05.2019.

²⁹¹ Graham GREENLEAF, “‘Modernised’ Data Protection Convention 108 and the GDPR”, *Privacy Laws & Business International Report*, Vol. 154, No: 22, Y: 2018, *University of New South Wales Law Research Paper*, No: 19-3, Y: 2019, s. 1, ss. 1-2.

²⁹² GVKT'ile ortak fakat daha genel olan 13 özellik şunlardır;

bireysel özerklik vurgulanmış, uluslararası kuruluşların Sözleşme’ye taraf olabilecekleri düzenlenmiş, yeni tanımlar yapılmış, veri işleme sürecinde şeffaflığı artırıcı yeni kuralları getirilmiş ve veri koruma otoritelerinin görev ve yetkileri genişletilmiştir. Ayrıca özel nitelikli veriler kategorisi genişletilerek genetik ve biyometrik veriler de GVKT’de olduğu gibi dahil edilmiştir. Yine GVKT’de yer alan, tasarımla veri koruma (*privacy by design*) ve varsayılan ayarlarla veri koruma (*privacy by default*) gibi yeni uygulamalar ile veri öznesinin temel hak ve özgürlüklerine ciddi müdahale oluşturabilecek veri sızıntılarının derhal bildirilmesi yükümlülüğü getirilmiştir. 108 Sayılı Sözleşme’den farklı olarak, Sözleşme 108+ ile üye devletler artık bazı alanları istisna olarak tutmak amacı ile bildirimde bulunamayacaktır. Sözleşme hükümlerinin gerçek ve ciddi bir ihlali söz konusu değil ise üye devletler arasında sınır ötesi veri aktarımı da serbet tutulmuştur²⁹³.

Öte yandan Sözleşme 108+, GVKT’nin tüm yeniliklerini de içermemektedir. Bu sebeple doktrinde GVKT’de yer alıp Sözleşme 108+’da yer almayan ilkelerin yaratacağı

“1. İşlemenin tüm yönlerinde gerekli olan orantılılık.

2. Daha güçlü olması aranan rıza şartları.

3. Veri işlemede daha fazla şeffaflık.

4. Bazı hallerde zorunlu Veri Koruma Etki Değerlendirmeleri.

5. Veri işlemenin mantığını bilme hakkı dahil otomatik karar vermedeki sınırlar.

6. Tasarımla veri koruma (*privacy by design*) ve varsayılan ayarlarla veri koruma (*privacy by default*).

7. Biyometrik ve genetik verilerin ekstra koruma gerektirmesi.

8. Meşru gerekçelerle veri işlenmesine itiraz hakkı.

9. Veri işleyicisi ve veri denetleyicisi için doğrudan sorumluluk.

10. Ciddi ihlallerde Veri Koruma Otoritesi’ne veri ihlali bildirimi.

11. Kararların alınması, idari yaptırımlar ve hukuk yolları için Veri Koruma Otoriteleri.

12. Veri denetleyicileri için gereken hesap verilebilirlik.

13. Tarafların etkililiğin değerlendirilmesine izin vermesi ve yardımcı olması.”

Detaylı bilgi için bkz. Graham GREENLEAF, “Convention 108+ and the Data Protection Framework of the EU”, *Conference on Convention 108+ Tomorrow’s Common Ground for Protection*, Council of Europe, Strasbourg, 21.06.2018, *University of New South Wales Law Research Paper*, No. 18-39, s. 3, ss. 1-7.

²⁹³ Convention 108+, Convention for the protection of individuals with regard to the processing of personal data, 18.05.2018, <https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1>, E.T. 18.05.2019; Elif KÜZECİ, “Avrupa Konseyi’nin 108 sayılı Kişisel Verilerin Korunması Sözleşmesi Yenilendi! Sözleşme 108+, Carpenter Kararı ve diğer bazı gelişmelere ilişkin bir değerlendirme”, *Medium*, <https://medium.com/@elfkzc/avrupa-konseynin-108-sayili-kisisel-verilerin-korunmasi-sozlesmesi-yenilendi-bc8daad9decc>, E.T. 18.05.2019.

farklılığın henüz nelere yol açabileceğinin belirsiz olduğu; fakat Sözleşme 108+'nın standartlarının 2023 yılına dek yeni küresel ilkeler olarak kabul edilebileceği dile getirilmektedir²⁹⁴.

B. İNSAN HAKLARI AVRUPA SÖZLEŞMESİ

İnsan Hakları Avrupa Sözleşmesi ya da asıl adı ile İnsan Hakları ve Temel Özgürlüklerinin Korunmasına İlişkin Sözleşme 2. Dünya Savaşı sonrası, savaş esnası gerçekleştirilen insan hakları ihlallerinin de etkisiyle Avrupa'yı bütünleştirmek gayesini taşıyan önemli sonuçlardan biridir. 4 Kasım 1950 tarihinde Avrupa Konseyi üye ülkeleri, İnsan Hakları Evrensel Beyannamesi'nde bulunan temel hakları güvence altına almak için bu sözleşmeyi imzalamışlardır²⁹⁵.

İHEB'in aksine İHAS, yalnızca bir bildiri olmaktan öte hukuki bağlayıcılığı olan bir metindir. Bu sebeple insan hakları korumasını da bir adım öteye taşımıştır. İHAS, bir "Başlangıç" ve üç bölümden oluşmaktadır. İlk bölümde temel haklar ve özgürlükler yer alırken, ikinci bölüm İnsan Hakları Avrupa Mahkemesi'ne ilişkin düzenlemeleri ve son bölüm ise çeşitli hükümleri içermektedir. Sözleşme'nin yürürlüğe girdiği 3 Eylül 1953'ten bugüne çeşitli protokoller aracılığıyla değişikliklere uğramış ve yeni hak ve

²⁹⁴ GVKT'de yer alıp Sözleşme 108+'da yer almayan en az dokuz ilkedен bahsedilmektedir. Bu ilkeler;

"1. Ülkedışılık (extraterritoriality) söz konusu olduğundaki yükümlülükler.

2. Yabancı veri işleyici ve denetşeyicilerinden istenen yerel temsil.

3. Veri öznesi tarafından üretilen içeriğın taşınabilirliğı.

4. Unutulma hakkı.

5. Hassas verilerin işlenmesinde zorunlu veri koruma görevlisi atanması.

6. Yüksek risk söz konusu ise veri öznelerine veri ihlali bildirimi.

7. Kamu yararı güden özel şirketlerin veri koruma otoriteleri ve mahkemeler önünde temsili.

8. Yıllık küresel ciroya dayanan azami ölçekte idari para cezaları.

9. Şikayetlerin çözümü için uluslararası unsurlar ve diğer veri koruma görevlileri ile iş birliğı yapma."

GREENLEAF, "Convention 108+ and the Data Protection Framework of the EU", *Conference on Convention 108+ Tomorrow's Common Ground for Protection*, s. 4.

²⁹⁵ HARRIS, O'BOYLE, WARBRICK, *Law of the European Convention on Human Rights*, s. 1; Javier Garcia ROCA, "The Preamble, The Convention's Hermeneutic Context: A Constitutional Instrument of Public Order", *Europe of Rights: A Compendium on the European Convention on Human Rights*, Eds. Javier Garcia ROCA, Pablo SANTOLAYA, Martinus Nijhoff Publishers, 2012, s. 1, ss. 1- 26.

özgürlükler eklenmiş olsa da metin ve İnsan Hakları Avrupa Mahkemesi bölgesel düzlemde en iyi örnek olma özelliklerini korumaktadırlar²⁹⁶.

İHEB, insan hakları koruması için bir minimum hak kataloğu oluşturmaktadır. Buna göre her üye devlet belirli hak ve özgürlükleri, vatandaş olup olmamasına bakmaksızın tüm insanlara garanti etmekle yükümlüdür. Bu hak ve özgürlüklerin bir kısmına bakılacak olursa, yaşam hakkı, özgürlük ve güvenlik hakkı, adil yargılanma hakkı, özel yaşama ve aile yaşamına saygı hakkı, düşünce, vicdan ve din özgürlüğü, ifade özgürlüğü, toplanma ve dernek kurma özgürlüğü, evlenme hakkı, etkili bir iç hukuk yoluna başvuru hakkı Sözleşme kapsamında düzenlenmiştir²⁹⁷.

İnsan Hakları Avrupa Mahkemesi, Sözleşme’yi yorumlarken hazırlandığı ilk zamanki hal ve o zamanki niyetleri değil, günümüz şartlarını esas alır. Bu bakımdan İHEB, yaşayan bir enstrüman olarak nitelendirilmektedir²⁹⁸. Bu bakımdan Sözleşme’nin “Özel Yaşam ve Aile Yaşamına Saygı” başlıklı 8. maddesi ise, çalışmamız kapsamında teknolojinin mahremiyet üzerindeki neticeleri ile “Özel Yaşamın Gizliliği Hakkı” ve bu hakkın bünyesinde değerlendirilerin “Kişisel Verilerin Korunması Hakkı”nı da barındıran şekliyle yorumlanmaktadır.

1. İHAM Kararları Bağlamında Mahremiyet Kavramı ve Özel Yaşamın Gizliliği ve Korunması Hakkı

“Özel Yaşamın Gizliliği ve Korunması Hakkı”, ilk defa 19. yüzyılda kullanılan bir hak olarak karşımıza çıkmaktadır. Bu durum yukarıda belirtildiği üzere, 1890 yılında Harvard Law Review’de yayımlanan ve Samuel D. Warren ile Louis Brandeis’e ait olan “Mahremiyet Hakkı” isimli makale ile olmuştur. Bu makalede mahremiyet hakkının

²⁹⁶ Janneke GERARDS, *General Principles of the European Convention on Human Rights*, Cambridge University Press, 2019, s. 1; HARRIS, O’BOYLE, WARBRICK, *Law of the European Convention on Human Rights*, s. 1 vd.

²⁹⁷ GERARDS, *General Principles of the European Convention on Human Rights*, s. 11- 18.

²⁹⁸ GERARDS, *General Principles of the European Convention on Human Rights*, s. 51- 53; ROCA, “The Preamble, The Convention’s Hermeneutic Context: A Constitutional Instrument of Public Order”, s. 22- 24.

temeli, 19. yüzyıl İngiliz hukukundaki “mahremiyet” konseptine ve kişilerin mahremiyeti ile ilgili vakıaların şayet ilgilinin onayı olmaksızın veya kamusal olarak zaten daha evvelden bilinmedikçe yayımlanmasının yasaklayan 11 Mayıs 1868 tarihli Fransız Basın Kanunu’na dayandırılmıştır²⁹⁹.

“Mahremiyet Hakkı”nın tanımının Warren ve Brandeis’in kült makaleleri dışında bir metinde karşımıza çıkması ise, daha evvel dile getirildiği üzere 1967 yılında Nordik Konferansı’nda olmuştur³⁰⁰. Bu tanıma göre;

*“Mahremiyet Hakkı, kişinin kendi yaşamını sürdürmesi için, minimum ölçüde müdahalede bulunularak, yalnız bırakılma/ kalma hakkıdır.”*³⁰¹

Dolayısıyla mahremiyet hakkı genel itibarıyla, bilgi gizliliği ve yalnız bırakılma haklarını karşılamaktadır. Bu bakımdan dar bir anlamı vardır³⁰². “Özel Yaşamın Gizliliği ve Korunması Hakkı” ise, mahremiyet hakkına nazaran ulusüstü insan hakları belgelerine, özellikle 2. Dünya Savaşı sonrası yoğun bir şekilde girmiştir³⁰³. İnsan Hakları Evrensel Beyannamesi’nin 12. maddesi, Medeni ve Siyasal Haklar Sözleşmesi’nin 17. maddesi, Amerikan İnsan Hakları Sözleşmesi’nin 11. maddesi, Afrika İnsan ve Hakların Hakkı Sözleşmesi’nin 18. maddesi ve İnsan Hakları Avrupa Sözleşmesi’nin 8. maddesi, “Özel Yaşamın Gizliliği ve Korunması Hakkı”nı düzenlemiştir.

İnsan Hakları Avrupa Sözleşmesi’nin 8. maddesinin başlığı, “Özel Yaşam ve Aile Yaşamına Saygı”dır. Bu madde ile güvence altına alınan dört alt kategori bulunmaktadır³⁰⁴. Bunlar; “Özel Yaşama Saygı Hakkı”, “Aile Yaşamına Saygı Hakkı”,

²⁹⁹ WARREN, BRANDEIS, “The Right to Privacy”, s. 214; PROSSER, “Privacy”, ss. 383- 423.

³⁰⁰ International Commission of Jurists, “The Protection of Privacy”, *UNESCO International Social Science Journal*, Vol. XXIV, No: 3, 1972, s. 448.

³⁰¹ International Commission of Jurists, “Conclusions of the Nordic Conference”, Mayıs 1967, Cenevre, s. 2, <http://www.icj.org/wp-content/uploads/2013/06/Right-to-privacy-seminar-report-conclusions-1967-eng.pdf>, E.T. 11.12.2016.

³⁰² HARRIS, O’BOYLE, WARBRICK, *Law of the European Convention on Human Rights*, s. 361- 362.

³⁰³ ARSLAN ÖNCÜ, *Avrupa İnsan Hakları Sözleşmesinde Özel Yaşamın Korunması Hakkı*, s. 3.

³⁰⁴ HARRIS, O’BOYLE, WARBRICK, *Law of the European Convention on Human Rights*, s. 363- 381.

“Konuta Saygı Hakkı” ve “Haberleşmeye Saygı Hakkı”dır³⁰⁵. Bu hakların tamamının doktrinde birlikte ele alınması ve ayırım yapmanın pratikte pek önemli olmadığı gibi görüşler ileri sürüldüğü gibi³⁰⁶, “Özel Yaşama Saygı Hakkı”nın diğer alt kategorilerden bağımsız bir anlamı olduğunu savunan görüşler de mevcuttur³⁰⁷.

Anılan maddede yer alan özel yaşama saygı hakkının tanımsal çerçevesi ilk olarak, Avrupa İnsan Hakları Komisyonu tarafından *X- İzlanda*³⁰⁸ kararında ele alınmıştır. Kararda birçok Anglo-sakson ve Fransız yazarın özel yaşama saygı hakkını, mahremiyet hakkı, dilediğince yaşama hakkı ve aleniyetten koruma hakkı ile eşanlamlı olarak tanımladıkları ve fakat Komisyon’un bu fikre katılmayıp özel yaşama saygı hakkının bu kapsamla sınırlı olmadığı dile getirilmiştir. Komisyon’a göre özel yaşama saygı hakkı, kendi kişiliğini geliştirmek için başkaları ile ilişkiler kurup geliştirmeyi de kapsamaktadır.

Bu karardan günümüze değin İHAS düzleminde 8. madde, en geniş yorumlanan hükümlerden biridir, çünkü İHAM içtihatlarına bakıldığında, birçok farklı konu bu hak kapsamında değerlendirilmektedir³⁰⁹. *Pretty- Birleşik Krallık*³¹⁰ davası bu bakımdan önemli bir örnek olarak karşımıza çıkmaktadır. Bu davada, özel yaşam hakkının dejeneratif ve tedavi edilemeyen bir hastalıktan dolayı felç olmuş ve acı çeken insanlar için yardımcı intihar hakkını kapsayıp kapsamadığı ele alınmaktadır. Kararda her ne kadar

³⁰⁵ Söz konusu hakka ilişkin detaylı bilgi için bkz. ÜZELTÜRK, *1982 Anayasası ve İnsan Hakları Avrupa Sözleşmesine Göre Özel Hayatın Gizliliği Hakkı*; ARSLAN ÖNCÜ, *Avrupa İnsan Hakları Sözleşmesinde Özel Yaşamın Korunması Hakkı*.

³⁰⁶ Clare OVEY, Robin WHITE, *European Convention on Human Rights*, 3. Ed., Oxford University Press, 2002, s. 218.

³⁰⁷ Louise DOSWALD-BECK, “The Meaning of the ‘Right to Respect for Private Life’ under the European Convention on Human Rights”, *Human Rights Law Journal*, Vol. 4, No: 3, s. 283.

³⁰⁸ *X v. Iceland*, Application No: 6825/74, 18.05.1976, <http://echr.ketse.com/doc/6825.74-en-19760518/i>, E.T. 28.09.2017.

³⁰⁹ Arama ve el koyma, gizli izleme, göç hukuku, babalık ve kimliğe ilişkin haklar, çocuk ve aile hukuku, yardımcı üreme, intihar, tutuklu hakları, miras, kiralayan hakları, çevre koruması gibi birçok konu İHAS md. 8 bağlamında değerlendirilmektedir.

HARRIS, O’BOYLE, WARBRICK, *Law of the European Convention on Human Rights*, s. 361.

³¹⁰ *Pretty v. The United Kingdom*, Application No: 2346/02, 29.07.2002, <http://hudoc.echr.coe.int/eng?i=001-60448>, E.T. 29.05.2018.

özel yaşam hakkının yardımcı intihar hakkını kapsamadığına hükmedilmiş olsa da kişisel özerklik ilkesi oldukça detaylı bir biçimde ele alınmıştır. Öncelikle özel yaşam kavramının ayrıntılı bir tanımlamaya açık olmayan geniş bir terim olduğu dile getirilmiştir. Kişinin fiziksel ve psikolojik bütünlüğü, fiziksel ve sosyal kimliği, cinsiyet tanımı ve yönelimi, cinsel yaşam gibi kişisel alan içerisinde yer alan kavramlar 8. madde bağlamında korunmaktadır. Ayrıca Mahkeme'ye göre kişisel gelişim hakkı ile dış dünya ve diğer insanlarla ilişki kurma hakları da 8. maddenin korumasından yararlanmaktadır. Bu dava bakımından esas önemli nokta ise kişisel özerklik hakkı da 8. madde bağlamında değerlendirilmiştir. Fakat kişisel özerklik hakkının bilgilerin geleceğini belirleme hakkını da içerip içermediği konusunda cevapsız kalmıştır³¹¹.

İHAM 8. maddeye ilişkin birçok kararında genişlemeci bir yol izlemiştir. Bu bağlamda özel yaşam hem kişiler arası ilişkilerin gelişimini³¹² hem de özel alan ile kamusal alanda gerçekleşen (verilerle alakalı) bazı durumları içerisine almaktadır³¹³. Hatta Mahkeme, konumuz bağlamında, veri koruma hukukunun zorunlu olmayan bir özelliği olan üye devletlerin isteğe bağlı olarak yalnızca gerçek kişiler için değil, aynı zamanda tüzel kişiler için de veri koruma haklarını tanımalarına izin vererek firmalara ve ticari faaliyetlere yönelik mahremiyet korumasını tanıyacak kadar ileri gitmiştir³¹⁴. İHAM'ın bu genişleyen 8. madde yorumunda veriye erişim hakkı gibi bazı veri koruma haklarının kabulü en temelde devletin pozitif yükümlülükleri sayesinde

³¹¹ *Pretty v. The United Kingdom*, Par. 61, Application No: 2346/02, 29.07.2002, <http://hudoc.echr.coe.int/eng?i=001-60448> , E.T. 29.05.2018.

³¹² *Niemietz v. Germany*, Par. 29, Application No: 13710/88, 16.12.1992, <http://hudoc.echr.coe.int/eng?i=001-57887> , E.T. 29.05.2019.

³¹³ *Peck v. The United Kingdom*, Par. 57- 63, Application No: 44647/98, 28.04.2003, <http://hudoc.echr.coe.int/eng?i=001-60898> , E.T. 28.05.2019; *Perry v. The United Kingdom*, Application No: 63737/00, <http://hudoc.echr.coe.int/eng?i=001-61228> , E.T. 29.05.2019.

³¹⁴ *Société Colas Est and Others v. France*, Par. 40, Application No. 37971/97, 16.07.2002, <http://hudoc.echr.coe.int/eng?i=001-60431> , E.T. 30.05.2019; *Niemietz v. Germany*, Par. 30, Application No: 13710/88, 16.12.1992, <http://hudoc.echr.coe.int/eng?i=001-57887> , E.T. 29.09.2017.

gerçekleşmiştir³¹⁵. Bu pozitif yükümlülüklerle dayanılarak devletler özel sektör aktörlerinin gerçekleştirdiği mahremiyet ihlallerinden sorumlu tutulabilmiştir³¹⁶.

Niemietz- Almanya kararının detaylı içeriği, İHAM’ın “özel yaşam” kavramını ne ölçüde geniş yorumladığını göstermesi açısından önem arz etmektedir³¹⁷. Belirtildiği üzere İHAS’ın 8. maddesinde yer alan özel yaşam, bireylerin belli bir dereceye kadar diğer insanlarla ilişkiler kurup geliştirmesini de kapsamaktadır³¹⁸. Mahkeme’ye göre, her ne kadar özel yaşam kavramını tanımlama çabası gereksiz ve imkânsız olsa da bunu bireyin kendi yaşamını dilediği ve seçtiği gibi yaşaması anlamına gelen “giz alanı (inner circle)”³¹⁹ndan ibaret görmek ve dış dünyayı tamamen ayırık tutmak sınırlayıcı bir tutum olmaktadır³²⁰. Ayrıca profesyonel ya da mesleki faaliyetlerin özel yaşam kavramı dışında ele alınmasına dair bir ilke de söz konusu değildir ve çoğu zaman insanların özel ilişki kurabildikleri ortam mesleki yaşamları dâhilindedir³²¹. Dolayısıyla Mahkeme’nin adlandırması ile özel yaşam kavramının bu denli geniş olması, onu “kapsamlı bir tanım yapmaya elverişsiz” kılar³²².

³¹⁵ Devletin pozitif yükümlülükleri için bkz. BOYAR, “Devletin Pozitif Yükümlülükleri ve Dolaylı Yatay Etki”, *İnsan Hakları Avrupa Sözleşmesi ve Anayasa*, s. 53 v.d.

³¹⁶ Söz konusu özel sektör aktörleri doğrudan İHAM nezdinde dava adilemiyor olsalar da Mahkeme’nin içtihatlarına iç hukukta atıf yapılabilir. DE HERT, GUTWIRTH, “Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action”, *Reinventing Data Protection*, s. 17.

³¹⁷ *Niemietz v. Germany*, Application No: 13710/88, 16.12.1992, <http://hudoc.echr.coe.int/eng?i=001-57887>, E.T. 29.09.2017.

³¹⁸ *Niemietz v. Germany*, Par. 29, Application No: 13710/88, 16.12.1992, <http://hudoc.echr.coe.int/eng?i=001-57887>, E.T. 29.09.2017.

³¹⁹ Yaşar SALİHPAŞAOĞLU, “Özel Hayatın Kapsamı: Avrupa İnsan Hakları Mahkemesi İçtihatları Işığında Bir Değerlendirme”, *Gazi Üniversitesi Hukuk Fakültesi Dergisi*, C. XVII, Y. 2013, S. 3, s. 235.

³²⁰ *Niemietz v. Germany*, Par. 29, Application No: 13710/88, 16.12.1992, <http://hudoc.echr.coe.int/eng?i=001-57887>, E.T. 29.09.2017.

³²¹ Turan YILDIRIM, “Kamu Görevlilerinin Özel Hayatı: Cinsel Tercih”, *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, C. 24, S. 2, Y: 2018, s. 458, ss. 453- 481; *Niemietz v. Germany*, Par. 29, Application No: 13710/88, 16.12.1992, <http://hudoc.echr.coe.int/eng?i=001-57887>, E.T. 29.09.2017; *Fernandez Martinez v. Spain*, Par. 109, Application No: 56030/07, 12.06.2014, <http://hudoc.echr.coe.int/eng?i=001-145068>, E.T. 25.10.2018.

³²² ÜZELTÜRK, *1982 Anayasası ve İnsan Hakları Avrupa Sözleşmesine Göre Özel Hayatın Gizliliği Hakkı*, s. 3; YILDIRIM, “Kamu Görevlilerinin Özel Hayatı: Cinsel Tercih”, s. 455; *Bensaid v. United Kingdom*, Par. 47, Application No: 44599/98, 06.05.2011, <http://hudoc.echr.coe.int/eng?i=001-59206>, E.T. 29.09.2017.

Mahkeme *Société Colas Est and Others- Fransa* kararında, 8. madde kapsamında korunan konut kavramının içeriğini de dinamik yorum yolu ile genişleterek belirli durumlarda anılan maddenin güvence altına aldığı hakların bir şirketin kayıtlı ofisine, şubelerine veya diğer işletme binalarına saygı gösterme hakkını da kapsadığı şeklinde yorumlanabileceğine hükmetmiştir³²³.

Özel yaşamın ayrıntılı bir tanımı verilemeyecek kadar geniş bir kavram olduğuna dair *Peck- Birleşik Krallık* davasında İHAM, kamusal alandaki bir bireyin eylemlerinin görsel verileri kaydetmeyen fotografik donanımla izlenmesini özel yaşam hakkının ihlali olarak görmemekte, bunun için ayrıca verilerin kaydedilmesi ve bu kaydın sistematik veya kalıcı olması gibi durumların varlığını aramaktadır³²⁴.

2. Özel Yaşamın Korunması Hakkı Bağlamında Kişisel Verilerin Korunması

1970'lerin başında 108 Sayılı Sözleşme'nin yürürlüğe girmesini ve Avrupa Konseyi'nin otomatik veri işleme çalışmalarını haklı kılmak için, İHAS'ın 8. maddesinin bilgisayarların ilerlemesi sonucu oluşan durumlara karşı yeterli korumayı sağlamadığına inanılmaktaydı. 1980'lere gelindiğinde ise artık Avrupa Konseyi yargı sisteminin içtihatlarında bilgisayarların ilerlemesi sonucu oluşan ihlallere dair aynı maddenin tatmin edici bir koruma sağlayacak kadar etkili olduğu ve bu nedenle İHAS'a konuya dair ek bir hakkın tanınmasının gereksiz olacağı düşünülmekteydi³²⁵.

Bu bağlamda İHAM, İHAS'ı her olayın özelliklerine ve günün koşullarına göre yorumlamaktadır³²⁶. Bu geniş yorumlamanın da etkisiyle, her ne kadar İHAS'ta modern iletişim araçları açıkça düzenlenmese de bu araçlar ve kişisel verilerin işlenmesi ile ilgili

³²³ *Société Colas Est and Others v. France*, Par. 41, Application No. 37971/97, 16.07.2002, <http://hudoc.echr.coe.int/eng?i=001-60431>, E.T. 30.05.2019

³²⁴ *Peck v. The United Kingdom*, Par. 59, Application No: 44647/98, 28.04.2003, <http://hudoc.echr.coe.int/eng?i=001-60898>, E.T. 28.05.2019.

³²⁵ FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, s. 48, 94.

³²⁶ *Tyrer v. United Kingdom*, Application No: 5856/72, 25.04.1978, <http://hudoc.echr.coe.int/eng?i=001-57587>, E.T. 29.09.2017.

konular (telefon görüşmeleri³²⁷, telefon numaraları³²⁸, bilgisayarlar³²⁹, video ile gözetim³³⁰, ses kaydı³³¹, internet ve email³³² gibi.) Mahkeme tarafından 8. madde bağlamında ele alınmaktadır. Böylece 8. maddenin kademeli olarak genişlemesi olgusu devam etmiştir.

İHAM 1978 yılında ilk defa *Klass ve Diğerleri- Almanya*³³³ ile kişisel veri ve rıza meseleleri ile ilgili sayılabilecek bir kararı hükme bağlamıştır. Olayda 1968 yılında Almanya'da Temel Kanun'un 10. maddesi ve 13 Ağustos 1968 tarihli Kanun'da telekomünikasyon ve posta hakkının kısıtlanmasını konu eden bir değişiklik yapılarak kişilerin rızası aranmaksızın bazı belirli durumlarda gizli gözetime tabi tutulabilecekleri hüküm altına alınmıştır. Ayrıca bu değişiklikle, söz konusu gözetimin uygulanmasına dair mahkemeler önünde bir hukuk yolu sunulmamış; yerine yalnızca bir idari denetim sistemi getirilmiştir. Mahkeme burada söz konusu değişikliğin devletlere her ne kadar sınırsız bir takdir yetkisi vermese de suçun önlenmesi ve ulusal güvenliğin sağlanması meşru amaçlarını güttüğüne ve ihlal olmadığına hükmetmiştir. Ancak kararda kişisel verilerin korunması bakımından önemli bir tespit mevcuttur: Mahkeme, hukukun üstünlüğünün korunmasında ve özellikle de gizli gözetim sistemleri söz konusu

³²⁷ *Klass and Others v. Germany*, Application No: 5029/71, 06.09.1978, <http://hudoc.echr.coe.int/eng?i=001-57510>, 29.11.2017; *Amann v. Switzerland*, Application No: 27798/95, 16.02.2000, <http://hudoc.echr.coe.int/eng?i=001-58497>, E.T. 18.10.2017.

³²⁸ *Malone v. United Kingdom*, Application No: 8691/79, 02.08.1984, <http://hudoc.echr.coe.int/eng?i=001-57533>, E.T. 06.10.2017; *P.G. and J.H. v. The United Kingdom*, Application No: 44787/98, 25.12.2001, <http://hudoc.echr.coe.int/eng?i=001-59665>, E.T. 02.11.2017.

³²⁹ *Leander v. Sweden*, Application No: 9248/81, 26.03.1987, <http://hudoc.echr.coe.int/eng?i=001-57519>, E.T. 06.10.2017; *Amann v. Switzerland*, Application No: 27798/95, 16.02.2000, <http://hudoc.echr.coe.int/eng?i=001-58497>, E.T. 18.10.2017; *Rotaru v. Romania*, Application No: 28341/95, 04.05.2000, <http://hudoc.echr.coe.int/eng?i=001-58586>, E.T. 19.10.2017.

³³⁰ *Peck v. The United Kingdom*, Application No: 44647/98, 28.04.2003, <http://hudoc.echr.coe.int/eng?i=001-60898>, E.T. 28.05.2019; *Perry v. The United Kingdom*, Application No: 63737/00, <http://hudoc.echr.coe.int/eng?i=001-61228>, E.T. 29.05.2019.

³³¹ *P.G. and J.H. v. The United Kingdom*, Application No: 44787/98, 25.12.2001, <http://hudoc.echr.coe.int/eng?i=001-59665>, E.T. 02.11.2017.

³³² *Copland v. The United Kingdom*, Application No: 62617/00, 03.07.2007, <http://hudoc.echr.coe.int/eng?i=001-79996>, E.T. 29.05.2019.

³³³ *Klass and Others v. Germany*, Application No: 5029/71, 06.09.1978, <http://hudoc.echr.coe.int/eng?i=001-57510>, E.T. 29.11.2017.

olduğunda, gücün kötüye kullanılmasının önlenmesinde bir mekanizma olarak bağımsız bir üst denetim otoritesine ihtiyaç duyulduğunu belirtmiştir³³⁴.

Kişisel verilerin korunması konusunda İHAM'ın bakış açısını ortaya koyabilmek için *Klass ve Diğerleri- Almanya* kararına ilişkin değinilmesi gereken bir diğer mesele de İHAM'ın bu olayda olduğu gibi gizli gözetimin söz konusu olduğu hallerde katı bir orantılılık testi uygulamakta olduğudur. Şöyle ki Mahkeme'nin orantılılık değerlendirmesi, müdahalenin ağırlığı, bilginin hassaslığı ve uygulanan güvenlik önlemleri gibi unsurlara bakılarak gerçekleştirilmektedir³³⁵. Bu kararda da Mahkeme, vatandaşların gizli gözetiminin ancak demokratik kurumları koruyabilmek adına kesinlikle gerekli olunan hallerde yapılabileceğini hüküm altına almıştır³³⁶. Kişisel verilerin İHAM içtihatlarında korunmasında mevcut olan bu katı orantılılık testi ayrıca tutuklu ve hükümlülerin hukuki danışmanları ile mektuplarına elkonulmasında³³⁷, telefon dinlenmesi yoluyla toplanan verilerin kullanımında ve ayrımcılığa kolaylıkla sebep olabilecek hassas verilerin söz konusu olduğu hallerde de yapılmaktadır³³⁸.

İHAM, 1980'lerde birkaç defa veri korumanın 8. madde kapsamına giren bir konu olduğuna hükmetmiştir. Bu bağlamda 108 Sayılı Sözleşme'yi ilk kez *Malone- Birleşik Krallık*³³⁹ kararında bahis konusu etmiştir. Bu kararda ana hatları ile bir ceza soruşturması kapsamında telefonların İçişleri Bakanlığınca verilen bir izin ile polis adına bir posta görevlisi tarafından dinlenilmesi ve "ölçme" (metering) olarak adlandırılan bir teknik ile

³³⁴ *Klass and Others v. Germany*, Par. 10- 11, Application No: 5029/71, 06.09.1978, <http://hudoc.echr.coe.int/eng?i=001-57510>, 29.11.2017; DE HERT, GUTWIRTH, "Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action", *Reinventing Data Protection*, s. 19.

³³⁵ DE HERT, GUTWIRTH, "Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action", *Reinventing Data Protection*, s. 23.

³³⁶ *Klass and Others v. Germany*, Par. 42, Application No: 5029/71, 06.09.1978, <http://hudoc.echr.coe.int/eng?i=001-57510>, 29.11.2017.

³³⁷ *Campbell v. The United Kingdom*, Application No: 13590/88, 25.03.1992, <http://hudoc.echr.coe.int/eng?i=001-57771>, E.T. 30.05.2019.

³³⁸ *Z. v. Finland*, Application No: 22009/93, 25.02.1997, <http://hudoc.echr.coe.int/eng?i=001-58033>, E.T. 30.05.2019.

³³⁹ *Malone v. United Kingdom*, Application No: 8691/79, 02.08.1984, <http://hudoc.echr.coe.int/eng?i=001-57533>, E.T. 06.10.2017.

bilgilerin saklandığı iddiası mevcuttur. İngiltere’de anılan dönemde, suçun önlenmesi ve aydınlatılması amaçları ile uzun süredir bilinen bir uygulama olarak İçişleri Bakanlığı tarafından bir izin düzenlenerek iletişimin denetlenmesi yoluna gidilmekte ve fakat bu hususta herhangi bir kanuni düzenleme bulunmamaktaydı. İHAM’a göre bu durum, kamu yetkililerine tanınan takdir yetkisinin kapsam ve usulünü makul ve açık bir biçimde belirtmemektedir. Dolayısıyla söz konusu durum kanuna uygun olan bir müdahale teşkil etmemektedir. Ayrıca İHAM, bir önceki karara kıyasla özgürlük- güvenlik denkleminde tutumunu özgürlüğe yaklaştırarak bu kez iletişimin denetlenmesinin kanuni çerçevesi belirli standartlar dahilinde olmadıkça suçun önlenmesi için gerekli görmemiş³⁴⁰ ve telefon konuşmalarının tarihine, uzunluğuna ve özellikle aranan numaralara ilişkin bilgilerin kullanılmasının 8. maddeye ilişkin müdahale oluşturabileceği gerekçesiyle ve devamında suçun önlenmesi için ilgili kişinin rızası olmaksızın polise bu bilgilerin verilmesini İHAS md. 8 kapsamında koruma altına alınan hakkın ihlali olarak değerlendirmiştir³⁴¹. Anılan çoğunluk görüşünde 108 Sayılı Sözleşme’den söz edilmese de çoğunluk görüşüne farklı bir gerekçe ile katılan yargıç Pettiti’ye göre, iletişimin denetlenmesi konusu kesinlikle veri bankaları meselesinden ayrı düşünülemez çünkü iletişimin denetlenmesi sonucu elde edilen verilerin saklanması durumu gündeme gelmektedir. Buna göre yargıç Pettiti, 108 Sayılı Sözleşme’deki temel ilkelere, bir tedbirin 8. maddenin ihlal edilmesine neden olup olmadığını değerlendiren ölçütler olarak atıfta bulunmuştur³⁴².

1985 yılındaki *Lundvall- İsveç* kararında ise Mahkeme yine bir veri koruma meselesini 8. madde bağlamında incelemiştir. Buna göre İHAM mevcut olayda başvurucunun kesinleşmeyen ve o esnada hala itiraz edilebilir olan bir liste olan gecikmeli vergiler siciline tescili hususunu değerlendirmiş ve sicilin kamuya ve kredi

³⁴⁰ *Malone v. United Kingdom*, Par. 1, 3, 31- 82, Application No: 8691/79, 02.08.1984, <http://hudoc.echr.coe.int/eng?i=001-57533>, E.T. 06.10.2017.

³⁴¹ *Malone v. United Kingdom*, Par. 84-88, Application No: 8691/79, 02.08.1984, <http://hudoc.echr.coe.int/eng?i=001-57533>, E.T. 06.10.2017.

³⁴² *Malone v. United Kingdom*, Concurring Opinion of Judge Pettiti, Application No: 8691/79, 02.08.1984, <http://hudoc.echr.coe.int/eng?i=001-57533>, E.T. 06.10.2017.

bilgi şirketlerine açık olması sebebiyle olayın 8. madde kapsamında ele alınması gerektiğini belirtmiştir. Ancak bu durum her ne kadar 8. madde bağlamında değerlendirilse ve hakka bir müdahale olarak kabul edilse de İsveç'te uzun yıllara dayalı bir prensip olan resmî belgelere ücretsiz erişim hakkının Basın Özgürlüğü Kanunu'nda yer alması sebebiyle hukuka uygun ve demokratik bir toplumda gerekli olarak nitelenmiştir³⁴³.

Veri işleme konusuna dair dönüm noktası olarak adlandırılabilir 1980'lerde verilmiş bir diğer İHAM kararı da 1987 yılına ait *Leander- İsveç*³⁴⁴tir. Anılan başvuru, İsveçli bir marangozun askeri bir deniz üssüne dahil binaları da bulunan bir deniz müzesinde çalışmak için yaptığı başvurusu esnasında gizli bir polis dosyasına dayanan personel kontrol prosedürü ardından işe alınmaması üzerine gerçekleştirilmiştir. Bu kararda İHAM, polisin özel yaşamla ilgili bir bilgiyi sadece saklaması hususunun özel yaşam hakkına yönelik bir müdahale olduğunu kabul etmiş, ancak bu müdahaleyi ulusal güvenliğin korunması meşru amacı bağlamında ve 1969 tarihli Personel Kontrol Yönetmeliği'ne dayanıyor olması sebebiyle kanuna uygun bir müdahale olarak görmüştür. Mahkeme'ye göre ilgili Yönetmelik, kişisel verilerin korunması açısından yeterli güvenceyi sağlamaktadır. Bu güvenceler genel itibarıyla, yalnızca birbiri ile bağlantılı bilgilerin toplanmasına ve açıklanabilmesine izin verilmesi, bu verilere dayanılarak alınan kararlara itiraz etme hakkının tanınmış olması ve bu alandaki işlemlerin Meclis Adalet Komisyonu, Meclis Ombudsmanı ve Adalet Bakanı tarafından denetlenmesidir. Dolayısıyla Mahkeme'ye göre 8. maddede yer alan özel yaşam hakkının yanı sıra, 10. madde bağlamında bilgi alma özgürlüğü de şahsa kişisel konumuyla ilgili bilgi içeren bir sicile erişim hakkını vermez ve devletin bu bilgileri kişiye vermesi yükümlülüğünü içermez³⁴⁵.

³⁴³ *Lundvall v. Sweden*, Application No: 10473/83, 11.12.1985, <http://hudoc.echr.coe.int/eng?i=001-72432>, E.T. 30.05.2019.

³⁴⁴ *Leander v. Sweden*, Application No: 9248/81, 26.03.1987, <http://hudoc.echr.coe.int/eng?i=001-57519>, E.T. 06.10.2017.

³⁴⁵ *Leander v. Sweden*, Application No: 9248/81, Par. 48- 57 & 74- 75, 26.03.1987, <http://hudoc.echr.coe.int/eng?i=001-57519>, E.T. 06.10.2017.

Leander kararının en önemli yönü, İHAM her ne kadar ihlale hükmetmese de polis tarafından gerçekleştirilen sadece saklama amaçlı veri toplama işlemlerinin de İHAS md. 8 kapsamında hak ihlali teşkil edebileceğinin ilk kez dile getirilmesidir. Fakat bu noktada devletlerin geniş bir takdir hakkı olduğu da vurgulanmıştır³⁴⁶. Ayrıca, *Leander* kararı ile İHAM kişinin özel yaşamına ilişkin yalnızca saklanan ve kişinin detaylarına erişemediği bir bilginin, İHAS md. 8 bakımından ihlal oluşturabileceğini belirttiğinde, bu bilginin 108 Sayılı Sözleşme’de tanınan ve saklanmasını da kapsamına aldığı otomatik işlenen “kişisel veri” bağlamında olup olmadığına dair yeni bir soruyu ortaya çıkarmıştır. 108 Sayılı Sözleşme’ye göre kişisel veri, “Kimliği belirli ya da belirlenebilir bir gerçek kişi hakkındaki tüm bilgileri ifade” etmektedir³⁴⁷. Ancak bu soru cevapsız kalmıştır.

Söz konusu döneme dair diğer bir önemli karar da 7 Temmuz 1989 tarihli *Gaskin-Birleşik Krallık*³⁴⁸’tır. Anılan olayda, çocukluğu süresince birden fazla koruyucu aile yanına verilen ve kötü muameleye maruz kaldığı iddiasında olan başvuru, bu yaşadığı ihmal ve zarar sebebiyle kendisi ile ilgili kayıtlara erişim için öncelikle yerel mercilere başvurmuştur. 1955 tarihli Çocuk Yuvası Düzenleme Yönetmeliği’ne göre yerel otoritenin başvuru ve bakımı ile ilgili gizli kayıtları tutmak görevi bulunmaktadır; fakat Yüksek Mahkeme başvuruçunun bu talebine, kayıtların özel ve gizli oldukları savı ile olumsuz cevap vermiştir ve bu karar 27 Haziran 1980 tarihinde kesinleşmiştir. Devamındaki süreçte ilgili Belediye Meclisi, çocuk bakımı ile ilgili birçok yeni düzenlemeye imza atmış ve Kasım 1983’te başvuruçunun dosyasına erişim hakkını, diğer muhatapların rıza göstermesi halinde tanımıştır. Bu bağlamda, 23 Mayıs 1986 tarihinde

³⁴⁶ *Leander v. Sweden*, Par. 58- 68, Application No: 9248/81, Par. 48- 57 26.03.1987, <http://hudoc.echr.coe.int/eng?i=001-57519> , E.T. 06.10.2017.

³⁴⁷ Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, Art. 2/a, <https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37> , E.T. 18.10.2017.

³⁴⁸ *Gaskin v. United Kingdom*, Application No: 10454/ 83, 07.07.1989, <http://hudoc.echr.coe.int/eng?i=001-57491> , E.T. 10.01.2018.

başvurucunun toplamda 46 kişinin dahil olduğu 352 dökümandan, 19 kişinin dahil olduğu 65 dökümana erişimine izin verilmiştir³⁴⁹.

Gaskin- Birleşik Krallık davasının İHAM ve veri koruma içtihadı bakımından önem taşıyan hususuna bakacak olursak; bu davaya dek İHAM, 8. maddenin temel amacını, kişiyi kamusal otoritelerin keyfi müdahalelerinden ari tutmak ve ayrıca aile yaşamına dair saygı gösterilmesini sağlayıcı pozitif yükümlülükler içermesi olarak ele almaktaydı. Ancak bu davada başvuru, kendisi ile ilgili bir bilgiye engelsiz bir biçimde erişiminin sağlanmadığını iddia etmiştir. Bu noktada İHAM, başvuru durumundaki kişilerin Sözleşme tarafından korunan temel hakları bağlamında hayati menfaatleri olduğunu kabul etmiştir. Kararda, bu tarz kayıtların her ne kadar muhatapların rızaları neticesinde paylaşılması 8. madde ile uyumlu görünse de kişinin kendine dair bir bilgiyi edinmesinde muhatapın keyfi reddi gibi durumların da olabileceği göz önünde tutularak, bilgi alma ve bu bağlamda kişinin kendi çocukluğunu bilme ve anlama haklarının orantılılık ilkesi doğrultusunda incelenmesi ve erişim izninin bağımsız bir otorite tarafından hükme bağlanmasının daha yerinde olduğu ve olayda bu durumu inceleyen bir otoritenin yokluğunda ihlale hükmedilmesi gereği belirtilmiştir. Daha açık bir ifade ile Mahkeme hassas verilere veya bu verilere erişime ilişkin bir talep söz konusu olan durumlarda bağımsız bir mekanizmaya erişim olması gerektiğine hükmetmiştir³⁵⁰.

Ayrıca İHAM nezdindeki davalarda kişisel verilerin korunması konusuna dair olayların bir boyutu da verinin kamu otoritelerince saklanması ve saklanan veriye bireysel erişim taleplerinin reddidir. Yukarıda bahsedilen *Gaskin- Birleşik Krallık* kararında çocukluğu süresince birden fazla sayıda koruyucu aile yanına verilmiş olan ve kötü muameleye maruz kaldığı iddiasında olan başvuru, bu ailelerin kimliğine ilişkin verilere ulaşmak istemiş, fakat bu bilgilerin gizli olduğu belirtilerek başvuru kişinin erişimi

³⁴⁹ *Gaskin v. United Kingdom*, Application No: 10454/ 83, Par. 26, 07.07.1989, <http://hudoc.echr.coe.int/eng?i=001-57491>, E.T. 10.01.2018.

³⁵⁰ *Gaskin v. United Kingdom*, Application No: 10454/ 83, Par. 38- 41, 49, 07.07.1989, <http://hudoc.echr.coe.int/eng?i=001-57491>, E.T. 10.01.2018; DE HERT, GUTWIRTH, “Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action”, *Reinventing Data Protection*, s. 19.

engellenmiştir. İHAM bu noktada başvurucunun çocukluğuna dair bu bilgilerin özel yaşam kapsamına girdiğini belirtmiş ve erişimin engellenmesi kararının bağımsız bir otorite tarafından verilmemesi sebebiyle ihlale hükmetmiştir. Bu bakımdan söz konusu karar, kişisel verilere erişim bakımından oldukça önem taşıyan kararlardan biridir. Ancak burada Mahkeme açık bir şekilde, bu kararın kişisel verilere genel bir erişim hakkı kuralı oluşturmadığını açıkça belirtmektedir³⁵¹.

24 Nisan 1990 tarihli *Kruslin- Fransa* ve *Huvig- Fransa* kararlarında ise Mahkeme, telefon dinlemelerinin özel yaşama saygı hakkına doğrudan bir müdahale oluşturduğunu ve bir kanuna dayanması gerektiğini vurgulamıştır. Özellikle teknolojinin geldiği seviye sebebiyle giderek karmaşıklaşan bu sistemlere dair kanuni düzenlemenin ise mümkün olduğunca açık ve ayrıntılı kurallara sahip olması gerektiği vurgulanmıştır³⁵².

İHAM nezdinde veri koruma ile özel yaşam kesişiminde ilk başta görünen temel problem, “özel yaşamla ilgili bilgi- veri” ifadesinde geçen “özel” sıfatının “kamusal-umumi” kelimelerinin zıttı anlamında mı kullanıldığına ilişkindi. Avrupa İnsan Hakları Komisyonu, 1994 yılında *Friedl- Avusturya*³⁵³ kararında, bu konuya eğilmiştir. Anılan olayda, Avusturya vatandaşı olan bir kişi, evsizlerin durumuna dikkat çekmek amaçlı bir gösteri yürüyüşüne katılmış ve devamında polis ilgili kişinin yürüyüşteki fotoğraflarını çekerek bunları saklamıştır. Mahkeme, başvurucunun fotoğraflarının tamamen kamusal bir alanda, kişilerin kimlik bilgileri ile eşleşme olmaksızın anonim biçimde, yürüyüşün gerçekleşme koşullarını kaydetmek amacıyla ve herhangi bir kişisel verinin veya

³⁵¹ *Gaskin v. United Kingdom*, Application No: 10454/ 83, 07.07.1989, Par. 37, <http://hudoc.echr.coe.int/eng?i=001-57491>, E.T. 10.01.2018.

³⁵² *Kruslin v. France*, Application No: 11801/85, Par. 33, 24.04.1990, <http://hudoc.echr.coe.int/eng?i=001-57626>, E.T. 21.01.2018; *Huvig v. France*, Application No: 11105/84, Par. 32, 24.04.1990, [http://cambodia.ohchr.org/sites/default/files/echrsources/Huvig%20v.%20France%20\[24%20Apr%201990%20\[EN\].pdf](http://cambodia.ohchr.org/sites/default/files/echrsources/Huvig%20v.%20France%20[24%20Apr%201990%20[EN].pdf), E.T. 21.01.2018.

³⁵³ *Friedl v. Austria*, Application No: 15225/89, 31.01.1995, <http://hudoc.echr.coe.int/eng?i=001-57917>, E.T. 18.10.2017.

görüntünün veri işleme sistemine girmediği durumun özel yaşama müdahale teşkil etmediğine hükmetmiştir³⁵⁴.

2000 yılı ile birlikte İHAM, 108 Sayılı Sözleşme'nin sistemine de uygun olarak, içtihatlarında artık oldukça geniş bir biçimde ele aldığı "özel yaşam" kavramı doğrultusunda "özel yaşamla ilgili veri" (information relating to private life) anlayışını da genişletmiştir. *Amann- İsviçre*³⁵⁵ kararına konu olan olayda, tüy dökücü aletlerin satışını sağlayan başvurucu, Sovyet Elçiliği'nden aranmış ve kendisine "Perma Tweez" adlı pille çalışan bir tüy dökücü aletin siparişi verilmiştir. Bu esnada, söz konusu telefon görüşmesi savcılık tarafından dinlemeye tabi tutulmuş ve savcılık istihbarat servisinden satıcı ve sattığı mallarla ilgili bir soruşturma başlatılmasını talep etmiştir. Devamında savcılık, polisin bilgi verdiği hususlara dayanarak başvuran hakkında "ulusal güvenlik kartı endeksi için bir kart" (a card on the applicant for its national security card index) hazırlamıştır. İHAM'a göre özel yaşam, daha evvel anılan *Niemietz* kararında olduğu gibi, sınırlı bir biçimde tanımlanmamalıdır ve iş ya da profesyonel yaşamı özel yaşamdan ayırmak için bir sebep yoktur. Ayrıca bu durum 108 Sayılı Sözleşme ile de uyum göstermektedir. Bu bağlamda Mahkeme, başvuran hakkındaki kartta yer alan "Rus Elçiliği ile bir irtibatı olduğu" ve "şirketi aracılığı ile çeşitli işler yaptığı" ifadelerinin inkâr edilemeyecek bir şekilde başvuranın "özel yaşamı" ile ilgili veriler olduğunu, kişinin özel yaşamına dair verilerin saklanması da İHAS'ın 8. maddesi kapsamında ele alınması gerektiğini belirtmiştir³⁵⁶.

Bu karardan kısa bir süre sonra İHAM, 108 Sayılı Sözleşme'de yer alan geniş kapsamlı kişisel veri kavramını İHAS 8. madde kapsamında geniş yorumlanan özel yaşam kavramı ile ilişkilendirerek bazı umumi bilgilerin sistematik bir biçimde

³⁵⁴ *Friedl v. Austria*, Application No: 15225/89, Par. 49- 51, 31.01.1995, <http://hudoc.echr.coe.int/eng?i=001-57917>, E.T. 18.10.2017.

³⁵⁵ *Amann v. Switzerland*, Application No: 27798/95, 16.02.2000, <http://hudoc.echr.coe.int/eng?i=001-58497>, E.T. 18.10.2017.

³⁵⁶ *Amann v. Switzerland*, Application No: 27798/95, Par. 9- 11, 65- 67, 16.02.2000, <http://hudoc.echr.coe.int/eng?i=001-58497>, E.T. 18.10.2017.

saklanmak suretiyle “özel yaşam” kapsamında olabileceğine hükmetmiştir³⁵⁷. Dolayısıyla özel yaşamla alakalı bilgilerin mutlak surette umumi bilginin zıttı olması gerektiği algısını tamamiyla ortadan kaldırmıştır. *Rotaru- Romanya* kararına konu olan olayda, Romanya uyruklu başvuru Romanya İstihbarat Servisi tarafından edinilmiş kendi hakkındaki bilgilerin yanlış ve şerefine zedeleyici olduğu iddiasındadır. Bu bilgiler bir mektup vasıtası ile ortaya çıkmıştır ve genel itibarı ile başvuru kişinin elli yıl evvelki gençlik dönemine, hakkındaki cezai soruşturmalara ve dahil olduğu aşırı sağ siyasi faaliyetlerine dairdir. Başvuruda başvuru kişinin temel iddiası, kendisine dair saklanan yalnızca özel yaşamına ait bilgilerin değil, genel bilgilerin de İHAS md. 8 kapsamında değerlendirilmesi gerektiğidir. İHAM’da bu bilgilerin istihbarat servisi tarafından sistemli ve sürekli bir biçimde toplanması sebebiyle durumu md. 8 kapsamında “özel yaşam” dahilinde değerlendirmiştir. Ayrıca bazı bilgilerin isim benzerliği sebebiyle yanlış olması ve başvuru kişinin itibarını zedelemesi, meselenin İHAS md. 8 bağlamında ele alınmasını zorunlu hale getirmiştir³⁵⁸.

Mahkeme ayrıca özel yaşam hakkı kapsamında bir dereceye kadar kişilerin bilgilerinin geleceğini tayin hakkı da olduğunu kabul etmektedir. Bu bağlamda, kişisel dosyalara erişim³⁵⁹, kamuya açık dosyalardan kişisel verilerin silinmesi³⁶⁰, transseksüellerden resmi cinsel verilerini düzeltme hakkına ilişkin iddialar 8. madde kapsamında ele alınmıştır.

³⁵⁷ *Rotaru v. Romania*, Par. 43, Application No: 28341/95, 04.05.2000, <http://hudoc.echr.coe.int/eng?i=001-58586>, E.T. 19.10.2017.

³⁵⁸ *Rotaru v. Romania*, Application No: 28341/95, Par. 42- 44, 04.05.2000, <http://hudoc.echr.coe.int/eng?i=001-58586>, E.T. 19.10.2017.

³⁵⁹ *Gaskin v. United Kingdom*, Application No: 10454/ 83, 07.07.1989, <http://hudoc.echr.coe.int/eng?i=001-57491>, E.T. 10.01.2018; *McGinley and Egan v. The United Kingdom*, Application No: 21825/93& 23414/94, 28.01.2000, <http://hudoc.echr.coe.int/eng?i=001-58452>, E.T. 30.05.2019.

³⁶⁰ *Leander v. Sweden*, Application No: 9248/81, 26.03.1987, <http://hudoc.echr.coe.int/eng?i=001-57519>, E.T. 06.10.2017; *Segerstedt-Wiberg and others v. Sweden*, Application No. 62332/00, 06.09.2006, <http://hudoc.echr.coe.int/eng?i=001-75591>, E.T. 30.05.2019.

2001 yılında ise İHAM, *P.G. ve J.H.- Birleşik Krallık*³⁶¹ kararında Rotaru içtihadını geliştirmek amacıyla 108 Sayılı Sözleşme'ye atıfta bulunmuştur. Bu karara göre, sokakta yürüyen bir kimse kaçınılmaz olarak orada bulunan toplumun diğer üyelerine de görünür hale gelir. Kişinin sokakta yürümesinin teknolojik araçlarla gözetiminde de aynı özellik görülmektedir. Fakat özel yaşama ilişkin kaygılar esas olarak, ortada sistematik ya da kalıcı bir biçimde kayıt altına alma söz konusu olduğunda ortaya çıkar. Bu bakımdan güvenlik güçlerinin bir kişi hakkında bilgi toplaması (telefon dinlemeleri de dahil olmak üzere), müdahaleci veya gizli bir yöntemle olmasa dahi, İHAS'ın 8. maddesi bağlamında değerlendirilir. Olay özelinde ise, başvuruçuların tutuldukları ve hücrede oldukları esnada seslerinin kayıt altına alınması da bu kapsamdadır. Bu noktada İHAM, kişisel verilerin korunmasında temel bir ilke olan amacın sınırlandırılmasına (amaca bağlılık ilkesi) değinerek kişisel verinin öngörülebilir kullanımı ötesinde kullanılamayacağına da hükmetmiştir³⁶².

2006 yılında *Segerstedt-Wiberg- İsveç* kararına konu olayda başvuruçular İsveç Güvenlik Polisi tarafından kendileri hakkında tutulan kayıtlara erişmek istemektedirler. Ancak talepleri ulusal güvenliği tehdit edebileceği veya polis faaliyetlerini engelleyebileceği gerekçesiyle reddedilmektedir. İHAM öncelikle verilerin kaydedilmesinin 1998 tarihli Polis Veri Yasası'nda hukuki bir temeli olduğu tespitini yaparak, yasada yetkili makamlara verilen takdir yetkisinin kapsamı ve uygulama şeklinin yeterince açık bir şekilde düzenlendiğini belirtmektedir. Ayrıca bilgilere bütünüyle erişilmesinin reddedilmesiyle ilgili olarak, İsveç'in ulusal güvenlik çıkarları ve terörizmle mücadelesi ile başvuranların özel yaşam hakkının dengelenmek zorunda olduğunu dile getirmektedir. Ancak İHAM, başvuruçulardan Segerstedt-Wiberg harici olanlar bakımından, 1960'lardan kalma verilerinin depolanmasının, söz konusu ulusal

³⁶¹ *P.G. and J.H. v. The United Kingdom*, Application No: 44787/98, 25.12.2001, <http://hudoc.echr.coe.int/eng?i=001-59665>, E.T. 02.11.2017.

³⁶² *P.G. and J.H. v. The United Kingdom*, Par. 43- 44, 57, 59, Application No: 44787/98, 25.12.2001, <http://hudoc.echr.coe.int/eng?i=001-59665>, E.T. 02.11.2017; DE HERT, GUTWIRTH, "Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action", *Reinventing Data Protection*, s. 19.

güvenlik ve terörle mücadele amaçları bakımından gerekli olmadığından bahisle kamuya açık dosyalardan kişisel verilerin silinmesi iddialarını 8. madde bakımından kabul etmiştir³⁶³.

İHAM 2007 yılında *Copland- Birleşik Krallık* davasında ise telefon, internet ve email iletişimi bakımından önemli bir karara imza atmıştır. Bu karara göre, Mahkeme'nin daha önceki *Amann- İsviçre* içtihadında dile getirdiği üzere, işyerinden gelen telefon görüşmeleri 8. madde kapsamında özel yaşam içerisinde değerlendirilmektedir. Buradan hareketle dava konusu olayda işyerinden gönderilen mailler ile işyerindeki internet kullanımının izlenmesiyle elde edilen bilgiler de bu bağlamda değerlendirilmiştir. Mevcut davada başvurucuya telefon görüşmelerinin izlendiği ve bundan sorumlu olacağı konusunda herhangi bir uyarıda bulunulmamıştır. Bu nedenle başvurucuda iş telefonundan yapılan aramaların gizliliği konusunda makul bir beklenti vardır. İHAM'a göre aynı beklenti, başvurucunun e-posta ve internet kullanımı için de geçerli olmalıdır. Dolayısıyla davada 8. madde bakımından ihlal söz konusudur³⁶⁴.

2008 yılındaki *S. ve Marper- Birleşik Krallık*³⁶⁵ davasında İHAM, parmak izleri, DNA profilleri ve hücre örneklerinin tanımlanmış veya tanımlanabilir olmaları sebebiyle 1998 tarihli Veri Koruma Kanunu'na göre kişisel veri oluşturduğuna ve bunların yalnızca saklanmalarının özel yaşam hakkına bir müdahale oluşturduğuna hükmetmiştir. İHAM özellikle hücrel örneklerin elde edilmesi, genetik bilimi ve bilgi teknolojilerinin gelişim hızı göz önüne alındığında geleceğe yönelik kullanımları bakımından genetik bilgiye bağlı özel yaşamın çıkarlarının yeni yollarla ya da günümüzde tahmin edilemeyecek bir biçimde olumsuz şekilde etkilenebileceği olasılığını da göz önünde bulundurmaktadır. Ayrıca hücrel örneklerin benzersiz birer genetik kod içermeleri sebebiyle hem kişiler hem de akrabaları hakkında kişisel veri teşkil ediyor olduğu belirtilmiştir. Buna karşın

³⁶³ *Segerstedt-Wiberg and others v. Sweden*, Par. 87- 90, Application No. 62332/00, 06.09.2006, <http://hudoc.echr.coe.int/eng?i=001-75591> , E.T. 30.05.2019.

³⁶⁴ *Copland v. The United Kingdom*, Par. 41, 44, Application No: 62617/00, 03.07.2007, <http://hudoc.echr.coe.int/eng?i=001-79996> , E.T. 29.05.2019.

³⁶⁵ *S. and Marper v. The United Kingdom*, Application Nos: 30562/04 and 30566/04, <http://hudoc.echr.coe.int/eng?i=001-90051> , E.T. 03.11.2017.

DNA örneklerinin çok daha sınırlı biçimde kişisel veri oluşturduğu ve bu verilerin de objektif ve reddedilemez kendine has olan numerik bir kod biçiminde kayıt altına alındığı ve bunların yalnızca sınırlı sayıda kişi tarafından analiz edilebileceği dile getirilmiştir. Fakat kuşkusuz DNA örnekleri, özellikle kişiler arası genetik ilişkileri ortaya çıkarabilmeleri bakımından kişilerin özel yaşam haklarına doğrudan bir müdahale teşkil etmektedir³⁶⁶. Parmak izleri bakımından ise İHAM, bu verilerin her ne kadar hücrel örnekler ve DNA örnekleri kadar bilgi içermeseler de objektif ve reddedilemez karakterleri dolayısıyla içeriğinden ziyade doğrudan kimliklendirmeye sebep olmaları bakımından kamusal otoritelerce düzenli ve kalıcı olarak kayıtlanmaları ve saklanmalarının özel yaşam bakımından endişeler doğurabileceğini belirtmiştir³⁶⁷.

2012 yılındaki *Khelili- İsviçre*³⁶⁸ kararıyla ise İHAM, bir kişisel verinin özel yaşamın herhangi bir yönünü etkileyip etkilemediğini belirlemek için verinin toplanışı, saklanması, verinin ne şekilde kullanıldığı, işlendiği, mahiyeti ve işleme sonucu edinilen sonuçların dikkate alınmasının gerektiğini belirtmiştir³⁶⁹.

İHAM 2015 yılında *R.E.- Birleşik Krallık* kararı ile birlikte sıkı güvenlik önlemleri gerektiren avukat- müvekkil telefon görüşmeleri konusunda ilkelerin belirlenmesi konusunda bir başlangıç yapmıştır. Olayda, Kuzey İrlanda'da bir polis memurunun öldürülmesi ile ilgili üç kez gözaltına alınıp tutuklanan başvuru, hassas tutuklular olarak adlandırılan zihinsel bozukluğu olan kişi veya başka türlü zihinsel olarak savunmasız olan çocuklar ile kararda uygun bir yetişkin olarak geçen zihinsel olarak bozulmuş ya da zihinsel olarak savunmasız insanlarla başa çıkmada deneyimli bir kişi veya akraba ya da vasi olan kişiler veya avukatları arasındaki görüşmelerin gizli gözetim rejimi hakkında şikayetçi olmuştur. Mevcut davada İHAM, bu tür hukuki görüşmelerin

³⁶⁶ *S. and Marper v. The United Kingdom*, Application Nos: 30562/04 and 30566/04, Par. 39, 71- 75, <http://hudoc.echr.coe.int/eng?i=001-90051> , E.T. 03.11.2018.

³⁶⁷ *S. and Marper v. The United Kingdom*, Application Nos: 30562/04 and 30566/04, Par. 78, 84- 86, <http://hudoc.echr.coe.int/eng?i=001-90051> , E.T. 03.11.2018.

³⁶⁸ *Khelili v. Switzerland*, Application No: 16188/07, <http://hudoc.echr.coe.int/eng?i=001-107032> , E.T. 03.11.2018.

³⁶⁹ *Khelili v. Switzerland*, Application No: 16188/07, Par. 55, <http://hudoc.echr.coe.int/eng?i=001-107032> , E.T. 03.11.2018.

gizli gözetimi konusunda Sözleşme'nin 8. maddesinin ihlal edildiğine karar vermiştir. Olayda gizli gözetim yoluyla elde edilen malzemelerin güvenli bir şekilde ele alınması, depolanması ve imhası için düzenlemelere ilişkin rehber ilkelerin 22 Haziran 2010'dan beri uygulandığı belirtilmiştir. Ancak başvuru Mayıs 2010'da gözaltına alınmış ve bu tarihte söz konusu rehber ilkeler uygulamaya konulmamıştır. Dolayısıyla Mahkeme o tarihteki yasal düzenlemelerin başvuruçunun avukatı ile gerçekleştirdiği görüşmelerin korunması için yeterli güvenceyi sağladığı konusunda emin olamamıştır. Öte yandan Mahkeme, tutuklular ile zihinsel olarak bozulmuş ya da zihinsel olarak savunmasız insanlarla başa çıkmada deneyimli bir kişi veya akraba ya da vasi olan kişilerin görüşmelerinin aynı yasal imtiyazlara sahip olmaması dolayısıyla 8. maddenin ihlal edilmediğine hükmetmiştir³⁷⁰.

2016 yılında ise Mahkeme *Karabeyoğlu- Türkiye* kararında, bir Cumhuriyet Savcısı olan başvuruçunun Ergenekon Davası'nın ceza soruşturması kapsamında telefonlarının dinlenmesi ve ayrı bir disiplin soruşturması kapsamında elde edilen bilgilerin kullanımını incelemiştir. Mahkeme, ceza soruşturması sırasında yapılan dinlemenin demokratik bir toplumda, hukukun üstünlüğünün gerektirdiği asgari koruma derecesine sahip olduğunu, zira telefon dinlemesinin nesnel olarak makul bir şüpheye dayanarak ilgili mevzuata uygun olarak yapıldığını tespit etmiştir. Mahkeme'ye göre, başvuranın özel hayatına saygı gösterme hakkına müdahale edilmesi, ulusal güvenlik ve suçun önlenmesi için gerekli olmuştur. Bu bakımdan İHAM ceza soruşturması ile bağlantılı olarak telefon dinleme hususunda 8. maddenin ihlal edilmediğine hükmetmiştir. Öte yandan disiplin soruşturması bağlamında, elde edilen bilgilerin kullanımının kanuna aykırı olduğuna ve ilgili mevzuatın iki açıdan ihlal edildiğine hükmetmiştir. Buna göre disiplin soruşturmasında kullanılan bilgiler, toplandıkları amaçtan başka amaçlar için kullanılmış ve soruşturma sona erdikten sonra 15 günlük süre

³⁷⁰ *R.E. v. The United Kingdom*, Application No: 62498/11, Par. 140- 143, 165- 168, <http://hudoc.echr.coe.int/eng?i=001-158159>, E.T. 19.05.2019.

içinde imha edilmemiştir. Bu bakımdan elde edilen bilgilerin disiplin soruşturmasında kullanılmasının 8. maddeyi ihlal ettiğine karar vermiştir³⁷¹.

İHAM'ın 2017 yılında verdiği *Mustafa Sezgin Tanrıkulu- Türkiye* kararında başvuru, yurtdışı bağlantılı silahlı terör örgütlerinin faaliyetlerine yönelik suç delillerinin elde edilebilmesi için bir buçuk aylık dönemdeki tüm telefon görüşmelerinin detay bilgilerinin kendisine verilmesini isteyen MİT'in talebini kabul eden Diyarbakır Ağır Ceza Mahkemesi'nin kararına ilişkin şikayetçi olmuştur. Mahkeme öncelikle 4422 Sayılı Kanun'a göre yetkililerin dinleme kararı alabilmesi için kanunda belirtilen suçları işlediğinden kuvvetle şüphelenilen kişilerin spesifik olarak belirtilmesi gerektiğini hüküm altına almıştır. Bu belirleme, isim, adres, telefon numarası veya ilgili başka bilgilerin belirtilmesi suretiyle yapılmalıdır. Fakat olayda Diyarbakır Ağır Ceza Mahkemesi, Türkiye Cumhuriyeti'nde bulunan herkesin iletişiminin denetlenmesi için bu yetkiyi veren bir karara hükmetmiştir. Ayrıca İHAM söz konusu 4422 Sayılı Kanun'a, başka suretle bir delil elde edilemeyecek olmasının muhtemel olduğu durumlarda başvurulması gerektiğine dikkat çekmiştir. Tüm bu sebeplerle Mahkeme, mevcut davadaki müdahale kararının anılan kanuna uygun olmadığını tespit ederek Sözleşme'nin 8. maddesinin ihlal edildiğine karar vermiştir³⁷².

2018 yılında hükme bağlanan *Benedik- Slovenya* kararı ise, Slovenya polisinin belirli bir dosya paylaşım ağı kullanıcılarının izlenmesi sırasında İsviçre emniyet makamları tarafından kaydedilen dinamik bir IP adresi ile ilişkili abone bilgilerine erişmek için mahkeme emri alamamasıyla ilgilidir. İHAM bu olayda 8. maddenin ihlal edildiğine karar vermiştir. Mahkeme'ye göre polisin dinamik IP adresi ile ilgili abone bilgilerini almak için dayandığı yasal hüküm açıklıktan yoksun olması sebebiyle keyfi müdahaleye sebep olarak Sözleşme'nin “kanuna uygun olma” standardını

³⁷¹ *Karabeyoğlu v. Turkey*, Application No: 30083/10, Par. 96, 110- 111, 119- 121, <http://hudoc.echr.coe.int/eng?i=001-163455>, E.T. 19.05.2019.

³⁷² *Mustafa Sezgin Tanrıkulu v. Turkey*, Application No: 27473/06, Par. 55- 60, <http://hudoc.echr.coe.int/eng?i=001-175464>, E.T. 19.05.2019.

karşılamamaktadır. Ayrıca olaya müdahil olan polis kuvvetlerinin bağımsız bir biçimde denetimlerini sağlayacak bir denetim mekanizması da bulunmamaktadır³⁷³.

İHAM'ın 8. maddeye ilişkin olarak 2019 yılının Temmuz ayında karara bağladığı *Gorlov ve Diğerleri- Rusya* kararı ise gözaltında tutulan kişilerin hücrelerinin kapalı devre kameralar (CC TV) ile gözetimi hakkındadır. Başvurucu olan üç erkek, hücrelerinin sürekli olarak CC TV'ler ve kadın gardiyanlar tarafından gözetlenmesinin 8. madde bağlamında özel yaşamlarına saygı haklarının ihlal ettiğini belirterek başvuruda bulunmuştur. Mahkeme ilk olarak söz konusu olayda özel yaşam hakkına bir müdahale olduğunu ancak bu müdahalenin 8/2. madde doğrultusunda erişilebilir ve öngörülebilir bir kanuna uygun olmadıkça ihlal sonucunu doğuracağını belirtmiştir. Somut olay özelinde ise İHAM, gözetim konusunda ilgili kanuni düzenlemenin ortak alanlar ve yerleşim yerlerinin gözetlemeye tabi olup olmadığı hususunu, gözetimin günün hangi saatlerinde, hangi süre ile ve hangi koşullar altında gerçekleştirilebileceği konularını cevapsız bıraktığı tespitinde bulunmuştur. Bu bakımdan iç hukukta her ne kadar söz konusu gözetime ilişkin kanuni bir düzenleme bulunsa da yasal çerçevenin gereken açıklık, kesinlik ve belirlilik ilkelerini barındırmadığından bahisle 8. maddenin ihlal edildiğine karar vermiştir. Burada ayrıca belirtilmelidir ki Mahkeme, ceza infaz kurumlarının belirli alanlarının ve hatta bazı tutukluların devamlı izlenmelerinin, somut olaya göre gerekli olabileceğine de dikkat çekmiştir³⁷⁴.

3. Özel Yaşamın Korunması Hakkı Bağlamında Sağlık Verilerinin Korunması

Daha önce belirttiğimiz üzere İHAM, kişisel verilerin korunması meselesinde görece çekingen bir tavır takınıyor denilebilecektir. Fakat bu tutum, sağlık verileri bakımından farklılık arz etmektedir. İHAM, sağlık verilerinin korunması hususunda çok daha istekli görünmektedir. Ancak genel veri koruma bağlamında ve hangi ölçüde

³⁷³ *Benedik v. Slovenia*, Application No: 62357/14, Par. 130, 132- 134, <http://hudoc.echr.coe.int/eng?i=001-182455>, E.T. 19.05.2019.

³⁷⁴ *Gorlov and Others v. Russia*, Application Nos: 27057/06, 56443/09, 25147/14, 02.07.2019, Par. 83, 97-100, <http://hudoc.echr.coe.int/eng?i=001-194247> , E.T. 18.05.2019.

korunacağı mı ya da güçlendirilmiş koruması olan özel veri kategorilerinden olarak mı değerlendirileceği oldukça tartışmalıdır.

1997 yılındaki *Z.- Finlandiya* davasında, HIV virüsü taşıyıcısı olan erkeğin insan öldürme ve tecavüz suçlarına dair dosyasında kendisinin ve eşinin tıbbi kayıtlarının bulunması ve bu bilgilerin basında yer almasının İHAS md. 8 bakımından özel yaşam ihlali oluşturup oluşturmadığını incelenmektedir. İHAM, tıbbi verilerin korunmasının İHAS'ın 8. maddesindeki özel yaşama saygı hakkı kapsamında büyük önem arz ettiğini, Sözleşmeciler tarafların hukuk sistemleri bakımından sağlık verilerinin gizliliğinin hayati önem taşıdığını dile getirmiştir³⁷⁵. Mahkeme'ye göre bu bilgiler yalnızca 108 Sayılı Sözleşme bakımından “kişisel veri” oluşturmakla kalmaz, aynı zamanda böyle bir koruma olmaksızın bireylerin özel ve aile yaşamlarını oldukça negatif biçimde etkileyebilme ihtimalini içermektedir. Bu bakımdan tıbbi açıdandan yardıma muhtaç olan kişiler uygun tedaviyi almaları gerekmesine rağmen, kendilerine dair böylesi mahrem bir bilgiyi sağlıklarını tehlikeye atma ve hatta hastalığın bulaşma ihtimallerinde dahi paylaşmaktan kaçınabilirler³⁷⁶.

Sağlık verilerine ilişkin bir diğer önemli karar ise 2008 yılına ait *I- Finlandiya*³⁷⁷ kararıdır. Hasta kayıtlarının korunması hakkında olan ilgili karar, pozitif yükümlülük doktrinine kişisel verilerin korunması bakımından önemli bir yenilik getirmiştir³⁷⁸. Davaya konu olan olayda, HIV pozitif olan ve tedavi gördüğü hastanede çalışan olan hastanın gizli olması gereken kayıtları, meslektaşları tarafından hukuksuz bir biçimde istişare edilmiştir. İHAM bu kararda özel yaşamın gizliliğinin devletlere yalnızca hakka müdahalede bulunmaktan kaçınma yükümlülüğü değil, ayrıca kişiler arasındaki ilişkiler alanında özel yaşamın korunması bakımından gerekli önlemlerin alınması gibi pozitif

³⁷⁵ *Z v. Finland*, Application No: 22009/93, Par. 95, <http://hudoc.echr.coe.int/eng?i=001-58033> , E.T. 08.11.2018.

³⁷⁶ *Z v. Finland*, Application No: 22009/93, Par. 96, <http://hudoc.echr.coe.int/eng?i=001-58033> , E.T. 14.08.2018.

³⁷⁷ *I v. Finland*, Application No: 20511/03, <http://hudoc.echr.coe.int/eng?i=001-87510> , E.T. 15.08.2018.

³⁷⁸ Paul DE HERT, *Citizen's Data and Technology: An Optimistic Perspective*, The Hague Dutch Data Protection Authority, 2009, s. 25; FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, s. 102.

yükümlülüğünün de olduğunu vurgulamaktadır. İHAM ayrıca sağlık verisinin mahremiyetinin sağlanmasının yalnızca İHAS ve özel yaşam hakkı bakımından önem arzemediği, bu durumun sağlık sistemine olan güveni de doğrudan etkilediğini belirtmiştir³⁷⁹.

2008 yılına ait ve yukarıda söz konusu ettiğimiz *S. ve Marper- Birleşik Krallık* davası da DNA profilleri ve hücre örnekleri bakımından bu başlık altında yeniden dile getirilmelidir. Buna göre Mahkeme, DNA profilleri ve hücre örneklerinin tanımlanmış veya tanımlanabilir olmaları sebebiyle kişisel veri oluşturduğuna ve bunların yalnızca saklanmalarının dahi özel yaşam hakkına bir müdahale oluşturduğuna hükmetmiştir³⁸⁰.

2014 yılında İHAM *L.H.- Letonya* kararında başvuru, kişisel tıbbi verilerinin bir Devlet ajansı tarafından rızası olmadan toplanmasının özel yaşam hakkını ihlal ettiğini iddia etmiştir. Bu kararda Mahkeme öncelikle özel yaşama saygı hakkı bağlamında sağlık verilerinin korunmasının önemini vurgulamaktadır. Özellikle Letonya kanunlarının, bir Devlet kurumu tarafından toplanabilecek özel verilerin kapsamını, başvuruçunun yedi yıllık bir süre boyunca ayırım gözetmeksizin ve önceden herhangi bir değerlendirme yapmadan toplanmasına neden olacak şekilde sınırlamadığını kaydetmiştir. Bu bakımdan İHAM, geçerli kanunların yetkili makamlara verilen takdir yetkisinin kapsamını ve uygulama şeklini yeterince net bir şekilde belirtmediğinden bahisle 8. maddenin ihlal edildiğini hüküm altına almıştır³⁸¹.

İHAM'ın kişisel veri meselesiyle alakalı tüm bu genel içtihatlarına bakıldığında, kişisel verilerin korunmasının temelinin görüldüğü kadar sağlam olmadığı sonucuna varılabilecektir. Her ne kadar *Klass, Leander, Amann, P.G. ve J.H.* gibi içtihatlarla özerklik ve kişisel veri kavramları geliştirilerek Mahkeme'nin mahremiyet ve özel yaşam

³⁷⁹ *I v. Finland*, Application No: 20511/03, Par. 36, 38, <http://hudoc.echr.coe.int/eng?i=001-87510> , E.T. 29.08.2018.

³⁸⁰ *S. and Marper v. The United Kingdom*, Application Nos: 30562/04 and 30566/04, Par. 68, <http://hudoc.echr.coe.int/eng?i=001-90051> , E.T. 03.11.2017.

³⁸¹ *L.H. v. Latvia*, Application No: 52019/07, Par. 57- 60, <http://hudoc.echr.coe.int/eng?i=001-142673> , E.T. 19.05.2019.

kavramlarının ötesine geçilse de temel veri koruma kurallarının Strazburg korumasında mevcut olmadığı söylenebilecektir. Hem Komisyon tarafından verilen kararlarda hem de Mahkeme tarafından verilen kararlarda görülmektedir ki kişisel verilerin işlenmesinin tüm yönleri İHAS tarafından korunmamaktadır³⁸². Mahkeme ayrıca 8. maddenin kişisel verilere erişim için genel bir hak vermediğini de belirtmiştir. Söz gelimi *Leander* kararında İHAM açıkça böyle bir hakkı inkâr etmemiş; fakat meseleden de bahsetmemiştir³⁸³. Bu durumda bazı otomatik işleme faaliyetlerinin 8. madde kapsamı dışında kalıp kalmadığı net değildir³⁸⁴. Bu husus çalışmamızda incelenen 2018 yılına dek olan tüm kararlarda bu biçimdedir. Her ne kadar son olarak Şubat 2019’da yayımlanan Bilgi Metni³⁸⁵’nin başlığı “Kişisel Verilerin Korunması” olsa da bağımsız bir kişisel verilerin korunması hakkının yokluğu yanında ayrıca kararlar hüküm altına alınırken hangi bakımdan kişisel verilerin korunması hakkının 8. maddenin altında ihlal edildiği açıkça ele alınmamaktadır. Mahkeme’nin gözünde, özel hayatı etkileyen kişisel verilerin işlenmesi ve kişilerin özel hayatlarını etkilemeyen kişisel verilerin işlenmesi biçiminde bir ayrım vardır. Bu bakımdan İHAM, 8. madde kapsamına giren kişisel verilerle bu kapsama girmeyen kişisel verileri ayırmaktadır. Oysa veri koruma hukukunda kişiye dair belirli ya da belirlenebilir tüm bilgiler kişisel veriyi oluşturmaktadır. Sonuç olarak Avrupa Konseyi’nin yargılama organı olan İHAM tüm bu sebeplerle Avrupa Veri Koruma Hukuku’nun eksik bir ayağını oluşturmaktadır.

³⁸² DE HERT, GUTWIRTH, “Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalisation in Action”, *Reinventing Data Protection*, s. 24.

³⁸³ *Leander v. Sweden*, Application No: 9248/81, 26.03.1987, <http://hudoc.echr.coe.int/eng?i=001-57519>, E.T. 30.05.2019.

³⁸⁴ Herke KRANENBORG, “Access to Documents and Data Protection in the European Union: On the Public Nature of Personal Data”, *Common Market Law Review*, Vol. 45, Issue: 4, 2008, s. 1093- 1094, ss. 1079-1114.

³⁸⁵ Kaldı ki Bilgi Metinleri İHAM’ı bağlamamaktadır. *Factsheet- Personal Data Protection*, European Court of Human Rights, Press Unit, February 2019, https://www.echr.coe.int/Documents/FS_Data_ENG.pdf, E.T. 19.05.2019.

II. AVRUPA BİRLİĞİ

Avrupa Veri Koruma Hukuku'nun şekillenmesinde en büyük etkiye sahip belgeler Avrupa Birliği kapsamında düzenlenmiştir denilebilir. Bunun sebebi, özellikle 95/46/AT Sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi ve Veri Koruma Reformu'nun temeli olan 2016/679 Sayılı Genel Veri Koruma Tüzüğü'nün AB bünyesinde doğmuş olmalarıdır. 95/46/ AT Sayılı Direktif, üye devletler bakımından her ne kadar doğrudan uygulama alanına sahip olmasa da ilerleyen bölümlerde görüleceği üzere, AB üyesi olmayan Türkiye bakımından dahi kanun yapımında temel alınan belge olmuştur. GVKKT ise, üye devletlerde doğrudan uygulanıyor olması ve uygulama alanını AB dışını da kapsamaması bakımından Direktif'in çok daha ötesine geçmiştir. Ayrıca 2000 yılında kabul edilen AB Temel Haklar Şartı da kişisel verilerin korunmasını anayasal düzeyde ayrı bir temel hak olarak tanımış olması bakımından önem taşımaktadır.

Kişisel verilerin korunmasının AB hukuk düzeninde temel hak olarak tanınması birçok bakımdan pozitif değerlendirilmiştir. 95/46/AT Sayılı Direktif iki temel amaca sahipti: Kişisel verilerin iç pazarda serbestçe dolaşımı ve temel hak ve özgürlüklerin korunması. Her ne kadar her iki amacın da eşit derecede önemli olduğu söylene de zamanla ekonomik bakış açısı daha baskın hale gelmiştir³⁸⁶. Kaldı ki Direktif'in, özel sektör dostu birkaç hüküm içermesi sebebiyle insan haklarını korumak bakış açısının çok da net olmadığını belirten bazı görüşler de mevcuttur. Bu bakımdan Temel Haklar Şartı'nda kişisel verilerin korunmasının ayrı bir hak olarak tanınması, Direktif'in bu eksikliğini giderme yolu olarak da değerlendirilmiştir³⁸⁷. Kişisel verilerin korunmasının Temel Haklar Şartı tarafından bağımsız bir temel hak olarak tanınması ayrıca, yukarıda

³⁸⁶ Commission of the European Communities, *First Report on the Implementation of the Data Protection Directive (95/46/EC)*, COM (2003) 265, Brussels, 15.05.2003, http://eur-lex.europa.eu/LexUriServ/site/en/com/2003/com2003_0265en01.pdf, E.T. 28.05.2019.

³⁸⁷ Serge GUTWIRTH, *Privacy and the Information Age*, For the Rathenau Institute, Raf CASERT (Çev.), Rowman& Littlefield, 2002, s. 91- 94.

ele alındığı üzere, İHAM'ın konuya ilişkin içtihadında öngöremediği birçok hukuki soruna da çözüm sunmaktadır³⁸⁸.

Tüm bu nedenlerden dolayı bu bölümde öncelikle kişisel verilerin korunması hakkını 8. maddesinde düzenleyen AB Temel Haklar Şartı ve maddenin içeriği ele alınacaktır. Devamında Adalet Divanı kararlarına konu olan ve Şart'ın 8. maddesini atıflayan bazı önemli içtihatlarla yer verilecektir. Ardından kişisel verilerin korunmasına özgülenmiş 95/46/AT Sayılı Direktif'te yer alan temel ilkeler, haklar ile sorumluluk rejimi incelenecek ve Adalet Divanı'nın Direktif'in maddelerine ilişkin içtihadi yorumları ortaya konacaktır. Veri Koruma Reformuna Götüren Diğer Düzenlemeler başlığı altında ise 97/66/AT Sayılı Telekomünikasyon Sektöründe Kişisel Verilerin İşlenmesi ve Özel Yaşamın Korunması Direktifi, Amsterdam Antlaşması Md. 286, 2002/58/EC Sayılı Elektronik İletişimde Kişisel Verilerin İşlenmesi ve Özel Yaşamın Korunması Direktifi, 45/2001 Sayılı Topluluk Kurum ve Organları tarafından Kişisel Verilerin İşlenmesi ve Verilerin Serbest Dolaşımı bakımından Bireylerin Korunması Direktifi, 2006/24/EC Sayılı İletişim Trafik Verilerinin Saklanması Direktifi ve Lizbon Antlaşması ele alınacaktır. Sonrasında ise Veri Koruma Reformu ve Reform'un odak noktası olan GVKT'nin içeriği ortaya konarak 95/46/AT Sayılı Direktif ile mukayesi yapılacaktır ve nihayetinde Reform öncesi ve sonrasında ulusal hukuk düzenlerinde gerçekleşen yeniliklerden bahsedilecektir.

A. AB TEMEL HAKLAR ŞARTI

Avrupa Birliği Temel Haklar Şartı, birlik nezdinde korunan temel hakları düzenleyen ve 2009 yılında Lizbon Antlaşması ile hukuken bağlayıcı olmuş bir metindir. Bu metinle AB alanındaki kişilerin sahip oldukları kişisel, siyasi, ekonomik ve sosyal haklar aynı düzenleme altında toplanmıştır. İlgili haklar altı farklı bölüm (saygınlık, özgürlükler, eşitlik, dayanışma, vatandaşların hakları, adalet) başlığı altında incelenmektedir. Daha detaylı biçimde ifade edilecek olursa, AB Adalet Divanı

³⁸⁸ DE HERT, GUTWIRTH, "Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalisation in Action", *Reinventing Data Protection*, s. 9.

içtihatlarında yer alan haklar, İHAS'ta düzenlenen haklar ve AB ülkelerinin ortak anayasal gelenekleri ile diğer uluslararası düzenlemelerde bulunan diğer hak ve ilkeler Şart'ın içeriğini oluşturmaktadır³⁸⁹.

AB Temel Haklar Şartı, AB hukuk rejiminde temel hakların kaynağı değildir. Bu haklar, AB Adalet Divanı tarafından temel alınan “insan haklarına saygı” ilkesinden yola çıkılarak türetilmiştir. Bu bakımdan Şart, yeni hakların yaratılması gibi bir misyon üstlenmemiş, aksine AB hukukunda varolan hakların yeniden ele alınması usulünü izlemiştir. Ayrıca Şart'da yer alan haklar arasında herhangi bir hiyerarşi mevcut değildir. Bu bakımdan bir hakkın diğerine üstünlüğü söz konusu olamaz ve çatışan haklar arasında dengeleme söz konusudur³⁹⁰. Ancak belirtilmelidir ki kişisel verilerin korunması hakkının tanınmasında olduğu gibi, şu ana dek en yenilikçi ve güncellenmiş insan hakları kataloglarından birini içermektedir. Bu bakımdan mahkemelerin yeni çıkan hukuki zorlukları ele almalarında referans alabilecekleri bir metin olarak değerlendirilmektedir³⁹¹.

1. Kapsam ve İçerik

Kişisel verilerin korunması hakkı, anılan Şart'ın 8. maddesinde düzenlenmektedir. Söz konusu maddenin temelini, 95/46/AT sayılı Direktif, 108 sayılı Sözleşme ve İHAS'ın 8. maddesi oluşturmaktadır. Fakat İHAS'tan farklı olarak Şart'ta kişisel verilerin korunması hakkı, özel yaşamın gizliliği hakkından ayrı düzenlenmiştir³⁹².

³⁸⁹ Paul CRAIG, Grainne DE BURCA, *EU Law- Text, Cases and Materials*, Oxford University Press, 2007, s. 14- 15; “Why do we need the Charter?”, European Commission, https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights/why-do-we-need-charter_en, E.T. 01.09.2018.

³⁹⁰ CRAIG, DE BURCA, *EU Law- Text, Cases and Materials*, s. 15; “Charter of Fundamental Rights of the EU Right by Right Analysis”, UK Government's Analysis- 05.12.2017, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/664891/05122017_Charter_Analysis_FINAL_VERSION.pdf, E.T. 01.09.2018.

³⁹¹ Federico FABBRINI, *The EU Charter of Fundamental Rights and the Rights to Data Privacy: The EU Court of Justice as a Human Right Court*, iCourts Working Paper Series, No: 19, 2015, s. 9.

³⁹² FABBRINI, *The EU Charter of Fundamental Rights and the Rights to Data Privacy: The EU Court of Justice as a Human Right Court*, s. 5- 7; “Why do we need the Charter?”, European Commission,

Bu düzenleme ile AK'nin 108 Sayılı Sözleşmesi ve AB'nin 95/46/AT Sayılı Direktif'i kıyaslandığında ayrıca görülmektedir ki kişisel verilerin korunması artık özel yaşamın korunması hakkı gibi temel hak ve özgürlüklerin bir parçası değil, onlardan bağımsız bir temel hak olarak ele alınmaktadır³⁹³.

'Kişisel verilerin korunması' ile ilgili 8. maddeye göre, *'Herkesin kendisiyle ilgili kişisel verilerin korunmasına hakkı vardır'*. İkinci paragrafta ise verilerin “belirli amaçlar için adil biçimde, ilgili kişinin rızasına ya da yasalarca belirlenmiş diğer meşru temellere dayanarak” işleneceğinden söz etmektedir. Buna göre kişisel verilerin korunması hakkı, 95/46/AT Sayılı Direktif'teki koşullar altında kullanılmakta ve Şart'ın 52. maddesinde belirtilen koşullar doğrultusunda sınırlandırılabilir³⁹⁴. Bu iki ayrı düzenlemeye başvurulması durumu ise, hakkın doğası ve içeriğindeki farklı unsurlar konusunda Direktif'teki hakkın uygulanmasına dair koşullar ile Şart'ın 52. maddesinde belirtilen sınırlandırılma koşulları bakımından sorunlara yol açabilecektir³⁹⁵.

Şart'ın anılan 8. maddesi, AB hukuku kapsamında ve veriye erişim hakkı olan bireylerce adil bir biçimde işlenmesini düzenlemektedir. Ayrıca bu maddeye göre veri koruma kurallarına uygunluğun bağımsız bir otorite tarafından kontrolü gerekmektedir³⁹⁶. Bu maddeye dair açıklamada ayrıca belirtilmektedir ki, bu madde Avrupa Topluluğu (Amsterdam) Antlaşması'nın 286. maddesi, 95/46/AT Sayılı Direktif, İHAS'ın 8. maddesi ve 108 Sayılı Sözleşme'ye dayanmaktadır. Açıklayıcı notlara göre,

https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights/why-do-we-need-charter_en , E.T. 01.09.2018.

³⁹³ DE HERT, GUTWIRTH, “Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action”, *Reinventing Data Protection*, s. 7.

³⁹⁴ Draft Charter of Fundamental Rights of the European Union, 11.10.2000, 4473/00, Convent 49, http://www.europarl.europa.eu/charter/pdf/04473_en.pdf , E.T. 21.01.2019.

³⁹⁵ FABBRINI, *The EU Charter of Fundamental Rights and the Rights to Data Privacy: The EU Court of Justice as a Human Right Court*, s. 5- 7, 14; HUSTINX, "EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation", https://edps.europa.eu/data-protection/our-work/publications/speeches-articles/eu-data-protection-law-review-directive_en , E.T. 04.11.2018.

³⁹⁶ “Charter of Fundamental Rights of the EU Right by Right Analysis”, UK Government's Analysis-05.12.2017, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/664891/05122017_Charter_Analysis_FINAL_VERSION.pdf , E.T. 01.09.2018.

Şart'ın 7. maddesinde güvence altına alınan haklar ise, İHAS'ın 8. maddesinde güvence altına alınan haklara karşılık gelir³⁹⁷. Bu noktada hem 7. hem de 8. maddeler, müdahalenin katı koşullara tabi olduğu klasik temel hakların tipik örnekleridir.

2. İlgili İçtihat

AB Temel Haklar Şartı, Adalet Divanı'nın içtihatlarında gün geçtikçe daha yoğun biçimde yer almakta ve önem taşımaktadır. Temel itibarıyla belirtilmelidir ki Divan, Temel Haklar Şartı'na dijital dünya ile etkileşime giren kişilerin veri gizliliğine ilişkin haklarının korunmasını önemli ölçüde genişleten yeni bir içtihat alanı oluşturmuştur.

Lizbon Anlaşması'nın yürürlüğe girmesinden birkaç ay sonra Divan, Şart'ta da konu edilen denetim otoritesinin tam bağımsız olması hususunda *Avrupa Komisyonu-Almanya Federal Cumhuriyeti* kararını vermiştir. Ulusal denetim otoritesinin tam bağımsız olmamasının hem Direktif'i ihlal ettiğine hem de Şart'ın 8. maddesinin gerekliliğine hükmetmiştir³⁹⁸. Ayrıca Almanya'nın Direktif'te yer alan bu “tam bağımsızlık” ifadesini iç hukukuna yanlış bir biçimde aktardığını belirterek AB hukukunun ihlal edildiğini de belirtmiştir. Devamındaki üç davada Divan, AB Temel Haklar Şartı md. 8/3 ve AB'nin İşleyişine Dair Anlaşma md. 16/2'den yola çıkarak bağımsız denetim şartının kişisel verilerin korunmasının temel şartı olduğunu belirtmiştir³⁹⁹.

³⁹⁷ Explanations relating to the Charter of Fundamental Rights of the European Union and Article 7, document CONVENT 49, http://www.europarl.europa.eu/charter/pdf/04473_en.pdf , 11.10.2000, E.T. 19.01.2019.

³⁹⁸ Case C-518/07 *European Commission v. Federal Republic of Germany*, 09.03.2010, <http://curia.europa.eu/juris/celex.jsf?celex=62007CJ0518&lang1=en&type=TEXT&ancre=> , E.T. 26.01.2019.

³⁹⁹ Case C-614/10, *European Commission v. Republic of Austria*, 16.10.2012, Par. 37, <https://eur-lex.europa.eu/legal-content/EN/TEXT/?uri=CELEX%3A62010CJ0614> , E.T. 06.11.2018; Case C-288/12, *European Commission v. Hungary*, 08 April 2014, Par. 48, <https://eur-lex.europa.eu/legal-content/EN/TEXT/?uri=CELEX%3A62012CJ0288> , E.T. 06.11.2018; *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, 08.04.2014, Par.

2010 yılında *Volker und Markus Schecke GbR ve Hartmut Eifert- Land Hessen* davasında olayın taraflarından biri, iletişim bilgilerinin ve aldıkları yıllık tarımsal yardımların miktarının bir internet sitesinde yayımlanmasına itiraz eden Alman çiftçiler olmuştur. Bu davada Divan, bu verilerin, belli yasal düzenlemeler çerçevesinde, bir sitede yayınlanmasının İHAS'ın 8. maddesi kapsamında kişisel verilerin korunması hakkına haksız bir müdahale oluşturduğuna karar vermiştir⁴⁰⁰. Ayrıca Adalet Divanı, Lizbon Anlaşması'nın ardından ilgili durumun AB Temel Haklar Şartı kapsamında da değerlendirilmesi gerektiğini dile getirmiştir. Bu bağlamda, Şart'ın 8. maddesinde ele alınan kişisel verilerin korunması hakkının 7. maddedeki özel hayata saygı hakkı ile doğrudan ilişkili olduğunu ve fakat mutlak bir hak teşkil etmediğini de vurgulamıştır. Dolayısıyla gerekli şartlar sağlandığı takdirde, kişisel veriler işlenebilecek ve Şart'ın 52/1. maddesi doğrultusunda hakka dair belli bazı sınırlamalar getirilebilecektir. Ancak Divan'a göre olay özelinde, bir internet sitesinde gelir verilerinin yayınlanması, Şart'ın 7. maddesi bağlamında özel hayata saygı hakkının ihlali anlamına gelmektedir. Ayrıca Divan, internet sitesinde bu bilgilerin yayınlanması sebebiyle, Şart'ın 8/2. maddesi bağlamında kişisel verilerin işlenmesi ve çiftçilerin bu yayına rıza vermemeleri gerekçeleriyle kişisel verilerin korunması hakkına müdahale oluşturduğuna belirtmiştir. Çiftçilere dair isim ve gelir verilerinin bir internet sitesinde yayınlanması düzenlemesine bakıldığında, Divan kanun koyucunun daha az müdahaleci bir alternatif düşündüğüne ikna olmamıştır. Bu durum orantılılık ilkesini aşmıştır⁴⁰¹.

Daha kapsamlı ve açık bir Divan kararı ise, pasaportlardaki parmak izlerinin depolanmasıyla ilgili 2013 yılındaki *Michael Schwarz- Stadt Bochum* kararıdır. Anılan olayda bir Alman vatandaşı, pasaport başvurularında parmak izlerinin alınmasına dair

68, <http://curia.europa.eu/juris/celex.jsf?celex=62012CJ0293&lang1=en&type=TEXT&ancre=> , Erişim Tarih: 27.01.2019.

⁴⁰⁰ Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen*, 09.11.2010, Par. 30- 44, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62009CJ0092> , E.T. 28.01.2019.

⁴⁰¹ Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen*, 09.11.2010, Par. 45- 52, 60, 64, 86, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62009CJ0092> , E.T. 28.01.2019.

yasal bir düzenlemeye itiraz etmiştir. Başvurucu bu durumun, Şart'ın 7. maddesinde düzenlenen özel yaşama saygı hakkı ile 8. maddede düzenlenen kişisel verilerin korunması haklarına aykırı olduğunu belirtmiştir. Divan da bir kişinin parmak izlerinin alınması ve bu parmak izlerinin pasaportta saklanmasıyla özel yaşama saygı ve kişisel verilerin korunması haklarına bir tehdit oluşturduğunu belirtmiştir. Açıktır ki, pasaport başvurusunda bulunan herkes, parmak izi verme işlemine rıza göstermek zorunda bırakılmıştır; ancak bu tür yolculuklar yapmak isteyen Birlik vatandaşları parmak izlerinin işlenmesine itiraz etmekte özgür değildirler. Şart'ın 8. maddesinde düzenlenen hak mutlak bir hak da olmadığından kanunla belirlenmiş meşru bir amaçla sınırlanabilecektir. Fakat Divan'a göre bu durumda özel yaşam ve kişisel verilerin korunmasının toplumdaki işlevleri ile ilgili olarak da düşünülmesi gerektiği akıldan çıkarılmamalıdır. Söz konusu davada parmak izi alınmasının hakkın özüne ilişkin bir müdahale oluşturduğuna dair ortaya herhangi bir delil konulamadığının da altı çizilmiştir. Tüm bu sebeplerle Divan pasaport başvurularında parmak izlerinin alınması uygulamasını içeren Yönetmelik'in Şart'ın 8. maddesinin ihlali sonucunu doğurmadığına hükmetmiştir⁴⁰².

Böylelikle gerek *Volker und Markus Schecke GbR ve Hartmut Eifert- Land Hessen* davasında, gerekse *Michael Schwarz- Stadt Bochum* kararında Divan, Şart'ın 8. maddesinde düzenlenen kişisel verilerin korunması hakkının mutlak bir hak teşkil etmediğinden bahisle belli şartlar dahilinde sınırlanabileceğine hükmetmiştir.

Kolluk amaçlı olarak iletişim verilerinin kayıt altına alınmasına ilişkin bir birleşik dava olan 8 Nisan 2014 tarihli *Digital Rights Ireland Ltd- İletişim, Denizcilik ve Doğal Kaynaklar Bakanlığı ve Diğerleri ile Kärntner Landesregierung ve Diğerleri* kararında ise Divan, 2006/24/EC Sayılı İletişim Trafik Verilerinin Saklanması Direktifi'n, Şart'ın 7. ve 8. maddeleri bağlamında incelemiştir. 2006/24/EC Sayılı Direktif'in "Ceza Adaleti (Terör Suçları)" başlıklı 7. Bölümü'nde yer alan düzenlemeye göre telefon iletişimi servis

⁴⁰² Case C-291/12 *Michael Schwarz v Stadt Bochum*, 17.10.2013, Par. 12, 29- 30, 32- 33, 39, 63- 66, <http://curia.europa.eu/juris/celex.jsf?celex=62012CJ0291&lang1=en&type=TEXT&ancre=> , E.T. 31.01.2019.

sağlayıcıları, suçu önlemek, tespit etmek, soruşturmak, kovuşturmak ve Devlet'in güvenliğini korumak amaçlarıyla kanunların öngördüğü bir süre boyunca bu sağlayıcılarla ilgili trafik ve konum verilerini tutmak zorundadır. Bu olayda Divan'ın Büyük Dairesi, Direktif aracılığı ile elde edilen verilerin uzun süre tutulabileceği ve sonrasında emniyet güçleri tarafından kullanılmalarının muhtemel olduğunu belirterek kişiler üzerinde sürekli gözetleniyorlarmış hissi yaratabileceğini belirtmiştir⁴⁰³. Direktif her ne kadar iletişimin içeriğinin kayıt altına alınmasına izin vermiyorsa da Divan'a göre özel yaşamı doğrudan ve spesifik olarak etkilemekte ve bu nedenle Şart'ın özel yaşama dair 7. maddesini ihlal etmektedir. Divan bu kararda 7. maddeye daha fazla odaklanmıştır. Ayrıca kişisel verilerin saklanması da veri işlenmesi olduğu için, Şart'ın 8. maddesi ile güvence altına alınan kişisel verilerin korunması temel hakkına da müdahale etmektedir. Bu bakımdan Divan'a göre söz konusu maddedeki veri koruma gerekliliklerini de karşılamalıdır; fakat kanunla belirlenmiş meşru bir temelden yoksundur⁴⁰⁴. Divan, Şart'ın 8/3. maddesi ve AB'nin İşleyişine Dair Anlaşma'nın 16/2. maddesinden yola çıkarak bağımsız denetim şartının kişisel verilerin korunmasının temel şartı olduğunu ve fakat Şart'ın 8/3. maddesinin bu temel şartın anılan davalar bakımından yerine getirilmediğini de üstü kapalı bir biçimde belirtmiştir⁴⁰⁵.

Yakın tarihli bir karar olan *Patrick Breyer- Bundesrepublik Deutschland* davasında ise Divan, kişisel veri kavramını günümüz teknolojik gelişmeleri doğrultusunda ele almış ve "dinamik" IP adreslerini de kişisel veri olarak kabul etmiştir. Anılan karara göre, internete her yeniden bağlanıldığında yeni bir IP adresi verilmek

⁴⁰³ Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, 08.04.2014, Par. 37, <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A62012CJ0293> , E.T. 31.01.2019.

⁴⁰⁴ Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, 08.04.2014, Par. 28- 29, 35-36, <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A62012CJ0293> , E.T. 05.02.2019.

⁴⁰⁵ Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, 08.04.2014, Par. 68-69, <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A62012CJ0293> , E.T. 05.02.2019.

suretiyle sürekli deęişiklik gösteren IP adresi anlamına gelen dinamik IP, kişiyi belirlenebilir kılabilceęi için kişisel veri olarak kabul edilmiştir⁴⁰⁶.

Lizbon Anlaşması ile bağlayıcı hale gelen Şart, kendinden önceki düzenlemelerden farklı olarak 8. maddesinde tanınan kişisel verilerin korunması hakkını anayasal düzeyde bağımsız bir temel hak olarak ele almaktadır. Oysa 108 Sayılı Sözleşme ve birazdan ele alınacak olan 95/46/AT Sayılı Direktif kişisel verilerin korunmasını mevcut temel hakların bir parçası olarak ele almıştır. Fakat Divan söz konusu Şart'ı henüz yeterince etkili bir biçimde kullanamamaktadır.

Yukarıda anılan davalarda görülmüştür ki Divan, Şart'ın 8. maddesinin gerçek işlevini ortaya koymaya çalışmış, ancak hala bu maddenin rolünü net bir şekilde aydınlatamamıştır. Örneğin *Volker und Markus Schecke GbR ve Hartmut Eifert- Land Hessen* davasını öncelikle İHAS'ın 8. maddesi bakımından değerlendirmiş olması şaşırtıcıdır. Bu tespitin ardından internet sitesinde davaya konu olan bilgilerin yayınlanması sebebiyle, Şart'ın 8/2. maddesi bağlamında kişisel verilerin işlenmesi ve veri öznelerinin bu yayına rıza vermemeleri gerekçeleriyle kişisel verilerin korunması hakkına müdahale oluşturduğunu da eklemiştir. Ancak burada her ne kadar Şart ışığında bir değerlendirme yapsa da tıpkı İHAM içtihatlarındaki gibi orantılılık değerlendirmesi yaparak bu ilkenin aşıldığına hükmetmiştir.

Sonrasında ele alınan *Digital Rights Ireland Ltd- İletişim, Denizcilik ve Doğal Kaynaklar Bakanlığı ve Diğerleri ile Kärntner Landesregierung ve Diğerleri* birleşik davasında ise kolluk amaçlı olarak iletişim verilerinin kayıt altına alınması hususunu esas olarak Şart'ın 7. maddesinde düzenlenen özel yaşamın korunması bakımından değerlendirmiş olması da 8. maddede yer alan kişisel verilerin korunması hakkına tam bir yönelimi henüz gerçekleştirmediğine ilişkin yorumlanabilecektir.

⁴⁰⁶ Case C-582/14, *Patrick Breyer v Bundesrepublik Deutschland*, 19.10.2019, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0582>, E.T. 04.02.2019.

Aşağıda görüleceği üzere 95/46/AT Sayılı Direktif veri koruma meselesini hem verinin ekonomik boyutu ile hem de temel hakların korunması boyutu ile ele almıştır. Fakat ekonomik bakış açısı uygulamada ağır basmıştır⁴⁰⁷. Şart'ın veri koruma hakkını bağımsız bir hak olarak tanıması, Direktif'in temel haklar boyutuna vurgu yaparak bunu düzeltmenin bir yolu olarak görülebilir. Ayrıca doktrinde Şart'ta açık bir biçimde tanınan bu hakla İHAM içtihadında cevaplanamayan sorunların çözülebileceğine dair görüşler de bulunmaktadır⁴⁰⁸. Bunun dışında Şart'ın yenilikçi ve Lizbon Anlaşması sonrası bağlayıcı dili, Adalet Divanı'nın kişisel verilerin korunması bağlamında önünü açabilecek nitelikte olarak değerlendirilmektedir⁴⁰⁹. Tüm bu içtihadi değerlendirmelerin sonucunda görülmektedir ki, kişisel verilerin korunması hakkına dair hukuki düzenlemeler yeterli olsa da yargısal mekanizmalar bu hakkı yeterli düzeyde veri korumasının sağlanması için etkili biçimde analiz edememektedir. Elbette ki veri koruma ve mahremiyet- özel yaşam arasındaki ilişki hem İHAM hem Adalet Divanı'nın belirttiği üzere, oldukça açıktır; ancak günümüzde veri korumasını yalnızca mahremiyet- özel yaşam çerçevesinden değerlendirmek de hakkın bağımsız niteliğine zarar vermektedir. İyimser bir bakış açısı ile Adalet Divanı'nın gelişmeci anlayışının giderek çok daha baskın hale geleceği ve kişisel verilerin korunması hakkının Şart'ta düzenlenmiş bağımsız ve temel bir hak statüsü ile ele alınacağı çok daha derinlikli kararlara imza atılacağı düşünülmektedir.

B. 95/ 46/ AT SAYILI KİŞİSEL VERİLERİN İŞLENMESİ VE SERBEST DOLAŞIMI BAKIMINDAN BİREYLERİN KORUNMASINA İLİŞKİN AVRUPA PARLAMENTOSU VE AVRUPA KONSEYİ DİREKTİFİ

Avrupa Konseyi, “veri koruma” kavramının gündeme getirilmesinde ve yasal çerçevenin oturmasında oldukça başarılı olmuştur. Ancak 108 Sayılı Sözleşme'nin

⁴⁰⁷ Commission of the European Communities, *First Report on the implementation of the Data Protection Directive (95/46/EC)*, COM (2003) 265, Brussels, 15.05.2003, http://eur-lex.europa.eu/LexUriServ/site/en/com/2003/com2003_0265en01.pdf, E.T. 01.06.2019.

⁴⁰⁸ DE HERT, GUTWIRTH, “Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action”, s. 9.

⁴⁰⁹ FABBRINI, *The EU Charter of Fundamental Rights and the Rights to Data Privacy: The EU Court of Justice as a Human Right Court*, s. 18.

uygulanması bakımından bazı üye ülkeler başarılı olamamış ve Sözleşme'yi geç uygulamışlardır⁴¹⁰.

1995 tarihli AB Veri Koruma Direktifi, Nisan 2016'da AB Konseyi ve Avrupa Parlamentosu tarafından kabul edilen Genel Veri Koruma Tüzüğü'nün 25 Mayıs 2018'de doğrudan uygulanmaya başlamasına dek, kişisel verilerin işlenmesini Avrupa sathında düzenleyen temel hukuki metin olmuştur. Bu bakımdan denilebilir ki, veri koruma hukukunun gelişim sürecinde, Genel Veri Koruma Tüzüğü'nden sonra en temel ikinci metindir. Söz konusu metin, 27 AB üye ülkesi ve hatta İzlanda, Lihtenştayn ve Norveç'i de kapsayan Avrupa Ekonomik Alanı'nda uygulanmıştır⁴¹¹.

95/ 46/ AT Sayılı Direktif, 24 Ekim 1995 tarihinde AB'nin uyum, entegrasyon ve Avrupa iç pazarını kurma saiklerinin bir yansıması olarak, özel ve kamu sektörlerinde veri korumasını gerçekleştirmek için kabul edilmiştir⁴¹². Anılan dönemde üye ülkelerin ulusal hukuk düzlemlerinde kendi veri koruma kanun ve düzenlemeleri bulunmaktaydı. İşte bu üye devletlerin ulusal mevzuat çeşitliliği ve konunun Avrupa Topluluğu düzleminde yeknesak bir koruma sistemine sahip olmayışı, veri öznelerinin temel bir hakkı olan özel yaşam haklarını zedeleyen ve sınırötesi veri akışını engelleyebilen bir durum oluşturmaktaydı. Malların, sermayenin, hizmetlerin ve insanların serbest dolaşımı, verinin de serbest dolaşımını elzem hale getirmekteydi⁴¹³. Veri koruma konusuna dair ulusal düzenlemelerdeki bu çeşitlilik ayrıca, tek elden bir direktif düzenlenmesi

⁴¹⁰ HUSTINX, "EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation", s. 9, https://edps.europa.eu/data-protection/our-work/publications/speeches-articles/eu-data-protection-law-review-directive_en, E.T. 04.11.2018.

⁴¹¹ GALETTA, DE HERT, "A European Perspective on Data Protection and Access Rights", <http://irissproject.eu/wp-content/uploads/2014/06/European-level-legal-analysis-Final1.pdf>, E.T. 03.09.2018.

⁴¹² Commission of the European Communities Communication on the Protection of Individuals in relation to the Processing of Personal Data in the Community and Information Security (COM) (90) 314 final- SYN 287&288, 13 Eylül 1990, s.4, <http://aei.pitt.edu/3768/1/3768.pdf>, E.T. 04.11.2018.

⁴¹³ *Handbook on the European Data Protection Law*, 2018, European Union Agency for Fundamental Rights and Council of Europe, s. 29.

hususunda katalizör görevi görmüştür⁴¹⁴. Üye devletlerin belirli bir hedefe ulaşmalarını gerektiren ancak her üye ülkenin bu hedefe nasıl ulaşacağına ilişkin belirlediği aynı kuralları, kendi kanunları ile uygulamalarına izin veren bu Direktif, AB genelinde 28 tane veri koruma kanununun düzenlenmesine temel oluşturmuştur⁴¹⁵. Her ne kadar kişisel verinin işlenmesi bakımından ortak veri koruma kuralları Direktif’in temel gayelerinden olsa da bürokratik birimler ve özel işletmelerin veri toplama, saklama ve analiz edebilmeleri için ihtiyaçları da önemli gerekçeler arasındadır⁴¹⁶.

Veri korumanın temel hakların korunması ile doğrudan bağlantısı olması sebebiyle Direktif’in bir amacı, özel yaşam ve bağlantılı temel hakların üst düzeyde korunmasıdır. Bu bakımdan Direktif, İngilizce’de olan “*privacy- mahremiyet*” kavramını “*respect for private life- özel yaşama saygı*” kavramının mümkün olan en yakın eşanlamlısı olarak kullanmaktadır⁴¹⁷. Diğer önemli amacı ise, üye ülkeler arası kişisel verilerin serbestçe dolaşımının sağlanması önündeki engellerin kaldırılmasıdır⁴¹⁸. Direktif’in başlığına da bakılacak olursa metnin amacının, veri öznesinin temel haklarının korunması ile verinin bir üye ülkeden diğer bir üye ülkeye serbestçe dolaşımını aynı anda sağlamak ve bu esnada İHAM’ın 8 ve 10. maddelerine uygun hareket etmek olduğu görülecektir⁴¹⁹.

⁴¹⁴ Sian RUDGARD, “Origins and Historical Context of Data Protection Law”, *European Privacy*, International Association of Privacy Professionals (IAPP), 2012, https://iapp.org/media/pdf/publications/European_Privacy_Chapter_One.pdf, E.T. 20.09.2018.

⁴¹⁵ Kyle PETERSEN, “GDPR: What (and Why) You Need to Know about EU Data Protection Law”, *UTAH Bar Journal*, Vol. 31, No:4, s. 12, ss. 12- 16.

⁴¹⁶ GALETTA, DE HERT, “A European Perspective on Data Protection and Access Rights”, <http://irissproject.eu/wp-content/uploads/2014/06/European-level-legal-analysis-Final1.pdf>, E.T. 03.09.2018.

⁴¹⁷ FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, s. 131.

⁴¹⁸ HUSTINX, “EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation”, s. 9, https://edps.europa.eu/data-protection/our-work/publications/speeches-articles/eu-data-protection-law-review-directive_en, E.T. 04.11.2018; FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, s. 125.

⁴¹⁹ RUDGARD, “Origins and Historical Context of Data Protection Law”, https://iapp.org/media/pdf/publications/European_Privacy_Chapter_One.pdf, E.T. 20.09.2018.

Söz konusu Direktif'in başlığına bakıldığında önemli bir husus daha göze çarpmaktadır. Buna göre Direktif, "veri koruma" ya da "kişisel verilerin korunması"nı değil; "kişisel verilerin işlenmesi bakımından bireylerin korunması"nı esas almaktadır. Daha açık bir deyişle Direktif, veriyi ya da kişisel veriyi korumayı değil; gerçek kişinin temel hak ve özgürlüklerini ve özellikle özel yaşam hakkını kişisel verinin işlenmesi bağlamında korumayı tanımlamıştır. Ayrıca 1. maddesinde üye ülkeler arasında kişisel verilerin serbestçe dolaşımı bakımından tüm sınırlamaları da yasaklamaktadır. İşte bu, "özel yaşamın korunması" ve "kişisel verinin sınırötesi akışı" temel gayeleri köklerini 1980 tarihli OECD Rehber İlkeleri'nde bulmaktadır⁴²⁰. O zamandan beri bu iki gayenin dengelenmesi arayışı, veri koruma belgelerinin temel özelliğini oluşturmaktadır.

1. Kapsam ve İçerik

95/46/AT Sayılı Direktif oldukça geniş kapsamlı bir metindir. Bu bağlamda 3/1. maddesine göre, dosyalama sisteminin parçasını oluşturması istenen veya bir dosyalama sisteminin parçasını oluşturan kişisel verilerin otomatik araçlar dışında işlenmesine veya kişisel verilerin otomatik yollarla kısmen ya da tamamen işlenmesine uygulanmaktaydı. Özellikle özel sektör bakımından faaliyetler genel itibarıyla Direktif'in koruma alanına girmektedir. Direktif'in kapsamı 3. madde ile ortaya konmakta idi. Bu maddenin ikinci fıkrasına göre bazı alanlardaki kişisel verilerin işlenmesi Direktif'in kapsamı dışındaydı. Öncelikle Direktif,

"ceza hukuku alanındaki Devlet faaliyetleri ve devlet güvenliği, savunma, kamu güvenliğine ilişkin verilerin işlenmesi için herhangi bir durumda ve Avrupa Birliği Anlaşmasının V. ve VI. Başlıklarında belirtilenler gibi, topluluk hukuku kapsamının dışına düşen bir faaliyet esnasındaki"

kişisel verilerin işlenmesine uygulanmamıştır. Ancak söz konusu metnin bir Direktif olması sebebiyle bazı üye ülkeler bu alanları da veri koruma hukukuna hâkim temel ilkeler

⁴²⁰ FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, s. 130.

kapsamında koruma altına almıştır⁴²¹. Direktif’in kapsamı dışında kalan bir diğer alan da “bir gerçek kişi tarafından, tamamen kişisel veya ev içi faaliyeti esnasında”ki kişisel verilerdir.

95/46/ AT Sayılı Direktif, başta özel yaşam olmak üzere, gerçek kişilerin temel hak ve özgürlüklerinin korunmasını temel amaçlarından biri olarak ortaya koymaktadır. Bu doğrultuda içeriğinde yer alan esaslar bağlamında söz konusu amacı gerçekleştirirken, 108 Sayılı Sözleşme’de bulunan ilkeleri de bir adım ileri taşıyarak güçlendirir ve genişletir. İlaveten Başlangıç’ta da belirtildiği üzere, üye ülkeler arasında kişisel verilerin serbestçe dolaşımı için iç pazar kurularak ekonomik ve sosyal entegrasyonun sağlanması da bir diğer önemli amaçtır. Direktif ayrıca 108 Sayılı Sözleşme’den ileri gelen “veri koruması özel yaşamın gizliliğini sağlar.” ilkesini ve dolaylı bir biçimde OECD Rehber İlkeri’nden verinin serbest dolaşımı ile bireylerin korunmasını dengelemek gerektiği fikrini de benimsemiştir⁴²².

Direktif’in 2. maddesine göre kişisel veri,

*“tanımlanmış veya tanımlanabilir bir gerçek kişiyle ilgili herhangi bir bilgi ('veri öznesi') anlamına gelir; tanımlanabilir bir kişi, doğrudan veya dolaylı olarak, özellikle bir kimlik numarasına veya fiziksel, fizyolojik, zihinsel, ekonomik, kültürel veya sosyal kimliğine özgü bir veya daha fazla faktöre referansla tanımlanabilen bir kişidir”*dir.

Bu tanımın kapsamına bakıldığında, 108 Sayılı Sözleşme’ye göre daha dar bir düzenleme olduğu görülecektir; çünkü 108 Sayılı Sözleşme’nin 3/2. maddesine göre Sözleşme,

“topluluklar, dernekler, vakıflar, şirketler, kurumlar ve tüzel kişiliğe sahip olsun veya olmasın, doğrudan veya dolaylı olarak gerçek kişilerin bir araya gelmesiyle oluşmuş her çeşit diğer kuruluş hakkında da”

⁴²¹ Clemens ARZT, “Data Protection Versus Fourth Amendment Privacy: A New Approach Towards Police Search and Seizure”, *Criminal Law Forum*, Vol. 16 (3-4), Y. 2005, s.194, ss. 183- 230.

⁴²² FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, s. 156.

uygulanabilmektedir.

Direktif'in uygulama alanını daraltan düzenlemeler böyle olmakla birlikte, Direktif'in temel ilkeleri, 1980 tarihli OECD İlkeleri ve büyük ölçüde 108 Sayılı Sözleşme'nin temel prensiplerini içermektedir⁴²³. Direktif veri işlemeyi;

“silme veya tahrip etme, engelleme, birleştirme veya sıralama, sağlama ya da dağıtma, iletmeye açıklama, toplama, kaydetme, organizasyon, depolama, adaptasyon veya değiştirme, kurtarma, danışma gibi otomatik ya da otomatik olmayan araçlarla kişisel veriler üzerinde yapılan herhangi bir faaliyet veya faaliyet dizisi”

olarak açıklamıştır. Görüleceği üzere, kişisel verilerin işlenmesi, uzun ve birçok işlemi bünyesinde barındırır bir süreçtir⁴²⁴. Ayrıca Sözleşme'de belirtilmeyen ancak Direktif'de düzenlenen, meşru bir biçimde veri işlemenin altı kriteri bulunmaktadır. Buna göre⁴²⁵;

1. Verinin işlenmesi için veri öznesi, açık ve kesin bir biçimde rızasını vermiş olmalıdır⁴²⁶. Ya da;
2. Verinin işlenmesi, veri öznesinin taraf olduğu bir sözleşmenin yerine getirilmesi için gerekli olduğunda veya bir sözleşme yapmadan önce veri öznesinin talebi varsa önlem almak için gerçekleştirilebilir. Ya da;
3. Verinin işlenmesi, denetleyicinin özne olarak bulunduğu yasal bir yükümlülük mevcutsa söz konusu olabilir. Ya da;

⁴²³ GALETTA, DE HERT, “A European Perspective on Data Protection and Access Rights”, <http://irissproject.eu/wp-content/uploads/2014/06/European-level-legal-analysis-Final1.pdf>, E.T. 03.09.2018.

⁴²⁴ Hayrunnisa ÖZDEMİR, “Haberleşmenin Gizliliği ve Kişisel Veriler”, *Erzincan Üniversitesi Hukuk Fakültesi Dergisi*, C. XIII, S. 1-2, Y. 2009, s. 291, ss. 285- 303.

⁴²⁵ Directive 95/ 46/ EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046>, E.T. 12.09.2018.

⁴²⁶ 95/ 46/ AT Sayılı Direktif, hangi koşullarda açık rızanın olduğuna dair bir düzenleme içermemektedir. Avrupa Veri Koruma Otoritesi'ne göre açık rıza mutlaka serbestçe verilene spesifik olan ve verilip verilmediğine dair herhangi bir şüphe barındırmayan rızadır. European Data Protection Supervisor, *Guidelines on the processing of personal data with regard to the management of conflicts of interest in EU institutions and bodies*, 08.12.2014, s.15, https://edps.europa.eu/sites/edp/files/publication/14-12-08_coi_guidelines_en.pdf, E.T. 13.09.2018.

4. Verinin işlenmesi, veri öznesinin hayati menfaatlerinin⁴²⁷ korunması için gerekliyse gerçekleştirilebilir. Ya da;
5. Verinin işlenmesi, kamu menfaatinin mevcut bulunduğu bir görevin ifası için veya verinin açıklandığı 3. bir şahıs veya denetleyiciye yetki veren bir kamu otoritesinin işleminin gerçekleşmesi için gerekiyorsa söz konusu olabilir. Son olarak;
6. Verinin işlenmesi, veri öznesinin temel hak ve hürriyetlerine dair menfaatler ile çatışma olmadıkça, denetleyici veya verinin açıklandığı 3. bir kişi/ kişilerin hukuki menfaatleri için gerekli olduğunda gerçekleştirilebilir.

Direktif'in 8. maddesi de kapsam belirtmesi bakımından, hassas verilerin korunmasına ilişkin özel bir düzenleme içermektedir. Bu bağlamda maddenin ilk fıkrasında sağlık durumu veya cinsel yaşama ilişkin verilerin işlenmesi ve sendika üyeliği, dini veya felsefi inançlar, siyasi görüş, ırk veya etnik köken açıklayan kişisel verilerin işlenmesinin üye devletlerce yasaklanabileceği ortaya konulmaktadır. Ayrıca aynı maddenin beşinci fıkrasına göre, suçlar, adli hükümler veya güvenlik tedbirlerine ilişkin verilerin işlenmesi özel önlemlere tabi kılınabilecektir. Görüldüğü gibi Direktif, hassas verileri oldukça geniş tutmuştur. Buna karşın bazı üye ülkeler hassas veri kavramını daha da geniş bir biçimde ele almaktadır. Söz gelimi, Polonya ve Estonya'da "genetik bilgiler", İzlanda'da "ten rengi, alkol- ilaç- uyuşturucu kullanımı", İtalya'da "dernek üyeliği", Estonya'da ayrıca "engellilik durumu"na dair veriler hassas veri kabul edilmektedir⁴²⁸.

İlerleyen hükümlerde (16- 18. maddeler) ise, veri işlemenin gizliliği ve güvenliğinin ne şekilde sağlanabileceği ile işlemenin denetlenmesinin şartları ele alınmaktadır. Yine Direktif'in 13. maddesinde veri işleme konusuna getirilen muafiyet

⁴²⁷ Direktif'in Başlangıç metnine bakıldığında, veri öznesinin hayatı için korunması gereken bir çıkarının olması gerektiği ifade edilmektedir. Dolayısıyla bu durum yalnızca ölüm kalım durumları bakımından geçerli olacaktır. Peter CAREY, *Data Protection: A Practical Guide to UK and EU Law*, Oxford University Press, 2004, s. 19.

⁴²⁸ Cemil KAYA, "Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi", *İÜHFİM*, C. LXIX, S. 1-2, Y. 2011, s. 319, ss. 317- 334.

ve sınırlamalar düzenlenmektedir. Buna göre üye devletler, ulusal güvenlik, savunma, kamu güvenliği, suçların önlenmesi, AB'nin veya üye devletin ekonomik menfaati veya hak ve özgürlükler ile veri öznesinin korunması gibi sebeplerle hak ve yükümlülükleri sınırlandırabileceklerdir. Ayrıca bilimsel araştırma amacıyla da bazı sınırlamalar yapılabilecektir.

Direktifin bölgesel kapsamı ise 4. maddede ortaya konmaktadır. Buna göre Direktif, bir AB üyesi devletin topraklarında kurulmuş denetleyicinin faaliyetleri bağlamında yürütülen kişisel verilerin işlenmesi için geçerlidir. Bu bakımdan verilerin işlendiği yere bakılmamaktadır. Denetleyicinin AB alanında kurulmadığı hallerde ise, işleme için kullanılan araçların bulunduğu üye devletin kanunu dikkate alınacaktır⁴²⁹.

Belirtildiği üzere 95/ 46/ AT Sayılı Direktif, o dönemde ulusal hukuk düzenlerinde var olan veri koruma ilkeleri ile 108 Sayılı Sözleşme'deki kuralları daha genişleterek uygulamaktadır. Bu bağlamda, her üye ülkenin en az bir "tümüyle bağımsız" denetim otoritesi kurması gereği, Avrupa veri koruma hukukuna etkili ve önemli bir katkı sağlamıştır. Söz konusu denetim otoritesi, Direktif'in ulusal hukuka nasıl uygulandığına bağlı olarak, önceden kontrol veya danışma, şikâyetin ele alınması, denetimler ve diğer yaptırım faaliyetlerini gerçekleştirebilir⁴³⁰. Ayrıca Direktif, Avrupa sathında detaylı ve kapsayıcı bir veri koruma sistemi kurmuş⁴³¹ ve üye ülkeler bakımından kişisel verilerin serbest dolaşımını tanımıştır. Bu bakımdan Direktif'in 1/2. maddesine göre kişisel verinin bir üye ülkeden diğerine serbestçe taşınmasını sağlamak gereklidir. Üye devletlerdeki bağımsız denetim otoriteleri dışında Direktif 29. maddesi ile, kişisel verilerin işlenmesine dair bireylerin korunması hakkında bir "Çalışma Grubu" kurulmuştur. Direktif'in ilgili maddelerine göre (28 ile 30. maddeler) bu grup, danışma statüsünde olup Avrupa

⁴²⁹ Article 29 Working Party, Opinion 8/2010 on Applicable Law, 16 December 2010 (WP 179), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp179_en.pdf , E.T. 05.11.2018.

⁴³⁰ HUSTINX, "EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation", s. 11, https://edps.europa.eu/data-protection/our-work/publications/speeches-articles/eu-data-protection-law-review-directive_en , E.T. 04.11.2018.

⁴³¹ *Handbook on the European Data Protection Law*, 2018 Ed., European Union Agency for Fundamental Rights and Council of Europe, s. 29.

Komisyonu'ndan bir temsilci ile üye devletlerin bağımsız denetim otoritelerinin temsilcilerinden oluşmaktadır.

95/ 46/ AT Sayılı Direktif'in üç temel özelliği bulunmaktadır. Bunlardan ilkinde göre, Direktif kural koyarken ve kurallara istisna düzenlerken ihtiyatlı bir bakış açısı izlemektedir. Bunun sebebi de özel yaşam ve temel haklar ile verinin serbest dolaşımı arasında hakkaniyetli bir dengeye ulaşmaktır. Direktif'in ikinci özelliği ise, veri öznesi ile veri işleme denetleyicisinin hakları ve karşılıklı pozisyonlarını tanımlayarak aralarındaki ilişkiye vurgu yapmasıdır. Üçüncü ve son olarak ise Direktif, üye devletlere maddelerin etkili bir biçimde uygulanması konusunda son sözü söylemeleri için belli bir manevra alanı tanımaktadır⁴³².

Görüleceği üzere, 95/ 46/ AT Sayılı Direktif'in kişisel verilerin korunmasının temel bir hak olarak tanınmasında yeri çok büyüktür⁴³³. Fakat Avrupa nezdinde esas öncü düzenlemeler, OECD'nin 1980 tarihli “*Özel Yaşamın Gizliliğinin ve Sınır Ötesi Kişisel Veri Dolaşımının Korunmasına İlişkin Rehber İlkeler*”i ile Avrupa Konseyi'nin 1981 tarihli ve 108 sayılı “*Kişisel Verilerin Otomatik Olarak İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşme*”sidir. Bu düzenlemelerin ardından kişisel verilerin korunması hakkının gelişimi AB Adalet Divanı ve İHAM'ın içtihatları ile olmuştur. Fakat bunlardan farklı olarak AB Temel Haklar Şartı'nın ortaya çıkması ile kişisel verilerin korunması hakkı açık biçimde bir metinde tanınarak yerini daha sağlamlaştırmıştır⁴³⁴.

⁴³² GALETTA, DE HERT, “A European Perspective on Data Protection and Access Rights”, <http://irissproject.eu/wp-content/uploads/2014/06/European-level-legal-analysis-Final1.pdf>, E.T. 03.09.2018.

⁴³³ Gloria Gonzales FUSTER, Raphael GELLERT, “The Fundamental Right of Data Protection in the European Union: In Search of an Unchartered Right”, *Review of Law, Computers & Technology*, Vol. 26, No: 1, 2012, s. 74- 75, ss. 73- 82.

⁴³⁴ GALETTA, DE HERT, “A European Perspective on Data Protection and Access Rights”, <http://irissproject.eu/wp-content/uploads/2014/06/European-level-legal-analysis-Final1.pdf>, E.T. 03.09.2018.

AB hukuk sisteminde direktifler, doğrudan ulusal hukuk düzenine entegre olmazlar. Bunun için direktifin, üye devlet tarafından kendi iç hukuk düzenine aktarılması gerekmektedir. Bu aktarım yapılırken ise üye devlet, direktif hükümleri üzerinde takdir hakkına sahiptir. Hal böyle olunca 95/ 46/ AT Sayılı Direktif özelinde konulan temel kurallar üye devletler bağlamında homojenize bir biçimde iç hukuk sistemlerine taşınamamıştır. Ayrıca Direktif, genel olarak formüle edilmiş kavramları ve açık standartları benimsemiştir⁴³⁵. Ulusal hukuk sistemlerince tanımlar ve kurallar birbirinden farklı algılanmış ve bu sebeple Avrupa genelinde oldukça çeşitli bir veri koruma düzeni ortaya çıkmıştır. 1990’lardan günümüze dek bilgi teknolojilerinde yaşanan olağanüstü hızlı gelişmeler bir yandan insan hayatını kolaylaştırıcı yararlar sağlarken, diğer taraftan veri işleme, depolama, aktarım vb. gibi hususlarda daha önce akla gelmeyen ve insan onurunu tehlikeye atabilecek riskleri de getirmiştir⁴³⁶. Bu iki temel durum ise, 95/46/AT Sayılı Direktif’in yenilenmek zorunda olduğu gerçeğini doğurmuştur⁴³⁷.

Açıktır ki veri koruma konusu, yalnızca AB kapsamında üye ülkeleri belirli kurallarla yaptırım altına almakla gerçekleştirilemez. AB alanı dışındaki veri korumada da belirli bir standart sağlanmazsa, veri koruma ilkelerinden kaçmak istenildiğinde, adeta kurlsız “veri cennetleri” kapsamındaki veriler aktarılabilecektir. Bu durum ise, veri işlenmesinde birey hak ve özgürlüklerinin eşit düzeyde korunması gayesine ters düşecektir⁴³⁸. Bu bakımdan verilerin üçüncü ülkelere aktarımını da belli kurallara tabi kılmak önem arz etmiştir. En geniş şekilde ifade edecek olursak, 95/46/AT Sayılı Direktif, bir üçüncü ülkeye veri aktarımı gerçekleştirilmesi halinde, anılan üçüncü ülkede “yeterli” düzeyde veri korumasının mevcut olmasını aramaktadır⁴³⁹.

⁴³⁵ HUSTINX, "EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation", s. 9, https://edps.europa.eu/data-protection/our-work/publications/speeches-articles/eu-data-protection-law-review-directive_en, E.T. 04.11.2018.

⁴³⁶ Anabela Susana DE SOUSA GONÇALVES, “The Cross Border Regulation of Online Data Privacy and the Judicial Cooperation”, *Jusletter IT*, 26.02.2015, s. 6.

⁴³⁷ *Handbook on the European Data Protection Law*, 2018 Ed., European Union Agency for Fundamental Rights and Council of Europe, s. 30.

⁴³⁸ KÜZECİ, *Kişisel Verilerin Korunması*, s. 175.

⁴³⁹ KÜZECİ, *Kişisel Verilerin Korunması*, s. 174.

95/46/AT Sayılı Direktif, IV. Bölümü'nde kişisel verilerin üçüncü ülkelere aktarımını ele almaktadır. Buna göre, veri aktarımları ancak üçüncü ülkenin yeterli koruma sağlaması halinde gerçekleşebilecektir. Uygun koruma olmayan hallere ilişkin olarak da veri aktarımını mümkün kılacak yollar için bir dayanak sağlamaktadır. Direktif'in kabul edilmesinden uzun bir süre sonra, ABD yeterli koruma şartını gerçekleştirmemiştir. 1990'ların sonuna doğru gelindiğinde ise, ABD şirketlerinin "Güvenli Liman" İlkeleri olarak bilinen bazı veri koruma kurallarına uymalarına izin veren bir dizi düzenlemeyi benimseme fikri doğrultusunda Avrupa Komisyonu'nun birimleri ve ABD Ticaret Bakanlığı birlikte çalışmıştır⁴⁴⁰.

Daha detaylı ifade edilecek olursa Direktif'in 25. maddesine göre, bir AB üyesi ülkeden üçüncü bir ülkeye veri aktarımı ancak söz konusu üçüncü ülke yeterli koruma seviyesi sağlarsa mümkün olacaktır⁴⁴¹. Üçüncü bir ülkenin aktarılabilecek veri için "yeterli" düzeyde bir koruma sağladığı ise, veri transfer faaliyetinin tüm koşullarının incelenmesi halinde anlaşılabilir. Verinin aktarılacağı ülkedeki meslek kuralları, güvenlik tedbirleri, yürürlükteki genel ve sektörel kanunlar, son varış ülkesi, kaynak ülke, önerilen faaliyet, süre, amaç ve verilerin yapısı hususlarına ise özellikle önem verilecektir. Dolayısıyla her bağımsız olay, bu şartlar ışığında değerlendirilmelidir.

Üçüncü ülkeleye veri aktarımında, söz konusu ülkede yeterli düzeyde bir koruma olması şartının bazı istisnaları da bulunmaktadır. Direktif'in 26. maddesine göre bu istisnalar;

- Bireyin açık rızası,
- Belirli bir sözleşmenin ifası veya veri aktarımının sözleşme öncesi bir ilişkinin yürütülmesi için gerekli oluşu,

⁴⁴⁰ Nurullah TEKİN, "Kişisel Verilerin Korunması ile İlgili Türkiye'deki Kanun Tasarısı'nın Avrupa Birliği Veri Koruma Direktifi Işığında Değerlendirilmesi", *Uyuşmazlık Mahkemesi Dergisi*, S. 4, 2014, s. 241, ss. 222- 262; Safe Harbor Privacy Principles Issued by the U.S. Department Of Commerce, 21.07. 2000, <https://rm.coe.int/16806af271> , Erişim Tarihi, 06.10.2018.

⁴⁴¹ Case C-101/01, Criminal Proceedings against Bodil Lindqvist, 06.10.2003, Par. 69- 71, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=ecli:ECLI:EU:C:2003:596> , E.T. 05.02.2019.

- Önemli bir kamu yararı,
- Bir kanuni hakkın tesisi,
- Veri öznesinin hayati menfaati,
- Herkese açık olan kamu kayıtlarının devri biçimindedir.

Ayrıca aynı maddenin 2. fıkrasına göre, verinin aktarımının söz konusu olduğu üçüncü bir ülkede “yeterli” düzeyde bir korumanın olmadığı halde, bireyin mahremiyeti ve temel hak ve özgürlüklerinin korunması önlemlerini içeren karşılıklı anlaşmalar kurularak üçüncü ülkeye veri aktarımında bulunabilir.

95/46/AT Sayılı Direktif’in 29. maddesi doğrultusunda, kişisel verilerin işlenmesine dair bireylerin korunması hakkında bir “Çalışma Grubu” kurulmuştur. Danışma amaçlı ve bağımsız olan bu grup, “yeterli düzeyde koruma” ifadesine de açıklık getirmeye gayret etmiştir. Çalışma grubuna göre 24 Temmuz 1998 tarihli Çalışma Raporu’nda, yeterli düzeyin hangi temel ilkeler bağlamında sağlanacağı da belirtilmiştir. “Yeterli düzeyde koruma”yı sağlayacak olan bu ilkeler⁴⁴²;

- *Amaca Bağlılık İlkesi*: Bu ilkeye göre, veriler yalnızca belirli bir amaç doğrultusunda işlenmeli, daha sonra bu amaç dışında kullanılmamalı ve daha fazla iletilmemelidir.
- *Veri Kalitesi ve Orantılılık İlkesi*: Veri doğru, yeterli, ilgili ve gerektiğinde güncel olmalıdır. Ayrıca aktarım ve işlenme amacını da aşmamalıdır.
- *Şeffaflık İlkesi*: Hakkaniyetin sağlanması için bireylere üçüncü ülkedeki işlemin amacı ve veri denetleyicisinin kimliği ile gerekli olduğu sürece diğer bilgiler sağlanmalıdır.

⁴⁴² Working Party on the Protection of Individuals with regard to the Processing of Personal Data, DG XV D/5025/98 WP 12, Working Document on Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive, 24 July 1998, s. 5- 6, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1998/wp12_en.pdf , E.T. 07.02.2019.

- *Güvenlik İlkesi:* Veri denetleyicisi, işleme sürecinde doğabilecek risklere uygun teknik ve kurumsal güvenlik önlemlerini almalıdır.
- *Erişim- Düzeltme ve İtiraz Hakları:* Veri öznesi, kendisi ile ilgili tüm verilerin bir kopyasını alma ve hatalı olan verileri düzeltme haklarına sahip olmalıdır.
- *İleriye Dönük Transferde Kısıtlamalar:* Kişisel verilerin, orijinal veri aktarımının alıcısı tarafından daha fazla aktarılmasına, yalnızca ikinci alıcının yeterli bir koruma seviyesi sağlaması halinde izin verilmelidir.

Çalışma Raporu, bu temel prensiplerin yanında, yeterli düzeyde koruma olması için uygun düzeyde bir rıza, veri öznelerine yardım ve uygun bir tazminatın olması gerektiğini belirtmiştir. Ayrıca, hassas veriler, doğrudan pazarlama ve otomatik karar alma konularında da özel kurallar getirmektedir. Dahası, öz düzenleme yoluyla veya sözleşme düzenlemeleri ile yeterli korumanın sağlanabileceği de dile getirilmiştir⁴⁴³.

2. İlgili İçtihat

Hali hazırda tüm AB üyesi olan devletler, 95/46/AT Sayılı Direktif'i ulusal hukuk sistemlerine aktarmıştır. Bununla birlikte Direktif'in iç hukuka aktarılması yeni üye olan devletler bakımından bir üyelik koşulu olmuştur. Durum böyle olsa da Direktif'in yanlış uygulamaları sebebiyle Avrupa Komisyonu çeşitli yasal işlemler başlatmıştır⁴⁴⁴.

Adalet Divanı, 95/46/AT Sayılı Direktif'in uygulamasına ilişkin bazı önemli kararlara imza atmıştır. Bu kararların bir kısmında İHAM içtihatlarına da yer vermiş, Temel Haklar Şartı'nın da uygulamaya girmesi ile bu özelliğine devam etmiştir. Aşağıda

⁴⁴³ Working Party on the Protection of Individuals with regard to the Processing of Personal Data, DG XV D/5025/98 WP 12, Working Document on Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive, 24 July 1998, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1998/wp12_en.pdf, E.T. 07.02.2019.

⁴⁴⁴ HUSTINX, "EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation", s. 12, https://edps.europa.eu/data-protection/our-work/publications/speeches-articles/eu-data-protection-law-review-directive_en, E.T. 06.11.2018.

ele alınan kararlar, 2016 yılında ortaya çıkan Veri Koruma Reformu'na dek süren anlayışı ortaya koyabilmek adına seçilmiştir.

Divan öncelikle Direktif'in uygulama alanına ilişkin olarak, 2003 yılında *Rechnungshof- Österreichischer Rundfunk ve Diğerleri ve Christa Neukomm ve Joseph Lauermann- Österreichischer Rundfunk* isimli birleştirilmiş davalarda Direktif'in üye bir ülkenin kamu sektörüne ya da bir ibadethane veya yardım kuruluşunun internet sitesine uygulanabileceğine hükmetmiştir⁴⁴⁵. Ayrıca yine bu davada Direktif'in İHAS'ın 8. maddesi kapsamına giren bir alana uygulanması gerektiği hallerde ise, bu madde doğrultusunda yorum yapılması gerektiğine karar vermiştir⁴⁴⁶. Buna göre İHAM 8. maddeyi ihlal edebilecek ya da ihlal etmeyecek veri işleme süreçleri arasında ayırım yapmıştır. Öncelikle bir kişinin mesleki gelirine ilişkin üçüncü şahıslara iletmek amacıyla veri toplama, İHAS'ın 8. maddesi kapsamına girmektedir. Dolayısıyla İHAM'a göre özel yaşam kavramı kısıtlayıcı bir şekilde yorumlanmamalı ve profesyonel nitelikteki faaliyetler de özel yaşam kavramı kapsamında değerlendirilmelidir. Bir işverenin çalışanlarının isimleri ve aldıkları ücretleri kayıt altına alması, veri koruma kurallarına uyulduğu müddetçe, özel hayat kapsamında sorun teşkil etmezken, bu verilerin bir kamu otoritesi gibi üçüncü bir kişiye iletilmesi ve sonrasında kullanılması 8. maddenin ihlali anlamına gelecektir⁴⁴⁷. Görüleceği üzere bu durum, veri koruma alanında "özel yaşam" ve "veri koruma" farklarını ortaya koyması bakımından da önem arz etmektedir.

⁴⁴⁵ Joined Cases C-465/00, C-138/01 and C-139/01, *Rechnungshof v Österreichischer Rundfunk and Others and Christa Neukomm and Joseph Lauermann v Österreichischer Rundfunk*, 20 May 2003, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=ecli:ECLI:EU:C:2003:294>, E.T. 01.01.2019.

⁴⁴⁶ Joined Cases C-465/00, C-138/01 and C-139/01, *Rechnungshof v Österreichischer Rundfunk and Others and Christa Neukomm and Joseph Lauermann v Österreichischer Rundfunk*, 20.05.2003, Par. 68- 92, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=ecli:ECLI:EU:C:2003:294>, E.T. 02.01.2019.

⁴⁴⁷ *Amann v. Switzerland*, Application No: 27798/95, 16.02.2000, Par. 65, <http://hudoc.echr.coe.int/eng?i=001-58497>, E.T. 17.01.2019; *Rotaru v. Romania*, Application No: 28341/95, 04.05.2000, Par. 43, <http://hudoc.echr.coe.int/eng?i=001-58586>, E.T. 19.10.2017; Joined Cases C-465/00, C-138/01 and C-139/01, *Rechnungshof v Österreichischer Rundfunk and Others and Christa Neukomm and Joseph Lauermann v Österreichischer Rundfunk*, 20.05.2003, Par. 68- 92, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=ecli:ECLI:EU:C:2003:294>, E.T. 02.01.2019.

2003 yılında hüküm altına alınan *Lindqvist* isimli bir diğer kararda da Direktif'in kural olarak internete de uygulanacağı, fakat üçüncü ülkelerle veri akışını düzenleyen hükümlerin, bir internet sitesinde bulunan kişisel verilere uygulanamayacağı hüküm altına alınmıştır⁴⁴⁸. Bu kararda ayrıca, Direktif'in 3. maddesinde yer alan ve Direktif'in uygulama alanı dışında kalan bir istisna olan “*bir gerçek kişi tarafından, tamamen kişisel veya ev içi faaliyeti esnasında*”ki kişisel verilerin, belirsiz ve sınırsız sayıda insanın erişebilir olduğu kişisel verileri değil, sadece bireylerin özel yaşamı veya aile yaşamı boyunca yürütülen faaliyetler bağlamında geçerli olduğuna karar vermiştir. Dolayısıyla bu istisna yalnızca bireylerin özel yaşam ve aile yaşamları sırasında yürütülen faaliyetlerle ilgili olarak yorumlanmalıdır. Örneğin internette belirsiz sayıdaki insana yayımlanan kişisel faaliyetlere veya hanehalkı faaliyetlerine ilişkin verilerin işlenmesinde bu istisna uygulanmayacaktır⁴⁴⁹. Ayrıca bu davada, kendine ait bir internet sitesinde, çalışmış olduğu bir Protestan Kilisesi'nde kendisi ile birlikte gönüllü çalışan bazı kişiler hakkında kişisel verilerini yayınlamamış olan kişi bakımından durumun diğer bir ülkeye veri aktarımı sayılıp sayılmadığını da incelemiştir. Bu bağlamda bir internet sitesine başka bir ülkede bulunan kişi tarafından yüklenen ve üçüncü bir ülkedeki kişinin bilgisayarında görünen veriler doğrudan bu iki kişi arasında değil, sayfanın bulunduğu barındırma sağlayıcısının⁴⁵⁰ bilgisayar altyapısı aracılığıyla aktarılmaktadır. Bu durumda kişisel bilgilere üçüncü bir ülkeden erişen kişi, bu verilere erişebilmek için ilave bazı işlemler yapmak durumundadır ve dolayısıyla bu verilere doğrudan ulaşılması gibi bir

⁴⁴⁸ Case C-101/01, Criminal Proceedings against *Bodil Lindqvist*, 06.10.2003, Par. 24-27, 69- 71, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=ecli:ECLI:EU:C:2003:596> , E.T. 01.01.2019.

⁴⁴⁹ Case C-101/01, Criminal proceedings against *Bodil Lindqvist*, 06.11.2003, Par. 47, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62001CJ0101> , E.T. 18.01.2019.

⁴⁵⁰ İngilizce ismi “hosting” olan barındırma işlemi, bir internet sitesinde web sayfalarını yüklemek için gereken alanı, bilgisayarlardan daha güçlü olan sunucu denen makineler üzerinden sağlama işlemidir. Bir diğer ifade ile “*uzaktan bağlanan bilgisayarlara sunulmak üzere üçüncü taraflara ait bazı bilgileri veya örün sayfalarını saklamak*” biçiminde ifade edilmektedir. TÜBA Türkçe Bilim Terimleri Sözlüğü, “konakçılık”, <http://www.tubaterim.gov.tr> , E.T. 19.05.2019.

durum söz konusu değildir. Divan bu durumu, üçüncü bir ülkeye veri aktarımı teşkil etmediği şeklinde yorumlamıştır⁴⁵¹.

Direktif'in uygulama alanı ve işlerliğine dair sorunları ortaya koyması bakımından önem arzeden ve kamu güvenliği söz konusu olduğunda veri işleme kurallarında bir istisna sağlayan Avrupa Adalet Divanı'nın önemli bir kararı da 11 Eylül 2001'deki terör saldırılarının ardından sınır koruma maksadı ile havayolu yolcu verilerinin (Passenger Name Records- PNR) ABD'ye iletilmesine ilişkin karardır. Söz konusu olay, 95/46/AT Sayılı Direktif'in uygulama alanına dair tartışmalı bir alanı oluşturmaktadır.

Anılan kararın giriş kısmında,

“23 Şubat 2004'te (Avrupa Birliği Konseyi) Konsey'in, Komisyon'a topluluk adına PNR havayolu verilerinin hava taşımacıları tarafından işlenmesi ve aktarılması konusunda ABD ile bir anlaşma yapması için müzakere yetkisi verdiği”

hususunu ele alınmaktadır. Bunun üzerine Komisyon ABD Hükümeti ile görüşmeler gerçekleştirmiş ve nihayetinde bir anlaşmaya varmıştır. 14 Mayıs 2004'te de bu anlaşma ile uzlaşılan korumanın yeterli düzeyde olduğuna karar vermiştir⁴⁵². Devamında ise AB Konseyi, Avrupa Parlamentosu'nun konuya dair kararını beklemeksizin ve Parlamento'nun gereken sürede görüşünü bildirmediğini belirterek 17 Mayıs 2004'te bu kararı onaylamıştır⁴⁵³. İşte bu sürecin sonunda Avrupa Parlamentosu, Konsey ve Komisyon'a Adalet Divanı nezdinde dava açmıştır.

⁴⁵¹ Case C-101/01, Criminal proceedings against *Bodil Lindqvist*, 06.11.2003, Par. 2, 60-61, 68- 70, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62001CJ0101> , E.T. 18.01.2019.

⁴⁵² Commission Decision of 14 May 2004 on the Adequate Protection of Personal Data Contained in the Passenger Name Record of Air Passengers Transferred to the United States' Bureau Of Customs and Border Protection, Par. 14, 2004/535/EC, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32004D0535> , E.T. 17.01.2019.

⁴⁵³ Council Decision of 17 May 2004 on the Conclusion of an Agreement Between the European Community and the United States of America on the Processing and Transfer of PNR Data by Air Carriers to the United States Department of Homeland Security, Bureau Of Customs And Border Protection, Par.

Adalet Divanı 30 Mayıs 2006'da Parlamento'yu haklı bularak Konsey ve Komisyon'un işlemlerini geçersiz kılmıştır. Bu karar özellikle bazı noktaları bakımından farklılık teşkil etmektedir. Öncelikle Divan, her ne kadar kararlarında AB'nin taraf olmadığı anlaşma ya da sözleşmelere yer vermiyorsa da 3. paragrafında İHAS'ın 8. maddesine yer vermiştir. Bu durum kararın adeta bu madde üzerine yoğunlaşacağı izlenimini vermiştir. Ancak Divan, anlaşmanın iptaline dair gerekçeleri ortaya koyarken bu maddeye yalnızca 62. paragrafta yer vermiştir. Bu durum oldukça dikkat çekicidir, çünkü Divan'ın meseleye bakış açısının yalnızca özel yaşam hakkı bağlamında olması gerektiği niyeti tam anlamıyla net bir şekilde karşımıza çıkmamaktadır⁴⁵⁴. Divan'ın bu kararı ile, kişisel verileri toplayarak kamu güvenliği gerekçesi ile bu bilgileri bir şekilde ABD'ye aktaran özel sektör teşebbüslerinin akıbeti belirsiz hale gelmiştir⁴⁵⁵. Ayrıca Konsey ve Komisyon'un ABD ile anlaşma yapması yetki bakımından incelenmiş; fakat anlaşma içeriğinin Avrupa veri koruma ilkelerine uygunluğu bakımından bir inceleme yapılmamıştır. Bu sebeple Adalet Divanı'nın aynı içerikte ve usule uygun farklı bir anlaşma söz konusu olduğundaki tavrı belirsiz kalmıştır⁴⁵⁶.

Divan'ın 2008 yılındaki *Tietosuojaaltuutettu- Satakunnan Markkinapörssi Oy ve Satamedia Oy* kararına konu olan olayda ise Markkinapörssi şirketi 1994 yılında, birkaç yıl boyunca Veropörssi gazetesinin bölgesel basımlarında vergi verilerinden alıntılar yayınlamak amacıyla Finlandiya vergi makamlarından kamuya açık veriler toplamıştır. Bu yayınlarda yer alan bilgiler, geliri belirli eşikleri aşan yaklaşık 1.2 milyon gerçek kişinin, ad-soyad, kazanılmış ve kazanılmamış gelirleri ve bunlara uygulanan servet vergisine ilişkin detaylardır. Veropörssi gazetesi, açıklanan kişisel verilerin talep üzerine

2-3, 2004/496/EC, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32004D0496> , E.T. 17.01.2019.

⁴⁵⁴ Elspeth GUILD, Evelien BROUWER, "The Political Life of Data: The ECJ Decision on the PNR Agreement between the EU and the US", *Centre for European Policy Studies Policy Brief*, No: 109, July 2006, <https://www.files.ethz.ch/isn/24402/PB110.pdf> , E.T. 17.01.2019.

⁴⁵⁵ Joined Cases C-317/04 and C-318/04 *European Parliament v Council of the European Union and Commission of the European Communities*, 30.05.2006, Par. 54- 61, 67- 70, <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A62004CJ0317> , E.T. 17.01.2019.

⁴⁵⁶ GUILD, BROUWER, "The Political Life of Data: The ECJ Decision on the PNR Agreement between the EU and the US", <https://www.files.ethz.ch/isn/24402/PB110.pdf> , E.T. 17.01.2019.

ve bedelsiz olarak kaldırılabilmesine dair bir beyanda bulunmuştur. Markkinapörssi şirketi ayrıca bu kişisel bilgileri bir yandan CD-ROM diskleri şeklinde Veropörssi'nin aynı hissedarlarına ait olan Satamedia'ya da aktarmıştır. Bu bağlamda anılan şirket, cep telefonu kullanıcılarına yaklaşık 2 EUR'luk bir ücret karşılığında Veropörssi gazetesinde yayınlanan bilgileri almalarına olanak tanıyan bir servisi olan bir mobil telefon şirketi ile anlaşma imzalamıştır. İşte bu davada Divan, 95/ 46/ AT Sayılı Direktif'in Başlangıç 12. paragraf ve md. 3/2'de yer alan istisnaların, toplanan verilerin sınırsız sayıda insan için erişilebilir olmasını sağlamak gayesine sahip olan Markkinapörssi ve Satamedia şirketlerinin faaliyetleri için geçerli olmadığına hükmetmiştir⁴⁵⁷.

Anılan bu olay daha sonra 27.06.2017 tarihinde İHAM tarafından karara bağlanmıştır. Burada, meselenin 8. maddede yer alan özel yaşam hakkı ile 10. maddede bulunan basın özgürlüğü arasında doğru dengenin kurulması gereğine vurgu yapılmıştır. Büyük Daire, ifade özgürlüğü hakkını özel yaşama saygı hakkına karşı dengeleme konusunda yerel makamlara geniş bir takdir payı vermiştir. Büyük Daire'ye göre, vergi verilerinin yayınlanması ile kamu yararına yönelik bir tartışmaya katkı sağlanmamıştır. Ayrıca, Finlandiya'da belirli vergi verilerinin kamuya açık olmasına rağmen, bu verilerin şirketler tarafından yayınlanmasının sınırsız ve yasama organı tarafından tasarlanmayan bir ölçüde verileri erişilebilir kılmasına dair bir ayırım yapılması gerektiğine dikkat çekilmiştir. Nihayetinde İHAM, Finlandiya mahkemeleri ve makamlarının anılan iki şirketin vergi kişisel verilerini olduğu gibi işlemelerini yasakladıkları olayda ifade özgürlüklerinin ihlal edilmediğine hükmetmiştir. Mahkeme, kısıtlamaların kanunla öngörülmüş olduğu ve vergi mükelleflerinin mahremiyet hakkını korumak için meşru bir amaç edindiği sonucuna varmıştır⁴⁵⁸.

Divan'ın veri koruma otoritelerinin bağımsızlığı konusuna ilişkin birden fazla kararı bulunmaktadır. Bunlardan 2010 yılındaki *Avrupa Komisyonu- Almanya Federal*

⁴⁵⁷ Case C-73/07 *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy*, 16.12.2008, Par. 44, <https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:62007CJ0073> , E.T. 18.01.2019.

⁴⁵⁸ *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*, Application No: 931/13, 27.06.2017, Par. 122, 198-199, <http://hudoc.echr.coe.int/eng?i=001-175121> , E.T. 18.01.2019.

Cumhuriyeti kararında, birden fazla yerde “tam bağımsızlık”tan söz etmiştir. Divan’a göre bunun anlamı, denetim otoritesi üzerindeki doğrudan ya da dolaylı dış etkenlerden bağımsız karar verme gücüdür. Bu bakımdan denetim otoriteleri görevlerini yerine getirirken, nesnel ve tarafsız davranmaları gerektiği hüküm altına alınmıştır. Divan burada Direktif’te yer alan “tam bağımsızlık” kavramının kesin biçimde herhangi bir dış etkiden arınmış olmak anlamına geldiğini belirtmiştir⁴⁵⁹. Bu husus, 2012 yılında *Komisyon- Avusturya*⁴⁶⁰ ve 2014 yılında *Komisyon- Macaristan*⁴⁶¹ kararlarında yinelenmiştir.

Divan’ın, Direktif’de yer alan meşru veri işleme kriterleri hakkında olan 2011 yılındaki *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) ve Federación de Comercio Electrónico y Marketing Directo (FECMD)- Administración del Estado* kararında ise, veri öznesinin rızasının yokluğu halinde işlenen verilere dair İspanya’nın Direktif’in 7/(f). maddesini doğru bir şekilde iç hukukuna aktaramadığına hükmetmiştir. Başvuranlar, kişisel verilerin işlenmesinde bir veri denetleyicisinin meşru çıkarlarına dayanarak işlenen verinin kamu malı olması şartını ilave olarak getiren İspanya’nın ulusal veri koruma kanununa itiraz etmişlerdir. Divan, 95/ 46/ AT Sayılı Direktif’in 7. maddesinde düzenlenen “Meşru Şekilde Veri İşleme Kriterleri”nin yeterince kesinlikte olduğuna, üye devletlerin bu bakımdan ek koşullar getiremeyeceklerine ve bu hükmün iç hukukta doğrudan etkiye sahip olduğuna hükmetmiştir⁴⁶².

⁴⁵⁹ Case C-518/07, *European Commission v. Federal Republic of Germany*, 9 Mart 2010, Par. 3-6, 19, 30, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62007CJ0518> , E.T. 06.11.2018.

⁴⁶⁰ Case C-614/10, *European Commission v. Republic of Austria*, 16 October 2012, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62010CJ0614> , E.T. 06.11.2018.

⁴⁶¹ Case C-288/12, *European Commission v. Hungary*, 08 April 2014, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0288> , E.T. 06.11.2018.

⁴⁶² Joined Cases C-468/10 and C-469/10 *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECMD) v. Administración del Estado*, 24.11.2011, Par. 37- 38, 49, 51- 55, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62010CJ0468> , E.T. 18.01.2019.

Divan'ın veri denetleyicisinin veri güvenliği için uygun bir güvenlik seviyesi belirlemesi hakkındaki 30 Mayıs 2013 tarihli *Worten* kararına⁴⁶³ göre, bu seviye belirlenirken teknolojinin durumu, uygulamaların maliyeti, korunacak verilerin niteliği ile varolan risk dikkate alınmalıdır. Ayrıca yine bu konuda daha evvel 2009 yılında hüküm altına aldığı bir kararında da aynı yönde, veri güvenliğinin teminini sağlamaya yönelik olarak alınacak teknik ve idari tedbirlerin uygulama maliyetlerinin de hesaba katılması gerektiğini dile getirmiştir⁴⁶⁴.

Adalet Divanı 12 Aralık 2013 tarihli *X*. kararında, veri öznesinin veri sorumlusuna başvurduğu hallerde veri sorumlusunun ücret talep edip edemeyeceği sorusunu cevaplandırmıştır. Anılan karara göre, 95/46/AT Sayılı Direktif'in 12/(a). maddesinde yer alan "aşırı gecikme ve masraf olmaksızın" ibaresi, başvurunun ücretsiz yapılmasını gerektirmektedir. Fakat karara göre bu ifadede, veri sorumlusunun ücret talep ettiği durumlarda, ücretin aşırı olmadığı sürece ödenmesi de yasaklanmamaktadır. Bu bakımdan söz konusu maddenin, ücret alınmasını engellemek biçiminde yorumlanmaması gerektiğine hükmedilmiştir⁴⁶⁵.

Bugüne kadar Divan'ın en çok ses getiren kararı olarak adlandırabileceğimiz ve kısaca "*Google Kararı*" olarak anılan 2014 yılındaki davada Divan, Direktif'e dayanarak "Unutulma Hakkı"nı tanımıştır. Buna göre olayda Avukat Costeja González adını Google arama motoruna yazdığına günlük bir gazetenin iki farklı tarihli sayfasının linki çıkmakta ve bu link verilen sayfalarda sosyal güvenlik borçlarının iyileştirilmesi için mülkünü satmak zorunda kalmasına ilişkin bilgiler yer almaktadır. Divan bu kararda ilke olarak kişinin özel yaşamının gizliliği hakkının, arama motorunun ekonomik çıkarı ile söz konusu kişi adıyla yapılan arama üzerine kamunun bilgiye erişim hakkının üzerinde

⁴⁶³ Case C-342/12 *Worten – Equipamentos para o Lar SA v. Autoridade para as Condições de Trabalho (ACT)*, 30.05.2013, Par. 24, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0342&from=FR>, E.T. 27.04.2019.

⁴⁶⁴ Case C-553/07 *College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer*, Par. 62, 07.05.2009, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62007CJ0553&from=EN>, E.T. 27.04.2019.

⁴⁶⁵ Case 486/12 *X*, 12.12.2013, Par. 20- 23, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0486>, E.T. 04.04.2019.

olduğunu ve bu kuralın yalnızca kamunun bilgiyi öğrenmede üstün bir yararı bulunmakta ise uygulanmayacağını hükme bağlamıştır. Bu bakımdan kişinin ismine dayalı olarak üçüncü kişiler tarafından internet ortamında yasal olarak işlenmiş ve yayınlanmış kişisel verilerinin geçersiz, eksik, tamamen ilgisiz veya sonradan ilgisiz hale geldiği ve böylece işlenme amacını aştığı ve bu sebeple arama motorları tarafından internet ortamına yüklenen söz konusu kişisel verilerin ve buna ilişkin sonuç listesinde yer alan bilgilerin silinmesi gerektiği belirtilmiştir⁴⁶⁶. Böylece 95/46/AT Sayılı Direktif’in hükümlerini ilerici biçimde yorumlayarak Direktif’te bulunmayan “unutulma hakkı”nı tanımıştır.

Divan’ın veri öznesinin veri korumasına dair sahip olduğu haklara ilişkin bir kararı da 17 Temmuz 2014 tarihli *Y.S.- Minister voor Immigratie, Integratie en Asiel* ve *Minister voor Immigratie, Integratie en Asiel- M. ve S.* isimli birleştirilmiş bir davadır. Buna göre veri öznesinin özel yaşama saygı hakkının, kendisiyle ilgili bilgilerin doğru olması ve hukuka uygun bir şekilde işlenmesi hususunu da kapsadığı belirtilmiştir. Veri öznesinin kendisi hakkındaki verilere erişim hakkının, verinin düzeltilmesi, silinmesi ya da engellenmesi hususlarını da içerdiği ve veri öznesinin hukuka aykırı biçimde verisinin işlenmesinden dolayı uğradığı zarar için veri denetleyicisinden tazminat hakkı bulunduğu da hüküm altına alınmıştır⁴⁶⁷.

Adalet Divanı’nın 11 Aralık 2014 tarihli *Reynes* kararında ise 95/46/AT Sayılı Direktif’in 3/2. maddesinde yer alan istisna hükümlerinden “tamamen kişisel veya ev içi aktiviteler” ifadesinden ne anlaşılması gerektiği ortaya konulmaktadır. Bahis konusu olayda hırsızlıktan korunmak amacı ile evin girişine konulan kamerayla elde edilen veriler mevcuttur. Divan’a göre, istisna içeren hükümler dar yorumlanmalıdır. Üstelik kamerayla elde edilen her verinin kişisel ya da ailevi nitelikte olmadığı dile getirilmiştir.

⁴⁶⁶ Case C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, 13.05.2014, Par. 94, 100, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131>, E.T. 19.05.2019.

⁴⁶⁷ Joined Cases C-141/12 *Y.S. v. Minister voor Immigratie, Integratie en Asiel* and C-372/12 *Minister voor Immigratie, Integratie en Asiel v. M. and S.*, 17.07.2014, Par. 8, 44, <http://curia.europa.eu/juris/document/document.jsf?docid=155114&doclang=EN>, E.T. 22.04.2019.

Dolayısıyla evin girişine konulan kameredan elde edilen veriler, tamamen kişisel ya da ev içi faaliyetler kapsamında değildir⁴⁶⁸.

Facebook İrlanda Ltd.'nin kullanıcılarının kişisel verilerini ABD'ye aktarması ve kullanıcıların verilerini oradaki sunucularda tutmasına ilişkin 2015 yılındaki *Maximillian Schrems- Veri Koruma Komiseri* kararında Divan, 95/46/AT Sayılı Direktif'in 25/6. maddesinde yer alan "yeterli koruma seviyesi" kavramındaki "yeterli"(*adequate*) kelimesinin üçüncü bir ülkenin, AB hukuk düzeninde garanti edilenle koruma ile birebir aynı şekilde bir koruma sağlamak için gerekli olamayacağına dikkat çekmiştir. Ancak "yeterli koruma seviyesi" teriminin, üçüncü ülkenin kendi iç hukuku veya uluslararası taahhütleri gereği, 95/46/AT Sayılı Direktif ile AB alanında güvence altına alınmış olan temel hak ve özgürlüklerin korunmasını sağlaması gereği de vurgulanmıştır⁴⁶⁹.

Adalet Divanı'nın yukarıda anılan bazı kararlarının incelenmesi neticesinde görülmektedir ki Divan, 95/46/AT Sayılı Direktif'e dair uygulamanın mümkün olduğunca açıklığa kavuşması için uygulama alanından, kişisel verilerin kapsamına, denetim makamlarının bağımsızlığından veri aktarımına dair birçok alanda geliştirici yorumlarda bulunmaktan kaçınmamıştır. Öyle ki bu kapsamda Direktif'te yer almayan ve Direktif'in oldukça etraflı analizi neticesinde ortaya çıkardığı yeni bir haktan da söz edilmiştir (Unutulma Hakkı). Divan'ın yenilikçi yorumu neticesinde ortaya çıkan bu hak, daha sonra Veri Koruma Reformu ile gelen GVKT'de açıkça tanınmıştır. Adalet Divanı her ne kadar 95/46/AT Sayılı Direktif nezdinde bu gibi olumlu gelişmeleri gerçekleştirse de yukarıda ele alındığı üzere, tıpkı Lizbon Anlaşması ile bağlayıcı hale gelen Şart'ın uygulamasında olduğu gibi, İHAM içtihatlarının etkisini tam anlamıyla üzerinden atamamıştır. Bu sebeple kişisel verilerin korunması hakkını tam anlamıyla bağımsız bir temel hak olarak değerlendirmek yerine, özel yaşam hakkı bağlamında ele almaya devam etmektedir. Bu bakımdan AB'nin yargı organı olan Divan'ın, üzerine

⁴⁶⁸ Case C-212/ 13 *František Ryneš v. Úřad pro ochranu osobních údajů*, 11.12.2014, Par. 30, 35, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62013CJ0212> , E.T. 22.04.2019.

⁴⁶⁹ Case C-362/14 *Maximillian Schrems v. Data Protection Commissioner*, 06.11.2015, Par. 73, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62014CJ0362&from=FR> , E.T. 22.04.2019.

düşen ortak AB Hukuku'nu yaratma görevini Direktif'in yorumu ve uygulaması bakımından mümkün olduğunca gerçekleştirmiş olduğu söylenebilse de hakkın bağımsız niteliğine katkısı görece daha az olmuştur.

C. VERİ KORUMA REFORMUNA GÖTÜREN DİĞER DÜZENLEMELER

1. 97/66/AT Sayılı Telekomünikasyon Sektöründe Kişisel Verilerin İşlenmesi ve Özel Yaşamın Korunması Direktifi

Aralık 1997'de kabul edilen ve 95/46/AT Sayılı Direktif'in tamamlayıcılarından olan 97/66/AT Sayılı Telekomünikasyon Sektöründe Kişisel Verilerin İşlenmesi ve Özel Yaşamın Korunması Direktifi, adından da anlaşılacağı üzere telekomünikasyon sektöründe kişisel verilerin işlenmesi ve bu bağlamda özel yaşamın korunmasına dairdir.

Anılan Direktif'in amacı, telekomünikasyon sektöründeki kişisel verilerin işlenmesiyle ilgili olarak, temel hak ve özgürlüklerin ve özellikle özel yaşam hakkının eşdeğer düzeyde korunmasını ve bu tür veriler ile telekomünikasyon ekipman ve hizmetlerin serbest dolaşımını sağlamaktır. 97/66 /AT Sayılı Direktif, 95/46/AT Sayılı Direktif'in genel kurallarını somut bir sektör için geliştiren, lex specialis olarak düzenleyen bir metindir. Fakat söz konusu Direktif yalnızca bu sebeple yapılmamıştır. Direktif'in 2. maddesinde, 95/46/AT Sayılı Direktif'teki tanımlar kabul edilmekle beraber, 97/66/AT Sayılı Direktif'in amaçları doğrultusunda belli kavramlar da yeniden tanımlanmıştır⁴⁷⁰.

Uygulamaya bakıldığında ise, 97/66/AT Sayılı Direktif'in kişisel verilerin korunmasını ne ölçüde belirleyip tamamladığı ile ilgili net bir tablo ortaya konulamamıştır. Direktif'te yer alan hakların ve özel yaşam kavramının Direktif bağlamında anlamları da belirsizdir. Ayrıca Direktif'in İngilizce olan halinde hem

⁴⁷⁰ Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector, Art. 1, 2, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31997L0066&from=EN> , E.T. 26.10.2018.

“privacy”, hem “private life”, hem de “confidentiality” kavramları iletişimin gizliliğini ifade etmek için kullanıldığı görülmektedir⁴⁷¹.

97/66/AT Sayılı Direktif, bugün dahi önemini taşıyan bir durum olarak, istenmeyen arama ve fakslara uygulamak için “tüketicinin özel yaşam hakkı”na dair hükümler içermektedir. 12. maddeye bakıldığında, doğrudan pazarlama için faks dahil olmak üzere insan müdahalesi olmaksızın kullanılan herhangi bir otomatik arama makinesinin kullanımı için bir seçim rejimi mevcuttur⁴⁷². Bu madde daha sonra, elektronik posta ile ya da SMS yoluyla kurulan istenmeyen mail ve mesajlara dair düzenlemelere yol açmıştır⁴⁷³.

3. Avrupa Topluluğu (Amsterdam) Antlaşmasının 286. Maddesi

95/46/AT Sayılı Direktif, üye devletlerin Direktif’in içeriğini aktarma ve hükümlerini kabul etmelerini zorunlu kılar, ancak topluluk kurum ve kuruluşlarını doğrudan bağlamaz⁴⁷⁴.

95/46/AT Sayılı Direktif’in kabulünden iki yıl sonra Amsterdam Antlaşması imzalanmış ve 1 Mayıs 1999 tarihinde yürürlüğe girmiştir. Bu antlaşma oldukça önemli değişiklikler getirmiştir. Bunlardan kişisel verilerle ilgili olan düzenleme 286. maddede yer almaktadır. Buna göre; 1 Ocak 1999 tarihinden itibaren, kişisel verilerinin işlenmesi ve bu verilerin serbest dolaşımı ile ilgili bireylerin korunmasına dair topluluk düzenlemeleri, AT Antlaşması tarafından ya da ilgili antlaşma uyarınca kurulan kurum

⁴⁷¹ Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector, Preamble Par. 1, 3, 5, 6, 8, 13, 17, 18, 19, 21, 22, Art. 1, 5, 7, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31997L0066&from=EN>, E.T. 26.10.2018.

⁴⁷² Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector, Art. 12, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31997L0066&from=EN>, E.T. 26.10.2018.

⁴⁷³ Lodewijk F. ASSCHER, Judith VAN ERVE, *Regulating Spam: Directive 2002/ 58 and Beyond*, The Institute For Information Law- University of Amsterdam, 2004, s. 23- 27.

⁴⁷⁴ FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, s. 143.

ve organlara uygulanacaktır. Anılan madde kişisel verilerin serbest dolaşımı fikrinin, yapıldığı dönem itibarıyla, yeni ve muğlak yapısını ortaya koymaktadır. Son olarak ise bu madde ile Ocak 1999 tarihinden itibaren AT kurum ve organlarına uygulanacak olan hükümlerin takibi için yeni ve bağımsız bir denetim organının kurulması öngörülmüştür⁴⁷⁵.

4. 2002/58/AT Sayılı Elektronik İletişimde Kişisel Verilerin İşlenmesi ve Özel Yaşamın Korunması Direktifi

31 Temmuz 2002 tarihinde yürürlüğe giren 2002/58/AT Sayılı Elektronik İletişimde Kişisel Verilerin İşlenmesi ve Özel Yaşamın Korunması Direktifi de tıpkı 97/66/AT Sayılı Direktif gibi, 95/46/AT Sayılı Direktif'in bir diğer tamamlayıcısıdır⁴⁷⁶. Anılan hukuki düzenleme, sektörel bazda yapılan düzenlemelerin en önemlilerinden biridir.

97/66/AT Sayılı Telekomünikasyon Sektöründe Kişisel Verilerin İşlenmesi ve Özel Yaşamın Korunması Direktifi, kamuya açık elektronik iletişim hizmetlerinin kullanıcıları için kişisel verilerin ve özel yaşamın eşit düzeyde korunması amacıyla pazardaki yeni gelişmeler doğrultusunda elektronik iletişim sektöründeki yeni teknolojilere adapte edilmeliydi⁴⁷⁷. Bu sebeple 2002/58/AT Sayılı Direktif, elektronik iletişimde kişisel verilerin korunmasını yeni teknolojilere uyumlu hale getirmek için kabul edilmiştir.

⁴⁷⁵ Treaty establishing the European Community (Amsterdam consolidated version), Art. 286, <https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:11997E286>, E.T. 29.10.2018.

⁴⁷⁶ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications), <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN>, E.T. 29.10.2018.

⁴⁷⁷ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications), Preamble Par. 4, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN>, E.T. 29.10.2018.

Bahis konusu direktifin en önemli özelliği, 95/46/AT Sayılı Direktif'ten farklı olarak tüzel kişilerin de kişisel verilerinin korunmasını düzenlemesidir⁴⁷⁸.

5. 45/2001/AT Sayılı Topluluk Kurum ve Organları tarafından Kişisel Verilerin İşlenmesi ve Verilerin Serbest Dolaşımı bakımından Bireylerin Korunması Direktifi

Avrupa Komisyonu, Amsterdam Antlaşması'nın 286. maddesinde belirtilen yükümlülükleri uygulamak için 1999 yılında, bireylerin Topluluk kurumları ve organları tarafından kişisel verilerin işlenmesine ilişkin olarak korunması ve bu verilerin serbest dolaşımı konusunda bir regülasyon taslağı kabul etmiştir⁴⁷⁹. Anılan bu taslak 18 Aralık 2000 tarihinde, AT kurum ve organları tarafından kişisel verilerin işlenmesi sırasında gerçek kişilerin korunması amacıyla 45/2001/AT Sayılı Direktif'e temel oluşturmuştur⁴⁸⁰.

Bu metin ile Topluluk alanında bulunan tüm organ ve kurumlarca gerçekleştirilen her türlü veri işleme hallerinde uyulması gereken esaslar düzenlenmiştir. Bu bağlamda Direktif'in amacı, Topluluk kurum ve organları tarafından kişisel verinin işlenmesi esnasında gerçek kişilerin temel hak ve özgürlüklerini korumak ve kişisel verilerin üye ülkeler veya 95/46/AT Sayılı Direktif'i uygulayan ülkelerin ulusal kanunlarına tabi olan alıcılar için serbest akışını kısıtlamamak veya yasaklamamaktır⁴⁸¹.

⁴⁷⁸ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications), Preamble Par. 7, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN>, E.T. 29.10.2018.

⁴⁷⁹ FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, s. 144.

⁴⁸⁰ Regulation (EC) No: 45/2001 of the European Parliament and of the Council of 18 December 2000 on the Protection of Individuals with regard to the Processing of Personal Data by the Community Institutions and Bodies and on the Free Movement of Such Data, <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32001R0045>, E.T. 29.10.2018.

⁴⁸¹ Regulation (EC) No: 45/2001 of the European Parliament and of the Council of 18 December 2000 on the Protection of Individuals with regard to the Processing of Personal Data by the Community Institutions and Bodies and on the Free Movement of Such Data, Art. 1, <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32001R0045>, E.T. 30.10.2018.

45/2001/AT Sayılı Direktif'in 1/2. maddesi Avrupa Veri Koruma Denetçisi adında bir kurum oluşturmuştur ve bu kurum, Direktif'in hükümlerinin uygulanmasını denetlemekle görevlendirilmiştir⁴⁸².

Direktif'e göre kişisel veriler⁴⁸³;

- Adil ve hukuka uygun olarak işlenmelidir.
- Belirli, açık ve meşru amaçlarla toplanmalıdır. Toplanan verinin tarihi, istatistiki ve bilimsel amaçlarla daha fazla işlenmesi durumunda, amaç dışı kullanımın engellenmesi için veri güvenliğinin sağlanması gerekmektedir.
- Yeterli ve uygun ölçüde işlenmeli ve aşırı biçimde işlenmemelidirler.
- Doğru ve güncel biçimde işlenmelidir. Hatalı, eksik ya da toplanması gerekenden fazla toplanırsa verilerin silinmesi ya da düzeltilmesi için her türlü makul girişimde bulunulmalıdır.
- Verinin toplanmasını ve daha fazla işlenme amacı dışında kullanımını engelleyecek şekilde öznesinin belirlenmesini sağlayacak formda tutulmalıdır. Verinin tarihi, istatistiki ve bilimsel amaçla uzun süreli olarak tutulmasının gerekmesi halinde anonimleştirilmesi gerekmektedir. Bu mümkün değil ise, veri öznelerinin şifrlenmesi gerekmektedir.

⁴⁸² Regulation (EC) No: 45/2001 of the European Parliament and of the Council of 18 December 2000 on the Protection of Individuals with regard to the Processing of Personal Data by the Community Institutions and Bodies and on the Free Movement of Such Data, Art. 1/2 and Chapter V, Art. 41 et al., <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32001R0045> , E.T. 30.10.2018.

⁴⁸³ Regulation (EC) No: 45/2001 of the European Parliament and of the Council of 18 December 2000 on the Protection of Individuals with regard to the Processing of Personal Data by the Community Institutions and Bodies and on the Free Movement of Such Data, Art. 4, <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32001R0045> , E.T. 29.10.2018.

6. 2006/24/AT Sayılı İletişim Trafik Verilerinin Saklanması Direktifi (Kamu İletişim Ağları veya Kamuya Açık İletişim Servislerinde Üretilen veya İşlenen Verilerin Saklanması Direktifi)

2006 yılında yayınlanan Avrupa Parlamentosu'nun 2006/24/AT Sayılı Veri Saklama Direktifi, ciddi suçların soruşturulması, tespit edilmesi ve kovuşturulmasına hizmet etmek için kamuya açık elektronik iletişim ağlarının operatörlerinin ağlarında üretilen veya işlenen belirli verilerin depolanmasını gerektirir. Anılan düzenlemeden etkilenen alanlar, sabit ağ telefonu, mobil telefonun yanı sıra internet erişimi, internet elektronik postası ve internet telefonu gibi mecralarda, iletişimin içeriğine girilmeksizin, trafik ve konum verileridir. Direktif anılan verilerin altı ay ila iki yıl arasındaki bir süre boyunca kayıt altına alınmasını düzenler⁴⁸⁴.

Öncelikle 2006/24/AT Sayılı Direktif'in internet erişimi, internet elektronik postası ve internet telefonu alanlarına dair uygulanacak temel şartlarına bakıldığında hangi verilerin saklanması tasarıldığı anlaşılabilecektir. Buna göre;⁴⁸⁵

- İletişimin kaynağını izlemek ve tanımlamak için gerekli veriler,
- Bir iletişimin varış noktasını tanımlamak için gerekli veriler,
- Bir iletişimin tarih, saat ve süresini belirlemek için gerekli veriler,
- İletişim türünü tanımlamak için gerekli veriler,
- İnternet erişimi, internet e-postası ve internet telefonu ile ilgili kullanıcıların iletişim ekipmanlarını tanımlamak için gerekli veriler.

⁴⁸⁴ Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC, L 105/54, <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32006L0024> , E.T. 08.02.2019.

⁴⁸⁵ Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC, Art. 5, L 105/54, <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32006L0024> , E.T. 08.02.2019.

Anılan verilerin saklanması gereğini güden 2006/24/AT Sayılı Direktif'in uygulanması birçok bakımdan tartışmalı olmuştur. Yukarıda belirttiğimiz üzere, içerik verilerinin saklanması kesinlikle yasaktır. Ancak teknik açıdan bakıldığında modern elektronik iletişim altyapısında içerik, trafik veya konum verileri arasındaki sınır bazen belirsizleşmektedir. Ayrıca Direktif'in dili, teknik hususlardan yoksun oluşu sebebiyle belirsizdir⁴⁸⁶.

7. Lizbon Anlaşması

Avrupa Birliği Antlaşması (ABA) ve Avrupa Birliği'nin İşleyişine İlişkin Antlaşma (ABİA) olan iki temel antlaşmayı değiştiren Lizbon Anlaşması, 13 Aralık 2007'de 27 AB üyesi devlet tarafından imzalanmış ve 1 Aralık 2009'da yürürlüğe girmiştir⁴⁸⁷. Lizbon Anlaşması'nın yürürlüğe girmesi, Avrupa veri koruma hukukuna oldukça önemli etkiye bulunmuştur. Bu Anlaşma ile, hem AB Temel Haklar Şartı bağlayıcı hale gelmiş hem de adli ve emniyet işleri bakımından iş birlikleri ile dış işleri ve güvenlik alanlarında ortak bir veri koruması sağlanmıştır⁴⁸⁸.

Lizbon Antlaşması'nın yürürlüğe girmesinden bu yana, AB hukukunda temel haklara ilişkin ana hüküm, AB Anlaşması'nın 6. maddesidir. Bu anlaşma ile öncelikle Avrupa Temel Haklar Şartı'na, AB Anlaşması md. 6/1'deki anlaşmalar ile aynı hukuki değer atfedilmiştir⁴⁸⁹. Dolayısıyla anılan Şart ve kişisel verilerin korunması bağlamında

⁴⁸⁶ Gerald STAMPFEL, Wilfried GANSTERER, Martin ILGER, "Implications of the EU Data Retention Directive 2006/24/EC", *Sicherheit 2008: Sicherheit, Schutz und Zuverlässigkeit*, 2.-4. April 2008, Saarbrücker Schloss, <https://eprints.cs.univie.ac.at/331/1/ImplicationsEUDR.pdf>, E.T. 08.02.2019.

⁴⁸⁷ Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, 13.12.2007, C 306/1, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12007L%2FTXT>, E.T. 17.02.2019.

⁴⁸⁸ 286. maddeyi değiştiren 16 B. maddesi ve 25a. maddesi, Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, 13.12.2007, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12007L%2FTXT>, E.T. 28.05.2019.

⁴⁸⁹ Ingolf PERINCE, "The Treaty of Lisbon and Fundamental Rights", *The Lisbon Treaty- EU Constitutionalism without a Constitutional Treaty*, Stefan GRILLER, Jacques ZILLER (Ed.), European Community Studies Association of Austria (ECSA Austria) Publication Series, Vol. 11, SpringerWienNewYork, 2008, s. 240, ss. 235- 256; Consolidated Version of the Treaty on European Union, Art. 6, 26.10.2012, C 326/13, <https://eur-lex.europa.eu/resource.html?uri=cellar:2bfl40bf-a3f8->

doğaldır ki 8. madde yalnızca AB kurum ve organları için değil, AB hukuku kapsamında hareket eden üye devletler için de bağlayıcı hale gelmiştir⁴⁹⁰. AB Anlaşması'nın 6/2. maddesi ise, AB'nin İHAS'a katıldığını açık bir biçimde dile getirmektedir. 6. maddenin son fıkrası ise, İHAS'ta bulunan ve üye devletlerin ortak anayasal geleneklerinden kaynaklanan temel hakları, AB hukukunun genel ilkelerinden saymaktadır.⁴⁹¹

Avrupa veri koruma hukuku bağlamında ayrıca, kişisel verilerin korunması hakkı AB'nin genel ilkeleri arasında sayılan ve Avrupa Topluluğu Kurucu Anlaşması'nın 286. maddesi yerine geçen AB'nin İşleyişine İlişkin Anlaşma'nın 16/1. maddesinde özel olarak ele alınmıştır. Anılan maddeye göre; *“Herkes, kendisiyle ilgili kişisel verilerin korunması hakkına sahiptir.”* Görüleceği üzere bu fıkra, AB Şartı'nın 8. maddesi ile aynı biçimdedir. AB'nin İşleyişine İlişkin Anlaşma'nın 16/2. maddesi ise, Avrupa Parlamentosu ve Konsey'e, AB yasalarına uygun biçimde veri işleme amacı ile kişisel verilere ilişkin kurallar koyması için yeni bir yasal dayanak sağlar ve bu kurallara uygunluğun bağımsız bir otorite tarafından kontrol edileceğini hatırlatır. Bu doğrultuda AB Anlaşması'nın 39. maddesi de Avrupa Konseyi'nin üye devletler tarafından kişisel verilerin işlenmesi sırasında bireylerin korunmasına ve bu verilerin serbest dolaşımına ilişkin kuralları belirleyen bir karar kabul edeceğini ve bu kurallara uyulmasının bağımsız otoritelerin denetimi altında olduğunu belirtmiştir⁴⁹².

[4ab2-b506-fd71826e6da6.0023.02/DOC_1&format=PDF](http://www.europarl.europa.eu/charter/pdf/text_en.pdf) , E.T. 25.01.2019; Charter of Fundamental Rights of the European Union, Art. 51, 18.12.2000, C 364/, http://www.europarl.europa.eu/charter/pdf/text_en.pdf , E.T. 25.01.2019.

⁴⁹⁰ HUSTINX, "EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation", s. 18- 19, https://edps.europa.eu/data-protection/our-work/publications/speeches-articles/eu-data-protection-law-review-directive_en , E.T. 06.11.2018.

⁴⁹¹ PERNICE, "The Treaty of Lisbon and Fundamental Rights", s. 240; Consolidated Version of the Treaty on European Union, Art. 6, 26.10.2012, C 326/13, https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506fd71826e6da6.0023.02/DOC_1&format=PDF , E.T. 17.02.2019

⁴⁹² Consolidated version of the Treaty on the Functioning of the European Union, Art. 16, 26.10.2012, C 326, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT> , E.T. 25.01.2019.

Bu gelişmelerin tamamı göstermektedir ki, 95/46/AT Sayılı Direktif’te ele alınan bazı ilkeler AB düzeyinde birincil- öncül ilkeler arasına girmiştir.

D. VERİ KORUMA REFORMU

Avrupa Komisyonu, Avrupa’yı dijital çağa uygun hale getirmek ve artık teknolojik gelişmelerin gerisinde kalan 95/46/AT Sayılı Direktif’i yenilemek için Ocak 2012’de AB Veri Koruma Reformu’nu (Reform) gerçekleştirmiştir. Anılan Reform iki temel metinden oluşmaktadır: Bunların ilki, 2016/ 679 Sayılı AB Genel Veri Koruma Tüzüğü’dür (GVKT). İkincisi ise ceza hukuku alanında 2016/ 680 Sayılı Veri Koruma Direktifi’dir. Öncelikle GVKT, kişilerin kişisel verilerini daha iyi kontrol etmelerini sağlamıştır. Aynı zamanda modern ve ortak kurallar, bürokrasiyi azaltmak gayesini gütmektedir. İlaveten tüketicinin güveni güçlendirilerek işletmelerin dijital pazarın olanaklarından en iyi şekilde yararlanması sağlanmaya çalışılmıştır⁴⁹³.

Veri koruma alanında AB nezdinde ilk veri koruma direktifi, yukarıda anlatıldığı üzere, 95/46/AT Sayılı Direktif olmuştur. Bu düzenleme sonrasında yukarıdaki bölümlerde ele alındığı üzere teknolojik gelişmelerdeki hız, metni âtil bırakmıştır. Bunun üzerine 22 Haziran 2011 tarihinde Avrupa Veri Koruma Denetçisi, 'AB'de Kişisel Veri Korumasına dair Kapsamlı bir Yaklaşım' isimli Avrupa Komisyonu görüşü üzerine bir görüş metni yayınlamıştır. Tüm çerçevenin çizilmesi sonrası Avrupa Komisyonu da 25 Ocak 2012’de AB genelinde kapsamlı bir veri koruma reformu için bir taslak sunmuştur. 7 Mart 2012 tarihinde ise Avrupa Veri Koruma Denetçisi, Komisyon’un veri koruma kuralları reform paketine ilişkin bir görüşü kabul etmiştir. Mart 2012’de Madde 29 Çalışma Grubu, veri koruma reformuna dair bir taslak hazırlamıştır. Yaklaşık iki yıl sonra

⁴⁹³ European Commission, Press Release, “Agreement on Commission’s EU Data Protection Reform will boost Digital Single Market”, Brussels, 15.12.2015, http://europa.eu/rapid/press-release_IP-15-6321_en.htm, E.T. 23.02.2019.

12 Mart 2014'te Avrupa Parlamentosu, Genel Kurul'da 621 kabul 10 ret ve 22 çekimser oyla GVKT'ye güçlü bir destek vermiştir⁴⁹⁴.

Avrupa Parlamentosu, Konsey ve Komisyon 15 Aralık 2015 tarihinde, yeni veri koruma kuralları olan AB Genel Veri Koruma Tüzüğü üzerinde bir anlaşmaya varmıştır⁴⁹⁵. Bu düzenleme neticesinde teknolojik gelişmelerin gerisinde kalmayan, çok daha modern ve iş birliğine dayalı bir veri koruma çerçevesi oluşturulmuş ve 14 Nisan 2016'da Avrupa Parlamentosu tarafından onaylanmıştır⁴⁹⁶. Nihayetinde 95/46/AT Sayılı Direktif'i tamamıyla ortadan kaldırıp onun yerini alan GVKT, bir diğer adıyla 2016/679 Sayılı Direktif, 24 Mayıs 2016'da yürürlüğe girmiş ve 25 Mayıs 2018'den beri geçerli olmuştur⁴⁹⁷.

Avrupa Veri Koruma Reformu'nun bel kemiğini oluşturan Genel Veri Koruma Tüzüğü, her ne kadar 95/46/AT Sayılı Direktif'in temel ilkeleri üzerine kurulsun da daha spesifik veri koruma gereklilikleri, daha sert bir uygulama ve daha global bir kapsama sahiptir. Komisyon'un amacı, 95/46/AT Sayılı Direktif'in çeşitli ülkelerdeki farklı uygulamalarının yeknesaklaştırmaktır. Bununla birlikte GVKT ile sınırötesi suçluluk ve terörizm konularında uluslararası iş birliğinin kolaylaşması amaçlanmıştır. Bu düzenleme ile veri özneleri, kişisel verileri kötüye kullanıldığında daha fazla başvuru seçeneği ile

⁴⁹⁴ Paul DE HERT, Vagelis PAPAKONSTANTINOU, "The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?", *Computer Law & Security Review: The International Journal of Technology Law and Practice*, 2016, s. 1-4, ss. 1- 16; "The History of the General Data Protection Regulation, https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en , E.T. 24.02.2019.

⁴⁹⁵ DE HERT, PAPAKONSTANTINOU, "The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?", *The International Journal of Technology Law and Practice*, s. 1-4; European Commission, Press Release, "Agreement on Commission's EU Data Protection Reform will boost Digital Single Market", Brussels, 15.12.2015, http://europa.eu/rapid/press-release_IP-15-6321_en.htm , E.T. 22.02.2019.

⁴⁹⁶ European Commission, Statement, "Joint Statement on the Final Adoption of the New EU Rules for Personal Data Protection, Brussels, 14.04.2016, http://europa.eu/rapid/press-release_STATEMENT-16-1403_en.htm , E.T. 22.02.2019.

⁴⁹⁷ The History of the General Data Protection Regulation, https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en , E.T. 24.02.2019.

birlikte verileri üzerinde çok daha fazla kontrol sahibi olmuşlardır⁴⁹⁸. Ayrıca belirtilmelidir ki, Avrupa Veri Koruma Hukuku'nun yasal düzenlemeler bakımından kabul edilen "Üçüncü Dalga"sı da veri koruma kurallarını yeknesak hale getiren Genel Veri Koruma Tüzüğü ile olmuştur⁴⁹⁹.

Bahis konusu Reform'un bilinen ayağı AB Genel Veri Koruma Tüzüğü'dür⁵⁰⁰. Bunun yanında ceza hukuku alanında hazırlanan Veri Koruma Direktifi de Avrupa Veri Koruma Reformu'nun bir parçasıdır⁵⁰¹. Bu düzenlemeye göre mağdurların, tanıkların ve şüphelilerin verilerinin bir ceza soruşturmasında kolluk tarafından kullanılmasında veya bir kanunun uygulanmasında usulüne uygun olarak korunması amaçlanmıştır. Söz konusu 2016/680 Sayılı Direktif'e göre kolluk kuvvetleri tarafından toplanan veriler⁵⁰²;

- Yasal ve adil bir şekilde işlenmiş olmalıdır.
- Açık, meşru ve belirtilen amaç doğrultusunda toplanmış ve sadece bu amaç doğrultusunda işlenmiş olmalıdır.
- İşlendikleri amaç ile ilgili ve yeterli olmalı, ancak fazla olmamalıdır.
- Doğru ve gerektiğinde güncel olmalıdır.

⁴⁹⁸ DE HERT, PAPAKONSTANTINOU, "The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?", *The International Journal of Technology Law and Practice*, s. 4; European Commission, Press Release, "Agreement on Commission's EU Data Protection Reform will boost Digital Single Market", Brussels, 15.12.2015, http://europa.eu/rapid/press-release_IP-15-6321_en.htm, E.T. 23.02.2019.

⁴⁹⁹ CHARLESWORTH, "CCTV, the GDPR and the Third Wave of Data Protection", *The Watching The Watchers*, s. 4-6.

⁵⁰⁰ European Commission, Press Release, "Agreement on Commission's EU Data Protection Reform will boost Digital Single Market", Brussels, 15.12.2015, http://europa.eu/rapid/press-release_IP-15-6321_en.htm, E.T. 23.02.2019.

⁵⁰¹ Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to 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, and repealing Council Framework Decision 2008/977/JHA, 04.05.2016, L 119/89, <https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=celex:32016L0680>, E.T. 24.02.2019.

⁵⁰² Protecting personal data when being used by police and criminal justice authorities (from 2018), Summaries of EU Legislation, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3A310401_3, E.T. 24.02.2019.

- Kişinin tanımlanmasına izin veren bir formda tutulurken, verinin işleme amacı için gerekenden fazla tutulmamalıdır.
- Yetkisiz veya yasadışı işlemlere karşı koruma da dahil olmak üzere uygun şekilde güvenlik altına tutulmalıdır.

Görüleceği üzere 2016/680 Sayılı Direktif ile ceza kanunu uygulayıcılarının kişisel verilerin kökenine göre artık farklı veri koruma kuralları uygulamalarına gerek kalmamıştır. Bu ise, zamandan ve paradan tasarruf sağlayacak ve suçla mücadelede verimliliği artıracaktır. Aynı zamanda yasalar bağlamında bir yeknesaklık oluşturularak AB genelinde kolluk kuvvetlerinin ceza soruşturmaları için gerekli bilgileri daha etkili bir şekilde paylaşmalarını sağlayarak suçluluk ve terörle mücadelede daha etkin bir sınır ötesi iş birliği de oluşturulabilecektir⁵⁰³.

1. Genel Veri Koruma Tüzüğü'nün Getirdikleri

95/46/AT Sayılı Direktif'in uzun yıllar uygulanması sonucu ortaya çıkmıştır ki, AB üye ülkeleri arasında veri korumanın birbirinde farklı kurallara tabi olması, yasal belirsizliklere yol açmış ve bu belirsizlikler ekonomik faaliyetler bakımından engel teşkil ederek rekabetin bozulmasına sebep olmuştur. Dolayısıyla veri koruma alanında çok daha hızlı ve yeknesak bir etki doğurması için Genel Veri Koruma Tüzüğü, 95/46/AT Sayılı Direktif'in aksine, AB üye ülkelerinin başka bir işlemine gerek kalmaksızın doğrudan uygulanmaktadır. Çünkü AB Hukuku'nda "Direktif" kavramı, tüm üyelerin gerçekleştirmesi gereken hedefleri belirleyen hukuki metinlerdir. Ancak bu hedefin nasıl gerçekleştirileceği hususunda üye ülkeler özgür bırakılmıştır. Dolayısıyla en kısa deyişle direktif bir çerçeve belgedir. İç hukukta bu çerçevenin içeriği çok daha detaylı bir biçimde düzenlenmektedir⁵⁰⁴. Öte yandan 95/46/AT sayılı Direktif'in yerini alan GVKT ise bir tüzüktür. AB Hukuku'nda "Tüzük" kavramı ise, bağlayıcı bir hukuki metindir. Bu

⁵⁰³ European Commission, Statement, "Joint Statement on the final adoption of the new EU rules for personal data protection", Brussels, 14 April 2016, http://europa.eu/rapid/press-release_STATEMENT-16-1403_en.htm, E.T. 24.02.2019.

⁵⁰⁴ "Regulations, Directives and other acts", EU Law, https://europa.eu/european-union/eu-law/legal-acts_en, E.T. 20.04.2019.

bakımdan üye ülkelere doğrudan uygulanmaktadır⁵⁰⁵. Böylece ortak veri koruma kuralları kişisel verilerin serbest akışındaki olası engelleri kaldırmaktadır⁵⁰⁶.

Genel Veri Koruma Tüzüğü, uzun bir müzakere süreci sonrası Nisan 2016'da tamamlanmış ve 25 Mayıs 2018 tarihinde yürürlüğe girmiştir. Bu yenilik, Avrupa'nın o zamana değin uygulamada olan veri koruma hukuku alanında oldukça kapsamlı ve önemli bir düzenlemedir. Bu yeni düzenlemenin kurallarına uymak için çoğu zaman teknik hususlarda yeni mühendislik işlerinin gerçekleştirilmesi, daha evvel mevcut olmayan yazılı Veri Koruma Etki Değerlendirmesi hazırlanması, kapsamlı bir biçimde dahili saklama ve kayıtlama imkanlarının ortaya çıkması, denetleyici ve işleyiciler arasında sözleşme görüşmelerinin yapılması ve birçok durumda AB alanında ikamet eden bir Veri Koruma Görevlisi atanması gerekecektir⁵⁰⁷. Görülmektedir ki, GVKT ile veri koruması güçlenmiş, bireylere yeni veri koruma hakları sağlanmış, kişisel verileri elinde bulunduran kurum ve kuruluşların sorumlulukları artmıştır.

a) Uygulama Alanı

Yeni Tüzük, 95/46/AT Sayılı Direktif'ten çok daha geniş bir alana uygulanabilmektedir. Daha detaylı bir ifade ile GVKT, iki durumda uygulanabilir olmaktadır: Veri işleyicisi ya da veri denetleyicisinin AB'de bulunduğu ve bulunmadığı haller.

GVKT'nin 3. maddesine göre veri denetleyicisi veya işleyicisi olan gerçek veya tüzel kişinin anılan faaliyeti AB sınırları içerisinde gerçekleştirdiğinde Tüzük yer

⁵⁰⁵ “Regulations, Directives and other acts”, EU Law, https://europa.eu/european-union/eu-law/legal-acts_en, E.T. 20.04.2019.

⁵⁰⁶ Paul VOIGT, Axel VON DEM BUSSCHE, *The EU General Data Protection Regulation (GDPR)- A Practical Guide*, Springer International Publishing, 2017, s. 2; AB Hukuk Sistemi'ne ilişkin detaylı bir çalışma için bkz. Abdullah DİNÇKOL, “Bir Pozitif Hukuk Kaynağı Olarak Avrupa Birliği Hukuk Sistemi”, *Hukuk Felsefesi ve Sosyolojisi Arkivi*, S. 22, İstanbul Barosu Yayınları, 2010, ss. 189- 214.

⁵⁰⁷ Daphne KELLER, “The Right Tools: Europe's Intermediary Liability Laws and the EU 2016 General Data Protection Regulation”, *Berkeley Technology Law Journal*, Vol. 33, 2018, s. 329, ss. 297- 377.

bakımından uygulama alanı bulacaktır. Bu ifadeden çıkarılacak önemli bir sonuç ise, verisi işlenen veri öznesinin AB vatandaşı olması şartının aranmadığıdır.

Özellikle anılan ikinci hal, Veri Koruma Reformu'nun getirdiği en önemli yeniliklerden birini oluşturmaktadır. Buna göre GVKT'nin uygulamasında artık “ülkedışılık (extraterritoriality)” prensibi esastır. Bunun anlamı, GVKT'nin uygulanması için artık veri denetleyicisinin AB alanında ikamet etmesi gerekmemektedir. Artık GVKT, AB alanında ikamet eden sakinlerin verilerini işleyen ya da işleme niyeti olan kuruluşlara uygulanmaktadır⁵⁰⁸. AB sınırları içerisinde bulunan kişilerin, AB vatandaşı olmalarına ya da AB’de sürekli bir ikametlerinin bulunmasına gerek yoktur⁵⁰⁹. İlaveten, AB içinde bulunan veri ihracatçısı ve AB dışında bulunan veri ithalatçısı, verilerin korunması adına, AB Standart Sözleşme maddelerine dayanan bir sözleşme yapabilir⁵¹⁰.

Tüzük’ün yer bakımından uygulamasını ortaya koyan 3. madde bağlamında ele alınması gerekli bir diğer düzenleme de AB sınırları içerisindeki veri öznelerine mal veya hizmet sunulduğu hallerde de GVKT'nin uygulama alanı bulacağı hususudur. Söz gelimi AB’de ikamet eden gerçek kişilere yönelik mal ve hizmet sunan bir internet sitesi de bu kapsamda değerlendirilebilmektedir. 3. maddede bulunan ve yer bakımından uygulamayı genişleten son husus ise, AB’de ikamet eden gerçek kişilerin kişisel verilerinin “gözlemlendiği” her olayda Tüzük’ün uygulamaya konulacağına dair düzenlemesidir. Buna göre kişinin özellikle internet hareketlerinin izlenmesini sağlayan her türlü uygulamaya (örneğin *cookies*- çerezler gibi eklentiler, *webtracking* yöntemi, bazı sosyal

⁵⁰⁸ W. Gregory VOSS, “European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield and the Right to Delisting”, Business Lawyer, Vol. 72, No: 1, Winter 2016/ 2017, January 2017, s. 222; Ivan KLEKOVIC, “EU GDPR vs. European Data Protection Directive”, EU GDPR Academy, 30.10.2017, <https://advisera.com/eugdpracademy/blog/2017/10/30/eu-gdpr-vs-european-data-protection-directive/>, E.T. 26.02.2019.

⁵⁰⁹ Mesut Serdar ÇEKİN, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu*, On İki Levha Yayıncılık, İstanbul, 2018, s. 31.

⁵¹⁰ Anılan Standart Sözleşme Maddeleri, Avrupa Komisyonu veya ulusal Denetim Otoriteleri tarafından kabul edilen sözleşmeye bağlı maddelerdir ve tamamen ve değiştirilmeden kullanılırsa, uluslararası veri transferleri için uygun bir koruma görevi görmektedirler. VOIGT, VON DEM BUSSCHE, *The EU General Data Protection Regulation (GDPR)- A Practical Guide*, s. 6.

medya platformlarında beğeniler üzerine *targeted advertising*- hedefli reklam gibi uygulamalar) sahip internet siteleri Tüzük'ün kapsamına girecektir⁵¹¹.

GVKT bakımından ilk defa olarak, AB alanında bulunmayan fakat GVKT'nin uygulaması kapsamına giren kuruluşlar için, AB sınırlarında bir temsilci atanması zorunlu kılınmıştır. Böylece AB'deki temsilci, veri özneleri ve denetim makamları bakımından iletişim kurulacak nokta olacaktır⁵¹².

Görüleceği üzere GVKT kapsamında şirketler, 95/46/AT Sayılı Direktif ile önceden var olan yükümlülüklerin güçlendirilmesinin yanı sıra yeni veri koruma yükümlülükleriyle karşı karşıya kalmışlardır. Kanun koyucu, küresel bir ekonomi ve yeni teknolojilerin zorluklarını olabildiğince göz önüne alarak, çok geniş bir uygulama alanı yaratmıştır. Bu bağlamda hem veri koruma kuralları hem de Tüzük kapsamında verilecek para cezaları arttırılmış ve dolayısıyla uygulama alanı genişleyen GVKT kapsamına giren veya girebilecek olan pek çok şirket, kendi veri koruma prosedürlerini yeni düzenlemeye uyarlamıştır⁵¹³.

Tüzük belirtildiği üzere, Avrupa alanındaki tüketicilerin kişisel verilerini işleyen tüm işletmelere uygulanır. Bu sebeple AB genelinde veri koruma kurallarının tümünü uyumlu hale getirmekte ve tüm süreci basitleştirmektedir. İlaveten hem kamu hem de özel sektör yeni düzenlemenin kapsamındadır. Bazı tahminlere göre GVKT'nin 75.000 veri koruma görevlisi pozisyonu yaratacağı ifade edilmiştir. Ayrıca başka bir tahminde,

⁵¹¹ ÇEKİN, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu*, s. 32- 34.

⁵¹² VOIGT, VON DEM BUSSCHE, *The EU General Data Protection Regulation (GDPR)- A Practical Guide*, s. 5.

⁵¹³ VOIGT, VON DEM BUSSCHE, *The EU General Data Protection Regulation (GDPR)- A Practical Guide*, s. 2; Christina TIKKINEN-PIRI, Anna ROHUNEN, Jouni MARKKULA, "EU General Data Protection Regulation: Changes and implications for personal data collecting companies", *Computer Law & Security Review: The International Journal of Technology Law and Practice*, 2017, s. 2, ss. 1- 20.

GVKT'ye uyumluluğun sağlanması için kurum ve kuruluşların bilgi teknolojileri birimlerinin bütçelerini %16 ile %40 arası artırmaları gerektiği ileri sürülmüştür⁵¹⁴.

b) Kişisel Veri ve Özel Nitelikli Kişisel Veri

Teknolojik gelişmelerin etkisiyle “kişisel veri” kavramı GVKT ile yeniden tanımlanmıştır. Tüzük'ün 4. maddesine göre kişisel veri, belirli ya da belirlenebilir gerçek kişiyle ilgili her türlü veridir. Bu veriler, bir bireyi tanımlamak için kendi başlarına veya diğer verilerle birlikte kullanılabilecek herhangi bir bilgi olarak tanımlanmaktadır. Gerekçe'ye göre elde edilen verilerle üçüncü bir kişi kimlik tespitinde bulunabiliyorsa belirlenebilirlik gerçekleşmiş demektir. Söz gelimi IP adresleri, mobil cihaz tanımlayıcıları, coğrafi konum ve ayrıca parmak izleri, retina taramaları gibi biyometrik veriler kişisel veri kapsamındadır. Bir bireyin fiziksel, psikolojik, genetik, zihinsel, ekonomik, kültürel veya sosyal kimliği ile ilgili verileri de kişisel veri kapsamındadır. Söz konusu tanıma biyometrik ve genetik veriler eklenerek eski düzenlemeye kıyasla daha geniş bir anlayış hâkim olmaktadır. Kişinin profilini çıkarma veya tarayıcı geçmişini ya da satın alma geçmişini kullanarak profillemeye yapmak gibi uygulamalar, artık kişinin açık onayı olmadıkça GVKT bakımından kabul edilemez niteliktedir⁵¹⁵.

Veri öznesinin politik görüşü, dini ve felsefi inancı ya da sağlığı gibi hususlar kişisel verilerin özel kategorilerini (hassas veri) oluşturur. Bu veriler, kişinin özel yaşamına dair yüksek risk oluşturmaları ve ortaya çıktıklarında veri öznesine dair bazı yıkıcı sonuçlara yol açabilme ihtimalleri sebebiyle çok daha özel koruma gerektirir. Bu bakımdan anılan hassas veriler GVKT'de de daha kapsamlı biçimde koruma altındadır.

⁵¹⁴ KELLER, “The Right Tools: Europe’s Intermediary Liability Laws and the EU 2016 General Data Protection Regulation”, s. 329.

⁵¹⁵ KLEKOVIC, “EU GDPR vs. European Data Protection Directive”, <https://advisera.com/eugdpracademy/blog/2017/10/30/eu-gdpr-vs-european-data-protection-directive/>, E.T. 26.02.2019; Samantha BEAUMONT, “The Data Protection Directive versus the GDPR: Understanding key changes”, Synopsys Software Integrity Blog, 18.01.2018, <https://www.synopsys.com/blogs/software-security/dpd-vs-gdpr-key-changes/>, E.T. 27.02.2019; Prasad KRISHNA, “Comparison Table of GDPR- DPD”, Files, The Centre for Internet and Society, 07.02.2017, <https://cis-india.org/internet-governance/files/comparison-table-gdpr-dpd>, E.T. 04.03.2019.

Kural olarak ırk veya etnik kökene işaret eden kişisel veriler, politik görüşler, dini veya felsefi inançlar, sendika üyeliği, genetik veya biyometrik veriler ile kişinin cinsel yaşamı veya cinsel yönelimine ilişkin verilerin işlenmesi yasaktır⁵¹⁶. Bu durumun istisnaları ise GVKT'nin 9. maddesinde detaylı bir biçimde açıklanmaktadır. Buna göre özel kişisel veri kategorilerinin işlenmesi;

- Veri öznesinin açık rızası varsa,
- İstihdam veya sosyal güvenlik bakımından bir gereklilik söz konusu ise,
- Veri öznesinin ya da onun fiziksel ya da hukuki olarak rıza verme yetisine sahip olmadığı durumlarda diğer bir gerçek kişinin hayati çıkarlarını korumak için işlem yapmak gerekiyorsa,
- Bir vakıf, dernek veya kâr amacı gütmeyen başka bir kuruluş tarafından meşru faaliyetleri sırasında, işlemin yalnızca üyelere veya kuruluşun eski üyelerine veya bununla bağlantılı olarak düzenli temas halinde olunan kişilere bağlı olması şartıyla, anılan kuruluşların amaçları ile bağlantılı olarak işlenebilir. Ancak burada veri öznelere onayı olmadan bu veriler doğaldır ki, anılan kurumlar dışında açıklanamaz.
- Hak taleplerinin kullanılması, savunulması veya mahkemelerin yargı yetkisi dahilinde hareket ettikleri hallerde,
- Veri koruma hakkının özüne saygı duymak ve temel hak ve özgürlüklerin çıkarlarını korumak için uygun ve özel önlemler almak şartıyla, orantılı olarak ve meşru amaç doğrultusunda, Birlik veya üye devlet hukuklarında yer alan önemli kamu yararı sebepleri söz konusu ise,
- Koruyucu ya da mesleki tıbbın amaçları, çalışanın çalışma kapasitesinin değerlendirilmesi, tıbbi teşhis, sağlık ya da sosyal bakım ya da tedavi

⁵¹⁶ DE HERT, PPAKONSTANTINOU, “The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?”, *The International Journal of Technology Law and Practice*, s. 5- 6; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), Art. 9, L 119, 04.05.2016, <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX: 02016R0679-20160504> , E.T. 20.03.2019.

sağlanması ya da Birlik ya da üye devlet temelinde sağlık ya da sosyal bakım sistemleri ve hizmetlerinin yönetimi için ya da bir sağlık profesyoneli ile yapılan sözleşme söz konusu ise,

- Halk sağlığı alanında kamu yararı mevcutsa,
- Veri koruma hakkının özüne saygı gösterildiği, veri öznesinin temel haklarını ve çıkarlarını korumak için uygun ve özel önlemlerin mevcut olduğu hallerde, kamu yararı doğrultusunda bilimsel, tarihsel araştırma veya istatistiki amaçlarla

mümkün olabilmektedir.

c) Kişisel Verilerin İşlenme Şartları

GVKT'nin 4/2. maddesine göre veri işleme faaliyeti, “otomatik yöntemlerle olsun veya olmasın, kişisel veri veya kişisel veri setleri üzerinde gerçekleştirilen toplama, kaydetme, düzenleme, yapılandırma, saklama, uyarılma veya değiştirme, elde etme, danışma, kullanma, iletim yoluyla açıklama, yayma veya kullanıma sunma, uyumlaştırma ya da birleştirme, kısıtlama, silme veya imha gibi herhangi bir işlem veya işlem dizisidir.” Görüldüğü üzere veri işleme faaliyeti oldukça geniş kapsamlı bir alanı kapsamaktadır. İşte bu kadar çok işlemi bünyesinde barındıran işleme, GVKT kapsamında belli şartlar dahilinde gerçekleştirilebilmektedir.

En genel biçimi ile Tüzük'ün 5. maddesi kapsamında kişisel verilerin işlenmesine hâkim olan ilkelere bakıldığında kişisel veriler⁵¹⁷;

- Hukuka uygun, adil ve şeffaf biçimde,
- Açık, meşru ve sınırlı amaçlar doğrultusunda,
- Yeterli, yerinde ve gerekli olduğu kadar,
- Doğru ve güncel şekilde,

⁵¹⁷ DE HERT, PAPAKONSTANTINOU, “The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?”, *The International Journal of Technology Law and Practice*, s. 7- 9.

- Sınırlı bir süre için,
- Güvenli biçimde,
- Sorumluluk dahilinde, hesap verilebilir şekilde

işlenebilecektir.

GVKT'nin temel amacına bakıldığında, amacın AB alanındaki veri öznelerine verilerinin kullanılıp kullanılmadığı veya nasıl kullanıldığı konusunda kontrol sağlamak olduğu görülmektedir. Bu noktada ana prensip, kişisel verilerin işlenmemesidir. Bir işleme söz konusu olacak ise de yukarıda anılan veri işlemeye ilişkin temel ilkeler bağlamında “minimum” düzeyde gerçekleştirilmesi gerekir. Bu noktada GVKT öncelikle, herhangi bir kişisel verinin işlenmesi için, bu duruma açıkça rıza gösterilmesini aramaktadır. Ayrıca verinin spesifik olması ve veri öznesinin bilgilendirilmiş olması hususları da bu bakımdan önem taşımaktadır⁵¹⁸. Buna göre veri işleme, kanunen düzenlenmedikçe yasaktır. GVKT'nin “İşleme faaliyetinin hukuka uygunluğu” başlıklı 6. maddesine göre işleme faaliyeti⁵¹⁹;

- Veri öznesinin onay vermesi,
- Veri öznesinin taraf olduğu bir sözleşmenin mevcudiyeti,
- Denetleyicinin tabi olduğu kanuni bir yükümlülük sebebiyle veri işlemenin gerekli olması,
- Veri öznesi ya da başka bir gerçek kişinin hayati menfaatlerinin korunması için işlemenin gerekli olması,
- Kamu yararı veya denetleyicinin resmi bir yetkisinin bulunması,

⁵¹⁸ BEAUMONT, "The Data Protection Directive versus the GDPR: Understanding key changes", <https://www.synopsys.com/blogs/software-security/dpd-vs-gdpr-key-changes/> ; TIKKINEN-PIRI, ROHUNEN, MARKKULA, “EU General Data Protection Regulation: Changes and implications for personal data collecting companies”, s. 14.

⁵¹⁹ DE HERT, PAPAKONSTANTINO, “The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?”, *The International Journal of Technology Law and Practice*, s. 7- 9.

- Veri öznesinin çocuk olduğu hallerde bu kişinin korunması gereken menfaat ve temel hak ve özgürlüklerinin ağır bastığı haller dışında, denetleyici ya da üçüncü kişi tarafından gözetilen meşru menfaatler doğrultusunda işleme faaliyetinin gerekli olması,

durumlarında hukuka uygundur.

Veri işleme için gereken şartların birçoğu 95/46/AT Sayılı Direktif kapsamında düzenlenmiş ve devamında bu hükümler GVKT'ye taşınmıştır. Bunlar genel olarak, geçerli bir rıza, sözleşmeye dayalı bir gereklilik veya veri denetleyicisinin meşru çıkarıdır. Ayrıca bazı hallerde veri işlemenin amacıyla bir değişikliğe izin verilmektedir⁵²⁰.

Bu bağlamda bir diğer önemli nokta da grup şirketlerinin bünyesinde veri işlemenin ne şekilde düzenlendiğidir. Buna göre GVKT grup içi veri aktarımını, üçüncü kişilere veri aktarımı ile aynı şekilde ele almaktadır. Daha açık bir ifade ile grup içi veri transferleri de kanunen düzenlenmelidir⁵²¹.

d) Üçüncü Ülkelere Kişisel Veri Aktarımı

Üçüncü ülkelere veri aktarımı da GVKT'de oldukça kapsamlı biçimde düzenlenmiştir. Buna göre, GVKT'nin 5. Bölümündeki hükümler AB'den üçüncü ülkelere ve uluslararası kuruluşlara veri aktarımını düzenlemektedir. Kişisel verilerin AB dışındaki alıcılara aktarılması durumunda, bu tür bir aktarımın uygun bir düzeyde veri korumasını garanti altına almak için belirli güvencelere tabi olması gerekir. Bu bağlamda

⁵²⁰ VOIGT, VON DEM BUSSCHE, *The EU General Data Protection Regulation (GDPR)- A Practical Guide*, s. 5.

⁵²¹ VOIGT, VON DEM BUSSCHE, *The EU General Data Protection Regulation (GDPR)- A Practical Guide*, s. 5.

kurumlar üçüncü ülkelere veri aktarımı gerçekleştirecekse, iki aşamalı bir yaklaşım sergilemelidir⁵²²;

- Veri işleme faaliyetinin kanuni bir gerekçesi bulunmalıdır.
- Uygun güvenlik önlemleri alınmalıdır.

Buna göre Tüzük'ün 44. maddesine göre üçüncü bir ülke veya uluslararası bir kuruluşa veri aktarımı, veri denetleyicisi ve işleyici tarafından Tüzük'te düzenlenen ilgili hükümlere uyulması şartı ile gerçekleştirilebilecektir. Bu noktada belirtilmelidir ki, Veri Koruma Komisyonu söz konusu üçüncü ülke ya da uluslararası kuruluş ile ilgili olarak, belirli hususları dikkate alarak, yeterli düzeyde koruma sağlandığına ilişkin bir karar verebilir ve aktarım bu karara dayanılarak gerçekleştirilebilir. Bu karar mevcut değil ise, denetleyici veya işleyicinin uygun güvenceleri sağladığı hallerde de veri aktarımı gerçekleştirilebilecektir⁵²³.

Ayrıca bu bağlamda ABD'ye gerçekleştirilen veri transferleri de 95/46/AT Sayılı Direktif de olduğu gibi GVKT'de de "Mahremiyet Kalkanı (Privacy Shield)" kavramı kapsamında ele alınmaktadır. Bu kavram, Avrupa Komisyonu tarafından kabul edilen ve ABD'li kuruluşların uygun bir veri koruma seviyesini sağlamalarına dair hukuki bir çerçeve olup bu kuruluşların sertifika almalarını sağlayan bir sistemdir. Fakat Mahremiyet Kalkanı denen bu sistem, GVKT'ye uygunluk mekanizması değil; veri aktarımına dair şirketlerin GVKT'de bulunan ve kişisel verilerin üçüncü ülkelere aktarımı hususlarını düzenleyen maddeye uygunluğu sağlayan bir düzenlemedir⁵²⁴. Söz konusu Mahremiyet Kalkanı kuralları, Avrupa Adalet Divanı tarafından 6 Ekim 2015 tarihinde

⁵²² VOIGT, VON DEM BUSSCHE, *The EU General Data Protection Regulation (GDPR)- A Practical Guide*, s. 6.

⁵²³ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), Art. 45- 46, L 119, 04.05.2016, <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504> , E.T. 20.03.2019.

⁵²⁴ VOSS, "European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield and the Right to Delisting", s. 231.

geçersiz ilan edilen 2000 yılı Güvenli Liman (*Safe Harbor*) yeterlilik kararının halefi olarak belirlenmiştir⁵²⁵. Anılan Mahremiyet Kalkanı Kurallarına genel olarak bakılacak olursa⁵²⁶;

- *Bildirim İlkesi*: Toplanan verilerin türü, işlenme amacı, erişim ve seçim hakkı, ileriye dönük transfer ve sorumluluk şartları gibi işleme faaliyetlerinin ana unsurları hakkında veri öznelere bilgi verilmesi gerekmektedir.
- *Veri Bütünlüğü ve Amaç Sınırlama İlkesi*: İşlenen kişisel veriler, işleme amacı ile ilgili ve uyumlu olmalı. Ayrıca kullanım amacı için güvenilir, doğru, eksiksiz ve güncel olmalıdır. Bu kural, Mahremiyet Kalkanı kapsamındaki sertifikası bitip bitmediğine bakılmaksızın, işletme kişisel verileri sakladığı sürece bunun garanti edilmesi gerekir.
- *Seçim İlkesi*: Verileri üçüncü şahıslara ifşa edilecekse veya orijinal olarak toplandıklarından farklı veya yeni bir amaç için kullanılacaksa, şirketler veri öznelere bir vazgeçme fırsatı sunmalıdır.
- *İleriye Dönük Transfer için Hesap Verebilirlik İlkesi*: Kurumlar, üçüncü taraf alıcılara veri aktarımı için, Mahremiyet Kalkanı ilkeleri tarafından garanti edilene kadar uygun bir veri koruma düzeyi sağlayacaklarına ve alınan verileri yalnızca sınırlı ve belirli amaçlar doğrultusunda işleme koymakla yükümlü olduklarına dair sözleşmeler imzalamalıdır.
- *Güvenlik İlkesi*: Sertifikalı kuruluşlar, kişisel verilerin işlenmesinde ve kişisel verilerin niteliği dahilinde ortaya çıkan riskleri dikkate alarak kişisel verileri kayıp, kötüye kullanma ve yetkisiz erişim, verilerin açıklaması, verilerde

⁵²⁵ Anılan Güvenli Liman (*Safe Harbor*), Avrupa Adalet Divanı tarafından veri öznelere temel haklarına müdahaleyi sınırlayacak herhangi bir kural veya etkili bir hukuki koruma içermemesi nedeniyle eleştirilmekteydi. Case C-362/14 *Maximillian Schrems v. Data Protection Commissioner*, 06.10.2015, Par. 88-89, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362>, E.T. 21.03.2019.

⁵²⁶ VOIGT, VON DEM BUSSCHE, *The EU General Data Protection Regulation (GDPR)- A Practical Guide*, s. 122- 124; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), Art. 45-46, L 119, 04.05.2016, <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504>, E.T. 14.03.2019.

değişiklik ve imhalardan korumak için makul ve uygun önlemleri almak zorundadır.

- *Erişim İlkesi*: Erişim sağlama yükünün veya masrafının ihlale göre orantısız olması haricinde, veri öznelerinin bir kuruluş tarafından tutulan kendileri hakkındaki verilere erişimi olmalı ve bu verileri doğrulama, hatalı ise değiştirme ve silme yetkilerine sahip olmalıdırlar.
- *İstihdam- İcra ve Sorumluluk İlkesi*: Bireyler, şikâyet ve ihtilafları konusunda bedel ödemediği soruşturma ve sorunlarının süratle çözülmesi için hazır bulunan bağımsız başvuru mekanizmalarına kolayca erişebilmelidir. Bu amaçla, Mahremiyet Kalkanı kuralları bağlamında sertifikalı kuruluşlar kendilerini gönüllü olarak seçilen bir uyumsuzluk çözüm kuruluşuna teslim etmek zorundadır.

e) Veri Öznesinin Hakları

GVKT'nin 12 ile 22. maddeleri arasında veri öznesinin hakları düzenlenmektedir⁵²⁷. Öncelikle 12. maddesine göre veri öznesi, kişisel verilerini işleyen veri denetleyicisinden söz konusu işlemeye dair kapsamlı bilgi alabilmektedir. Bu bilgiyi yazılı ya da sözlü alabileceği gibi, elektronik yollar da dahil olmak üzere diğer yollarla da edinebilecektir. Denetleyici, gerçekleştirdiği veri işlemeye ilişkin bilgileri gecikmeksizin ve her hâlükârda talebin alındığı tarihten itibaren bir ay içerisinde veri öznesine iletmelidir. Söz konusu sürenin yetmediği hallerde, taleplerin karmaşıklığı ve sayısı dikkate alınarak iki ay uzatma verilebilecektir.

Veri öznesi ayrıca kendisi ile ilgili kişisel verilerin işlenip işlenmediğini denetleyiciden teyit etmek hakkına sahiptir. Şayet verilerin işlenmesi söz konusu ise veri öznesi bu verilere erişim hakkına ve GVKT'nin 15. maddesine göre denetleyiciden işlemeye ilişkin şu bilgileri talep etmek hakkına sahiptir;

⁵²⁷ DE HERT, PAPA KONSTANTINOU, "The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?", s. 10- 11.

- İşleme amacı,
- Verilerin kategorileri,
- Verilerin açıklandığı ya da açıklanacağı alıcılar veya alıcı kategorileri,
- Verilerin saklanacağı süre,
- Veri öznesine ilişkin kişisel verilerin düzeltilmesi, silinmesi veya söz konusu verilerin işlenmesinin kısıtlanmasını talep etme veya işleme faaliyetine itiraz etme hakkının bulunup bulunmadığı,
- Bir denetim makamına şikâyetle bulunma hakkı,
- Verilerin veri öznesinden değil de başka kaynaklardan edinilmesi halinde bu kaynaklara ilişkin bilgiler.

Ayrıca GVKT'nin 16. ve 17. maddelerine göre veri öznesinin kişisel verilerin silinmesi veya eksik kişisel verilerin düzeltilmesi hakları da mevcuttur. Unutulma hakkına göre verileri tutmak için yasal bir gerekçe bulunmadığı müddetçe bireyler verilerinin artık işlenmesini istemediğinde verileri silinebilecektir. Bunlar dışında veri öznesinin veri işleme faaliyetinin kısıtlanmasını talep etme hakkı da mevcuttur.

95/46/AT sayılı Direktif'te yer almayan ve GVKT'nin 20. maddesinde ele alınan "Veri Taşınabilirliği Hakkı" da bu bakımdan dile getirilmesi gereken yeniliklerdendir. Buna göre veri öznesi, kendisi ile ilgili olarak bir veri denetleyicisine sağlamış olduğu kişisel verileri, yapılandırılmış, yaygın olarak kullanılan ve makine tarafından okunabilecek bir formatta alma hakkına da sahiptir. Hatta bu bağlamda aldığı verileri kişisel verilerin sağlandığı denetleyicinin herhangi bir engellemesi olmaksızın başka bir denetleyiciye de iletme hakkına sahiptir⁵²⁸. Görüldüğü üzere bu hak veri öznesine oldukça geniş bir hâkimiyet sağlasa da doktrinde kullanımına dikkat edilmesi gerektiği,

⁵²⁸ TIKKINEN-PIRI, ROHUNEN, MARKKULA, "EU General Data Protection Regulation: Changes and implications for personal data collecting companies", s. 14.

aksi halde veri öznesinin kişisel verisini gereğinden fazla erişilebilir kılabilceği ve hakkın varoluş amacına ters düşebileceği belirtilmektedir⁵²⁹.

Veri öznesinin ayrıca bazı icrai hakları da vardır. Bunlardan ilki GVKT'nin 21. maddesinde yer alan itiraz hakkıdır. Bu hakka göre veri öznesi, kendi özel durumuna ilişkin gerekçeli olarak kendisi ile ilgili kişisel verilerin işlenmesine herhangi bir zamanda itiraz etme hakkına sahiptir. Şayet denetleyici, veri öznesinin menfaatleri ile hak ve özgürlüklerinden daha ağır basan meşru gerekçeler göstermedikçe bu kişisel verileri işleyemeyecektir. Bu bağlamda veri öznesi, doğrudan pazarlama amacıyla işlenen kişisel verilere herhangi bir zamanda itiraz etme hakkına da sahiptir.

Veri öznesi kendisine ait verinin ne zaman saldırıya uğradığını bilme hakkına da sahiptir. GVKT'nin 34. maddesine göre veri ihlali veri öznesi olan gerçek kişinin hak ve özgürlükleri açısından yüksek bir riske sebebiyet verecek ise, denetleyici veri ihlalinin gecikmeksizin veri öznesine bildirmelidir. Ayrıca şirketler ve kuruluşlar, ciddi veri ihlallerini ulusal veri denetleme otoritesine mümkün olan en kısa sürede bildirilmeli ve böylece kullanıcılar uygun önlemleri alabilmelidir.

Veri öznesinin önemli haklarından bir diğeri de denetim makamına şikâyetle bulunma hakkıdır. Buna göre veri koruma kurallarının uygulamasından sorumlu olan denetim makamına şikâyetle bulunmak bir “hak” olarak ele alınmaktadır. Buna göre bir veri öznesi, kişisel verilerinin işlendiği bir durumda, bunun GVKT'yi ihlal ettiğini düşündüğünde, diğer yollar saklı kalmak üzere, mutlak mesken, işyeri veya iddia edilen ihlalin olduğu AB üye devleti başta olmak üzere bir Denetim Makamı'na şikayette bulunma hakkına sahiptir⁵³⁰.

⁵²⁹ Barbara ENGELS, “Data Portability among Online Platforms”, *Internet Policy Review- Journal on Internet Regulation*, Vol. 5, Issue: 2, Y. 11.06.2016, s. 2, ss. 1-17.

⁵³⁰ P.T.J. (Pietr) WOLTERS, “The Enforcement by the Data Subject Under the GDPR”, *Journal of Internet Law*, Vol.22, No:8, February 2019, s. 21-22, ss. 21- 31; VOSS, “European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield and the Right to Delisting”, s. 225; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data, and

f) Veri Denetleyicisi ve Veri İşleyicisi

GVKT'nin yürürlüğe girmesi ile kurumlar kendi veri koruma sistemlerinin GVKT ile uyumlu olmalarını sağlamak için bazı yapısal yenilikleri yerine getirmek durumunda kalmıştır. Bu bağlamda her ne kadar kişisel verilerin işlenmesinin amaçlarını ve araçlarını belirleyen gerçek veya tüzel kişi, kamu otoritesi, kurum veya diğer birimleri karşılayan veri denetleyicisi kavramı 95/46/AT Sayılı Direktif'te yer alsa da veri işleyicisi kavramı ilk defa GVKT ile düzenlenmiştir. Buna göre veri işleyicisi, veri denetleyicisi adına verileri işleyen gerçek ya da tüzel kişi, kamu otoritesi, ajans veya başka bir kurumdur. İşleyici aynı zamanda kişisel verilerin güvenliğinden sorumlu olan varlıktır. Ayrıca GVKT'nin 82. maddesinde "Tazminat Hakkı ve Sorumluluk" başlığı altında, veri işleyicisinin doğrudan ilk defa yükümlülüklerini ihlal ettiği için sorumlu tutulabileceği dile getirilmektedir.

Bu noktada kamu kuruluş veya organlarının veri denetleyicisi ya da işleyicisi oldukları hallere ilişkin birkaç husus belirtilmelidir. GVKT'nin 27. maddesine göre AB alanında kurulu olmayan veri denetleyicisi veya işleyicilerinin AB içerisinde temsilci belirlemesi gerekmektedir. Ancak bu zorunluluk kamu kuruluş veya organlarının denetleyici ya da işleyici oldukları hallerde söz konusu değildir. Temsilci bakımından mesele böyle olmakla birlikte GVKT'nin 37. maddesi bakımından ise kamu kuruluş ve organlarının veri denetleyicisi oldukları hallerde bir veri koruma görevlisi belirlemeleri gerekmektedir.

Yeni Tüzük ile artık hem veri denetleyicisi hem de veri işleyicisi mevcut kurallar bakımından müşterek olarak sorumludurlar. Bu durum ise veri aktarımında her ikisinin de sorumlu olduğu yeni bir düzeni ortaya çıkarmıştır. Oysa 95/46/AT Sayılı Direktif'te yalnızca veri denetleyicisi sorumlu tutulmaktaydı⁵³¹. GVKT'de ise veri işleyicisi kişisel

Repealing Directive 95/46/EC (General Data Protection Regulation), Art. 12, L 119, 04.05.2016, <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504>, E.T. 07.03.2019.

⁵³¹ Bu bakımdan veri denetleyicisi ya da veri işleyicisi ayrımı, 95/46/AT sayılı Direktif'in yürürlükte olduğu dönemde çok daha önem taşımaktaydı. Ancak somut olayda şirketin kendini nasıl adlandırdığına değil,

verileri işlemek ve aktarmak istediğinde mutlaka veri denetleyicisi ile bir sözleşme yapmalıdır⁵³².

GVKT'ye göre veri denetleyicisi iki durumda bildirimde bulunma ve bilgi vermeden sorumludur. Bunlardan ilki veri ihlali mevcut olduğunda denetleme makamlarına yapılan bildirimdir. GVKT, veri denetleyicisine kişisel verilerin ihlali durumunda denetleme makamlarına yönelik bir raporlama görevi getirmektedir. Kişisel veri ihlali, ihlalin farkına varılmasından itibaren en geç 72 saat içinde denetim otoritesine bildirmelidir. Eğer denetim otoritesine geç haber verilmişse, mutlaka bir gecikme sebebi sunulmalıdır. Ayrıca veri ihlalinin, hak ve özgürlüklerin kullanımına yüksek risk getirmesi muhtemel olması durumunda, veri öznesine de bilgi vermelidir. Bu durumda veri denetleyicisine denetim makamından destek gelecektir⁵³³.

Söz konusu veri denetleyici ve veri işleyicileri GVKT'ye uygunluklarını kanıtlamak için işleme faaliyetlerinin kayıtlarını tutmak zorundalardır. Düzenlemenin 30. maddesine göre işleme faaliyeti esnasında tutulması gereken kayıtlar⁵³⁴;

gerçekte yaptığı işlemlerin niteliğine bakılmaktaydı. Bu konuda 2006 yılında Belçika Veri Koruma Otoritesi, "Dünya Bankalararası Mali Telekomünikasyon Derneği (SWIFT)" kuruluşuna ilişkin bir soruşturma yürütmüştür. Burada SWIFT her ne kadar tüm müşterileri ile yaptığı sözleşmelerde kendini "veri işleyicisi" olarak adlandırsa da Veri Koruma Otoritesi, SWIFT'in müşterilerinin kişisel verilerini işlevsel biçimde kontrol ettiğini ve müşterilerinin rızası olmadan kişisel verilerini ABD Hükümeti ile paylaştığından bahisle, Belçika Veri Koruma Kanunu'nu ihlal ettiğine hükmetmiştir.

PETERSEN, "GDPR: What (and Why) You Need to Know about EU Data Protection Law", s. 13- 14.

⁵³² VOSS, "European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield and the Right to Delisting", s. 226; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), Art. 28/3, L 119, 04.05.2016, <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504>, E.T. 14.03.2019.

⁵³³ VOIGT, VON DEM BUSSCHE, *The EU General Data Protection Regulation (GDPR)- A Practical Guide*, s. 4; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), Art. 33, L 119, 04.05.2016, <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504>, E.T. 14.03.2019.

⁵³⁴ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of

- Denetleyicinin ve uygun olan hallerde ortak denetleyici, denetleyici temsilcisi ve veri koruma görevlisinin adı ve iletişim bilgileri,
- İşlemenin amaçları,
- Kişisel veri ve veri öznese kategorilerinin bir açıklaması,
- Üçüncü ülkelerdeki veya uluslararası kuruluşlardaki alıcılar dahil olmak üzere kişisel verilerin açıklandığı veya açıklanacağı alıcı kategorileri,
- Mümkünse, üçüncü bir ülkeye veya uluslararası bir kuruluşa kişisel veri aktarımında söz konusu ülke veya uluslararası kuruluşun tanımlanması, 49/1. maddenin ikinci alt paragrafında belirtilen transferlerde belirlenen uygun güvenceler,
- Mümkünse, farklı veri kategorileri için öngörülen zaman sınırlamaları,
- Mümkünse, md. 32/1’de öngörülen teknik ve yapısal güvenlik önlemlerinin genel bir açıklamasıdır.

GVKT’ye göre, veri denetleyicisinin Veri Koruma Kurumu’ndaki online sicile kişisel veri işleme faaliyetleri hakkında bilgi girmesi ve bu bağlamda bir kuruluşun veri işleme kayıtlarını dahili olarak tutma ve isteğe bağlı olarak erişilebilir kılmasının şartı olarak en az 250 çalışanı olması gerekmektedir. Fakat veri işlemenin⁵³⁵;

- Veri öznesinin hak ve özgürlükleri için bir risk oluşturduğu hallerde,
- Ara sıra değil; daimî gerçekleştiği hallerde,
- Özel veri kategorilerine ilişkin olduğu hallerde,
- Ceza mahkumiyeti veya suçlara dair kişisel verilerin işlendiği hallerde,

such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), Art. 30, L 119, 04.05.2016, <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX: 02016R0679-20160504>, E.T. 07.03.2019.

⁵³⁵ KLEKOVIC, “EU GDPR vs. European Data Protection Directive”, <https://advisera.com/eugdpracademy/blog/2017/10/30/eu-gdpr-vs-european-data-protection-directive/>, E.T. 26.02.2019.

kuruluřta 250 alıřan olması řartı aranmaksızın veri iřleme kayıtlarının dahili olarak tutulması mmkn olacaktır.

g) nleyici Veri Koruma- Denetim ve Yaptırım Sistemi

GVKT ncelikli olarak kiřisel verilerin iřlenmesinden doęacak tehlikelerin tespiti ve bunların nlenmesine nem vermektedir. Bu bakımdan veri denetleyicisi ilk elden sorumludur ve bu sorumluluk sebebiyle gereken tedbirleri kendisi belirlemelidir.

Bu baęlamda Tzk'te yer alan yeni bir messese olarak ncelikle, "Veri Koruma Etki Deęerlendirmesi" ele alınmalıdır. GVKT'nin 35. maddesine gre, zellikle yeni teknolojilerin kullanılması amalanan bir veri iřleme faaliyetinin, veri znelerinin hak ve zgrlklerine yksek risk oluřturması muhtemelse, iřletmelerin riskleri azaltmak iin uygun nlemleri belirlemek amaıyla nleyici bir "Veri Koruma Etki Deęerlendirmesi" yapması gerekmektedir. Deęerlendirme sonucunda hangi nlemlerin fayda saęlayacaęı belirlenemiyorsa, denetim makamına danıřılabilir⁵³⁶. Bu deęerlendirme ile amalanan, oluřabilecek riskleri ngrerek minimuma indirmektir. Tzk'n ilgili maddesi, veri iřlemeye ne zaman devam edileceęi, deęerlendirmeye konu olacak bilginin tr, deęerlendirmeye gre yksek risk teřkil eden veri iřleme ncesinde denetim otoritesine danıřmaya iliřkin bilgiler iermektedir⁵³⁷. Ayrıca devam eden iřleme faaliyetleri veya devam eden iřleme faaliyetlerinin risk potansiyelini deęiřtiren bir durum sz konusu olmuřsa, rneęin veri iřleme amalarındaki bir deęiřiklik veya iřlenen verilerin kendisinde bir deęiřiklik olması durumunda, yeniden bir Veri Koruma Etki Deęerlendirmesi sz konusu olabilir. Veri Koruma Etki Deęerlendirmesi iki ařamada gerekleřtirilir;

⁵³⁶ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), Art. 35/1, L 119, 04.05.2016, <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX: 02016R0679-20160504> , E.T. 07.03.2019.

⁵³⁷ VOSS, "European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield and the Right to Delisting", s. 228.

- Veri denetleyicisi iç deęerlendirmeyi yapmaktadır.
- Őayet yüksek bir risk tespit edilirse, Denetim Makamı'na danıřılmaktadır.

Anılan deęerlendirme mutlak surette kiřisel verilerin korunmasını saęlamalı ve GVKT'ye uygunluęu ortaya koymalıdır⁵³⁸.

GVKT'nin daha az denetim, daha çok sorumluluk fikrinden yola çıkarak oluřturduęu bir dięer önleyici müessese de "Veri Koruma Görevlisi (VKG)" belirlenmesidir. Her ne kadar çoęu AB üyesi bu kavramla yeni tanışmıř olsa da veri koruma görevlisi kavramı Alman Veri Koruma Kanunu'nda 30 yılı ařkın bir süredir yer almaktadır⁵³⁹. Buna göre özel kuruluřlar, ana faaliyetleri veri öznelerinin sürekli ve düzenli olarak iřlenmesi veya büyük ölçüde özel veri kategorilerinin iřlenmesi (söz gelimi saęlık verileri) ise, bir veri koruma görevlisi atamakla yükümlüdürler. Veri denetleyicisi ve veri iřleyicisi⁵⁴⁰;

- Őayet veri iřleme, yargı görevini sürdüren mahkemeler harici bir kamu otoritesi veya organı tarafından yürütölmekteyse,
- Veri denetleyicisi veya iřleyicisinin temel faaliyetleri, veri öznelerinin büyük ölçekte düzenli ve sistematik olarak izlenmesini gerektiren iřlemlerden oluřuyorsa,
- Veri denetleyicisi veya iřleyicisinin temel faaliyetleri, 9. madde kapsamında büyük miktarda özel nitelikli veri kategorileri veya 10. madde kapsamında cezai hüküm ve suçlarla ilgili kiřisel veriler kapsamındaysa,

⁵³⁸ VOIGT, VON DEM BUSSCHE, *The EU General Data Protection Regulation (GDPR)- A Practical Guide*, s. 47.

⁵³⁹ VOIGT, VON DEM BUSSCHE, *The EU General Data Protection Regulation (GDPR)- A Practical Guide*, s. 53.

⁵⁴⁰ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), Art. 37, L 119, 04.05.2016, <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504>, E.T. 21.03.2019.

Veri Koruma Görevlisi atayacaktır⁵⁴¹. Şirket gruplarının olduğu hallerde, grup işletmelerinin tamamı veya bir kısmı için tek bir VKG atanabilir. Anılan görevli, şirketin GVKT'ye uygunluğunu izlemek gibi sorumlulukları başarıyla gerçekleştirebilmek için uzmanlığına ve mesleki niteliklerine göre atanmalıdır⁵⁴².

Belirtildiği üzere GVKT, önleyici veri koruma kavramlarına vurgu yapmaktadır. GVKT ile veri koruma alanında ilk defa kuruluşardan özel yaşam kavramını göz önünde bulundurarak ihlal önleyici ürünler geliştirmeleri istenmektedir. Bu kavramlar, tasarımla veri koruma (*privacy by design*) ve varsayılan ayarlarla veri koruma (*privacy by default*) olarak karşımıza çıkmaktadır. Tasarımla veri koruma, bir kuruluş içerisindeki farklı bölümler tarafından ürün ve hizmetlere dair süreçlerde veri koruma ilkeleri dikkate alınarak ürün tasarlanması, politika ve ürün gelişiminin sağlanması ve veri koruma amaçlı önlemlerin en erken şekilde alınmasını sağlar. Bu durum özellikle büyük işleme faaliyetleri olan işletmelerle ilgilidir. Varsayılan ayarlarla veri koruma ise, bir kuruluşun uyguladığı prosedürleri ve ayarları ifade eder. Bu bakımdan, yalnızca belli amaçlarla veri toplanması, ancak gereken asgari miktarda verinin saklanması ve sadece gereken süre içerisinde verinin muhafazası kapsam dahilindedir⁵⁴³.

⁵⁴¹ VOIGT, VON DEM BUSSCHE, *The EU General Data Protection Regulation (GDPR)- A Practical Guide*, Springer International Publishing, 2017, s. 53.

⁵⁴² VOIGT, VON DEM BUSSCHE, *The EU General Data Protection Regulation (GDPR)- A Practical Guide*, s. 3; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), Art. 37, L 119, 04.05.2016, <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504>, E.T. 07.03.2019.

⁵⁴³ VOIGT, VON DEM BUSSCHE, *The EU General Data Protection Regulation (GDPR)- A Practical Guide*, s. 4; PETERSEN, "GDPR: What (and Why) You Need to Know about EU Data Protection Law", s. 15- 16; TIKKINEN-PIRI, ROHUNEN, MARKKULA, "EU General Data Protection Regulation: Changes and implications for personal data collecting companies", s. 14- 15; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), Art. 25, L 119, 04.05.2016, <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504>, E.T. 07.03.2019.

Yukarıda veri işleme faaliyetlerinin kayıtlarının tutulması şartından bahsederken ele alındığı üzere, kurum ve kuruluşlar kişisel verilerin korunmasını güvence altına almak için yeni Tüzük kapsamında teknik ve yapısal bazı güvenlik önlemleri almalıdır. Bu bağlamda uygun veri koruma seviyesi, somut olaya göre, her veri işleme faaliyetinde doğabilecek risk potansiyeline göre belirlenmelidir. GVKT’de ele alınan bazı güvenlik önlemlerine bakacak olursak⁵⁴⁴;

- Bir veri kaydındaki kişisel olarak tanımlanabilir bilgi alanlarının bir veya daha fazla yapay tanımlayıcı veya takma ad ile değiştirildiği bir veri yönetimi ve tanımlama prosedürü olan takma adlandırma- maskeleye⁵⁴⁵ ve kişisel verilerin şifrelenmesi,
- İşleme sistem ve servislerinin devam eden gizliliğinin, bütünlüğünün, kullanılabilirliğinin ve esnekliğinin sağlanması;
- Fiziki veya teknik bir sorun halinde durumu ve kişisel verilere erişimi zamanında düzeltebilme yeteneği;
- Veri işleme güvenliğini sağlamak için teknik ve yapısal önlemlerin etkinliğini düzenli olarak test etme, inceleme ve değerlendirme,

imkanlarının bulunduğu görülür.

Bunların dışında GVKT’nin düzgün biçimde uygulanması amacı ile, zorunluluk teşkil etmese de “Davranış Kuralları ve Belgelendirme” adı altında bulunan düzenlemeler sayesinde Tüzük’e uygunluğun incelenmesi imkânı da sunulmaktadır. GVKT’nin 40. maddesine göre Davranış Kuralları, belirli bir sektör veya teknoloji için GVKT kapsamındaki yükümlülükleri belirtmektedir. Belgelendirme ise, belgeli- sertifikalı

⁵⁴⁴ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), Art. 32, L 119, 04.05.2016, <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504> , E.T. 07.03.2019.

⁵⁴⁵ Gabe MALDOFF, “Top 10 operational impacts of the GDPR: Part:8- Pseudonymization”, *The International Association of Privacy Professionals*, 12.02.2016, <https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-8-pseudonymization/> , E.T. 07.03.2019.

faaliyetlerin Tüzük ile uyumluluğunu ortaya koymaktadır. Anılan düzenlemelerin kullanılması, GVKT'ye uygunluğu denetleme makamlarına ispatlamak için önem arz etmektedir⁵⁴⁶.

GVKT'nin getirdiği en temel değişikliklerden biri de idari cezalar bakımından olmuştur. Burada iki farklı durum karşımıza çıkmaktadır⁵⁴⁷;

- Veri işleyici veya veri denetleyicisinin GVKT bakımından yükümlülüklerini ihlal ettikleri, kurallara uymadıkları halde (non-compliance), 10 milyon €'ya kadar para cezası veya şirketin dünya çapındaki gelirinin %2'sine tekabül eden para cezasından hangisi daha yüksekse ona hükmedilir.
- Rızanın koşullarını ihmalî (negligence) ve veri öznesinin haklarının ihlali durumunda ise, 20 milyon €'ya kadar para cezası veya şirketin dünya çapındaki gelirinin %4'üne tekabül eden para cezasından hangisi daha yüksekse ona hükmedilir.

Ayrıca icrai bakımdan Denetim Makamları'nın görev ve soruşturma yetkileri genişletilmiştir. Buna göre Denetim Makamları'nın görevleri iki kategoriye ayrılmaktadır⁵⁴⁸;

⁵⁴⁶ VOIGT, VON DEM BUSSCHE, *The EU General Data Protection Regulation (GDPR)- A Practical Guide*, s. 5; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), Art. 40, L 119, 04.05.2016, <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504>, E.T. 14.03.2019.

⁵⁴⁷ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), Art. 83, L 119, 04.05.2016, <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504>, E.T. 22.03.2019.

⁵⁴⁸ VOIGT, VON DEM BUSSCHE, *The EU General Data Protection Regulation (GDPR)- A Practical Guide*, s. 201; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), Art. 57,

- GVKT'nin uygulanması ve uygulanmasının izlenmesi gibi veri öznesinin hak ve özgürlüklerinin derhal korunmasına hizmet eden görevler.
- Veri koruma konusunda kamu bilincini teşvik etmek, ilgili taraflara bilgi ve tavsiye sağlamak, diğer Denetim Makamları ile iş birliği yapmak gibi dolaylı olarak bu amaca hizmet edecek görevler.

Denetim Makamları'nın soruşturma yetkileri de GVKT'nin 58. maddesinde düzenlenmektedir. Öncelikle GVKT tüm AB ülkelerinde uygulanabildiği için, soruşturma yetkileri tüm AB genelinde söz konusu olacaktır. Denetim Makamları'nın soruşturma yetkileri⁵⁴⁹;

- Veri denetleyicisi ve veri işleyicisi veya gerekli yerlerde bunların temsilcisinden görevlerinin yerine getirilmesi için ihtiyaç duyduğu her türlü bilgiyi sağlamasını emretmek,
- Veri koruma denetimleri biçiminde soruşturmalar yürütmek,
- Madde 42/7 uyarınca verilen sertifikalar hakkında bir inceleme yapmak,
- GVKT'nin ihlal edildiği iddiasını veri denetleyicisi veya işleyicisine bildirmek;
- Görevlerinin yerine getirilmesi için denetleyici ve işleyiciden gereken tüm kişisel verilere ve tüm bilgilere erişim sağlamak,
- Birlik veya üye devlet usul kanunlarına uygun olarak, herhangi bir veri işleme ekipmanı ve aracı dahil olmak üzere denetleyicinin ve işleyicinin herhangi birine erişim sağlamak,

L 119, 04.05.2016, <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504>, E.T. 22.03.2019.

⁵⁴⁹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), Art. 58, L 119, 04.05.2016, <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504>, E.T. 22.03.2019.

şeklinde ele alınmaktadır. Soruşturma yetkilerinin kullanılması, Denetleme Makamı'nın tabi olduğu ilgili AB Üye Devlet usul kanunları doğrultusunda gerçekleşecektir. Dolayısıyla farklı Denetim Makamları için farklı ulusal usuli düzenlemeler söz konusu olabilecektir. Her bir soruşturma, olayın kendine özgü koşulları göz önünde bulundurularak uygun, gerekli ve orantılı olacaktır⁵⁵⁰.

GVKT 82. maddesinde, "Tazminat Hakkı ve Sorumluluk" başlığı altında, veri işleyicisinin doğrudan ilk defa yükümlülüklerini ihlal ettiği için sorumlu tutulabileceği dile getirilmektedir. Bu nedenle, veri işlemeye katılan tüm kuruluşlar gelecekte potansiyel olarak sorumlu tutulabilecektir. Bir ihlal sonucu maddi veya manevi bakımdan zarar gören herhangi bir kişi ise, yaşanan zarara ilişkin olarak denetleyici veya işleyiciden tazminat alma hakkına sahiptir⁵⁵¹.

Yine bu bağlamda GVKT'nin idari para cezalarına ilişkin hükümleri kesin değildir; çünkü Denetim Makamları'nın para cezası uygulama yetkisi AB üye devletlerinin hukukları doğrultusundadır. Şayet GVKT, AB üye devletlerinin iç hukuklarına aykırı bir düzenleme içeriyorsa, Denetim Makamları cezai ve idari başka cezalar da verebilmeye yetkilidirler⁵⁵². Denetim Makamları GVKT'nin ihlal edildiği hallerde başka bazı düzeltici yetkilere de sahiptirler. Buna göre⁵⁵³;

⁵⁵⁰ VOIGT, VON DEM BUSSCHE, *The EU General Data Protection Regulation (GDPR)- A Practical Guide*, s. 204.

⁵⁵¹ VOIGT, VON DEM BUSSCHE, *The EU General Data Protection Regulation (GDPR)- A Practical Guide*, s. 205- 206.

⁵⁵² Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), Art. 83- 84, L 119, 04.05.2016, <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504>, E.T. 23.03.2019.

⁵⁵³ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), Art. 58, L 119, 04.05.2016, <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504>, E.T. 23.03.2019.

- Amaçlanan veri işleme faaliyetinin GVKT'yi ihlal etmesinin muhtemel olduğu durumlarda veri denetleyicisi ve veri işleyicisine uyarı vermek.
- Amaçlanan veri işleme faaliyetinin GVKT'yi ihlal etmesinin muhtemel olduğu durumlarda veri denetleyicisi ve veri işleyicisine kınama cezası vermek.
- Veri denetleyicisi ve işleyicisine, veri öznesinin haklarını GVKT kapsamında kullanma taleplerine uyması için talimat vermek.
- Veri denetleyicisi ve işleyicisine işlem operasyonlarını, uygun olduğu durumlarda, belirtilen bir şekilde ve süre de GVKT ile uyumlu hale getirmesini emretmek.
- Veri denetleyicisine, şayet bir kişisel veri ihlali varsa veri öznesi ile iletişim kurmasını emretmek.
- Veri işlenmesine geçici veya kesin bir sınırlama getirmek.
- Kişisel verilerin işlenmesinin düzeltilmesi, silinmesi veya sınırlandırılmasını emretmek ve verilerin açıklandığı alıcılara anılan işlemleri bildirmek.
- GVKT bağlamında gereken şartları taşıyan kuruluşlara verilen sertifikaları, gerekli görülen durumlarda geri çekmek veya gerekli şartları taşımadığı ya da sonradan taşımadığı görülen kuruluşların sertifikalarının iptali ya da sertifika verilmemesi hususlarında sertifikasyon kuruluşuna emretmek.
- Her bir vakanın özelliklerini dikkate alarak yukarıda belirtilen diğer düzeltici önlemler yerine idari para cezası vermek.
- Üçüncü ülke alıcılarına veri akışının askıya alınmasını emretmek.

Denetim Makamları'nın düzeltici yetkileri bunlar olmakla birlikte, AB kanun koyucusunun öncelikli tercihi genelde idari para cezaları yönünde olmaktadır. Bu nedenle ilgili kuruluşlar GVKT'ye uygun davranma ve Denetim Makamları'nın direktifleri konusunda oldukça özenli olmalıdır⁵⁵⁴.

⁵⁵⁴ VOIGT, VON DEM BUSSCHE, *The EU General Data Protection Regulation (GDPR)- A Practical Guide*, s. 210.

GVKT'ye uyulmadığı durumlarda gerek idari paza cezaları gerekse düzeltici işlemler yukarıdaki gibi olmakla birlikte, ayrıca iç hukuk yolları bakımından da bazı düzenlemeler mevcuttur. Öncelikle GVKT, veri işlemeye dair farklı taraflar için yargı yolları sunmakta, fakat bir mahkemenin bir davayı ele almasına dair kuralları öngörmemektedir⁵⁵⁵. Bu bağlamda GVKT'nin 78. maddesi, bir denetim makamına karşı etkili bir iç hukuk yoluna başvurma⁵⁵⁶ hakkını ele almaktadır. Söz konusu düzenlemeye göre, başka bir idari veya adli olmayan çözüm yoluna başvurulmasına engel olunmaksızın, her gerçek veya tüzel kişinin bir Denetim Makamı'nın kendileriyle ilgili yasal bağlayıcılığı olan bir kararına karşı etkili bir iç hukuk yoluna başvurma hakkı vardır. Ayrıca yetkin olan Denetim Makamı'nın üç ay içerisinde bir şikayeti ele almadığı veya yapılan bir şikayetin seyri veya sonucu hakkında veri öznesini bilgilendirmediği hallerde söz konusu veri öznesinin, diğer yolları saklı kalmak kaydıyla, etkili bir kanun yoluna başvurma hakkı vardır. Bu düzenleme, veri denetleyici ve işleyicilerine Denetleme Makamları'nın kararlarına mahkemeler önünde hesap sorabilme imkânı vermektedir. Bir Denetim Makamı'na karşı açılacak davalar, söz konusu Denetim Makamı'nın kurulu bulunduğu AB üye devletinin ulusal usul hukukuna göre ve o ülke mahkemelerinde açılır⁵⁵⁷.

⁵⁵⁵ VOIGT, VON DEM BUSSCHE, *The EU General Data Protection Regulation (GDPR)- A Practical Guide*, s. 214.

⁵⁵⁶ Tüzük'ün orijinal İngilizce metninde bu ifade “*an effective judicial remedy*” biçiminde yer almaktadır. Avrupa Birliği Bakanlığı tarafından yapılan çeviride ise söz konusu ifade “*etkili bir kanun yolu*” olarak ele alınmıştır. Ancak Tüzük'te kastedilenin etkili bir iç hukuk yolu olduğu görülmektedir.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), Art. 58, L 119, 04.05.2016, <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504> , E.T. 23.03.2019; Avrupa Birliği Resmî Gazetesi, 4.5.2016, L 119/1, md. 78, <https://www.kisiselverilerinkorunmasi.org/wp-content/uploads/2017/09/GDPR-Türkçe-Çeviri-AB-Bakanlığı.pdf> , E.T. 16.05.2019.

⁵⁵⁷ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), Art. 78, L 119, 04.05.2016, <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504> , E.T. 23.03.2019.

GVKT'nin 77. maddesi ise, veri öznesi bakımından bir Denetim Makamı'na şikâyetle bulunma hakkını ele almaktadır. Buna göre bir veri öznesi, kişisel verisi işlendiğinde bunun GVKT'yi ihlal ettiğini düşündüğünde, diğer yollar saklı kalmak üzere, mutlak mesken, işyeri veya iddia edilen ihlalin olduğu AB üye devleti başta olmak üzere bir Denetim Makamı'na şikâyetle bulunma hakkına sahiptir. Öte yandan söz konusu veri öznesi, GVKT'nin 79. maddesi uyarınca bir veri denetleyicisi veya veri işleyicisine karşı da yargı yoluna gidebilmektedir. Bahis konusu dava, bir denetleyici veya bir işleyiciye karşı, bunların bir işletmesinin bulunduğu AB üye devletinin mahkemelerinde açılır. Veri denetleyicisi veya işleyicisi üye devletin kamu yetkilerinin kullanımı ile ilgili hareket eden bir kamu kuruluşu değilse, veri öznesinin mutlak meskeninin bulunduğu AB üye devletinin mahkemelerinde açılabilir.

h) Yeni Teknolojiler Bağlamında Veri İşleme

GVKT bakımından getirilen bazı başka değişikliklere, ortaya çıkan yeni alanlar kapsamında değinmek gerekmektedir. Buna göre teknik değişim ve gelişmeler, veri işleme alanında yeni yollar ve seçenekler doğurmaktadır. Bu durum özellikle oldukça büyük ölçeklerde verilerin işlenebilmesinin giderek hızlandığı, kolaylaştığı ve maliyetlerinin düştüğü günümüz dünyasında önem taşıyor hale gelmiştir. Bu doğrultuda, veri işleme bakımından kuruluş ve işletmeler için yeni fırsatlar doğarken, bireylerin haklarının korunması bakımından oldukça riskli durumlara sebebiyet verme ihtimalini de barındırmaktadır. Dolayısıyla veri öznesinin haklarının korunması için GVKT belli bazı hükümleri genel ve soyut biçimde düzenlemiştir. Bu durum aynı zamanda her gün ilerleme gösteren bu alanda teknolojik gelişmelere ayak uydurarak GVKT'nin yaşayan bir enstrümana dönüşmesini de sağlamak içindir. Bu noktada büyük veri (*big data*), bulut bilişim (*cloud computing*), *blockchain* ve nesnelerin interneti (*internet of things*) gibi özel veri işleme faaliyetleri ele alınmaktadır.

"Büyük Veri (*big data*)" terimi, teknik bir ifadeden ziyade, veri işlemeye yönelik belirli bir yaklaşımı ifade eder. Veri işleme sürecinde birçok işletme, geniş veri kümelerini toplayabilen, işleyen, sınıflandıran ve analiz edebilen teknolojilere sahiptir.

İşlenen bu verilerden de belli bir getiri sağlamaktadırlar. Büyük veri uygulamaları gerçek verileri işlese de bu yolla insan davranışlarını anlayıp tahmin etmek ve hatta yönlendirmek için oldukça büyük miktarlarda veri kullanır. Bu durum, hedefli reklamcılık ya da makro ve mikro düzeyde kullanıcı davranış analizleri biçimindeki kavramlarla büyük veri bağlamında ortaya çıkar⁵⁵⁸.

Büyük veri, kişisel veri içerdiği anda GVKT'nin kapsamına girmektedir. Şayet kuruluşlar GVKT'nin uygulamasına dahil olmak istemiyorlarsa, ellerindeki verileri anonimleştirebileceklerdir. Büyük veri uygulamalarında, her ne kadar gerçek veriler kullanılsa da zamanla biriken mevcut bilgiler anonimleşmektedir. Fakat biriken anonim bilgilerle son işlenen gerçek verilerin birleştirilmesi neticesinde ortaya çıkan veriler belirli kişilerle kolaylıkla ilişkilendirilebilir. Bu ise, anonimleştirmenin her zaman bir çözüm olmadığını ortaya koymaktadır; çünkü bu şekilde kişiler yeniden tanımlanarak ortaya çıkarılabilecektir⁵⁵⁹.

Veri öznesi olan tüketicilerin, sosyal medya, mobil cihazlar, oyun platformları ve online video sistemleri gibi teknolojik mecralar üzerinden internet üzerindeki tüm hareketlerini takip ederek dijital hedef profillerinin oluşmasını sağlayan teknolojiye sahip günümüzün bazı dijital veri pazarlamacıları adeta yeni bir “Vahşi Batı” olan “Büyük Veri Çağı” olarak adlandırmaktadır⁵⁶⁰. İşte bu gibi büyük veri işleme faaliyetinde ortaya çıkan veri öznelerinin davranış analizleri neticesinde özellikle profil çıkarma, AB kanun koyucusunun oldukça önem verdiği ve GVKT'nin 22. maddesinde yer verdiği bir kavramdır. Buna göre, veri öznesinin kendisi ile ilgili hukuki sonuçlar doğuran veya

⁵⁵⁸ VOIGT, VON DEM BUSSCHE, *The EU General Data Protection Regulation (GDPR)- A Practical Guide*, s. 235- 236; Christopher KUNER, Fred H. CATE, Christopher MILLARD, Dan Jerker B. SVANTESSON, “The Challenge of ‘Big Data’ for Data Protection”, *International Data Privacy Law*, Vol. 2, No: 2, Y: 2012, s. 47, ss. 47- 49; Abid MEHMOOD, Iynkaran NATGUNANATHAN, Yong XIANG, Guang HUA, Song GUO, “Protection of Big Data Privacy”, *IEEE Access*, Vol. 4, Y: 2016, s. 1821, ss. 1821- 1834.

⁵⁵⁹ KUNER, CATE, MILLARD, SVANTESSON, “The Challenge of ‘Big Data’ for Data Protection”, s. 48.

⁵⁶⁰ Jeff CHESTER, “Cookie Wars: How New Data Profiling and Targeting Techniques Threaten Citizens and Consumers in the ‘Big Data’ Era”, *European Data Protection: In Good Health?*, Eds. Serge GUTWIRTH, Ronald LEENES, Paul DE HERT, Yves POULLET, Springer, 2012, s. 53, ss. 53- 78.

benzer biçimde kendisini kayda değer şekilde etkileyen profil çıkarma da dahil olmak üzere yalnızca otomatik işleme faaliyetine dayalı bir karara tabi olmama hakkı bulunmaktadır. İlaveten büyük verilerin GVKT'ye uygun biçimde işlenmesine dair diğer bir önemli nokta da şeffaflık ilkesi doğrultusunda veri öznelerine kişisel verilerinde gerçekleştirilen faaliyetler hakkında bilgi verilmesi gereğidir. Dolayısıyla veri denetleyicisi, verinin işlenmesinden önce veri öznesine, işlemenin amaçları, yasal dayanağı, bilginin kaynağı ve denetleyicinin kimliği hakkında bilgi vermekle yükümlüdür. Fakat büyük veri işlemelerinde, verilerin hangi amaçla işlendiğinin ortaya konması oldukça zor olacaktır; çünkü büyük verileri işleyen ticari kuruluşlar büyük verileri ticari amaçlarla nasıl kullanılabileceğini anlamak için büyük miktarda veri işlerler. Bu sebepten dolayı verilerin işlenme amacı, işlemenin sonucu olarak ortaya çıkar; verinin işlenmesinin öncesinde belli olmaz. Ancak amaç sınırlaması ilkesine göre de kişisel veriler yalnızca açık ve meşru amaçlar için toplanılacaktır. İşleme amacı ne kadar genel olursa, risk daha da artacağı için korumanın kapsamının da artması gerekmektedir⁵⁶¹.

Bir diğer özel veri işleme faaliyeti de bulut bilişim (cloud computing) sahasında gerçekleşmektedir. Buna göre bulut bilişim, bilişim teknolojisi uygulamalarının internet tabanlı kullanımına ve dağıtımına, işlem kapasitesine, depolama alanına odaklanan bir dizi teknoloji ve hizmet modelinden oluşur. Söz konusu kavramın henüz net bir tanımı yapılamasa da oldukça geniş bir tanım yelpazesi olduğu belirtilmektedir. Burada kavramın en geniş tanımı olarak kabul edilen Amerikan Ulusal Standartlar ve Teknoloji Enstitüsü'nün tanımını vermek gerekirse bulut bilişim, istenilen bir bilginin paylaşımlı bir bilgisayar kaynak havuzundan çok az bir efor ile hızlı bir şekilde edinilip dağıtılabilmesini sağlayan ve anılan havuza her yerden, her zaman, kolaylıkla

⁵⁶¹ Antoni ROIG, "Safeguards for the Right not to be Subject to a Decision based solely on Automated Processing (Article 22 GDPR)", *European Journal of Law and Technology*, Vol. 8, No: 3, Y: 2017, <http://ejlt.org/article/view/570/771>, E.T. 01.06.2019; VOIGT, VON DEM BUSSCHE, *The EU General Data Protection Regulation (GDPR)- A Practical Guide*, s. 238.

erişilebilmesini amaç edinmiş bir modeldir⁵⁶². Daha açık bir şekilde ve en kısa şekliyle, istenilen verinin internet üzerinden kullanımı olarak tanımlanabilecektir. Söz gelimi Google Drive, Apple Icloud, Dropbox ya da Microsoft SkyDrive gibi hizmetler istenilen yer, zaman ve mekânda internet üzerinde veri depolamayı ve kullanmayı sağlayan sanal sistemler bulut bilişim örnekleri olarak anılabilecektir. Görüleceği üzere bu hizmetler oldukça hızlı, kolay, düşük maliyetli veri depolama imkânı yaratmaktadır. Ancak öte yandan bulut bilişimde verilerin tam olarak hangi kontrol merkezinde tutulduğu, kimlerin bu verilere erişim sağlayabildiği, kimlerin sorumlu olduğu gibi birçok alanda sıkıntılar mevcuttur⁵⁶³. Ayrıca bu hizmetler sayesinde bilişim teknolojilerinin bir kısmı giderek herkes için erişilebilir ve uzmanlık gerektirmeyen bir hale evrilmekte ve bu durum veri güvenliğini de katlanarak riske etmektedir⁵⁶⁴.

İşte bu bağlamda kişisel veriler bulut bilişim sistemleri tarafından işlenmekte; ancak veri işleme süreci bulut bilişim servis sağlayıcıları tarafından sürdürülmektedir. Böylece GVKT kapsamında bulut bilişimde bulut hizmetlerinin müşterileri veri denetleyicisi; bulut servis sağlayıcıları da veri işleyicisi olarak kabul edilmektedirler. Fakat yine de kurumlararası sorumlulukların dağılımında her spesifik durum kendi şartları içinde değerlendirilmelidir. Söz gelimi bulut servis sağlayıcısının veri işleme araç ve amaçları üzerinde etkisi ne kadar fazlaysa, GVKT bakımından veri denetleyicisi olarak nitelendirilme ihtimali o kadar yüksektir⁵⁶⁵. Şayet bulut hizmet müşterisi veri

⁵⁶² Caesar WU, Rajkumar BUYYA, “Cloud Computing”, *Cloud Data Centers and Cost Modelling- A Complete Guide to Planning, Designing and Building a Cloud Data Center*, Morgan Kaufmann, 2015, s. 31, ss. 3- 41.

⁵⁶³ Bilge NARİN, Sevdâ ÜNAL, “Ünlü Fotoğraflarının Sızdırılmasındaki Etik Sorunlar: Türkiye Medyası Örneği”, *İletişim Hakkı ve Yeni Medya- Tehditler ve Olanaklar*, Eds. Tezcan DURNA, Mutlu BİNARK, Günseli BAYRAKTUTAN, Umag Vakfı Yayınları, 2019, s. 121, ss. 119- 138.

⁵⁶⁴ Bob DUNCAN, “Can EU Data Protection Regulation Compliance be Achieved When Using Cloud Computing?”, *Cloud Computing 2018: The Ninth International Conference on Cloud Computing, GRIDs, and Virtualization*, Eds. Bob DUNCAN, Yong Woo LEE, Aspen OLMSTED, 18- 22 February 2018, s. 1, ss. 1- 6; Article 29 Data Protection Working Party, Opinion 05/ 2012 on Cloud Computing, WP 196, 01.07.2012, s. 4, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf, E.T. 24.03.2019.

⁵⁶⁵ Article 29 Data Protection Working Party, Opinion 05/ 2012 on Cloud Computing, WP 196, 01.07.2012, s. 8, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf, E.T. 25.03.2019.

denetleyicisi olarak nitelendirilirse, GVKT bakımından uygun bir veri işleyicisi seçmek durumunda kalacaktır. Denetleyici veri işlemeyi kendi başına gerçekleştiremeyip bir bulut servis sağlayıcısına gönderdiğinde, denetleyici artık verilerin kontrolünü bütünüyle elinde tutamayabilir ve verileri korumak için gereken önlemleri alamaz. Dolayısıyla şayet ortada denetleyicinin veri işlemeyi bir bulut servis sağlayıcısına gönderdiği bir durum varsa, seçilen bulut servis sağlayıcısı veri işleme süreci için gereken uygun güvenlik önlemlerini almak zorundadır⁵⁶⁶. Ancak yine de GVKT'ye göre veri işlemekten esas sorumlu veri denetleyicisi olduğu için, bulut servis sağlayıcısını seçerken mümkün olduğunca veri koruma standartlarına bakılarak karar verilmelidir. Bu bağlamda müşteri ile bulut servis sağlayıcısının veri koruma yükümlülükleri, aralarındaki sözleşmede belirtilmelidir⁵⁶⁷.

Bulut bilişim bağlamında ele alınması gereken son husus da üçüncü ülkelerde yer alan bulut servis sağlayıcılarıdır. Buna göre, bulut bilişimde kişisel verilerin aktarımı genellikle üçüncü ülkelerde yer alan bulut servis sağlayıcılarına yapılmaktadır. Bu durumda AB dışındaki üçüncü bir ülkeye veri aktarımı söz konusu olduğunda, yukarıda belirtildiği üzere bu tür bir aktarımın uygun bir düzeyde veri korumasını garanti altına almak için belirli güvencelere tabi olması gerekmektedir⁵⁶⁸.

Veri işlemede bir başka yeni teknoloji de blockchain'dir. Blockchain teknolojisi, Bitcoin, Litecoin, Ethereum gibi dijital para birimlerinin kullanımı ile adını duyurmaya başlamıştır, çünkü bu birimlerin altyapılarını oluşturmaktadır. Ancak kavram yalnızca bundan ibaret değildir. En basit hali ile blockchain, dijital bilgilerin dağıtılmasını ancak kopyalanmamasını sağlayan bir sistemdir. Burada her bir verinin bir sahibi olmaktadır. Blockchain teknolojisine “*dağıtılmış bir ağda depolanan dijital defter*” biçiminde bir

⁵⁶⁶ Article 29 Data Protection Working Party, Opinion 05/ 2012 on Cloud Computing, WP 196, 01.07.2012, s. 5, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf, E.T. 25.03.2019.

⁵⁶⁷ VOIGT, VON DEM BUSSCHE, *The EU General Data Protection Regulation (GDPR)- A Practical Guide*, s. 240.

⁵⁶⁸ VOIGT, VON DEM BUSSCHE, *The EU General Data Protection Regulation (GDPR)- A Practical Guide*, s. 240.

benzetme yapılmaktadır⁵⁶⁹. Daha farklı bir anlatımla blockchain, kriptografi kullanılarak bağlanan, blok adı verilen ve sürekli büyüyen bir kayıt listesidir. Her blok, kendinden önceki bloğun şifrelemesini bir zaman damgası ve işlem verileri ile içermektedir⁵⁷⁰.

Blockchain teknolojisi ile GVKT ilişkisine geldiğimizde öncelikle daha önce belirtildiği üzere GVKT'nin 4. maddesine göre yalnızca kişisel veriler söz konusu olduğunda Tüzük devreye girmektedir. Blockchain teknolojisi ise ad, adres ya da e-mail kimliği içermemektedir. Bu bakımdan blockchain verisi genel olarak “anonim” olarak adlandırılmaktadır. Dolayısıyla anonim veriler GVKT kapsamına girmez ve veri koruma hukukunun kapsamı dışında kalabilir. Ancak bu durum blockchain ve GVKT ilişkisinde buzdağının yalnızca görünen yüzüdür. Çoğu olayda anonim olan kişinin ilave bir özel anahtarla tanımlanması ve artık anonimlikten çıkarak verisinin kişisel veri olması hali söz konusu olabilmektedir. Söz gelimi kişi, bitcoin ile bir şey satın alırken teslimat için adres vermektedir. Dolayısıyla aslında birçok blockchain uygulamasında anonimlik söz konusu değildir. Hukuki olarak takma adlandırma (*pseudonymity*) söz konusudur. GVKT'nin 4. maddesinde yer alan “takma adlandırma” tanımına bakıldığında,

“kişisel verilerin tanımlanmış veya tanımlanabilir bir gerçek kişiyle ilişkilendirilmesinin engellenmesi amacı ile, kişiye dair ilave bilgilerin ayrı tutularak teknik ve örgütsel önlemlerin alınması şartıyla, ilave verilerin kullanımı olmadan, belirli bir veri öznesine atfedilemeyecek şekilde işlenmesi anlamına gelir.”

denilmektedir. Dolayısıyla bu uygulamada bir kişi, mevcut bilgileri ilave bilgi ile birleştirme olanağına sahiptir ve kişiyi tanımlayabilmektedir. Anonimlikte ise öyle bir durum söz konusu olamaz. Bu bakımdan takma adlandırma da kişisel veri olduğundan birçok blockchain uygulaması GVKT kapsamında değerlendirilecektir. Ayrıca

⁵⁶⁹ Paul DUGHI, “A Simple Explanation of How Blockchain Works”, *Medium*, <https://medium.com/the-mission/a-simple-explanation-on-how-blockchain-works-e52f75da6e9a>, E.T. 04.05.2019.

⁵⁷⁰ Ameer ROSIC, “What is Blockchain Technology? A Step-by-Step Guide for Beginners”, *Blockgeeks*, <https://blockgeeks.com/guides/what-is-blockchain-technology/>, E.T. 04.05.2019.

belirtilmelidir ki, bugün anonim olarak kabul edilebilecek veriler, teknolojik gelişmelerle beş yıl içinde kişisel veri haline gelebilir⁵⁷¹.

GVKT'nin blockchain ile ilişkisini bir miktar daha aydınlatabilmek için blockchain ağlarından söz etmek gerekmektedir, çünkü ağların temel 4 türü bakımından Tüzük'ün uygulanması farklı biçimde karşımıza çıkmaktadır. Buna göre blockchain ağları temelde açık veya özeldir. Ayrıca bir diğer ayrım da ağ içindeki “mutabakat sistemine dahil olup olmama” (izin gerekmezsiniz blok oluşturabiliyor ve blok doğrulayabiliyorsa) bakımından yapılmaktadır. Şöyle ki, açık blockchain ağlarına isteyen herkes katılabilmektedir. Ancak açık ağa katılmanın ardından kişi mutabakat sistemine de izin almadan katılabiliyor, daha açık bir ifade ile blok oluşturabiliyor ve blok doğrulayabiliyorsa bu sistem “*Bütünüyle İzin Gerektirmeyen Blockchain Ağı*”dır. Burada ağa dahil olmak oldukça kolaydır ve ağa dahil olan kişilerin sayısı arttıkça ağda mevcut olan verilere erişim ve bu verilerin birer kopyasına sahip olunması durumu da söz konusu olacaktır⁵⁷². Dolayısıyla bu ağ türünün GVKT ile uyumlu olabilmesi oldukça zor görünmektedir. Öte yandan açık ağa katılmanın ardından kişi mutabakat sistemine izin alarak katılabiliyorsa bu sistem “*Kısmen İzin Gerektirmeyen Blockchain Ağı*”dır. Özel Blockchain ağlarında ise ağa ancak özel izin verilenler katılabilmektedir. Bu ağlarda sisteme izin alarak giren kişi eğer mutabakat sistemine izin almadan katılabiliyorsa “*Kısmen İzin Gerektiren Blockchain Ağı*” mevcuttur⁵⁷³. Kısmen izin gerektiren ve

⁵⁷¹ Christian WIRTH, Michael KOLAIN, “Privacy by Blockchain Design: A Blockchain-enabled GDPR-compliant Approach for Handling Personal Data”, *ERCIM Blockchain Workshop 2018: Blockchain Engineering: Challenges and Opportunities for Computer Science Research, Reports of the European Society for Socially Embedded Technologies (EUSSET)*, Vol. 2, No: 6, Y: 2018, https://dl.eusset.eu/bitstream/20.500.12015/3159/1/blockchain2018_03.pdf, E.T. 05.05.2019.

⁵⁷² Dominique GUEGAN, “Public Blockchain versus Private Blockchain”, *Centre de Economie Sorbonne (CES) Working Papers*, 2017, s. 2-4, ss. 1-6; Ahmet USTA, Serkan DOĞANTEKİN, *Blockchain 101*, Digital Age- BKM, 2017, s. 47- 48; Deborah DOBSON, “The 4 Types of Blockchain Networks Explained”, International Legal Technology Association, 2018, <https://www.iltanet.org/blogs/deborah-dobson/2018/02/13/the-4-types-of-blockchain-networks-explained>, E.T. 06.05. 2019.

⁵⁷³ GUEGAN, “Public Blockchain versus Private Blockchain”, *Centre de Economie Sorbonne (CES) Working Papers*, s. 2-4; USTA, DOĞANTEKİN, *Blockchain 101*, s. 48; DOBSON, “The 4 Types of Blockchain Networks Explained”, <https://www.iltanet.org/blogs/deborah-dobson/2018/02/13/the-4-types-of-blockchain-networks-explained>, E.T. 06.05. 2019.

kısmen izin gerektirmeyen ağlar ise bu statüleri sebebiyle somut olay bağlamında incelenerek GVKT ile uyumu ortaya konulabilecektir. Son blockchain ağında ise, sisteme izin alarak giren kişi, ayrıca mutabakat sistemine de izin alarak dahil olabiliyorsa “Bütünüyle İzin Gerektiren Blockchain Ağı”ndan söz edilmektedir⁵⁷⁴. Bu ağ türlerinin GVKT ile uyumu ise oldukça kolay olmaktadır. Burada ağın sahibi olan kişi ağın tüm izin usulünün de yürütücüsüdür. Dolayısıyla veri işleme kurallarını belirleyerek mevzuata uygun bir şekilde sistemi kurabilecektir.

Özel veri işleme faaliyetlerinin sonuncusu olarak, nesnelerin interneti (internet of things) ele alınmalıdır. Nesnelerin interneti kavramı, gündelik cihazlara ortak gömülü milyarlarca sensörün verileri kaydetmek, işlemek, depolamak ve aktarmak için tasarlandığı ve benzersiz tanımlayıcılarla ilişkilendirildiği gibi, diğer cihazlarla veya sistemlerle etkileşime giren bir altyapıyı ifade eder. Nesnelerin interneti, kesintisiz bir şekilde veri alışverişi yapmak üzere tasarlanan bu sensörler aracılığıyla gerçekleşen geniş kapsamlı bir veri işleme prensibine dayanmaktadır. Nesnelerin interneti oluşumları, cep telefonlarımızda yer alan söz gelimi spor takibi, yumurtlama döngüsü takibi yapan, nabız ölçen uygulamalar ya da bu tarz cihazlar tarafından toplanan verilere dayanarak, kullanıcının alışkanlıklarına veya faaliyetlerine karşılık gelen verilerin kombinasyonuna ve analizine dayanan uygulamalar ve hizmetler sunan bir oluşumdur. Bu bakımdan doğaldır ki oldukça yüksek miktarda kişisel veri bunlar gibi pek çok nesnelerin interneti hizmetleri ile toplanmakta ve paylaşılmaktadır. Özellikle kullanıcılara kişiselleştirilmiş deneyimler sağlamak için kullanıcıların verileri kesintisiz biçimde bu sistemlere bağlanmıştır. Dolayısıyla kapsamlı ve kesintisiz bir biçimde veri işlenmesini gerektirir ve bu durum çok sayıda gizlilik riskini de içermektedir. Tüm bu sebeplerle nesnelerin interneti ile GVKT’nin de yolu kesişmektedir⁵⁷⁵. Bu bakımdan GVKT’de yer alan ve tüm

⁵⁷⁴ GUEGAN, “Public Blockchain versus Private Blockchain”, *Centre de Economie Sorbonne (CES) Working Papers*, s. 2-4; USTA, DOĞANTEKİN, *Blockchain 101*, s. 48; DOBSON, “The 4 Types of Blockchain Networks Explained”, <https://www.iltanet.org/blogs/deborah-dobson/2018/02/13/the-4-types-of-blockchain-networks-explained> E.T. 06.05. 2019.

⁵⁷⁵ Sandra WACHTER, “The GDPR and the Internet of Things: A Three-Step Transparency Model”, *Law, Innovation and Technology Journal*, Vol. 10, S. 2, Y: 2018, s. 267, ss. 266- 294; Article 29 Data Protection Working Party, Opinion 8/ 2014 on the Recent Developments on the Internet of Things, WP 223,

bu risklere ilişkin birçok hüküm, nesnelerin interneti hizmetleri ile ortaya çıkan gizlilik risklerinin hafifletilmesine yardımcı olabilecektir⁵⁷⁶.

2. 95/46/AT Sayılı Direktif ve Genel Veri Koruma Tüzüğü'nün Karşılaştırılması

GVKT 25 Mayıs 2018'de yürürlüğe girdiğinde, 1995 tarihli 95/46/AT Sayılı Direktif'in yerini almıştır⁵⁷⁷. Avrupa Veri Koruma Reformu'nun temelini oluşturan bu

16.09.2014, s. 4, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf, E.T. 25.03.2019.

⁵⁷⁶ WACHTER, "The GDPR and the Internet of Things: A Three-Step Transparency Model", s. 266.

⁵⁷⁷ GVKT'nin yürürlüğe girmesi sonrası veri korumaya dair dünya çapında ses getiren en büyük olay Facebook'a verilen para cezası olmuştur. Söz konusu olayda ABD Başkanı Donald Trump'ın seçim çalışmalarını yürüten takımıyla çalışan ve İngiltere'deki Brexit oylamasını kazanan seçim kampanyasını yürüten Cambridge Analytica adlı veri analiz şirketi, Facebook vasıtasıyla 50 milyon kişinin profil bilgilerini izinsiz bir biçimde ele geçirerek kişilerin seçim tercihlerini etkileyen bir algoritma geliştirmiştir. Bu doğrultuda 1 milyon dolar harcama yapılarak kişilerin siyasi tercihlerini etkileyebilecek kişiye özel reklamlar üretildiğine dair kriz 2018 yılının başlarında patlak vermiştir. Bu haberin ardından hem Birleşik Krallık Parlamentosu hem de Avrupa Parlamentosu Facebook sitesinin kurucusu Mark Zuckerberg'i ifadeye çağırmıştır. Bu gelişmeler doğrultusunda hem Birleşik Krallık'ta hem de ABD'de yaklaşık 71 milyon kişi uluslararası insan hakları sözleşmeleri ve anayasalar tarafından korunan özel yaşam hakkının, mahremiyetin, kişilik haklarının ihlal edilmesi ve bu ihlal sonucu elde edilen verilerin demokratik süreçleri etkilemekte kullanılması gerekçeleriyle Facebook'a ve Cambridge Analytica şirketlerine dava açmıştır. Bu oldukça güncel ve dünya çapındaki kriz ile GVKT'nin ilişkisine bakıldığında, dünya çapındaki tüm şirketlerin GVKT'ye uygunluğunu sağlamaları için son tarih 25 Mayıs 2018 tarihiydi. Bu nedenle tüm şirketler müşterilerinden GVKT'nin hükümleri doğrultusunda, kişisel verilerini alabilmek, işleyebilmek ve paylaşabilmek için tam, sade ve anlaşılabilir bir dilde açık izin almak durumunda kalmıştır. Ayrıca GVKT'ye göre veri kullanma, işleme ve paylaşım şartlarında bir değişiklik olması hallerinde izin güncellenmesi aranmaktadır. Yine anılan düzenlemeye göre Cambridge Analytica krizi gibi bir sızıntı durumunda şirket, öğrenilmeden itibaren 72 saat içerisinde düzenleyici kurumlara açıklama yapmak zorundadır.

Facebook, anılan kriz sonrası dünya genelinde kaybettiği ünü yeniden inşa etmek ve GVKT'de düzenlenen şirketin yıllık gelirinin %4'üne dek olan ağır para cezaları sebebiyle, dünya genelindeki kullanıcılarına GVKT ile uyumlu gizlilik kurallarını uygulamaya başladı. Bu noktada Facebook kullanıcılarından reklam hedeflemesi için paylaştıkları kişisel bilgileri ve yüz tanımaya izin verip vermedikleri konularında ne tür verilerinin işlenmesini onayladıklarını incelemelerini istemiştir.

Heather KELLY, "Facebook will push privacy alert to users outside EU ahead of GDPR", *CNN Money*, 24.05.2018, https://money.cnn.com/2018/05/24/technology/facebook-gdpr-us/index.html?utm_content=20180524T12%3A36%3A40&utm_source=twmoney&utm_term=image&utm_medium=social, E.T. 01.03.2019; Carole CADWALLADR, Emma GRAHAM-HARRISON, "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach", *The Cambridge Analytica Files*, 17.03.2018, <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence->

yeni Tüzük’ün önceki Direktif ile farklarını etraflıca ortaya koymak, Reform’un temel mantığının anlaşılması için önem taşımaktadır.

İlk olarak belirtilmelidir ki, “Kişisel Veri” kavramı her ne kadar 95/46/AT Sayılı Direktif’te yer alıyorsa da GVKT ile kapsamı değiştirilmiştir. 95/46/AT Sayılı Direktif bakımından kişisel veri kavramı, isim, fotoğraf, e-posta adresi, telefon numarası, adres ve sosyal güvenlik ya da banka hesabı gibi kişisel kimlik numaraları vb. verileri içermektedir. GVKT ile ise, kişisel veri kavramına biyometrik ve genetik veriler eklenerek eski düzenlemeye kıyasla daha geniş bir anlayış oluşturulmuştur.

GVKT’nin uygulama alanı, 95/46/AT Sayılı Direktif’e göre oldukça genişlemiştir. Bu bağlamda veri denetleyicisi veya veri işleyicisinin AB’de olması hali, denetleyici bakımından Direktif’te de mevcuttu. Fakat Veri Koruma Reformu’ndan bahsetmemize sebep olan en büyük yeniliklerden biri, yalnızca verileri işlenen veri öznelerinin AB alanında ikamet etmeleri durumu bütünüyle yeni bir düzenlemedir. Bu bakımdan GVKT’nin uygulamasında “ülkedışılık (extraterritoriality)” prensibi esastır. Dolayısıyla GVKT’nin uygulanması için artık veri denetleyicisinin AB alanında ikamet etmesi şartı, 95/46/AT Sayılı Direktif’in aksine, aranmamaktadır⁵⁷⁸.

95/46/AT Sayılı Direktif’e göre, veri işleme faaliyetleri kayıt altına alınmaktaydı. GVKT’ye göre ise, veri denetleyicilerinin Veri Koruma Kurumu’ndaki online sicile kişisel veri işleme faaliyetleri hakkında bilgi girmesi zorunlu değildir. Bir kuruluşun

us-election , E.T. 01.03.2019; Matthew ROSENBERG, Nicholas CONFESSORE, Carole CADWALLADR, “How Trump Consultants Exploited the Facebook Data of Millions”, 17.03.2018, <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html> , E.T. 01.03.2019; Burçak ÜNSAL, “Facebook/ Cambridge Analytica skandalının veri koruma çabalarına etkisi”, *Digital Age*, 03.05.2018, <https://digitalage.com.tr/facebook-cambridge-analytica-skandalinin-veri-koruma-cabalarına-etkisi/> , E.T. 01.03.2019.

⁵⁷⁸ KLEKOVIC, “EU GDPR vs. European Data Protection Directive”, <https://advisera.com/eugdpracademy/blog/2017/10/30/eu-gdpr-vs-european-data-protection-directive/> , E.T. 26.02.2019; KRISHNA, “Comparison Table of GDPR- DPD”, <https://cis-india.org/internet-governance/files/comparison-table-gdpr-dpd> , E.T. 04.03.2019.

zorunlu olarak veri işleme kayıtlarını dahili olarak tutma ve isteğe bağlı olarak erişilebilir kılmasının şartı olarak en az 250 çalışanı olması gerekmektedir⁵⁷⁹.

Hukuki olarak veri işlemenin temel şartı olan veri öznesinin rızası, doğaldır ki 95/46/AT Sayılı Direktif’te yer alıyor olsa da GVKT ile birlikte “bilgilendirme” ve “münhasırlık” ilkeleri bağlamında yeniden ele alınmaktadır. Rızanın öncesinde veya rıza esnasında kuruluşun kişisel verileri hangi biçimde kullanmaya niyetli olduğu, verileri hangi sürede işleyeceği ve saklayacağı, bireyin temel haklarının ve bu hakları korumak için gereken hukuki yolların neler olduğunun açıklaması gerekmektedir. Ayrıca rıza eylemi artık dolaylı bir vazgeçme şeklinde değil, aktif, açık, yeterince aydınlatılmış bir eylemi ifade etmektedir⁵⁸⁰. 95/46/AT Sayılı Direktif’te bulunmayan, çocuklara ilişkin rıza ise GVKT’nin 8. maddesinde mevcuttur. Buna göre rıza, çocuğun en az 16 yaşında olması halinde hukuka uygundur. Üye devletler ise 13 yaşından küçük olmamak kaydıyla farklı bir yaş belirleyebilecektir. Bu sınır her AB üye ülkesinin mevzuatına göre değişmekle birlikte⁵⁸¹, belli bir yaşa kadar çocukların aileleri ya da yasal temsilcileri tarafından verilmektedir.

Her ne kadar 95/46/AT Sayılı Direktif’te veri öznesi için varolan haklar arasında bulunsa da “doğrudan pazarlama amacıyla işlenen kişisel verilere itiraz etme hakkı” ve “veri taşınabilirliği hakkı” GVKT ‘da yeni tanımları ile yer almışlardır⁵⁸². İlaveten “veri işlemeyi kısıtlama hakkı” da hem eski hem yeni düzenlemede yer alan fakat kapsamı

⁵⁷⁹ KLEKOVIC, “EU GDPR vs. European Data Protection Directive”, <https://advisera.com/eugdpracademy/blog/2017/10/30/eu-gdpr-vs-european-data-protection-directive/>, E.T. 26.02.2019.

⁵⁸⁰ KLEKOVIC, “EU GDPR vs. European Data Protection Directive”, <https://advisera.com/eugdpracademy/blog/2017/10/30/eu-gdpr-vs-european-data-protection-directive/>, E.T. 26.02.2019.

⁵⁸¹ AB üyesi ülkelerin ulusal mevzuatlarına göre bu yaş sınırı 13 ile 18 arasında değişmektedir. KLEKOVIC, “EU GDPR vs. European Data Protection Directive”, <https://advisera.com/eugdpracademy/blog/2017/10/30/eu-gdpr-vs-european-data-protection-directive/>, E.T. 26.02.2019.

⁵⁸² TIKKINEN-PIRI, ROHUNEN, MARKKULA, “EU General Data Protection Regulation: Changes and implications for personal data collecting companies”, s. 14, 17; KLEKOVIC, “EU GDPR vs. European Data Protection Directive”, <https://advisera.com/eugdpracademy/blog/2017/10/30/eu-gdpr-vs-european-data-protection-directive/>, E.T. 26.02.2019.

geniřletilen haklardandır. Veri öznesi eski düzenleme ile verilerin yanlış olması veya verilerin eksik olması nedeniyle verilerin işlenmesini engelleyebilmekteydi. GVKT’de ise, aynı hak daha ayrıntılı bir biçimde, veri denetleyicisinin üzerindeki yükümlölükler ile birlikte bulunmaktadır⁵⁸³.

95/46/AT Sayılı Direktif uyarınca veri öznesi, veri işlemenin amacı, işleme kategorileri, alıcılar veya otomatik kararın kapsamı hakkında bilgi sahibi olabilmekteydi. Veri öznesinin kişisel verilerine erişebilme hakkı denilen bu hak, GVKT’de çok daha detaylı biçimde düzenlenmektedir. Artık veri öznesi, saklama süresi, belirli hakların varlığı, veri kaynağı ve işlemenin sonuçları hakkında da bilgi sahibi olabilir. Söz konusu yenilik ile, AB mukimlerinin ellerini daha güçlendirerek şeffaf bir ortam hazırlanmasına yardımcı olmak amaçlanmıştır. Ayrıca bu konuda veri denetleyicisinin yükümlölükleri de belirtilmektedir. Veri denetleyicileri de bu bilgileri talep eden veri öznesinin kişisel verilerinin bir kopyasını elektronik biçimde ve ücretsiz olarak vermelidir⁵⁸⁴.

95/46/AT Sayılı Direktif yalnızca veri öznesinin, verilerin yanlış veya eksik olması nedeniyle ya da yasadışı işleme durumunda verilerin niteliğı nedeniyle verilerin silinmesini talep etme hakkını içermekteydi. GVKT’da ise, AB mukimlerine kişisel verilerine ilişkin olarak veri denetleyicilerinden unutulma haklarını kullanmak talebinde bulunabilmeleri hakkı tanınmıştır. Buna göre veri denetleyicileri istekte bulunan veri öznesinin tüm kişisel verilerini silmeli, bu verilerin daha fazla kullanılmasına son vermeli

⁵⁸³ KRISHNA, “Comparison Table of GDPR- DPD”, <https://cis-india.org/internet-governance/files/comparison-table-gdpr-dpd> , E.T. 04.03.2019.

⁵⁸⁴ BEAUMONT, "The Data Protection Directive versus the GDPR: Understanding key changes", <https://www.synopsys.com/blogs/software-security/dpd-vs-gdpr-key-changes/> ; KRISHNA, “Comparison Table of GDPR- DPD”, <https://cis-india.org/internet-governance/files/comparison-table-gdpr-dpd> , E.T. 04.03.2019.

ve varsa üçüncü tarafların kullanımını durdurmalıdır. Bu bakımdan unutulma hakkı⁵⁸⁵ da GVKT’de ilk defa düzenlenen haklar arasındadır⁵⁸⁶.

95/46/AT Sayılı Direktif ile GVKT arasındaki bir diğer önemli fark da veri işleyicisinin hukuki bir metin altında düzenlenip düzenlenmemesi hususudur. Buna göre veri işleyicisi 95/46/AT Sayılı Direktif’te bulunmuyorken, GVKT kapsamında düzenlenmektedir. Artık hem veri denetleyicisi hem de veri işleyicisi GVKT’deki kurallar bakımından müşterek olarak sorumludurlar. Oysa 95/46/AT Sayılı Direktif’te, yalnızca veri denetleyicisi sorumlu tutulmaktaydı.

Veri koruma kurallarının uygulamasını denetleme için denetim makamı 95/46/AT Sayılı Direktif’in aksine, GVKT’de daha detaylı düzenlenmiştir. Bu bağlamda ilk defa GVKT’de denetim makamına şikâyetle bulunmak bir “hak” olarak düzenlenmiştir⁵⁸⁷.

95/46/AT Sayılı Direktif’te yer almayan bir diğer yenilik de veri koruma görevlisidir. Denetim ve yaptırım uygulamalarından önce mutlaka önleyici yollara başvurulmasına yönelten GVKT’ye göre veri koruma görevlisi, kuruluşun temel iş etkinliğine dair veri işleme ile ilgili olarak veri öznelerinin sistemli ve düzenli biçimde büyük ölçekte izlenmesi, büyük ölçekli özel veri ve suç kategorilerinin işlenmesi veya bir

⁵⁸⁵ “Unutulma Hakkı”na ilişkin detaylı bilgi için bkz. Meg LETA JONES, *Ctrl + Z: The Right to Be Forgotten*, New York University Press, New York, 2016; Can YAVUZ, *İnternetteki Arama Sonuçlarından Kişisel Verilerin Kaldırılması Unutulma Hakkı*, Seçkin Yayıncılık, Ankara, 2018; Eren SÖZÜER, *Unutulma Hakkı İnsan Hakları Hukuku Perspektifinden bir İnceleme*, On İki Levha Yayıncılık, İstanbul, 2017; Aydın AKGÜL, “Kişisel Verilerin Korunmasında Yeni Bir Hak: ‘Unutulma Hakkı’ ve AB Adalet Divanı’nın ‘Google Kararı’”, *TBB Dergisi*, C. 27, S. 116, Ocak 2015, ss. 11- 38.

⁵⁸⁶ TIKKINEN-PIRI, ROHUNEN, MARKKULA, “EU General Data Protection Regulation: Changes and implications for personal data collecting companies”, s. 14, 17; BEAUMONT, “The Data Protection Directive versus the GDPR: Understanding key changes”, <https://www.synopsys.com/blogs/software-security/dpd-vs-gdpr-key-changes/> ; KRISHNA, “Comparison Table of GDPR- DPD”, <https://cis-india.org/internet-governance/files/comparison-table-gdpr-dpd> , E.T. 04.03.2019.

⁵⁸⁷ KRISHNA, “Comparison Table of GDPR- DPD”, <https://cis-india.org/internet-governance/files/comparison-table-gdpr-dpd> , E.T. 04.03.2019.

kamu kuruluđu tarafından yrtlen veri iřlemesi gibi durumlarda zorunlu olarak atanan bir kiřidir⁵⁸⁸.

Yine nleyici yollar bakımından GVKT, kendisine uyumluluđu saęlamak iin bir “Veri Koruma Etki Deęerlendirmesi” yapılmasını dzenlemektedir. Byle bir dzenleme, 95/46/AT Sayılı Direktif’te bulunmamaktaydı. Bu deęerlendirme ile amalanan, oluřabilecek riskleri ngrerek minimuma indirmeye yardımcı olmaktır⁵⁸⁹.

GVKT cezalar konusunda da 95/46/AT Sayılı Direktif’ten ok daha aęır dzenlemeler iermektedir. Bu cezalar veri znesine, kurallara uyulmaması sebebiyle maruz kaldıkları iřlemlerden bir zarar grmeleri halinde tazminat hakkı vermektedir⁵⁹⁰.

E. VERİ KORUMA REFORMU NCESİ GELİřMELER İLE REFORMUN ULUSAL HUKUK DZENLERİNE ETKİSİ

95/46/AT Sayılı Direktif’in yrrlęe girdięi 1995 yılında, Avrupa’da Schengen Blgesi’nin de kurulması ulusal normların yeni bir evreye girmesine sebep olmuřtur. Direktif ye lkelere, ulusal mevzuatlarını ierięe uygun hale getirmeleri iin 3 yıl sre vermiřtir. Bu baęlamda Direktif’in kabul edildięi esnada henz İtalya ve Yunanistan’da kiřisel verilerin korunmasıyla ilgili zel bir dzenleme bulunmamakta ve dięer ye lkeler ise i hukuklarında yer alan dzenlemeleri Direktif’e uygun hale getirmek zorundalardı⁵⁹¹.

⁵⁸⁸ KRISHNA, “Comparison Table of GDPR- DPD”, <https://cis-india.org/internet-governance/files/comparison-table-gdpr-dpd>, E.T. 04.03.2019.

⁵⁸⁹ VOIGT, VON DEM BUSSCHE, *The EU General Data Protection Regulation (GDPR)- A Practical Guide*, s. 5; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), Art. 40, L 119, 04.05.2016, <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504>, E.T. 14.03.2019.

⁵⁹⁰ KLEKOVIC, “EU GDPR vs. European Data Protection Directive”, <https://advisera.com/eugdpracademy/blog/2017/10/30/eu-gdpr-vs-european-data-protection-directive/>, E.T. 26.02.2019.

⁵⁹¹ FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, s. 147.

Durum böyle olmakla beraber uygulamada ulusal mevzuatların Direktif'e uyarlanması beklenenden yavaş olmuştur. 1999 yılında Avrupa Komisyonu, iç hukuklarını Direktif'e uyarlamayan ülkelere karşı tatbikat başlatmıştır. Direktif'in yürürlüğe girmesinden itibaren üç yıl içinde Komisyon'un, Direktif'in uygulanmasına dair Avrupa Konseyi ve Avrupa Parlamentosu'na bir rapor sunması amaçlanmıştı. Fakat 2001 yılında konudan sorumlu komiser, üye devletlerin Direktif kurallarını iç hukuklarına aktarma hızlarının yavaşlığı sebebiyle raporun ertelenmek zorunda olduğunu duyurmuştur⁵⁹².

95/46/AT sayılı Direktif'in yürürlüğe girmesi sonrası AB üye ülkelerinin önemli bir bölümü, Direktif'in belirlediği çerçeveye uygun hukuki düzenlemeler yapmakta ve Direktif'in kurallarını iç hukuka aktarmakta başarısız olmuşlardır⁵⁹³. Üstelik ilerleyen zamanlarda iç hukuka aktarımı geç bir şekilde başarmış olsalar dahi, Direktif'in AB Hukuku kapsamında zorlayıcı değil de yalnızca çerçeve belirleyen özelliği sebebiyle pratikte ülkeden ülkeye değişen birçok farklı kuralı barındıran uygulamalara sebebiyet vermişlerdir. Bu sebeple yukarıda belirtildiği üzere Avrupa Komisyonu, hem Avrupa'yı dijital çağa uygun hale getirmek ve artık teknolojik gelişmelerin gerisinde kalan 95/46/AT Sayılı Direktif'i yenilemek, hem de bu Direktif'in çeşitli ülkelerdeki farklı uygulamalarını uyumlulaştırmak için Ocak 2012'de AB Veri Koruma Reformu'na girişmiştir. İşte bu Reform'un temelini oluşturan ve 25 Mayıs 2018'den beri uygulanan GVKT, AB kapsamındaki tüm kuralları yeknesak hale getirmiş ve veri koruma hukukunu güçlendirmiştir. Söz konusu Tüzük anılan tarihten itibaren AB üye ülkelerinde doğrudan bağlayıcı hale gelmiştir. Bu bakımdan üye ülkelerin iç hukuklarındaki düzenlemeleri GVKT hükümleri doğrultusunda değiştirmeleri için ise iki yıllık süre öngörülmüştür. Bu bakımdan Reform öncesi durumu ve Reform'un ardından uygulamaya geçen GVKT'nin

⁵⁹² Avrupa Komisyonu, Veri Koruma Direktifi'nin (95/46/AT Sayılı) Uygulanmasına Dair İlk Rapor, COM/2003/0265 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52003DC0265> , E.T. 31.11.2018.

⁵⁹³ Türkay HENKOĞLU, *Bilgi Güvenliği ve Kişisel Verilerin Korunması*, Yetkin Yayınları, Ankara, 2015, s. 60.

AB üye ülkeleri bakımından etkilerini incelemek, ulusalüstü uygulamaların ulusal hukukta hem anayasal hem de yasal ölçekte ne gibi değişikliklere yol açtığını görmek bakımından önem taşımaktadır.

Almanya 1970’lerde Federal Veri Koruma Kanunu’nu birden çok defa revize etmiştir. 1983 yılında ise, Alman Federal Mahkemesi bu alanda oldukça önemli bir karar olan “Nüfus Sayım Kararı”nda verilerin korunmasını Alman Anayasası’nın 1. ve 2. maddelerine dayandırmıştır. Bu kararla birlikte Almanya’da verilerin korunması, Anayasa’nın insan onurunu ve kişiliğin korunması ilkeleri ile ele alınır olmuştur. Karar ile ayrıca kişisel verilerin kullanımına ancak veri öznesinin rızası ile ya da Kanun’da açıkça öngörülmesi halinde izin verildiği hüküm altına alınmıştır. Bu doğrultuda 1990 yılında yeni bir Federal Veri Koruma Kanunu yürürlüğe girmiştir. Bu Kanun ile birlikte kararda anılan anayasal gereklilikler düzenlenmiştir. 2001 yılında ise yeni bir değişiklik daha gerçekleştirmiş ve 95/46/AT sayılı Direktif kuralları iç hukuka aktarılmıştır⁵⁹⁴. 1990 tarihli söz konusu Federal Veri Koruma Kanunu, GVKT’nin yürürlüğe girmesine dek, birçok değişiklik geçirerek, yürürlükte kalmıştır. 25 Mayıs 2018 sonrası da değiştirilmiş Alman Veri Koruma Kanunu hükümleri, GVKT’nin uygulamasını desteklemektedir⁵⁹⁵.

1978 yılından beri bir Veri Koruma Kanunu olan Avusturya, 2000 yılında bunu revize etmiştir. GVKT’den sonra ise 2000 tarihli Veri Koruma Kanunu’nu, Tüzük’ün de çeşitli maddelerinin ilk uygulaması sayılabilecek 25 Mayıs 2018 tarihli Veri Koruma Değişiklik Kanunu ile önemli ölçüde değiştirilmiştir⁵⁹⁶.

⁵⁹⁴ Edith PALMER, *Online Privacy Law: Germany Country Report*, Library of Congress, June 2012, <https://www.loc.gov/law/help/online-privacy-law/2012/germany.php> , E.T. 01.05.2019.

⁵⁹⁵ Jenny GESLEY, *Online Privacy Law: Germany Country Report*, Library of Congress, December 2017, <https://www.loc.gov/law/help/online-privacy-law/2017/germany.php> , E.T. 01.05.2019; Kanun metni için bkz. https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl#_bgbl_%2F%2F*%5B%40attr_id%3D%27bgbl117s2097.pdf%27%5D_1556892189832 , E.T. 03.05.2019.

⁵⁹⁶ Handbook on *Data Protection Laws of the World-* Austria, 10.01.2019, DLA Piper, <https://www.dlapiperdataprotection.com/index.html?t=law&c=AT&c2=> , E.T. 30.04.2019; Kanun metni için bkz. https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2017_I_120/BGBLA_2017_I_120.pdfsig , E.T. 03.05.2019.

1992’den beri konu ile ilgili spesifik yasal düzenlemesi olan Belçika ise, 95/46/AT Sayılı Direktif’i uygulamak için 1998 yılında bu düzenlemede değişikliğe gitmiştir. 1994 yılında ise özel yaşam hakkını düzenleyen bir hükmü Anayasası’na entegre etmiştir⁵⁹⁷. GVKT’nin Belçika iç hukukuna aktarımı ise birkaç kanun ile gerçekleşmiştir. 30 Temmuz 2018’de yeni bir Veri Koruma Kanunu yürürlüğe girmiş ve Tüzük’ün düzenlemelerine daha fazla tanım, istisna ve ilave gereklilikler getirmiştir⁵⁹⁸.

Birleşik Krallık, ilk defa 1984 yılında bir Veri Koruma Yasası’nı uygulamaya koymuştur. Bu Yasa ortaya çıkar çıkmaz birçok bakımdan eleştirilmiştir. Özellikle elle tutulan dosyaların korumasının ihmal edilmiş olması ve kayıt yükümlülüğünden zorunlu muafiyet gibi hususlar bu eleştirilerin odak noktasını oluşturmuştur. Ayrıca ulusal güvenliğe ilişkin bilgisayarlar Yasa’nın kapsamının dışında tutulmuş, suç tespiti, vergilendirme ve göçmenlik kontrolü amacı ile tutulan verilere de erişim sınırlandırılmıştır. Bu bakımdan söz konusu Yasa oldukça yetersiz bir görünüm arzietmekteydi⁵⁹⁹. Devamında 1998 yılında, eski Yasa’nın hemen hemen aynısı olan ve özel yaşamdan bahsetmeyen bir Veri Koruma Yasası kabul edilmiştir. Bu Yasa, 95/46/AT sayılı Direktif’e dayanmaktadır. Ayrıca aynı yıl İnsan Hakları Yasası kabul edilerek İnsan Hakları Avrupa Sözleşmesi’nde yer alan haklar ve bu bağlamda özel yaşam hakkının uygulanması zorunlu kılınarak anılan hakkın Birleşik Krallık’taki uygulaması bakımından önemli bir adım atılmıştır. Veri saklama politikası 1998 tarihli Veri Koruma Yasası’nın ardından 2016 tarihli Araştırma Yetkileri Yasası kapsamında ele alınmıştır. 2018 yılında ise, Birleşik Krallık’ın son Veri Koruma Yasası, her ne kadar bazı konularda

⁵⁹⁷ FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, s. 149.

⁵⁹⁸ Handbook on Data Protection Laws of the World- Belgium, 17.10.2018, DLA Piper, <https://www.dlapiperdataprotection.com/index.html?t=law&c=BE&c2=> , E.T. 30.04.2019; Kanun metni için bkz. <https://www.timelex.eu/sites/default/files/pdf/Nieuwe-belgische-privacywet-30-07-2018.pdf> , E.T. 03.05.2019.

⁵⁹⁹ WARREN, DEARNLEY, “Data Protection Legislation in the United Kingdom From development to statute 1969- 84”, s. 254.

eleştiriliyor olsa da GVKT'nin uygulamasını genişleten bir görünümle yürürlüğe girmiştir⁶⁰⁰.

Çek Cumhuriyeti ise 1992'de düzenlenmiş kişisel verilere dair bir kanunu, 2000 yılındaki Kişisel Verilerin Korunması Kanunu ile ilga etmiştir⁶⁰¹. 12 Mart 2019 tarihinde ise GVKT'nin hükümlerinin iç hukuktaki yansıması olacak olan Veri İşleme Kanunu kabul edilmiş ve 10 Nisan 2019'da Başkan tarafından imzalanmıştır. Yürürlüğe girmesi için Resmî Gazete'de yayımlanması beklenmektedir⁶⁰².

1978 yılında veri koruma ile ilgili iki kanunu mevcut olan Danimarka'da bu düzenlemelerin yerine 2000 yılında Kişisel Verilerin İşlenmesi Hakkında Kanun kabul edilmiştir⁶⁰³. GVKT sonrasında ise, 25 Mayıs 2018'de yürürlüğe girecek biçimde, 17 Mayıs 2018'de Veri Koruma Kanunu'nu kabul edilmiş ve bu Kanun 25 Mayıs 2018'de yürürlüğe girmiştir⁶⁰⁴.

1996 yılına gelindiğinde ilk ulusal Kişisel Verilerin Korunması Kanunu'nu yapan Estonya, bu Kanun'u 2003 yılında yürürlükten kaldırarak yeni bir düzenleme yapmıştır⁶⁰⁵. GVKT bakımından gereken ek şartlar 15 Ocak 2019'da yürürlüğe giren yeni

⁶⁰⁰ Data Protection Act 2018, Factsheet – Overview, Department for Digital, Culture, Media and Sport, 23.05.2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/711162/2018-05-23_Factsheet_1_-_Act_overview.pdf , E.T. 01.05.2019; Warwick ASHFORD, “New UK Data Protection Act not welcomed by all”, Computer Weekly, 24.05.2018, <https://www.computerweekly.com/news/252441814/New-UK-Data-Protection-Act-not-welcomed-by-all> , E.T. 01.05.2019.

⁶⁰¹ FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, s. 155.

⁶⁰² Register of Commission Expert Groups and Other Similar Entities, E03461 - Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, Updated Table GDPR Implementation Member States, 11.04.2019, <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=30306> , E.T. 03.05.2019.

⁶⁰³ FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, s. 153.

⁶⁰⁴ Handbook on Data Protection Laws of the World- Denmark, 10.01.2019, DLA Piper, <https://www.dlapiperdataprotection.com/index.html?t=law&c=DK&c2=> , E.T. 30.04.2019; Kanun metni için bkz. http://www.ft.dk/samling/20171/lovforslag/L68/som_vedtaget.htm , E.T. 03.05.2019.

⁶⁰⁵ FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, s. 155.

Kişisel Verilerin Koruması Kanunu ve Kişisel Verilerin Korunmasına dair Uygulama Kanunu ile sağlanmıştır⁶⁰⁶.

1958 tarihli Fransa Anayasası kişisel verilerin korunmasına ilişkin bir hüküm barındırmamıştır. Bu bakımdan veri koruma meselesine dair ilk ve temel kanun 6 Ocak 1978 tarihli Bilgi Teknolojileri, Veri Dosyaları ve Medeni Haklar Kanunu'dur. Fransa, Avrupa Komisyonu'na Kanun'un 95/46/AT Sayılı Direktif ile tutarlı olduğunu ve bunun revize edileceği bildirmiş ve devamında 2004 yılında Direktif doğrultusunda 1978 tarihli Kanun'da değişiklikler yapmıştır⁶⁰⁷. Çevrimiçi (online) gizlilik ile ilgili olarak ise Ekim 2016'da Dijital Cumhuriyet Kanunu isimli bir düzenleme yapılmıştır. Bu Kanun genel olarak, ağ tarafsızlığını (internet trafiğinde tarafsız yönetim ilkesi) sağlama, bilgi ekonomisini geliştirme ve bireylerin dijital dünyaya erişimini artırma ile ilgilidir. Bunun yanı sıra Kanun birçok maddesinde çevrimiçi gizlilik konusunda hükümler içermektedir⁶⁰⁸. GVKT'nin ardından 20 Haziran 2018 tarihli kişisel verilerin korunmasına ilişkin bir Kanun ile 1978 tarihli Bilgi Teknolojileri, Veri Dosyaları ve Medeni Haklar Kanunu'nda Tüzük bakımından gerekli uyarlamalar yapılmıştır. 12 Aralık 2018'de ise uygulamayı basitleştirmek ve AB Veri Koruma Hukuku'na uyumu sağlamak adına gereken resmi düzeltmeler için bir Kararname yayımlanmıştır. Bu Kararname 1 Haziran 2019 tarihinde yürürlüğe girmiştir⁶⁰⁹.

Finlandiya ise 1987 yılından beri varolan kişisel veri koruma mevzuatını 1999 yılında gözden geçirmiş ve aynı yıl bir Kişisel Veriler Kanunu düzenleyerek 95/46/AT Sayılı Direktif'i iç hukukuna adapte etmiştir. Bu bağlamda aynı yıl gerçekleşen anayasal

⁶⁰⁶ Handbook on Data Protection Laws of the World- Estonia, 10.01.2019, DLA Piper, <https://www.dlapiperdataprotection.com/index.html?t=law&c=EE&c2=> , E.T. 03.05.2019; Kanun metni için bkz. <https://www.riigiteataja.ee/akt/104012019011> , E.T. 03.05.2019.

⁶⁰⁷ ATWILL, *Online Privacy Law: France Country Report*, Library of Congress, June 2012, <https://www.loc.gov/law/help/online-privacy-law/2012/france.php> , E.T. 03.05.2019.

⁶⁰⁸ Nicolas BORING, *Online Privacy Law: France Country Report*, Library of Congress, December 2017, https://www.loc.gov/law/help/online-privacy-law/2017/france.php#_ftn1 , E.T. 03.05.2019.

⁶⁰⁹ Handbook on Data Protection Laws of the World- France, 23.01.2019, DLA Piper, <https://www.dlapiperdataprotection.com/index.html?t=law&c=FR&c2=> , E.T. 03.06.2019; Kararname metni için bkz. <https://www.legifrance.gouv.fr/eli/decret/2018/8/1/JUSC1815709D/jo/texte> , E.T. 03.06.2019.

reformda da ilgili hukuki düzenlemelere yer vermeyi amaçlamıştır⁶¹⁰. GVKT'nin devamında ise, 1 Ocak 2018'de Tüzük Ek Uygulama Kanunu yürürlüğe girmiştir⁶¹¹. 13 Kasım 2018'de ise yeni bir Veri Koruma Kanunu'nu kabul edilmiş ve 1 Ocak 2019'da yürürlüğe girmiştir⁶¹².

Hollanda 2000 yılında Kişisel Verilerin Korunmasına İlişkin Kurallar Kanunu'nu kabul etmiştir. 2001'de ise bu Kanun'da 95/46/AT Sayılı Direktif'teki düzenlemelere istinaden değişiklikler gerçekleştirilmiş ve bu konu ile ilgili olarak Avrupa Komisyonu'na bildirimde bulunulmuştur. İlgili Kanun'da bu kez 1 Ocak 2016'da yürürlüğe giren değişiklikler yapılmıştır⁶¹³. Bu Kanun genel itibarıyla 95/46/AT Sayılı Direktif'in kapsamı dışında kalan pek fazla düzenleme içermemekteydi. GVKT sonrasında ise, 22 Mayıs 2018'de Tüzük'e ilişkin bir Uygulama Kanunu Resmî Gazete'de yayınlanmış ve GVKT ile aynı tarihte, yani 25 Mayıs 2018'de yürürlüğe girmiştir. Bu bakımdan Hollanda temel kanuni yükümlülüğünü zamanında yerine getirmiştir⁶¹⁴.

95/46/AT Sayılı Direktif'i gereken süre içerisinde iç hukukuna aktarmadığı gerekçesiyle 2001 yılında Avrupa Komisyonu tarafından İrlanda'ya karşı dava açılmıştır. Ardından 2003 yılında İrlanda Veri Koruma Kanunu ile mevzuatını güncellemiştir. GVKT'den sonra 2018 yılında ise İrlanda veri koruma hukuku büyük ölçüde Tüzük'e uyarlanarak yeni bir Veri Koruma Kanunu yapılmıştır. Böylelikle öncesinde yürürlükte

⁶¹⁰ FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, s. 152.

⁶¹¹ Handbook on Data Protection Laws of the World- Finland, 10.01.2019, DLA Piper, <https://www.dlapiperdataprotection.com/index.html?t=law&c=FI&c2=>, E.T. 30.04.2019.

⁶¹² Register of Commission Expert Groups and Other Similar Entities, E03461 - Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, Updated Table GDPR Implementation Member States, 11.04.2019, <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=30306>, E.T. 03.05.2019; Kanun metni için bkz. <http://www.finlex.fi/fi/laki/ajantasa/2018/20181050>, E.T. 03.05.2019.

⁶¹³ Wendy ZELDIN, Online Privacy Law: Netherlands Country Report, June 2012, Library of Congress, https://www.loc.gov/law/help/online-privacy-law/2017/netherlands.php#_ftn9, E.T. 02.05.2019.

⁶¹⁴ Paul BREITBARTH, "The GDPR Implementation Act in The Netherlands", National Adaptations of the GDPR, E-Conference, Blog Droit Européen, June 2018, <https://blogdroiteuropeen.files.wordpress.com/2018/06/paul-1.pdf>, E.T. 02.05.2019; Uygulama Kanunu metni için bkz. https://www.eerstekamer.nl/wetsvoorstel/34939_aanpassingswet_algemene, E.T. 03.05.2019.

olan 1988 ve 2003 tarihli Veri Koruma Kanunları, ulusal güvenlik, savunma ve uluslararası ilişkiler alanları dışında, yürürlükten kalkmıştır. İlgili alanlarda 2018 tarihli Kanun da dahil olmak üzere hem 1998 hem de 2003 tarihli Kanunlar uygulanmaktadırlar. GVKT'nin uygulama alanı bakımından ise esas alınacak düzenleme 25 Mayıs 2018 tarihli Veri Koruma Kanunu'dur⁶¹⁵.

1978 İspanya Anayasası, bireylerin kişisel ve aile yaşamlarının korunmasına dair düzenlemesinde insan onurunun korunması için bilgi teknolojilerinin kullanılmasına sınırlamalar getirilmesi gerektiğini belirtmiştir. Bu hüküm, anılan yıllarda anayasal bir normda bulunma ihtimali oldukça az olan biçimi ile İspanya veri koruma hukukunun temelini oluşturmaktadır. İspanya 1999 yılında, 95/46/AT Sayılı Direktif'i iç hukukuna aktarmak için Kişisel Verilerin Korunmasına dair Organik Kanun'u yürürlüğe koymuştur⁶¹⁶. GVKT'ye dek, anılan Kanun'da Avrupa Veri Koruma Hukuku'nda meydana gelen değişikliklerin ardından birçok değişiklik gerçekleştirilmiştir. GVKT'nin ardından ise İspanya Meclisi, 7 Aralık 2018 tarihinde dijital hakları garanti eden Veri Korumaya dair Temel Kanun'u kabul etmiştir⁶¹⁷.

İsveç'e baktığımızda 1973'te kişisel verilerin gizliliğini korumak için kapsamlı bir Veri Koruma Kanunu'nu kabul eden ilk ülke olduğu değerlendirilmektedir. Söz konusu Kanun ile ülke, 1995 yılında 95/46/AT Sayılı Direktif'in kabulünden önce, gereken hukuki düzenlemeleri yapabilmek için bir komite oluşturmuştur. 1998 yılında yeni bir Kişisel Veri Kanunu, Direktif'i iç hukuka aktarmıştır⁶¹⁸. İsveç, Adalet Divanı'nın 2014'te Veri Saklama Direktifi'ni geçersiz kıldığı kararı ve 2014'teki "unutulma hakkı"

⁶¹⁵ Handbook on *Data Protection Laws of the World*- Ireland, 11.01.2019, DLA Piper, <https://www.dlapiperdataprotection.com/index.html?t=law&c=IE&c2=> , E.T. 02.05.2019; Kanun metni için bkz. <http://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html> , E.T. 03.05.2019.

⁶¹⁶ RODRIGUEZ-FERRAND, *Online Privacy Law: Spain Country Report*, <https://www.loc.gov/law/help/online-privacy-law/2012/spain.php> , E.T. 02.05.2019.

⁶¹⁷ Handbook on *Data Protection Laws of the World*- Spain, 14.01.2019, DLA Piper, <https://www.dlapiperdataprotection.com/index.html?t=law&c=ES> , E.T. 02.05.2019; Kanun metni için bkz. <https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673> , E.T. 03.05.2019.

⁶¹⁸ Elin HOFVERBERG, *Online Privacy Law: Sweden Country Report*, Library of Congress, June 2012, <https://www.loc.gov/law/help/online-privacy-law/2012/sweden.php> , E.T. 01.05.2019.

kararı gibi önemli kararlara dair düzenlemeleri ve GVKT'yi 2012'den bu yana dikkate alsa da, Divan 2016 yılında İsveç veri saklama kurallarını AB veri koruma kurallarına aykırı bulmuştur⁶¹⁹.

İtalya Anayasası, özel yaşamın gizliliğine ilişkin açık bir garanti sunmamaktadır. Her ne kadar Anayasa'da bulunmasa da hakkın varlığına dair yargısal tartışma 1950'lerde başlamıştır. Anayasa Mahkemesi tarafından bir hak olarak tanınması ise ancak 1973 yılında olmuştur. Özel yaşam hakkı teknoloji geliştikçe, bireylerin kendileri hakkında ne tür bilgiler toplandığını ve bu bilgilerin nasıl kullanılacağını bilme ve belirleme haklarını korumak için genişletilmiştir. İtalya, 1996 yılında Kişisel Verilerin İşlenmesi ile ilgili Kişilerin ve Diğer Öznelerin Korunması hakkında bir Kanun kabul etmiş ve 95/46/AT sayılı Direktif'i iç hukukuna almıştır. Bu Kanun 2003 yılında, kişisel verilerin korunması hakkını açıkça kabul eden Kişisel Verilerin Korunması Kanunu tarafından yürürlükten kaldırılmıştır⁶²⁰. GVKT düzenlemesinden sonra ise, 19 Eylül 2018'de yürürlüğe giren bir yasama kararnamesi ile 2003 tarihli Kişisel Verilerin Korunması Kanunu Tüzük ile uyumlu hale getirilmiştir⁶²¹.

2001 yılında Güney Kıbrıs Rum Cumhuriyeti de veri korumaya dair hukuki düzenlemeler yapmıştır. GVKT sonrası Güney Kıbrıs'ta 31 Temmuz 2018 tarihli Kişisel Verilerin İşlenmesine ve Bu Verilerin Serbest Dolaşmasına Karşı Gerçek Kişilerin Korunması Kanunu kabul edilmiştir⁶²².

⁶¹⁹ HOFVERBERG, *Online Privacy Law: Sweeden Country Report*, Library of Congress, December 2017, <https://www.loc.gov/law/help/online-privacy-law/2017/sweden.php> , E.T. 01.05.2019.

⁶²⁰ Laura ANDRIULLI, *Online Privacy Law: Italy Country Report*, June 2012, Library of Congress, <https://www.loc.gov/law/help/online-privacy-law/2012/italy.php> , E.T. 02.05.2019.

⁶²¹ Handbook on *Data Protection Laws of the World*- Italy, 10.01.2019, DLA Piper, <https://www.dlapiperdataprotection.com/index.html?t=law&c=IT&c2=> , E.T. 02.05.2019; Değiştirilmiş Kanun metni için bkz. <https://www.garanteprivacy.it/documents/10160/0/Codice+in+materia+di+protezione+dei+dati+personali+%28Testo+coordinato%29.pdf/b1787d6b-6bce-07da-a38f-3742e3888c1d?version=1.6> , E.T. 03.05.2019.

⁶²² Handbook on *Data Protection Laws of the World*- Cyprus, 10.01.2019, DLA Piper, <https://www.dlapiperdataprotection.com/index.html?t=law&c=CY&c2=> , E.T. 03.05.2019; Kanun metni için bkz. <https://www.mof.gov.cy/mof/gpo/gpo.nsf/All/FA3AA1D6DA54AB4BC2>

Letonya ise 2001 yılında yürürlüğe giren Kişisel Verilerin Korunması Kanunu'nu 2000 yılında kabul etmiştir. GVKT'nin ardından uygulaması için Kişisel Verilerin Hukuki Korumasına dair Kanun 16 Temmuz 2018'de yürürlüğe girmiştir⁶²³.

1996 yılında Litvanya Kişisel Verilerin Hukuki Koruması Kanunu'nu yürürlüğe sokmuş ve 2001 yılında 108 Sayılı Sözleşme'yi onaylamıştır. GVKT sonrası ise 5 Temmuz 2018'de yeni bir Kişisel Verilerin İşlenmesine dair Kanun yürürlüğe girmiştir⁶²⁴.

Direktif'i gereken süre içerisinde iç hukukuna aktarmaması nedeniyle Avrupa Komisyonu Lüksemburg'u 2001 yılında kınamıştır. Ardından 2002 tarihli Kişisel Verilerin İşlenmesi Bakımından Kişilerin Korunması Hakkında Kanun ile Direktif'in hükümleri en nihayetinde iç hukuka taşınmıştır⁶²⁵. 1 Ağustos 2018 tarihinde ise GVKT'nin uygulanması için Ulusal Veri Koruma Kominyonu'nun Organizasyon Kanunu ve Genel Veri Koruma Çerçevesine dair Kanun'u yürürlüğe girmiştir. Böylece 2002 tarihli Veri Koruma Kanunu yürürlükten kaldırılmıştır⁶²⁶.

Macaristan ise 1992 yılında Kişisel Verilerin Korunması ve Kamu Yararı Verilerine Kamusal Erişim Hakkında Kanun'u kabul etmiştir⁶²⁷. GVKT'nin uygulanması bakımından ise Macaristan Parlamentosu iki aşamalı bir yol izlemiştir. Buna göre

[2582DB00356767/\\$file/4670%2031%207%202018%20PARARTHMA%201o%20MEROS%20I.pdf](https://www.dlapiperdataprotection.com/index.html?t=law&c=PL&c2=) , E.T. 03.05.2019.

⁶²³ Handbook on Data Protection Laws of the World- Lithuania, 16.10.2018, DLA Piper, <https://www.dlapiperdataprotection.com/index.html?t=law&c=PL&c2=> , E.T. 03.05.2019; Kanun metni için bkz. <https://www.e-tar.lt/portal/lt/legalAct/43cddd8084cc11e8ae2bfd1913d66d57> , E.T. 03.05.2019.

⁶²⁴ Register of Commission Expert Groups and Other Similar Entities, E03461 - Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, Updated Table GDPR Implementation Member States, 11.04.2019, <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=30306> , E.T. 03.05.2019; Kanun metni için bkz. <https://likumi.lv/ta/id/300099-fizisko-personu-datu-apstrades-likums> , E.T. 03.05.2019.

⁶²⁵ FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, s. 153- 154.

⁶²⁶ Handbook on Data Protection Laws of the World- Luxembourg, 10.01.2019, DLA Piper, <https://www.dlapiperdataprotection.com/index.html?t=law&c=LU&c2=> , E.T. 02.05.2019; Kanun metni için bkz. <http://legilux.public.lu/eli/etat/leg/loi/2018/08/01/a686/jo> , E.T. 03.05.2019.

⁶²⁷ FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, s. 155.

öncelikle mevcut olan Bilginin Geleceğini Belirleme ve Bilgi Edinme Hakkına dair 2011 tarihli Kanun'da değişikliğe gidilmiştir. Bu değişiklikler, Veri Koruma Otoritesi'nin atanması ve ilk defa veri ihlali halinde bu Otorite'ye ceza verme yetkisi yerine ikaz yetkisinin verilmesine ilişkindir. Bu hali ile Kanun 30 Haziran 2018'de yürürlüğe girmiştir. Bilginin Geleceğini Belirleme ve Bilgi Edinme Hakkına dair 2011 tarihli Kanun'da ikinci değişiklik ise, 2016/680 sayılı Direktif sebebiyle ilgili düzenlemeyi bütünüyle kabul etmek biçiminde olmuştur⁶²⁸.

2001 yılında Malta da kişisel verilerin korunması ile ilgili hukuki düzenlemeleri yapmıştır. Malta Parlamentosu 24 Mayıs 2018 tarihinde Veri Koruma Kanunu'nu kabul etmiştir. Anılan düzenleme 29 Mayıs 2018'de uygulamaya konulmuştur⁶²⁹.

Polonya, 29 Ağustos 1997 tarihinde Kişisel Verilerin Korunması Kanunu'nu kabul etmiştir. GVKT bakımından ise, 12 Eylül 2017'de kişisel verilerin korunmasına ilişkin iki adet taslak kanun yayımlamıştır. İlki, 25 Mayıs 2018'de yürürlüğe giren Kişisel Verilerin Korunması Kanunu'dur. Bir diğeri ise bu Kanun'un Uygulama Kanunu'dur. Yeni Veri Koruma Kanunu ile önceki Kanun'a kıyasla çok daha geniş yetkileri olan bir veri koruma otoritesi olan Kişisel Verilerin Korunması Ofisi kurulmuştur⁶³⁰.

Portekiz, 1976 tarihli Anayasası'nda bilgi teknolojileri ile bağlantılı olarak kullanılan kişisel verilerin korunması hakkını anayasal bir hak olarak garanti altına alan ilk Avrupa ülkesidir. Ancak otomatik veri işlemenin şeffaf olması gereği ile özel yaşam ve aile yaşamı dahil diğer temel hak ve özgürlüklere saygı duyan ve vatandaşlara çeşitli

⁶²⁸ Handbook on Data Protection Laws of the World- Hungary, 10.01.2019, DLA Piper, <https://www.dlapiperdataprotection.com/index.html?t=law&c=HU&c2=> , E.T. 03.05.2019; Kanun'un değiştirilmiş hükümleri için bkz. <https://www.parlament.hu/irom41/00335/00335-0003.pdf> , E.T. 03.05.2019.

⁶²⁹ Register of Commission Expert Groups and Other Similar Entities, E03461 - Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, Updated Table GDPR Implementation Member States, 11.04.2019, <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=30306> , E.T. 03.05.2019.

⁶³⁰ Handbook on Data Protection Laws of the World- Poland, 11.01.2019, DLA Piper, <https://www.dlapiperdataprotection.com/index.html?t=law&c=PL&c2=> , E.T. 03.05.2019; İlgili kanuni süreç için bkz. <http://www.sejm.gov.pl/sejm8.nsf/PrzebiegProc.xsp?nr=2410> , E.T. 03.05.2019.

güvenceler sunan Bilgisayarlarda Veri Koruma Hakkında 10 sayılı Kanun'u 29 Nisan 1991'de kabul etmiştir. 1997 yılında 95/46/AT sayılı Direktif'in iç hukuka aktarabilmek için Anayasa'nın 35. maddesi değiştirilmiştir. Devamında Direktif'i ulusal mevzuata geçiren 26 Ekim 1998 tarih ve 67 sayılı Veri Koruma Kanunu kabul edilmiştir⁶³¹. 24 Ağustos 2015 tarihinde 67 sayılı Veri Koruma Kanunu'nda 95/46/AT sayılı Direktif uyarınca değişikliğe gidilmiştir. GVKT'nin ardından ise, Portekiz'in veri koruma hukuku GVKT'nin etkisi altındadır. Bu bağlamda Tüzük'ün uygulanmasına ilişkin kanun tasarısı ise henüz Parlamento'dadır⁶³².

Romanya da 2001 yılında 95/46/AT Sayılı Direktif'i kabul etmiş ve kişisel verilerin korunması ve serbetçe dolaşımları hakkında hukuki bir düzenleme gerçekleştirmiştir. GVKT'nin hükümlerinin uygulaması için ise, 31 Temmuz 2018'de GVKT'nin Uygulamasına dair Önlemlere ilişkin 190/2018 sayılı Kanun yürürlüğe girmiştir⁶³³.

1998'de Slovakya, Dosyalama Sistemlerinde Kişisel Verilerin Korunması Kanunu'nu düzenlemiştir. GVKT'nin ardından ise Tüzük'ün uygulaması için 25 Mayıs 2018'de Veri Koruma Kanunu yürürlüğe girmiştir⁶³⁴.

Slovenya ise 1990'ların başında kişisel verilerin korunması ile ilgili düzenlemeyi kabul etmiştir ve söz konusu bu düzenlemede, 1999 yılındaki Kişisel Verilerin

⁶³¹ SOARES, *Online Privacy Law: Portugal Country Report*, https://www.loc.gov/law/help/online-privacy-law/2012/portugal.php#_ftn6, E.T. 02.05.2019.

⁶³² Handbook on Data Protection Laws of the World- Portugal, 11.01.2019, DLA Piper, <https://www.dlapiperdataprotection.com/index.html?t=law&c=PT>, E.T. 02.05.2019.

⁶³³ Register of Commission Expert Groups and Other Similar Entities, E03461 - Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, Updated Table GDPR Implementation Member States, 11.04.2019, <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=30306>, E.T. 03.05.2019; Kanun metni için bkz. http://www.cdep.ro/pls/proiecte/upl_pck2015.proiect?cam=2&idp=16976, E.T. 03.05.2019.

⁶³⁴ Register of Commission Expert Groups and Other Similar Entities, E03461 - Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, Updated Table GDPR Implementation Member States, 11.04.2019, <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=30306>, E.T. 03.05.2019; Kanun metni için bkz. <https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/18/20180525>, E.T. 03.05.2019.

Korunması Kanunu ile değişikliğe gidilmiştir⁶³⁵. GVKT sonrası ise, her ne kadar bir veri koruma düzenlemesi hazırlanmış olsa da genel seçimler ve yeni bir hükümet kurulması nedeniyle yürürlüğe giren bir kanun mevcut değildir⁶³⁶.

1992 yılında Yunanistan ise, 108 Sayılı Sözleşme’yi onaylamıştır. 1997 yılında da 95/46/AT Sayılı Direktif’in kurallarını iç hukuka taşıdığı 2472 Sayılı Kişisel Verilerin İşlenmesi Hakkında Kanun’u kabul etmiştir. Bu tarihe dek, veri işleme konusunu düzenleyen herhangi bir ulusal belgeyi kabul etmemiştir⁶³⁷. GVKT’nin uygulanması için gereken hukuki önlemler 20 Şubat 2018 tarihinde bir Kanun Tasarısı ile ortaya konmuştur; ancak bu metin henüz yürürlüğe girmemiştir⁶³⁸.

Yukarıda açıklandığı üzere, Veri Koruma Reformu öncesi, 95/46/AT Sayılı Direktif üye ülkelere kademeli olarak aktarılmış ve bu durum “kişisel veri”, “veri koruma” gibi kavramlarının tüm Avrupa’ya yayılmasını sağlamıştır. Ancak yalnızca az bir kısmı Direktif ve 108 Sayılı Sözleşme’de olduğu gibi “*kişisel verilerin korunması özel yaşamın gizliliğine hizmet etmektedir.*” fikrini açıkça içermektedir⁶³⁹. GVKT bakımından ise, her ne kadar çoğu AB ülkesi iç hukuklarında Tüzük’ün uygulamasına dair hükümlerde yeni düzenleme ve değişiklikler yapmışsa da bir kısmı GVKT’yi benimsemek konusunda yavaş kalmış ve kalmaktadır.

⁶³⁵ FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, s. 155.

⁶³⁶ Handbook on Data Protection Laws of the World- Slovenia, 10.01.2019, DLA Piper, <https://www.dlapiperdataprotection.com/index.html?t=law&c=SI&c2=>, E.T. 03.05.2019.

⁶³⁷ FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, s. 149.

⁶³⁸ Sotiris I. DEMPEGIOTIS, Eirini G. CHAGIOU, “Personal Data Protection”, Greek Law Digest, 05.03.2019, <http://www.greeklawdigest.gr/topics/data-protection/item/111-personal-data-protection>, Handbook on Data Protection Laws of the World- Greece, 17.10.2018, DLA Piper, <https://www.dlapiperdataprotection.com/index.html?t=law&c=GR&c2=>, E.T. 30.04.2019.

⁶³⁹ FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, s. 156.

ÜÇÜNCÜ BÖLÜM

AVRUPA VERİ KORUMA HUKUKUNUN TÜRK HUKUK SİSTEMİNE ETKİSİ

Avrupa Veri Koruma Hukuku'nun 1970'lerden günümüze geçirdiği tüm safhalar, hazırlanan hukuki düzenlemeler ile bunların mahkeme kararlarına yansımaları ele alındıktan sonra kişisel verilerin korunmasının Türkiye'deki görünümünün ele alınması gerekmektedir. Bu bakımdan ilk olarak bu hakkın anayasal açıdan ne şekilde korunduğu önem taşımaktadır. Çalışmamızın bu kısmında, kişisel verilerin korunmasının bağımsız bir anayasal hak olarak tanınması süreci ortaya konacaktır. Bu noktada anayasa hukuku bakımından böyle bir hakkın temel kanunla korunması gereği, Alman Federal Anayasa Mahkemesi'nin meşhur nüfus sayım kararı ile ilişkilendirilerek ele alınacak ve 2010 tarihli Anayasa Değişiklikleri ile hukukumuzda nihayet bağımsız bir anayasal hak olarak giren kişisel verilerin korunması hakkına ilişkin düzenleme incelenecektir. Ayrıca kişisel verilerin korunmasının bir hak olarak tanınmasından önce de Anayasa'da yer alan diğer bazı temel hak ve özgürlüklerle ilişkilendirilerek anayasa hukuku korumasından yararlandığı tespiti ile bu hak ve özgürlüklere değinilecektir. Kişisel verilerin korunması ile ilgili hükümlere yönelik önemli mahkeme kararları ise "Anayasal Düzenlemeler" başlığı altında ele alınmayıp iç içe geçmiş örüntülerini ortaya koyabilmek adına "İlgili Anayasal İçtihat" başlığı altında, temel hak ve özgürlüklerin sınırlandırılmasında esas alınan ölçütler bağlamında bağımsız bir biçimde ele alınacaktır.

Anayasal görünümü bu biçimde çerçevelenen hakka ilişkin olarak yasal gelişim hususunda ise ilk olarak, her ne kadar 1981 tarihli 108 Numaralı Sözleşme imzaya açıldığı gün imzalarsa da ilgili yasal düzenlemenin 2016 yılına dek yapılmamış olmasının veri koruma bağlamında yarattığı negatif etkiden bahsedilecektir. Avrupa Veri Koruma Hukuku'nun gelişim süreci ile kıyaslandığında oldukça geriden gelen Türkiye'nin, 6698 Sayılı Kişisel Verilerin Korunması Kanunu'nun hangi bakımlardan Veri Koruma Reformu'nun gerisinde kaldığı, Kanun'un içeriğinden bahsedilerek açıklanmaya çalışılacaktır.

I. ANAYASAL HÜKÜMLER VE KANUNİ DÜZENLEME

A. ANAYASAL DÜZENLEMELER

1. Kişisel Verilerin Korunması Hakkı (AY md. 20/3)

Anayasa, bir devletin temel yapısını, kuruluşunu, iktidarın devroluş biçimi düzenlemekle birlikte, iktidar karşısında bireylerin temel hak ve özgürlüklerini de düzenleyen metinlerdir. Daha açık bir ifadeyle Anayasal düzenlemeler, kişinin temel hak ve özgürlüklerini koruma altına almaktadır. Bunun yanı sıra, bir özgürlüğün Anayasa’da hak olarak tanınması ile devletin bu alana müdahalesi önlenmek istenmektedir. Ayrıca Anayasa, iç hukuk düzeninde normlar hiyerarşisi bakımından en üst sırada yer almaktadır. Bu bakımdan da bir temel hak ve özgürlüğün yalnızca yasal olarak düzenlenmeyip ayrıca anayasal olarak da metin altına alınması bu ilkenin normlar hiyerarşisi gereğince, Anayasanın üstünlüğü ilkesinden de yararlanabilmesini sağlamaktadır⁶⁴⁰.

Bireyin verilerine dair karar verme özgürlüğü ve buna yönelik tehlikeler sebebiyle bireyin anayasal olarak korunması ve özellikle kamusal organların sınırsız bir şekilde veri işleyebilme yetkisine anayasal sınırların konulması gereği ile kişisel verilerin korunması bir temel hak olarak kabul edilmiştir. Dolayısıyla kişisel verilerin korunması, birey açısından bir hak olduğu kadar, kamusal organlar bakımından bir yükümlülüktür⁶⁴¹. İlaveten yukarıda belirtildiği üzere, bir temel hak olarak Anayasa’da kayıt altına alınan kişisel verilerin korunması hakkı, normlar hiyerarşisi gereğince Anayasanın üstünlüğü ilkesine de işlerlik kazandırmaktadır.

Kişisel verilerin korunması hakkı, demokratik bir toplumsal yapı bakımından da önem arz etmektedir. Şayet birey, kendisi hakkındaki verilerin kim tarafından, nerede, nasıl, hangi gerekçe ile bulunduğunu bilemezse kişisel verileri üzerindeki bir korumadan

⁶⁴⁰ Erdoğan TEZİÇ, *Anayasa Hukuku Genel Esaslar*, Beta, Gözden Geçirilmiş 14. Baskı, 2012, s. 93- 98.

⁶⁴¹ Oğuz ŞİMŞEK, *Anayasa Hukukunda Kişisel Verilerin Korunması*, Beta, 2008, s. 113; AKGÜL, *Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması*, s. 219.

da bahsedilemeyecektir. Böylesi bir ortamda hem kişinin özgürlük alanı ihlal edilecek, hem de kişinin kendi yaşamını belirleyebildiği özgürlükçü bir demokrasi mümkün olabilecektir. Bu bakımdan kişisel verilerin korunması hakkı, kişinin diğer temel hak ve özgürlüklerinin kullanılması için de oldukça önemlidir⁶⁴².

Kişisel verilerin korunması hakkı temel bir hak olarak, yasal bir temele ya da ilgilinin rızasına dayalı olmadan kişinin verilerine bir müdahale olduğu hallerde bu verilerin ve dolayısıyla ilgili kişinin korunmasını ve ayrıca bu kişinin verileri üzerinde serbestçe karar verebilmesini sağlamayı amaçlamaktadır⁶⁴³.

Kişisel verilerin korunması hakkının anayasal bir temele oturtulma çabasının ilk ve önemli bir örneği olarak Alman Federal Anayasa Mahkemesi'nin nüfus sayım kararı ele alınmalıdır. 1983 yılında Alman Federal Hükümeti, Nüfus Sayım Kanunu ışığında genel nüfus sayımı yapmayı planlıyordu. Fakat halkta, böylesi istatistiksel bir nüfus sayımının mahremiyete gereksiz bir müdahale olduğu duygusu hakimdi. Bu bağlamda ilgili kanun, Alman Federal Anayasa Mahkemesi'nin (*Bundesverfassungsgericht*) önüne gitti. Mahkeme 1984'te, Nüfus Sayım Kanunu'nun kısmen anayasaya aykırı olduğuna karar vererek sayımı iptal etmiştir⁶⁴⁴.

Alman Federal Anayasa Mahkemesi bu kararda, insan onurundan yola çıkarak kişilik hakkının korunması ile bağlantı kurmuştur. Kişinin öz belirleme hakkı, genel kişilik hakkının bir parçasıdır. Bu nedenle, her insana özgür ve özerk bir kişilik geliştirme imkânı verme fikriyle yakından bağlantılıdır. Kararın en önemli noktası da kişinin verileri üzerindeki verilerin korunmasına dair hakkının, insan onuru ve kişiliğin serbestçe

⁶⁴² ŞİMŞEK, *Anayasa Hukukunda Kişisel Verilerin Korunması*, s. 112- 114; AKGÜL, *Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması*, s. 220.

⁶⁴³ ŞİMŞEK, *Anayasa Hukukunda Kişisel Verilerin Korunması*, s. 114.

⁶⁴⁴ Gerrit HORNUNG, Christoph SCHNABEL, "Data protection in Germany I: The population census decision and the right to informational self-determination", *Computer Law & Security Report*, Vol.: 25, Issue 1, 2009, ss. 84-88, s. 84; WEBB, "A Comparative Analysis of Data Protection Laws in Australia and Germany", s. 6.

geliştirilmesi hakkından çıkartılarak bağımsız bir hak olarak anayasal bir temele oturtulmasıdır⁶⁴⁵.

Karara konu olan Nüfus Sayım Kanunu, vatandaşlar için yaptırıma bağlı olarak istatistiki amaçlarla kapsamlı bilgilerin açıklanması yükümlülüğünü getirmekteydi. Dolayısıyla Alman Federal Anayasa Mahkemesi bu durumun, bireyin kişisel verilerinin geleceğini belirleme hakkını ihlal ettiğine hükmetmiştir. Mahkeme’ye göre, haklarına yapılan müdahalelerin gerekli görülmesi durumunda, vatandaşların kişisel verilerinin işlenmesiyle bağlantılı olan kişilik risklerini değerlendirebilecekleri bir pozisyona getirilmeleri gerekir. Bu nedenle, veri işlemenin kapsamı, yoğunluğu ve amacı şeffaf olmalıdır. Alman Federal Anayasa Mahkemesi özellikle kişinin verilerine gizli biçimde müdahaleler olabileceğini dikkate alarak, veri işlemede veriler arası çok yönlü bağlantıların kurulması halinde görünüşte önemsiz gibi görünen verilerin başka bazı verilerle birleşerek kişinin davranış tarzının belirlenebilmesinin mümkün olabileceğini ve bu sebeple anayasal açıdan korunmalarının çok daha elzem olduğunu vurgulamıştır. Ancak Mahkeme’ye göre, yine doğaldır ki bu durum kişinin kendi verileri üzerinde bir mülkiyet hakkına sahip olduğu anlamına gelmez; kamu yararı dolayısıyla bu hakka müdahale mümkündür⁶⁴⁶.

Mahkeme nüfus sayım kararında, daha sonra 95/46/AT Sayılı Direktif’te ve GVKT’de de yer alan, tüm Avrupa’da veri korumanın temel ilkeleri olarak kabul edilebilecek veri denetçisinin yükümlülükleri, veri öznesinin hakları, amaç belirleme ve orantılılık gibi bir dizi veri koruma ilkesini benimsemiştir⁶⁴⁷.

Anayasal temelleri bu şekilde atılan kişisel verilerin korunması hakkı, kişiye ait verilerin kendisini değil, bu verilerin kişinin istemi dışında ortaya dökülmesi halinde

⁶⁴⁵ HORNUNG, SCHNABEL, “Data protection in Germany I: The population census decision and the right to informational self-determination”, s. 86.

⁶⁴⁶ HORNUNG, SCHNABEL, “Data protection in Germany I: The population census decision and the right to informational self-determination”, s. 86.

⁶⁴⁷ HORNUNG, SCHNABEL, “Data protection in Germany I: The population census decision and the right to informational self-determination”, s. 87.

kişinin zarar görecektir özgürlüklerinin korunmasını amaçlamaktadır. Dolayısıyla kişinin verilerinin anayasal olarak korunması, diğer birçok temel hak ve özgürlüğün de korunmasını sağlamaktadır⁶⁴⁸.

Bununla birlikte kişisel verilerin korunması hakkı, sınırsız bir hak olarak formüle edilmemiştir. Kamu yararının söz konusu olduğu hallerde müdahale mümkün olabilmektedir. Söz gelimi kişisel verilerin korunması hakkına, devletin hukuk devleti ve sosyal devlet olması gereği ile yürüttüğü görevlerinde bilgi gereksinimi duyduğunda başvuracağı sınırlamalar bu bağlamda değerlendirilir. Doğardır ki söz konusu sınırlamalar- müdahaleler ölçülülük ilkesi bağlamında değerlendirilmelidir. Ölçülülük ilkesi ise, temel hakkın sınırlandırılmasında başvuru araç, sınırlama amacını gerçekleştirmeye elverişli olması ve araçla amaç arasında bir ölçüsüzlük bulunmaması gerektiğine işaret etmektedir⁶⁴⁹. İlâveten kişisel verilerin korunması hakkına yapılacak müdahale ve sınırlamalar bakımından normların açıklığı ilkesine de uyulmalı; bu bağlamda kişisel verilerin korunması hakkında sınırlamaya imkân tanıyan yasal düzenlemelerin açık ve herkesçe anlaşılabilir olması gerekmektedir. Yine bu kapsamda belirtilmelidir ki, kişisel verilerin korunması hakkına yapılacak sınırlamalarda amaca bağlılık ilkesi de mutlak surette dikkate alınmalıdır. Buna göre, veri toplama, işleme ve saklama belirli bir amaç doğrultusunda gerçekleştirilmeli ve bu amaçtan sapılmamalıdır⁶⁵⁰.

Kişisel verilerin korunması bakımından hukuksal düzenlemeler anlamında Türkiye ise geri kalmıştır. Avrupa Konseyi'nin 108 Numaralı Kişisel Verilerin Otomatik İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşmesi 28 Ocak 1981 tarihinde imzaya açılmış ve Türkiye bu Sözleşme'yi aynı gün imzalamıştır. Fakat ilgili hukuki düzenleme yapılmadığı için anılan Sözleşme'nin uygun bulma kanununun kabulü

⁶⁴⁸ ŞİMŞEK, *Anayasa Hukukunda Kişisel Verilerin Korunması*, s. 119.

⁶⁴⁹ Ergun ÖZBUDUN, *Türk Anayasa Hukuku*, 17. Basım, Yetkin Yayınları, Ankara, 2017, s. 116- 117.

⁶⁵⁰ ŞİMŞEK, *Anayasa Hukukunda Kişisel Verilerin Korunması*, s. 125- 126.

ancak 30 Ocak 2016 tarihinde olabilmıştır⁶⁵¹. Bu durum sebebiyle Türkiye anılan dönemde, Konsey üyesi devletler arasında konuyla ilgili kapsayıcı bir düzenleme yapmamış tek ülkedir⁶⁵².

Daha evvel dile getirildiği üzere, Avrupa’da özellikle 1970’lerle birlikte bir ivme yakalayan söz konusu hak, öncelikle 12 Eylül 2010 tarihinde gerçekleşen referandum sonrası kabul edilen Anayasa Değişikliği⁶⁵³ ile 1982 tarihli Türkiye Cumhuriyeti Anayasası’nın 20. maddesinin 3. Fıkrasına eklenmiş⁶⁵⁴ ve ardından 7 Nisan 2016

⁶⁵¹ Murat Volkan DÜLGER, “Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması”, *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi*, C. 3(2), Y. 2016, s. 106, ss. 101- 167.

⁶⁵² KÜZECİ, *Kişisel Verilerin Korunması*, s. 284.

⁶⁵³ 07.05.2010 tarih ve 5982 sayılı Türkiye Cumhuriyeti Anayasasının Bazı Maddelerinde Değişiklik Yapılması Hakkında Kanun ile yapılan Anayasa değişiklikleri, 12.09.2010 tarihindeki referandum ile kabul edilmiştir. 22.09.2010 tarih ve 846 sayılı Yüksek Seçim Kurulu Kararı da 23.09.2010 tarih ve 27708 sayılı Resmî Gazete’de yayımlanmıştır. Resmî Gazete, 23.09.2010 Perşembe, S. 27708, Yüksek Seçim Kurulu Kararı, Karar No: 846, <http://www.resmigazete.gov.tr/eskiler/2010/09/20100923-10.htm> , E.T. 05.04.2019.

⁶⁵⁴ Kişisel verilerin korunması hakkı her ne kadar 1982 tarihli Türkiye Cumhuriyeti Anayasası’na 2010 yılında 20/3. Madde ile girmişse de bu tarihten önceki iki Anayasa Taslak ve Önerisi’nde de kendisini göstermiştir. 2007 yılında Türkiye Barolar Birliği, öncelikle bir Bilim Kurulu’na bir Anayasa Önerisi hazırlatmış, ardından ilgili düzenlemeyi Yasama Meclisi’ne sunmuştur. Söz konusu Öneri’nin “*Kişisel bilgi ve verilerin korunması*” başlıklı 33. Maddesine göre; “*Herkes kendi yaşamına ve varlığına ilişkin özel bilgi ve verilerin gizli tutulmasını ve korunmasını isteme hakkına sahiptir. Bu bilgiler, ancak kişinin iznine veya kanunda öngörülen hukukun geçerli sayacağı başka bir nedene dayalı olarak kullanılabilir. Herkes, kendisi hakkında toplanmış olan veya bilişim kayıtlarında yer alan bilgilere erişme, bunlarda düzeltme yaptırma ve bu bilgilerin amaçları doğrultusunda kullanılıp kullanılmadığını bilme hakkına sahiptir.*”

Bu kuralların uygulanması, kanunla kurulmuş bağımsız bir makam tarafından sağlanır ve denetlenir.” Türkiye Barolar Birliği, *Türkiye Cumhuriyeti Anayasa Önerisi*, Haz. Rona AYBAY, Fazıl SAĞLAM, Süheyl BATUM, Oktay UYGUN, Korkut KANADOĞLU, Ece GÖZTEPE, Faruk BİLİR, Teoman ERGÜL, Geliştirilmiş Gerekçeli Yeni Metin, 2011, 5. Baskı, <http://tbbyayinlari.barobirlik.org.tr/TBBBooks/tcao-423.pdf> , E.T. 04.04.2019. Öneri’de yer alan maddenin dikkat çekici bir özelliği, “bağımsız bir makam tarafından hakkın uygulanışının denetlenmesi” hükmüdür.

Yine aynı yıl, bu kez Adalet ve Kalkınma Partisi’nin Prof. Dr. Ergun ÖZBUDUN başkanlığında bir Bilim Kurulu’na hazırlattığı Anayasa Taslağı da “Kişisel Bilgilerin Korunması” başlıklı 20. Maddesinde; “*Herkes, kendisiyle ilgili kişisel bilgi ve verilerin korunması hakkına sahiptir.*”

Bu bilgiler, ancak kişinin açık rızasına veya kanunla öngörülen meşru bir sebebe dayalı olarak kullanılabilir. Herkes, kendisi hakkında toplanmış olan veya kayıtlarda yer alan bilgilere erişme, bunlarda düzeltme yaptırma ve bu bilgilerin amaçları doğrultusunda kullanılıp kullanılmadığını öğrenme hakkına sahiptir.” diyerek söz konusu hakkı anayasal koruma altına almıştır. Ergun ÖZBUDUN, “Türkiye Cumhuriyeti Anayasa Önerisi”, Haz. Ergun ÖZBUDUN, Zühtü ARSLAN, Yavuz ATAR, Fazıl Hüsnu

tarihinde 6698 sayılı Kişisel Verilerin Korunması Kanunu’nun yürürlüğe girmesi ile güvence altına, bazı hususlarda eksiklikler de olsa, alınmıştır.

2010 Anayasa Değişikliği ile 1982 Anayasası’nın 20/3. maddesine getirilen kişisel verilerin korunması düzenlemesine bakıldığında;

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

denilmektedir. Buna göre kişisel verilerin korunması hakkı (Anayasa ifade ile, kişisel verilerin korunmasını isteme hakkı), kişisel verilerle ilgili bilgilendirilme, erişim, düzeltme ve sildirme hakkı ile kişisel verilerin amacı doğrultusunda kullanılıp kullanılmadığını öğrenme halarını kapsamaktadır. Öncelikle belirtilmelidir ki, bu madde ile kişisel verilerin korunması hakkı anayasal güvence altına alınmıştır. Kişisel verilerin korunması hakkı, bir özgürlük değil, hak alanı olarak düzenlenmiştir. Bilindiği üzere özgürlükler dokunulmazlığı ifade ederken, haklar talep edilebilirliği vurgulamaktadır⁶⁵⁵. Bu bakımdan kişisel verilerin korunmasının hak kavramı çatısı altında oluşu talep edilebilirliği sağlaması açısından çok daha yerinde olmuştur. Artık kişisel verilerin korunması mutlak surette 1982 Anayasası’nın 20/3. maddesi bağlamında

ERDEM, Levent KÖKER, Serap YAZICI, 2007, <http://bianet.org/bianet/siyaset/101746-akp-nin-anayasa-taslaginin-tam-metni> , E.T. 04.04.2019. Bu Taslak’ta ise, kişisel verilerin işlenmesini denetleyecek bağımsız bir organa yer verilmemiştir. Bu durum doktrinde eleştirilmiş; ancak zaten getirdiği düzenlemelerle Hakimler ve Savcılar Yüksek Kurulu, Anayasa Mahkemesi, Danıştay ve Yüksek Öğretim Kurulu’nun oluşumunu Meclis’te yer alan çoğunluğa göre belirleyen bu Taslak’ın, anılan hakkın uygulamasını bağımsız bir organca denetlenmesini düzenlemesinin beklenmeyeceği dile getirilmiştir. Oktay UYGUN, “İnsan Hakları Açısından Yeni Anayasa Çalışmaları”, *Kamu Hukuku İncelemeleri – İnsan Hakları, Demokrasi, Hukuk Devleti ve Egemenlik*, 2. Baskı, On İki Levha Yayıncılık, İstanbul, 2013, s. 199- 235; Aynı yönde bkz. Fikret İLKİZ, “Kişisel Verilerin Korunması Kanunu”, <http://bianet.org/bianet/insan-haklari/174173-kisisel-verilerin-korunmaması-kanunu> , E.T. 04.04.2019.

⁶⁵⁵ Bülent TANÖR, Necmi YÜZBAŞIOĞLU, 1982 Anayasasına Göre Türk Anayasa Hukuku, 12. Baskı, Beta, 2012, s. 133.

değerlendirilmelidir. Bunun yanı sıra kişisel verilerin korunması hakkına dair söz konusu anayasal düzenleme ile taraf olduğumuz uluslararası düzenlemelerde yer alan veri korumaya dair yükümlülüklerimize ilişkin anayasal dayanak sağlanmıştır⁶⁵⁶.

Bu hüküm, veri korumaya dair bazı temel hususları içermekte ve eskiye nazaran daha etkin bir koruma sağlamaktadır. Fakat bu düzenleme bazı noktalarda eksiktir⁶⁵⁷. Buna göre, daha önce 2007 tarihli Ergun ÖZBUDUN Anayasa Taslağı eleştirisinde dile getirildiği üzere, bu düzenleme de hakkın uygulamasını denetleyecek bağımsız bir organdan yoksundur. Daha önceki bölümlerde dile getirildiği üzere, Avrupa Birliği Adalet Divanı, birçok kararında “bağımsız denetim organları”nın varlığını, AB Temel Haklar Şartı md. 8/3 ve AB’nin İşleyişine Dair Anlaşma md. 16/2’den yola çıkarak kişisel verilerin korunmasının temel şartı olduğunu belirtmiştir⁶⁵⁸. Durum böyle olmakla birlikte, 1982 Anayasası’nın 20/3. maddesinde böyle bir eksiklik bulunsa da bağımsız bir denetim organı oluşturulabilir. İkinci bir eksiklik olarak ise madde metninde niçin kişisel verilerin korunması hakkı değil de kişisel verilerin korunmasını isteme hakkının düzenlenmiş olduğu eleştirilmektedir. Ayrıca kişisel verilerin korunması hakkı Anayasa ile güvence altına alınmış olması nedeniyle, hakkın sağlanması kural ve hakkın sınırlandırılması ise istisna teşkil etmelidir. Fakat madde metninde kişisel verilerin ancak kanunda öngörülen hallerde veya kişinin açık rızası ile işlenebilmesi ifadesi dikkat çekmekte ve kişisel verilerin hangi durumlarda işlenebileceği ele alınmaktadır. Oysa Anayasa’nın 13. maddesine göre de temel hak ve özgürlükler yalnızca Anayasa’nın ilgili maddelerinde belirtilen sebeplere bağlı olarak sınırlandırılabilir. Böylesi bir

⁶⁵⁶ AKGÜL, *Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması*, s. 222.

⁶⁵⁷ Eleştiriler için ayrıca bkz. KÜZECİ, *Kişisel Verilerin Korunması*, s. 290-291; KÜZECİ, “Anayasal Bir Hak: Kişisel Verilerin Korunması”, s. 146.

⁶⁵⁸ Case C-614/10, *European Commission v. Republic of Austria*, 16 October 2012, Par. 37, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62010CJ0614>, E.T. 04.04.2019; Case C-288/12, *European Commission v. Hungary*, 08 April 2014, Par. 48, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0288>, E.T. 04.04.2018; *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, 08.04.2014, Par. 68, <http://curia.europa.eu/juris/celex.jsf?celex=62012CJ0293&lang1=en&type=TEXT&ancre=>, E.T. 04.04.2019.

durum ise hakkın koruma alanını riske ederek, ölçüsüz sınırlamaya sebep olarak hakkın varlığını tehlikeye düşürebilecektir⁶⁵⁹.

Anayasa maddesine ilişkin ana eksikler bunlar olarak görülmekte ise de hakkın efektif bir hukuki korumaya sahip olabilmesinin önündeki bir diğer engel de 20/3 hükmünde belirtilen “*Kişisel verilerin korunmasına ilişkin usul ve esslar kanunla belirlenir.*” ifadesindeki kanunun yapımının 7 Nisan 2016 tarihine dek yapılmamış olmasıdır. Türkiye’de bu tarihe dek kişisel verilerin korunmasına dair müstakil bir kanun ve veri işleme sürecini denetleyecek bir kurum bulunmuyordu. Yine de ilgili dönemde kişisel verilerin tamamen korumasız kaldığı söylenemese de tam ve etkili bir korumanın sağlanabilmesi için spesifik kanunun yapılması için uzun süre beklenmiştir.

Türkiye her ne kadar kişisel verilerin korunması hakkını Anayasa’da ayrı bir hak olarak düzenlemeyi 2010 yılında, bu hakka özgülenmiş kanunu yapmayı 2016 yılına bırakmışsa da ilgili konu bu tarihler öncesinden de bazı anayasal ve yasal düzenlemelerle kısmen de olsa korunuyordu denebilir. Şöyle ki, Türk Medeni Kanunu, Türk Borçlar Kanunu, Türk Ceza Kanunu gibi bazı temel kanunlar anılan hakka dair çeşitli güvencelere yer vermiştir. Ancak bu çalışmanın kapsamı bağlamında aşağıda özellikle inceleneceği üzere, Anayasa’da yer alan bazı temel hak ve özgürlükler, kişisel verilerin korunmasını belli başlı boyutları ile gerçekleştirmiştir.

2. İlgili Diğer Haklar

Yukarıda belirtildiği üzere, 2010 yılında gerçekleşen Anayasa Değişikliği ile 1982 tarihli Türkiye Cumhuriyeti Anayasası’nın 20. maddesinin 3. Fıkrasına “*Kişisel Verilerin Korunması Hakkı*” artık temel hak ve özgürlükler arasında düzenlenmektedir. Bu düzenleme öncesinde ise söz konusu hak, tıpkı kendi tarihi gelişim sürecinde olduğu gibi, başka birçok temel hak ve özgürlük sayesinde korunmaktaydı. Kaldı ki kişisel verilerin korunmasının Anayasa’da ayrı bir hak kategorisi olarak düzenlenmeyip, başka bazı temel haklar bağlamında korunduğu birçok ülke Anayasası da mevcuttur. Kişisel verilerin

⁶⁵⁹ KÜZECİ, *Kişisel Verilerin Korunması*, s. 291.

korunmasının Anayasa’da ayrı bir hak olarak düzenlenmediği ülkelerde genel olarak özel yaşamın gizliliği hakkı şemsiyesinde bir koruma sağlanırken, söz gelimi Fransa’da “Özgürlük Hakkı” nezdinde, Almanya’da ise “Genel Kişilik Hakkı” çerçevesinde güvence bulmaktadır. Bu durum kişisel verilerin korunmasının bir hak olarak kabul edilmesinin öncesinde düzenlenen Anayasalar bakımından böyledir. Öte yandan sonrasında yapılan Portekiz İspanya, Avusturya gibi bazı ülke Anayasaları da kişisel verilerin korunmasına ayrı bir hak kategorisi olarak yer vermektedir⁶⁶⁰. Dolayısıyla bu bağlamda görülmektedir ki, kişisel verilerin korunması hakkı, başka birçok hak ve özgürlük nezdinde de korunabilmektedir.

Kişisel verilerin korunması, daha önce de belirtildiği üzere, en temelde özel yaşamın gizliliği ile doğrudan ilgi olsa ve onun içerisinde büyüyüp gelişse de insan onuru, kişinin maddi ve manevi varlığını geliştirme hakkı, düşünce özgürlüğü ve başka birçok temel hak ve özgürlükle oldukça ilgilidir. Bu haklar, kendi koruma alanları sayesinde kişisel verilerin korunması hakkına da hizmet etmektedirler. Aşağıda ele alınacak olan, kişisel verilerin korunmasına çeşitli yönlerden temel oluşturmuş anayasal hakların korunması açısından 1982 Anayasası’nın 40. maddesinin de bu noktada dile getirilmesi gerekmektedir. “Temel hak ve hürriyetlerin korunması” başlıklı 40. maddeye göre;

“Anayasa ile tanınmış hak ve hürriyetleri ihlal edilen herkes, yetkili makama geciktirilmeden başvurma imkanının sağlanmasını isteme hakkına sahiptir.

Devlet, işlemlerinde, ilgili kişilerin hangi kanun yolları ve mercilere başvuracağını ve sürelerini belirtmek zorundadır.”

Dolayısıyla kişi, verilerinin korunmasını anayasal hak ve özgürlükler bağlamında temellendirdiğinde 40. maddede dile getirilen yetkili makamlara başvurabilmelidir.

⁶⁶⁰ KÜZECİ, *Kişisel Verilerin Korunması*, s. 286- 287; SOARES, *Online Privacy Law: Portugal*, December 2017, <https://www.loc.gov/law/help/online-privacy-law/portugal.php> , E.T. 07.09.2017; Constitution of the Portuguese Republic 1976- 7th Revision 2005, <http://www.en.parlamento.pt/Legislation/CRP/Constitution7th.pdf> , E.T. 07.09.2017; FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, s. 71.

Ancak Anayasa Hukuku bağlamında yalnızca bu haklarla veri koruma hukukunun tüm alanları korunamamakta ve bu nedenle bireyin kişisel verilerinin, son yıllarda hızla gelişen teknoloji karşısında bütünüyle korunabilmesi için çok daha kapsamlı olan kişisel verilerin korunması hakkına ihtiyaç vardır. Bu bakımdan zaten kişisel verilerin korunması hakkı da felsefi temellerini belli başlı haklar da bulsa da zamanla bu hakların sınırlarını aşarak ayrı bir hak kategorisi olarak tanınmıştır.

a) İnsan Onuru ve Kişiliğin Serbest Geliştirilmesi Hakkı (Başlangıç ve AY md. 17)

İnsan onuru kavramı 1945 tarihli Birleşmiş Milletler Şartı'nda nihai bir hedef olarak ele alınmıştır. 1948 tarihli İnsan Hakları Evrensel Beyannamesi de hem Başlangıç metninde hem de 1, 22 ve 23. maddelerinde “insan onuru” kavramına değinmiş ve bu kavramı düzenlemenin temel taşlarından biri olarak görmüştür. Özellikle Başlangıç'ta belirtildiği üzere, her insan onur ve haklar bakımından eşittir ve herkes onurunun ve kişiliğinin serbestçe gelişimi için ekonomik, sosyal ve kültürel haklara sahiptir⁶⁶¹. 1966 tarihli İkiz Paktlar olarak anılan Medeni ve Siyasal Haklar Sözleşmesi ile Ekonomik, Sosyal ve Kültürel Haklar Sözleşmesi'ne de bakıldığında, “insanlık onuru”ndan bahsedilmektedir⁶⁶². İnsan Hakları Avrupa Sözleşmesi de insan onurunun güvenceleri olarak, Sözleşme'nin 3, 4 ve 8. maddelerini görmektedir⁶⁶³. Avrupa Temel Haklar Şartı

⁶⁶¹ Preamble, Art. 1, Art. 22, Art. 23, Universal Declaration of Human Rights, United Nations General Assembly, Resolution 217 A, 10.12.1948, <https://www.un.org/en/universal-declaration-human-rights/> , E.T. 30.03.2019.

⁶⁶² Preamble, Art. 13, International Covenant on Economic, Social and Cultural Rights, United Nations General Assembly, Resolution 2200 A, 16.12.1966, <https://www.ohchr.org/en/professionalinterest/pages/cescr.aspx> , E.T. 30.03.2019; Preamble, Art. 10, International Covenant on Civil and Political Rights, United Nations General Assembly, Resolution 2200 A, 16.12.1966, <https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx> , E.T. 30.03.2019.

⁶⁶³ ŞİMŞEK, *Anayasa Hukukunda Kişisel Verilerin Korunması*, s. 128.

da öncelikle Başlangıç metninde ve devamında Birinci Bölümü ve 1. maddesinde insan onuru ve insan onurunun dokunulmazlığı kavramlarını ele almaktadır⁶⁶⁴.

İnsan onuru kavramının 1982 tarihli Türkiye Cumhuriyeti Anayasası'ndaki görünümüne bakıldığında öncelikle Başlangıç metni incelenmelidir. Buna göre,

“Her Türk vatandaşının ... onurlu bir hayat sürdürme ve maddi ve manevi varlığını bu yönde geliştirme hak ve yetkisine doğuştan sahip olduğu” belirtilmektedir. 1982 Anayasası'nın 2. maddesinde ise, *“Türkiye Cumhuriyeti, ...başlangıçta belirtilen temel ilkelere dayanan ... bir hukuk Devletidir.”*

kuralı hüküm altına alınmıştır. Bu ifadeden çıkarılacak bir anlam da Başlangıç'ta 6. paragrafta belirtilen “onurlu bir hayat sürdürme ve maddi ve manevi varlığını geliştirme hak ve yetkisi”nin Cumhuriyetin temel nitelikleri arasında sayıldığıdır. Anayasa'nın 4. maddesinin de 2. maddede ele alınan Cumhuriyetin temel niteliklerini değiştirilemeyen ve değiştirilmesi teklif dahi edilemeyen kurallar arasında sayması sebebiyle, kişinin “onurlu bir hayat sürdürme ve maddi ve manevi varlığını geliştirme hak ve yetkisi”ne sahip olduğu bir hukuk devleti ilkesinin de değiştirilemeyeceği iddia edilebilir. Ayrıca 17. maddede,

“Herkes, yaşama, maddi ve manevi varlığını koruma ve geliştirme hakkına sahiptir.

Kimseye işkence ve eziyet yapılamaz; kimse insan haysiyetiyle bağdaşmayan bir cezaya veya muameleye tabi tutulamaz.”

denilmektedir. 32. maddede ise, *“Düzeltilme ve cevap hakkı, ancak kişilerin haysiyet ve şereflerine dokunulması veya kendileriyle ilgili gerçeğe aykırı yayınlar yapılması hallerinde tanınır ve kanunla düzenlenir.”* hükmü yer almaktadır⁶⁶⁵.

⁶⁶⁴ Preamble, Art. 1, Art. 25, Art. 31, Charter of Fundamental Rights of the European Union, 2012/C 326/02, 26.10.2012, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT> , E.T. 30.03.2019.

⁶⁶⁵ Başlangıç, Md. 17, Md. 32, 1982 Tarihli Türkiye Cumhuriyeti Anayasası, 18.10.1982, <https://www.mevzuat.gov.tr/MevzuatMetin/1.5.2709.pdf> , E.T. 30.03.2019.

Anayasa Mahkemesi insan onurunu şu şekilde tanımlamıştır:

“insanın ne durumda, hangi koşullar altında bulunursa bulunsun, salt insan oluşunun kazandırdığı değer tanınmasını ve sayılmasını anlatır.

Bu, öyle bir davranış çizgisidir ki, ondan aşağı düşünce, davranış, ona muhatap olan insanı, insan olmaktan çıkarır. İnsan onuru kavramını, toplumların kendi görenek ve geleneklerine ve topluluk kurallarına göre, saygıya değer olabilmesi için bir insanda bulunmasını zorunlu gördükleri niteliklerle karıştırmamak gereklidir.”⁶⁶⁶

Anayasa Mahkemesi bu kararında insan onuru kavramını belli bir topluma özgü değerleri ifade eden bir kavram olarak değil; evrensel olarak tanımlamıştır. Gerek Anayasa hükümleri gerekse Anayasa Mahkemesi’nin insan onuru tanımı incelendiğinde görülmektedir ki, Türk Anayasa Hukukunda bu kavram Anayasa ile korunan değerlerin en üst basamağında değerlendirilmeli ve bu kavramın korunması temel haklar kataloğunun en üstünde yer almaktadır⁶⁶⁷. İnsan onuru, özgürlük ve eşitlikle birlikte özgürlükler hukukunun iskeleti, hak ve özgürlüklerin temeli olarak da adlandırılmaktadır⁶⁶⁸.

İnsan onuru kavramının genel kabul gören bir tanımı bulunmamaktadır. Kavram dini, felsefi, tarihi olarak farklı biçimde tanımlanmıştır. Genel anlamda ortak bir çekirdek tanım olarak, insanın kendi sorumluluğu çerçevesinde kendi yaşamını belirleyebilme yeteneği, akıl ve vicdan sahibi insanın öz değeri gibi şekillerde tanımlama yapılabilir⁶⁶⁹. Bu bakımdan insan onuru, özgürlükçü ve demokratik bir hukuk devletin de temellerindendir. Dolayısıyla kişi kendine dair verilerine sahip çıkamayıp kişiliğini serbestçe geliştiremediğinde, zorunlu olarak şeffaflaştırılmış ve insan onurundan yoksun

⁶⁶⁶ AYM Kararı, E. 1963/ 132, K. 1966/29, T. 28.06.1966, AMKD, S. 4, s.187; Zafer GÖREN, “Avrupa Birliği Temel Haklar Şartı’nın Ana İlkesi: Dokunulmaz İnsan Onuru”, İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi, Y: 6, S. 12, Güz 2007/2, ss. 21- 37, s. 26.

⁶⁶⁷ GÖREN, “Avrupa Birliği Temel Haklar Şartı’nın Ana İlkesi: Dokunulmaz İnsan Onuru”, s. 34.

⁶⁶⁸ İbrahim Ö. KABOĞLU, *Özgürlükler Hukuku*, İmge Kitabevi, Ankara, 2002, s. 25.

⁶⁶⁹ Christopher MCCRUDDEN, “Human Dignity and Judicial Interpretation of Human Rights”, The European Journal of International Law, Vol. 19, No: 4, 2008, ss. 655- 724, s. 675, 724; UYGUN, “Çağımızın İnsan Onuruna Yöneltilmiş Tehditler Karşısında İnsan Haklarının Önemi”, s. 47- 48.

olarak obje haline dönüştürülmüş olur. Böyle bir ortamda ise, özgürlükçü ve demokratik bir toplum bulunmuyor demektir. Ayrıca kişisel verilerin korunması hakkı bakımından temel oluşturan haklardan olan maddi ve manevi varlığı geliştirme hakkı da kaynağını insan onurundan alır⁶⁷⁰.

Belirtildiği üzere, kişisel verilerin korunması hakkının temelinde esas olarak insan onuru ile birlikte kişinin maddi ve manevi varlığını koruma ve geliştirme hakkı da yatmaktadır. Bu ise, bir diğer söyleyişle kişiliğin serbestçe geliştirilmesi hakkıdır. Anılan hakkın kapsamı oldukça geniştir. Bu sebeple hakkın tam manası ile ortaya konulabilmesi oldukça güçtür. Genel itibarıyla insanın ihtiyaçları maddi ve manevi ihtiyaçlar olarak ikiye ayrılmaktadır. Bunun sebebi ise insanın maddi ve manevi varlık alanlarından oluşmasıdır. Bu alanların korunması ve geliştirilmesi ise, özgürlükçü ve demokratik bir ortamda, insan haklarının doğasını oluşturan insan onurundan kaynaklanarak kişinin söz konusu ihtiyaçlarının karşılanması ile gerçekleşecektir. Kişiliğin serbestçe geliştirilmesi hakkı, insanın varlık hakkını ve güvencesini oluşturmaktadır. Bu hak, tüm temel hak ve özgürlüklerin varlık nedenidir. Bu nedenle koruma alanı soyuttur ve her olay bağlamında değerlendirilmelidir⁶⁷¹.

Kişiliğin serbetçe geliştirilmesi hakkı, devlet iktidarının hukuk devletinin koşullarına uygun olmayan saldırıları yasaklamaktadır. Bu bakımdan kişinin dar kişisel yaşam alanını korumaktadır. Daha açık bir ifadeyle kişiliğin serbetçe geliştirilmesi hakkı, bireye içerisinde gözetlenmeksizin yalnız kalabileceği, kendisini geliştirebileceği, kendisinin güvenliğini sağlamış kişilerle özel olarak görüşebildiği bir özel alanın korunmasını garanti eder. Ayrıca bu hak, bireyin kendini dış dünyada kendini ifade edebilme özgürlüğünü de barındırmaktadır. Bu ise, kişisel verilerin korunması hakkıyla oldukça ilişkilidir. Örneğin, kişinin fotoğrafı, görüntüsü ya da sözlerinin kayıt altına alınması, bu kayıtların tekrar dinletilip dinletilmemesi ya da kimlerle paylaşılacağı gibi hususlar hep genel kişilik hakkı bakımından değerlendirilir. Anayasal bakımdan da tüm

⁶⁷⁰ KABOĞLU, *Özgürlükler Hukuku*, s. 25.

⁶⁷¹ Ali Tarık GÜMÜŞ, *Türk Anayasasında Kişinin Maddi ve Manevi Varlığını Koruma ve Geliştirme Hakkı*, Eğitim Akademi Yayınları, 2010, s. 3-4.

bu hususlara kişinin kendisinin karar vermesi gereği dolayısıyla kişisel verilerin korunması hakkı bakımından değerlendirilmektedir⁶⁷².

Doktrinde belirtildiği ve yukarıda ilişkileri ortaya konulduğu üzere, kişisel verilerin korunması hakkı, anayasa hukuku bağlamında insan onuru ile kişiliğin serbestçe geliştirilmesi (kişinin maddi ve manevi varlığını koruma ve geliştirme) hakkı ile varlık kazanmıştır. Sürekli gözetlendiğini ve kayıt altına alındığını hissedenden bir kişinin serbest hareket etmesi mümkün değildir. Burada Federal Almanya Anayasa Mahkemesi'nin insan onurunun ihlal edilip edilmediğini belirlemek için kullandığı, kişiyi obje haline getirmeme- araçsallaştırmama formülünü⁶⁷³ de dile getirmekte fayda vardır; çünkü kişi kamusal organların karşısında adeta bir obje haline getirilip araçsallaştırılıyorsa, maddi ve manevi varlığını hür bir biçimde geliştiremez; kişisel verilerinin korunması bakımından da, kendisine dair verileri kiminle, nerede, ne zaman, ne kadarı ile paylaşacağını belirleyemez ve nesneleşmiş olur⁶⁷⁴. Dolayısıyla kişisel verilerin korunması hakkının anayasal temellerini oluşturan insan onuru ve kişiliğin serbestçe geliştirilmesi hakları, kamusal organların veri toplarken, işlerken ya da saklarken bu haklara da uymaları gereğini beraberinde getirmektedir.

İnsan onuru ve kişiliğin serbestçe geliştirilmesi hakkı bireye, kendini geliştirebileceği bir alanın oluşturulmasını gerektirir. Bu alanda kişi, hem başkalarının müdahalelerinden istediği ölçüde sakınabilir, hem de yalnızca kendisi ile kalabilir. Kişisel verilerin korunması hakkı da pozitif hukuk bakımından tam bu noktada ortaya çıkar⁶⁷⁵.

⁶⁷² ŞİMŞEK, *Anayasa Hukukunda Kişisel Verilerin Korunması*, s. 133- 135.

⁶⁷³ UYGUN, *Devlet Teorisi*, s. 480.

⁶⁷⁴ KÜZECİ, *Kişisel Verilerin Korunması*, s. 293.

⁶⁷⁵ ŞİMŞEK, *Anayasa Hukukunda Kişisel Verilerin Korunması*, s. 136.

b) Özel Yaşamın Gizliliği (AY md. 20)

1982 Anayasası'nın 20. maddesine göre herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir⁶⁷⁶. Özel hayatın ve aile hayatının gizliliğine dokunulamaz. Maddenin ikinci fıkrasında kişilerin üstü, özel kağıtları ve eşyasının aranması ile el konulmasına ilişkin hükümler bulunmaktadır. Daha evvel de belirtildiği üzere, 2010 tarihinde maddenin 3. fıkrasına kişisel verilerin korunması düzenlemesi eklenmiştir⁶⁷⁷. Dolayısıyla bu fıkra ile kişisel verilerin korunması hakkı anayasal temellerini doğrudan bu maddede bulmaktadır.

İHAS'ın 8. maddesi, özel yaşama ve aile yaşamına saygı hakkını düzenlemektedir. Bu madde de konut ve haberleşmeye saygı hakları da yer almaktadır.

Özel yaşamın gizliliği, bir hak kategorisi olarak oldukça kapsamlı bir şemsiye hak olması hasebiyle içerisinde birçok alanı barındırmaktadır. Buna göre bireyin özel yaşamı üç alana ayrılmaktadır. Bunlar; kamuya açık alan, özel alan ve giz alanıdır⁶⁷⁸. Kişinin kamuya açık alanı, sosyal alanından ileri gelmektedir. Bu alan dışa dönüktür ve bu nedenle bu alana müdahale sıkı olmayan koşullara tabidir. Veri koruma hukuku bakımından ise, veri koruma genel ilkeleri bağlamında kamusal alanda kişinin verileri korunmaya devam etmektedir. Söz gelimi, kişinin kamusal bir alanda görüntülerinin ve sesinin hukuka aykırı olarak kayıt altına alınması ihtimalinde, özel yaşamın gizliliği ve kişisel verilerin korunması haklarının ihlali söz konusu olacaktır. Özel yaşamın içerisindeki özel alan ise, kişinin ailesine ve yakın çevresine açık olan alanıdır. Bu alan bağlamında kişi, çevresiyle belli bir düzeyde iletişim içerisinde olabilir. Dolayısıyla bu alan nisbi olarak koruma altındadır. Bunun anlamı, söz konusu alana çok sıkı koşullar

⁶⁷⁶ Özel Yaşamın Gizliliğine ilişkin AYMK E. 1996/68, K. 1999/1, K.T. 06.01.1999, AYMK E. 2006/ 167, K. 2008/86, K.T. 20.03.2008, AYMK E. 2011/150, K. 2013/30, K.T. 14.02.2013, *N.B.B. Başvurusu*, Başvuru No: 2013/5653, K.T. 03.03.2016 gibi birçok önemli karar II. İLGİLİ ANAYASAL İÇTİHAT başlığı altında kişisel verilerin korunması bağlamında incelenmiştir.

⁶⁷⁷ YILDIRIM, "Kamu Görevlilerinin Özel Hayatı: Cinsel Tercih", s. 453- 454.

⁶⁷⁸ ÜZELTÜRK, *1982 Anayasası ve İnsan Hakları Avrupa Sözleşmesine Göre Özel Hayatın Gizliliği Hakkı*, s. 133; Serap HELVACI, *Gerçek Kişiler*, Legal Yayıncılık, İstanbul, 2016, s. 117- 124.

altında, ölçülülük ilkesine uyularak ve kamu yararı nedeniyle müdahale edilebileceğidir. Son olarak özel yaşamın giz alanı ise, kişinin tüm kamusal müdahalelere kapalı olan, dokunulmaz alanını ifade etmektedir⁶⁷⁹.

Veri koruma hukuku bakımından özel yaşamın gizliliği genel olarak sağlanması gereken amaçlardan biridir. Ayrıca kişisel verilerin korunması hakkının temeli, daha önceki bölümlerde belirtildiği üzere, İHAS dahil pek çok düzenleme ve ülkede özel yaşamın gizliliği hakkında bulunmaktadır. Türk Anayasa Hukuku bakımından da durum böyle olmuştur. Kaldı ki, kişisel verilerin korunması hakkının 20. maddeye ek bir fıkra ile ilavesi de bu durumu teyitlemektedir. 2010 öncesinde ise özel yaşamın gizliliği hakkı, özel görünümüleri dışında, (konut dokunulmazlığı, haberleşme hürriyeti) 1982 Anayasası'nda mutlak olarak korunmaktadır ve bu nedenle 2010'da tanınan kişisel verilerin korunması hakkı öncesinde de oldukça sağlam biçimde temellendiği ve korunduğu görülebilecektir⁶⁸⁰.

c) Konut Dokunulmazlığı (AY md. 21)

1982 Anayasası'nın 21. maddesi ve İHEB'in 8. maddesi altında düzenlenen konut dokunulmazlığı, aslında özel yaşamın gizliliği hakkı bağlamında ele alınan bir alt başlık olarak düşünülebilecektir. Çünkü bu hak, özel yaşamın gizliliğini mekânsal olarak korumaktadır. Bu hak ile kişinin konutu içerisinde rahatsız edilmeksizin özel yaşamını koruyabilmesi mümkün olmaktadır. Bu hak da tıpkı özel yaşamın gizliliği hakkı gibi, kişisel verilerin korunmasını sağlayan haklardandır. Örneğin, kişinin konutunun hukuka aykırı biçimde gözetlenmesi, özel yaşamın özel ve giz alanlarına doğrudan müdahale oluşturacak ve bu şekilde elde edilmiş kişisel veriler sebebiyle bu hakkın da ihlalini doğuracaktır⁶⁸¹.

⁶⁷⁹ ŞİMŞEK, *Anayasa Hukukunda Kişisel Verilerin Korunması*, s. 140- 142.

⁶⁸⁰ KÜZECİ, *Kişisel Verilerin Korunması*, s. 295.

⁶⁸¹ ŞİMŞEK, *Anayasa Hukukunda Kişisel Verilerin Korunması*, s. 142.

d) Haberleşme Hürriyeti (AY md. 22)

1982 Anayasası'nın 22. maddesinde garanti altına alınan haberleşme hürriyeti, İHAS 8. maddesi ile özel yaşamın gizliliği hakkı bağlamında korunmaktadır. Buna göre herkes haberleşme hürriyetine sahiptir ve haberleşmenin gizliliği esastır.

“Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; haberleşme engellenemez ve gizliliğine dokunulamaz.”

Haberleşme hürriyetine dair söz konusu sınırlamalar, Anayasa'nın 13. maddesinde belirtilen temel hak ve özgürlüklerin sınırlandırılması esaslarına uygun olmalıdır. Bunlar harici, haberleşmeye katılan tarafların rızası olmaksızın haberleşmenin gizliliğinin öğrenilmesi, bu hakka bir müdahale teşkil eder.

Söz konusu hakkın kişisel verilerin korunması ile ilişkisine bakıldığında, haberleşmenin gizliliğine hukuka aykırı biçimde müdahalelerin yakından incelenmesi gerekmektedir. Buna göre, hukuka aykırı biçimde ihlal edilen haberleşme neticesinde kişinin verilerinin hukuka aykırı olarak dinlenilmesi ve kayıt altına alınması kişisel verilerin korunması hakkının da ihlali anlamına gelmektedir. Ayrıca özellikle günümüz cep telefonu, e-posta, internet üzerinden yapılan görüntülü görüşmeler vb. gibi uygulamaları düşünüldüğünde, haberleşmenin gizliliği ve kişisel verilerin korunması haklarının kamusal organların müdahalesini yasaklaması sebebiyle, her gün nasıl bir arada tehdit altında olabilecekleri de görülecektir. Haberleşme özgürlüğü, kişinin gerçekleştirdiği haberleşmenin gizlilik ve güvenilirliğini korumakta ve veri koruma hukukuna bu yönü ile hizmet etmektedir⁶⁸².

⁶⁸² ŞİMŞEK, *Anayasa Hukukunda Kişisel Verilerin Korunması*, s. 149- 150.

e) Din ve Vicdan Hürriyeti (AY md. 24)

1982 Anayasası'nın 24. maddesi ve İHEB'in 9. maddesinde düzenlenmiş olan din ve inanç hürriyeti, kişisel verilerin korunması bakımından ayrı bir önem arz etmektedir⁶⁸³. Söz konusu hakkın konusu olan kişinin din ve inancı, GVKT başta olmak üzere birçok uluslararası ve ulusal düzenlemelerce hassas veri olarak nitelendirilmektedir. Hassas veri olarak din ve inanç konuları veri işleme yasağına tabidirler. Kişinin dinsel alanında kişisel verileri, mutlak olarak korunan çekirdek alanda yer alır⁶⁸⁴. Dini ve vicdani kanaatleri açıklamama ve bundan dolayı kınanamama hakkı da hem İHAS 15. maddesinde, hem de 1982 Anayasası 15. madde bağlamında olağanüstü dönemlerde dahi korunmaktadır. Ancak bu hak bağlamında yer alan ibadet özgürlüğü ise, belirli koşullar altında korunmaktadır. 1982 Anayasası'nın 24. maddesi de bu bağlamda inanç özgürlüğünü sınırsız olarak korurken, ibadet özgürlüğünü 14. maddede korunan değerler bakımından kötüye kullanılmamak şartıyla garanti altına almaktadır⁶⁸⁵.

f) Düşünce Hürriyeti (AY md. 25- AY md. 26)

1982 Anayasası'nın 25. maddesi, “*Düşünce ve kanaat hürriyeti*” başlığını taşıırken, 26. maddesi “*Düşünceyi açıklama ve yayma hürriyeti*” başlığına sahiptir. Anılan haklar İHAS md. 10'da da düşünce özgürlüğü başlığı altında ele alınmaktadır. Anayasa hukukunda dokunulmaz alanlar içerisinde yer alan bu özgürlük yalnızca kişinin düşüncelerini serbest bir biçimde açıklayabilmesini garanti altına almakla kalmaz; ayrıca düşünceyi açıklama özgürlüğüne karşı müdahalelere dair de bireyi koruma altına alır⁶⁸⁶. 25. maddede yer alan “*Düşünce ve kanaat hürriyeti*” mutlak biçimde korunmaktadır. 1982

⁶⁸³ Din ve vicdan hürriyetine ilişkin *AYM E. 1979/9, K. 1979/44, K.T. 27.11.1979* ve *AYM E. 1995/17, K. 1995/16, K.T. 21.06.1995* ile İHAM'ın 2 Mayıs 2010 Tarihli *Sinan ISIK- Türkiye* kararları II. İLGİLİ ANAYASAL İÇTİHAT- B. DEMOKRATİK TOPLUM DÜZENİNDE GEREKLİLİK 2. Ölçülülük Başlığı altında kişisel verilerin korunması bağlamında incelenmiştir.

⁶⁸⁴ ŞİMŞEK, *Anayasa Hukukunda Kişisel Verilerin Korunması*, s. 137.

⁶⁸⁵ ÖZBUDUN, *Türk Anayasa Hukuku*, s. 79- 81; TANÖR, YÜZBAŞIOĞLU, 1982 Anayasasına Göre Türk Anayasa Hukuku, s. 170- 172.

⁶⁸⁶ İbrahim Ö. KABOĞLU, “Pozitif Anayasa Hukukunda Düşünce Özgürlüğünün Sınırları”, *Hukuk Felsefesi ve Sosyolojisi Arkivi*, Ed. Hayrettin ÖKÇESİZ, İstanbul, 1998, s. 205 vd.

Anayasası'nın 15/2. maddesi uyarınca da savaş, seferberlik, sıkıyönetim ve olağanüstü hallerde dahi kimse din, vicdan, düşünce ve kanaatlerini açıklanmaya zorlanamayacaktır.

Düşünce özgürlüğü, kişisel verilerin korunması hakkıyla da ilişkilidir. Mutlak olarak korunan düşünce özgürlüğü, öncelikle dış dünyaya yansımamış, kişilerin zihninde olan fikirlerin özgürlüğüdür. Bu alanın veri koruma hukuku ile oldukça önemli bir bağlantı noktası bulunmaktadır. Şöyle ki, internet üzerindeki her hareket bir iz bırakmaktadır. Herhangi bir siteye girildiğinde, alışveriş yapıldığında, haber ya da makale okunduğunda, tüm bunlar toplanılıp bir profillemeye yapılarak sonraki girişlerde kişiye bu tercihleri doğrultusunda ürün, bilgi vb. sunulması gibi durumlar, aslında kişinin yalnız kendisine saklı kaldığını düşündüğü bir alanın genele açılması durumunu yaratır ve bu nedenle özel yaşamın gizliliği hakkı ve düşünce özgürlüğünün ihlalini doğurabilmektedir⁶⁸⁷. Bir diğer boyutuyla kişinin düşüncelerini serbestçe ifade edebilmesini garanti altına alana düşünce özgürlüğü, kişiye açıklamalarının muhatabı ve içeriği ile ilgili karar verebilme hakkını garanti etmektedir. Dolayısıyla kişisel verilerin üzerindeki belirleme hakkının bir unsurunu teşkil eder. Fakat esas olarak düşünce özgürlüğünün içerisinde bulunan düşünceyi açıklama özgürlüğünün negatif boyutu, kişisel verilerin korunması hakkı ile çok daha yakından ilgilidir. Buna göre, devlet kişiyi düşüncelerini açıklamaya ve bunları başka biri ile paylaşmaya zorlayamaz. Bu bakımdan kişinin gizli kalmasını istediği verilerini açıklamaya zorlanamaması ve bunların giz alanında kalmalarını sağlamak hususları, kişisel verilerin korunması hakkının doğrudan konusunu oluşturmaktadır. Bu bakımdan bahis konusu hakkın kısmi garantileri arasındadır⁶⁸⁸.

g) Toplantı ve Gösteri Yürüyüşü Düzenleme Hakkı (AY md. 34)

1982 Anayasası'nın 34. maddesinde düzenlenen toplantı özgürlüğü, İHAS md. 11'de garanti altına alınmıştır. Bu özgürlük kişiye, belli bir grupla kamuya karşı kendini ifade hakkı vermektedir. Bu bakımdan kişisel verilerin korunması hakkı ile bu hakkın

⁶⁸⁷ KÜZECİ, *Kişisel Verilerin Korunması*, s. 297.

⁶⁸⁸ ŞİMŞEK, *Anayasa Hukukunda Kişisel Verilerin Korunması*, s. 146- 148.

ilişkisi daha dolaylı biçimde karşımıza çıkar. Şöyle ki, kişi toplantı özgürlüğünü kullandığında kişisel verileri anonimleşmez. Kişi toplantı çevresinde kamusal bir alanda kendini göstermektedir ve bu bakımdan doğaldır ki kendisi, sözleri ve davranışları gizli kalmaz. Kişi böyle bir toplantıya katıldığında, kendisine dair anılan verilerin bilineceğini göz önünde bulundurmalıdır. Bu bakımdan toplantı ve gösteri yürüyüşü düzenleme hakkı ile kişisel verilerin korunması çok daha dar bir anlamda kesişim gösterirler. Kişi böyle bir toplantıya katıldığının ve davranışları ile sözlerinin kayıt altına alındığını bilir ve bu kayıt nedeniyle kendisine bir zarar gelebileceğini düşünürse, bu haktan yararlanmaktan vazgeçebilir. İşte böylesi bir ihtimalde kişisel verilerinin bu kapsamda kayıt altına alındığını düşünen bireyin, toplantı ve gösteri yürüyüşü hakkına özgürce kullanabilmesi için kişisel verilerin korunması hakkının güvencesine ihtiyacı vardır⁶⁸⁹.

h) Bilgi Edinme Hakkı (AY md. 74)

1982 Anayasası'nın 74. maddesi ve 4982 Sayılı Bilgi Edinme Hakkı Kanunu ile temel bir hak olarak garanti edilen bilgi edinme hakkı, kişilerin kamu faaliyetleri hakkında bilgiye ulaşabilmelerini karşılamaktadır. Hakkın negatif boyutu ise, bilgiyi almama hakkını da kapsamaktadır. Bu hak ile kişinin, ulaşılabilir kaynaklardan, herhangi bir engele takılmaksızın bilgi alabilmesi güvence altına alınmaktadır. Dolayısıyla bu hakkın da kişisel verilerin korunması hakkı ile bir ilişkisi mevcuttur.

4982 Sayılı Bilgi Edinme Hakkı Kanunu'nun 3. maddesine göre bilgi, "*Kurum ve kuruluşların sahip oldukları kayıtlarda yer alan bu Kanun kapsamındaki her türlü veri*" anlamına gelmektedir. Bu kanun kapsamında herkes, bilgi edinme hakkına sahiptir. Anılan kanunun "Özel hayatın gizliliği" başlığını taşıyan 21. maddesine göre,

"Kişinin izin verdiği hâller saklı kalmak üzere, özel hayatın gizliliği kapsamında, açıklanması hâlinde kişinin sağlık bilgileri ile özel ve aile hayatına, şeref ve haysiyetine, meslekî ve ekonomik değerlerine haksız

⁶⁸⁹ ŞİMŞEK, *Anayasa Hukukunda Kişisel Verilerin Korunması*, s. 147- 148.

müdahale oluşturacak bilgi veya belgeler, bilgi edinme hakkı kapsamı dışındadır.”

Bu bakımdan ancak kamu yararının gerektirdiği hallerde kişisel bilgi veya belgeler, kurum ve kuruluşlar tarafından, veri öznesine en az 7 gün önceden haber verilerek yazılı rızası alınmak koşuluyla açıklanabilecektir⁶⁹⁰. Dolayısıyla görülmektedir ki, bilgi edinme hakkı her ne kadar kişisel verilerin korunmasını tümüyle sağlayamasa da kişiyi belli bir seviyede müdahaleden korumaktadır. Ayrıca bu hak sayesinde kişi, kamusal makamların kendisi hakkında veri kayıtlayıp kayıtlamadığını ya da verilerin niteliğini öğrenebilecek ve buna göre kişisel verilerin korunması hakkı bağlamında veri öznesi olması sıfatıyla kendini müdahalelerden koruyabilecektir. Kişinin bilgi edinme hakkından faydalanmadığı ihtimalde ise, kendisi hakkında kamusal makamların elinde bulunan verileri öğrenemeyeceğinden, verilerini kişisel verilerin korunması hakkı bakımından koruyabilmesi de mümkün olamayacaktır.

B. KANUNİ DÜZENLEME

Avrupa Konseyi'nin 108 Numaralı Kişisel Verilerin Otomatik İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşmesi 28 Ocak 1981 tarihinde imzaya açılmış ve Türkiye bu Sözleşme'yi aynı gün imzalamıştır. Ancak anılan Sözleşme'nin uygun bulma kanununun kabulü ancak 30 Ocak 2016 tarihinde gerçekleşebilmiştir. Kişisel verilerin korunmasının anayasal bir hak olarak düzenlenmesi ise, 12 Eylül 2010 tarihinde gerçekleşen referandum sonrası kabul edilen Anayasa Değişikliği⁶⁹¹ ile gerçekleşmiş ve 1982 tarihli Anayasası'nın 20/3. maddesine eklenmiştir.

Tarihsel süreçte yukarıda da görüleceği üzere, Avrupa'nın oldukça gerisinde kalan Türkiye'de veri koruma hukukuna dair sayılabilecek belki de ilk çalışma 1979

⁶⁹⁰ ŞİMŞEK, *Anayasa Hukukunda Kişisel Verilerin Korunması*, s. 145.

⁶⁹¹ 07.05.2010 tarih ve 5982 sayılı Türkiye Cumhuriyeti Anayasasının Bazı Maddelerinde Değişiklik Yapılması Hakkında Kanun ile yapılan Anayasa değişiklikleri, 12.09.2010 tarihindeki referandum ile kabul edilmiştir. 22.09.2010 tarih ve 846 sayılı Yüksek Seçim Kurulu Kararı da 23.09.2010 tarih ve 27708 sayılı Resmî Gazete'de yayımlanmıştır. Resmî Gazete, 23.09.2010 Perşembe, S. 27708, Yüksek Seçim Kurulu Kararı, Karar No: 846, <http://www.resmigazete.gov.tr/eskiler/2010/09/20100923-10.htm>, E.T. 05.04.2019.

yılında Durmuş TEZCAN tarafından hazırlanmıştır⁶⁹². 1989’da ise konuya ilişkin ilk kanun çalışmalarının başladığı aktarılmaktadır⁶⁹³. Kişisel verilerin korunmasına ilişkin kanun tasarılarına incelendiğinde karşımıza en sonuncusu nihayet kanunlaşmış olan, 1995, 2003, 2011, 2014 ve 2016 tarihli beş adet kanun tasarısı çıkmaktadır. Yeni Tasarı 18 Ocak 2016’da TBMM’ye sevk edilmiş, Adalet Esas ve Alt Komisyonu’ndaki görüşmeleri 12 Şubat 2016’da tamamlanmış ve 24 Mart 2016 tarihinde TBMM’de kabul edilmiştir. Kabul edilen 6698 sayılı Kişisel Verilerin Korunması Kanunu 7 Nisan 2016 tarihinde Resmî Gazete’de yayınlanarak bazı hükümleri bu tarihte, bazı hükümleri ise altı ay sonra yürürlüğe girmiştir⁶⁹⁴. Böylelikle kişisel verilerin korunmasına ilişkin özel bir kanunun kabulü gerçekleşmiştir. Bu hak, en temelde bir insan hakkıdır ve Anayasa’nın koruması altındadır. Ayrıca bir kanun ile de korunuyor olması etkin bir koruma yolunda önemli bir adımdır.

Her ne kadar veri koruma hukukunun ilk ortaya çıkışı, en kapsamlı veri tekeline sahip olan devlete karşı olsa da, günümüzde teknolojik gelişmelerin bizi getirdiği nokta, özel sektörün de hatta belki de giderek kamunun önüne geçecek şekilde veri işliyor olma realitesidir. BM’ye göre 2011 yılında tüm dünyada üretilen toplam veri, o zamana değin insanlık tarihinde üretilen toplam veriden fazladır. Bu yönüyle veri, petrolden daha değerli görülmektedir⁶⁹⁵. Ekonomik değeri ve özel sektörle ilişkisi böylesine artan verinin iç hukuk kapsamında da korunması, sınıraşan niteliği ağır basan veri işleme bakımından büyük önem taşımaktadır. GVKT’nin 45. maddesi üçüncü bir ülkeye veri aktarımını ancak o ülkede “yeterli düzeyde” koruma sağlanması halinde kabul etmektedir. Dolayısıyla henüz AB üyesi olmayan Türkiye açısından kişisel verilerin korunmasının “yeterli düzeyde” olmadığına kanaat getirilirse gerek ekonomik gerek adli ve gerekse

⁶⁹² Bkz. Durmuş TEZCAN, “Bilgisayarın Hukukta Kullanılması ve Özellikle Adli Sicil Sisteminin Mekanik Hale Dönüştürülmesi”, Adalet Dergisi, 1979, Y: 70, No: 1-2, ss. 53- 79.

⁶⁹³ Bahri ÖZTÜRK, Elif ALTINOK ÇALIŞKAN, “Kişisel Verilerin Korunması Kanunu Hakkında Genel Değerlendirmeler ve Anayasaya Aykırılık Sorunu”, *Fasikül Hukuk Dergisi*, Mart 2018, S. 100, s. 278, ss. 277- 336.

⁶⁹⁴ 07.04.2016 Tarih ve 29677 Sayılı Resmî Gazete, Kişisel Verilerin Korunması Kanunu, Kanun No: 6698, Kabul Tarihi: 24.03.2016, Md. 32.

⁶⁹⁵ Adrien BASDEVANT, Jean-Pierre MIGNARD, *L’Empire des Données: Essai sur la Société, les Algorithmes et la Loi*, Don Quichotte éditions, Paris, 2018, s. 10.

diğer bazı alanlardaki iş birlikleri mümkün olamayacaktır. Üstelik 6698 sayılı KVKK yürürlüğe girene dek, AB'ye aday adayı olan Türkiye'nin adaylık süreci bakımından veri koruma hukuku alanına özel bir kanunun düzenlenmesi kişisel verilerin korunması alanındaki bir gereklilik olarak karşımıza çıkmıştır⁶⁹⁶. 6698 sayılı Kanun'un kabul edilmesinden sonra ise, her ne kadar Kanun'un varlığı olumlu olarak nitelendirilse de Avrupa standartları ile uyumlu olmadığı belirtilmiştir⁶⁹⁷.

6698 sayılı KVKK'nın temeli 95/46/AT sayılı Direktif'tir. AB Hukuku'nda "Direktif" kavramı, tüm AB üyelerinin gerçekleştirmesi gereken bir hedef belirleyen hukuki metinleri karşılamaktadır. Ancak bu hedefin nasıl gerçekleştirileceği ülkelere bırakılmıştır. Bu bakımdan görülmektedir ki, direktif bir çerçeve belgedir. İç hukukta bu çerçevenin içeriği çok daha detaylı bir biçimde düzenlenmektedir⁶⁹⁸. Bu durumun da etkisiyle KVKK, 33 maddeden oluşan genel hatlı bir metin olarak karşımıza çıkmaktadır⁶⁹⁹. Öte yandan 95/46/AT sayılı Direktif'in yerini alan GVKT ise bir tüzüktür ve 99 maddeden oluşmaktadır. AB Hukuku'nda "Tüzük" kavramı, bağlayıcı bir hukuki metindir. Bu bakımdan üye ülkelere doğrudan uygulanmaktadır⁷⁰⁰. Dolayısıyla Türkiye KVKK'nın hükümlerini, Birleşik Krallık, Fransa gibi kimi devletlerin gerçekleştirdiği

⁶⁹⁶ Avrupa Komisyonu Türkiye 2014 Yılı İlerleme Raporu, Komisyon Tarafından Avrupa Parlamentosuna, Konseye, Ekonomik ve Sosyal Komiteye ve Bölgeler Komitesine Sunulan Bildirim, Genişleme Stratejisi ve Başlıca Zorluklar 2014-2015, Brüksel, 08.10.2014, s. 6.

⁶⁹⁷ Avrupa Komisyonu Türkiye 2018 Yılı İlerleme Raporu, Komisyon Tarafından Avrupa Parlamentosuna, Konseye, Ekonomik ve Sosyal Komiteye ve Bölgeler Komitesine Sunulan Bilgilendirme, AB Genişleme Politikasına İlişkin 2018 Bilgilendirmesi, Strazburg, 17.04.2018, s. 5.

⁶⁹⁸ "Regulations, Directives and other acts", EU Law, https://europa.eu/european-union/eu-law/legal-acts_en, E.T. 20.04.2019.

⁶⁹⁹ Uygulamada her ne kadar 2018 tarihli Birleşik Krallık Veri Koruma Kanunu gibi detaylı ve çok sayıda maddesi olan "Veri Koruma Kanunları"na rastlansa da (215 maddeden oluşmaktadır.), aynı zamanda yine 2018 tarihli Fransız Veri Koruma Kanunu gibi KVKK ile benzerlik gösteren daha genel çerçeveli ve az sayıda maddesi bulunan (37 maddedir.) metinler bulunabilmektedir.

Daha detaylı bilgi için bkz. Data Protection Act 2018, <http://www.legislation.gov.uk/ukpga/2018/12/contents>, E.T. 20.04.2019; LOI n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, <https://www.legifrance.gouv.fr/eli/loi/2018/6/20/JUSC1732261L/jo/texte/fr>, E.T. 20.04.2019.

⁷⁰⁰ "Regulations, Directives and other acts", EU Law, https://europa.eu/european-union/eu-law/legal-acts_en, E.T. 20.04.2019.

şekilde, 25 Mayıs 2018’de tüm AB üyesi ülkelerde doğrudan uygulama bulan GVKT’ye uyarlamalıdır.

1. Uygulama Alanı

a) Konu Açısından

1982 tarihli Anayasa’nın 20/3. maddesine göre kişisel verilerin korunması(nı isteme) anayasal bir hak olarak düzenlenmektedir. Fakat KVKK’da kişisel verilerin korunması “hakkı” ifadesi yer almamaktadır. İlaveten her ne kadar KVKK’ya ilişkin Alt Komisyon Raporu ve Adalet Komisyonu Raporu’nda “kişisel verilerin korunması hakkı”ndan bahsedilse de KVKK’nın Genel Gerekçesi ya da Madde Gerekçeleri’nde de bir hak biçiminde yer almamaktadır. Bu bakımdan KVKK’nın 1. maddesinde Kanun’un amaçlarından birinin, “...*kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak*” olduğu belirtilmektedir. Kişisel verilerin korunmasının anayasal bir hak olması ve KVKK’nın amaçlarından birinin temel hak ve özgürlüklerin korunması olduğunu dikkate aldığımızda, bu konudaki eksiklik bir parça olsun azaltılabilmektedir. Ancak kişisel verilerin korunması hakkının KVKK’da da temel bir hak olarak tanımlanması, meselenin temel hak ve özgürlükler ekseninden ele alındığını çok daha net biçimde ortaya koyacaktır⁷⁰¹.

KVKK’nın 3/1. maddesi, “kişisel veri” kavramını tanımlamaktadır. Buna göre, “*Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi... ifade eder.*” Yukarıda ele alınan birçok uluslararası düzenleme ile içtihatlarla bakıldığında, bu genel-geçer tanım iç hukukta ilk defa bir metinde yer almaktadır. Unutulmamalıdır ki AYM, Kanun’dan daha önce kişisel verilerin korunması hakkıyla ilgili 9 Nisan 2014 tarihli bir kararında⁷⁰² kişisel veri kavramını “...*belirli veya kimliği belirlenebilir olmak şartıyla, bir*

⁷⁰¹ KÜZECİ, *Kişisel Verilerin Korunması*, s. 320.

⁷⁰² AYMK E.2013/122, K. 2014/74, K.T. 09.04.2014.

kişiyi ilişkin bütün bilgileri ifade etmektedir.” biçiminde KVKK ile oldukça benzer biçimde tanımlamıştır. Bu kararda ayrıca,

“...adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil; telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler, IP adresi, e-posta adresi, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kalan tüm veriler”in

kişisel veri olarak kabul edildiği belirtilmiş ve böylece kavramın sınırlarının nerelere erişebileceği açıklanmaya çalışılmıştır. Söz gelimi, bir kimsenin kimliği, etkin kökeni, fiziksel özellikleri, sağlık durumu, genetik verileri, öğrenim veya istihdam durumu, ikamet adresi, kredi kartı bilgileri, banka ve sigorta kayıtları, adli arşiv ve genel bilgi toplama kayıtları, düşünce ve inançları, alışveriş alışkanlıkları, telefon rehberi, fotoğrafı, IP adresi, parmak izi, cep telefonundan gönderdiği kısa mesajları, elektronik postaları, sosyal paylaşım sitelerindeki aktiviteleri, en son gittiği restoran, bar ya da müze gibi veriler Kanun bağlamında da kişisel veri kapsamındadır⁷⁰³.

KVKK’nın 2. maddesi, diyerek uygulama alanının konusu kapsamına giren işleme hallerinden söz etmektedir. Bu bağlamda KVKK kişisel verilerin;

- Tamamen ya da kısmen otomatik olan kayıt araçları ile işlenmesi⁷⁰⁴

⁷⁰³ AKGÜL, *Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması*, s. 8-9; DÜLGER, “Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması”, *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi*, s. 108.

⁷⁰⁴ Otomatik araçlar ile işleme, verilerin otomasyon sistemlerinin kullanıldığı yöntemlerle işlenmesidir. Daha açık bir şekilde ifade etmek gerekirse, otomasyon sistemleri ile işleme mekanik aygıtlar vasıtasıyla yapılan veri işlemedir. Doktrinde, otomatik araçlar ile işlemenin bilişim sistemleriyle yapılan işlemler gibi dijital (sayısal) işlemleri de içerecek şekilde anlaşılması ve bunun da KVKK kapsamında olması gerektiği ifade edilmektedir. DÜLGER, “Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması”, *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi*, s. 112; DÜLGER, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 669.

- Herhangi bir dosyalama sisteminin parçasını oluşturmak şartıyla otomatik olmayan araçlar ile işlenmesi

hallerini koruma altına almaktadır. Daha açık bir söyleyişle, kişisel veriler üzerindeki otomatik olan tüm veri işleme etkinlikleri KVKK kapsamındadır. Otomatik olmayan veri işleme etkinlikleri bakımından ise, şayet bu etkinlikler bir veri kayıt sisteminin parçası ise KVKK kapsamında korunmaktadırlar. Tam otomatik veri işleme usulünde, veriyi toplayan sistem bütünüyle kendi başına çalışmaktadır. Kısmi otomatik veri işleme usulünde ise, sistem tarafından veri toplanırken insan müdahalesi de bulunmaktadır. Söz gelimi akıllı telefonlar ya da bilgisayarlar tarafından yapılan tüm veri işlemler otomatik veri işleme usulüyle gerçekleştirilmektedir. Kişisel verilerin işlenmesi dendiğinde ilk işleme yöntemi olarak akla dijital ortamda otomatik kayıt sistemleri gelse de dijital olmayan (analog) biçimde söz gelimi kâğıt üzerinde gerçekleştirilen veri işleme sistemleri de bu işlemin belirli kriterlere göre yapılandırılarak işlendiği bir dosyalama sistemine kayıtlaniyorsa KVKK'nın koruma alanına girecektir. Örneğin, hasta kayıt dosyaları ya da öğrenci dosyaları gibi belirli bilgiler kişi, tarih, yer gibi kıstaslar doğrultusunda işlemeye hazır biçimde bir kayıt sisteminde yer alıyorsa bu doğrultuda değerlendirilebilecektir⁷⁰⁵. Ek olarak bu madde özelinde belirtilmelidir ki, işlemin gerçek veya tüzel kişilerce ya da kamu veya özel sektör tarafından gerçekleştirilmesi arasında bir fark gözetilmemektedir.

Yukarıdaki her iki KVKK hükmü de oldukça hızlı değişen ve gelişen teknoloji alanında kişisel verilerin korunmasında bir eksiklik olmaması adına ortaya yeni çıkabilecek durumlara karşı “teknoloji nötr (teknoloji geçirmez.)”⁷⁰⁶ hükümler olarak değerlendirilebilecektir. 3. maddede yer alan “kişisel veri” tanımında “her türlü bilgi” ibaresi bu bakımdan oldukça önemlidir. Şu an için mevcut olmayan fakat ileride veri koruma hukukunun konu kapsamına giren hususlar da KVKK kapsamında

⁷⁰⁵ ÇEKİN, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu*, s. 22- 23.

⁷⁰⁶ AB veri koruma sisteinde teknoloji nötr düzenlemeler ile ilgili bkz. KÜZECİ, *Kişisel Verilerin Korunması*, s. 318.

değerlendirilebilecektir. İşte bu her türlü bilginin kişisel veri kapsamına girebilmesi için de mutlaka belirli ya da belirlenebilir gerçek kişi ile ilişkilendirilebilmesi gerekmektedir. 2. maddede yer alan veri işleme yöntemlerinde de belirli bir veri işleme yönteminden bahsedilmeyip yalnızca genel olarak veri işlemeden söz edilmektedir. Teknoloji nötr olan bu madde ise, hem KVKK'nın hangi veri işleme yöntemi kullanılırsa kullanılsın dolanılmasına engel olacak⁷⁰⁷ hem de teknolojinin gelişme hızıyla ortaya yeni çıkabilecek veri işleme usullerini KVKK kapsamının dışına atmayacaktır.

“Kişisel veri” tanımına ilişkin GVKT'nin 4/1. maddesine yer alan *“tanımlanmış veya tanımlanabilir bir gerçek kişiye ilişkin her türlü bilgi”* biçimindeki tanım da KVKK ile benzerlik göstermektedir. Ancak KVKK'den farklı olarak GVKT'de kişinin ne şekilde tanımlanabilir olduğu da açıkça düzenlenmektedir. Buna göre kişi, isim, kimlik numarası, konum verileri, çevrimiçi tanımlayıcı ya da söz konusu gerçek kişinin fiziksel, fizyolojik, genetik, ruhsal, ekonomik, kültürel veya toplumsal kimliğine özgü bir ya da daha fazla sayıda faktöre bakılarak doğrudan veya dolaylı olarak tanımlanabilmelidir.

“Veri işleme usulleri” bakımından ise GVKT'nin 2. maddesinde,

“Bu Tüzük, kişisel verilerin tamamen ya da kısmen otomatik araçlarla işlenmesine ve kişisel verilerin otomatik araçlar haricinde bir dosyalama sisteminin parçasını oluşturan veya bir dosyalama sisteminin parçasını oluşturması amaçlanan araçlarla işlenmesine uygulanır.”

hükmü bulunmaktadır. Burada görülecektir ki, kişisel verilerin tam ya da kısmi otomatik araçlarla veya bir dosyalama sisteminin parçası olması kaydı ile otomatik olamayan araçlarla işlenmesi hususları KVKK ile aynıdır. Yalnızca bu düzenlemede, bir dosyalama sisteminin parçasını oluşturması amaçlanan otomatik olmayan araçlarla işleme halinin de GVKT kapsamında olduğu belirtilmiştir. Buna göre, verinin otomatik olmayan şekilde

⁷⁰⁷ ÇEKİN, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu*, s. 23.

işlenip sonradan bir kayıt sistemine dahil olmasının öngörüldüğü ihtimalde de GVKT uygulama alanı bulacaktır⁷⁰⁸.

Son olarak belirtilmelidir ki, GVKT'nin 2. maddesi ile oldukça yakından ilişkili olarak KVKK'nın 4/2. maddesine bakıldığında, veri işleme faaliyeti söz konusu olduğunda

“...otomatik yöntemlerle olsun veya olmasın kişisel veri veya kişisel veri setleri üzerinde gerçekleştirilen toplama, kaydetme, düzenleme, yapılandırma, saklama, uyarlama veya değiştirme, elde etme, danışma, kullanma, iletim yoluyla açıklama, yayma veya kullanıma sunma, uyumlaştırma ya da birleştirme, kısıtlama, silme veya imha gibi herhangi bir işlem veya işlem dizisi”

gerçekleştirilmektedir. Bu maddenin KVKK'dan farkı ise, GVKT'de otomatik olan ya da otomatik olmayan tüm veri işleme usulleri arasında bir ayrım gözetilmediğidir⁷⁰⁹.

b) Kişi Açısından

KVKK'nın 3/1-ç maddesine göre, “*Kişisel verisi işlenen gerçek kişi*” “ilgili kişi” kavramı ile karşılanmaktadır. Ayrıca görüleceği üzere ilgili kişi yalnızca gerçek kişi olmaktadır. Belirtilmelidir ki amacı başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak olan KVKK'nın ilgili kişiyi yalnızca gerçek kişiler olarak kabul etmesi yerinde bir karar olmuştur⁷¹⁰. Açıktır ki insan hakları yalnızca insan olmaktan kaynaklanan ve doğuştan gelen haklardır. Bu bakımdan tüzel kişilerin kişisel verilerin korunması hakkının öznesi olması çelişkili bir durum yaratabilirdi.

⁷⁰⁸ ÇEKİN, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu*, s. 24.

⁷⁰⁹ KÜZECİ, *Kişisel Verilerin Korunması*, s. 328.

⁷¹⁰ Doktrinde tüzel kişilere ilişkin veri korumasının kanun koyucunun yasama faaliyeti ile her zaman gerçekleştirebileceği ve tüzel kişilerin itibarlarının zedelenmesihisinde manevi tazminat talebinde bulunabilmeleri dolayısıyla verilerinin korunması hususunda haklı bir beklentiden söz edilebileceği belirtilerek bu konuda açık kapı bırakan örneklere de rastlamak mümkündür. Bkz. ÇEKİN, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu*, s. 21.

KVKK her ne kadar tüzel kişileri kapsam dışı bıraksa da AYM'nin 4 Aralık 2014 tarihli kararı⁷¹¹, tüzel kişileri hakkın öznesi olarak kabul etmesi bakımından tartışmalı bir karar olarak karşımıza çıkmaktadır. Esas olarak bu kararda tartışılan mesele, hakkın koruma alanının tüzel kişileri de kapsayıp kapsamadığı olmuştur. İlgili kararda, 6475 sayılı Posta Hizmetleri Kanunu'nun belli maddelerinin Anayasa'nın 20. maddesinde düzenlenen kişisel verilerin korunması hakkı dahil birçok maddesine aykırılığı ileri sürülerek iptali istenmiştir. Kararda,

“Kişisel veri kavramı, belirli veya kimliği belirlenebilir olmak şartıyla, bir kişiye ilişkin bütün bilgileri ifade etmektedir. Bu bağlamda, bir kişinin kendisinin veya ailesinin sürekli ve geçici olarak konakladığı, ikamet ettiği yerlere ait bilgiler (fiziki adresler) de kişisel veri niteliğindedir. Aynı şekilde, elektronik posta olarak adlandırılan ve elektronik iletişim ağı üzerinden gönderilen ve internette ya da kullanıcının bilgisayarında kaydedilebilen her türlü yazı, ses, resim ya da dil iletilerinin de kişisel veri niteliğinde olduğu kabul edilmektedir.”

denilerek hem fiziki adreslerin hem de elektronik posta adreslerinin kişisel veri kavramına dahil olduğu belirtilmektedir. Ancak esas olarak bu kararda tartışılan mesele, yukarıda belirtildiği üzere, hakkın koruma alanının tüzel kişileri de kapsayıp kapsamadığı olmuştur. Buna göre;

“Anayasa'nın 20. maddesinde kişisel verilerin kişi bakımından korunma alanının gerçek kişiler ya da tüzel kişileri veya her ikisini içine alıp almadığı konusunda bir açıklık bulunmamaktadır. Maddenin gerekçesinde de buna ilişkin bir değerlendirme yoktur. Her ne kadar Anayasa'nın 20. maddesinde daha ziyade gerçek kişilerin özel hayatı ve bu bağlamda gerçek kişilere ilişkin kişisel verilerin korunma altında bulundurulduğu ileri sürülebilir ise de madde metninde kişisel verilerle ilgili olarak "herkes" tabirinin kullanılması dikkate alındığında, tüzel kişilere ilişkin verilerin de 20. madde kapsamında değerlendirilmesi gerekeceği açıktır.

...Bu durumda, Anayasa'nın 20. maddesinde kişisel verilerin "ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebileceği"nin açıkça ifade edilmesi karşısında, tüzel kişilerin

⁷¹¹ AYM E. 2013/84, K. 2014/ 183, K.T. 04.12.2014.

kişisel veri niteliğinde bulunan fiziki veya elektronik adreslerinin, yetkili kişi ya da organlarının rızaları alınmaksızın, dava konusu kural uyarınca PTT A.Ş. tarafından reklam ve tanıtım amacıyla toplanıp kaydedilmesinin ve bunların üçüncü kişilere verilmesinin, Anayasa'nın 20. maddesine aykırılık oluşturduğu açıktır. Tüzel kişilere ilişkin kişisel verilerin ilgili kanunlar gereği ya da kişilerin kendilerince kamuya açıklanmış olması veya açık sicillerde yer almış olması, söz konusu verilerin ticari amaçlarla üçüncü kişilere aktarımına rıza gösterildiği anlamına gelmez.”

ifadesi ile AYM, tüzel kişileri de hakkın öznesi olarak kabul etmiş ve tüzel kişilerin rızası olmaksızın kendilerine ait kişisel verilerinin kaydedilerek üçüncü kişilere verilmesini kişisel verilerin korunması hakkının ihlali olarak görmüştür.

Anılan karar doktrinde, kaynağını insan onuru ve bireysel özerklikten alan kişisel verilerin korunması hakkının öznesinin gerçek kişi dışında tüzel kişi olamayacağı ve tüzel kişilere dair bilgilerin ancak bir gerçek kişi ile ilişkili olduğu ölçüde korunabileceği belirtilerek eleştirilmektedir⁷¹². 6698 sayılı KVKK'nın 2. maddesinin kapsamı ortaya konulurken,

“Bu Kanun hükümleri, kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında uygulanır.”

diyerek, kişisel verilerinin işleneceği kişilerin gerçek kişiler, verileri işleyenlerin ise, gerçek veya tüzel kişiler olabileceğini ortaya koymaktadır. Ayrıca GVKT'de tanımların yer aldığı 4. maddeye bakıldığında da kişisel verinin tanımında şu ifade dikkati çekmektedir; “*kişisel veri*’ tanımlanmış veya tanımlanabilir bir gerçek kişiye ilişkin her türlü bilgidir (*'veri sahibi'*).” Buna göre kişisel veri, ancak gerçek kişiye ilişkin bir veridir. 95/46/AT Sayılı Direktif de tıpkı GVKT ve KVKK gibi, yalnızca gerçek kişilerin verilerini koruyan bir yaklaşım benimsemişti.

⁷¹² KÜZECİ, *Kişisel Verilerin Korunması*, s. 303.

Öte yandan Adalet Divanı'nın 9 Kasım 2010 tarihli *Volker und Markus Schecke GbR ve Hartmut Eifert- Land Hessen* birleştirilmiş kararı ise tüzel kişilerin hakkın öznesi olması konusunda farklı bir tespit yapmıştır. Anılan karara göre, tüzel kişilerin adı şayet doğrudan gerçek kişi olan ortaklarını tanımlamakta ise AB Temel Haklar Şartı'nın özel yaşama saygı hakkının düzenlendiği 7. ve kişisel verilerin korunması hakkını ele alan 8. maddelerini ışığında koruma talep edilebileceklerdir⁷¹³. Ayrıca dünya genelindeki bir eğilim de tüzel kişilerin giderek kendi çıkarları için özel yaşam ve veri koruma haklarına başvurması biçimindedir. Bu bağlamda son zamanlarda öne çıkan bir dava olarak *Big Brother Watch ve Diğerleri- Birleşik Krallık*'ta, gerçek bir kişi ile birlikte üç tane limited şirket İngiltere Hükümeti aleyhine yasadışı kitlesel gözetleme uygulamalarına ilişkin İHAM nezdinde grup davası başvurusunda bulunmuştur⁷¹⁴. Ancak GVKT gibi uluslararası düzenlemeler ve KVKK gibi ulusal metinler hakkın öznesi olarak yalnızca gerçek kişileri tanırsalar da, yukarıda bahis konusu olan tüm bu gelişmeler tüzel kişilerin özel yaşam ve kişisel verilerin korunması haklarına dair korunması için yeterli midir yoksa kaynağını insan onuru, özerklik veya özgürlük gibi bireysel çıkarlardan alan özel yaşam ve veri koruması yalnızca gerçek kişilere mi aittir sorusu uluslararası alanda giderek daha fazla tartışılır hale gelmektedir.

Burada altı önemle çizilmelidir ki, tüzel kişilere ilişkin veriler içerisinde bir gerçek kişiyi belirlenebilir kılan türden bir bilgi bulunmakta ise, açıktır ki kişisel verilerin korunması hakkı ve KVKK kapsamında değerlendirilecektir⁷¹⁵.

GVKT'nin 4/1. maddesi, verisi işlenen gerçek kişiye “*veri öznesi (data subject)*” demektedir. Avrupa veri koruma hukukunda, bir önceki 95/46/AT sayılı Direktif'in 2/(a). maddesinde de bu kavram takip edilmekteydi. Bu bakımdan KVKK'nın neden aynı

⁷¹³ Joined Cases C-92/09 and C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen*, 09.11.2010, Par. 53, <http://curia.europa.eu/juris/celex.jsf?celex=62009CJ0092&lang1=en&type=TEXT&ancre=>, E.T. 28.01.2019.

⁷¹⁴ Söz konusu davada başvurucular, dava “Ek”inde detaylı olarak belirtilmiş ve karar metninin birinci paragrafında “*şirketler, yardım kuruluşları, organizasyonlar ve bireyler*” biçiminde ifade edilmiştir. *Big Brother Watch and Others v. The United Kingdom*, Application Nos: 58170/ 13, 62322/ 14 and 24960/ 15, Par. 1, Appendix, <http://hudoc.echr.coe.int/eng?i=001-186048>, E.T. 19.08.2019.

⁷¹⁵ KÜZECİ, *Kişisel Verilerin Korunması*, s. 326.

kavram yerine farklı bir adlandırmaya yöneldiğini kestirmek mümkün görünmemektedir. Yine aynı maddede belirtildiği üzere, yalnızca gerçek kişiler GVKT'nin koruma alanındadır. Bu bakımdan KVKK ile Tüzük uyumludur.

Yeniden belirtilmelidir ki KVKK'da veri işleyenlerin sorumluluğu bakımından gerçek veya tüzel kişi ayrımı yapmaksızın veri işleyen herkese yükümlülükler atfedilmiştir (KVKK md. 3/1(ğ)- (ı)). Aynı şekilde GVKT de bu ayrımı tercih etmemiştir (GVKT md. 4/7- 8). Dolayısıyla KVKK bu bakımdan GVKT ile çelişmemektedir.

c) Yer Açısından

KVKK'nın ilk üç maddesi, yukarıda belirtildiği üzere, Kanun'un amaç, konu ve kişi bakımından uygulama alanını ortaya koymaktadır. Oysa KVKK'nın yer açısından uygulama alanına dair özel bir düzenlemesi bulunmamaktadır. Bu bakımdan Kanun'un uygulanması, vatandaş ya da yabancı tarafından işlenmesi farketmeksizin devletin ülkesinde işlenen tüm suçları takip etmek yetkisinin olması anlamına gelen mülkilik prensibi doğrultusunda olacaktır⁷¹⁶. Daha açık bir söyleyişle, Türk hukukunun geçerli olduğu bir yerde kişisel verilerin işlenmesi söz konusu ise, KVKK uygulama bulacaktır.

GVKT bakımından ise durum oldukça farklılık arz etmektedir. Buna göre, Veri Koruma Reformu'nun getirdiği en önemli düzenlemelerden biri, GVKT'nin uygulamasındaki “ülkedışılık (extraterritoriality)” prensibidir. Buna göre GVKT'nin uygulanması için veri denetleyicisinin AB sathında ikamet etmesi gerekmektedir; AB sathında ikamet eden sakinlerin verilerini işleyen ya da işleme niyeti olan bir kuruluş olması Tüzük'ün uygulama bulabilmesi için yeterli olmaktadır⁷¹⁷.

⁷¹⁶ Devrim AYDIN, “Ceza Kanunlarının Yer Yönünden Uygulanması”, *TBB Dergisi*, Y. 2011, S. 94, s. 133, ss. 131- 148.

⁷¹⁷ VOSS, “European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield and the Right to Delisting”, s. 222; KLEKOVIC, “EU GDPR vs. European Data Protection Directive”, <https://advisera.com/eugdpracademy/blog/2017/10/30/eu-gdpr-vs-european-data-protection-directive/> , E.T. 26.02.2019.

Kişisel verilerin korunması gibi sınırötesi bir konuda KVKK'nın yer bakımından uygulamaya dair belirleyici bir düzenleme yapmamış olması bir eksiklik olarak karşımıza çıkmaktadır. Özellikle yurtiçinde KVKK'ya uygun biçimde işlenip yurtdışına aktarılan veriler bakımından bu eksiklik oldukça önem taşımaktadır. Şöyle ki, bu aşamadan sonra hukuka uygun olark yurtdışına aktarılan verilerin yurtdışında kötüye kullanılmaları halinde ilgili kişinin kime başvurabileceği sorusu belirsiz kalmaktadır. Burada KVKK'nın dolanılması tehlikesi de karşımıza çıkmaktadır⁷¹⁸.

d) İstisnalar

KVKK, kişisel verilerin korunmasına ilişkin temel ilkeleri ortaya koyarken bir yanda da birçok hükümde istisnalara yer vermektedir. Bu bakımdan KVKK'da bulunan istisnalar üçe ayrılmaktadır;

- İlgili maddelerin kendi içinde düzenlenen istisnalar
- 28/1. maddede yer alan istisnalar (KVKK'dan tamamıyla istisna tutulan alanlar)
- 28/2. maddede yer alan istisnalar (KVKK'nın belli hükümlerinden istisna tutulan alanlar)

KVKK'nın kişisel verilerin işlenmesinde uyulacak “*Genel İlkeler*” başlıklı 4. maddesi, “*Kişisel verilerin işlenme şartları*”nı içeren 5. maddesi, “*Özel nitelikli kişisel verilerin işlenme şartları*” başlıklı 6. maddesi, “*Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi*”ni düzenleyen 7. maddesi, “*Kişisel verilerin aktarılması*” başlıklı 8. maddesi, “*Kişisel verilerin yurtdışına aktarılması*” başlıklı 9. maddesine bakıldığında, KVKK kapsamında kamu ve özel sektörde veri işlemenin temel ilkelerinin düzenlenmiş olduğu görülmektedir. Bu bağlamda öncelikle belirtilmelidir ki KVKK kapsamında veri işlemek isteniyorsa, ilgili maddelerde yer alan istisna hükümlerinin dikkatle incelenmesi gerekmektedir. Bu maddelerde birden fazla olacak şekilde başka

⁷¹⁸ ÇEKİN, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu*, s. 28.

bazı kanunlara atıf yapılmaktadır. Söz gelimi 4/1. maddede, kişisel verilerin bu Kanun’da ve “*diğer kanunlarda*” öngörülen usul ve esaslara göre işleneceği belirtilmektedir. Bir diğer örnek olarak verilerin silinmesi, yok edilmesi veya anonim hale getirilmesini içeren 7. maddeye göre verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesi hakkında diğer kanunlarda yer alan hükümler saklı tutulmaktadır. Veri aktarımı hususunda 8. madde ve yurtdışına veri aktarılması konusundaki 9. madde de diğer kanunlarda yer alan hükümleri saklı tutmaktadır. Görüleceği üzere kişisel verilerin korunması konusunda temel olan Kanun, konu ile ilgili ana ilkelerinde dahi yalnızca genel bir çerçeve çizmektedir. Bu durum öncelikle KVKK’nın kapsayıcı bir kanun olması önünde bir engel olarak görülebilecektir. Ayrıca başka hangi kanunlarda veri işleme esaslarına ilişkin hükümlere bakılması gerektiğinin ilk bakışta belirlenememesi gibi bir duruma da neden olmaktadır.

Söz konusu istisnalar bazı hükümlerden daha geniş bir uygulama alanı bulabilecektir. Örneğin normal şartlarda hassas verilerin işlenmesi çok daha özellikli ilkeler doğrultusunda gerçekleşmektedir. Bunun sebebi ise, hassas veriler dolayısıyla kişilerin ayrımcılık gibi bazı durumlarla karşılaşmaları ihtimalidir⁷¹⁹. KVKK’nın 6/3. maddesine göre, sağlık ve cinsel hayat dışındaki ırk, etnik köken, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançlar, kılık ve kıyafet, dernek, vakıf ya da sendika üyelikleri, sağlık, cinsel hayat, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili veriler ile biyometrik ve genetik veriler “*kanunlarda öngörülen hallerde*” ilgilinin açık rızası olup olmadığına bakılmaksızın işlenebilmektedir. Bu ise, temel amacı ayrımcılığa maruz kalınmasını önlemek olan özel nitelikli verilerin KVKK’nın 5/2(a). maddesinde yer alan “*Kanunlarda açıkça öngörülme*” ilkesinin dahi aranmaksızın öncelikli olarak başka herhangi bir kanunda öngörülen hükümlere göre işlenmesine sebep olacaktır⁷²⁰. Bu

⁷¹⁹ Kişisel verilere ilişkin bu ayrımın kabul görmediği örnekler de bulunmaktadır. İlerleyen bölümde incelenen, Alman Federal Mahkemesi’nin 1983 yılında verdiği “Nüfus Sayım Kanunu Kararı”na göre, veriler arasında “önemliler” ve “daha az önemliler” gibi bir ikilik yaratılmadan somut olaya göre durum gerektiriyorsa bazı verilere ayrıcalık tanınabilmelidir.

Bkz KÜZECİ, *Kişisel Verilerin Korunması*, s. 253.

⁷²⁰ KÜZECİ, *Kişisel Verilerin Korunması*, s. 332.

durum ise doğaldır ki, istisna olan bir hükmün ana kural hale gelmesine sebep olacak ve KVKK'nın uygulama alanını ve varlık sebebini daraltacaktır.

Kanun'un uygulama alanı bakımından ele alınması gereken bir diğer düzenleme de 28/1. maddede yer alan istisnalardır. Bu hükme göre bazı alanlar KVKK'nın uygulamasından bütünüyle istisna tutulmuştur. Buna göre;

- Gerçek kişilerin kendileri veya aynı konutta yaşayan aile bireyleri ile ilgili verileri işlemesi,
- İstatistik, araştırma ve planlama amacıyla verilerin işlenmesi,
- Sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında verilerin işlenmesi,
- Önleyici, koruyucu ve istihbari faaliyetler kapsamında verilerin işlenmesi,
- Soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin verilerin işlenmesi,

KVKK'nın uygulamasından muaf tutulmuştur.

İstisnai düzenlemelerden ilki olan, gerçek kişilerin kendileri veya aynı konutta yaşayan aile bireyleri ile ilgili verileri işlediği durumda bu veriler öncelikle üçüncü kişilere verilmemeli ve veri güvenliğine ilişkin yükümlülöklere uyulmalıdır. Burada “aynı konutta yaşayan aile bireyleri” ile ilgili veriler bu istisna kapsamında değerlendirilmektedir. Düzenlemenin temel gayesi, gerçek kişilerin “ev içi” veri işleme faaliyetleri kapsamında gereksiz ve orantısız zorluklarla karşılaşmasının önlenmesidir. Gerçek kişilerin başkalarına ait verileri kötüye kullanmaları son yıllarda artıyor olsa da Kanun kişisel ve aile içi kullanımı bu kapsamdan çıkarmak istemiştir⁷²¹. Burada “aynı konutta beraber yaşayan” herkes bu kapsamda değildir. Bu istisna, GVKT'de de benzer biçimde düzenlenmektedir. Tüzük'ün 2/2. maddesine göre; “*Bu Tüzük...tamamen kişisel veya ev faaliyeti esnasında bir gerçek kişi tarafından... kişisel verilerin işlenmesine*

⁷²¹ ÇEKİN, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu*, s. 26.

uygulanmaz.” Düzenlemeye biraz daha yakından bakıldığında görülecektir ki GVKT “kişisel veya ev faaliyeti” ibaresini içermekle KVKK’ya göre çok daha geniş bir alanı bu kapsamın dışına çıkarmaktadır. Söz gelimi, aynı evde birbirlerinin aile üyesi olmaksızın beraber yaşayan iki arkadaşın aynı wi-fi hattı üzerinden internete bağlanarak oluşturdukları internet trafiği GVKT nezdinde kapsam dışı iken, KVKK 28. madde doğrultusunda bir istisna oluşturmayacaktır. Yine burada değinilmesi gereken bir diğer husus da istisnanın tamamıyla kişisel veya ailevi veriler bakımından uygulanması gerekliliğidir. Adalet Divanı, 11 Aralık 2014 tarihli *Reynes* kararında⁷²² bu hükümlerin dar yorumlanması gerektiğini ve hırsızlıktan korunmak amacı ile evin girişine konulan kamerayla elde edilen verilerin kişisel ya da ailevi nitelikte olmadığını belirtmiştir.

Bu bağlamda gerçek kişilerin aynı konutta yaşayan aile bireyleri ile ilgili verileri işlemesi istisnası olan KVKK’nın 28/1(a) düzenlemesi ile ilgili olarak Anayasa Mahkemesi’nin 28 Eylül 2017 tarihli kararına değinmek yerinde olacaktır⁷²³. Bu kararda KVKK’nın birçok maddesi incelenmiş ve Kanun’un Anayasa’ya aykırı olmadığı hüküm altına alınmıştır. Davaya konu olan (a) bendindeki husus,

“Kişisel verilerin, üçüncü kişilere verilmemek ve veri güvenliğine ilişkin yükümlülöklere uyulmak kaydıyla gerçek kişiler tarafından tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında işlenmesi”

hâlinde 6698 sayılı Kanun hükümlerinin uygulanmayacağıdır. Bu hükme dair Mahkeme öncelikle hakkın özü değerdendirmesi yapmış ve

“...bir kişinin gerek kendi gerekse aynı konutta birlikte oturduğu aile fertlerine ilişkin kişisel verileri işlemesinin, söz konusu birlikte yaşamının doğal ve zorunlu bir sonucu olduğu anlaşılmaktadır... hakların kullanılmasını son derece zorlaştıran veya onu kullanılamaz duruma düşüren kayıtlara bağlandığı da söylenemeyeceğinden hakkın özüne dokunmadığı açıktır.”

⁷²² Case C-212/ 13 *František Ryneš v. Úřad pro ochranu osobních údajů*, 11.12.2014, Par. 30, 35, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62013CJ0212>, E.T. 22.04.2019.

⁷²³ AYMK E. 2016/125, K. 2017/143, K.T. 28.09.2017.

diyerek bu ihtimali ortadan kaldırmıştır. Mahkeme aile fertlerinin birbirlerine ait bazı kişisel verilerini işleyebileceğini ve bu durumun kanun koyucunun takdir yetkisi kapsamında düzenlendiğini, aile fertlerinin birbirlerinin kişisel verilerini işlemelerindeki yoğunluk ve sıklığı düşünerek veri işleme usulünün kolaylaştırıldığını belirtmiştir. Mahkeme'ye göre;

“Kanun koyucunun kuralla takdir yetkisi kapsamında gerçek kişilerin kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili söz konusu faaliyet ve yükümlülüklerin sıklık ve yoğunluk derecesini de dikkate alarak bunlarla ilgili veri işleme prosedürünü kolaylaştırmayı amaçladığı anlaşılmaktadır. Aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında tanınan dava konusu istisnanın başta çocuklar olmak üzere aile fertlerinin özerk varlığını, onurunu, maddi ve manevi bütünlüğünü ortadan kaldırmayı amaçlayan ya da bu amaca matuf bir hukuki müessese olmadığı aksine Anayasa'nın 41. maddesi ve başta 4721 sayılı Kanun olmak üzere diğer kanunlardan kaynaklanan aile fertleriyle ilgili hukuki faaliyet ve yükümlüklerin tam ve zamanında yerine getirilebilmesi suretiyle ailenin ve özellikle çocukların korunmasını sağlamaya yönelik olduğu açıktır.”

Ayrıca Mahkeme, ebeveynlerin çocukları üzerindeki velayet haklarını yerine getirirken Medeni Kanun'dan kaynaklanan yükümlülüklere uygun davranmaları gerektiği, uygun davranılmadığı takdirde 5395 Sayılı Çocuk Koruma Kanunu'nun devreye gireceğini ve çocuğun haklarının bu şekilde korunacağını belirtmiştir. Bu bakımdan AYM, bu kuralla ulaşılmak istenen amaç arasında makul bir denge kurulduğunu ve kuralın demokratik toplum düzeninin gerekleri ve ölçülülük ilkesine ters düşmediğini de hükme bağlamıştır. Oysa bu madde hükmü bakımından önemle belirtilmelidir ki, velayet ilişkisi çocukların varlığını, onurunu, maddi ve manevi bütünlüğünü yok sayma hakkı vermemektedir. Her ne kadar aile fertlerinin birbirlerinin kişisel verilerini işlemeleri oldukça masum görünüyor olsa da özellikle günümüz teknolojisi ve çocuk hakları ilişkisi düşünüldüğünde artık bir çocuğun dijital kimliği doğrudan doğumla başlamaktadır. Bu bakımdan her durumun spesifik olarak değerlendirilmesinin çok daha yerinde olabileceği düşünülmektedir.

Kanun'dan bütünüyle muaf tutulan bir diğer istisna da verilerin resmi istatistik ile anonim hâle getirilerek araştırma, planlama ve istatistik gibi amaçlarla işlenmesidir. Resmi istatistikleri düzenlemek Türkiye İstatistik Kurumu'nun (TÜİK) görevlerindendir. Söz konusu Kurum'un temel kanunu olan 5429 sayılı Türkiye İstatistik Kanunu iki defa AYM önüne gitmiştir⁷²⁴. Sadece bu bilgi dahi, Kanun'a ve dolayısıyla TÜİK'in resmi istatistiki verileri işlemesine dair oldukça tartışmalı bir durum olduğunu ortaya koyabilecektir. İlaveten bu istisna hükmünde *“Kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi.”* İbaresinde yer alan “gibi” ifadesi başka hangi amaçlarla veri işlenmesinin istisna kapsamında değerlendirilmesi gerektiği konusunda belirsizlik yaratmaktadır. Ayrıca “araştırma” ifadesi ile kastedilen de belirsizdir. Şayet bilimsel araştırma söz konusu ise, bir başka istisna hükmü olan 28/1(c). maddesinde yer alan “bilimsel amaçlarla” işlenen verilerin oluşturduğu istisna düzenlemesi de anlamsız kalacaktır⁷²⁵.

KVKK kapsamına girmeyen üçüncü bir istisna da tıpkı GVKT'nin 85. maddesinde⁷²⁶ olduğu gibi, ifade özgürlüğü ile kişisel verilerin korunması hakkı arasında bir denge kurmaya yönelik olan, verinin

⁷²⁴ Bu kararlardan ilki, Anayasa Mahkemesi'nin 20 Mart 2008 tarihli kararıdır (AYMK E. 2006/ 167, K. 2008/86, K.T. 20.03.2008). AYM burada, 5429 sayılı Kanun'un bilgi toplama, saklama, işleme ve değiştirme tekeli olan idareye ve diğer kişilere karşı korumasız bırakıldığını, veri toplamanın sınırlarına yasal düzenlemede yer verilmediğini belirtmektedir. Ayrıca kararın oldukça önemli bir noktası da en güçlü veri tekelinin idarede olduğunun ve bunun sınırlandırılması gereğinin vurgulanmasıdır. Bu kararın ardından AYM 5429 sayılı Türkiye İstatistik Kanunu'na ilişkin bu defa 12 Ekim 2011 tarihinde başka bir kararı (AYMK E. 2010/12, K. 2011/135, K.T. 12.10.2011) hüküm altına almış; ancak bu defa anılan Kanun Anayasa'ya uygun görülmüştür.

⁷²⁵ KÜZECİ, *Kişisel Verilerin Korunması*, s. 334.

⁷²⁶ GVKT md. 85'e göre; *“Gazetecilik amaçları ve akademik, sanatsal veya edebi anlatım amaçları doğrultusunda işleme de dahil olmak üzere, üye devletler bu Tüzük uyarınca kişisel verilerin korunması hakkı ile ifade ve bilgi edinme özgürlüğü hakkını kanunla bağdaştırır.*

Gazetecilik amaçları veya akademik, sanatsal veya edebi anlatım amacıyla gerçekleştirilen işleme faaliyeti açısından, üye devletler, kişisel verilerin korunması hakkı ile ifade ve bilgi edinme özgürlüğünü bağdaştırma amacıyla gerekli olmaları durumunda, Bölüm II (ilkeler), Bölüm III (veri sahibinin hakları), Bölüm IV (kontrolör ve işleyici), Bölüm V (kişisel verilerin üçüncü ülkeler veya uluslararası kuruluşlara aktarılması), Bölüm VI (bağımsız denetim makamları), Bölüm VII (işbirliği ve tutarlılık) ve Bölüm IX (spesifik veri işleme durumları) ile ilgili olarak muafiyetler veya derogasyonlar sağlar.

*“millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi”*dir.

İfade özgürlüğü ile kişisel verilerin korunması hakkı arasında bir menfaat dengesinin oluşması gerektiğini ifade eden Adalet Divanı’na göre, ticari bir unsur içeren vergi mükelleflerinin gazetede yayınlanması, ifade özgürlüğü ve gazetecilik kapsamında ele alınmıştır⁷²⁷.

28/1. madde bağlamında oldukça önemli bir istisna hükmü de,

*“Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi”*dir.

Madde gerekçesinde “Millî İstihbarat Teşkilatı ile diğer istihbarat birimlerinin...” işlediği verilerin Kanun kapsamı dışında tutulmakta olduğu belirtilmektedir. Anılan hüküm doğrultusunda oldukça geniş ve önemli bir alan Kanun’un kapsamı dışında bırakılmıştır. Her ne kadar söz konusu veri işleme, millî savunma, millî güvenlik, kamu güvenliği, kamu düzeni veya ekonomik güvenlik açılarından önemi büyük olsa da yarışan değerler arasında bir denge kurulmaya çalışılarak veri işlemenin veri koruma hukukunun temel ilkeleri nazara alınarak gerçekleştirilmesi Kanun’un ruhuna çok daha uygun olurdu.

28/1. madde kapsamında KVKK’nın uygulamasından bütünüyle muaf tutulan son düzenleme ise, verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi halidir. Bu istisna oldukça geniş kapsamlı bir alandır ve bütünüyle veri koruma kapsamından çıkarılması temel hak ve özgürlükler bakımından oldukça sorunlu bir alan oluşturmaktadır. Bu istisna

Her üye devlet 2. paragraf uyarınca kabul ettiği kanun hükümlerini ve bunları etkileyen sonraki değişiklik kanunu veya değişiklikleri, herhangi bir gecikmeye mahal vermeksizin, Komisyon’a bildirir.”

⁷²⁷ Case C-73/07 Tietosuoja- ja valtuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy, 16.12.2008, Par. 44, <https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:62007CJ0073> , E.T. 22.04.2019.

bakımından AYM'nin 27 Şubat 2019 tarihli bir karar olan *Fatih Saraman Başvurusu*⁷²⁸ dikkatle incelenmelidir. Karara konu olayda, 18 yaşından küçük olduğu esnada hakkında beş ay hapis cezasına hükmedilmiş ancak sonrasında cezası para cezasına çevrilmiş ve cezası ertelenmiş olan başvurucunun, başvurduğu ve başarılı olduğu bir işe alım işleminde başlatılan güvenlik ve arşiv soruşturması sonunda hakkında hırsızlık suçundan işlem yapıldığının tespiti ve ilgili düzenleme uyarınca öngörülen “*güvenlik soruşturması olumlu olmak*” şartı gereğince işe alımının gerçekleşmemesi söz konusudur. Bu bağlamda AYM, davaya konu olan işlemin dayanağı olan düzenlemenin kişisel verilere ilişkin süre, stoklama, kullanım, üçüncü kişilerin erişimi, verilerin gizliliği, bütünlüğü ve imhası konusundaki usullerdeki yetki aşımı ve keyfiliğe karşı yeteri kadar güvenceye sahip olmalarını sağlayacak açık ve detaylı kuralların bulunmadığını ve bu sebeple müdahalenin dayanağı olan düzenlemenin kanunilik şartını sağlamadığını ele alarak Anayasa'nın 20. maddesinde yer alan özel hayata saygı hakkının ihlal edildiği sonucuna varmıştır. Görülmektedir ki, yargı makamları ve infaz mercileri tarafından gerçekleştirilen veri işleme hallerinin bütünüyle KVKK kapsamında ya da daha geniş bir ifadeyle veri korumanın temel ilkeleri kapsamında çıkarılması oldukça hayati sonuçlara neden olabilecektir.

Bir diğer istinsa tutulan grup ise, KVKK'nın 28/2. maddesinde bulunan alanlardır. Anılan alanlar KVKK'nın belli hükümlerinin uygulamasından muaf tutulmaktadır. KVKK'nın uygulanmayacak olan hükümleri sırasıyla, 10. maddede yer alan *veri sorumlusunun aydınlatma yükümlülüğü*, 11. maddede yer alan *zararın giderilmesini talep etme hakkı hariç olmak üzere ilgili kişinin diğer hakları* ve 16. maddede yer alan *Veri Sorumluları Sicili'ne kayıt yükümlülüğü*dür. Bu düzenlemeler aşağıda belirtilecek hallerde veri işlenmesi durumlarına uygulanmayacaktır. Buna göre kişisel veri işlemenin;

- Suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması,
- İlgili kişinin kendisi tarafından alenileştirilmesi neticesinde olması,

⁷²⁸ *Fatih Saraman Başvurusu*, Başvuru No: 2014/7256, K.T. 27.02.2019.

- Kanun'un verdiği yetkiye dayanılarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olması,
- Bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olması,

hallerinde, KVKK'nın 10., zararın giderilmesini talep etme hakkı hariç 11. ve 16. maddeleri uygulanmayacaktır. Ancak burada önemle belirtilmelidir ki bu veriler, üçüncü kişilere verilmemelidir ve işlenmelerinde veri güvenliğine ilişkin yükümlülöklere uyulması zorunludur.

KVKK'nın 28/1. maddesinde olduđu gibi bu düzenlemede de devletin faaliyetlerine dair hususlar oldukça geniş bir biçimde istisna alanında tutulmaktadır. Dolayısıyla devlet ilgili konularda veri işlerken, Kanun'un veri koruması sınırlı olacaktır. Bilindiğı üzere kişisel verilerin korunması hakkı mutlak bir hak değildir; ancak veri korumanın belli bir seviyede sağlanması gerekliliğı de ortadadır. Böylesi geniş ve hatta belirsiz olarak nitelenebilecek istisnalar veri korumanın anlamını yitirmesine sebep olabilecektir. Bu sebeple hukuka uygun veri işleme, meşru amaçlar için veri işleme, amacın gerektirdiğı ölçüde ve sürede veri işleme gibi bazı temel veri koruma ilkeleri istisnasız uygulanmalıdır⁷²⁹.

6698 sayılı KVKK'nın Anayasa'ya aykırılığı iddiasıyla açılan 28 Eylül 2017 tarihli karar⁷³⁰ da Kanun'un pek çok maddesi ile birlikte istisnaların yer aldığı 28. maddesinin de iptali istenmiştir. Davaya konu olan (a) bendindeki husus, KVKK'nın tamamen uygulanmayacağı alanlardan olan, gerçek kişiler tarafından tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında verilerin işlenmesi halidir. Bu hükme dair Mahkeme öncelikle hakkın özüne dokunmadığını belirmiştir. Davaya konu olan ve (ç) bendinde yer alan ve KVKK'nın uygulanmayacağı bir diğer

⁷²⁹ KÜZECİ, *Kişisel Verilerin Korunması*, s. 339.

⁷³⁰ AYMK E. 2016/125, K. 2017/143, K.T. 28.09.2017.

istisna veri işleme durumu ise, “...önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi”dir. AYM’ye göre, kişisel verilerin korunması hakkı sınırsız bir hak olmayıp “Anayasa’da Devlete bir görev olarak yüklenen millî güvenliğin ve kamu düzeninin sağlanması ile suç işlenmesinin önlenmesi amaçlarıyla sınırlandırılması mümkündür.” Bu bağlamda Mahkeme hem İHAM’a hem de 108 Numaralı Sözleşme’ye atıf yaparak bu sınırlamanın

“Anayasa’da devlete verilen görevlerin gereği olarak millî güvenliğin, kamu düzeninin ve suç işlenmesinin önlenmesini sağlamak amacıyla yapıldığından demokratik toplum düzeni bakımından alınması gereken tedbirler kapsamında”

değerlendirmektedir.

İstisnalara dair ilgili düzenlemenin ele alındığı bu AYM kararının detaylı inceleme ve eleştirisi ilgili başlık altında yer almaktadır⁷³¹.

2. Temel İlkeler

KVKK’nın 4. maddesine göre, veri işlemede uyulması gereken belli asgari şartlar ve ilkeler bulunmaktadır. Bu ilkelere aykırı hareket edilmesi, veri işlemeyi hukuka aykırı hale getirir. Söz konusu ilkeler;

- Hukuka ve dürüstlük kurallarına uygun olma
- Doğru ve gerektiğinde güncel olma
- Belirli, açık ve meşru amaçlar için işlenme
- İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma
- İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme şeklindedir.

Burada yer alan ilkeler, tüm veri işleme faaliyetlerinde uyulması gereken asgari bir ölçüttür. Kanun’un geneli gibi, söz konusu ilkeler de 95/46/AT sayılı Direktif ile

⁷³¹ Detaylı analiz için bkz. İlgili Anayasal İçtihat başlığı.

benzerlik göstermektedir. Bu ilkelerin yanı sıra 4-9. maddeler arası olan kurallar, veri işlemenin mihenk taşlarıdır. KVKK kapsamında hukuka uygun veri işlemenin gerçekleştirilmesi için, temel ilkeler, kişisel verilerin işlenme şartları, özel nitelikli verilerin işlenme şartları, verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi, yurtiçinde ve yurtdışında veri aktarımına dair tüm kurallara uygunluk gerekmektedir.

4. maddede yer alan temel ilkelere daha yakından bakmadan önce belirtilmelidir ki KVKK kapsamında esas kural, kişisel verilerin işlenmemesidir. Anayasa'nın 20/3. maddesine göre; *“Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir.”* Dolayısıyla kişisel verilerin işlenmesinin kural olarak yasak olmasının sebebi, Anayasa'nın ilgili hükmüdür. Bu maddeye dayanılarak yapılan 6698 sayılı KVKK da verilerin nasıl işlenebileceğinin anahtarını sunmaktadır. En temel şekliyle, kişinin rızası ve kanuni bir temel mevcut ise, kişisel veriler işlenebilecektir.

GVKT bakımından da kural olarak işlenmesi mümkün olmayan verinin işlenebilmesi için gerekenler düzenlemeye yer almaktadır. Günümüzde ise teknolojinin geldiği nokta sebebiyle bu durum kimi zaman eleştirilmektedir⁷³². Ancak gözden kaçırılmamalıdır ki, veri işlemenin ana kural, işlememenin ise istisna olduğu bir forma yönelindiği görülmektedir. Dolayısıyla hem KVKK hem GVKT bakımından yakın zamanda yeni bir arayışa gidilmesi mümkün olabilecektir.

Veri işleme ilk başta KVKK'nın 4. maddesinde yer alan temel ilkelere uyulması ile olacaktır. Söz konusu ilkelere uyulmayarak da veri işlenmesi mümkündür; ancak bu durumda veri işleyen kişi Kanun'da yer alan yaptırımlarla karşılaşacaktır. Zaten Kanun'un varoluşunun bir diğer anlamı da hukuka uygun veri işlemeyenlerin karşılaşacağı yaptırımları düzenlemektir.

Temel ilkelere daha yakından bakılacak olursa, ilk olarak veri işlemenin hukuka ve dürüstlük kuralına uygun olması gerektiği belirtilmektedir. Buna göre, hukuka uygun

⁷³² ÇEKİN, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu*, s. 43.

veri işleme, ilgilinin rızası ile ve ancak KVKK'da açıkça izin verilen hallerde mümkündür. Dürüstlük kuralı ise, veri işleyen kişinin bunu gerçekleştirirken haklarını kötüye kullanmaması gerektiğini ifade eder⁷³³.

Bir diğer temel ilke de doğru ve güncel olma ilkesidir. Kişisel veriler işlenirken doğru ve gerektiğinde güncel olmalıdır. Bu noktada veri sorumlusu bilgilerin doğruluk ve güncelliğini sağlamak için kendisinden beklenen tüm önlemleri almalıdır. “Gerektiğinde” güncel olma ifadesi ise, söz gelimi arşivsel bilgiler gibi bazı durumlarda güncel olmayan eski verilerin saklanması gerekebileceği ile ilgilidir⁷³⁴.

Temel ilkelerden bir diğeri de “Belirli, açık ve meşru amaçlar için işleme” biçiminde ifade edilen şeffaflık ilkesidir. Bu ilke sayesinde ilgili kişi veri işleme sürecini kontrol edebilecektir. Bu bakımdan ilgili kişi ile paylaşılan bilginin somut, açık ve anlaşılır olması gerekmektedir. Dolayısıyla ilgili kişinin kafasını karıştıracak biçimde, oldukça uzun veya ağdalı bir dille kaleme alınan metinlerin açık rızanın verilmesine uygun olmadığı aşikardır. KVKK'nın 11. maddesi bağlamında ilgili kişi, veri sorumlusuna başvurmak suretiyle birçok hakka sahiptir⁷³⁵. Bu doğrultuda şeffaflık

⁷³³ Belirtilmektedir ki, burada konu olan dürüstlük kuralı Medeni Kanun'un 2/2. Maddesinde yer alan dürüstlük kuralı değildir. Daha ziyade veri işleyen kişilerin (veri sorumlusu veya bu kişi adına veri işleyen 3. Kişi) Kanun'da yer alan haklarını adil biçimde kullanmalarını karşılamaktadır.

ÇEKİN, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu*, s. 45.

⁷³⁴ ÇEKİN, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu*, s. 53.

⁷³⁵ KVKK md. 11: “Herkes, veri sorumlusuna başvurarak kendisiyle ilgili;

a) Kişisel veri işlenip işlenmediğini öğrenme,
b) Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,
c) Kişisel verilerin işleme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,
ç) Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,
d) Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme,
e) 7 nci maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme,
f) (d) ve (e) bentleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,
g) İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,
ğ) Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme, haklarına sahiptir.”

ilkesinin amacına ulaşabilmesi, ilgilinin hakları ile birlikte değerlendirilerek mümkün olacaktır.

Bir başka temel ilke de en genel ifadesi ile amaca bağlılık ilkesidir. Bu ilke, veri işlemenin amacı ile bağlantılı olmasını kapsamaktadır. Kanun koyucu burada, veri işlenirken amacın en başta ortaya konarak, hangi sebeple bu işlemin gerçekleştirildiğinin bilinmesi ve bunun harici durumlarda işlemenin hukuksuz olacağının anlaşılmasını istemiştir. Veri sorumlusu veriyi işlemeden önce mutlaka amaç ya da amaçlarını ortaya koymalıdır; fakat bu, herhangi bir amaç belirtip istenildiği şekilde veri işlenmesi anlamına gelmemektedir. Amaç, veri işlenmesini en asgari düzeyde gerçekleştirmek olmalıdır. İlâveten belirtilmelidir ki, yalnızca veri işlemek, bu veriyi toplamak ve depolamak bir amaç değildir⁷³⁶. Ayrıca maddede de belirtildiği üzere amacın belirli ve açık olması gerekmektedir. Söz gelimi bir internet sitesinden alışveriş yaparken üye olmanız gerektiği ve üyelik işlemini tamamlarken “hizmet kalitesini artırabilmek ve sizi gelecekte yapacağımız kampanyalardan haberdar etmek” ifadesine onay vererek kişisel verilerinizin işlenmesi sağlanmak istendiğinde, şüphesiz bu soyut amaç veri işleme için muğlak kalacaktır. Amaç, belirli, açık ve meşru olmak zorundadır⁷³⁷. Ayrıca amacın ortaya konulmasında işin kapsamı ve hitap ettiği kitle de önem taşımaktadır ve bu bağlamda sunulması gereken detaylar farklılık gösterebilir.

Burada 95/46/AT sayılı Direktif’in 29. maddesi uyarınca kurulmuş olan Veri Koruma Çalışma Grubu’nun “Amaç Sınırlama” ile ilgili verdiği bazı örneklerle bakmak faydalı olabilecektir. Buna göre örneğin, küçük bir kasabada yerel halka satış yapan ve müşterileri hakkında yalnızca sınırlı bilgi toplayan yerel bir dükkânın, kişiselleştirilmiş teklifleri bildirmek ve mallarını tüm Avrupa’da satmak için hedeflenen reklamları yapmak için internet sitesinde karmaşık analitik kullanan büyük bir perakende şirketi

⁷³⁶ ÇEKİN, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu*, s. 46.

⁷³⁷ Working Party on the Protection of Individuals with regard to the Processing of Personal Data, Opinion 03/2013 on purpose limitation, 02.04.2013, s. 15- 20, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf, E.T. 23.04.2019.

kadar çok ayrıntılı bir şekilde amaç belirtmesi gerekmez. Bir diğer örnek ise, Facebook gibi Avrupa çapında faaliyet gösteren bir sosyal ağ web sitesinin, farklı kültürlerde geniş bir kullanıcı grubunu hedeflemesi dolayısıyla amaçlarını belirlerken bunun biçimine ve sağladığı bilgilerin netliğine özel dikkat göstermesi gerektiğidir⁷³⁸. Amaca bağlılık ilkesi bakımından önemli bir nokta olarak “işleme esnasında amacın değişmesi” ihtimaline de değinilmesi yerinde olacaktır. Bu bağlamda belirtilmelidir ki, KVKK’nın 95/46/AT sayılı Direktif’i esas alarak düzenlenmiş olmasının da etkisiyle, bu ihtimal Kanun’da değerlendirilmemiştir. Oysa günümüzde veri işlemenin adeta bir kural haline geldiği bir ortamda bu ihtimale ilişkin de bir düzenleme bulunması yerinde olabilirdi. GVKT’ye baktığımızda ise, 6/4. maddesinde kişisel verilerin toplanma amacı dışında bir amaca yönelik olarak yapılan işleme faaliyetlerinin de düzenlendiği görülmektedir. Bu maddeye göre, veri öznesinin rızasının yeniden alınması halinde veya maddede bulunan diğer unsurlar gerçekleştirildiğinde verinin ilk toplama amacı dışında bir amaçla verinin işlenmeye devam edilebileceği görülmektedir.

KVKK kapsamında veri işlemenin bir diğer temel ilkesi, işlemenin amacı ile sınırlı ve ölçülü olmasıdır. Bu ilke kapsamında asgari ölçüde veri işlenmelidir. Daha açık bir ifade ile, varılmak istenen amaca veri işlenmeksizin ulaşılabiliriyorsa, veri işlenmemelidir. Fakat bu amaca ancak veri işlenmesi ile ulaşılabiliriyorsa, bu noktada da en az gereken biçimde işlenmelidir⁷³⁹.

Maddede yer alan son ilke ise, işlemenin ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesidir. Bu ilke verilerin belirsiz bir süre, ilanihaye tutulmasını engellemek içindir. Kişisel verilerin mütemadiyen muhafaza edilmesi, kişi için adeta bir “Demokles Kılıcı” yaratabilecek; bu ise, kişisel verilerin korunması hakkının temel felsefesinde yer alan kişiliğin serbestçe geliştirilmesi

⁷³⁸ Working Party on the Protection of Individuals with regard to the Processing of Personal Data, Opinion 03/2013 on purpose limitation, 02.04.2013, s. 51, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf, E.T. 23.04.2019.

⁷³⁹ ÇEKİN, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu*, s. 53; Mesut Serdar ÇEKİN, “6698 sayılı Kişisel Verilerin Korunması Kanunu’nun Big Data (Büyük Veri) ve İrade Serbestisi Açısından Değerlendirilmesi”, İÜHFİM, C. LXXIV, S. 2, Y. 2016, s. 637, ss. 629- 644.

hakkına ters düşecektir⁷⁴⁰. Saklanan veriye ihtiyacın sona ermesi halinde ise derhal yok edilmesi gerekir. Açıktır ki, meşru amaç gerçekleşene kadar verinin saklanması hukuka uygundur⁷⁴¹. KVKK'nın 16. maddesinde “Veri Sorumluları Sicili” düzenlenmektedir. Bu maddeye göre verileri işleyen gerçek ve tüzel kişiler, veri işlemeyen önce Veri Sorumluları Sicili'ne, belli hususların yanı sıra kişisel verilerin işlendikleri amaç için gerekli olan azami sürenin de bildirimini yaparak kaydolacaklardır.

Temel ilkelere ilişkin olarak belirtilmelidir ki, Kanun kapsamında bu ilkelerin nasıl sağlanacağına dair bir hüküm mevcut değildir. Öte yandan GVKT'nin 25/1. maddesinde özel ve olağan veri korumasında genel ilkelerin ne şekilde uygulanması gerektiğini ve daha evvel belirtildiği üzere, bir yenilik olarak, tasarımla veri koruma ve varsayılan ayarlarla veri koruma gibi önleyici veri koruma usullerine de yer vererek ortaya koymaktadır. İlgili maddeye göre;

“Kontrolör, son teknoloji, uygulama maliyeti ve işleme faaliyetinin mahiyeti, kapsamı, bağlamı ve amaçlarının yanı sıra işleme faaliyetinin gerçek kişilerin hakları ve özgürlükleri açısından teşkil ettiği çeşitli olasılıklar ve ciddiyetlere sahip riskleri dikkate alarak, hem işleme yönteminin belirlenmesi esnasında hem de işleme faaliyeti esnasında, verilerin en alt düzeye indirilmesi gibi veri koruma ilkelerinin etkili bir şekilde uygulanması ve bu Tüzük'ün gerekliliklerinin yerine getirilmesine yönelik olarak gerekli güvencelerin entegre edilmesi amacı ile tasarlanan takma ad kullanımı gibi uygun teknik ve düzenlemeye ilişkin tedbirler uygular ve veri sahiplerinin haklarını korur.”

Temel ilkelere ilişkin olarak son olarak belirtilmelidir ki, Kanun'un tamamen ya da kısmen uygulanmayacağı istisnalara başvurulmasında dahi Kanun'daki kurallara uygunluk, kişisel verilerin korunmasının tam anlamıyla gerçekleştirilebilmesi için önem taşımaktadır.

⁷⁴⁰ KÜZECİ, *Kişisel Verilerin Korunması*, s. 342.

⁷⁴¹ Nilgün BAŞALP, *Kişisel Verilerin Korunması ve Saklanması*, Yetkin Yayınevi, Ankara, 2004, s. 39.

3. Kişisel Verilerin İşlenme Şartları

Daha önce belirtildiği üzere, Anayasa'nın 20/3. maddesine göre kişisel veriler ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Bunun anlamı, temel bir hak olarak Anayasa'da düzenlenen kişisel verilerin korunması hakkı, ancak hakkın öznesinin rızası ya da kanunda öngörülen hallerde bir sınırlamaya maruz kalabilecektir.

Kişisel verilerin işlenme şartları, KVKK'nın 5. maddesinde ele alınmaktadır. Ana kural, tıpkı Anayasa'da olduğu gibi, ilgili kişinin rızası olmadan veri işlenememesidir. Bu bakımdan Kanun, hukuka uygun biçimde veri işlemek için açık rızayı aramaktadır. Gerekçe'ye bakıldığında dayanağının 95/46/AT sayılı Direktif olduğu belirtilen "açık rıza"nın tanımı, Kanun'un 3/1(a). maddesine göre; *"Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı"* karşılamaktadır. Bu tanıma göre, belirli, bilgilendirmeye dayanan ve özgür irade ile açıklanan bir bildirim söz konusudur. Bu rıza sıradan bir rıza değildir. Açık rızanın sadece bir formalite olarak düşünülmemesi ve gerçekten ilgili kişinin niyetini yansıtır yansıtmadığı hususunda detaylı bir inceleme yapılması gerekmektedir⁷⁴². 95/46/AT sayılı Direktif de *"veri öznesinin rızasını açık bir biçimde verdiğinde"* verinin işlenebileceğinden ve bu rızanın, her ne kadar uygulamada sorunlar oluşabilse de bilgilendirilmiş ve gönüllü olması gerektiğinden söz etmektedir⁷⁴³. GVKT'nin 4/11. maddesine göre ise açık rıza, *"veri öznesinin bir beyanı yoluyla ya da açık bir onaylama fiiliyle kişisel verilerinin işlenmesine cevaz verdiğini gösteren özgür, spesifik, bilinçli ve açık bir göstergesidir."* Görüleceği üzere, GVKT'de yer alan tanım çok daha anlaşılır ve somuttur. Belirtilmelidir ki, açık rıza veri işlemenin bir önşartıdır. Dolayısıyla açık rızanın, verinin işlenmesinden önce alınması gerekmektedir. Bunun dışında Tüzük'e göre rızanın açık/ pozitif bir eylemle ortaya konulması şarttır. Bu bağlamda, rızanın daima aktif bir hareket veya

⁷⁴² ÇEKİN, "6698 sayılı Kişisel Verilerin Korunması Kanunu'nun Big Data (Büyük Veri) ve İrade Serbestisi Açısından Değerlendirilmesi", *İÜHFM*, s. 636- 637, 640.

⁷⁴³ Detaylı bilgi için bkz. Eleni COSTA, *Consent in European Data Protection Law*, Nijhoff Studies in European Union Law, Martinus Nijhoff Publishers, 2013, s. 110 vd.

bildirim yoluyla verilmesi gerektiği, GVKT bakımından söz gelimi önceden işaretlenmiş kutucuklarla rızanın verilemeyeceği anlamına gelir⁷⁴⁴.

Kanun'un 5/2. maddesinde ise, açık rıza olmadan veri işlemenin mümkün olabildiği haller ele alınmaktadır. Bunun dışında yukarıda belirtildiği üzere, veri işleme esnasında ayrıca Kanun'un 4. maddesinde düzenlenen temel ilkeler de hesaba katılmalıdır. Dolayısıyla her ne kadar 5. maddenin başlığı "Kişisel verilerin işleme şartları" olsa da kişisel verileri işlenirken 4. ve 5. maddeler bir arada dikkate alınmalıdır. 5/2. madde bakımından öncelikle veri işlemenin "*kanunlarda açıkça öngörülmesi*" aranmaktadır. Bunun anlamı, başka kanunlarda veri işlemeye cevaz veren hükümlerin olması halinde kişisel verilerin işlenebileceğidir. Gerekçe'de bu konuda verilen örneklerden biri, kolluk tarafından bir suç soruşturması sebebiyle, 2559 sayılı Polis Vazife ve Salahiyet Kanunu'nun 5. maddesine göre şüphelilerin parmak izlerinin alınması halidir.

Açık rıza olmaksızın veri işlemenin mümkün olabileceği diğer bir hal ise,

*"Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması"*dır.

Burada kişinin;

- Fiili bir imkânsızlık sebebiyle rızasını açıklayamayacak halde olması veya rızasına hukuki geçerlilik tanınmaması hallerinden birinde olup

⁷⁴⁴ Opt-in ya da opt- out metodunda veri öznesinin verilerinin belli bir amaç için kullanılmasını istemediğinde bir kutucuğa tik atmak (opt-out) ya da verisinin işlenmesine onay verdiği hallerde buna dair kutucuğa onay için tik atmak (opt-in) durumlarını ifade etmektedir. CAREY, *Data Protection: A Practical Guide to UK and EU Law*, s. 254; Working Party on the Protection of Individuals with regard to the Processing of Personal Data, Guidelines on consent under Regulation 2016/679, 28.11.2017 and Revised 10.04.2018, s. 15- 16, https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51030 , E.T. 25.04.2019; Milda MACENAITE, Eleni KOSTA, "Consent for Processing Children's Personal Data in the EU: Following in US Footsteps?", *Information & Communications Technology Law*, 2017, Vol. 26, No: 2, s. 156- 158, ss. 146- 197.

- Kendisinin ya da bir başkasının hayatı ve beden bütünlüğünün korunması için veri işlemenin zorunlu olması gerekmektedir.

Veri işlemenin açık rıza olmaksızın işlenebileceği bu hale ilişkin olarak Gerekçe’de şöyle bir örnek verilmiştir:

“kişinin şuurunun yerinde olmadığı veya akıl hastası olması sebebiyle rızasının geçerli olmadığı bir durumda, hayat veya beden bütünlüğünün korunması amacıyla, tıbbi müdahale yapılması sırasında, kişisel verileri işlenebilecektir.”

Ancak bu örnek Kanun’un 6/1. maddesine göre açıktır ki, sağlık verisidir ve bu maddede ele alınan “Özel nitelikli kişisel verilerin işlenme şartları”na tabidir⁷⁴⁵.

İlgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin olanaklı olduğu üçüncü bir hal de, “Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması” halidir. Bazı durumlarda bir sözleşmenin kurulması ya da ifası için bazı verilerin işlenmesi elzemdir. Bu başlığa dair kalıcı ve güncel bir örnek ise internet üzerinden yapılan alışverişlerdir. Buna göre kişi internet üzerinden bir mal almak istediğinde, kurulan sözleşme icabı adresini, kredi kartı bilgilerini ve bazı durumlarda T.C. Kimlik Numarasını vermek durumundadır. Gerekçe’de verilen örnekler ise,

*“yapılan bir sözleşme gereği paranın ödenmesi için alacaklı tarafın hesap numarasının alınması ile bir bankayla kredi sözleşmesi yapılması sırasında bankanın, o kişiye ait maaş bordrosunu, tapu kayıtlarını, icra borcu olmadığına dair belgeyi sözleşmenin kurulması için istemesi”*dir.

Rıza aranmaksızın veri işlemenin mümkün olduğu bir başka hal ise, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için veri işlemenin zorunlu olmasıdır. Veri sorumlusunun KVKK kapsamında yükümlülükleri genel itibarıyla 10. ve 12. maddelerde düzenlenmektedir. Bunun dışında ise, veri sorumlusunun başka kanuni

⁷⁴⁵ KÜZECİ, *Kişisel Verilerin Korunması*, s. 346.

düzenlemelerden kaynaklanan yükümlülükleri de mevcut olabilmektedir. Gerekçe’de verilen örnek bu bakımdan aydınlatıcı olacaktır. Buna göre,

“bir şirketin çalışanına maaş ödeyebilmesi için, banka hesap numarası, evli olup olmadığı, bakmakla yükümlü olduğu kişiler, eşinin çalışıp çalışmadığı, sosyal sigorta numarası gibi verileri işlemesi”

bu kapsamda değerlendirilecektir.

Kişisel verinin ilgili kişinin kendisi tarafından alenileştirilmiş olması halinde de rıza aranmaksızın bu verilerin işlenebilmesi mümkündür. Gerekçe’de bu duruma dair bir örnek mevcut değildir. Onun yerine;

“ilgili kişinin kendisi tarafından alenileştirilen bir başka ifadeyle herhangi bir şekilde kamuoyuna açıklanmış olan kişisel verileri işlenebilecektir. Çünkü ilgili kişi tarafından alenileştirilen ve böylelikle herkes tarafından bilinebilecek hale gelen bu tür verilerin işlenmesinde, korunması gereken hukuki yararın ortadan kalktığı kabul edilmektedir.”

şeklinde bir ifade yer almaktadır. Buna göre alenileştirme, ilgili kişi tarafından kamuoyuna açıklanarak kişisel verilerin herkesçe bilinebilirliğinin sağlanmasıdır. Ancak bu ifade oldukça muğlaktır. Şöyle ki, bir kariyer sitesinde özgeçmiş ile birlikte konulan bir fotoğrafın herkesçe görüntülenebilmesi ya da kişinin isminin herhangi bir arama motoruna yazılması sonucu bulunduğu kurumsal ya da sosyal medya siteleri üzerinden fotoğrafının ya da başka kişisel bilgilerinin görüntülenebilmesi halinde, bu fotoğraf ve bilgiler “alenileştirilmiş” olacak ve bu sebeple kişinin rızası olmaksızın her yerde işlenebilecek midir? Yine bir başka örnek olarak, kartvizit sahibi bir kişinin cep telefonu, adresi gibi verilerini kartviziti üzerinden paylaşıyor olması, bu bilgilerin herkes tarafından bilinebilecek hale gelmesi sonucu korunmalarına dair hukuki yararın ortadan kalktığı sonucunu doğuracak mıdır? İşte böylesi belirsiz bir kavramın varabileceği sonuçlar, kişisel verilerin korunması hakkı bakımından oldukça sakıncalı olabilecektir. Dolayısıyla kişisel verinin ilgili kişinin kendisi tarafından alenileştirilmiş olması halinde de rıza aranmaksızın bu verilerin işlenebilmesi durumunun hem Kişisel Verileri Koruma

Kurumu kararları, hem de mahkeme içtihatları ile uygulamasının netleştirilmesi çok daha isabetli olacaktır. Doktrinde bazı yazarlarca bu konuya ilişkin olarak, kişisel verilerin ilgili kişi tarafından alenileştirilmesinin, her durumda ve şekilde istenildiği gibi işlenebileceklerini ifade etmediği, ilgili kişinin bu verileri alenileştirme sebeplerine de bakılması gerektiği ve her durumda KVKK'nın temel ilkelerinin izlenmesi gerektiği ifade edilmektedir⁷⁴⁶.

KVKK'nın 5. maddesinde yer alan ve açık rıza aranmaksızın veri işlenebilecek hallerden bir diğeri de *“Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olduğu haller”*dir. Bu ifadenin anlaşılabilmesi adına Gerekçe’de, bir şirketin kendi çalışanı tarafından açılan bir davada ispat için bazı verileri kullanması veya kısıtlı bir kişinin haklarının korunması amacıyla vasinin veya kayyımın, kısıtlının mali bilgilerini tutması örnekleri verilmiştir. Daha açıklayıcı ve net olmak adına kapsamı daha belirli ve ilk örneğe yakın bir örnek verilebilir. Buna göre, işten ayrılan bir çalışanın işe iade davası açması gibi bir ihtimalde, işverenin davanın kesinleşmesine dek çalışana ait gerekli bilgileri saklaması bu kapsamda değerlendirilebilecektir.

Nihayet açık rıza aranmaksızın veri işlenebilecek son hal ise, *ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması*dır. “Meşru menfaat” kavramı, hukuk düzeni içerisinde onay verilen her türlü hukuki, ekonomik veya kişisel yarardır⁷⁴⁷. Bu düzenlemede yer alan “veri sorumlusunun meşru menfaatleri” ifadesinin kapsamı ise, ancak uygulama ile belirlenebilecektir. Düzenlemenin dilinden de anlaşılacağı üzere, ilgili kişinin temel hak ve özgürlükleri ile veri sorumlusunun meşru menfaatleri arasında bir denge kurulması şarttır. Gerekçe’de yer alan örneğe göre,

“bir şirket sahibi, çalışanlarının temel hak ve özgürlüklerine zarar vermemek kaydıyla, onların terfileri, maaş zamları yahut sosyal haklarının düzenlenmesinde ya da işletmenin yeniden yapılandırılması

⁷⁴⁶ KÜZECİ, *Kişisel Verilerin Korunması*, s. 347- 348.

⁷⁴⁷ ÇEKİN, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu*, s. 72.

sürecinde görev ve rol dağıtımında esas alınmak üzere çalışanların kişisel verilerini işleyebilecektir.”

Bu örnekte veri sorumlusu olan işverenin meşru menfaatleri, şirketin terfi, maaş zammı ve sosyal hakların düzenlenmesi ile şirketin yeniden yapılandırılmasıdır. Ancak bir kez daha altı çizilmelidir ki, verileri işlenen ilgili kişilerin temel hak ve özgürlüklerinin zarar görmemesi, bu düzenlemenin uygulanmasının ana koşuludur. Burada önemle belirtilmelidir ki, Anayasa Hukukunda temel hak ve özgürlüklere zarar vermemek biçiminde bir ifade bulunmaz; bu ifadeye karşılık gelebilecek kavramlar, temel hak ve özgürlüklerin sınırlandırılması ve ihlali ifadeleridir.

Bir kez daha belirtilmelidir ki veri işlenmesi için KVKK'nın 5. maddesi doğrultusunda ana kural, ilgili kişinin açık rızasıdır. Yukarıda ele alınan diğer tüm haller mümkün olduğunca dar yorumlanmalıdır⁷⁴⁸.

Kişisel verilerin işlenmesine ilişkin şartlar büyük ölçüde 95/46/AT sayılı Direktif'in 7. maddesi ile benzerlik göstermektedir. Ancak GVKT bakımından önemle belirtilmelidir ki, veri işlemenin hukuka uygun olmasını sağlayan şartlar daha kapsamlı ve veri öznesinin haklarını koruyucu ibareler içermektedir. Söz gelimi veri öznesinin tarafı olduğu bir sözleşmenin yapılmasından önce “veri öznesinin talebi doğrultusunda adımlar atılması için” veri işlemenin gerekli olması aranmaktadır. KVKK'dan daha kapsamlı olan açık rıza olmaksızın bir diğer veri işleme şartı da veri öznesinin kişisel verilerinin korunmasını gerektiren menfaatleri veya temel hakları ve özgürlüklerinin bir kontrolör veya üçüncü bir kişi tarafından gözetilen meşru menfaatlere ağır basması haricinde, söz konusu menfaatler doğrultusunda işleme faaliyetinin gerekli olması halidir. Burada veri öznesinin çocuk olması hali özellikle belirtilmiştir. GVKT'de ayrıca veri işlemenin hukuka uygun hale gelmesinde rıza bakımından “çocuk” olan veri öznesi için özellikli bir düzenlemenin de mevcut olduğunu burada vurgulamak gerekir. GVKT'nin

⁷⁴⁸ Aynı yönde bkz. ŞİMŞEK, *Anayasa Hukukunda Kişisel Verilerin Korunması*, s. 208; Fikret İLKİZ, “Kişisel Verilerin Korunması ve Kanun Tasarısı”, *Güncel Hukuk*, 2009, S. 7- 67, s.16, ss. 12- 23; KÜZECİ, *Kişisel Verilerin Korunması*, s. 350.

“Bilgi toplumu hizmetleriyle ilgili olarak çocuğun rızasına uygulanan koşullar” başlıklı 8/1. maddesine göre; veri öznesinin kişisel verilerinin işlenmesine onay verdiği hallerde,

“doğrudan bir çocuğa bilgi toplumu hizmetleri sağlanması ile ilgili olarak, çocuğun en az 16 yaşında olması halinde, ilgili çocuğun kişisel verilerin işlenmesi hukuka uygundur. Çocuğun 16 yaşından küçük olması halinde, söz konusu işleme faaliyeti, ancak rızanın çocuk üzerinde velayet hakkı bulunan kişi tarafından verilmesi veya onaylanması halinde ve verildiği veya onaylandığı ölçüde hukuka uygundur.”

Ayrıca yine aynı fıkra da belirtildiği üzere, üye devletler yaş koşulunu 13 yaşından küçük olmamak kaydıyla kanunla değiştirerek ilgili amaçlara yönelik olarak daha küçük bir yaş belirleyebilecektir⁷⁴⁹.

Kişisel verilerin işlenmesi başlığı altında ele alınması gereken bir diğer önemli nokta da özel nitelikli kişisel verilerin işlenmesidir. KVKK’nın 6/1. maddesine göre, ırk, etnik köken, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançlar, kılık ve kıyafet, dernek, vakıf ya da sendika üyeliği, sağlık, cinsel hayat, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili veriler ile biyometrik⁷⁵⁰ ve genetik veriler özel nitelikli

⁷⁴⁹ GVKT’de yer alan çocuğun rızasına ilişkin özel hüküme dair daha detaylı bilgi için bkz. MACENAITE, KOSTA, “Consent for Processing Children’s Personal Data in the EU: Following in US Footsteps?”, ss. 146- 197.

⁷⁵⁰ Bu noktada güncel bir gelişme olarak, özel nitelikli kişisel verilerin bir türü olan biyometrik verilere ilişkin 27 Haziran 2019 tarihinde TBMM’de “*Sporda Şiddet ve Düzensizliğin Önlenmesine Dair Kanunda Değişiklik Yapılmasına Dair Kanun Teklifi*”ne değinmek yerinde olacaktır. Öncelikle belirtilmelidir ki anılan Teklif 20 maddeden oluşmaktadır. Ancak kişisel verilerin korunması bakımından sorunlu olan ilgili düzenlemesi 3/(d). maddesidir. Bu maddeye göre; “*Seyircilerin müsabaka ve seyir alanlarına girişlerinde biyometrik yöntemlerle kimlik doğrulama sisteminin kurulmasına ilgili federasyonun görüşü alınarak Bakanlıkça karar verilir. Buna ilişkin gerekli teknik donanım, spor tesisinin kullanım hakkına sahip kurum ve kuruluşlar tarafından tesis edilir.*” denmektedir. Burada konu olan biyometrik veriler, parmak izi, retina ya da iris taraması, avuç içi okuma, DNA bilgisi gibi kişiyi tanımlamada yüzde yüze yakın sonuç veren verilerdir. Belirtilmelidir ki bu verilerin işlenebilmesi için ana kural kişinin rızasıdır. Açık rıza dışında KVKK’nın 5/2. maddesine göre veri işlemenin “*kanunlarda açıkça öngörülmesi*” aranmaktadır. Bu düzenleme ayrıca aynı Kanun’un 4. maddesinde belirtilen genel ilkeleri doğrultusunda kişisel verilerin belirli, açık ve meşru amaçlar için, amaçla bağlantılı, sınırlı ve ölçülü olarak işlenmesini gerektirmektedir. Bu bağlamda ilk olarak belirtilmelidir ki ilgili düzenlemede söz konusu verileri kimin, hangi amaçla, ne kadar süreyle işlenebileceği belirtilmemektedir. Bu ise açıktır ki hukuka aykırıdır. Ayrıca bir spor müsabakasına gitmek için kişinin ve hatta 18 yaşından küçük çocukların dahi biyometrik verilerinin zorla

verilerdir. Aynı hükme göre, özel nitelikli kişisel verilerin de işlenmesi için ilgili kişinin açık rızası aranmaktadır. Ancak KVKK'nın birçok maddesinde görüldüğü üzere, burada da bu ana kurala istisna getirilerek açık rıza olmaksızın özel nitelikli verilerin işlenebileceği haller düzenlenmiştir. Bu hükme göre, ırk, etnik köken, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançlar, kılık ve kıyafet, dernek, vakıf ya da sendika üyeliği, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili veriler ile biyometrik ve genetik veriler, başka kanunlarda öngörülen hallerde ilgili kişinin açık rızası olmaksızın işlenebilecektir. Sağlık ve cinsel hayata ilişkin veriler ise, kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amaçları ile sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgili kişinin açık rızası aranmaksızın işlenebilecektir.

Burada dikkat çekici bir düzenleme mevcuttur. KVKK'nın 5. maddesinde yer alan olağan veri işlemede, açık rıza aranmaksızın veri işlenebilmesi için *“Kanunlarda açıkça öngörülme”* aranmaktadır. Oysa 6/3. maddede özel nitelikli kişisel verilerin açık rıza aranmaksızın işlenebileceği halleri belirtirken, ırk, etnik köken, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançlar, kılık ve kıyafet, dernek, vakıf ya da sendika üyeliği, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili veriler ile biyometrik ve genetik verilerin *“kanunlarda öngörülen hallerde ilgili kişinin açık rızası aranmaksızın”* işlenebileceğini hüküm altına almıştır. Olağan verilerin işlenmesi için aranan *“kanunun açıkça öngörmesi”* düzenlemesi, özel nitelikli ve Gerekçe'de de belirtildiği üzere,

alınması ve bunun müsabakayı izlemek için şart koşulması, kişisel verilerin işlenmesinde temel şartlara, KVKK'ya ve GVKT'ye aykırı ve keyfi bir durum oluşturacaktır. Üstelik her gün gelişen teknoloji neticesinde yeni biyometrik yöntemlerin de ortaya çıkabileceği düşünüldüğünde, anılan Teklif ile söz konusu Kanun'un kapsamı ve yaratacağı tahribat gücünün belirsiz bir hale geleceği neredeyse mutlaklıktır. Öte yandan biyometrik verilere ilişkin tüm yetkinin Bakanlık'a verilmesi de idarenin bu verileri keyfi kullanımı riskini beraberinde getirmektedir. Özellikle Mart 2019'daki Yerel Seçim'de İBB Seçimi'nin sonuçlarına Yüksek Seçim Kurulu nezdinde itiraz esnasında, kısıtlı olan seçmenlerin sağlık verilerinin bir siyasi parti tarafından elde edilmiş olduğu ve bunun TBMM'de açıkça dile getirildiği düşünüldüğünde durumun vehameti daha da belirgin bir şekilde görülebilecektir. Dolayısıyla söz konusu Teklif'in kanunlaşması halinde gerek Anayasa ve 6698 Sayılı KVKK'ya, gerekse İHAM ve GVKT'ye aykırı bir düzenleme ortaya çıkacağından iptali de kaçınılmaz olacaktır/ olmalıdır.

başkaları tarafından öğrenildiği takdirde ilgili kişinin mağdur olabilmesine veya ayrımcılığa maruz kalabilmesine neden olabilecek nitelikte olan hassas veriler⁷⁵¹ bakımından yalnızca “*kanunun öngörmesi*” biçimine dönüşmüştür. Oldukça hassas nitelikteki sağlık ve cinsel hayata ilişkin verilerin işlenmesi bakımından ise “*kanunun öngörmesi*” hali dahi aranmamaktadır. Açıktır ki bu durum, özel niteliği olan kişisel verilerin doğaları gereği daha yüksek bir koruma gerektirmelerine karşın korumalarını zayıflatmaktadır⁷⁵². Sağlık ve cinsel hayata ilişkin verilerin işlenmesinin Kanun harici yönetmelik, tüzük gibi düzenleyici işlemlerle öngörülmesi mümkün olabilecek midir? Bu sorunun yanıtı, Anayasa’nın 20/3. maddesinin açık lafzı ve 13. maddede yer alan temel hak ve özgürlüklerin ancak kanunla sınırlandırılabilmesi ilkesi gereği olumsuz olacaktır.

Özel nitelikli kişisel verilerin işlenme şartları başlıklı 6. maddenin son fıkrasında ise, Kişisel Verileri Koruma Kurulu tarafından ayrıca belirlenen yeterli önlemlerin alınması, hassas verilerin işlenmesi bakımından aranan bir diğer şart olarak karşımıza çıkmaktadır. Bu doğrultuda, Kurul’un 31 Ocak 2018 tarih ve 2018/10 No’lu kararında “*Özel Nitelikli Kişisel Veri İşleyen Veri Sorumluları Tarafından Alınması Gereken Yeterli Önlemler*” belirlenmiştir⁷⁵³. Bu önlemler kapsamında veri sorumluları tarafından

⁷⁵¹ DÜLGER, “Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması”, *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi*, s. 109.

⁷⁵² KÜZECİ, *Kişisel Verilerin Korunması*, s. 353.

⁷⁵³ “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. Karara göre; “Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler:

1- Özel nitelikli kişisel verilerin güvenliğine yönelik sistemli, kuralları net bir şekilde belli, yönetilebilir ve sürdürülebilir ayrı bir politika ve prosedürün belirlenmesi,

2- Özel nitelikli kişisel verilerin işlenmesi süreçlerinde yer alan çalışanlara yönelik,

a) Kanun ve buna bağlı yönetmelikler ile özel nitelikli kişisel veri güvenliği konularında düzenli olarak eğitimler verilmesi,

b) Gizlilik sözleşmelerinin yapılması,

c) Verilere erişim yetkisine sahip kullanıcıların, yetki kapsamlarının ve sürelerinin net olarak tanımlanması,

ç) Periyodik olarak yetki kontrollerinin gerçekleştirilmesi,

d) Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkilerinin derhal kaldırılması. Bu kapsamda, veri sorumlusu tarafından kendisine tahsis edilen envanterin iade alınması,

3- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, elektronik ortam ise

özel nitelikteki kişisel verilerin işlenmesi için politikaların belirlenmesi, verilerin işleme süreçlerinde yer alan çalışanlara yönelik kural ve önlemler, verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamların elektronik veya fiziksel ortam olmasına göre değişiklik gösteren kural ve önlemler ile bu verilerin aktarılması sırasında dikkate alınması gereken hususlara ilişkin bir dizi detaylı düzenleme yer almaktadır.

Özel nitelikli kişisel veriler bakımından akla gelebilecek bir başlık da T.C. Kimlik Numaraları olabilecektir. Ulusal kimlik numaraları her ne kadar hassas veriler arasında sayılmasa da hem KVKK'nın esas aldığı 95/46/AT sayılı Direktif'te hem de GVKT'de konuya ilişkin ayrı hüküm bulunmaktadır⁷⁵⁴. GVKT bu konuda üye devletlere işlenmeye özgü koşulları belirleme imkânı tanımaktadır. Ayrıca ulusal kimlik numarası veya başka bir belirtecin ancak Tüzük uyarınca veri öznesinin hakları ve özgürlüklerine ilişkin uygun

-
- a) Verilerin kriptografik yöntemler kullanılarak muhafaza edilmesi,
 - b) Kriptografik anahtarların güvenli ve farklı ortamlarda tutulması,
 - c) Veriler üzerinde gerçekleştirilen tüm hareketlerin işlem kayıtlarının güvenli olarak loglanması,
 - ç) Verilerin bulunduğu ortamlara ait güvenlik güncellemelerinin sürekli takip edilmesi, gerekli güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,
 - d) Verilere bir yazılım aracılığı ile erişiliyorsa bu yazılıma ait kullanıcı yetkilendirmelerinin yapılması, bu yazılımların güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,
 - e) Verilere uzaktan erişim gerekiyorsa en az iki kademeli kimlik doğrulama sisteminin sağlanması,
- 4- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, fiziksel ortam ise
- a) Özel nitelikli kişisel verilerin bulunduğu ortamın niteliğine göre yeterli güvenlik önlemlerinin (elektrik kaçağı, yangın, su baskını, hırsızlık vb. durumlara karşı) alındığından emin olunması,
 - b) Bu ortamların fiziksel güvenliğinin sağlanarak yetkisiz giriş çıkışların engellenmesi,
- 5- Özel nitelikli kişisel veriler aktarılacaksa
- a) Verilerin e-posta yoluyla aktarılması gerekiyorsa şifreli olarak kurumsal e-posta adresiyle veya Kayıtlı Elektronik Posta (KEP) hesabı kullanılarak aktarılması,
 - b) Taşınabilir Bellek, CD, DVD gibi ortamlar yoluyla aktarılması gerekiyorsa kriptografik yöntemlerle şifrelenmesi ve kriptografik anahtarın farklı ortamda tutulması,
 - c) Farklı fiziksel ortamlardaki sunucular arasında aktarma gerçekleştiriliyorsa, sunucular arasında VPN kurularak veya sFTP yöntemiyle veri aktarımının gerçekleştirilmesi,
 - ç) Verilerin kağıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemlerin alınması ve evrakın "gizlilik dereceli belgeler" formatında gönderilmesi gerekir.
- 6- Yukarıda belirtilen önlemlerin yanı sıra Kişisel Verileri Koruma Kurumunun internet sitesinde yayımlanan Kişisel Veri Güvenliği Rehberinde belirtilen uygun güvenlik düzeyini temin etmeye yönelik teknik ve idari tedbirler de dikkate alınmalıdır." biçimindedir.

⁷⁵⁴ 95/46/AT sayılı Direktif md. 8/7; GVKT md. 87.

güvenceler çerçevesinde kullanılabileceğini belirtmektedir. Durum Avrupa veri koruma hukuku bakımından böyle olmakla birlikte KVKK'da T.C. Kimlik Numaralarına dair bir hüküm bulunmamaktadır. Oysa uygulamada neredeyse her alanda, ilgili ilgisiz birçok işlemin gerçekleşmesi için bu numaraların işlenmesi durumu mevcuttur. Söz gelimi bir internet alışverişi esnasında, bu alışverişin neticesinde ürünün eve teslimi sırasında, faturalandırma işlemlerinde, hastane işlemlerinde, bankacılık işlemlerinde, internet üzerinden yapılan bağışlarda vb. birçok alanda işlenen kimlik numaralarımıza dayanarak oluşturulabilecek profillerin ne denli detaylı olabileceğini düşünürsek, Kanun kapsamında ayrı bir düzenleme yapılması oldukça önem taşımaktadır⁷⁵⁵.

4. Kişisel Verilerin Aktarımı

KVKK'nın "*Tanımlar*" başlıklı 3. maddesinde yer aldığı üzere, kişisel verilerin aktarılması da bir veri işleme biçimidir. Kanun bu veri işleme yöntemini, işlemeye ilişkin genel kuralları içeren 5. ve 6. maddelerde ele almak yerine, kişisel verilerin yurtiçinde üçüncü kişilere aktarılmasını 8. maddede, kişisel verilerin yurtdışına aktarılmasını 9. Maddede münferit olarak düzenlemektedir.

a) Yurt İçinde Üçüncü Kişilere Aktarılması

KVKK'nın "*Kişisel verilerin aktarılması*" başlıklı 8. maddede bulunan verilerin aktarımları, Gerekçe'de de belirtildiği üzere 9. maddede yurtdışına veri aktarımı düzenlendiğinden, kural olarak verinin yurtiçinde üçüncü kişiye aktarımını içermektedir. Bu hüküm, veri işlemeye ilişkin genel kurallardan farklılık göstermemektedir. Daha açık bir söyleyişle, veri aktarımı tıpkı veri işlemede olduğu gibi açık rıza olmaksızın gerçekleştirilemez. Ancak kişisel verilerin işleme şartlarında açık rıza aranmaksızın işleme yapılabilecek haller (md. 5/2) ile özel nitelikli kişisel verilerin işlenmesinde açık rıza aranmaksızın işleme yapılan hallerde kişisel verilerin aktarılması mümkün

⁷⁵⁵ KÜZECİ, *Kişisel Verilerin Korunması*, s. 355.

olabilecektir (md. 8/2). Bu düzenlemeye göre ayrıca, veri aktarımına dair başka kanunlardaki hükümler saklı tutulmuştur.

b) Yurtdışına Aktarılması

KVKK'nın yer bakımından uygulanmasına ilişkin spesifik bir hükmün bulunmadığı daha önce dile getirilmişti. Bu bağlamda yeniden belirtilmelidir ki, Kanun'un uygulaması, mülkiyet prensibi kapsamında, Türk hukukunun geçerli olduğu bir yerde kişisel verilerin işlenmesi halinde söz konusu olacaktır⁷⁵⁶. Bu kapsamda Kanun'un koruması yalnızca bu alanla sınırlı olacaktır.

Günümüzde verinin giderek artan değeri ve sınırsız dolaşımı sebebiyle ulusal düzenlemelerin uygulama alanı oldukça sınırlı kalmaktadır. Bu sebeple ulusal düzenlemeler verinin uluslararası dolaşımına ilişkin özel düzenlemeler içermektedir. Fakat doğaldır ki bu düzenlemeler verinin yurtdışındaki hukuka aykırı kullanımları için bir düzenleme değildir ve verinin yurtdışına aktarımı öncesi bazı önlemlerin alınmasını içermektedirler. KVKK'nın "*Kişisel verilerin yurtdışına aktarılması*" başlığını taşıyan 9. maddesi de bu kapsamdadır. Anılan madde ilk planda kural olarak kişisel verilerin ilgilinin "açık rıza"sı olmaksızın yurtdışına aktarılamayacağını belirtmektedir. Daha önce belirtildiği üzere, belirli, bilgilendirmeye dayanan ve özgür irade ile açıklanan bir bildirim anlamına gelen açık rızanın yurtdışına aktarım amaçlı alınabilmesi için ise, verinin yurtdışına aktarımının yapılacağını söylenmesi yeterli olmayıp hangi ülkeye ve ne amaçla aktarım yapılacağını bildirilmesi yerinde olacaktır⁷⁵⁷.

Yurtdışına veri aktarımı da yurtiçinde aktarımda olduğu gibi, kişisel verilerin işleme şartlarında açık rıza aranmaksızın işleme yapılabilecek haller (md. 5/2) ile özel nitelikli kişisel verilerin işlenmesinde açık rıza aranmaksızın işleme yapılan hallerde kişisel verilerin yurtdışına aktarılması mümkün olabilecektir. Daha açık bir söyleyişle

⁷⁵⁶ AYDIN, "Ceza Kanunlarının Yer Yönünden Uygulanması", s. 133.

⁷⁵⁷ Aynı yönde bkz. ÇEKİN, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu*, s. 85.

Kanun, kişisel verilerin işlenmesi ile bu verilerin yurt dışına aktarılması bakımından aynı şartları aramaktadır. Yurtdışına aktarım bakımından bunun dışında ek tedbirlerin alınması gereği ortaya konmaktadır. Bu düzenleme bakımından ilgili kişinin rızası aranmaksızın yurtdışına veri aktarımı için esas olan yukarıdaki şartlarla birlikte, kişisel verinin aktarılacağı yabancı ülkede;

- Yeterli korumanın bulunması

ya da

- Yeterli korumanın bulunmaması durumunda Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurul'un izninin bulunması

şartlarından birinin gerçekleşmesi gereğidir. Kurul'un yabancı bir ülkeye veri aktarımı için gereken, ülkenin yeterli korumaya sahip olup olmadığına ve yeterli koruma olmayan hallerde aktarım için izin verip vermeyeceğine karar verirken bazı hususları dikkate almak zorundadır. Buna göre Kişisel Verilerin Korunması Kurulu;

- Türkiye'nin taraf olduğu uluslararası sözleşmeler,
- Aktarımın yapılması planlanan ülke ile karşılıklılık durumu,
- Tüm somut olaylar nezdinde verinin niteliği, işlenme amacı ve süresini,
- Aktarımın yapılması planlanan ülkenin konuya dair mevzuat ve uygulamasını,
- Aktarımın yapılması planlanan ülkedeki veri sorumlusunun taahhüt ettiği önlemleri,

dikkate alarak ve ihtiyaç duyarsa ilgili kurum ve kuruluşların görüşünü alarak yurtdışına veri aktarımına izin verecek ya da vermeyecektir. Kişisel Verileri Koruma Kurulu, bu doğrultuda yurtdışına veri aktarımında veri sorumlusunun taahhüt edeceği önlemler için hazırlanacak taahhütnamede yer alacak asgari unsurları belirlemiştir. Buna göre, “Veri Sorumlusundan Veri Sorumlusuna Aktarım” başlıklı ilk düzenleme, “*Veri Aktaran Veri Sorumlusunun Yükümlülükleri*”, “*Veri Alıcısının Yükümlülükleri*”, “*Ortak Hükümler*”

ve taahhütnamenin matbu halini içermektedir. “Veri Sorumlusundan Veri İşleyene Aktarım” başlıklı diğer düzenleme de “Veri sorumlusunun yükümlülükleri”, “Veri işleyenin yükümlülükleri”, “Ortak Hükümler” ve taahhütnamenin matbu halini içermektedir⁷⁵⁸.

Daha evvel ele alındığı üzere Adalet Divanı, bir ülkenin yeterli korumaya sahip olup olmadığına karar verilirken, üçüncü bir ülkenin, AB hukuk düzeninde garanti edilenle koruma ile aynı seviyede bir koruma sağlamasının şart olmadığını belirtmiştir. Üçüncü ülke burada yalnızca, kendi iç hukuku veya uluslararası taahhütleri gereği AB sathında güvence altına alınmış olan temel hak ve özgürlüklerin korunmasını sağlamalıdır⁷⁵⁹.

Kişisel verilerin yurtdışına aktarılması bakımından üzerinde durulması gereken bir diğer husus da Kanun’un 9/5. maddesinde düzenlenen “*Uluslararası sözleşme hükümleri saklı kalmak kaydıyla Türkiye’nin veya ilgili kişinin menfaatinin ciddi bir şekilde zarar göreceği durumlar*”dır. Böyle bir durumun söz konusu olduğu hallerde kişisel veriler ancak ilgili kamu kurum veya kuruluşunun görüşü alınarak Kurul’un izni ile yurt dışına aktarılabilir. Söz konusu düzenleme TBMM’ye sevk edilen ve sonrasında Adalet Komisyonu’nda görüşülen metinde yer almamakla birlikte, Genel Kurul’a sunulan bir önerge ile kabul edilmiştir. Düzenlemenin diline bakıldığında, “*Türkiye’nin veya ilgili kişinin menfaatinin ciddi bir şekilde zarar göreceği durumlar*” ile ne kastedildiği belirsizdir. Ciddi bir şekilde zarar görmek ifadesinin içerdiği anlama dair Gerekçe’de de belirleyici bir ifade yer almamaktadır. Ayrıca görüşü alınacak ilgili kamu kurum ve kuruluşu ifadesindeki kurum ve kuruluşların her somut olay bazında belirlenmesi güçlük yaratabilecektir⁷⁶⁰. Her ne kadar Gerekçe’de “Dışişleri Bakanlığı ya da ilgili kamu kurum ve kuruluşları” denilerek yurtdışına veri aktarımında Türkiye’nin

⁷⁵⁸ Kişisel Verileri Koruma Kurulu, “Yurtdışına Veri Aktarımında Veri Sorumlularınca Hazırlanacak Taahhütnamede Yer Alacak Asgari Unsurlar”, <https://www.kvkk.gov.tr/Icerik/2053/Yurtdisina-Aktarim> , E.T. 25.04.2019.

⁷⁵⁹ Case C-362/14 *Maximillian Schrems v. Data Protection Commissioner*, 06.11.2015, Par. 73, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62014CJ0362&from=FR> , E.T. 22.04.2019.

⁷⁶⁰ KÜZECİ, *Kişisel Verilerin Korunması*, s. 357.

ya da ilgili kişinin menfaatinin ciddi bir şekilde zarar göreceği durumlarda görüşü alınacak Dışişleri Bakanlığı değişmez aktörlerden biri haline gelse de diğer kurum ve kuruluşlar belirsizliğini korumaktadır.

Yurtdışına veri aktarımına ilişkin olarak belirtilebilecek son husus, KVKK'nın 9/6. maddesine göre kişisel verilerin yurtdışına aktarılmasına dair diğer kanunlarda yer alan hükümlerin saklı olmasıdır. Gerekçe'ye baktığımızda örnek olarak 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun'un adı geçerken, uluslararası bilgi değişimi konusunda Malî Suçları Araştırma Kurulu Başkanı'na yetki veren 12. ve 19. maddelerinin öncelikli olarak uygulanacağı belirtilmiştir. Ancak anılan maddeler 2 Nisan 2018 tarih ve 703 sayılı KHK'nın 15. maddesi ile yürürlükten kaldırılmıştır.

Sonuç olarak KVKK bakımından yurtdışına veri aktarımı iki basamaklı bir denetimi içermektedir. Bu bakımdan ilk olarak Kanun'un 5. ve 6. maddelerinde düzenlenen şartlar dikkate alınmalıdır. Şayet bu şartlara uygunluk söz konusu ise, 9. maddede düzenlenen ve verilerin yurtdışına aktarımı için öngörülen şartların gerçekleştirilip gerçekleştirilmediği incelenmelidir.

5. Veri Öznesinin Hakları (KVKK md. 3- İlgili Kişi)

Kişisel verilerin korunması, veri işlemenin hukuka uygun halde olması ile gerçekleşmektedir. Hukuka uygun veri işleme de Kanun'da yer alan veri işleme şartlarının ilgili kişi tarafından denetlenebilmesi ile mümkün olabilmektedir. İşte ilgili kişinin veri işlemeyi denetleyebilmesi imkânı, bu kişiye tanınan haklar sayesinde mümkün olabilmektedir. KVKK'nın 11. maddesinde ilgili kişinin hakları yer almaktadır. Bu bağlamda 4. İle 9. maddeler arasında yer alan kişisel verilerin işleme şartları, 11. maddede yer alan ilgili kişinin hakları ile oldukça ilişkilidir.

Kanun'un 11. maddesine göre ilgili kişinin ilk olarak *“Kişisel veri işlenip işlenmediğini öğrenme hakkı”* bulunmaktadır. Bu bağlamda mantık çerçevesinde söz konusu hakkın, kişinin kendisine ilişkin veri işlenip işlenmediğini öğrenmesine ilişkin olduğu sonucuna varmak gerekecektir. Aksi durumda herhangi bir ilgili kişi, üçüncü bir

kişi hakkında da veri işlenip işlenmeyeceğini öğrenebilecektir, ki bu durum doğaldır ki, hakkın koruma kapsamı dışındadır. Ayrıca yine hükmün lafzından anlaşılmaktadır ki veri sorumlusu ilgili kişi hakkında veri işlediğini söylemesinin yanında, şayet işlememişse bunu da açık bir şekilde belirtmelidir. Veri sorumlusu, ilgili kişiye verisinin işlenip işlenmediğini bildirirken somut olayın koşullarına göre sözlü, yazılı veya elektronik bildirim yapabilecektir⁷⁶¹. GVKT'nin 15. maddesi, “*Veri öznesinin erişim hakkı*” başlığı altında kendisi ile ilgili kişisel verilerin işlenip işlenmediğini veri denetleyicisinden teyit etme hakkını düzenlemektedir.

İlgili kişinin sahip olduğu bir diğer hak da “*İşlenen kişisel verilere ilişkin bilgi talep etme hakkı*”dır. Bu hak, bir önce ele alınan hakkın adeta devamı niteliğindedir; çünkü kişisel verisinin işlenip işlenmediğini veri sorumlusundan öğrenen ilgili kişi, şayet verisi işlenmişse bu defa işlenen verilerine ilişkin olarak bilgi talep edebilecektir. Burada işlenen verinin kendisinin ilgili kişi ile paylaşılması gerektiği açıktır; çünkü yukarıda belirtildiği üzere, ilgili kişinin hakları bu kişiye hukuka uygun veri işlenmesi hususunda yardımcı olmakta ve kişi, veri işlemeyi bu biçimde denetleyebilmektedir. Açıktır ki kişi, içeriğini öğrenebildiği verinin düzeltilmesini, silinmesini, yok edilmesini ya da anonim hale getirilmesini isteyebilecektir. Bir önceki paragrafta bahis konusu olan GVKT'nin 15. maddesi ayrıca, kendisine dair işleme faaliyeti olması halinde, kişisel verilere erişim hakkına sahip olmaktadır. Tüzük'te ayrıca veri öznesinin kişisel verilerine erişim hakkı ile ilişkili olarak değerlendirilebilecek bir diğer hakkı da 20. maddede düzenlenen “*Veri taşınabilirliği hakkı*”dır. Buna göre veri öznesi, kendisi ile ilgili olarak bir veri denetleyicisine sağlamış olduğu kişisel verileri, yapılandırılmış, yaygın olarak kullanılan ve makine tarafından okunabilecek bir formatta alma hakkına da sahiptir. Hatta bu bağlamda aldığı verileri kişisel verilerin sağlandığı denetleyicinin herhangi bir engellemesi olmaksızın başka bir denetleyiciye de iletme hakkına sahiptir⁷⁶².

⁷⁶¹ Bildirimin sözlü, yazılı veya elektronik yapılabilmesi hususunda bkz. ÇEKİN, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu*, s. 90.

⁷⁶² TIKKINEN-PIRI, ROHUNEN, MARKKULA, “EU General Data Protection Regulation: Changes and implications for personal data collecting companies”, s. 14.

İlgili kiři ayrıca, “*Kişisel verilerin işleme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme hakkı*”na da sahiptir. Hukuka uygun veri işlemenin en temel kurallarından biri de belirtildiğı üzere, belirli, açık ve meşru amaçlar için veri işlemedir. Bu ilke ile doğrudan ilişkili olan bu hakkın amacına bakıldığında ilgili kişinin, veri işlemenin meşru amaçlar doğrultusunda gerçekleştirilip gerçekleştirilmediğini denetlemesine yardımcı olmak için tanındığı aşıkardır. KVKK’dan farklı olarak GVKT, veri öznesinin haklarını düzenlerken “*Veri sahibinden kişisel verilerin toplandığı hallerde sağlanacak bilgiler*” başlıklı 13. maddesinde kontrolörün, kontrolörün temsilcisinin ve veri koruma görevlisinin kimlik ve irtibat bilgilerinin sağlanacağından söz etmektedir. Ayrıca Kanun ile benzer şekilde, veri öznesine kişisel verilerin planlanan işleme amaçlarının da bildirilmesi gereğini hem bu madde hem de “Veri öznesinin erişim hakkı” başlıklı 15. madde bakımından hüküm altına alınmıştır.

Bir diğer ilgili kişinin sahip olduğu hak ise, “*Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme hakkı*”dır. Bu hak ile ilgili kiři, KVKK kapsamında yurt içinde ve yurt dışında üçüncü kişilere veri aktarımı gerçekleştirildiğinde söz konusu kişileri bilecek ve veri sorumlusunun hukuka uygun bir aktarım için üzerine düşenleri yapıp yapmadığını denetleyebilecektir. Ayrıca verilerinin aktarıldığı üçüncü kişileri bile ilgili kiři, bu kişilere de taleplerini ileri sürmeye devam edebilecektir. Bu hükme benzer bir düzenleme GVKT’nin 13. maddesi bağlamında da bulunmaktadır. Ancak anılan madde Kanun’a kıyasla oldukça detaylıdır. Buna göre kontrolör, kişisel verileri üçüncü bir ülke veya uluslararası kuruluşa aktarmayı amaçlıyorsa bu husus, aktarıma ilişkin olarak Komisyon tarafından bir yeterlilik kararı verilip verilmediğı ya da belli bazı aktarımlar olması halinde uygun güvencelerin neler olduğuna ilişkin atıf ve bu güvencelerin bir nüshasının elde edilme yolları veya bunların nereden sağlandığı bilgilerini de veri öznesi ile paylaşmalıdır.

Veri işlenip işlenmediğini öğrenme ve işlenen veriler bakımından bilgi talep etme hakları ile yakından ilişkili olan bir diğer hak ise, “*Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme hakkı*”dır. GVKT’nin 16. maddesi de “*Düzeltilme Hakkı*”nı ele almaktadır. Bu hakkın içeriğı ise, veri öznesinin

kendisi ile ilgili doğru olmayan kişisel verilerin düzeltilmesini isteme ve eksik kişisel verilerini tamamlama haklarından oluşmaktadır. Bu bakımdan KVKK'nın 11/(d). maddesi bakımından eksik veya yanlış işlenen veriler için ilgili kişinin, tamamlama ve düzeltme hakları bulunduğunu kabul etmek daha uygun olacaktır⁷⁶³. Düzeltme hakkının kullanılması için talebin belli bir şarta uyularak gerçekleştirilmesini gerektirmez; yalnızca eksik tamamlama ya da yanlışın düzeltilmesinin anlaşılması, yapılacak bildirim bakımından yeterlidir. Bunlar dışında belirtilmelidir ki söz konusu hak, temel esaslardan olan, kişisel verilerin doğru ve gerektiğinde güncel olması ile de örtüşmektedir.

İlgili kişinin bir diğer hakkı, KVKK'nın 7. maddesi bağlamında, *“kişisel verilerin silinmesini veya yok edilmesini isteme hakları”*dır. Bu maddeye göre, kişisel verilerin işlenmesini gerektiren sebepler ortadan kalkmış ise, veriler re'sen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinebilecek, yok edilebilecek veya anonim hâle getirilebilecektir. Ayrıca bu maddenin son fıkrasında belirtildiği üzere, kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin usul ve esaslar, Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'te düzenlenmektedir. Bu düzenlemeye göre kişisel verilerin silinmesi, *“kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.”*⁷⁶⁴. Kişisel verilerin yok edilmesinden anlaşılması gereken ise, *“kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi”* olmalıdır⁷⁶⁵. Son olarak kişisel verilerin anonim hale getirilmesi ise, *“kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek”* biçime dönüştürülmesidir⁷⁶⁶. GVKT'nin *“Veri sahibinin erişim hakkı”* başlıklı 15. maddesi bakımından ise, KVKK'dan daha kapsamlı şekilde, veri öznesinin hem kendisi

⁷⁶³ Aynı yönde bkz. ÇEKİN, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu*, s. 91.

⁷⁶⁴ Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik, md. 8.

⁷⁶⁵ Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik, md. 9.

⁷⁶⁶ Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik, md. 10.

hakkındaki kişisel verilerin düzeltilmesi ve silinmesini veri denetleyicisinden isteme hakları mevcuttur; hem de veri işlenmesinin kısıtlanmasını talep etme⁷⁶⁷ ve işleme faaliyetine itiraz hakları mevcuttur.

İlgili kişinin sahip olduğu bir başka hak da daha önce sayılan haklarla oldukça ilişkili olan “*Kişisel Verilerin Düzeltilmesi ile silinmesini veya yok edilmesini isteme hakları bağlamında yapılan işlemlerin, veri aktarımı yapılan üçüncü kişilere bildirilmesi hakkı*”dır. Bu hak bakımından belirtilmelidir ki, üçüncü kişilere veri aktarımı gerçekleştirildiği hallerde veri sorumlusu, ilgili kişinin talebi üzerine veriyi düzelttiği, sildiği ya da yok ettiği hallerde bu durumu üçüncü kişiye de beildirmeli ve üçüncü kişi de veriye bu işlemlerden gerekeni yapmalıdır. Ancak görüldüğü üzere burada yalnızca, veri sorumlusunun üçüncü kişiye “bildirim hakkı” düzenlenmektedir. Bu bakımdan verinin aktarıldığı üçüncü kişi şayet aynı zamanda veri sorumlusu değilse, ilgili kişi burada kendi haklarını ileri süremeyecektir. Dolayısıyla bu ihtimal bakımından Kanun’da bir eksiklik söz konusudur⁷⁶⁸.

İlgili kişinin bir diğer hakkı ise, “*İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme hakkı*”dır. Bu düzenleme bakımından öncelikle “profilleme (profiling)” kavramının içeriği belirlenmelidir. GVKT’nin 4/4. maddesine göre profilleme ya da profil çıkarma, “bir gerçek kişinin işteki performansı, ekonomik durumu, sağlığı, kişisel tercihleri, ilgi alanları, güvenilirliği, davranışları, konumu veya

⁷⁶⁷ GVKT md. 18’e göre;

- Veri öznesi kişisel verilerin doğruluğuna itiraz etmişse,
- Veri öznesi, hukuka aykırı bir veri işlemenin mevcut olması halinde kişisel verilerin silinmesine itiraz etmiş ve yerine verilerin kullanımının kısıtlanmasını talep etmişse,
- Veri denetleyicisinin işleme amaçları doğrultusunda artık kişisel verilere ihtiyaç duymadığı ve fakat veri öznesinin bazı iddialarda bulunması durumunda bu iddiaların incelenmesi veya savunulması amacıyla söz konusu verilere ihtiyaç duyuluyorsa,
- Veri öznesinin işleme faaliyetine itiraz etmesi halinde, veri denetleyicisinin meşru gerekçelerinin veri öznesinin meşru gerekçelerine ağır basıp basmadığı doğrulanana kadar,

Veri işleme faaliyetinin kısıtlanması istenebilecektir.

⁷⁶⁸ Aynı yönde bkz. ÇEKİN, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu*, s. 96- 97.

hareketlerine ilişkin hususların analiz edilmesi veya tahmin edilmesi başta olmak üzere söz konusu gerçek kişiye ilişkin belirli kişisel özelliklerin değerlendirilmesi için kişisel verilerin kullanımını ihtiva eden her türlü otomatik kişisel veri işleme biçimidir.” Söz gelimi bir veri komisyoncusu, müşterileri adına veya kendi amaçları doğrultusunda farklı kamusal ve özel kaynaklardan veri toplayabilir. Veri komisyoncusu bu kapsamda, bireyler üzerinde profiller geliştirmek için derler ve bunları kategorilere ayırarak yerleştirir. Bu bilgileri mal ve hizmetlerinin hedeflenmesini geliştirmek isteyen şirketlere satabilir (Kişinin bir arama motorunda bilgisayar aradığı bilgisinin işlenmesi ve analizi sonucu o kişiye bilgisayar kılıfı öneren bir sistemin varlığı gibi). Veri komisyoncusu, bir kişiyi kendi çıkarlarına göre belirli bir kategoriye yerleştirerek profil oluşturma işlemini gerçekleştirir⁷⁶⁹. İşte bu durumda şayet veri komisyoncusunun analizi gerçekleştirmesi ve kategorilere ayırması gibi işlemler bir insanın katkısı ya da etkisi olmaksızın münhasıran otomatik sistemler aracılığı ile gerçekleştiriliyorsa, KVKK’nın 11/(g). maddesi uyarınca ilgili kişinin kendisi hakkında aleyhe bir sonuç ortaya çıkması halinde buna itiraz hakkı bulunmaktadır. KVKK’da her ne kadar kısıtlı bir alan bakımından itiraz hakkı düzenlenmiş olsa da GVKT özelinde itiraz hakkı daha geniş ve özellikli bir alana dokunmaktadır. Tüzük’ün 21. maddesine göre veri öznesinin itiraz hakkının içeriği;

- Kamu yararına gerçekleştirilen bir görevin yerine getirilmesi veya veri denetleyicisine verilen resmi bir yetkinin uygulanması hususunda işleme faaliyetinin gerekli olması

veya

- Özellikle veri öznesinin çocuk olduğu hallerde, veri öznesinin kişisel verilerin korunmasını gerektiren menfaatleri veya temel hakları ve özgürlüklerinin bir denetleyici veya üçüncü bir kişi tarafından gözetilen meşru menfaatlere ağır

⁷⁶⁹ Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP 251rev.01, 06.02.2018, s. 8, https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49826 , E.T. 28.04.2019.

basması haricinde, söz konusu menfaatler doğrultusunda işleme faaliyetinin gerekli olması

hallerine dayalı olarak kendisi ile ilgili, profil çıkarma da dahil olmak üzere, kişisel verilerin işlenmesine herhangi bir zamanda itiraz edebileceği biçimindedir. İtiraz hakkının işletilebileceği bir diğer durum da, veri öznesinin kişisel verilerinin doğrudan pazarlama amacı ile işlenmesine herhangi bir zamanda itiraz edebilmesi halidir⁷⁷⁰.

KVKK'nın 11. maddesi bağlamında ilgili kişinin sahip olduğu son hak ise, *“Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme hakkı”*dır. Bu hak kişiye tazminat talebi sağlamaktadır. Buna göre, kişisel verilerin hukuka aykırı işlenmesi kişinin maddi ve manevi zarara uğramasına sebep olabilecektir. Bu noktada kişi, Türk Medeni Kanun'u Genel Hükümler

⁷⁷⁰ Her ne kadar KVKK'da pazarlama amacı ile işlenen verilere itiraz hakkı gibi bir müessese bulunmasa da Kişisel Verilerin Korunması Kurulu 16 Ekim 2018 tarihinde *“Veri sorumluları ve veri işleyenler tarafından ilgili kişilerin e-posta adreslerine veya SMS ya da çağrı ile cep telefonlarına reklam bildirimleri/aramaları yönlendirilmesinin önüne geçilmesini teminen ilke kararı”* almıştır. Bu karara göre, *“...İlgili kişilerin rızalarını almadan veya ...işleme şartlarını sağlamadan, telefon numaralarına SMS göndermek, arama yapmak veya e-posta adreslerine posta göndermek suretiyle reklam içerikli ileti yönlendiren veri sorumluları ile veri sorumluları adına reklam içerikli mesaj/e-posta göndermek veya arama yapmak amacıyla ilgili kişilerin açık rızaları bulunmaksızın bu verileri kullanan veri işleyenlerin söz konusu veri işleme faaliyetlerini... derhal durdurması gerektiği,*

- *...veri sorumlusunun (Kanun'un ilgili hükümleri bağlamında) ...uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorunda olduğu ve ...bu kişilerle birlikte müştereken sorumlu olduğu,*
- *Belirtilen şekilde söz konusu faaliyetlerde bulunan veri sorumluları hakkında (idari para cezası) tesis edileceği,*
- *Bahse konu şekilde işlenen kişisel verilerin hukuka aykırı olarak elde edilmiş olabileceği de göz önüne alınarak... (5237 sayılı TCK md. 136) ...çerçevesinde ilgili veri sorumluları hakkında gerekli hukuki işlemlerin tesisi için... ilgili Cumhuriyet Başsavcılığına bildirileceği”* hüküm altına alınmıştır.

Veri sorumluları ve veri işleyenler tarafından ilgili kişilerin e-posta adreslerine veya SMS ya da çağrı ile cep telefonlarına reklam bildirimleri/aramaları yönlendirilmesinin önüne geçilmesi ile ilgili Kişisel Verileri Koruma Kurulunun 16/10/2018 Tarihli ve 2018/119 Sayılı İlke Kararı, <https://www.kvkk.gov.tr/Icerik/5299/2018-119> , E.T. 28.04.2019.

bakımından, özellikle kişilik hakkının ihlali üzerine her zaman maddi ve manevi tazminat talebinde bulunabilecektir⁷⁷¹.

6. Veri Sorumlusunun Yükümlülükleri

KVKK'nın 10. ve 12. maddelerinde veri sorumlusunun yükümlülükleri düzenlenmiştir. 10. madde "*Veri sorumlusunun aydınlatma yükümlülüğü*"nü ele alırken, 12. maddede, "*Veri güvenliğine ilişkin yükümlülükler*"i bulunmaktadır.

Aydınlatma yükümlülüğüne göre veri sorumlusu ya da yetkilendirdiği kişi, kişisel verilerin elde edilmesi esnasında ilgili kişiyi bazı hususlarda aydınlatmakla yükümlüdür. Buna göre veri sorumlusu;

- Veri sorumlusunun ve varsa temsilcisinin kimliği hakkında,
- Kişisel verilerin işlenme amacına ilişkin,
- İşlenen kişisel verilerin kimlere ve hangi amaçla aktarılabilmesi hususunda,
- Kişisel verinin toplanma yöntemi ve hukuki sebebine dair,
- 11. maddede düzenlenen ilgili kişinin haklarına ilişkin olarak,

kişisel verilerin işlendiği sırada ilgili kişiyi aydınlatmakla yükümlüdür. Bu bilgilerin ilgili kişi ile paylaşılması ile hem şeffaflık gerçekleşecek hem de ilgili kişi haklarından faydalanırken kimlere ne gibi taleplerle başvurabileceğini de öğrenmiş olacaktır.

Kanun'un 2. maddesi bağlamında düzenlenen veri güvenliğine ilişkin yükümlülüklerden ilki, kişisel verilerin hukuka aykırı olarak işlenmesi ve erişilmesini önlemek ile verilerin muhafazasını sağlamak amaçlarıyla, "*uygun güvenlik düzeyini temin için gerekli idari ve teknik tedbirlerin alınması*"dır. Bu bağlamda Kanun, veri sorumlusuna yalnızca gerekli önlemleri alması hususunda bir yükümlülük yüklemekte,

⁷⁷¹ Hüseyin Can AKSOY, *Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması*, Çakmak Yayınevi, Ankara, 2010, s. 82- 87; Kişilik hakkını koruyucu davalar bakımından detaylı bir çalışma olarak bkz. Serap HELVACI, *Türk ve İsviçre Hukuklarında Kişilik Hakkını Koruyucu Davalar*, Beta, 2001.

saldırıları önlemekle yükümlü kılmamaktadır. Dolayısıyla veri sorumlusu, kendisine düşen teknik ve idari tedbirleri almışsa sorumluluktan kurtulmaktadır. Teknik ve idari tedbirlerden genel olarak anlaşılması gereken ise, çalışanların sürekli bilgilendirilmesi, eğitime tabi tutulması, güncel ve değişken şifrelerle yetkisiz erişimin engellenmesi, veri kullanım politikalarının belirlenmesi, denetim yapılması veya siber saldırılara karşı gerekli tedbirlerin alınması gibi faaliyetlerdir. Anılan önlemler sürekli denetlenmeli ve günün koşullarına uyarlanmalıdır⁷⁷². Teknik ve idari tedbirler belirlenirken somut olaya göre karar verilmelidir. Daha evvel belirtildiği üzere, Adalet Divanı *Worten* kararında⁷⁷³ veri denetleyicisinin veri güvenliği için uygun bir güvenlik seviyesi belirlemesinde, teknolojinin durumu, uygulamaların maliyeti, korunacak verilerin niteliği ile varolan riskin dikkate alınması gereğini vurgulamıştır.

Uygun güvenlik düzeyinin veri sorumlusunca temin edilmesi, verilerin hukuka aykırı olarak işlenmesini önlemek, hukuka aykırı erişilmesini önlemek ve muhafazasını sağlamak amaçlarını içermektedir. Ancak burada amaçlara ilişkin bir belirleme yapmak gerekmektedir. Her ne kadar 12. maddede bu hususlar uygun güvenlik düzeyini temin etmenin amaçları olarak ayrı ayrı düzenlenmiş olsa da tüm bu “*hukuka aykırı işleme ve erişilmeyi önleme ile muhafazasını sağlama*” halleri, Kanun’un 3/1(e). maddesi uyarınca “Kişisel verilerin işlenmesi” olarak değerlendirilmektedir. Bu bakımdan KVKK’nın neden özel olarak bu amaçları ayrı ayrı ele alarak uygun güvenlik düzeyinin sağlanması bakımından ayrı amaçlarmış gibi değinildiklerini anlamak güçtür. Doktrinde bu duruma ilişkin olarak, veri işlemenin türleri olan bu kavramların Kanun’daki bu tanımdan bağımsız biçimde yorumlanmaları gerektiği, aksi takdirde bu hükmün bir anlamı olmayacağı belirtilmektedir. Buna görüşe göre, “*kişisel verilerin hukuka aykırı işlenmesi*”nden kişisel verilerin nasıl ve ne şekilde işlenmesi gerektiğini; “*kişisel verilerin hukuka aykırı erişimi*”nden kişisel verilerin işlenip işlenmeyeceklerini anlamak

⁷⁷² ÇEKİN, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu*, s. 105- 106.

⁷⁷³ Case C-342/12 *Worten – Equipamentos para o Lar SA v. Autoridade para as Condições de Trabalho (ACT)*, 30.05.2013, Par. 24, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0342&from=FR>, E.T. 27.04.2019.

ve “*kişisel verilerin muhafazasının sağlanması*”ndan da verilerin bozulmadan, değiştirilmeden veri sorumlusunda bulundurulması anlaşılmaktadır⁷⁷⁴.

Veri sorumlusu tarafından yukarıda belirtilen amaçlar doğrultusunda uygun güvenlik düzeyinin sağlanması için her türlü teknik ve idari önlemi alırken, ilk olarak KVKK’nın 4. ve 9. maddeleri arasındaki şartlara göre veri işleminin hukuka uygunluk denetimi yapılacaktır. Devamında veri sorumlusu, kişisel verilere hukuka aykırı erişimi önlemelidir. Hukuka aykırı erişimin önlenmesi hem fiziksel olarak, hem de bilgisayar, cep telefonu gibi araçlarla veri sistemlerine ulaşılmasını engellemeyi kapsamaktadır. Fiziksel olarak engelleme, bir güvenlik alanı oluşturularak bu alana yetkisiz kişilerin girmesinin önüne geçilmesi biçiminde olabilir. Sistemsel olarak erişimin engellenmesi ise, verilere belli bir sistem üzerinden erişim yetkisi verilen kişilerin yalnızca gerektirdiği ölçüde sisteme müdahil olabilmeleri, sisteme giriş yetkisi olmayanların ise, teknik vasıtalar aracılığı ile sistemlere girmesinin önüne geçilmesi biçiminde gerçekleştirilmesidir. Nihayetinde uygun güvenlik düzeyinin sağlanması için kişisel verilerin muhafazasını sağlayıcı teknik ve idari tedbirler ise, verilerin yok olması veya kaybedilmesine karşı gereken önlemlerin alınmasını kapsamaktadır⁷⁷⁵.

KVKK’nın 3/1(ğ). maddesine göre veri işleyen, “*Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi*” anlamına gelmektedir. 12/2. madde ise,

“Veri sorumlusu, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, birinci fıkrada belirtilen tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumludur.”

düzenlemesini hüküm altına almıştır. Buna göre veri sorumlusu, veri işleyenle birlikte uygun güvenlik düzeyini sağlamak bakımından gereken idari ve teknik tedbirleri alma

⁷⁷⁴ ÇEKİN, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu*, s. 108.

⁷⁷⁵ ÇEKİN, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu*, s. 109- 110.

konusunda müşterek olarak, yani müteselsil biçimde sorumludur. Dolayısıyla veri sorumlusu, kişisel verileri işlenmesi işini bir başkasına da vermiş olsa, kendisinin sorumluluğu devam etmektedir. Her ne kadar veri sorumlusu ile veri işleyen arasındaki ilişki bakımından Kanun’da başka bir düzenleme bulunmasa da veri sorumlusu veri işleyene ihtiyaç duyması halinde mutlaka aralarında bir sözleşme akdederek KVKK’da yer alan tüm yükümlülüklerden sorumlu olacağını müteselsil sorumluluğun kapsamında açıkça düzenlemelidir.

Veri sorumlusunun yükümlülükleri bakımından ele alınması gereken bir başka husus da KVKK’nın 12/3. maddesinde belirtilen, veri sorumlusunun Kanun’un uygulanmasını sağlamak için kendi kurum veya kuruluşunda, gerekli denetimleri yapmak veya yaptırmak zorunluluğudur. Bu bakımdan veri sorumlusu Kanun’un ilk elden uygulayıcısı ve denetleyicisidir.

Bir diğer yükümlülük de veri sorumlusu ve veri işleyen bakımındandır. Buna göre ilgili kişiler öğrendikleri kişisel verileri, görevlerinden ayrılışları dahi, bu Kanun hükümlerine aykırı biçimde başkalarına açıklayamayacak ve işleme amacı dışında kullanamayacaklardır.

Son olarak veri sorumlusunun “Kurul’a Bildirim Yükümlülüğü” bulunmaktadır. Bu yükümlülük, işlenen kişisel verilerin hukuka aykırı olarak başkaları tarafından elde edilmesi hâlinde, bu durumun en kısa sürede ilgili kişiye ve Kurul’a bildirilmesini kapsamaktadır. Buradaki yükümlülük ilgili kişi ve Kurul’a bildirimden ibarettir. Bunun amacı, veri sorumlusunun kusuru olsun veya olmasın gerçekleşen saldırıyı durdurmak, devamını engellemek ve yeniden tekrarını önlemek için Kurul ile iş birliğidir. Devamında Kurul, gerektirmesi halinde, hukuka aykırı biçimde veri elde edilmesine ilişkin olarak internet sitesi ya da uygun göreceği farklı bir yöntemle bildiri yayınlayabilecektir.

GVKT bakımından yükümlülük meselesi, KVKK’ya nazaran bir miktar farklılık arz etmektedir. Daha önce belirtildiği üzere, veri işleyicisi kavramı 96/46/AT sayılı Direktif’te yer almamaktaydı. Bu kavram ilk defa GVKT ile düzenlenmiştir. Buna göre

veri işleyicisi, veri denetleyicisi adına verileri işleyen gerçek ya da tüzel kişi, kamu kurum ve kuruluşu veya başka bir kurumdur. Veri denetleyicisi ise, yalnız başına ya da başkalarıyla birlikte kişisel verilerin işlenmesinin amaçlarını ve araçlarını belirleyen gerçek veya tüzel kişi, kamu otoritesi, kurum veya diğer birimlerdir. Tıpkı KVKK gibi hem veri denetleyicisi hem de veri işleyicisi GVKT'deki kurallar bakımından müşterek olarak sorumludurlar. Oysa 95/46/AT Sayılı Direktif'te, yalnızca veri denetleyicisi sorumlu tutulmaktaydı. Bu bakımdan KVKK her ne kadar 96/46/AT sayılı Direktif'i esas almış olsa da ondan daha ilerici bir düzenlemeyi hayata geçirmiştir. KVKK bakımından yukarıda önerildiği üzere, GVKT'de de veri işleyicisi ile veri denetleyicisinin bir sözleşme yapmaları gereği mevcuttur⁷⁷⁶.

Veri denetleyicisinin GVKT bakımından sorumluluğuna bakıldığında, öncelikle veri koruma bakımından idari ve teknik önlemleri alarak veri öznesinin haklarını korumakla yükümlü olduğu görülmektedir. Söz konusu durumun işleyici bakımından yansması ise, veri koruma bakımından idari ve teknik önlemleri almak için yeterli güvenceleri sağlayan işleyicilerin kullanılması şartını içermektedir. KVKK'nın aksine GVKT'de veri denetleyicisi ile işleyici arasındaki ilişkinin koşulları ve Sözleşme'nin içeriği de düzenlenmektedir⁷⁷⁷. Veri denetleyicisinin ayrıca, KVKK'ya benzer biçimde, kişisel verilerin ihlali durumunda denetleme makamlarına yönelik bir raporlama görevi mevcuttur. Buna göre kişisel veri ihlalinin farkına varılmasından itibaren en geç 72 saat içerisinde ihlal denetim otoritesine bildirmelidir. İhlal, hak ve özgürlüklerin kullanımı bakımından risk yaratıyorsa, veri öznesine bilgi vermelidir⁷⁷⁸. Veri denetleyicisi ve

⁷⁷⁶ VOSS, "European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield and the Right to Delisting", s. 226.

⁷⁷⁷ GVKT md. 28.

⁷⁷⁸ VOIGT, VON DEM BUSSCHE, *The EU General Data Protection Regulation (GDPR)- A Practical Guide*, s. 4; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), Art. 33, L 119, 04.05.2016, <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504>, E.T. 14.03.2019.

işleyicisi belli hallerde, KVKK’da bulunmayan bir müessese olarak, “Veri Koruma Denetleyicisi” de atamakla görevlidir⁷⁷⁹.

7. Denetim ve Yaptırım Sistemi

KVKK, anayasal bir hak olan kişisel verilerin korunması hakkına ilişkin esas ve usulleri düzenleyen bir kanundur. Bu Kanun, kişisel verilerin korunması için yukarıda açıklanan birçok ilke ve düzenlemeyi getirmektedir. Hukuka uygun bir biçimde veri işlenmesi, verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi, veri sorumlusu ile ilgili kişinin hak ve yükümlülüklerine uygunluğu, veri güvenliği gibi birçok hususta temel ilkelerin takibini sağlamak, denetlemek, hukuka aykırı veri işlenmesini engellemek ve yaptırım altına almak için ise 21. maddesinde Kişisel Verilerin Korunması Kurulu’nu oluşturmuştur.

Kişisel verilerin korunması bakımından Kanun kapsamında hukuki yaptırım (tazminat), idari yaptırım ve cezai yaptırım sistemi benimsenmiştir. İlaveten kişisel verilerin işlenmesinden önce verileri işleyen gerçek ve tüzel kişi veri sorumlularının kayıt altına alınacakları “Veri Sorumluları Sicili” oluşturulmuştur. Yine bu bağlamda “Veri Sorumlusuna Başvuru” ve “Kurul’a Şikâyet” mekanizmaları da veri korumasına hizmet eden müesseseler olarak karşımıza çıkmaktadır. Bu sistemler incelenirken kişisel

⁷⁷⁹ Veri denetleyicisi ve veri işleyicisi;

- Veri işleme, yargı görevini sürdüren mahkemeler harici bir kamu kurum veya kuruluşu tarafından yürütülmekteyse,
- Veri denetleyicisi veya işleyicisinin temel faaliyetleri, veri öznelerinin büyük ölçekte düzenli ve sistematik olarak izlenmesini gerektiren işlemlerden oluşuyorsa,
- Veri denetleyicisi veya işleyicisinin temel faaliyetleri, 9. Madde kapsamında büyük miktarda özel nitelikli veri kategorileri veya 10. Madde kapsamında cezai hüküm ve suçlarla ilgili kişisel veriler kapsamındaysa,

“Veri Koruma Görevlisi” atayacaktır.

VOIGT, VON DEM BUSSCHE, *The EU General Data Protection Regulation (GDPR)- A Practical Guide*, s. 53; TIKKINEN-PIRI, ROHUNEN, MARKKULA, “EU General Data Protection Regulation: Changes and implications for personal data collecting companies”, s. 14; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), Art. 37, L 119, 04.05.2016, <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504>, E.T. 21.03.2019.

verilerin korunması sisteminde esas olanın önleyici koruma olduğu⁷⁸⁰, verileri hukuka aykırı biçimde işlenmesi neticesinde hükmedilecek her yaptırımın aslında önleme faaliyetinin muadili olmayacağı unutulmamalıdır.

a) Bir Denetim Organı Olarak Kişisel Verilerin Korunması Kurulu

KVKK'nın 19. maddesi, Kanun ile verilen görevlerin yerine getirilmesi amacıyla idari ile mali özerkliğe ve kamu tüzel kişiliğine sahip “*Kişisel Verilerin Korunması Kurumu*”nu kurmuştur. Kurul ve Başkanlık’tan oluşan bu Kurum’un karar organı “*Kişisel Verilerin Korunması Kurulu*”dur. Bu Kurul, hukuka uygun bir biçimde veri işlenmesi için Kanun’da düzenlenmiş olan temel ilkelerin takibini sağlamak, denetlemek, hukuka aykırı veri işlenmesini engellemek ve yaptırım altına almakla görevli ve yetkilidir.

Kişisel verilerin korunmasını etkili bir biçimde gerçekleştirebilmek için bağımsız bir denetim organının mevcudiyeti, Avrupa veri koruma hukukunun önemli özelliklerinden biridir. GVKT’nin 52. maddesinde denetim makamlarının görevlerini yerine getirip ve yetkilerini kullanırken tamamen bağımsız bir biçimde hareket etmeleri gerektiği hüküm altına alınmıştır. Yine Tüzük’ün 53. maddesine göre denetim makamının her üyesi ülkenin Parlamentosu, Hükümet, Devlet Başkanı veya ülkenin iç hukuku bağlamında atama yetkisi verilmiş bağımsız bir organ tarafından ve şeffaf bir usulle belirlenmelidir. Bazı AB üye ülkeleri bakımından görülmektedir ki, veri koruma otoritelerinin üyelerinin seçimi ve atanması aşamalarına ülkelerin Parlamentolar’ı etkili bir biçimde katılmaktadır. Söz gelimi, İrlanda, Lüksemburg ve Birleşik Krallık’ta Kurulları’nın bazı üyeleri Hükümet tarafından atanabilmektedir. Danimarka ve Hollanda’da ise bazı Kurul üyeleri Adalet Bakanı tarafından atanmaktadır. Polonya’da ise üyeler Senato’nun onayı neticesinde Parlamento tarafından seçilmektedirler⁷⁸¹.

⁷⁸⁰ KÜZECİ, *Kişisel Verilerin Korunması*, s. 368.

⁷⁸¹ TEKİN, “*Kişisel Verilerin Korunması ile İlgili Türkiye’deki Kanun Tasarısı’nın Avrupa Birliği Veri Koruma Direktifi Işığında Değerlendirilmesi*”, s. 255.

KVKK'ya göre Kurul, dokuz üyeden oluşur. Kurul'un beş üyesi Türkiye Büyük Millet Meclisi, dört üyesi Cumhurbaşkanı tarafından seçilmektedir. Ayrıca, Kurul üyelerinin görev süresi 4 yıl olup, görev süresi biten üye yeniden seçilebilmektedir. GVKT'nin 54. maddesinde *“Denetim makamının kurulmasına ilişkin kurallar”*a bakıldığında, bir denetim makamı olarak Kurul'un kuruluşu, üye olmak için gereken nitelikler ve uygunluk koşulları, üyelerin belirlenmesine dair kurallar ve usuller, üyelerinin en az dört yıl olacak görev süresi, üyelerin yeniden tayin edilip edilemeyeceği ile tayin edilmeleri halinde, kaç dönem olacağı, üyelerin yükümlülükleri ile görevleri sırasında ve sonrasında üyelikle bağdaşmayan eylemler, meslekler ve menfaatlere ilişkin yasakları düzenleyen koşullar ve göreve son verilmesini düzenleyen kuralların Kanun tarafından düzenlenmesi gerektiği belirtilmektedir. Bu düzenleme ışığında KVKK'ya baktığımızda, Kurul'a dair hemen hemen tüm bu düzenlemelerin 21. maddede bulunduğunu görürüz. Bu bakımdan Kurul'a ilişkin düzenlemelerin Avrupa veri koruma standartları ile uygunluk gösterdiği söylenebilecektir. Fakat burada önemli bir hususun altı çizilmelidir. Buna göre Kişisel Verileri Koruma Kurulu'nun çoğunluk üyelerinin TBMM'de çoğunluğa sahip siyasi iktidar ve partili bir Cumhurbaşkanı tarafından belirlenmesi, görünüşte de olsa tarafsızlık ilkesine gölge düşürme ihtimaline sahiptir⁷⁸². Dolayısıyla Kurum'un uygulamaları, omuzlarındaki sorumluluk dolayısıyla, bu noktada karar verebilmek adına tek belirleyici olacaktır.

Hükümlerin bir kısmına daha yakından bakılacak olursa, bir kısmının Kurul'un bağımsızlığını sağlamak için düzenlendiği görülecektir. Buna göre Kurul öncelikle görev ve yetkilerini bağımsız olarak yerine getirmeli ve kullanmalıdır. Ayrıca Kurul'a görev alanına giren konularla ilgili olarak hiçbir organ, makam, merci veya kişi emir ve talimat veremeyecek, tavsiye veya telkinde bulunamayacaktır. Bir diğer güvence de Kurul üyelerinin görevleri sebebiyle işledikleri iddia edilen suçlara ilişkin soruşturmalarının, 4483 sayılı Memurlar ve Diğer Kamu Görevlilerinin Yargılanması Hakkında Kanun'a göre yapılacağı ve bu kişiler hakkında soruşturma izninin Cumhurbaşkanı tarafından

⁷⁸² DÜLGER, “Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması”, *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi*, s. 162- 163.

verileceğidir. Disiplin soruşturması ve kovuşturmasında da 657 sayılı Kanun hükümleri uygulanacaktır. Son olarak Kurul üyelerinin süreleri dolmadan herhangi bir nedenle görevlerine son verilemez.

Avrupa veri koruma hukukunun mihenk taşlarından birinin, denetim organının bağımsızlığı olduğu dile getirilmişti. Ayrıca AB Adalet Divanı da bu konuda birçok karara izma atmış ve aslolanın “tam bağımsızlığı sağlamak” olduğunu, bunun da denetim otoritelerinin görevlerini yerine getirirken mümkün olduğunca objektif ve tarafsız davranması ile sağlanacağını hüküm altına almıştır⁷⁸³. Bu noktada belirtilmelidir ki, KVKK kapsamında oluşturulan Kurul’a ilişkin düzenlemeleri Kurul’un oluşumu ve diğer özellikleri Avrupa veri koruma sistemine uygun düşse de, yalnızca Kanun’un maddeleri değil, uygulaması da belirleyici şekilde önem taşımaktadır. Her ne kadar 2018 AB İlerleme Raporu’na göre⁷⁸⁴ Kişisel verilerin korunmasına ilişkin mevzuatın henüz Avrupa standartlarıyla uyumlu olmadığı dile getirilmiş ve bunun bir sebebinin de Kişisel Verileri Koruma Kurumu’nun yetkilerine ilişkin olduğu belirtilmişse de Kurul’un oluşumu hakkında bir eleştiri yapılmamıştır.

Kişisel Verilerin Korunması Kurulu’nun görev ve yetkilerine bakacak olursak, Kanun’un 22. maddesinde oldukça detaylı bir şekilde düzenlenmiş olduğunu görürüz. Avrupa veri koruma sisteminde ve GVKT özelinde tam bağımsızlığı mütemadiyen vurgulanan bir denetim organı olarak Kurul’a bir anayasal hak olarak kişisel verilerin korunmasına yönelik bu denli detaylı görev ve yetkinin verilmesi, Türkiye özelinde hakkın en önemli koruyucusu olmak ve mutlak özerkliğini sağlamak misyonunu yüklemektedir. Bu bakımdan Kurul’un hakkın uygulamasını gerçekleştirme, denetim,

⁷⁸³ Case C-518/07 *European Commission v. Federal Republic of Germany*, 09.03.2010, Par. 19, <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62007CJ0518:EN:HTML>, E.T. 26.03.2019.

⁷⁸⁴ Avrupa Komisyonu Türkiye 2018 Yılı İlerleme Raporu, Komisyon Tarafından Avrupa Parlamentosuna, Konseye, Ekonomik ve Sosyal Komiteye ve Bölgeler Komitesine Sunulan Bilgilendirme, AB Genişleme Politikasına İlişkin 2018 Bilgilendirmesi, {COM(2018) 450 nihai} - {SWD(2018) 150 nihai} - {SWD(2018) 151 nihai} – {SWD(2018) 152 nihai} - {SWD(2018) 154 nihai} - {SWD(2018) 155 nihai} – {SWD(2018) 156 nihai } Ekindeki KOMİSYON ÇALIŞMA DOKÜMANI 2018 Türkiye Raporu, Strazburg, 17.04.2018, SWD(2018) 153 Nihai, s. 5, 33.

önleme, düzenleme ve kurumsal yönetime ilişkin görev ve yetkileri bulunmaktadır. Buna göre;

- Kişisel verilerin, temel hak ve özgürlüklere uygun şekilde işlenmesini sağlamak,
- Hak ihlali iddiasındakilerin şikâyetlerini karara bağlamak,
- Re'sen görev alanına giren konularda kişisel verilerin kanunlara uygun olarak işlenip işlenmediğini incelemek ve gerektiğinde geçici önlemler almak,
- Özel nitelikli kişisel verilerin işlenmesi için aranan yeterli önlemleri belirlemek,
- Veri Sorumluları Sicilinin tutulmasını sağlamak,
- Kendi görev alanı ile Kurum'un işleyişine ilişkin konularda gerekli düzenleyici işlemleri yapmak,
- Veri güvenliğine ilişkin yükümlülükleri belirlemek amacıyla düzenleyici işlem yapmak,
- Veri sorumlusunun ve temsilcisinin görev, yetki ve sorumluluklarına ilişkin düzenleyici işlem yapmak,
- Kanun'da öngörülen idari yaptırımlara karar vermek,
- Kişisel verilere ilişkin hüküm içeren mevzuat taslakları hakkında görüş bildirmek,
- Kurum'un stratejik planını karara bağlamak, amaç ve hedeflerini, hizmet kalite standartlarını ve performans kriterlerini belirlemek,
- Kurum'un bütçe teklifini görüşmek ve karara bağlamak,
- Kurum'un performansı, mali durumu, yıllık faaliyetleri ve ihtiyaç duyulan konular hakkında hazırlanan rapor taslaklarını onaylamak ve yayımlamak,
- Taşınmaz alımı, satımı ve kiralanması konularındaki önerileri görüşüp karara bağlamak,
- Kanunlarla verilen diğer görevleri yerine getirmektir.

Anılan bu görev ve yetkiler dışında Kurul'un çalışma esaslarına bakıldığında özellikle vurgulanması gereken bir husus, 23/5 ve 23/6. maddelerdeki düzenlemelerdir. Belirtildiği üzere Kurul, kişisel verilerin korunması hakkının ilk elden uygulayıcısı ve yorumlayıcısıdır. Bu bakımdan her ne kadar mahkeme kararları gibi içtihadi faaliyetler önem taşısa da Kurul kararları hakkın uygulamasının temel yol göstericileri olacaktır.

Kurul üyelerinin her ne kadar çalışmaları sırasında ilgili ve üçüncü kişilere ait öğrendikleri sırları saklama yükümlülükleri bulunsada kararların aleniyeti hakkı ilişkin pratiğı göstermesi bakımından veri korumanın gerçekleştirilmesine oldukça katkı sağlayabilecektir. Ancak KVKK'nın yukarıda anılan bentlerinde belirtilmektedir ki, Kurul toplantılarındaki görüşmeler, aksi kararlaştırılmadıkça, gizlidir ve Kurul ancak gerekli gördüğü kararları kamuoyuna duyuracaktır. Bu bakımdan söz konusu hükümler, tam bağımsız olması gereken ve bunu şeffaflıkla destekleyebilecek olan Kurul'un önünde bir engel olarak değerlendirilebilecektir.

Kişisel Verilerin Korunması Kurumu'nun bir diğer ayağı da "Başkanlık"tır. Başkanlık, Başkan Yardımcısı ve hizmet birimlerinden oluşmaktadır. Kurum'un ve Kurul'un en üst amiri olan Başkan'ın işleyiş bakımından oldukça geniş bir alana yayılan yönetim ve temsili sağlamaya yönelik görevleri mevcuttur⁷⁸⁵. Başkanlık'ın görevleri ise, daha ziyade Kurum'un görev ve yetki kapsamındaki iş ve işlemlerin yürütülmesidir⁷⁸⁶.

⁷⁸⁵ KVKK md. 24/3; "Başkanın görevleri şunlardır:

- a) Kurul toplantılarını idare etmek.
- b) Kurul kararlarının tebliğini ve Kurulca gerekli görülenlerin kamuoyuna duyurulmasını sağlamak ve uygulanmalarını izlemek.
- c) Başkan Yardımcısını, daire başkanlarını ve Kurum personelini atamak.
- ç) Hizmet birimlerinden gelen önerilere son şeklini vererek Kurula sunmak.
- d) Stratejik planın uygulanmasını sağlamak, hizmet kalite standartları doğrultusunda insan kaynakları ve çalışma politikalarını oluşturmak.
- e) Belirlenen stratejilere, yıllık amaç ve hedeflere uygun olarak Kurumun yıllık bütçesi ile mali tablolarını hazırlamak.
- f) Kurul ve hizmet birimlerinin uyumlu, verimli, disiplinli ve düzenli bir biçimde çalışması amacıyla koordinasyonu sağlamak.
- g) Kurumun diğer kuruluşlarla ilişkilerini yürütmek.
- ğ) Kurum Başkanı adına imzaya yetkili personelin görev ve yetki alanını belirlemek.
- h) Kurumun yönetim ve işleyişine ilişkin diğer görevleri yerine getirmek."

⁷⁸⁶ KVKK md. 25/4: "Başkanlığın görevleri şunlardır:

- a) Veri Sorumluları Sicilini tutmak.
- b) Kurumun ve Kurulun büro ve sekreteryası işlemlerini yürütmek.
- c) Kurumun taraf olduğu davalar ile icra takiplerinde avukatlar vasıtasıyla Kurumu temsil etmek, davaları takip etmek veya ettirmek, hukuk hizmetlerini yürütmek.
- ç) Kurul üyeleri ile Kurumda görev yapanların özlük işlemlerini yürütmek.
- d) Kanunlarla mali hizmet ve strateji geliştirme birimlerine verilen görevleri yapmak.

Kişisel Verilerin Korunması Kurulu, kişisel verilerin korunması açısından bir veri ihlallerini önleme ve denetleme mekanizması olduğunu özellikle üç kurum bağlamında ortaya koymaktadır. Bunlardan ilki, “*Veri Sorumlusuna Başvuru*”dur. KVKK’nın 13. maddesine göre ilgili kişi, Kanun’un uygulanmasıyla ilgili taleplerini ilk olarak veri sorumlusuna iletecektir. Bunu yazılı olarak veya Kurul’un belirleyeceği diğer yöntemle gerçekleştirir. Veri sorumlusu başvuruyu kabul edebilir ya da gerekçesi ile reddedebilir. Bu başvuruyu en kısa sürede ve en geç 30 gün içinde sonuçlandırmak zorundadır. Bu başvuru ücretsizdir. Fakat yapılacak işlem ilave bir maliyet gerektirirse, o durumda Kurul tarafından belirlenen tarife göre ücretlendirilebilecektir. Bu ihtimalde şayet başvuruya konu olan husus veri sorumlusunun bir hatasından kaynaklanıyorsa ücret iade edilecektir. Daha evvel belirtildiği üzere Adalet Divanı da veri sorumlusuna başvuru halinde “makul seviyede bir ücretin istenebileceğine hükmetmiştir⁷⁸⁷. Bu bakımdan ilgili durum Avrupa veri koruma sistemine aykırılık teşkil etmeyecektir.

İkinci kurum ise, Kanun’un 14. maddesinde düzenlenen “*Kurul’a Şikâyet*” müessesesidir. Buna göre veri sorumlusuna başvuru neticesinde başvurunun reddedildiği veya başvuruya verilen cevabın yetersiz bulunduğu ya da en geç 30 gün içinde cevap verilmediği hallerde Kurul’a şikâyet yoluna gidilebilecektir. Burada ilgili kişi, veri sorumlusunun cevabını öğrendiği tarihten itibaren veya veri sorumlusunun başvuruya

e) Kurumun iş ve işlemlerinin yürütülmesi amacıyla bilişim sisteminin kurulmasını ve kullanılmasını sağlamak.

f) Kurulun yıllık faaliyetleri hakkında veya ihtiyaç duyulan konularda rapor taslaklarını hazırlamak ve Kurula sunmak.

g) Kurumun stratejik plan taslağını hazırlamak.

ğ) Kurumun personel politikasını belirlemek, personelin kariyer ve eğitim planlarını hazırlamak ve uygulamak.

h) Personelin atama, nakil, disiplin, performans, terfi, emeklilik ve benzeri işlemlerini yürütmek.

ı) Personelin uyacağı etik kuralları belirlemek ve gerekli eğitimi vermek.

i) 10/12/2003 tarihli ve 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu çerçevesinde Kurumun ihtiyacı olan her türlü satın alma, kiralama, bakım, onarım, yapım, arşiv, sağlık, sosyal ve benzeri hizmetleri yürütmek.

j) Kuruma ait taşınır ve taşınmazların kayıtlarını tutmak.

k) Kurul veya Başkan tarafından verilen diğer görevleri yapmak.”

⁷⁸⁷ Case 486/12 X, 12.12.2013, Par. 20- 23, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0486>, E.T. 04.04.2019.

yanıt vermesi gereken en geç 30 günlük süresinin bitiminden itibaren 30 gün içerisinde ve herhalükarda 60 gün dolduğunda şikâyetle bulunabilir. Kurul şikâyet üzerine veya ihlal iddiasını kendiliğinden öğrenmesi durumunda inceleme yapabilecektir⁷⁸⁸. Bir ihbar veya şikâyetin Kurul tarafından incelemeye alınması için belli bir konuyu içermesi, yargı mercilerinin görevine giren konularla ilgili olmaması, ihbar veya şikâyeti yapanın adı-soyadı, imzası iş ya da ikametgâh adreslerinden birinin bulunması gerekmektedir⁷⁸⁹. Şikâyet üzerinden 60 gün geçmiş ve Kurul hala bir cevap vermemiş ise talep reddedilmiş anlamına gelir. Ancak bir ihlal tespit edilirse Kurul, hukuka aykırılıkların veri sorumlusu tarafından giderilmesine karar verir ve bu kararı ilgililere tebliğ eder. Anılan karar, tebliğden itibaren gecikmeksizin ve en geç 30 gün içinde yerine getirilmek zorundadır.

⁷⁸⁸ Bu noktada Kurul’un ihlal iddiasını re’sen öğrendiği ve incelediği, 10.05.2019 itibarıyla yayınlamış olduğu KVKK rejiminin ilk büyük ihlali ve şimdiye dek hükmedilen en büyük miktartlı idari para cezası olarak anılabilecek 2019/104 Sayı ve 11.04.2019 tarihli Facebook Kararı’na da değinmek gerekmektedir. Söz konusu olaydaki iddia, 13- 25 Eylül 2018 tarihleri arasında Facebook üzerinden bazı üçüncü taraf uygulamalar, bu süre içerisinde yetkisini aşan düzeyde Facebook’ta yer alan fotoğraflara erişmiş olunabileceği hususundadır. Kurul kararında ilk olarak veri ihlaline dair veri sorumlusu tarafından Kurul’a yapılması gereken bildirim yükümlülüğünün gerçekleştirilmediğini belirtmektedir. Kurul, 12 günlük veri ihlalinin API hatası denilen teknik bir probleme Facebook tarafından zamanında müdahale edilmediği ve gereken teknik ve idari tedbirlerin alınmasında şirketin ihmali olduğunu dile getirmektedir. Olayda, yalnızca Facebook üzerinde paylaşım yapılan fotoğraflara değil, ayrıca henüz taslak halinde olan paylaşım yapılmayan fotoğraflara da erişim sağlandığının, bu sebeple de kullanıcıların izin vermiş olduğundan çok daha fazla fotoğrafa erişim sağlanmasını KVKK’nın 4/2-a ve 12/1. Maddelerinde yer alan “Hukuka ve dürüstlük kurallarına uygun olma” ve 4/2-ç’de bulunan “işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma” ilkelerine aykırı olduğuna hükmetmiştir. Ayrıca Kurul, kişilerin paylaşım yaptığı fotoğraflarına ilişkin veri ihlali haricinde paylaşım yapılmayıp taslak olarak kalan fotoğrafların da olaya konu olması ve Facebook’un üçüncü taraf uygulamaların bu fotoğraflara da erişim sağlayıp sağlayamadığını belirleyememesini veri akışının şirket tarafından kontrol edilememesine bağlamaktadır. Bu ise “veri güvenliği”ne dair yükümlülüklerin de ihlali anlamına gelmektedir.

Tüm bu sebepler dolayısıyla Kurul, KVKK’nın 18. Maddesi uyarınca 1.100.000 TL idari para cezasına ve veri ihlalinin 18.09.2018 tarihinde tespit edilmiş ancak Kurul’a bildirim yapılmamış olmasından bahisle 550.000 TL idari para cezasına hükmetmiştir.

Karar, Kurul’un KVKK uygulamasını oldukça sağlam bir çerçeveye oturtmak istediğini göstermesi bakımından oldukça önemlidir. Yalnızca bir Facebook yetkilisinin veri ihlalinin açıklanmış olması üzerine Kurul’un re’sen harekete geçmesi ve incelemeyi gerçekleştirmesi ise veri sorumlusunun ihlal bildirim yükümlülüğünün ne kadar ciddiye alınması gereken bir sorumluluk olduğunu göstermektedir.

“Facebook nezdinde gerçekleşen veri ihlalinin değerlendirilmesi” ile ilgili Kişisel Verileri Koruma Kurulunun 11.04.2019 tarih ve 2019/104 sayılı Kararı Özeti, 10.05.2019, <https://www.kvkk.gov.tr/Icerik/5450/2019-104>, E.T. 21.05.2019.

⁷⁸⁹ 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun, md. 4 ve 6.

Bu noktada Kurul uygulamada hem başvuru hem şikâyet sürelerinin hesaplanmasında farklılıklar olduğunu görmüş ve bu bakımdan 24 Ocak 2019 tarihinde “*Veri Sorumlusuna Başvuru ve Kurula Şikâyet Sürelerinin Hesaplanmasına İlişkin 2019/9 sayılı Kararı*” yayımlamıştır⁷⁹⁰. Bu karara göre üç özellikli durumda süre hesabının nasıl yapılacağı açıklanmıştır. Karara göre;

- “İlgili kişi tarafından yapılan başvuruya veri sorumlusunca 30 gün içinde bir cevap verilmesi halinde ilgili kişinin veri sorumlusunun cevabını müteakip 30 gün içerisinde şikâyetle bulunabileceği, bu itibarla söz konusu hallerde ilgili kişinin veri sorumlusuna başvurduğu tarihten itibaren 60 günlük süresinin bulunmadığı,
- İlgili kişi tarafından yapılan başvuruya veri sorumlusunca bir cevap verilmediği durumda ise ilgili kişinin veri sorumlusuna başvurduğu tarihten itibaren 60 gün içinde Kurula şikâyetle bulunabileceği,
- İlgili kişi tarafından yapılan başvuruya veri sorumlusunca Kanunda tanınan 30 günlük süre sonrasında bir cevap verilmesi halinde ilgili kişinin, Kanunda veri sorumlusuna tanınan 30 günlük süre sonrasında verilecek cevabı beklemekle yükümlü olmadığı ve veri sorumlusuna tanınan sürenin dolması ile birlikte Kurula şikâyetle bulunabileceği göz önüne alınarak, ilgili kişinin veri sorumlusunun kendisine cevap verdiği tarihten itibaren 30 gün değil, veri sorumlusuna başvurduğu tarihten itibaren 60 gün içinde Kurula şikâyetle bulunabileceği” belirtilmiştir.

Eğer bu inceleme sonucunda ortada yaygın bir ihlal olduğu tespit edilmişse, Kurul bir ilke kararı alır. İlke kararları yayımlanır. Ortada şayet telafisi güç veya imkânsız zararların olduğu ve açıkça hukuka aykırı bir durum söz konusu ise Kurul, veri işlenmesini ya da verinin yurt dışına aktarılmasını durdurabilecektir.

⁷⁹⁰ *Veri Sorumlusuna Başvuru ve Kurula Şikâyet Sürelerinin Hesaplanmasına İlişkin Kişisel Verileri Koruma Kurulunun 24.01.2019 tarih ve 2019/9 sayılı Kararı*, <https://www.kvkk.gov.tr/Icerik/5358/Kamuoyu-Duyurusu> , E.T. 27.04.2019.

Bu noktada üçüncü kurum ise “*Veri Sorumluları Sicili*”dir. Yukarıda görüldüğü üzere KVKK’ya göre, Sicil’in tutulmasını sağlamak Kurul’un görevleri arasında zikredilse de Sicil’i tutmakla görevli olan merci Başkanlık’tır. Bahis konusu Sicil’e, Kurum’un internet sayfası olan www.kvkk.gov.tr üzerinde, kısa adı VERBİS olan modülden başvuru yapılmaktadır. Söz konusu başvurular ve sorgulama işlemleri, 26 Nisan 2019 tarihinde internet sitesinde belirtildiği üzere, e-devlet üzerinden de yapılabilmektedir⁷⁹¹. Bu bağlamda veri işlemeye geçmeden önce, veri işleyecek olan gerçek ve tüzel kişiler VERBİS’e kayıt yaptırmak zorundadır. Kayıt yaptıracak gerçek ve tüzel kişiler bakımından bir ayrıma gidilmemiş, yalnızca Kurul tarafından bu zorunluluğa istisnalar tanınabileceği belirtilmiştir. Ancak istisnanın belirlenebilmesinde, işlenen kişisel verinin niteliği, sayısı, veri işlemenin kanundan kaynaklanması veya üçüncü kişilere aktarılma durumu gibi objektif kriterler göz önüne alınacaktır. İlaveten Kanun’un 28/2. maddesi doğrultusunda;

- Kişisel veri işlemenin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olduğu,
- İlgili kişinin kendisi tarafından alenileştirilmiş kişisel verilerin işlendiği,
- Kişisel veri işlemenin Kanun’un verdiği yetkiye dayanarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olduğu,
- Kişisel veri işlemenin bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olduğu,

durumlarda Veri Sorumluları Sicili’ne kayıt zorunluluğu bulunmamaktadır.

Kanun’un 16/3. maddesine göre, Veri Sorumluları Sicili’ne kayıt başvurusunda yapılacak bildirimde, veri sorumlusu ve varsa temsilcisinin kimlik ve adres bilgileri, veri işleme amacı, veri konusu olacak kişi grubu ve grupları ile bu kişilere ait veri kategorileri

⁷⁹¹ Kişisel Verileri Koruma Kurumu, “VERBİS Hizmetleri Artık e-Devlet Kapisında”, <https://www.kvkk.gov.tr/Icerik/5429/VERBIS-Hizmetleri-Artik-e-Devlet-Kapisinda> , E.T. 27.04.2019.

hakkındaki açıklamalar, verilerin aktarılabileceği alıcı veya alıcı grupları, yabancı ülkelere aktarımı öngörülen veriler, veri güvenliğine ilişkin alınan tedbirler ve verilerin işlendikleri amaç için gerekli olan azami süre mevcut olmalıdır. Bu hususlardan bir tanesinde dahi değişiklik söz konusu ise, derhal Başkanlık’a bildirilmelidir.

Veri Sorumluları Sicili’ne kayıt ile ilgili olarak uygulamada özellikle kimlerin bu yükümlülükten istisna tutulacağı hususu önem arzemiş ve bu bağlamda Kurul tarafından birçok karar hüküm altına alınmıştır. İlk olarak 2 Nisan 2018 tarihli “Veri Sorumluları Siciline Kayıt Yükümlülüğünden İstisna Tutulacak Veri Sorumluları ile ilgili 2018/32 Sayılı Karar”a bakıldığında, Kanun’un 16/2. maddesi uyarınca Sicil’e kayıttan müstesna tutulacak veri sorumluları belirtilmiştir⁷⁹². Buna göre;

- Herhangi bir veri kayıt sisteminin parçası olmak kaydıyla yalnızca otomatik olmayan yollarla kişisel veri işleyenler,
- Noterler,
- Dernek, vakıf ve sendikalardan yalnızca ilgili mevzuat ve amaçlarına uygun, faaliyet alanlarıyla sınırlı ve sadece kendi çalışanlarına, üyelerine, mensuplarına ve bağlılıklarına yönelik kişisel veri işleyenler,
- Siyasi partiler,
- Avukatlar,
- Serbest Muhasebeci Mali Müşavirler ve Yeminli Mali Müşavirler,

Veri Sorumluları Sicili’ne kayıt yükümlülüğünden muaftır. Bu listeye daha sonra 28 Haziran 2018 tarihinde başka bir kararla “Gümrük Müşavirleri”⁷⁹³, 5 Temmuz 2018

⁷⁹² Veri Sorumluları Siciline Kayıt Yükümlülüğünden İstisna Tutulacak Veri Sorumluları ile ilgili Kişisel Verileri Koruma Kurulunun 02/04/2018 Tarihli ve 2018/32 Sayılı Kararı, <https://www.kvkk.gov.tr/Icerik/4233/2018-32> , E.T. 27.04.2019.

⁷⁹³ Gümrük Müşavirlerinin Sicile Kayıt İstisnası Hakkında Görüş Talebi ile ilgili Kişisel Verileri Koruma Kurulunun 28/06/2018 Tarihli ve 2018/68 Sayılı Kararı, <https://www.kvkk.gov.tr/Icerik/5269/2018-68> , E.T. 27.04.2019.

tarihinde bir başka kararla “Arabulucular”⁷⁹⁴, 19 Temmuz 2018 tarihinde diğer bir kararla “Yıllık çalışan sayısı 50’den az ve yıllık mali bilanço toplamı 25 milyon TL’den az olan gerçek veya tüzel kişi veri sorumlularından ana faaliyet konusu özel nitelikli kişisel veri işleme olmayanlar”⁷⁹⁵ bakımından da istisna getirilmiştir. Ayrıca Kanun’un Geçici 1/2. maddesinde yer alan “*Veri sorumluları, Kurul tarafından belirlenen ve ilan edilen süre içinde Veri Sorumluları Siciline kayıt yaptırmak zorundadır.*” hükmü uyarınca Kurul, 19 Temmuz 2018 tarihinde meseleyi hüküm altına almıştır⁷⁹⁶. Bu karar doğrultusunda;

- Yıllık çalışan sayısı 50’den çok veya yıllık mali bilanço toplamı 25 milyon TL’den çok olan gerçek ve tüzel kişi veri sorumluları için Veri Sorumluları Sicili’ne zorunlu kayıt süresi *1 Ekim 2018 ile 30 Eylül 2019* tarihleri arasındadır.
- Yıllık çalışan sayısı 50’den az ve yıllık mali bilanço toplamı 25 milyon TL’den az olmakla birlikte ana faaliyet konusu özel nitelikli kişisel veri işleme olan gerçek ve tüzel kişi veri sorumluları için Veri Sorumluları Sicili’ne zorunlu kayıt süresi *1 Ocak 2019 ile 31 Mart 2020* tarihleri arasındadır.
- Yurtdışında yerleşik gerçek ve tüzel kişi veri sorumluları için Veri Sorumluları Sicili’ne zorunlu kayıt süresi *1 Ekim 2018 ile 30 Eylül 2019* tarihleri arasındadır.
- Kamu kurum ve kuruluşu veri sorumluları için Veri Sorumluları Sicili’ne zorunlu kayıt süresi *1 Nisan 2019 ile 30 Haziran 2020* tarihleri arasındadır.

b) Yaptırım Sistemi

Daha önce belirtildiği üzere, kişisel verilerin korunmasında esas olan önleyici korumadır. Veri koruması sağlanırken yaptırım bakımından KVKK kapsamında dikkate

⁷⁹⁴ Arabulucuların Veri Sorumluları Siciline Kayıt Zorunluluğundan İstisna Tutulması ile ilgili Kişisel Verileri Koruma Kurulunun 05/07/2018 Tarihli ve 2018/75 Sayılı Kararı, <https://www.kvkk.gov.tr/Icerik/5270/2018-75> , E.T. 27.04.2019.

⁷⁹⁵ Veri Sorumluları Siciline Kayıt Yükümlülüğünden İstisna Tutulacak Veri Sorumluları ile ilgili Kişisel Verileri Koruma Kurulunun 19/07/2018 Tarihli ve 2018/87 Sayılı Kararı, <https://www.kvkk.gov.tr/Icerik/5271/2018-87> , E.T. 27.04.2019.

⁷⁹⁶ Sicile Kayıt Yükümlülüğünün Başlama Tarihleri ile ilgili Kişisel Verileri Koruma Kurulunun 19/07/2018 Tarihli ve 2018/88 Sayılı Kararı, <https://www.kvkk.gov.tr/Icerik/5272/2018-88> , E.T. 27.04.2019.

alınaca üç usul; tazminat yolu ile hukuki yaptırım, kabahatler ve idari para cezaları ile idari yaptırım ve suç ve cezalar özelinde de cezai yaptırım sistemidir.

Tazminat hukuku bakımından incelenecek olursa, kişisel verilerin hukuka aykırı işlenmesi kişinin maddi ve manevi zarara uğramasına sebep olabilecektir. Bu noktada kişi, kişilik hakkı ihlali ile ilgili olarak ne zaman ve nasıl gerçekleşirse gerçekleşsin Türk Medeni Kanunu Genel Hükümler ve Borçlar Hukuku bağlamında her zaman tazminat talebinde bulunabilecektir⁷⁹⁷. Nitekim bu durum, KVKK'nın 14/3. maddesinde, kişilik hakları ihlal edilenlerin Genel Hükümler'e göre tazminat isteyebilecekleri biçiminde koruma altına alınmıştır. İlaveten yukarıda belirtildiği üzere, Kanun'un 11. maddesinde düzenlenen "İlgili Kişinin Hakları"ndan biri de verilerinin Kanun'a aykırı olarak işlenmesi halinde zarara uğramışsa bu zararın giderilmesini talep etmedir.

KVKK'nın 18. maddesi "Kabahatler" başlığını taşımaktadır. Kanun'un belli düzenlemelerinin ihlali halinde Kurul, belli oranlar arasında idari para cezalarına hükmedebilecektir. İdari para cezaları, veri koruma hukukunda en çok rastalanan yaptırım türüdür⁷⁹⁸ ve GVKT bakımından da daha önce belirtildiği üzere, miktarları artırılan bu cezalar oldukça önem arz etmektedir. Buna göre;

- Md. 10 bağlamında aydınlatma yükümlülüğünün ihlali halinde *5000 TL ile 100 000 TL* arasında,
- Md. 12 bağlamında veri güvenliğine ilişkin yükümlülüklerin ihlali halinde *15 000 TL ile 1 000 000 TL* arasında,
- Md. 15 bağlamında Kişisel Verileri Koruma Kurulu tarafından verilen kararların yerine getirilmemesi halinde *25 000 TL ile 1 000 000 TL* arasında,

⁷⁹⁷ AKSOY, *Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması*, s. 82- 83; Murat Volkan DÜLGER, *Bilişim Suçları*, Seçkin Yayınevi, Ankara, 2004, s. 265.

⁷⁹⁸ KÜZECİ, *Kişisel Verilerin Korunması*, s. 370.

- Md. 16 bağlamında Veri Sorumluları Sicili'ne kayıt ve bildirim yükümlülüğüne aykırı hareket halinde 20 000 TL ile 1 000 000 TL arasında değişen oranlarda idari para cezası verilebilecektir.

Görüleceği üzere anılan idari para cezaları arasındaki makas oldukça geniştir. Bunun sebebi Gerekçe'de açıklanmıştır. Buna göre Kurul karar verirken Kabahatler Kanunu'nun 17/2. maddesini esas alacaktır. Dolayısıyla Kurul idari para cezasına hükmederken, işlenen kabahatin haksızlık içeriği, failin kusuru ve ekonomik durumunu beraber değerlendirerek bir sonuca varacaktır. Bununla özellikle ekonomik olarak çok farklı seviyelerde olabilecek gerçek ve tüzel kişiler düşünülmüş ve şirketlerin ekonomik durumlarına göre bir belirleme yapılacağı belirtilmiştir. Bu her ne kadar yerinde bir tutum olarak değerlendirilebilirse de GVKT'nin 83. maddesinde olduğu gibi, para cezalarında alt ve üst sınırlara karar verilirken, şirketlerin yıllık cirosunun belli miktardaki yüzdelerini dikkate almak çok daha net karar verilmesini sağlayacaktır.

KVKK'nın idari para cezalarına ilişkin düzenlemesinde dikkat çeken bir diğer husus da yalnızca dört eylemle sınırlı tutulmasıdır. Buna göre, aydınlatma yükümlülüğünün ihlali, veri güvenliğine ilişkin yükümlülüklerin ihlali, Kişisel Verileri Koruma Kurulu tarafından verilen kararların yerine getirilmemesi ve Veri Sorumluları Sicili'ne kayıt ve bildirim yükümlülüğüne aykırı hareket söz konusu olduğunda idari para cezası seçeneği gündeme gelecektir. Buna göre anılan dört eylem dışında kalan bazı eylemler hakkında idari para cezasına hükmedilemeyecektir. Kanun'un 4. maddesinde yer alan temel ilkelere uygun hareket edilmediği, söz gelimi veri işlemenin meşru amaçla gerçekleşmediği ya da ölçüsüz biçimde yapıldığı gibi örneklerde idari para cezasına hükmedilemeyecektir.

İdari para cezası kararlarına karşı yargı yoluna gidilebilecektir. Bu cezalar yalnızca veri sorumlusu olan gerçek kişiler ile özel hukuk tüzel kişileri hakkında uygulanabilecektir. İdari para cezası gerektiren eylemler kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları bünyesinde işlenirse, Kurul'un yapacağı bildirim üzerine, ilgili kamu kurum ve kuruluşunda görev yapan memurlar ve diğer kamu

görevlileri ile kamu kurumu niteliğindeki meslek kuruluşlarında görev yapanlar hakkında disiplin hükümlerine göre işlem yapılacaktır ve sonuç Kurul'a bildirilecektir.

Son olarak KVKK'nın 17. maddesinde kişisel verilere ilişkin suçlar düzenlenmektedir. Bu bağlamda kişisel verilere dair gerçekleşen hukuka aykırılıklar bakımından 5237 Sayılı Türk Ceza Kanunu'nu (TCK) ile doğrudan bir bağlantı kurulmuştur. TCK bakımından “*Kişisel verilerin kaydedilmesi*” suçunun düzenlendiği 135. madde, “*Verileri hukuka aykırı olarak verme veya ele geçirme*” suçunun düzenlendiği 136. madde ve nitelikli hallerinin düzenlendiği 137. madde, “*Verileri yok etmeme*” suçunun düzenlendiği 138. madde, “*Tüzel kişiler hakkında güvenlik tedbiri uygulanması*” başlıklı 140. madde ve tüm bu suçların işlenmesi dolayısıyla tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerinin uygulanacağına dair 139. madde uygulama alanı bulacaktır⁷⁹⁹. TCK kapsamında düzenlenen suç tipleri, “*Kişisel verilerin kaydedilmesi*”, “*Verileri hukuka aykırı olarak verme veya ele geçirme*” ve “*Verileri yok etmeme*”dir. Bu suçlara bakıldığında, her birinin veri işleme kapsamında oldukları görülecektir. Öte yandan KVKK bakımından veri işleme, verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi kapsamaktadır. Bu bakımdan TCK'da yer alan suçlardan çok daha fazla ve farklı ihtimalle veri işlenmesi mümkündür. Ancak suçta ve cezada kanunilik ve kıyas yasağı sebebiyle TCK'da belirtilen haller dışında bir suç ihdası mümkün görünmemektedir⁸⁰⁰.

TCK'nın 135/2. maddesine göre;

“Kişisel verinin, kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel

⁷⁹⁹ Suç tiplerine ilişkin detaylı bir anlatım için bkz. Murat Volkan DÜLGER, *Kişisel Verilerin Korunması Hukuku*, Hukuk Akademisi, İstanbul, 2019, 309- 370.

⁸⁰⁰ Aynı yönde bkz. KÜZECİ, *Kişisel Verilerin Korunması*, s. 376.

yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması durumunda birinci fıkra uyarınca verilecek ceza yarı oranında artırılır.”

Bu durum, verileri hukuka aykırı olarak verme veya ele geçirme suç tipinin nitelikli halidir. Görüleceği üzere burada belirtilen bazı veriler, hassas veri niteliğini haizdir. Ancak KVKK'nın 6/1. maddesinde ele alınan özel nitelikli verilerle örtüşmemektedir. Bu bakımdan da söz konusu suç tipinin KVKK'da yer alan bazı hassas verileri için uygulanırken, bazılarına uygulanmayacağı gibi bir sonuç ortaya çıkmaktadır⁸⁰¹.

KVKK'da yer alan yaptırım sistemi bu şekilde olmakla beraber görülmektedir ki belli alanlarda yeterli olamamaktadır. Özellikle idari para cezaları açısından dile getirildiği üzere, miktarlar arası makas oldukça geniştir. Her ne kadar bunun sebebi olarak Kabahatler Kanunu'nun 17/2. maddesinin esas alınacak olmasını gösterse de alt ve üst sınırlara karar verilirken, şirketlerin yıllık cirosuna dair bir belirleme yapılması daha olumlu bir yöntem olabilirdi. Ayrıca bu noktada KVKK'nın idari para cezalarına ilişkin düzenlemesinde ele alınması gereken bir diğer husus da idari para cezası verilecek hallerin yalnızca aydınlatma yükümlülüğünün ihlali, veri güvenliğine ilişkin yükümlülüklerin ihlali, Kişisel Verileri Koruma Kurulu tarafından verilen kararların yerine getirilmemesi ve Veri Sorumluları Sicili'ne kayıt ve bildirim yükümlülüğüne aykırı hareket biçimindeki dört eylemle sınırlı tutulmasıdır. Bu dört eylem dışında kalan eylemler hakkında idari para cezasına hükmedilemeyecektir.

KVKK'nın yaptırım sisteminde dile getirilen suçlar bakımından da belirtildiği üzere Kanun'a göre, TCK'da yer alan suç tiplerinden çok daha fazla ve farklı ihtimallerle veri işlenmesi mümkündür. Ancak suçta ve cezada kanunilik ve kıyas yasağı sebebiyle TCK'da belirtilen haller dışında hukuka aykırı veri işlenmesi durumunda ceza hukuku alanına girilemeyecektir. Bu ise açıktır ki veri işlemeye dair somut olaylar bakımından eksik ve adaletsiz durumlar doğurabilecektir. Yine TCK bakımından bir diğer önemli

⁸⁰¹ Aynı yönde bkz. KÜZECİ, *Kişisel Verilerin Korunması*, s. 376.

eksiklik ise, 135/2. maddede verileri hukuka aykırı olarak verme veya ele geçirme suç tipinin nitelikli hali bakımından karşımıza çıkmaktadır. Bu fıkrada bazı hassas veriler bahis konusu olmaktadır. Oysa bu hassas veriler, KVKK'nın 6/1. maddesinde ele alınan özel nitelikli verilerle örtüşmemektedir. Bu bakımdan da söz konusu suç tipinin KVKK'da yer alan bazı hassas verileri için uygulanırken, bazılarına uygulanmayacağı gibi bir sonuç ortaya çıkmaktadır, ki bu durum da tıpkı az önce belirtilen örnek de olduğu gibi, hassas verilere dair somut olaylar bakımından tutarsız ve adaletsiz durumlara sebebiyet verebilecektir.

KVKK'da yer alan tüm bu yaptırım türlerine yakından bakıldığında son olarak belirtilmelidir ki, kişisel verilerin korunması hukuku alanında esas olan önleyici yaptırımlardır; fakat Kanun'da düzenlenen bu sistem zarar gerçekleşmeden önce değil, gerçekleşikten sonra devreye girmektedir⁸⁰².

II. İLGİLİ ANAYASAL İÇTİHAT

Kişisel verilerin korunması hakkı ve ilgili olan diğer temel hak ve özgürlüklerin anayasal görünümü yukarıdaki biçimdedir. Ancak bu anayasal hakkın anayasa yargısındaki uygulaması için Anayasa Mahkemesi'nin konuyla ilgili kararlarını incelemek yerinde olacaktır. Bu bakımdan öncelikle AYM'nin Genel Kurul kararlarının (iptal ve itiraz yolları) özel hayatın gizliliği ve sonrasında kişisel verilerin korunması hakları bağlamında 1979'dan günümüze değin değişimi ele alınacak ve başta özel hayatın gizliliği olmak üzere temel hak ve özgürlüklerin sınırlandırılmasında esas alınan yöntem ve güvencelere göre bir ayrıma gidilecektir (kanunilik, nedene bağlılık, ölçülülük). Devamında aynı ayrım takip edilerek kişisel verilerin korunması hakkının Eylül 2012'den bu yana AYM'nin bireysel başvuru kararlarındaki görünümü, bazı önemli kararlara değinilerek ortaya konulmaya çalışılacaktır.

⁸⁰² Aynı yönde bkz. ÇEKİN, “6698 sayılı Kişisel Verilerin Korunması Kanunu’nun Big Data (Büyük Veri) ve İrade Serbestisi Açısından Değerlendirilmesi”, *İÜHFM*, s. 636- 638.

A. KANUNİLİK VE ÖZELLİKLE VERİ İŞLEMENİN KANUNİLİĞİ

1982 Anayasası'nın 20. maddesinin 3. fıkrasında kişisel verilerin korunması hakkına ilişkin özel bir kanun kaydı konulmuştur. Bu düzenlemeye göre; “*Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir.*” Bunun anlamı, veri işleme hallerinin neler olacağı ancak kanunda gösterilebilecektir. Daha farklı bir deyişle, kişisel verilerin işlenmesi kanunilik prensibi ışığında gerçekleştirilebilecektir.

Bu madde ile “*verilerin işleme hallerinin neler olacağının kanunda gösterilmesi*” zorunluluğunun öngörülmesi, kanunilik standardını diğer tüm ölçütlerin önüne geçirmiştir. Dolayısıyla ölçülülük ve hakkın özü ilkeleri de kanunilik ilkesiyle korunabilir hale gelmiştir denebilecektir. Ancak yine de belirtmek gerekir ki Anayasa hükmü yalnızca Kişisel Verilerin Korunması Kanunu'nun yürürlüğe girmesi şartına indirgenmemelidir. Anılan Kanun yürürlükte olsa da olmasa da esas olan, konuya dair tüm düzenlemelerde temel hak ve özgürlük güvencelerinin mevcudiyetidir⁸⁰³.

Anayasal devlet, temel hak ve özgürlükleri en üst düzeyde korumakla yükümlüdür. Bu bağlamda temel hak ve özgürlüklerin sınırlandırılmasında her ne kadar ortak kesin bir kural olmasa da demokrasi ile yönetilen ülkelerin anayasalarında bazı ölçütlerde uzlaşa sağlanmıştır⁸⁰⁴.

1982 Anayasası bakımından ise temel hak ve özgürlüklerin sınırlanması rejiminin bel kemiği 13. maddedir. 2001 yılında yapılan değişiklikle madde genel bir güvence hükmü haline gelmiş ve temel hak ve özgürlüklerin sınırlandırılmasında kademeli sisteme geçilmiştir. Bu sistem basit yasa kaydı, nitelikli yasa kaydı ve yasa kaydı öngörülme haklar şeklindedir⁸⁰⁵. Basit yasa kaydı içeren bazı hak ve özgürlüklerde sadece kanun ile

⁸⁰³ Elif KÜZECİ, *Kişisel Verilerin Korunması*, 3. Baskı, Turhan Kitabevi, Ankara, 2019, s. 294.

⁸⁰⁴ Sibel İNCEOĞLU, “Hak ve Özgürlükleri Sınırlama ve Güvence Rejimi”, *İnsan Hakları Avrupa Sözleşmesi ve Anayasa*, Ed. Sibel İNCEOĞLU, Avrupa Konseyi, 2013, Ankara, s. 23, ss. 23- 52.

⁸⁰⁵ Temel hak ve özgürlüklerin sınırlandırılmasında kademeli sistemin ele alındığı ilk temel eser olarak bkz. SAĞLAM, *Temel Hakların Sınırlanması ve Özü*, Ankara Üniversitesi Siyasal Bilgiler Fakültesi Yayınları: 506, S.B.F. İnsan Hakları Merkezi Yayınları: 4, Ankara, 1982.

sınırlama yapılabileceği belirtilerek başka hiçbir sınırlama sebebi öngörülmemiştir. Böylece kanun koyucuya genel bir sınırlama yetkisi verilmiştir. Nitelikli yasa kaydı içeren temel hak ve özgürlükler bakımından ise sınırlama sebepleri tahdidi olarak belirtilerek söz konusu temel hak ve özgürlüğün ancak o sebeplerle sınırlanabilmesi kabul edilmiştir. Yasa kaydı öngörülmeyen temel hak ve özgürlükler bakımından ise açıktır ki hiçbir sınırlama yetkisi verilmemiştir. Dolayısıyla bu temel hak ve özgürlükler ilke olarak sınırlandırılmaz⁸⁰⁶.

Temel hak ve özgürlüklerin kanunla sınırlanması bu bakımdan oldukça önemli bir role sahiptir. İç hukukta kanun kavramı daha ziyade şekli anlamda kullanıldığı için sınırlamanın seçilmiş bir organ tarafından yapılması durumu mümkün olmaktadır. Bu bakımdan sınırlama çok sesli bir biçimde gerçekleştirilir ve yalnızca yürütmenin tekeline bırakılmaz. Ayrıca kanunilik sayesinde sınırlama erişilebilir, öngörülebilir ve kesin olmakta ve bu sayede hukuki belirlilik ile hukuk güvenliği de sağlanmaktadır⁸⁰⁷.

Uluslararası düzenlemelerden söz gelimi İHAS, 8- 11. maddelerinde bulunan düşünce ve ifade özgürlüğü, din ve vicdan hürriyeti, özel yaşam, aile yaşamı ve haberleşme özgürlüğü gibi temel hak ve özgürlüklerin de kanunlarda belirtilen şartlarla ve ancak kanunla sınırlanabileceğini düzenlemektedir⁸⁰⁸. Bu noktada kişisel verilerin korunması hakkı da bu kapsamda ele alınmaktadır.

Temel hak ve özgürlüklerin sınırlandırılmasında yasamanın rolü oldukça önemlidir, ancak yeterli değildir. Çünkü yasama da hak ve özgürlükleri gereğinden fazla sınırlayabilme ya da idareye sınırsız yetki verme eğilimi gösterebilmektedir. Dolayısıyla kanun koyucuya verilen temel hak ve özgürlükleri sınırlama yetkisinin ancak belli

⁸⁰⁶ SAĞLAM, *Temel Hakların Sınırlanması ve Özü*, s. 99- 108; İNCEOĞLU, “Hak ve Özgürlükleri Sınırlama ve Güvence Rejimi”, s. 24.

⁸⁰⁷ İNCEOĞLU, “Hak ve Özgürlükleri Sınırlama ve Güvence Rejimi”, s. 25; Hukuk devleti ilkesinin temel unsurlarından biri olan hukuki belirlilik ilkesine ilişkin detaylı bir çalışma olarak bkz. Selda ÇAĞLAR, *Hukuk Devletin Hukuki Belirlilik İlkesi Üzerinden Değerlendirilmesi*, Beta, 2013.

⁸⁰⁸ HARRIS, O’BOYLE, WARBRICK, *Law of the European Convention on Human Rights*, s. 344.

nedenlere dayalı olarak kullanılabilmesi de önemli bir güvence ölçütü olarak karşımıza çıkmaktadır⁸⁰⁹.

Bu bağlamda kişisel verilerin korunması hakkı bağlamında ele alınacak ilk karar, AYM'nin 6 Ocak 1999 tarihli kararı⁸¹⁰ olan ve 1774 sayılı Kimlik Bildirme Kanunu'na getirilen, Kanun'un 2. maddesinde sayılan özel veya resmi her türlü konaklama tesislerinden Bakanlıkça belirlenenlerin ilan tarihinden itibaren üç yıl içindeki tüm kayıtlarını bilgisayarlarında tutmak ve bilgisayar terminallerini kolluk kuvvetlerinin bilgisayarlarına bağlamak suretiyle kendilerindeki kişisel verileri kolluk kuvvetleri ile paylaşmalarına ilişkin kanun maddesine ilişkindir. Bu maddenin 1982 Anayasası'nın 20. maddesinde yer alan "Özel hayatın gizliliği" hakkına aykırılık oluşturması sebebiyle düzenlemenin iptali ve yürürlüğünün durdurulması talep edilmiştir.

Anayasa Mahkemesi bu kararda,

"...Vatandaşın seyahat, dilediği yerde oturma ve dilediği alanda çalışma hürriyeti Anayasa ile sağlanmış temel haklardan olmakla beraber kamu güvenliğini ve düzenini sağlamakla görevli Devlet örgütlerinin bu konuda bazı bilgilere sahip olması gerektiği ve bunun büyük önemi çok açık bir gerçektir. Esasen bu bilgilerin toplanmasını sağlamak maksadıyla Anayasa'ya uygun olarak alınacak kanuni tedbirlerin yukarıda sözü edilen temel hakların özü ile doğrudan doğruya bir ilgisi de bulunmamaktadır."

diyerek söz konusu düzenlemenin özel hayatın gizliliği hakkının kullanılmasını imkansızlaştırmadığı ya da zorlaştırmadığını belirtmiştir. Ayrıca,

"...temel hak ve hürriyetlerin, Devletin ülkesi ve milletiyle bölünmez bütünlüğünün, millî egemenliğin, Cumhuriyetin, millî güvenliğin, kamu düzeninin, genel asayişin, kamu yararının, genel ahlâkın ve genel sağlığın korunması amacı ile ve ayrıca Anayasanın ilgili maddelerinde öngörülen özel sebeplerle, Anayasanın sözüne ve ruhuna uygun olarak kanunla sınırlanabileceği, bu sınırlamaların demokratik toplum düzeninin gereklerine aykırı olamayacağı, öngörüldükleri amaç dışında kullanılamayacağı, maddede yer alan genel sınırlama sebeplerinin temel hak ve hürriyetlerin tümü için geçerli olduğu..."

⁸⁰⁹ AKAD, VURAL DİNÇKOL, BULUT, *Genel Kamu Hukuku*, s. 308.

⁸¹⁰ AYM E. 1996/68, K. 1999/1, K.T. 06.01.1999.

belirtilerek “*dava konusu kuralın, kamu düzeni, genel asayiş ve kamu yararını sağlama amacına yönelik olması ve demokratik toplum düzeninin gereklerine de aykırı bir yönü bulunma...*”dışından bahisle iptal istemini reddetmiştir. AYM kararda genel olarak detaylı bir analiz yapmaksızın milli güvenlik, kamu düzeni ve kamu yararı nedenleri ile özel hayatın gizliliği hakkına yapılan sınırlamanın hangi bakımlardan demokratik toplum düzeninde gerekli olduğunu ortaya koymamıştır.

Görüldüğü üzere bu hüküm, kolluk kuvvetlerinin bilgisayarlarında kişisel bilgilerin toplanması yetkisini ele almaktadır; ancak bu yetki kullanılırken hangi kurallara uyulması gerektiği belirtilmemiştir. Belirtildiği üzere, anayasal bir devlette esas olan, temel hak ve özgürlüklerin sınırlandırılmasının yasama organınca ve kanunla gerçekleştirilmesidir. Bu durum kanunilik ilkesinin bir gereğidir. Fakat 1774 Sayılı Kimlik Bildirme Kanunu’nda yer alan bu düzenlemede kişisel verilerin toplanması esnasında uyulması gereken hususlar mevcut değildir ve bu sebeple kanunilik bakımından da eksiklik teşkil etmektedir.

1774 sayılı Kimlik Bildirme Kanunu’nun genel gerekçesine bakıldığında;

"Demokratik idare tarzına sahip Batı memleketlerinde de çeşitli şekillerde uygulandığı bilinen kimlik bildirme sisteminin tesisi ile elde edilecek bilgiler, kolluk hizmetlerinin yürütülmesinde büyük faydalar sağlayacağı gibi, kamu hizmetlerini ifa eden diğer kuruluşlar için de gerektiğinde yararlanılacak değerli bir kaynak olacaktır."

ifadesi göze çarpmaktadır. Bu ifade oldukça genel ve veri işlemenin amacını spesifik biçimde ortaya koymamaktadır. KVKK’nın 4. maddesinde yer alan, kişisel verilerin işlenmesinde uyulması gereken ilkeler ışığında 1774 sayılı Kimlik Bildirme Kanunu’na getirilen düzenleme, kolluk kuvvetlerine verdiği geniş yetkinin hangi amaçlarla, hangi veriler kapsamında, ne kadar süre ile olacağı gibi hususları belirtmemektedir. Bu ise doğrudan kanunilik ilkesini zedeleyici bir görünüm arz etmekte ve kişisel verilerin hukuka aykırı biçimde kayıt altına alınmasına sebep olan bir düzenleme teşkil etmektedir.

Anayasa Mahkemesi'nin 20 Mart 2008 tarihli ve veri koruma hukuku ile ilgili bir diğer kararı⁸¹¹ ise 5429 sayılı Türkiye İstatistik Kanunu'nun istatistiksel birimlerinin⁸¹² kendilerinden istenen verileri vermekle yükümlü olduklarına ilişkin düzenlemesinin iptali istemidir. Anılan Kanun'un 8. maddesi, *"İstatistiksel birimler kendilerinden istenen veri veya bilgileri başkanlığın belirleyeceği şekil, süre ve standartlarda eksiksiz ve doğru olarak ücretsiz vermekle yükümlüdür"* şeklindedir. Görüleceği üzere bu maddede söz konusu veri veya bilgilerin kime verileceği de belirtilmemiştir. Aynı Kanun'un 54/2. maddesi ise, Başkanlık veya kurum ve kuruluşlar tarafından program kapsamında istenen bilgileri geçerli bir mazeret olmaksızın belirlenen şekil ve sürede vermeyen veya eksik veren veya hatalı verenler hakkında gerçekleştirilecek yaptırımları (uyarma ve idari para cezası) düzenlemektedir. AYM'ye göre,

"Maddede açıklayıcı bir düzenleme bulunmadığı için, "kişisel veri" veya "isteme bağlı veri" olarak adlandırılan, belirli veya belirlenebilir kişilerle ilgili her türlü bilgilerin istenebileceği kuşkusuzdur.

İstatistiksel birimlerin kendilerinden istenen bilgileri belirlenen şekil ve sürede eksiksiz ve hatasız olarak vermek zorunluluğuna uyulmaması idari para cezası yaptırımına bağlanmış olmasına karşın, istenilecek veri ve bilgilerin kapsamı ya da sınırlarının ne/neler olacağına, başka bir anlatımla, temel hak ve özgürlüklere müdahale niteliğinde olan veri ve bilgilerin bu zorunluluk kapsamında bulunup bulunmadığına ilişkin herhangi bir düzenlemeye rastlanmamaktadır. Dolayısıyla, istatistiksel birimler kendilerinden istenildiği takdirde her türlü bilgiyi temel hak ve özgürlüklerine müdahale niteliğinde olsa bile vermek zorundadırlar.

Anayasa'nın ...20. madde gerekçesinde, özel hayatın korunmasının her şeyden önce bu hayatın gizliliğinin korunması, resmi makamların özel hayata müdahale edememesi anlamına geldiği belirtilmiştir.

AİHM kararlarında da belirtildiği gibi, özel hayat bütün unsurlarıyla tanımlanamayacak kadar geniş bir kavram olup devletin yetkili temsilcileri tarafından ilgililer hakkında rızası olmaksızın bilgi

⁸¹¹ AYMK E. 2006/ 167, K. 2008/86, K.T. 20.03.2008.

⁸¹² *İstatistiksel Birimler*: "Haklarında veri toplanacak gerçek ve tüzel kişiler ile kurum ve kuruluşları ifade etmektedir." Tanım için bkz. KÜZECİ, *Kişisel Verilerin Korunması*, 3. Baskı, s. 292.

toplamasının her zaman söz konusu kişinin özel hayatını ilgilendireceği kuşkusuzdur.

Anket formlarında yer alan bazı sorular özel yaşamın gizliliği ile düşünce ve kanaatin açıklanması sonucunu doğurabilir. Bir ülkede en güçlü veri tekeli idaredir. Bu gücün sınırlandırılması özel yaşamın ve düşünce ve kanaat özgürlüğünün korunması bakımından önemlidir.

Anayasa'nın 20. ve 25. maddelerinde yer alan güvencelere rağmen itiraza konu 8. madde hükmüyle kişiler, bilgi toplama, saklama, işleme ve değiştirme tekeli olan idareye ve diğer kişilere karşı korumasız bırakılmış, veri toplamının sınırlarına yasal düzenlemede yer verilmemiştir.”

Görüldüğü üzere AYM itiraz konusu kuralları, 1982 Anayasası'nın 20. ve 25. maddeleri uyarınca incelemiş ve anılan düzenlemelerin bu maddelere aykırı olduğuna karar vererek iptal etmiştir. Öncelikle belirtilmelidir ki AYM bu kararla kişisel veri kavramını, “belirli veya belirlenebilir kişilerle ilgili her türlü bilgi” olarak tanımlamıştır. Ayrıca kararın oldukça önemli bir noktası da en güçlü veri tekelinin idarede olduğunun ve bunun sınırlandırılması gereğinin vurgulanmasıdır. Bahis konusu düzenleme ile idareye sınırsız veri toplama tekelinin verilmesi ve bu konuda herhangi bir sınırın belirlenmemiş olması da özel yaşamın gizliliği ile düşünce ve kanaat hürriyetinin ihlali olarak değerlendirilmiştir. Kararda bir karşı oy bulunmakta ve bu karşı oy, veri koruma hukuku bakımından oldukça sorunlu bir anlayışı ortaya koymaktadır. Karşı oya göre,

“Özel hayata ilişkin soruların tanımlanamayacak kadar geniş olması, ekonomik, sosyal ve siyasal alanlara ilişkin bilgi ve verilerinde kapsamının büyüklüğü gözetildiğinde, belirtilen konularda yasal sınırlamalar getirilmesinin imkansızlığı ortadadır.”

Bu kararı 6698 sayılı KVKK bağlamında değerlendirecek olursak, Kanun kapsamında istatistiksel birimlerden istenilecek veri ve bilgilerin kapsamının belirsizliği KVKK'nın 4. maddesinde ele alınan kişisel verilerin işlenmesinde uyulacak ilkelere, özellikle “Belirli, açık ve meşru amaçlar için işlenme” ile “İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma” ilkelerine ve dolayısıyla kanunilik ilkesine aykırılık teşkil etmektedir.

Mahkeme'nin, 2010 Değişiklikleri'nden sonra vermiş olduğu 14 Şubat 2013 tarihli bir başka kararı⁸¹³ da hassas veri (özel nitelikli kişisel veri)lerden olan sağlık verilerine ilişkindir. Söz konusu karar, 663 sayılı Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname'nin bazı maddelerinin Anayasa'ya aykırılıkları iddiasıyla iptaline yöneliktir. Anılan KHK'nın 16. maddesinde, Rehberlik ve Teftiş Başkanlığı düzenlenmiştir. Maddenin ikinci fıkrası, denetime tâbi olan gerçek ve tüzel kişilere, gizli dahi olsa bütün belge, defter ve bilgilerin talep edilmesi durumunda ibraz etme, para ve para hükmündeki evrakı ve ayniyatı ilk talep hâlinde gösterme, sayılmasına ve incelenmesine yardımcı olma ödevini yüklenmiştir. Mahkeme bu hükmü;

“Anayasa'nın 'Özel Hayatın Gizliliği' başlıklı 20. maddesinin birinci fıkrasında, ‘... Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.’ denilmiştir. Buna göre, Anayasa'nın 20. maddesinde düzenlenen ve 'Kişinin Hakları ve Ödevleri' başlıklı ikinci bölümünde yer alan özel hayatın gizliliği ve kişisel verilerin korunması hakkına ilişkin olarak kanun hükmünde kararname ile düzenleme yapılması mümkün değildir.

KHK'nın 16. maddesinin (2) numaralı fıkrasının birinci cümlesiyle gerçek kişilerin gizli bilgilerinin sağlık denetçilerine ibrazı zorunluluğunun getirilmiş olması, özel hayatın gizliliği ve kişisel verilerin korunması hakkına ilişkin bir düzenleme niteliğindedir. Dolayısıyla kural, Anayasa'nın 91. maddesinin birinci fıkrasına aykırıdır.”

diyerek iptal etmiştir.

Kişisel verilerin korunması hakkıyla ilgili 9 Nisan 2014 tarihli bir başka AYM kararı⁸¹⁴ ise, 5809 sayılı Elektronik Haberleşme Kanunu'nun 51. maddesinin Anayasa'nın 2., 7., 13. ve 20. maddelerine aykırılığı iddiasıyla iptal edilmesi ve yürürlüğünün durdurulmasına karar verilmesi istemlidir. İlgili Kanun maddesi, “*Kurum, elektronik*

⁸¹³ AYMK E. 2011/150, K. 2013/30, K.T. 14.02.2013.

⁸¹⁴ AYMK E.2013/122, K. 2014/74, K.T. 09.04.2014.

haberleşme sektörüyle ilgili kişisel verilerin işlenmesi ve gizliliğinin korunmasına yönelik usul ve esasları belirlemeye yetkilidir." biçimindedir. Bu madde ile Bilgi Teknolojileri ve İletişim Kurumu'nun elektronik haberleşme sektörüyle ilgili kişisel verilerin işlenmesi ve gizliliğinin korunmasına yönelik usul ve esasları belirlemeye yetkili olduğu hükme bağlanmıştır. Kararın önemli bir noktası, kişisel veri kavramının kapsamlı bir tanımı yapılarak önemini ortaya koymasıdır. Kararda yer alan tanıma göre,

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

Bu karar, 2010 Anayasa Değişiklikleri sonrası kişisel verilerin korunması hakkını ismen bahis konusu eden kararlardan biri olarak hakkın insan onurunun korunması ile kişiliğin serbestçe geliştirilmesi hakkının özel bir biçimi olduğu vurgusunu yapmıştır. Söz konusu düzenleme, bir yürütme organı olarak Bilgi Teknolojileri ve İletişim Kurumu'na verdiği yetki ile göze çarpmaktadır. Karara göre;

"Yasama yetkisinin devredilemezliği ilkesi gereğince, Anayasa'nın açıkça kanunla düzenlenmesini öngördüğü konularda yürütme organına doğrudan ve ilk elden düzenleyici işlem yapma yetkisi verilemez. Elektronik haberleşme sektörüyle ilgili kişisel verilerin işlenmesi ve gizliliğinin korunmasına yönelik usul ve esasları belirleme yetkisini Bilgi Teknolojileri ve İletişim Kurumuna veren itiraz konusu kural, Anayasa'nın 20. maddesinde öngörülen kişisel verilerin korunmasına ilişkin usul ve esasların ancak kanunla düzenlenebileceğine ilişkin güvenceye aykırıdır."

Böylece, 1982 Anayasası'nın 20/3. maddesinde açık bir şekilde düzenlendiği üzere, kişisel verilerin korunması hakkının ancak kanunla sınırlandırılabilceği bir kez de AYM kararı ile vurgulanmış olmaktadır. Kaldı ki kişisel verilerin korunmasına dair usul ve esasları düzenleyen 6698 sayılı KVKK, ancak 7 Nisan 2016'da yürürlüğe girmiştir.

2 Ekim 2014 tarihli bir diğer AYM kararında⁸¹⁵, 6552 sayılı İş Kanunu ile Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılması ile Bazı Alacakların Yeniden Yapılandırılmasına Dair Kanun'un 126. ve 127. maddeleri ile değiştirilen 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un 3. ve 8. maddelerinin Anayasa'ya aykırılığı iddiasıyla iptali istenmektedir. 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un 3/4. maddesi; *"Trafik bilgisi Telekomünikasyon İletişim Başkanlığı tarafından ilgili işletmecilerden temin edilir ve hâkim tarafından karar verilmesi hâlinde ilgili mercilere verilir."* biçimindedir. Kanun'un 8. maddesi ise, *"Erişimin engellenmesi kararının gereği, derhal ve en geç kararın bildirilmesi anından itibaren dört saat içinde yerine getirilir (önceki düzenleme yirmi dört saat idi)."* şeklinde değiştirilmiştir.

6552 Sayılı Kanun'un 127. maddesiyle değiştirilen 5651 Sayılı Kanun'un 3/4. maddesinin incelenmesinde Mahkeme,

"Kişisel verilerin korunmasını isteme hakkına sağlanan anayasal güvencenin yaşama geçirilebilmesi için, bu hakkı ilgilendiren yasal düzenlemelerin, açık, anlaşılabilir ve kişilerin söz konusu haklarını kullanabilmelerine elverişli olması gerekir..."

Dava konusu kuralda geçen trafik bilgisi, 5651 sayılı Kanun'un 2. maddesinin (j) bendinde, taraflara ilişkin IP adresi, verilen hizmetin başlama ve bitiş zamanı, yararlanılan hizmetin türü, aktarılan veri miktarı ve varsa abone kimlik bilgileri şeklinde tanımlanmıştır. Dolayısıyla trafik bilgisi adı altında istenen bilgiler genel anlamda belirli veya kimliği belirlenebilir olmak şartıyla, bir kişiye ilişkin bütün bilgileri ifade eden kişisel veri kavramı içerisindedir. Kişisel verilerin korunması hakkı, kişinin insan onurunun korunmasının ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak, bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır..."

⁸¹⁵ AYMK E. 2014/149, K. 2014/151, K.T. 02.10.2014.

Dava konusu kural, yukarıda belirtilen kişisel veri niteliğinde olan ve ciddi suçların tespiti, soruşturulması ve kovuşturulmasında kullanılmak üzere gerçek ve tüzel kişilere ilişkin trafik bilgisinin, işlenmemiş veri hâlinde süreli olarak muhafaza edildiği erişim veya yer sağlayıcılardan, TİB tarafından herhangi bir gerekçe veya neden göstermeksizin temin edilmesine olanak sağlamaktadır. Söz konusu verilere ulaşılabilirlik, kişilerin tercihleri, düşünceleri ve davranışları hakkında fikir verebileceğinden kişilerin özel hayatlarına müdahale edilme riskini içermektedir. Kuralda, temin edilecek bilgiyle ilgili olarak herhangi bir konu ve amaç sınırlaması bulunmadığı gibi bilginin kapsamı, ne şekilde kullanılacağı, tutulacağı süre, temin edilme gerekçesi gibi hususlarla ilgili olarak da herhangi bir belirlilik bulunmamaktadır.

Anayasa'nın 20. maddesi, kişisel verilerin korunmasını isteme hakkına sağlanan anayasal güvenceyi, kişisel verilerin ancak kanunda öngörülen hâllerde veya kişinin açık rızasıyla işlenebileceği şeklinde belirtmiştir. Dolayısıyla bu hakkı ilgilendiren yasal düzenlemelerin, çerçevesi çizilmiş, açık, anlaşılabilir, kişilerin söz konusu haklarını kullanabilmelerine elverişli ve özel hayatlarını ilgilendiren veri, bilgi ve belgelerin resmi makamların keyfi müdahalelerine karşı korunmasını olanaklı hâle getirilmesi gerekmektedir. Bu durumda, verilerin işlenebileceği hâllerin kanunda açıkça yer alması zorunluluğu bulunmasına karşın, kuralda herhangi bir belirleme ve sınırlama yapılmaksızın doğrudan kişisel veri niteliğindeki trafik bilgisinin temin edilmesine ve işlenmesine olanak sağlanmasının bu yönüyle Anayasa'nın 20. maddesine aykırı olduğu açıktır.”

biçiminde ifade etmiştir.

Kişisel verilerin korunması hakkını ilgilendiren kanuni düzenlemelerin hangi ilkeler doğrultusunda hazırlanması gerektiği detaylı biçimde belirtilmiştir. Oysa söz konusu maddeye getirilen düzenlemeye bakıldığında yalnızca, kişisel veri olan internet trafik bilgisinin Telekomünikasyon İletişim Başkanlığı (TİB) tarafından temin edilmesi hususu belirtilmekte; fakat bu verilerin ne şekilde, hangi yolla, ne sürede vs. elde edileceği gibi hususlarında kanun sessiz kalmaktadır. Bu bakımdan ilgili hükmün hukuki belirlilikten yoksun olduğu açıktır. Kişisel veri teşkil eden söz konusu trafik verilerinin kapsamı, ne şekilde kullanılacağı, tutulacağı süre, temin edilme gerekçesi gibi hususların

belirsizliği, yürürlükteki hukukun bilinemezliğine sebep olabilecektir⁸¹⁶. Dolayısıyla söz konusu verilerin TİB tarafından herhangi bir kanunun öngörmüş olduğu kurala tabi olmadan istenildiği zaman ve biçimde elde edilebilmesi doğrudan Anayasa'nın 20/3. maddesinde yer alan kişisel verilerin korunması hakkına aykırıdır.

Bunun yanı sıra 1982 Anayasası'nın 15. maddesinde “*Temel hak ve hürriyetlerin kullanılmasının durdurulması*” düzenlenmektedir. Bu maddenin ikinci fıkrasına göre,

“Birinci fıkra da belirlenen durumlarda da, savaş hukukuna uygun fiiller sonucu meydana gelen ölümler (...) dışında, kişinin yaşama hakkına, maddi ve manevi varlığının bütünlüğüne dokunulamaz; kimse din, vicdan, düşünce ve kanaatlerini açıklamaya zorlanamaz ve bunlardan dolayı suçlanamaz; suç ve cezalar geçmişe yürütülemez; suçluluğu mahkeme kararı ile saptanıncaya kadar kimse suçlu sayılamaz.”

Bu düzenlemede güvence altına alınan haklar “sert çekirdek haklar”dır. Karara konu olan internet trafik bilgisinin Telekomünikasyon İletişim Başkanlığı (TİB) tarafından temin edilmesi ve fakat bu verilerin ne şekilde, hangi yolla, ne sürede vs. elde edileceği gibi hususların belirsizliği ise 15/2. maddede ele alınan, özellikle din, vicdan, düşünce ve kanaat hürriyetlerinin zaruri olarak açıklanmaları gibi sonuçlar doğurabilecektir. Bu ihtimalde ise düzenlemenin çekirdek alana dokunduğundan söz edilecek ve iptali gerekecektir.

Ceza mevzuatında kişisel veri kavramının içeriğine dair 12 Kasım 2015 tarihli AYM kararına⁸¹⁷ bakıldığında ise, 5237 sayılı Türk Ceza Kanunu'nda düzenlenen kişisel verileri hukuka aykırı olarak ele geçirme ve yayma suçuna dair düzenlemenin Anayasa'ya aykırı olduğu gerekçesi ile iptali için başvurulmuştur. Başvuru kararında söz konusu edilen Anayasa'nın 20. maddesi değil, ceza mevzuatında kişisel verilerle ilgili bir tanım

⁸¹⁶ Selda ÇAĞLAR, “Hukuk Devleti Açısından Hukuki Belirlilik- Hukuk Güvenliği İlişkisi”, *Hukuk Güvenliği*, Kamu Hukukçuları Platformu, Türkiye Barolar Birliği Yayınları, 2015, s. 34, ss. 25- 138; Hukuk devleti ilkesinin temel unsurlarından biri olan hukuki belirlilik ilkesine ilişkin detaylı bir çalışma olarak bkz. ÇAĞLAR, *Hukuk Devletinin Hukuki Belirlilik İlkesi Üzerinden Değerlendirilmesi*.

⁸¹⁷ AYMK E. 2015/32, K. 2015/102, K.T. 12.11.2015.

ve sınırlandırma yapılmamasından bahisle suçta ve cezada kanunilik ile belirlilik ilkelerinin düzenlendiği 38. maddesi olmuştur. Ancak AYM taleple bağlı olmadığı için, meseleyi Anayasa'nın 20. maddesi bakımından incelemiş ve kişisel veri kavramının ceza mevzuatındaki yansımalarını ortaya koymuştur. Buna göre,

“5237 sayılı Kanun'un "Kişisel verilerin kaydedilmesi" başlıklı 135. maddesinin gerekçesinde, gerçek kişiyle ilgili her türlü bilginin kişisel veri olarak kabul edilmesi gerektiği belirtilmiştir. Ayrıca, Kanun'un 134. ilâ 139. maddeleri arasında kişisel verilerin korunmasına yönelik hükümler yer almaktadır. Söz konusu maddelerde kişisel verilerin açık bir tanımı yer almamakla birlikte kişisel verilere yönelik olarak kişilerin özel hayatına ilişkin görüntü veya sesler, ‘siyasi, felsefi veya dini görüş’, ‘ırki köken’, ‘ahlaki eğilim’, ‘cinsel yaşam’, ‘sağlık durumu’ ve ‘sendikal bağlantılar’ gibi kavramlara yer verilmektedir.”

denilerek kişisel verilere ilişkin sınırlandırıcı olmayan bir sayım yapılmıştır. Ayrıca hem AYM'nin daha önce değindiğimiz kararlarındaki kişisel veri tanımları hem de Türkiye'nin taraf olduğu ya da olmadığı birçok uluslararası düzenlemede yer alan tanımlamalar, kanuni düzenlemeler, öğreti ve uygulama bakımından ortaya konulmuştur. Bu sebeple “kişisel veri” kavramının ceza hukuku mevzuatında belirsiz olduğu iddiası gerçekçi görülmemiş ve Anayasa'ya aykırılık iddiası reddedilmiştir.

AYM'nin bireysel başvuru kararları bağlamında kişisel verilerin korunması hakkına ilişkin içtihatları bakımından oldukça yeni sayılabilecek 27 Şubat 2019 tarihli bir kararı olan *Fatih Saraman Başvurusu*⁸¹⁸ ise kişisel verilerin korunması hakkının etkili güvencelenmesi açısından önemli bir karardır. Karara konu olayda, 18 yaşından küçükken başvuru hakkında 5 ay hapis cezasına hükmedilmiş ancak sonrasında hüküm para cezasına çevrilmiştir. Cezası ertelenmiş olan başvuruçunun 501 kişinin işe alınması planlanan sözleşmeli infaz ve koruma memurluğu sözlü ve yazılı sınavında 300. sırada yer alması ve hakkında başlatılan güvenlik ve arşiv soruşturması sonunda hırsızlık suçundan işlem yapıldığının tespiti söz konusudur. Ancak başvuruçunun Adalet

⁸¹⁸ *Fatih Saraman Başvurusu*, Başvuru No: 2014/7256, K.T. 27.02.2019.

Bakanlık Memur Sınav, Atama ve Nakil Yönetmeliği'nin ilgili maddesince öngörülen “güvenlik soruşturması olumlu olmak” şartı gereğince atamasının yapılmamıştır. Mahkeme bu olayda öncelikle olayın vuku bulduğu tarihte belirli kamu görevlerinde çalıştırılacak personel hakkında uygulanan güvenlik soruşturması ve arşiv araştırmasının kanuni dayanağının 4045 sayılı Kanun olduğunu dile getirmektedir. Bu Kanun'a dayanılarak Güvenlik Soruşturması ve Arşiv Araştırması Yönetmeliği çıkarılmıştır. Anılan Yönetmelik'in 4. maddesine göre “güvenlik soruşturması”,

“Kişinin kolluk kuvvetleri tarafından halen aranıp aranmadığının, kolluk kuvvetleri ve istihbarat ünitelerinde ilişkisi ile adli sicil kaydının ve hakkında herhangi bir tahdit olup olmadığının, yıkıcı ve bölücü faaliyetlerde bulunup bulunmadığının, ahlaki durumunun, yabancılar ile ilişkisinin ve sır saklama yeteneğinin mevcut kayıtlardan ve yerinden araştırılmak suretiyle saptanması ve değerlendirilmesini”

ifade ederken “arşiv araştırması”,

“Kişinin kolluk kuvvetleri tarafından halen aranıp aranmadığının, kolluk kuvvetleri ve istihbarat ünitelerinde ilişkisi ile adli sicil kaydının ve hakkında herhangi bir tahdit olup olmadığının mevcut kayıtlardan saptanmasını”

karşılacaktır. Mahkeme isabetli biçimde güvenlik soruşturması ve arşiv araştırmasından ne anlaşılması gerektiğini ortaya koyarken,

“Yönetmelik'te soruşturma ve araştırma sonucunu içeren bilgi ve belgelerin ilgilinin güvenlik makamlarındaki dosyasında süresiz olarak saklanacağı, güvenlik soruşturması ve arşiv araştırmasında olumsuz durumu saptananlarla ilgili bilgilerin Milli İstihbarat Teşkilatı ve Emniyet Genel Müdürlüğüne karşılıklı olarak birbirlerine aktarılacağı hükümlerine yer verilmiş olup kişilerin söz konusu bilgilere itiraz etme olanağı bulunmadığı gibi bilgilerin bir müddet sonra silinmesine de imkan verilmediği”

ni belirterek güvenlik soruşturması ve arşiv araştırmasının bu haliyle keyfiliğe açık bir durum yaratmakta olduğunu ortaya koymaktadır. Bu bağlamda davaya konu olan işlemin dayanağı olabilecek Kanun ve ilgili Yönetmelik'le ilgili olarak AYM, kişisel verilere

ilişkin süre, stoklama, kullanım, üçüncü kişilerin erişimi, verilerin gizliliği, bütünlüğü ve imhası konusundaki usullerdeki yetki aşımı ve keyfilğe karşı yeteri kadar güvenceye sahip olmalarını sağlayacak açık ve detaylı kuralların bulunmadığını ve bu sebeple müdahalenin dayanağı olan düzenlemenin kanunilik şartını sağlamadığını ele alarak Anayasa'nın 20. maddesinde yer alan özel hayata saygı hakkının ihlal edildiği sonucuna varmıştır.

AYM'nin kişisel verilerin korunması hakkı bakımından veri koruma hukukunun temel ilkelerine uygun analizler yaptığı bu kararına konu olan olayda esas alınan Güvenlik Soruşturması ve Arşiv Araştırması Yönetmeliği'ne bakıldığında görülmektedir ki, düzenlemede elde edilen verilerin saklanma süresi, silinip silinemeyeceği gibi hususlara ilişkin hükümler bulunmamaktadır. Bu ise açıktır ki, 6698 sayılı KVKK'nın hem 4. maddesinde ele alınan kişisel verilerin işlenmesinde uyulacak ilkelerden *“İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme.”* ilkesine hem de kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesini düzenleyen 7. maddesine ve bu bakımdan kararda da belirtildiği üzere Anayasa'nın 20/3. maddesine aykırılık oluşturmaktadır.

B. DEMOKRATİK TOPLUM DÜZENİNDE GEREKLİLİK

Anayasal bir devlette temel hak ve özgürlüklerin sınırlandırılmasında esas alınan diğer güvenceler ise diğer ölçütleri ise ölçülülük ilkesi ve hakkın özüne dokunma yasağıdır. 1982 Anayasası bu ölçütler yanında İHAS'tan alınan bir başka ifadeye, “demokratik toplum düzeninin gerekleri” ifadesine de yer vermektedir. Anayasa Mahkemesi de ölçülülük ve öze dokunma yasağını tıpkı Avrupa Mahkemesi gibi demokratik toplum düzeninin gerekleri ölçütü altında ele almak eğilimindedir.

Anayasa'da 2001 yılında gerçekleştirilen değişiklikle 13. maddeye eklenen ölçülülük ilkesine⁸¹⁹ göre Anayasa'da belirtilmiş nedenler doğrultusunda temel hak ve

⁸¹⁹ Ölçülülük ilkesi için detaylı olarak bkz. SAĞLAM, *Temel Hakların Sınırlanması ve Özü*; UYGUN, *1982 Anayasası'nda Temel Hak ve Özgürlüklerin Genel Rejimi*, s. 162 vd.; Yusuf Şevki HAKYEMEZ,

özgürlüklerin sınırlandırılmasında sınırlandırma amacı ile sınırlama aracı arasında ölçülü bir ilişki olmalıdır. Bu ise, kanunla getirilmiş sınırlamanın gerekli olmasını (gereklilik/ zorunluluk), sınırlama aracı ile sınırlama amacı arasında makul bir oranın bulunmasını (orantılılık/ dar anlamda ölçülülük) ve öngörülen amacı gerçekleştirmek bakımından elverişli nitelikte olmasını (elverişlilik) karşılamaktadır. Bu bağlamda adaletli, dengeli ve orantılı bir şekilde devletin bireyin haklarına yönelik sınırlamasının sınırlarını belirlemektedir⁸²⁰. Dolayısıyla bu ilke ışığında kişisel verilerin korunması hakkına ve diğer ilgili haklara yapılacak sınırlamada başvuru aracı sınırlama amacını gerçekleştirmeye elverişli olması, bu aracın sınırlama açısından gerekli olması ve araç ile amacın ölçülü olması gerekecektir.

Ölçülülük ilkesinin alt unsurlarına bakıldığında öncelikle elverişlilik ilkesinde başvuru önlemin ulaşmak istenen araç bakımından elverişli olması aranmaktadır. Bu ilke, alınan tedbirin ulaşmak istenen amaç için uygun olup olmadığı incelenmektedir⁸²¹. Ancak kanuni tedbirlerin elverişsizliği sebebiyle Anayasa'ya aykırılığa çok sık rastlanmamaktadır, çünkü kanun koyucunun koyduğu tedbirler genelde sınırlama amacını gerçekleştirmek için kısmen de olsa uygundur⁸²². Bir diğer unsur ise gereklilik ilkesidir. Anılan ilkeye göre, amaca varmaya elverişli birçok araç arasından en az müdahalede bulunmasını sağlayan seçilmelidir⁸²³. Bu bağlamda kişisel verilerin korunması hakkının sınırlanması durumunda da sınırlamanın amacının gerçekleştirilmesi

“Temel Hak ve Özgürlüklerin Sınırlandırılmasında Ölçülülük İlkesi”, Prof. Dr. Hayri DOMANIÇ'e 80. Yaş Günü Armağanı, C. II, İstanbul, 2001, s. 1293 vd.; Yüksel METİN, *Ölçülülük İlkesi- Karşılaştırmalı Bir Anayasa Hukuku İncelemesi*, Seçkin Yayıncılık, Ankara, 2002, s. 79 vd.; Yücel OĞURLU, *Karşılaştırmalı İdare Hukukunda Ölçülülük İlkesi*, Seçkin Yayıncılık, Ankara, 2002, s. 177 vd.

⁸²⁰ SAĞLAM, *Temel Hakların Sınırlanması ve Özü*, s. 112- 114; METİN, *Ölçülülük İlkesi- Karşılaştırmalı Bir Anayasa Hukuku İncelemesi*, s. 19- 20.

⁸²¹ SAĞLAM, *Temel Hakların Sınırlanması ve Özü*, s. 114; Yüksel METİN, “Temel Hakların Sınırlandırılması ve Ölçülülük: Ölçülülük Evrensel Bir Anayasal İlke midir?”, *Süleyman Demirel Üniversitesi Hukuk Fakültesi Dergisi*, Vol. 7, No: 1, Y: 2017, s. 8, ss. 1- 74.

⁸²² METİN, “Temel Hakların Sınırlandırılması ve Ölçülülük: Ölçülülük Evrensel Bir Anayasal İlke midir?”, s. 10.

⁸²³ METİN, “Temel Hakların Sınırlandırılması ve Ölçülülük: Ölçülülük Evrensel Bir Anayasal İlke midir?”, s. 11; METİN, *Ölçülülük İlkesi- Karşılaştırmalı Bir Anayasa Hukuku İncelemesi*, s. 31- 32.

için bu hak bakımından en yumuşak aracın seçilmelidir⁸²⁴. Amaca erişmek için kullanılan aracın elverişliliğine bakılmasının ardından aracın gerekli olup olmadığı tespit edilir. Son olarak orantılılık ilkesi (dar anlamda ölçülülük) ise, ilk iki denetimin gerçekleştirilmesinin ardından son adım olarak başvuru denetim yoludur. Buna göre ulaşılmak istenen amaç ile araç arasında ölçüsüz bir oran bulunmamalıdır. Bu aşamada müdahalenin ağırlığı ile gerçekleşen neticenin değeri arasında bir orantısızlık bulunup bulunmadığı ve şayet orantısız bir müdahale var ise bundan vazgeçilmesinin gerekip gerekmediği incelenmektedir⁸²⁵.

Ölçülülük ilkesi genel hatları ile böyle bir görünüm arz etmektedir. Öte yandan eğer temel hak ve özgürlüğe yapılan sınırlama hakkın esaslı unsurlarını yok sayacak biçimde ise hakkın özüne de dokunuyor demektir⁸²⁶. Her temel hakkın bir özü, cevheri olduğu fikrinden hareket eden öze dokunma yasağı, temel bir hakkın belli bir içeriğe sahip olduğu fikrini karşılamaktadır. Böylece temel hak ve özgürlükler kişilerin takdirinden bağımsız, objektif bir hale gelmektedir⁸²⁷. Bu noktada herhangi bir temel hak ve özgürlüğe yapılan bir sınırlama hakkın özüne doğru yönelmiş olsa dahi hakkın özüne dokunamayacaktır⁸²⁸.

Tüm bunlardan hareketle anayasa yargısında kişisel verilerin korunması hakkı ve başta özel hayatın gizliliği olmak üzere bağlantılı diğer haklar incelenirken öncelikle kanunla getirilmiş sınırlamanın gerekliliği, sınırlama aracı ile sınırlama amacı arasında makul bir oranın bulunup bulunmadığı ve öngörülen amacı gerçekleştirmek bakımından elverişliliği incelenir. Ayrıca kişisel verilerin korunması hakkına ilişkin bir müdahale

⁸²⁴ SAĞLAM, *Temel Hakların Sınırlanması ve Özü*, s. 115.

⁸²⁵ SAĞLAM, *Temel Hakların Sınırlanması ve Özü*, s. 116; METİN, “Temel Hakların Sınırlandırılması ve Ölçülülük: Ölçülülük Evrensel Bir Anayasal İlke midir?”, s. 13.

⁸²⁶ METİN, “Temel Hakların Sınırlandırılması ve Ölçülülük: Ölçülülük Evrensel Bir Anayasal İlke midir?”, s. 35.

⁸²⁷ SAĞLAM, *Temel Hakların Sınırlanması ve Özü*, s. 155; UYGUN, *1982 Anayasası'nda Temel Hak ve Özgürlüklerin Genel Rejimi*, s. 186.

⁸²⁸ SAĞLAM, *Temel Hakların Sınırlanması ve Özü*, s. 119.

gerçekleştirildiğinde bu müdahalenin hakkı kullanılamaz hale getirmemesi gerekmekte, başka bir ifade ile bu müdahalenin hakkın özüne dokunmaması aranmaktadır.

1. Hakkın Özüne Dokunma Yasağı

Anayasa Mahkemesi’nin Genel Kurul Kararları bağlamında değinilmesi gereken ve Mahkeme’nin kişisel verilerin korunmasına ilişkin bakış açısını ortaya koyması bakımından önemli kararlarından biri de 28 Eylül 2017 tarihli kararıdır⁸²⁹. KVKK’nın birçok maddesinin incelendiği ve Kanun’un Anayasa’ya aykırı olmadığı belirtilen bu AYM kararında Mahkeme tüm sınırlama yöntem ve ölçütlerine değinerek bir inceleme yapmış olsa da kararı esasen hakkın özü bağlamında değerlendirerek iptali istenen Kanun’un çoğu hükmünün hakkın özüne dokunmadığından bahisle Anayasa’ya uygun bulmuştur.

Buna göre ilk olarak KVKK’nın 4. maddesinin (2) numaralı fıkrasının (d) bendinde yer alan “...veya işlendikleri amaç için gerekli olan...” ibaresinin belirsiz, sübjektif, geniş ve yorumlayana göre değişebilecek nitelikte olduğundan bahisle kişisel verileri işleyen gerçek veya tüzel kişilerin ne kadar süre ile kişisel verileri muhafaza edebileceklerinin belirli olmadığı iddiası konu edilmiştir. Mahkeme bu hükmü öncelikle Anayasa’nın 20. maddesi bağlamında incelemiştir. Buna göre;

“...dava konusu kuralla kanun koyucunun, ilgili mevzuatta kişisel verilerin saklanması için bir süre öngörülmemesi durumunda bu verilerin ancak işlendikleri amaç için gerekli olan süre kadar muhafaza edilebilmesi suretiyle kişisel verilerin süresiz bir şekilde muhafaza edilmesi ihtimalini ortadan kaldırmaya yönelik bir düzenleme yapmayı ve kanunda muhafaza süresi belirtilmeyen kişisel verilerle ilgili olarak kişilere güvence sağlamayı amaçladığı anlaşılmaktadır...”

Ayrıca 6698 sayılı Kanun’un 16. maddesine göre Kişisel Verileri Koruma Kurulu gözetiminde Başkanlık tarafından kamuya açık olarak tutulan Veri Sorumluları Sicili’ne kişisel verileri işleyen gerçek ve tüzel kişiler tarafından veri işlenmeye başlanmadan önce bulunulması gereken kayıt başvurusunda yapılan bildirimde kişisel verilerin

⁸²⁹ AYM E. 2016/125, K. 2017/143, K.T. 28.09.2017.

işlendikleri amaç için gerekli olan azami sürenin de belirtilmesi gerekir... Dolayısıyla kuralda kişisel verilerin korunmasıyla ilgili uluslararası hukukta da temel ilkelerden biri olarak kabul edilen, verilerin amacın gerektirdiğinden daha uzun süre tutulmama ilkesine aykırı bir yön bulunmamaktadır.”

denilerek Anayasa’ya aykırılık tespit edilmemiştir.

İncelenen bir diğer düzenleme ise, KVKK’nın 5. maddesinin (2) numaralı fıkrasının (c), (ç), (e) ve (f) bentleri olmuştur. Anılan bu madde, kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği kuralının istisnalarını ele almaktadır. Bu maddeye dair Anayasa’ya aykırılık iddiası, istisnaların esas düzenleme hâline gelerek KVKK’nın uygulanmasında açık rızanın aranmasına gerek duyulmasının neredeyse imkânsız hâle getirildiği şeklindedir. Bu noktada Mahkeme, bu istisnaların hakkın özüne dokunmadığını ve demokratik toplum düzenine bir aykırılık teşkil etmeyerek ölçülü olduğunu söylemektedir:

“dava konusu kurallar, maddede belirtilen konularda gereklilik veya zorunluluk hâllerinde ortaya çıkacak bir ihtiyacın karşılanmasını sağlamaya yönelik olup hakkın özüne dokunmamaktadır... Kanun’da sınırlama aracının sınırlama amacına uygun ve orantılı şekilde kullanılmasını sağlayacak yasal güvencelere yer verildiği ve yeterli korumanın sağlandığı da dikkate alındığında dava konusu kurallarla getirilen sınırlamaların özel hayatın gizliliği ve kişisel verilerin korunması hakkının özünü zedelediği gibi amaç ile araç arasında makul denge kurduğu da açıktır. Dolayısıyla anılan kurallar, demokratik toplum düzeninin gereklerine aykırılık teşkil etmediği gibi özel hayatın gizliliği ve kişisel verilerin korunması hakkına ölçüsüz bir müdahale de teşkil etmemektedir.”

Anılan karara konu olan bir diğer KVKK düzenlemesi ise, Kanun’un 6/1. maddesinde yer alan “...mezhebi...”, “...kılık ve kıyafeti, ...” ibareleri ile yine aynı maddenin 3. fıkrasıdır. 6/3. maddenin ilk fıkrasında özel nitelikli kişisel veriler, diğer bir ifade ile hassas veriler sayılarak bu verilerin ilgilinin açık rızası olmaksızın işlenmesinin yasak olduğu belirtilmesine karşın

“cinsel hayat ve sađlık dıřındaki kiřisel verilerin kanunlarda ngrlen hllerde ilgili kiřinin aık rızası aranmaksızın iřlenebileceđi, cinsel hayata ve sađlıđa iliřkin kiřisel verilerin ise ancak kamu sađlıđının korunması, koruyucu hekimlik, tıbbi teřhis, tedavi ve bakım hizmetlerinin yrtlmesi, sađlık hizmetleri ile finansmanının planlanması ve ynetimi amacıyla sır saklama ykmllđ altında bulunan kiřiler veya yetkili kurum ve kuruluřlar tarafından ilgilinin aık rızası aranmaksızın iřlenebileceđi”

hususlarına iliřkindir. ncelikle 6/1. maddenin “...mezhebi...”, “...kılık ve kıyafeti, ...” ibareleri incelendiđinde, kiřilerin dini veya diđer inanlarını ortaya koyabilecek bu unsurların zel nitelikli veri olarak kabul edilmesinin sebebi olarak, bu verilerinin toplanmasına dayanak oluřturmak deđil, aksine bu verilere zel bir koruma sunmak olduđu ve bu tarz dzenlemelerin uluslararası belgelerde de bulunduđu belirtilerek Anayasa’ya aykırılık bulunmadıđına hkmedilmiřtir. 6/3. madde bakımından ise, kiřisel verilerin “kanunlarda ngrlen hallerde” ilgili kiřinin aık rızasının aranmaksızın iřlenebileceđine dair hkmn Anayasa’nın 20/3. maddesinin bir tekrarı olduđu belirtilerek bu durumun Anayasa’ya bir aykırılık oluřturmadıđı dile getirilmiřtir. te yandan sađlık ve cinsel hayata dair kiřisel verilerin ise, madde metninde anılan ve sayma yntemi ile sınırlı tutulduđu belirtilen sınırlama amalarının “hakların kullanılmasını son derece zorlařtıran veya onu kullanılamaz duruma dřren kayıtlara bađlandıđı sylenemeyeceđinden hakkın zne dokunmadıđı aıktır.” denilerek ze dokunma yasađının korunduđunu,

“Anayasa’da devlete verilen grevlerin geređi olarak kiřilerin sađlıklı bir řekilde yařam srdrmeleri iin genel sađlıđın korunması amacıyla dzenlenen dava konusu kural demokratik toplum dzeni bakımından alınması gereken tedbirler kapsamında kalmaktadır.”

ifade edilerek demokratik toplum dzenine aykırılık teřkil etmediđi ve “bu haklar ile toplum sađlıđının korunmasına ynelik nlemler arasındaki makul dengenin kurulduđu” belirtilerek lllk ilkesine de uyulduđu hkm altına alınmıřtır.

Burada dile getirilmelidir ki, zel nitelikli verilerden olan sađlık ve cinsel hayata iliřkin verilerin iřlenmesi kural olarak veri znesinin aık rızası ile olabilmektedir. Fakat

bu düzenleme neticesinde, cinsel hayata ve sağlığa ilişkin kişisel veriler ilgili kişinin açık rızası aranmaksızın

“kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından”

işlenebilmektedir. Kanaatimizce her ne kadar ilk üç amaç bakımından toplum sağlığının korunması ortak nokta ise de sağlık hizmetleri ile finansmanının planlanması amacının da düzenlenmesi meseleyi oldukça muğlak bir noktaya taşımaktadır. Belirtilmelidir ki bu düzenleme ile kişisel verilerin korunması hakkının kullanılması zorlaşmamakta ya da ortadan kalkmamaktadır. Bu sebeple hakkın özüne dokunan bir yönü yoktur. Burada dikkatle incelenmesi gereken, söz konusu sağlık hizmetleri ile finansmanının planlanması amacının demokratik toplum düzeninin gerekleri ile ölçülülük ilkesine uygunluğu olmalıdır. Her ne kadar kamu sağlığı gibi bir kamu yararı olsa da kişisel verilerin korunması hakkı ile bir dengenin kurulmadığı ve esas olanın kamu sağlığı olduğu görülecektir. Çünkü sağlık hizmetleri ve finansmanının planlanması amacı ile kişinin özel nitelikli verilerinden olan sağlık ve cinsel yaşama dair tüm kişisel verilerin rıza aranmaksızın toplanma, aktarma ve işlenmesi durumu söz konusudur. Her ne kadar Anayasa’nın 20/3. maddesinde “Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir.” denmişse de kanunda öngörülme hususu açık rızanın verilmeyeceği her halde kullanılmamalıdır.

Özel nitelikli kişisel veriler bakımından GVKT ışığında Avrupa standardına bakacak olursak, kural olarak ırk veya etnik kökene işaret eden kişisel veriler, politik görüşler, dini veya felsefi inançlar, sendika üyeliği, genetik veya biyometrik veriler ile kişinin cinsel yaşamı veya cinsel yönelimine ilişkin verilerin işlenmesi yasaktır⁸³⁰. Ancak

⁸³⁰ DE HERT, PAPAKONSTANTINOU, “The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?”, *The International Journal of Technology Law and Practice*, s. 5- 6; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), Art. 9, L 119,

GVKT'nin 9/2. maddesi uyarınca belli hallerde özel nitelikli kişiler veriler (hassas veriler) işlenebilecektir. Buna göre;

- Veri öznesinin açık rızası varsa,
- İstihdam veya sosyal güvenlik bakımından bir gereklilik söz konusu ise,
- Veri öznesinin ya da onun fiziksel ya da hukuki olarak rıza verme yetisine sahip olamadığı durumlarda diğer bir gerçek kişinin hayati çıkarlarını korumak için işlem yapmak gerekiyorsa,
- Bir vakıf, dernek veya kâr amacı gütmeyen başka bir kuruluş tarafından meşru faaliyetleri sırasında, işlemenin yalnızca üyelere veya kuruluşun eski üyelerine veya bununla bağlantılı olarak düzenli temas halinde olunan kişilere bağlı olması şartıyla, anılan kuruluşların amaçları ile bağlantılı olarak işlenebilir. Ancak burada veri öznelerinin onayı olmadan bu veriler doğaldır ki, anılan kurumlar dışında açıklanamaz.
- Hak taleplerinin kullanılması, savunulması veya mahkemelerin yargı yetkisi dahilinde hareket ettikleri hallerde,
- Veri koruma hakkının özüne saygı duymak ve temel hak ve özgürlüklerin çıkarlarını korumak için uygun ve özel önlemler almak şartıyla, orantılı olarak ve meşru amaç doğrultusunda, Birlik veya üye devlet hukuklarında yer alan önemli kamu yararı sebepleri söz konusu ise,
- Koruyucu ya da mesleki tıbbın amaçları, çalışanın çalışma kapasitesinin değerlendirilmesi, tıbbi teşhis, sağlık ya da sosyal bakım ya da tedavi sağlanması ya da Birlik ya da üye devlet temelinde sağlık ya da sosyal bakım sistemleri ve hizmetlerinin yönetimi için ya da bir sağlık profesyoneli ile yapılan sözleşme söz konusu ise,
- Halk sağlığı alanında kamu yararı mevcutsa,
- Veri koruma hakkının özüne saygı gösterildiği, veri öznesinin temel haklarını ve çıkarlarını korumak için uygun ve özel önlemlerin mevcut olduğu hallerde,

kamu yararı doğrultusunda bilimsel, tarihsel araştırma veya istatistiki amaçlarla

mümkün olabilmektedir.

Bahis konusu AYM kararına konu olay bakımından özel nitelikli verilerin işlenmesinde GVKT'nin bakış açısını incelediğimizde görülmektedir ki, özellikle önemli kamu yararı sebeplerinin söz konusu olduğu haller veya koruyucu ya da mesleki tıbbın amaçları, çalışanın çalışma kapasitesinin değerlendirilmesi ya da Birlik ile üye devlet temelinde sağlık ya da sosyal bakım sistemleri ve hizmetlerinin yönetimi hususlarında veri işlenmesine izin verilmesi mümkündür. Ancak bu ihtimallerde dahi veri koruma hakkının özüne saygı duyulması ve temel hak ve özgürlüklerin çıkarlarını korumak için uygun ve özel önlemler alınması şart koşulmakta ve bu işlemenin orantılı olarak ve meşru amaç doğrultusunda gerçekleştirilmesi gereği madde metninde belirtilmektedir. Ayrıca aynı maddenin son fıkrasına göre üye devletler, genetik, biyometrik ve sağlık verilerinin söz konusu olduğu hallerde ek koşullar getirebilecektir. Dolayısıyla her ne kadar KVKK'nın 6/3. maddesinde bulunan ve "sağlık ve cinsel hayata ilişkin kişisel verilerin sağlık hizmetleri ile finansmanının planlanması amacı ile ilgilinin açık rızası aranmaksızın işlenebileceği"nin belirtilmesi hususu GVKT ile benzerlik taşıyor gibi görünse de, iç hukuk bakımından esas problem bu hallerde işlemenin meşru amaçlar doğrultusunda ve orantılı olup olmadığı ve kişisel verilerin korunması hakkının özüne dokunup dokunmadığının yeterince incelenip incelenmediği olacaktır.

Yine bu kararda incelenen bir diğer KVKK hükmü de 7/2. maddedir. Anılan düzenlemeye göre, "*Kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesi ve buna ilişkin diğer kanunlarda yer alan hükümler saklıdır.*" Mahkeme bu düzenleme ile kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesine dair diğer kanunlarda hüküm bulunması hâlinde bunların öncelikle uygulanmasının amaçlanmakta olduğunu belirtmiştir. Bunun yanı sıra daha ayrıntılı düzenlenmiş olan özel durumların esas alınmasının sağlanmasının kamu yararı amacıyla gerçekleştirildiği

de dile getirilerek amaç ve araç arasında makul ve uygun bir ilişki kurulduğu ve orantılı olduğu, bu sebeple de ölçülülük ilkesine aykırı bir yön olmadığı ifadelerine yer verilmiştir.

İncelenen bir başka düzenleme de KVKK'nın 8/3. maddesi olmuştur. Söz konusu madde, *“Kişisel verilerin aktarılmasına ilişkin diğer kanunlarda yer alan hükümler saklıdır.”* şeklindedir. Bu madde bağlamında kişisel veriler, kural olarak ilgili kişinin açık rızası olmaksızın aktarılamaz. Fakat Kanun'un 5/2. maddesi uyarınca ve yeterli önlemler alınmak kaydıyla 6/3. maddesinde belirtilen şartlardan birinin bulunması hâlinde ilgili kişinin açık rızası aranmaksızın aktarılması mümkündür. Bu noktada kişisel verilerin aktarılmasına ilişkin diğer kanunlarda yer alan hükümlerin saklı olduğu da belirtilmektedir. Mahkeme bu maddenin de Anayasa'ya uygun olduğunu belirterek tıpkı 7/2. maddenin yorumlanması ile aynı gerekçelerle, açık bir ifadeyle, diğer kanunlarda hüküm bulunması hâlinde bunların öncelikle uygulanmasının amaçlanmakta olduğu ve daha ayrıntılı düzenlenmiş olan özel durumların esas alınmasının kamu yararı amacıyla gerçekleştirildiği dile getirilerek amaç ve araç arasında makul ve uygun bir ilişki kurulduğu ve orantılı olduğu, bu sebeple de ölçülülük ilkesine aykırı bir yön olmadığı gerekçelerine gönderme yaparak Anayasa'ya aykırılık tespit etmemiştir.

Karar bağlamında Anayasa'ya aykırılığı incelenen bir diğer KVKK maddesi ise, 9/6. maddedir. Bu maddeye göre, *“Kişisel verilerin yurtdışına aktarılmasına ilişkin diğer kanunlarda yer alan hükümler saklıdır.”* Bu madde bağlamında kişisel veriler, kural olarak ilgili kişinin açık rızası olmaksızın yurtdışına aktarılamaz. Fakat yine 7. maddede olduğu gibi, Kanun'un 5/2. maddesi uyarınca, yeterli önlemler alınmak kaydıyla 6/3. maddesinde belirtilen şartlardan birinin bulunması hâlinde ve kişisel verinin aktarılacağı yabancı ülkede yeterli korumanın bulunması hâlinde; yeterli korumanın bulunmaması durumunda ise Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurul'un izninin bulunması kaydıyla ilgili kişinin açık rızası aranmaksızın yurt dışına aktarılmasının mümkün olduğu hükme bağlanmaktadır. Dava konusu fıkra ise kişisel verilerin yurt dışına aktarılmasına ilişkin diğer kanunlarda yer alan hükümlerin saklı olduğu belirtilmektedir. Bu düzenleme de tıpkı 7/2. ve 8/3. maddeler ile aynı gerekçelerle Anayasa'ya uygun bulunmuştur.

Görüldüğü üzere yukarıda anılan 7/2., 8/3, ve 9/6. maddelerin hepsinde “...diğer kanunlarda yer alan hükümler saklıdır.” Bu durum görünüşte Anayasa’ya bir aykırılık teşkil etmiyorsa da aslında kişisel verilerin korunması hukuku bakımından belirsiz bir görünüm arz etmektedir. Şöyle ki, hukuk devletinin de temel unsurlarından olan hukuki belirlilik ilkesi⁸³¹, kişisel verilerin korunması hukukunun da temel ilkelerinden biridir. Söz konusu ilke, KVKK’nın 4. maddesi bakımından ele alındığında görülmektedir ki kişisel verilerin işlenmesi “belirli, açık ve meşru amaçlar doğrultusunda ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmelidir.” KVKK’nın bahis konusu maddeleri ise “diğer kanunlarda yer alan hükümler saklıdır.” diyerek Anayasa’nın 20/3. maddesinde yer alan “Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.” hükmünün de dolaylı olarak genişlediğinden söz edilebilecektir. Konuya dair temel kanun olan KVKK’nın bu şekilde birçok istisna hükmü içermesi, kişisel verilerin korunamaması riskini de beraberinde getirmektedir.

Mahkeme’nin incelediği bir diğer KVKK hükmü ise 13/2. maddedir. Anılan maddede veri sorumlusuna başvuru usulü ele alınmaktadır. Buna göre ilgili kişi, 6698 sayılı KVKK’nın uygulanmasıyla ilgili taleplerini yazılı olarak veya Kurul’un belirleyeceği diğer yöntemlerle veri sorumlusuna iletir. Veri sorumlusu başvuruda yer alan talepleri, talebin niteliğine göre en kısa sürede ve en geç otuz gün içinde ücretsiz olarak sonuçlandırmalıdır. Şayet işlem ayrıca bir maliyeti gerektiriyorsa, Kurul tarafından belirlenen tarifiedeki ücretin alınabileceği de öngörülmektedir. Mahkeme’ye göre; “işlemin ayrıca bir maliyeti gerektirmesi hâlinde Kurulca belirlenen tarifiedeki ücretin alınabileceği öngörülmek suretiyle kişisel veriler(e) erişim hakkına bir sınırlandırma getirildiği açıktır.” denilerek söz konusu durumun hakkın sınırlaması olduğu belirtilmiş; fakat bu sınırlamanın Anayasa’nın 20. maddesinde düzenlenen kişisel verilerin korunması hakkının kullanılmasını son derece zorlaştıran veya onu kullanılamaz

⁸³¹ Hukuk devleti ilkesinin temel unsurlarından biri olan hukuki belirlilik ilkesine ilişkin olarak bkz. ÇAĞLAR, *Hukuk Devletinin Hukuki Belirlilik İlkesi Üzerinden Değerlendirilmesi*; ÇAĞLAR, “Hukuk Devleti Açısından Hukuki Belirlilik- Hukuk Güvenliği İlişkisi”, *Hukuk Güvenliği*.

duruma düşüren bir durum olmadığı ve bu sebeple hakkın özüne dokunmadığı vurgulanmıştır. Bu ücretin belirlenmesinde işlemin maliyetinin esas alınacak olması ve Kurul’un tarifesi doğrultusunda hesaplanacak olması da hukuki güvenlik ve belirlilik ilkelerine uygun olarak nitelendirilmiştir. Oysa ölçülülük ilkesi bakımından en azından bir üst sınır öngörülmesi yerinde olurdu.

Karar’a konu olan diğer bir KVKK maddesi de 15/3. maddede yer alan “*Devlet sırrı niteliğindeki bilgi ve belgeler hariç*” ifadesidir. Bu madde genel olarak Kurul tarafından şikâyet üzerine veya resen incelemenin usul ve esaslarını içermektedir. Maddenin 3. fıkrasında, devlet sırrı niteliğindeki bilgi ve belgeler hariç olmak üzere, veri sorumlusunun Kurul’un inceleme konusuyla ilgili istemiş olduğu bilgi ve belgeleri on beş gün içinde göndermek ve gerektiğinde yerinde inceleme yapılmasına imkân sağlamak zorunda olduğu kuralı bulunmaktadır. Mahkeme öncelikle burada “devlet sırrı” kavramının belirsiz olmadığını, 5271 sayılı Ceza Muhakemesi Kanunu’nun 47/1. maddesinde yer alan tanımları⁸³² esas aldığını belirtmektedir. Dava konusu kuralın Anayasa’ya uygunluğu konusunda ise AYM,

“devlet sırrı niteliğindeki bilgi ve belgelerin ifşa edilmesini önlemeye yönelik dava konusu kuralın ulaşılmak istenen amaç için elverişli ve gerekli olduğu, amaç ve araç arasında makul ve uygun bir ilişki kurduğu ve öngörülen amaçla kişisel verilerin korunması hakkına yapılan sınırlamanın orantılı olduğu açıktır... böylece hem özel hayatın gizliliği ve kişisel verilerin korunması haklarının özünün zedelenmesinin önlendiği hem de bu haklar ile ülkede millî güvenliğin sağlanmasına yönelik önlemler arasındaki makul dengenin kurulduğu”

nu belirterek düzenlemenin Anayasa’ya aykırı olmadığını hükme bağlamıştır.

⁸³² Söz konusu tanıma göre, “*Açıklanması, Devletin dış ilişkilerine, milli savunmasına ve milli güvenliğine zarar verebilecek; anayasal düzeni ve dış ilişkilerinde tehlike yaratabilecek nitelikteki bilgiler, Devlet sırrı sayılır.*”

5271 sayılı Ceza Muhakemesi Kanunu, md. 47/1, <https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5271.pdf>, 12.04.2019.

Bir diğerk inceleme konusu olan madde de KVKK'nın 16/2. maddesidir. Bu maddeye göre, Kişisel Verileri Koruma Kurulu'nun gözetiminde, Başkanlık tarafından kamuya açık olarak Veri Sorumluları Sicili tutulacaktır. Bu sicil, kişisel verileri işleyen gerçek ve tüzel kişilerin veri işlemeye başlamadan önce kaydolmak zorunda oldukları bir ortamdır. Burada Anayasa'ya aykırılık iddiası, işlenen kişisel verinin niteliği, sayısı, veri işleminin kanundan kaynaklanması veya üçüncü kişilere aktarılma durumu gibi Kurulca belirlenecek objektif kriterler göz önüne alınmak suretiyle Kurul tarafından, Veri Sorumluları Sicili'ne kayıt zorunluluğuna istisna getirilebileceği hususuna ilişkindir. Burada Mahkeme dava konusu olan bu kuralın, uluslararası düzenlemelerde de veri koruma otoritelerine sicillere bildirim yapılması yükümlülüğünü kaldırma imkânı tanındığını belirterek,

“Kanun koyucunun dava konusu kuralla, söz konusu farklılıkları dikkate alarak kişisel verileri işleyen gerçek ve tüzel kişilerin tümünün Veri Sorumluları Siciline kaydolmasına gerek görmediği ve bazılarını Kurul tarafından belirlenecek objektif kriterler göz önüne alınmak suretiyle yine Kurul tarafından verilecek kararlar kayıt zorunluluğundan istisna tutmayı amaçladığı anlaşılmaktadır. Bu bağlamda kanun koyucunun takdir yetkisi kapsamında düzenlediği dava konusu kuralın amaç ve araç arasında makul ve uygun bir ilişki kurduğu ve orantılı olduğu anlaşıldığından ölçülülük ilkesine aykırı bir yönü bulunmadığını”

hüküm altına almıştır. Bu durumun veri sorumlularının veri güvenliğine dair yükümlülüklerini ortadan kaldırmadığını da belirtmiştir.

Bu maddeye ilişkin durumu daha detaylı olarak ortaya koyabilmek adına “veri sorumlusu” kavramını KVKK bakımından ele almak yerinde olacaktır. Kanun'un 3/1. maddesine göre veri sorumlusu, “Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi...” ifade etmektedir. 10. maddeye göre veri sorumlusunun kişisel verilerin elde edilmesi sırasında ilgili kişilere belli konularda bilgi vermesi gerekmektedir. Öte yandan 12. maddeye göre de veri sorumlusunun veri güvenliğine ilişkin birçok görev ve sorumlulukları bulunmaktadır. Veri sorumlusunun ele alındığı bir

diğer madde olan 13. maddede de veri öznelerinin Kanun'un uygulanmasıyla ilgili taleplerini veri sorumlusuna, kanuni görev ve sorumluluklarıyla ilgili taleplerini iletebileceklerini düzenlemektedir. Tüm bu maddelerle görülmektedir ki, veri sorumlusu oldukça önemli ve geniş kapsamlı yetkileri haizdir. Böylesi önemli yetki ve sorumlulukları olan veri sorumlusunun, verileri işlenen veri öznelerince bilinebilmesi açıktır ki birçok bakımdan önem taşımaktadır. Özellikle veri güvenliği bakımından, verilerin hangi amaçla işleneceği, kimlere veya hangi ülkelere aktarılabileceği, alınan tedbirler, azami süre ve bu hususlarda ortaya çıkan değişiklikler derhal Kurul Başkanlığı'na bildirilmektedir. Bu bakımdan anılan hususlar Veri Sorumluları Sicili'ne başvuruda alınan bilgiler olduğundan, KVKK'nın karara konu olan 16/2. maddesi bakımından Sicil'den muaf tutulan veri sorumluları bakımından veri öznesinin bu bilgilerden yoksun kalacağı açıktır. Bu durum ise Anayasa'nın 20/3. maddesinde yer alan kişisel verilerin korunması hakkının *"kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenme"* unsurlarını sakatlayacağı için Anayasa'ya aykırılık teşkil edecektir.

AYM tarafından Anayasa'ya uygunluğu incelenen bir diğer KVKK hükmü de 24/3(b) düzenlemesidir. Bu madde genel olarak Kişisel Verilerin Korunması Kurulu'nun Başkanı'nın görevlerini ele almaktadır. Dava konusu hüküm, *"Kurul kararlarının tebliğini ve Kurulca gerekli görülenlerin kamuoyuna duyurulmasını sağlamak ve uygulanmalarını izlemek"* görevinde *"Kurulca gerekli görülenlerin"* ibaresidir. Bu düzenleme ile Başkan'a verilen kararlardan Kurul tarafından gerekli görülen kararları kamuoyuna duyurma görevi verilmektedir. Başkan tarafından kamuoyuna duyurulacaktır. Burada açıktır ki Kurul'a kamuoyu ile paylaşılacak kararlar hususunda ilk elden belirleme yetkisi verilmiştir. AYM bu durumu kanun koyucunun takdir yetkisi bağlamında değerlendirerek Anayasa'ya aykırılık görmemiştir. Kurul'un kararları ile Kanun uygulamasının ilk elden belirleyicisi olması, veri koruma hukukunun pratikteki gelişimini göstermesi açısından oldukça önem taşımaktadır. Bu bakımdan 6698 Sayılı KVKK'nın uygulaması bakımından bazı Kurul kararlarının yayınlanmayacak olması

kişisel verilerin korunması hukukunun gelişimi açısından olumsuz bir gelişme olarak değerlendirilebilir.

KVKK'nın 28/1(a) ve (ç) düzenlemeleri de AYM'nin söz konusu kararının inceleme konularındandır. Bu maddede KVKK'nın hangi hallerde uygulanmayacağı, yani istisnalar ele alınmaktadır. Davaya konu olan (a) bendindeki husus, *“Kişisel verilerin, üçüncü kişilere verilmemek ve veri güvenliğine ilişkin yükümlülüklerle uyulmak kaydıyla gerçek kişiler tarafından tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında işlenmesi”* hâlinde 6698 sayılı Kanun hükümlerinin uygulanmayacağıdır. Bu hükme dair Mahkeme öncelikle hakkın özü değerlendirmesi yapmış ve yukarıda KVKK'nın *“İstisnaları”*nın anlatıldığı bölümde detaylıca açıklandığı üzere, söz konusu istisnanın hakkın özüne dokunmadığı belirtilmiştir⁸³³.

Davaya konu olan (ç) bendindeki düzenleme ise, KVKK'nın uygulanmayacağı bir diğer istisna olan,

“...kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi”

durumudur. AYM'ye göre, kişisel verilerin korunması hakkı sınırsız bir hak olmayıp *“Anayasa'da devlete bir görev olarak yüklenen millî güvenliğin ve kamu düzeninin sağlanması ile suç işlenmesinin önlenmesi amaçlarıyla sınırlandırılması mümkündür.”* Bu bağlamda Mahkeme hem İHAM'a hem de 108 Numaralı Sözleşme'ye atıf yaparak bu sınırlamanın *“Anayasa'da devlete verilen görevlerin gereği olarak millî güvenliğin, kamu düzeninin ve suç işlenmesinin önlenmesini sağlamak amacıyla yapıldığından demokratik toplum düzeni bakımından alınması gereken tedbirler*

⁸³³ KVKK'nın 28/1(a)'da yer alan aile fertlerine ilişkin istisna hükmünün konu edildiği 28 Eylül 2017 tarihli AYMK E. 2016/125, K. 2017/143 kararı için bkz. Üçüncü Bölüm: AVRUPA VERİ KORUMA HUKUKUNUN TÜRK HUKUK SİSTEMİNE ETKİSİ, B. KANUNİ DÜZENLEME, d) İstisnalar.

kapsamında” değerlendirmektedir. AYM, milli güvenliğin sađlanmasına yönelik tüm bu istisnaların özel hayatın gizliliđi ve kişisel verilerin korunması haklarının özünü zedelediđi, bu haklar ile ülkede millî güvenliğin sađlanmasına yönelik önlemler arasındaki makul dengenin kurulduđu hususlarına da dikkat çekmektedir. Dolayısıyla Mahkeme’ye göre dava konusu kuralla, özel hayatın gizliliđi ve kişisel verilerin korunması haklarına getirilen sınırlama, hakların özünü zedelememektedir ve demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırı bulunmamaktadır.

Öte yandan (ç) bendindeki bu düzenleme kişisel verilerin korunması meselesinde daha sınırlandırıcı bir tutuma sebebiyet verebilecektir. Bu ise veri korumanın varlık sebebini tehlikeye düşüren bir anlayıştır. Anılan hüküm doğrultusunda oldukça geniş ve önemli bir alan Kanun’un kapsamı dışında bırakılmıştır. Önleyici, koruyucu ve istihbari faaliyetler ifadesi oldukça belirsizdir. Bu kapsama giren konularda kamu kurumlarının hangi hallerde ve ne şekilde veri toplayacakları da belirtilmemiştir. Dolayısıyla kişisel verilerin korunması hakkının özüne dokunulması riski mevcuttur. Ayrıca bu düzenleme hukuk devletinin önemli prensiplerinden olan belirlilik ilkesine de uygun düşmemektedir. Her ne kadar söz konusu veri işleme, millî savunma, millî güvenlik, kamu güvenliđi, kamu düzeni veya ekonomik güvenlik amaçlarını sađlamak bakımından bu yetkiyi veriyor olsa da yarışan değerler arasında bir denge kurulmaya çalışılarak ve veri koruma hukukunun temel ilkeleri nazara alınarak veri işlemenin gerçekleştirilmesinin Kanun’un ruhuna çok daha uygun olacađı düşünülmektedir.

İstihbari faaliyetler açısından Avrupa standardını anlayabilmek için GVKT’ye baktığımızda da ulusal güvenlik alanında özel yaşam ve veri korumasını genişletmek adına düzenlemenin yetersiz kaldıđı görölmektedir. Yine de bu noktada 6/4. maddesi önem taşımaktadır. Bu maddeye göre,

“Kişisel verilerin toplama amacının dışında bir amaca yönelik olarak yapılan işleme faaliyetinin veri sahibinin rızasına dayanma durumu hariç, demokratik bir toplumda gerekli ve ölçülü bir tedbir teşkil eden Birlik veya üye devlet kanununa dayanmaması durumunda kişisel

verilerin asıl toplanma amacına uygun olup olmadığını değerlendirenken řu ilkelere de göz atılır:

a) Kişisel verilerin toplanma amaçları ile diğer işleme amaçları arasında herhangi bir bağlantı,

b) Veri öznesi ve denetleyici arasındaki ilişki başta olmak üzere kişisel verilerin toplandığı bağlam,

c) 9. madde uyarınca özel kategorilerdeki kişisel verilerin işlenip işlenmediği veya 10. madde uyarınca mahkûmiyet kararları ve ceza gerektiren suçlara ilişkin kişisel verilerin işlenip işlenmediği başta olmak üzere kişisel verilerin mahiyeti,

d) Planlanan diğer işleme faaliyetlerinin veri öznelerine olası yansımaları,

e) Şifreleme veya takma ad kullanımı da dahil olmak üzere uygun güvencelerin bulunması.”

Öte yandan 108 Sayılı Sözleşme’nin revizyonu neticesinde ortaya çıkan Sözleşme 108+’ın 11. maddesi ile GVKT’den çok daha kapsamlı şekilde ulusal güvenlik açısından yürütölen faaliyetler bakımından da üst düzey ilke ve güvenceler sağlamaktadır. Bu maddeye göre ilgili metinde yer alan hükümlerin hiçbirisi, veri öznelerine Sözleşme 108+’da öngöröülenden daha geniş bir koruma önlemi vermesi olasılığını sınırlayan veya başka biçimde etkileyen şekilde yorumlanamayacaktır. Mahremiyet Hakkına ilişkin BM Özel Raportörü olan Joseph A. Cannataci’nin 27 Şubat 2019 tarihinde BM İnsan Hakları Konseyi’ne sunduğu yıllık raporunda, tüm BM ölkelerine özellikle güvenlik ve istihbari faaliyetler bakımından Sözleşme 108+’a uymaları önerilmiştir. Ayrıca aynı raporda Sözleşme 108+’da yer alan başta orantılılık ve gereklilik olmak üzere istihbari faaliyetlere dair veri işlemede geçerli olan temel ilke ve standartların 2018 yılında İHAM nezdinde Büyük Daire’ye iletilen *Centrum for Rattvisa-*

*İsveç*⁸³⁴ ve *Big Brother Watch ve Diğerleri- Birleşik Krallık*⁸³⁵ kararlarında yer aldığından söz edilmiştir⁸³⁶. Tüm bunlardan hareketle KVKK'nın 28/1. maddesinin (ç) bendinde ele alınan önleyici, koruyucu ve istihbari faaliyetlerin Kanun'un kapsamı dışında bırakılması da Sözleşme 108+ bağlamında değerlendirildiğinde demokratik toplum düzeninde gerekli ve ölçülü olmadığı sonucuna varılabilecektir.

KVKK'nın birçok hükmünün AYM tarafından kapsamlı bir biçimde incelendiği karara konu olan ve başka bir hukuki düzenlemeyi konu eden son madde ise KVKK'nın 30/7. maddesidir. Bu madde ile 663 sayılı Kanun Hükmünde Kararname'nin 47. maddesi değiştirilmiştir. Sağlık Bakanlığı ve bağlı kuruluşlarının teşkilat, görev, yetki ve sorumluluklarını düzenleyen 663 sayılı KHK'nın 47. maddesinin 1. fıkrasında,

“Sağlık hizmeti almak üzere kamu veya özel sağlık kuruluşları ile sağlık mesleği mensuplarına müracaat edenlerin, sağlık hizmetinin gereği olarak vermek zorunda oldukları veya kendilerine verilen hizmete ilişkin kişisel verileri..”nin

⁸³⁴ *Centrum for Rattvisa v. Sweeden*, Application No: 35252/ 08, 19.06.2018, <http://hudoc.echr.coe.int/eng?i=001-183863>, E.T. 19.08.2019.

⁸³⁵ *Big Brother Watch and Others v. The United Kingdom*, Application Nos: 58170/ 13, 62322/ 14 and 24960/ 15, <http://hudoc.echr.coe.int/eng?i=001-186048>, E.T. 19.08.2019.

İHAM'ın 10 Temmuz 2019 tarihinde Büyük Daire'de görüşmeye başladığı *Big Brother Watch ve Diğerleri- Birleşik Krallık* davası, istihbarat servislerinin kişisel verileri rıza olmaksızın toplanmasının İHAS'ın 8. maddesini ihlal edip etmediği konusunda dikkat çekici dosyalardan biridir. Büyük Daire konu ile ilgili kararını henüz vermemiş olsa da anılan görüşmede istihbarat faaliyetleri ve veri korumaya ilişkin bazı önemli tespitlerde bulunmuştur.

Olayda başvuruçular İngiliz istihbaratının terör tehlikesini gerekçe göstererek genel veri toplama faaliyetlerinin ve bu verilerin başka istihbarat servisleri ile bir yargı kararına dayanmaksızın paylaşılmasının İHAS'ın 8. maddesini ihlal ettiğini iddia etmektedir. Büyük Daire'deki görüşmede Mahkeme, söz konusu veri toplama faaliyetinin demokratik bir toplumda gerekli olup olmadığı ve ölçülülük kriterleri bakımından değerlendirilmesi gerektiğini belirtmiştir. Ayrıca İHAM, devlet istihbarat çalışmaları sırasında verilerin toplanmasında devletin yetkisinin daha sınırlı olması ve daha dar bir alanı kapsamaması gerektiğini vurgulamıştır.

Grand Chamber Hearing Big Brother Watch and Others v. The United Kingdom, Press Release, Hearings, 10.07.2019, <http://hudoc.echr.coe.int/eng?i=003-6455876-8500167>, E.T. 20.08.2019.

⁸³⁶ *Report of the Special Rapporteur on the Right to Privacy*, Advanced Unedited Version, Par. 26- 29, 27.02.2019, Human Rights Council, Fortieth Session, 25.02-22.03.2019, <https://rm.coe.int/40th-hrc-session-report-of-the-special-rapporteur-on-the-right-to-priv/1680933f08>, E.T. 20.08.2019.

işlenebileceği hususu ile 2. fıkrasında ise,

“Sağlık hizmetinin verilmesi, kamu sağlığının korunması; koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi ile sağlık hizmetlerinin planlanması ve maliyetlerin hesaplanması amacıyla Bakanlık’ın bu fıkra kapsamında elde edilen verileri alarak işleyebileceği”

ve “Bu veriler(in), KVKK’da öngörülen şartlar dışında aktarılamayacağı” hususları ele alınmaktadır. Mahkeme bu fıkralara ilişkin olarak;

“Sağlık hizmetlerinin yerine getirilebilmesi, hasta takip sisteminin iyi bir şekilde işleyebilmesi ve hastaların sağlık hizmetlerinden en iyi şekilde yararlanabilmesi için söz konusu verilerin kamu veya özel sağlık kuruluşları ile sağlık mesleği mensupları tarafından işlenmesi gerektiğini”

Bakanlık’ın da “sağlık hizmetleriyle ilgili strateji ve hedefleri belirlemek, planlama, düzenleme ve koordinasyon yapmak, acil durum ve afet hâllerinde sağlık hizmetlerini planlamak ve yürütmek, bölgesel farklılıkları gidermeye ve herkesin sağlık hizmetine erişimini sağlamaya yönelik tedbirler almak, ilgili kurum ve kuruluşların insan sağlığını doğrudan ve dolaylı olarak etkileyen faktörler ve sosyal belirleyicilerle ilgili uygulamalarına ve düzenlemelerine yön vererek bunu temin için gerekli bildirimleri yapmak, görüş bildirmek ve müeyyide uygulamak gibi görev, yetki ve sorumluluklarını yerine getirmesi bakımından”

veri işleminin gerekli olduğunu hüküm altına almıştır. Dolayısıyla bu düzenlemeler kişisel verilerin korunması hakkının özüne dokunan ya da hakkı ölçsüz biçimde sınırlandıran hükümler olarak nitelendirilmemişlerdir. Ayrıca bu fıkralara ek olarak 3., 4. ve 5. fıkralar bakımından da,

“sağlık hizmetinin gereği olarak verilmesi zorunlu kişisel verilerin işlenmesi ve güvenliğine ilişkin genel çerçevenin belirlendiği... açık, net, anlaşılır, uygulanabilir olduğu ve kamu otoritelerinin keyfî uygulamalarına karşı koruyucu önlem içerdiği...”

hususları ortaya konularak iptal istemi bu düzenleme bakımından da reddedilmiştir.

2. Ölçülülük

Buna göre ilk olarak bir anayasal hak olan ve 1961 Anayasası'nın 19. maddesinde yer alan din ve vicdan hürriyetinin kişisel veriler ile ilişkisini AYM'nin 1587 sayılı Nüfus Kanunu'nun aile kütüklerinde yer alan "din" hanesine dair kararı bağlamında ele almak yerinde olacaktır⁸³⁷. İlgili kanunun 43. maddesine göre, nüfus kütüklerinde kişinin dini yer almaktadır. Söz konusu maddenin Anayasa'ya aykırılığı iddiasıyla itiraz yoluna gidilmiş ve Anayasa Mahkemesi bu maddenin Anayasa'ya uygunluğunu incelemiştir. Karara göre;

"...bu kural, kimsenin dini inanç ve kanaatlerini açıklamasına engel değildir. Anayasa'nın izin vermediği husus zorlamadır. Bu itibarla konuya (zorlama) ögesi açısından bakmak gerekmektedir.

Söz konusu 43. madde zorlayıcı nitelikte hiç bir hüküm içermemektedir. Nüfusa kaydolunurken kişinin, Anayasa'nın kastettiği anlamda dinî inanç ve kanaatlerini de değil, sadece dininin ne olduğunu açıklamasına yol açabilecek bir durum yaratmaktadır ki, bu kuralın zorlayıcı bir niteliği ve zorlama ile ilişkisi yoktur."

denilerek hükmün Anayasa'ya aykırı olmadığına karar verilmiştir.

Görüldüğü üzere AYM bu kararda detaylı bir analiz yapmaksızın ayrımın gerekçesini net biçimde ortaya koyamamıştır⁸³⁸. Karara ilişkin karşı oy yazılarına bakıldığında ise, Nüfus Kanunu'nun 43. maddesinin dini inanç ve kanaatleri açıklamaya zorlayıcı bir etki yarattığı, bu durumun Anayasa'nın özüne aykırılık oluşturduğu ifade edilerek ölçülülük ilkesi işaret edilmiştir. *"Kişilerin dinsel inanç ve kanılarını açıklamalarını zorunlu tutan bir yasa buyruğu din ve vicdan özgürlüğü ile bağdaşmamaktadır."* Daha açık bir ifade ile söz konusu düzenleme ölçsüzdür. Bir diğer karşı oy yazısına göre de *"Nüfus Yasası'nın 43. maddesindeki dinini sözcüğünü, kütüğe yazılması için sormak açıklanmasını istemektir. Yaptırımı da zorlamayı gösterir. Sonucu*

⁸³⁷ AYM E. 1979/9, K. 1979/44, K.T. 27.11.1979.

⁸³⁸ GÖZLER, *Türk Anayasa Hukuku*, s. 140- 141.

kınamayı doğurabilir, siyasal kökenli toplumsal saldırılara neden yapılabilir.” denilerek ölçülülük ilkesini ismen ele almasa da ölçüsüz bir durum yaratacağını belirtmiştir.

1979 tarihli kararla aynı konuya değinen 21 Haziran 1995 tarihli Anayasa Mahkemesi kararı ise⁸³⁹, 1587 sayılı Nüfus Kanunu'nun 43. maddesindeki "... *dinini* ..." sözcüğünün Anayasa'nın 2. ve 24. maddelerine aykırılığı ileri sürülerek iptali istemidir. Anayasa Mahkemesi bu konudaki ilk kararı doğrultusunda hüküm açıklamıştır:

“Bireyin kişilik tanıtım ya da belirleme bilgisi olarak nüfus kütüğüne yazılacak bu özelliklerin birinin diğerinden hiçbir farkı bulunmamaktadır. Bunlar, Ulusun demografik yapısının kamu yararını ilgilendirmesi nedeniyle "şahsî hal" bilgisi olarak nüfus kütüklerine geçirilmektedir.

Devletin nesnel öğeleri, ülke ve ulusu oluşturan insan topluluğudur. Devletin, vatandaşlarının özelliklerini bilmesi gerekir.”

diyerek açıklamaktadır. 1979 yılındaki karar ile neredeyse hiçbir farkı olmayan bu kararda da AYM,

“Anayasa'nın 'Kimse ... dinî inancı ve kanaatlerini açıklamaya zorlanamaz' kuralından, kişilerin hangi dine bağlı olduğunun bir bilgi olarak resmî kayıtlara geçirilemeyeceği anlamı çıkarılamaz. Anayasa'nın izin vermediği husus, zorlamadır...

Nüfus Yasası'nın 43. maddesinin, Yasa'nın tümüyle birlikte incelendiğinde, Anayasa'nın 24. maddesinde ifadesini bulan dinî inanç ve kanaatlerin zorla açıklanmaması ve dinî inanç ve kanaatlerinden dolayı kişinin kınanmaması ve suçlanmaması ile hiçbir ilgisinin bulunmadığı açıklıkla anlaşılmaktadır. Burada dinî inanç ve kanaatler yönünden herhangi bir zorlama olmadığı gibi, bir kınama ve suçlama da söz konusu değildir...söz konusu 43. madde zorlayıcı nitelikte hiçbir hüküm içermemektedir. Nüfusa kaydolunurken kişinin, Anayasa'nın öngördüğü anlamda dinî inanç ve kanaatlerinin değil, sadece kişinin özgün durumu yönünden kamu yararı, kamu düzeni ve sosyal gereksinimlerle ilgili olarak gözönünde bulundurulmak üzere dininin

⁸³⁹ AYM E. 1995/17, K. 1995/16, K.T. 21.06.1995.

ne olduğunun açıklanması söz konusu olmaktadır ki, bu kuralın da zorlayıcı bir niteliği ve zorlama ile bir ilişkisi bulunmamaktadır.”

denilerek söz konusu düzenleme Anayasa'nın 24. maddesine aykırı bulunmamıştır. Mahkeme yaptığı değerlendirmede terazinin ağır gelen kefesine devletin vatandaşlarının demografik özelliklerini bilmesi gereğinden hareketle kamu yararı ve kamu düzenini koymuştur.

Öte yandan anılan karara ilişkin yazılan karşı oylara bakıldığında, genel olarak söz konusu düzenlemenin Anayasa'nın 24. maddesinde yer alan kişinin dini inancı veya kanaatini açıklamama özgürlüğünü ortadan kaldırdığını, kişilerin bu hususu zorla açıklamak zorunda bırakıldığı belirtilmiştir. Söz konusu karşı oylara göre Nüfus Kanunu'nun 43. maddesindeki düzenlemenin hakkın özünü zedeleyerek hakkın kullanılmasını son derece zorlaştırmakta olduğu ve hakkın varlık amacından uzaklaştırdığı söylenebilecektir. Bu kararda da 1979 yılındaki aynı konulu kararda olduğu gibi, özel nitelikli bir verinin kanuni bir düzenlemeye dayanılarak kayıt altına alınması söz konusudur. Mevcut düzenlemede ise, Anayasa'nın 20/3. maddesinde kişisel verilerin kanunla öngörülen hallerde işlenebileceği söylenmektedir. 6698 sayılı Kişisel Verilerin Korunması Kanunu'na göre de özel nitelikli veri sayılan din bilgisinin işlenmesi, kanunlarda öngörülen hallerde mümkün olmaktadır. Ancak doğaldır ki bu durumda hakkın özüne dokunma yasağı da devreye girmelidir.

Meselenin günümüzdeki uygulaması ise, her ne kadar artık yeni kimliklerde din hanesi bulunmuyor olsa da yenidoğanın nüfus kütüğünde din hanesinin boş bırakılması istendiğinde, yazılı bir dilekçe ile bu durumun kayıt altına alınması ve bu hususun dilekçe yolu ile muhafaza edilmesi biçimindedir. Durumun özeti böyle olmakla birlikte kararın kişisel veriler ile ilişkisini açıklayacak olursak, öncelikle özel nitelikli verilere, diğer bir ifade ile hassas verilere ilişkin bir durum söz konusudur. Özel nitelikli veriler ise kural olarak işlenmesi yasak olan verilerdir. Bu çerçevede GVKT'nin 9. maddesi de dini veya felsefi inançları içeren verilerin işlenmesini yasaklamaktadır. Ancak bu maddenin 2.

fıkrası uyarınca anılan verilerin belli şartlar altında işlenmeleri mümkündür⁸⁴⁰. Bu bağlamda anılan karara konu olan din hanesine dair verinin işlenmesi ancak söz konusu şartlar mevcutsa mümkün olabilecektir. Bunların dışında, kişinin rızasının “zorunlu” olarak alındığı ya da din hanesini boş bırakmanın ancak bir dilekçe ile açıkça kayıt altına alınması şartı ile gerçekleştiği hallerde, bahis konusu özel nitelikli verinin hukuka aykırı olarak işlenmesi söz konusudur.

Özel nitelikli verilerin işlenme şartları bakımından 6698 Sayılı KVKK’nın 6. maddesi de bu tür verilerin ilgilinin açık rızası olmadan işlenmesini hukuka aykırı olarak

⁸⁴⁰ GVKT’nin 9/2. maddesine göre anılan nitelikteki hassas veriler,

- Açık rızanın söz konusu olduğu hallerde;
- Veri denetleyicisi veya veri öznesinin istihdam ve sosyal güvenlik ile sosyal hukuku koruma alanındaki yükümlülüklerinin gerçekleştirilmesi ve spesifik haklarının kullanılması amacıyla işleme faaliyetinin zorunlu olduğu hallerde;
- Veri öznesi veya başka bir gerçek kişinin hayati menfaatlerinin korunması açısından işleme faaliyetinin gerekli olduğu durumlarda;
- Bir vakıf, birlik veya kâr amacı gütmeyen başka bir organ tarafından siyasi, felsefi, dini veya sendika amacıyla uygun güvencelerle birlikte yürütülen meşru faaliyetleri esnasında işlemenin ve yalnızca organın üyeleri veya eski üyeleri ya da amaçlarıyla bağlantılı olarak kendisi ile düzenli olarak temas halinde bulunan kişilerle ilgili olması ve kişisel verilerin veri sahiplerinin rızası olmaksızın söz konusu organ dışında açıklanmadığı hallerde;
- Veri öznesi tarafından açık bir biçimde kamuya açıklanan kişisel verilerin mevcut olduğu durumlarda;
- Yasal iddialarda bulunulduğu, bu iddiaların uygulanması veya savunulması açısından veya mahkemelerin kendi yargı yetkisi çerçevesinde hareket ettiği durumlarda;
- Birlik veya üye devlet hukukuna dayalı olarak kayda değer ölçüde kamu yararının bulunduğu hallerde;
- Korumacı hekimlik veya meslek hekimliği amaçları doğrultusunda, Birlik ya da üye devlet hukukuna dayalı olarak veya bir sağlık profesyoneli ile yapılan sözleşme uyarınca ve 3. paragrafta atıfta bulunulan koşullar ve güvencelere tabi olarak çalışanın çalışma kapasitesinin değerlendirilmesi, tıbbi tanı, sağlık veya sosyal bakım hizmetlerinin veya tedavinin sağlanması ya da sağlık veya sosyal bakım sistemleri ve hizmetlerinin yönetildiği hallerde işlemenin gerekli olduğu durumlarda;
- Halk sağlığı alanında kamu yararına yönelik olarak işlemenin gerektiği hallerde;
- Kamu yararına yönelik arşivleme amaçları, bilimsel veya tarihi araştırma amaçları ya da istatistiki amaçlar doğrultusunda veri işlemenin gerektiği hallerde

işleme kısıtına uğramayacaklardır.

görmektedir. Ancak olaydaki gibi, sağlık ve cinsel hayat dışındaki verilerden olan din verisinin kanun ile öngörülmesi halinde kişinin rızası olmaksızın da işlenmesi mümkün olabilmektedir. Dolayısıyla din ibaresinin nüfus kütüklerinde bulunmasının bir kanuni düzenleme neticesinde gerçekleşmesinin kişisel verilerin korunması hakkına ölçülü bir müdahale oluşturup oluşturmadığına dair Mahkeme'nin analizi gerekecektir.

Konu ile ilgili olarak İHAM'ın bakış açısını da ortaya koyabilmek adına *Sinan Işık- Türkiye*⁸⁴¹ kararına da değinmek yerinde olacaktır. Davaya konu olayda başvuru Bay Işık, 2004 yılında nüfus cüzdanındaki din hanesinde yer alan "İslam" ibaresi yerine "Alevi" ibaresinin yer alması istemiyle Mahkeme'ye başvurmuş ancak Mahkeme, *"Aleviliğin İslamın bir alt grubu olduğuna atıfta bulunan kurum görüşünü uygun bulmuş ve bundan dolayı nüfus cüzdanında İslam ibaresinin yerinde olduğuna"* karar vermiştir. Başvurucu, nüfus cüzdanındaki din hanesi sebebiyle inancını açıklamak zorunda kaldığı gerekçesiyle temyize başvurmuş, fakat Yargıtay İlk Derece Mahkemesi'nin hükmünü onamıştır. İHAM bu olayda nüfus cüzdanlarındaki din ibaresinin Türk vatandaşlarını dini kanaat ve inançlarını açıklamaya mecbur bırakan bir tedbir teşkil etmediğine dair Hükümet savunmasını ikna edici bulmamış ve İHAS'ın 9. Maddesinin ihlal edildiğine hükmetmiştir. Burada önemle belirtilmelidir ki İHAM söz konusu ihlalin, *"başvurucunun inancının nüfus cüzdanında yer almamasından değil, zorunlu ya da isteğe bağlı olsun veya olmasın, nüfus cüzdanının bir din hanesini içermesi olgusundan kaynaklandığını"* vurgulamıştır⁸⁴².

AYM'nin 5429 sayılı Türkiye İstatistik Kanunu'na ilişkin 12 Ekim 2011 tarihindeki kararı⁸⁴³ ise Kanun'a 20 Mart 2008 tarihli karar sonrası iptal edilen düzenlemenin ardından yeniden eklenen iki yeni düzenlemeye ilişkindir. Buna göre, 5429 sayılı Kanun'un yeni 8. maddesi,

⁸⁴¹ *Sinan Isik v. Turkey*, Application No: 21924/ 05, 02.05.2010, <http://hudoc.echr.coe.int/eng?i=001-97087>, E.T. 21.08.2019.

⁸⁴² *Sinan Isik v. Turkey*, Application No: 21924/ 05, 02.05.2010, Par. 49, <http://hudoc.echr.coe.int/eng?i=001-97087>, E.T. 21.08.2019.

⁸⁴³ AYMK E. 2010/12, K. 2011/135, K.T. 12.10.2011.

“İstatistikî birimler, ülkenin ekonomi, sosyal, demografi, kültür, çevre, bilim, teknoloji ve ihtiyaç duyulan diğer alanlardaki resmi istatistikleri üretmek üzere, Anayasa’da belirlenen temel haklar ve ödevler çerçevesinde, kendilerinden istenen veri veya bilgileri, Başkanlığın belirleyeceği şekil, süre ve standartlarda eksiksiz ve doğru olarak ücretsiz vermekle yükümlüdür.”

şeklindedir. 54. madde ise, 8. maddede anılan yükümlülüğe uymayanların idari para cezasıyla cezalandırılmalarına ilişkindir.

Anılan karara göre 2008 yılındaki kararda Anayasa’ya aykırı bulunan eski düzenlemeden farklı olarak, bu düzenlemede bilgi verme yükümlülüğüne Anayasa’da belirlenen temel hak ve ödevlerin ihlal edilmemesi bir sınır olarak belirlenmiştir. Mahkeme,

“İtiraz konusu kurallarla istatistiklerin kamu yararı için önemi dikkate alınarak bireylere mecburi ve ücretsiz kamusal bir külfet yüklenmiştir. Karşılaştırmalı hukukta da bazı ülkelerde bireylere istatistik amaçlı bilgi verme yükümlülüğü getirildiği görülmektedir. Modern bir devlette kamu hizmetlerinin planlanması ve kamu güvenliğinin sağlanabilmesi için bireylerin kendileriyle ilgili pek çok bilgiyi kamu otoritelerine verme yükümlülüğü bulunmaktadır. Bu bilgilerin istatistik amacıyla toplanmış olması bilgi toplamayı kendiliğinden Anayasa’ya aykırı hale getirmez...

Anayasanın diğer maddelerinde güvence altına alınan hak ve ödevler gözetilerek bilgi talep edilebilecektir. İstenilen bilgilerin bu nitelikte olduğunu düşünen istatistikî birimler, nedenini açıklayarak bilgi vermekten kaçınabileceği gibi haklarında idari para cezası uygulanması halinde buna itiraz ederek istenilen bilginin temel haklarını ihlal edecek nitelikte olduğunu mahkemeler önünde de ileri sürebilirler.

5429 sayılı Kanun’un 54. maddesinin ikinci fıkrasında, istatistikî birimlerin kendilerinden istenen bilgileri geçerli bir mazereti olmaksızın belirlenen şekil ve sürede, eksiksiz ve hatasız olarak vermek zorunluluğuna uyulmaması idari para cezası yaptırımına bağlanmıştır...İdari makamlar bireyin temel haklarını ihlal edecek şekilde bilgi talep etmeme yükümlülüğündedirler. İdari makamların bu ödevini yerine getirmemesi halinde istatistikî birimler haklarını yargı

makamları önünde arayabileceklerdir. Bu durumda itiraz konusu kurallarla bireyin hakları ile kamu yararı arasında makul bir denge kurulduğu ve bireylerin haklarına ölçüsüz bir müdahaleye izin verilmediği anlaşıldığından Anayasanın 2. maddesindeki hukuk devleti ilkesine aykırılık görülmemiştir.”

Bu karar çeşitli açılardan eleştirilebilir. Öncelikle söz konusu düzenlemede yer alan ve Mahkeme tarafından bilgi verme yükümlülüğünün sınırı olarak görülen “Anayasa’da belirlenen temel haklar ve ödevler çerçevesinde” ifadesi gereğince anılan Kanun’a göre istatistiki birimler bilgi talep edildiğinde anayasal temel hak ve ödevler çerçevesinde bilgi vermekle yükümlü kılınmıştır. Görülmektedir ki bu ifade oldukça muğlaktır. Kaldı ki kararda olduğu üzere, bilgi verme yükümlülüğünün sınırı Anayasa’da belirlenen temel hakların ve ödevlerin ihlal edilmemesi olarak görülse dahi aksi durumda ne olacağı belirsizdir. Ayrıca kendilerinden bilgi talep edilen istatistiki birimlerin, istenen verilerin Anayasa’da belirlenen temel hak ve özgürlüklere ilişkin olduğunu düşündükleri hallerde bilgi vermekten kaçınabilecekleri ve idari para cezası verilmesi halinde bu hususu mahkemeler önünde de ileri sürebilecekleri ihtimali de istatistiki birimlere yeterli bir güvence sağlamamaktadır. Verilecek bilgilerin Türkiye İstatistik Kurumu Başkanlığı’nın belirleyeceği şekil, süre ve standartlarda eksiksiz, doğru ve ücretsiz olarak verilmesi yükümlülüğü de ‘Yasama Yetkisinin Devredilemezliği İlkesi’ gereğince, Anayasa’nın 20. maddesinde öngörülen kişisel verilerin korunmasına ilişkin usul ve esasların ancak kanunla düzenlenebileceğine ilişkin güvenceye aykırıdır. Anayasa’nın açıkça kanunla düzenlenmesini öngördüğü konularda yürütme organına doğrudan ve ilk elden düzenleyici işlem yapma yetkisi verilemez.

21 Eylül 2016 tarihli *Güzide Defne Samyeli Başvurusu* da⁸⁴⁴ tıpkı AYM’nin 12 Ekim 2011 tarihli kararının yukarıda anılan bölümü çerçevesinde değerlendirilebilir. Bu olayda, Türkiye İstatistik Kurumu tarafından gerçekleştirilen Hane Halkı Bütçe Anketi’ne geçerli bir mazereti olmaksızın katılmadığı gerekçesiyle idari para cezası verilmesinin özel hayatın gizliliği hakkını ihlal ettiği iddiası mevcuttur. AYM tarafından

⁸⁴⁴ *Güzide Defne Samyeli Başvurusu*, Başvuru No: 2014/4399, 21.09.2016.

burada kişisel verilerin korunması hakkının ihlal edilip edilmediği incelenirken öncelikle kanunilik ilkesinin sağlandığı belirtilmiş ve somut olayda başvurucuya idari para cezası verilmesinin dayanağı olarak 5429 sayılı Türkiye İstatistik Kanunu'nun 8. ve 54. maddeleri gösterilmiştir. Ayrıca bu düzenlemelerin, kamu düzeni ve ülkenin ekonomik refahı meşru amaçlarına yönelik olduğu da vurgulanmıştır. Mahkeme,

“Toplumsal tüketim harcamaları ile ekonomik düzeyinin belirlenmesi ve tespit edilen veriler ışığında devletin kamu güvenliği ve planlı kalkınma hususlarında ihtiyaç duyulan tedbirleri alması için hane halklarına yönelik anket yapılması demokratik bir toplumda gerekli olarak görülebilir.”

diyerek de dava konusu ankete katılmayan başvurucuya verilen idari para cezasını Anayasa'nın 20. maddesine aykırı bulmamıştır. Anayasa Mahkemesi burada bir demokratik toplumda gereklilik incelemesine girişmiş olsa da ölçülülük incelemesini gerektiği gibi yapmamıştır.

AYM'nin söz konusu bireysel başvuru kararını, yukarıda ele alınan ve tam da bu davaya konu edilen Türkiye İstatistik Kanunu'nun 8. ve 54. maddelerinin Anayasa'ya uygun bulan 12 Ekim 2011 tarihli kararı⁸⁴⁵ ile birlikte değerlendirdiğimizde öncelikle görülecektir ki AYM, bilgi verme yükümlülüğünün sınırını Anayasa'da belirlenen temel hak ve ödevlerin ihlal edilmemesi olarak belirlemiştir:

“İstenilen bilgilerin (Anayasa'da yer alan temel hak ve özgürlükleri ihlal ettiğini) bu nitelikte olduğunu düşünen istatistikî birimler, nedenini açıklayarak bilgi vermekten kaçınabileceği gibi haklarında idari para cezası uygulanması halinde buna itiraz ederek istenilen bilginin temel haklarını ihlal edecek nitelikte olduğunu mahkemeler önünde de ileri sürebilirler.”

Ancak kanaatimizce burada hem kanunilik ilkesi hem de menfaat dengesi sebebiyle ölçülülük bakımından sorunlu bir durum karşımıza çıkmaktadır. Şöyle ki, 8. ve 54. maddeler bağlamında verilecek bilgilerin Türkiye İstatistik Kurumu Başkanlığı'nın

⁸⁴⁵ AYM E. 2010/12, K. 2011/135, K.T. 12.10.2011.

belirleyeceği şekil, süre ve standartlarda eksiksiz, doğru ve ücretsiz olarak verilmesi yükümlülüğü de yasama yetkisinin devredilemezliğine ilişkin Anayasa'nın 7. maddesi yanında 20. maddesinde öngörülen kişisel verilerin korunmasına ilişkin usul ve esasların ancak kanunla düzenlenebileceğine ilişkin güvenceye de aykırıdır. Anayasa'nın münhasıran kanunla düzenlenmesini öngördüğü konularda yürütme organına doğrudan ve ilk el düzenleyici işlem yapma yetkisi verilemez. Ek olarak, kişisel bilgileri sınırsız şekilde toplayabilen, kullanabilen, işleyebilen, saklayabilen ve aktarabilen günümüz bilişim teknolojileri karşısında savunmasız ve zayıf hale gelen bireyin korunması hususunun bu karar ile ihmal edildiği düşünülmektedir. Yine 5429 sayılı Türkiye İstatistik Kanunu'nun 1. ve 8. maddelerinde belirtilen kamu düzeni ve ülkenin ekonomik refahı amaçları arasında makul bir dengenin olması aranmalıyken, kararda bunlar arasında ülkenin ekonomik refahı lehine bir değerlendirme yapılarak ölçülülük incelemesi gereğince yapılmadığı düşünülmektedir.

Ele alınan 14 Şubat 2013 tarihli kararda olduğu gibi, 663 sayılı KHK ve sağlık verileriyle ilgili bir diğer AYM kararı ise 4 Aralık 2014 tarihli⁸⁴⁶. Anılan kararda ele alınan düzenlemelerden biri de 12 Temmuz 2013 tarih ve 6495 sayılı Kanun'un 73. maddesi ile değiştirilen 663 sayılı KHK'nın “*Bilgi toplama, işleme ve paylaşma*” yetkisi başlığını taşıyan 47. maddesidir. Bu maddeye göre;

“Bakanlık ve bağlı kuruluşları, mevzuatla kendilerine verilen görevleri, e-devlet uygulamalarına uygun olarak daha etkin ve daha hızlı biçimde yerine getirebilmek için, bütün kamu ve özel sağlık kurum ve kuruluşlarından; sağlık hizmeti alanların, aldıkları sağlık hizmetinin gereği olarak ilgili sağlık kurum ve kuruluşuna vermek zorunda oldukları kişisel bilgileri ve bu kimselere verilen hizmete ilişkin bilgileri her türlü vasıta ile toplamaya, işlemeye ve paylaşmaya yetkilidir.

Bakanlık ve bağlı kuruluşları işlediği kişisel sağlık verilerini ilgili üçüncü kişiler ve kamu kurum ve kuruluşları ile ancak bu kişi ve kurumların bu verilere erişebileceği hususunda kanunen yetkili olması hâlinde görevlerini yapmalarına yetecek derecede paylaşabilir.

⁸⁴⁶ AYM E. 2013/114, K. 2014/184, K.T. 04.12.2014.

Bakanlık ve bağılı kuruluşları, mevzuatla kendilerine verilen görevleri yerine getirebilmek için gereken bilgileri, kamu ve özel ilgili bütün kişi ve kuruluşlardan istemeye yetkilidir. İlgili kişi ve kuruluşlar istenilen bilgileri vermekle yükümlüdür.”

Bu maddenin Anayasa’nın 2., 13., 20. ve 90. maddelerine aykırılığı ileri sürülerek iptali istenmiştir. Mahkeme, bu kararda sınırlama ölçütlerinden “demokratik toplumda gereklilik” ve “ölçülülük” ilkelerini etkili bir biçimde kullanmış ve iptale konu olan 3 fıkrayı da bu doğrultuda incelemiştir. Buna göre;

“Verilen yetkiyle özel hayatın ve kişisel verilerin korunması haklarına bir sınırlama getirildiği açık olup bu sınırlama, demokratik toplum düzeni bakımından alınması gereken tedbirler kapsamında kalmaktadır...

Anılan sınırlamayla, kişilerin her türlü kişisel bilgilerinin değil, sadece sağlık hizmetinin gereği olarak ilgili sağlık kurum ve kuruluşuna vermek zorunda oldukları bilgilerin toplanması, işlenmesi ve paylaşılması yetkisi verilmektedir. Dolayısıyla bu sınırlamanın özel hayatın ve kişisel verilerin korunması haklarını bütünüyle ortadan kaldırmadığı veya ciddi surette güçleştirip amacına ulaşmasına engel olmadığı da açıktır.

Ancak kuralda söz konusu kişisel bilgilerin "her türlü vasıta" ile toplanmasına, işlenmesine ve paylaşılmasına izin verilmesi, sınırlamayı, öngörülme amacının ötesinde kişisel bilgilerin gizliliğinin keyfi şekilde ihlal edilmesi sonucunu doğurabilecek bir araca dönüştürmektedir. Bu ise sınırlama aracıyla sınırlama amacı arasında bulunması gereken makul dengeyi bozmakta, özel hayatın ve kişisel verilerin korunmasını isteme haklarına kuralda belirtilen sınırlama amacı dışında ölçüsüz bir şekilde müdahale edilebilmesine imkân tanımaktadır.

47. maddenin dava konusu (2) numaralı fıkrasında da (1) numaralı fıkarda belirtilen yöntemlerle toplanan ve işlenen kişisel verilerin ilgili üçüncü kişiler ile kamu kurum ve kuruluşlarıyla paylaşılması öngörüldüğünden yukarıda belirtilen aynı gerekçelerle bu düzenleme de ölçülülük ilkesini ihlal etmektedir.

47. maddenin dava konusu (3) numaralı fıkrasında ise ... Bakanlık ve bağılı kuruluşlarına verilen görevler çok geniş bir alanı kapsamakta

olup bu görevlerin tamamının kişilerin özel hayatlarına müdahale edilmesini gerektirecek bir toplumsal zorunluluğu bünyesinde barındırdığı söylenemez. Dolayısıyla dava konusu kuralla sadece demokratik toplum düzeni yönünden zorunlu olan sınırlamalara değil, özel hayatın ve kişisel verilerin korunması haklarına yapılabilecek her türlü sınırlamaya izin verilmesi, bir başka ifadeyle, kuralda anılan haklara sınırlama getirilirken sınırlama aracının sınırlama amacına uygun ve orantılı olarak kullanılmasını temin edecek güvencelere yer verilmemesi ölçülülük ilkesine aykırı düşmektedir.”

denilerek ilgili fıkralar iptal edilmiştir. Görülmektedir ki bu karar, her ne kadar yine 6698 sayılı KVKK'nın düzenlenmesinden önce de olsa, insan haklarının sınırlama ölçütlerinden olan demokratik toplumda gereklilik ve ölçülülük ilkeleri sayesinde kişisel verilerin korunması hakkı bakımından bu verilerin işlenmesinde uyulması gereken ilkeler gözetilerek hükme bağlanmıştır. Öte yandan söz konusu karara üç üye, ölçülülük ilkesine uyulduğu ve Kanun'da sınırlandırma aracının sınırlandırma amacına uygun ve orantılı şekilde kullanılmasını sağlayacak kanuni güvencelere de yer verilmiş olması sebebiyle, toplumun genel sağlığı ve kişilerin sağlıklarının korunması kamu yararı ile kişisel verilerin korunması hakkı arasındaki makul dengenin kurulduğu savı ile karşı çıkmışlardır. Oysa ilgili kanun maddesine göre, bireylerin kişisel bilgileri ve onlara verilen sağlık hizmetine ilişkin bilgilerin her türlü vasıta ile toplanabilmesi, işlenebilmesi ve paylaşılabilmesi, bunların hangi araçlarla gerçekleştirileceğinin önceden bilinemeyişi bakımından bir belirsizlik yaratarak ölçülülük ilkesine aykırılık teşkil etmektedir. Aynı durum bir diğer fıkroda yer alan, Bakanlık ve bağlı kuruluşlarca toplanan, işlenen verilerin üçüncü kişiler ve diğer kamu kurum ve kuruluşlarına “görevlerini yapmalarına yetecek derecede” verilmesi bakımından da geçerlidir; çünkü bu ifade yine bir belirsizlik yaratmakta ve kişisel verilerin işlenmesinde uyulması gereken ilkelere, belirsiz ve açık olmaması bakımından aykırılık teşkil etmektedir.

AYM'nin biyometrik veriler bakımından verdiği 19 Mart 2015 tarihli karar⁸⁴⁷ ise, 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu'nun 67/3. maddesine getirilen yeni düzenlemeye dairdir. Buna göre;

"Ayrıca genel sağlık sigortalısı ve bakmakla yükümlü olduğu kişilerin sağlık hizmetlerinden ve diğer haklardan yararlanabilmeleri için sağlık hizmet sunucularına başvurdıklarında 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."

Söz konusu hükme, "biyometrik yöntemlerle kimlik doğrulamasının yapılması ve/veya" ibaresi eklenmiştir. Karar ile bu ifadenin Anayasa'nın 2., 13. ve 20. maddelerine aykırılığı ileri sürülerek iptali istenmiştir. Kararda öncelikle "biyometrik yöntemlerle kimlik doğrulama" ifadesinden ne anlaşılması gerektiği ortaya konulmuştur. Buna göre;

"Biyometrik yöntemlerle kimlik doğrulama, hizmet talep eden bir kullanıcının, ölçülebilir fizyolojik ve bireysel özellikler yoluyla gerçekleştirilen ve otomatik olarak doğrulanabilen kimlik denetleme yoluyla gerçek kullanıcı olup olmadığının doğrulanması anlamına gelmektedir."

Söz gelimi parmak izi okutulması bu kapsamda değerlendirilmektedir. Mahkeme burada elde edilen biyometrik verilerin sağlık sektöründeki sahteciliklerin önüne geçmek ve bu şekilde Sosyal Güvenlik Kurumu'ndan haksız menfaat temin edilmesini engellemeye yönelik olduğu ve bu sebeple kamu yararı bulunduğunu belirterek,

"itiraz konusu kuralla özel hayatın ve kişisel verilerin korunması haklarına yönelik olarak yapılan müdahalenin, öngörülen amaçla orantılı olduğu, müdahale edilen hakların özüne dokunmadığı ve demokratik toplum düzeninin gereklerine aykırılık teşkil etmediği anlaşıldığından Anayasa'ya aykırı bir yönü yoktur."

⁸⁴⁷ AYMK, E. 2014/180, K. 2015/30, K.T. 19.03.2015.

Öte yandan itiraz konusu kuralla öngörülen yöntemin sadece sağlık sektöründe bu hizmetten yararlanma amacıyla kullanılabileceği, bu nedenle elde edilen verilerin sadece bu amaçla sınırlı olarak ve hizmetin devamı için zorunlu olduğu müddetle sınırlı olmak üzere tutulabileceği dikkate alındığında, bu verilerin neden ve hangi gerekçeyle temin edileceğine ilişkin olarak konu, amaç ve kapsamı ile ne şekilde ve hangi süreyle kullanılacaklarına dair bir belirsizlik olduğu söylenemez.

Ayrıca itiraz konusu kuralda öngörülen yöntemle elde edilen verilerin amaç ve kapsam dışında depolanması ve kullanılması hâlinde 5237 sayılı Türk Ceza Kanunu'ndaki kişisel verilerin korunmasına ilişkin ceza hükümlerinin uygulanacak olması nedeniyle bu konuda kanuni güvence de bulunmaktadır.”

denilerek iptal istemi reddedilmiştir. Ancak bu karara beş üye katılmamıştır. Karşı oyda veri koruma hukuku bakımından oldukça önemli bir belirleme yapılmış ve Kanun’da her ne kadar “ve/ veya” bağlacı tercih edilmiş olsa da

“Sosyal Güvenlik Kurumu Sağlık Uygulama Tebliği'nde "ve/veya" bağlacı yerine "ve" bağlacı kullanıldığından biyometrik yöntemlerle kimlik doğrulaması uygulamada zorunlu hale getirilmiştir. Sağlık hizmetinden yararlanmak isteyenler biyometrik kimlik doğrulamasını kabul etmediklerinde sağlık hizmeti alamamaktadır. Bu da sağlık hizmeti almak isteyenlerden zorla kişisel veri alınması ile eşanlamlı...”

oluşu hususlarına dikkat çekilmiştir.

Burada belirtilmelidir ki, kişisel verilerin işlenmesinin temel şartı veri öznesinin açık rızasıdır. Bu düzenleme bakımından 6698 sayılı KVKK’nın 5. maddesine bakılacak olursa, açık rıza olmaksızın veri işlenilebilecek hallerden biri de “Kanunlarda açıkça öngörülme”dir. Olayda her ne kadar bir kanunda açıkça öngörülen bir veri işleme metodu varsa da düzenlemede biyometrik yöntemlerle yapılacak kimlik doğrulaması sonucu elde edilen kişisel verilerin toplanması ve işlenmesinin kapsamı ile bu verilerin ne şekilde silineceği, hangi süre ile tutulacakları hususları da belirsizdir. Bu ise, KVKK’nın 4. maddesinde ele alınan ve aslında temel veri işleme prensiplerinden yola çıkılarak hazırlanan kişisel verilerin işlenmesinde uyulması gereken ilkelerden “işlendikleri

amaçla bağlantılı, sınırlı ve ölçülü olma” ve “ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme” hususlarına da aykırılık teşkil etmektedir. Ayrıca karar tarihinde henüz, Anayasa’nın 20/3. maddesinde belirtilen ve kişisel verilerin işlenmesine dair usul ve esasların yer alacağı öngörülen kanuni düzenleme mevcut değildir. Dolayısıyla Avrupa Konseyi’nin 108 Numaralı Kişisel Verilerin Otomatik İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşmesi’nin 6. maddesine bakılmalıdır. İlgili maddeye göre,

“İç hukukta uygun güvenceler sağlanmadıkça, ırksal kökeni, siyasi düşünceleri, dini veya diğer inançları ortaya koyan kişisel veriler ile sağlık veya cinsel hayatla ilgili kişisel veriler, otomatik işleme tabi tutulmaz. Aynı şey ceza mahkumiyetiyle ilgili kişisel veriler için de geçerlidir.”

Görüleceği üzere, her ne kadar ilgili tarihte kişisel verilerin korunması hakkına dair gerekli kanuni düzenleme yapılmamış olsa da uluslararası metinlerde iç hukukta uygun güvencelerin mevcut olmadığı durumlarda sağlık verilerinin otomatik işleme tabi tutulamayacağı belirtilmektedir. Burada önemle altı çizilmelidir ki, kişisel verilerin korunmasına ilişkin gerekli kanuni altyapı olmadan ve teknik olanaklar sağlanmadan bir kamu ya da özel kuruluşun, kanunilik ve kişinin rızası koşullarını sağlaması halinde dahi veri işlemesi hukuka uygun değildir.

AYM’ye bireysel başvurular bağlamında kişisel verilerin korunması bakımından “Unutulma Hakkı”nın konu edildiği 3 Mart 2016 tarihli *N.B.B. Başvurusu*⁸⁴⁸ oldukça önem taşımaktadır. Başvuruya konu olay, ulusal ölçekte yayın yapan bir gazetenin internet arşivi sayfalarında, başvuru hakkında uyuşturucu kullandığı iddiasıyla yürütülen bir ceza kovuşturması neticesinde adli para cezasına hükmedildiğine dair 1998’de iki, 1999’da bir defa yayınlanan toplam üç adet haberin yayından kaldırılması yönündeki talebin reddedilmesine ilişkindir. AYM ilk olarak kişisel verilerin korunması hakkının kapsamını ortaya koymuş ve bu hakkın yalnızca kişisel verilerin işlenmesi sırasında değil, işlendikten sonra da düzeltilmesini veya silinmesini talep etme hakkını da

⁸⁴⁸ *N.B.B. Başvurusu*, Başvuru No: 2013/5653, K.T. 03.03.2016.

içerdiğini belirtmiştir. Bu doğrultuda Mahkeme, karara konu olan olayda başvurucunun geçmişte haber yapılmış ve gerçeğe aykırılığı ileri sürülmemiş meselenin artık hatırlanmasının istenmediğini, daha açık bir söyleyişle kararın odak noktasının, internet ortamındaki arşivlerdeki haber içeriğinde yer alan kişisel verilere erişimin engellenerek kişilerin unutulmasının sağlanması olduğunu belirtmiştir. Ayrıca olayın ifade ve basın özgürlüğü ile şeref ve itibarın korunması arasında dengenin kurulmasıyla ilgili olduğu ve anılan dengenin şeref ve itibar yönünden bireylerin unutulma hakkının kabul edilmesi ile sağlanabileceği hususu dile getirilmiştir:

“Anayasa’nın 17. Maddesinde düzenlenen kişinin manevi bütünlüğü bağlamında şeref ve itibarının korunması hakkı ve Anayasa’nın 20. Maddesinin üçüncü fıkrasında güvence altına alınan kişisel verilerin korunmasını isteme hakkı ile birlikte düşünüldüğünde, devletin bireye geçmişte yaşadıklarının başkaları tarafından öğrenilmesi engellenerek “yeni bir sayfa açma” olanağı verme hususunda bir sorumluluğu olduğu açıktır. Özellikle kişisel verilerin korunması hakkı kapsamında kişisel verilerin silinmesini talep edebilme hakkı, kişilerin geçmişte yaşadıkları olumsuzlukların unutulmasına imkân tanımayı kapsamaktadır. Dolayısıyla Anayasa’da açıkça düzenlenmeyen unutulma hakkı, internet vasıtasıyla ulaşılması kolay olan ve dijital hafızada bulunan haberlere erişimin engellenmesi için Anayasa’nın 5., 17. ve 20. Maddelerinin doğal sonucu olarak karşımıza çıkmaktadır.”

Mahkeme burada yerinde bir değerlendirme yaparak unutulma hakkının, basın özgürlüğünü ortadan kaldıracak biçimde her olaya uygulanmayıp, somut olaylar bağlamında değerlendirilmesi gerektiğini belirtmiş ve internette yer alan bir haberin unutulma hakkı bağlamında internet ortamından kaldırılması için,

“...yayının içeriği, yayında kaldığı süre, güncelliğini yitirme, tarihsel bir veri olarak kabul edilmeme, kamu yararına katkısı (toplumsal açıdan haberin değeri, haberin geleceğe ışık tutan niteliği) habere konu kişinin siyasetçi veya ünlü olup olmadığı, haber veya makalenin konusu, bu bağlamda haberin olgusal gerçekler ya da değer yargısı içerip içermediği, halkın ilgili veriye yönelik ilgisi gibi hususların”

dikkate alınması gereği ortaya konmuştur. Bu genel ilkeler çerçevesinde somut olayda,

“... toplumsal açıdan haber değerinin devam ettiği veya haberin geleceğe ışık tutacak nitelikte bir haber olduğu söylenemez.

Başvuru tarihi itibarıyla söz konusu haberin yaklaşık on dört yıl önceki bir olaya ilişkin olduğu ve böylelikle güncelliğinin yitirdiği açıktır. ... Bu bağlamda kamu yararı bakımından siyasi veya medyatik bir kişiliğe sahip olmayan başvuru hakkında internet ortamında yayınlanan haberlerin kolaylıkla ulaşılabilirliğinin başvurunun itibarını zedelediği açıktır.”

denilerek başvuru hakkındaki haberlerin unutulma hakkı kapsamında değerlendirilerek şeref ve itibarının korunması için anılan haberlere erişimin engellenmesi gerektiği ve böylece ifade ve basın özgürlükleri ile kişinin manevi bütünlüğünün korunması hakkı arasında adil bir denge kurulması gerektiği ve bu hususların eksikliği sebebiyle Anayasa’nın 17/1. maddesindeki şeref ve itibarın korunması hakkının ihlal edildiği hüküm altına alınmıştır.

Bu kararın Türk hukuku bakımından önemine değinecek olursak, anılan karar AYM’nin “unutulma hakkı”nı tanımış olduğu ilk karar olarak karşımıza çıkmaktadır⁸⁴⁹. AB Adalet Divanı’nın kısaca *Google- İspanya*⁸⁵⁰ olarak bilinen kararı ile uluslararası alanda tanınır hale gelen ve sonrasında GVKT’de açık bir biçimde tanınan bu hakka ilişkin olarak her ne kadar belirli bir düzenleme bulunmasa da AYM bu hakkı, Anayasa’nın kişinin maddi ve manevi varlığını geliştirme hakkı ve özel hayatın gizliliği bağlamında kişisel verilerin korunması hakları kapsamında değerlendirerek tanımıştır. Kaldı ki AYM daha sonra 4 Ekim 2017 tarihli *Asli Alp ve Şükrü Alp Başvurusu*⁸⁵¹,’nda yeniden, ifade ve basın hürriyeti ile şeref ve itibarın korunması arasındaki dengenin

⁸⁴⁹ Türk hukukunda “unutulma hakkı”nı tanıyan ilk karar Yargıtay Hukuk Genel Kurulu’nun 17 Haziran 2015 tarihli kararı olarak karşımıza çıkmaktadır. Bu kararda Yargıtay HGK unutulma hakkını bahis konusu ederek “davacının kişilik haklarının ihlal edildiği”ne hükmetmiştir.

YHGK, E. 2014/4-56, K. 2015/1679, K.T. 17.06.2015.

Aydın AKGÜL, “Kişisel Verilerin Korunmasında Yeni Bir Hak: ‘Unutulma Hakkı’ ve AB Adalet Divanı’nın ‘Google Kararı’”, TBB Dergisi, Y. 2016, S. 116, s. 34, ss. 11- 38.

⁸⁵⁰ *Google Spain SLand Google Inc. V. Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzalez*, 13.05.2014, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131>, E.T. 15.04.2019.

⁸⁵¹ *Asli Alp ve Şükrü Alp Başvurusu*, Başvuru No: 2014/18260, K.T. 04.10.2017.

unutulma hakkı ile kurulabileceğine değinerek bu hakkı anayasal içtihatlarla sağlamlaştırmıştır. Unutulma hakkı ayrıca 6698 sayılı KVKK bağlamında da ele alınabilecektir. İlgili Kanun'un 7. maddesine göre,

“Bu kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olan verilerin, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir.”

Kanun'un bu hükmü bağlamında da unutulma hakkı dile getirilebilecektir.

Kişisel verilerin korunması hakkının ele alındığı bir diğer karar ise 11 Mayıs 2016 tarihli *Bülent Kaya Başvurusu*⁸⁵²dur. Bu başvuruda, başvuru hakkında görülmekte olan bir ceza davasına ilişkin olarak İçişleri Bakanlığı Kaçakçılık, İstihbarat, Harekât ve Bilgi Toplama Daire Başkanlığı Bilgi Toplama Yönergesi uyarınca Bilgi Formu tanzim edilerek Genel Bilgi Toplama (GBT) sistemine kaydedilmesi ve söz konusu kaydın silinmesine dair yapılan başvuru ve açılan davanın reddi gerekçe gösterilerek özel hayatın gizliliğinin ihlal edildiği iddiası incelenmiştir. Bu kararda veri koruma hukukunun anayasal çerçevesi bakımından ortaya konan husus, kamu mercileri tarafından kayıt altına alınan kişisel verilerin hangi çerçevede elde edildiği, saklandığı, verilerin türü, işlenme şekli ve bunların neticesinde çıkacak sonuçların özel hayatın gizliliği hakkını ihlal edip etmediğidir. Mahkeme burada, kişisel veri olduğuna şüphe bulunmayan bilgilerin GBT sistemine kayıtlanmasını incelerken durumun kanuni dayanağının mutlaka,

“...kişisel verilerin kayıt, muhafaza ve kullanımını içeren tedbirlerin kapsamını ve uygulanmasını düzenleyen ve özellikle süre, stoklama, kullanım, üçüncü kişilerin erişimi, verilerin gizliliği, bütünlüğü ve imhası konusundaki prosedürlere ilişkin, muhataplarının yetki aşımı ve keyfiliğe karşı yeteri kadar güvenceye sahip olmalarını sağlayacak açık ve detaylı kuralları...”

içermesini esas almaktadır. Olaya esas düzenlemelerin kanunilik şartını taşıdığı belirtilerek özellikle kişisel verilerin korunması gibi özel yaşamın gizliliğinin oldukça

⁸⁵² *Bülent Kaya Başvurusu*, Başvuru No: 2013/2941, K.T. 11.05.2016.

hassas bir yönünün etkilendiği olaylarda mutlaka bireyin ve kamusal makamların yarışan menfaatleri arasında bir denge kurulması gereği dile getirilmektedir. AYM somut olay bakımından

“söz konusu verilerden, toplama, muhafaza ve kullanım hususunda tespit edilen amaç dışında yararlanıldığına ilişkin herhangi bir iddiada bulunulmadığı anlaşılmaktadır.

...başvuruya konu müdahalenin demokratik toplumda gerekli ve ölçülü olmadığı söylenemez.”

diyerek Anayasa’nın 20. maddesinin ihlal edilmediğine hükmetmiştir.

Anılan olay bakımından bir değerlendirme yapmadan önce, GBT sistemine kayıt hususunun kanuni dayanağının anlaşılması karar bakımından önem taşımaktadır. Buna göre, söz konusu uygulamanın kanuni temeli olarak gösterilen 2559 sayılı Kanun’un 7. maddesine dayanılarak hazırlandığı belirtilen Yönerge’nin 9/(a). maddesinde, (b) fıkrasında⁸⁵³ belirtilen suçları işlemiş ve yakalanmış olan sanıklar için de suç türüne uygun bilgi formu doldurulacağı ve yakalandığı ifadesi ile sistemde muhafaza edileceği belirtilmektedir. Ancak bu düzenlemeye detaylı bakıldığında bilgilerin toplanma

⁸⁵³ 2559 sayılı Polis Vazife ve Salahiyet Kanunu’nun 7. Maddesine dayanılarak hazırlanan “Bilgi Toplama Yönergesi’nin veri toplama ve kayıtlamaya dair temel alınan ilgili hükümleri için bkz. *Bülent Kaya Başvurusu*, Par. 26 vd., Başvuru No: 2013/2941, K.T. 11.05.2016.

"Sanıkların yakalanması halinde dahi bilgi formu düzenlenecek suç türleri ve bunlar hakkında yapılacak işlemler" başlıklı 9. maddesinin ilgili kısımları şöyledir:

"a) Bu maddenin (b) fıkrasında belirtilen suçları işlemiş ve yakalanmış olan sanıklar için suç türüne uygun bilgi formu doldurulur. Bilgi Toplama Programına veri girişi yapıldığında "YAKALANDI" seçeneği işaretlenir ve bilgi formunun ortasına "YAKALANDI" kaşesi basılır. Bilgi Toplama Programının "SUÇ DETAY BİLGİLERİ" sayfasındaki bölüme ve ilçe güvenlik kuvvetinde ve emniyet şube müdürlüklerinde kalan bilgi formuna soruşturmacı evrakının Cumhuriyet Başsavcılığına gönderiliş tarih ve numarası yazılır.

b) Sanığı yakalanmış olsa dahi hakkında bilgi formu açılacak suç türleri.

...

14- 3713 Satılı Terörle Mücadele Kanunu kapsamına giren suçlar

...

Bilgi Toplama Yönergesi’nin *"Şahıslar hakkında açılmış olan bilgi formlarının iptal edilmesi"* başlıklı 16/(b). Maddesi şöyledir: *"b) Yönerge'nin 9/b maddesi kapsamına giren suçlara ait bilgi formlarının iptali; Bu Yönerge'nin 9/b maddesinin bentlerinde yazılı suç sayılan fiilleri işleyenler hakkında adli makamlarca, beraat, ceza verilmesine yer olmadığı, davanın düşmesi veya dava zamanaşımı nedeniyle davanın ortadan kaldırılmasına karar verilmiş ve kararın kesinleşmiş olması halinde bilgi formları iptal edilir."*

koşulları, amacı, süresi gibi nitelikler bulunmadığı görülecektir. Genel Bilgi Toplama Yönergesi kaydedilen verilere ne olacağına ilişkin olarak da ikili bir ayırım yapmaktadır. Bu düzenlemeye göre,

- Yönerge'nin 9/(b). maddesi kapsamına girmeyen suçları işleyip firar edenlerin yakalanmaları halinde bu kişiler hakkında,
- Askeri suçlardan arananların Askerlik Şube Başkanlıklarınca takibinin durdurulmasına dair güvenlik güçlerine yazı gönderilenler hakkında,
- Belli hakları kullanmaktan yoksun bırakılma (kamu hizmetlerinden men) cezası alanlar hakkında,

kayıtlı veriler iptal edilip düşürülür. Öte yandan Yönerge'nin 9/(b). maddesi kapsamına giren suçlarda ise beraat veya dava zaman aşımı nedeniyle davanın ortadan kaldırılmasına karar verildiğinde bilgi formları iptal edilse dahi söz konusu formlar imha edilmemekte ve arşive alınmaktadır. Ayrıca af, şartlı tahliye, adli sicil kaydının silinmesi, cezanın paraya çevrilmesi, tecil edilmesi ve ceza zaman aşımı kararlarından biri verilse bile hakkındaki bilgi formu iptal edilmemektedir. Dolayısıyla sisteme kayıtlanan bazı verilerin hiç silinmemesi gibi bir durum ortaya çıkmaktadır⁸⁵⁴. Bu halde söz konusu

⁸⁵⁴ GBT Sistemine kayıtlanacak verilerin akıbeti konusunda bkz. Kaçakçılık İstihbarat Harekât ve Bilgi Toplama (KİHBİ) Daire Başkanlığı Bilgi Toplama Yönergesi, <https://kms.kaysis.gov.tr/Home/Goster/134544>, E.T. 16.04.2019.

Yönerge'nin 9/(b). Maddesi kapsamına girmeyen suçları işleyip firar edenlerin yakalanmaları halinde haklarında açılan bilgi formları iptal ve tasniften çıkarılarak imha edilir. Askeri suçlardan aranır iken Askerlik Şube Başkanlıklarınca takibinin durdurulmasına dair güvenlik güçlerine yazı gönderilenler hakkında bilgisayardaki kayıtları iptal edilir. Belli hakları kullanmaktan yoksun bırakılma (kamu hizmetlerinden men) cezası alanların bilgi formları verilen ceza süresinin bitiminde iptal edilir.

Yönerge'nin 9/(b). Maddesi kapsamına giren suçlarda ise Genel Bilgi Toplama Sistemi'ne kaydedilen bilgilerin iptal ve düşüm işlemleri, Yönerge'nin 17/(c), (d) ve 18/(a). maddelerine göre yapılacaktır. Buna göre; şüpheli/sanık yakalandığında, kişinin aranmasına ilişkin kayıt ile ilgili olarak düşüm işlemi yapılır ve sanığın "Aranıyor" kaydı "Yakalandı" şeklinde değiştirilerek, mevcut bilgi formuna "Yakalandı" kaşesi vurulur. Yönerge'nin 9/(b). Maddesinde yazılı suçları işleyenler hakkında beraat veya dava zaman aşımı nedeniyle davanın ortadan kaldırılmasına karar verildiğinde bilgi formları iptal edilir; ancak bu hallerde dahi bilgi formu imha edilmeyecek, yalnızca tasniften çıkarılarak iptal evrakı ekinde arşive alınacaktır. Yine Yönerge'nin 17/(d). maddesine göre; *"Sanık hakkında, af, şartlı tahliye, adli sicil kaydının silinmesi, cezanın paraya çevrilmesi, tecil edilmesi ve ceza zaman aşımı kararı verilmesi halinde bilgi formu iptal edilmeyecektir."*

verilerin kişinin ömrünün sonuna kadar saklanması durumu söz konusu olacak ve yalnızca GBT kapsamında bu verilere erişebilen görevliler dışında da bir kesimin arşivde sürekli tutulan bu verilere erişebilmesi tehlikesi doğabilecektir. Her ne kadar bu durumun başta terör olmak üzere suçla ve suçlulukla mücadele, kamu güvenliği ve kamu düzeni gibi meşru amaçlar bakımından zorunlu olduğu söylenebilecekse de uygulamada GBT sisteminin ölçüsüzce genişletilebileceği de dikkatten kaçmamalıdır. Bu bakımdan anılan kanuni düzenlemenin 6698 sayılı KVKK'nın kişisel verilerin işlenmesinde uyulacak ilkeleri içeren 4. maddesinin (ç) ve (d) bentlerinde belirtilen *“İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma”* ve *“İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme”* ilkelerine uygun düşmediği ve dolayısıyla Anayasa'nın 20. maddesine aykırılık teşkil ettiği söylenebilecektir.

Mahkûmiyet kararları ve ceza gerektiren suçlara ilişkin kişisel verilerin işlenmesi konusunda GVKT'nin ilgili 10. madde düzenlemesine baktığımızda bu verilerin işlenebilmesi;

- Resmi bir merciin denetimi altında veya
- Veri öznelerinin hak ve özgürlüklerine uygun güvenceler sağlanması şartıyla Birlik veya üye devlet kanunlarında düzenlenmiş olduğu

hallerde mümkün olabilmektedir. Yine aynı hükme göre GVKT, mahkûmiyet kararlarına ilişkin sicillerin yalnızca resmi merciin denetimi altında tutulabilmesine cevaz vermektedir. Daha açık bir deyişle suçlar ve mahkûmiyetler hakkında GVKT kapsamında kişisel verileri işlemek için hem Tüzük'ün 6. maddesine göre hukuka uygun bir şekilde veri işlemenin şartları sağlanmalı hem de 10. maddede bahsedilen yasal veya resmi yetkiye sahip olunmalıdır. Dolayısıyla GVKT'ye ilişkin bilgiler ışığında AYM kararına konu olan GBT Sistemi'ne kayıt ve devamında verilerin silinmemesi durumu incelendiğinde kanuni bir dayanağın mevcut olduğu görülse de bazı durumlarda verilerin saklanacağı sürenin sınırsız oluşu ve erişim izni olmayan görevlilerin de arşive erişim risklerinin bulunması sebepleriyle veri öznelerinin hak ve özgürlüklerine uygun güvencelerin sağlanamadığı ve GVKT'ye de aykırılık olduğu görülmektedir.

Avrupa Mahkemesi'nin de geçmişteki suç kayıtlarına ilişkin tutumunun anlaşılması bakımından *Bülent Kaya Başvurusu*'nun oldukça benzeri olan ve ilgili bölümde özellikle DNA örneklerinin kişisel veri oluşturması bakımından değerlendirilen *S. ve Marper- Birleşik Krallık*⁸⁵⁵ kararına da bu noktada değinmek önem arz etmektedir. Davaya konu olayda Birleşik Krallık vatandaşları Bay S. ve Bay Marper'in parmak izleri ve DNA örnekleri yakalandıkları esnada alınmıştır. Devamında Bay S. beraat etmiş ve Bay Marper aleyhindeki dava da uzlaşma neticesinde düşürülmüştür. Ancak kendilerinden alınan bu örnekler, 2001 tarihli Ceza Adaleti ve Polis Kanunu ile değişik Polis ve Cezai Delil Kanunu'nun ilgili hükmüne göre suçların soruşturulması esnasında alınan parmak izleri ve DNA örnekleri bazı durumlarda kişinin beraat ettiği hallerde dahi saklanabildikleri için talep etmelerine rağmen silinmemiştir. İHAM bu davada bahis konusu verilerin saklanması başvuranların özel yaşama saygı haklarına ilişkin ölçüsüz bir müdahale oluşturduğuna ve bu durumun demokratik bir toplumda gerekli olmadığına hükmetmiştir.

Kişisel verilerin korunması ile ilgili bir diğer bireysel başvuru kararı da 24 Mayıs 2018 tarihli *Kemal Karanfil Başvurusu*⁸⁵⁶dur. Karara konu olan olayda, Fethulahçı Terör Örgütü/Paralel Devlet Yapılanması (FETÖ/PDY) soruşturması kapsamında 20 Temmuz 2016 tarihinden beri tutuklu olan başvurucuya gelen veya başvurucu tarafından gönderilen mektupların Ulusal Yargı Ağı Bilişim Sistemi'ne kaydedilmesi nedeniyle özel hayata saygı hakkı ve haberleşme hürriyetinin ihlal iddiası mevcuttur. AYM İkinci Bölümü burada öncelikle olaya konu olan “mektupların kaydedilmesi” işleminin kişisel veri oluşturduğunu,

*“Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında
Bireylerin Korunması Sözleşmesi ile 6698 sayılı ...Kanun'a göre kişisel
bilgi, belirli veya belirlenebilir bir kişiye ilişkin herhangi bir bilgi*

⁸⁵⁵ *S. and Marper v. The United Kingdom*, Application Nos: 30562/04 and 30566/04, 04.12.2008, <http://hudoc.echr.coe.int/eng?i=001-90051> , E.T. 03.11.2017; Karara ve Türk adli yargı sisteminde DNA örnekleri ve profillerinin saklanması ile imhası konularına dair detaylı bir analiz için bkz. R. Barış ERMAN, “Adli Yargı Sisteminde DNA Örnekleri ve Profilleri- S. ve Marper- Birleşik Krallık Davası”, *Fasikül Hukuk Dergisi*, C. 2, S. 11, Y: 2010, ss. 20- 23.

⁸⁵⁶ *Kemal Karanfil Başvurusu*, Başvuru No: 2017/24776, K.T. 24.05.2018.

olarak tanımlanmakta... ceza infaz kurumlarında bulunan mahpusların yazdığı veya kendilerine hitaben yazılan mektupların UYAP sistemine taranması suretiyle kaydı sağlandığından sadece mektup içeriklerinin değil aynı zamanda mektuplardaki el yazısı, imza gibi mektubu yazanı belirlemeye yarayan her türlü bilgi kişisel veri sayılmaktadır.”

şeklinde ifade ederek olayı veri koruma hukuku bakımından incelemeye almıştır. Mahkeme ayrıca burada mektupların içeriklerinin ve biçiminin denetlenerek bir sisteme kaydedilmesini hem özel hayata hem de haberleşme hürriyetine müdahale olarak değerlendirmiştir. İlk olarak AYM bu müdahalenin kanunilik şartının, Adalet Bakanlığı'nın 10 Ekim 2016 tarihli Genelge niteliğinde bir düzenleyici işlem olan yazısı ile 5275 sayılı Kanun'un 38/(a). ve 68. maddelerinin 6698 sayılı KVKK bakımından mevcut olduğunu ve kamu düzeni ile güvenliğin sağlanması meşru amacının güdüldüğünü belirtmiştir. Bu bakımdan,

“Yazışmaların denetiminin amacının, öncelikle suç işlenmesinin önlenmesi ve ceza infaz kurumunun güvenliğinin sağlanması ve böylelikle kamu düzeninin korunması olduğu gözönüne alındığında denetimin bir parçası olan verilerin kaydı suretiyle bireyin mahremiyet hakkına yapılan müdahalenin toplum menfaati karşısında gerekli olmadığını söylemek mümkün görünmemektedir.

Öte yandan somut başvuruda uygulanan tedbirin mahpuslara gönderilen veya mahpuslarca başkalarına gönderilen mektupların UYAP ortamına kaydedilmesinden ibaret olduğu anlaşılmaktadır. Kişisel veri mahiyetindeki bu yazışmaların ceza infaz kurumunun yetkili personeli hariç herhangi bir üçüncü kişinin erişimine veya kullanımına açılması söz konusu değildir. Bu yazışmaların muhafazası hususunda yeterli düzenlemenin mevcut olduğu anlaşılmaktadır. Ayrıca bilgilere erişim yetkisi bulunan -çok sınırlı sayıdaki- yetkili kişilerin bunu kötüye kullanması veya kanunda öngörülen haller dışında başka kişi ve kurumlara vermesi veya onların erişimine dahi açık hale getirmesi halinde bunlara yönelik olarak uygulanacak idari, cezai ve hukuki müeyyideler kanunlarda öngörülmektedir.”

denilerek müdahalenin başvuruca aşırı bir külfet yüklediği ve güvenliğin sağlanmasındaki kamu yararı ile başvuruca kişisel verilerinin korunması ve haberleşme hürriyetine ilişkin yararı arasındaki makul dengenin gözetildiği sonucuna

varılarak Anayasa'nın hem 20. hem de 22. maddelerine aykırılık tespit etmemiştir. Diğer yandan durumun önemine dair Mahkeme tutuklu ve hükümlülerin mektuplarının kaydı hususunda kamu makamlarına sınırsız yetki verilmediğini ve meşru amacın ortadan kalktığı durumlarda ihlal sonucunun doğabileceğini de vurgulamıştır.

Bu karar bakımından üzerinde durulması gereken husus, Bakanlık'ın 10 Ekim 2016 tarihinde yayımladığı Genelge biçimindeki yazısıdır. Bu yazıya göre, tüm tutuklu ve hükümlülerin resmi makamlara veya savunması için avukatına verdiği kapalı zarf içindeki mektup, fakslar hariç diğer tüm faks ve dilekçelerin taranmak suretiyle UYAP sistemine kaydedilmesi gerektiği belirtilmektedir.

Tüm tutuklu ve hükümlülerin cezai süreçle ilgisi dahi olmayan tüm kişisel verilerinin UYAP sisteminde tutulacak olması, süre, üçüncü kişilerle paylaşım gibi unsurlar bakımından 6698 sayılı KVKK'nın 4. maddesinde ele alınan kişisel verilerin işlenmesine dair temel ilkelerden *“İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma”* ve *“İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme”* başlıklarına ve dolayısıyla Anayasa'nın 20/3. maddesinde düzenlenen kişisel verilerin korunması hakkına aykırılık teşkil ettiği söylenebilecektir.

Bireysel başvuru kararları bakımından kişisel verilerin korunması hakkına dair bir başka karar olarak 7 Haziran 2018 tarihli *E.Ç.A. Başvurusu*⁸⁵⁷ göze çarpmaktadır. Bu karara konu olayda, başvurucunun hırsızlık suçlarına ilişkin adli sicil kayıtlarının belli bir tarihten sonra silinmesine karşın Genel Bilgi Toplama Sistemi'nden silinmemesi ve hakkındaki bilgi formlarının iptal edilmemesinin Anayasa'nın 20. maddesinin ihlal ettiği iddiası söz konusudur. Başvurucu, hakkında uzun zaman önce verilmiş mahkûmiyet hükümlerinin GBT sisteminde hala bulunuyor olması sebebiyle polis kontrollerinde kendisine karşı tutumun değiştiğini ve aile üyelerinin yanında küçük düştüğünü ileri sürmüştür. Mahkeme burada kanunilik ve meşru amaç kriterlerinin, oldukça kısa biçimde

⁸⁵⁷ *E.Ç.A. Başvurusu*, Başvuru No: 2014/5671, K.T. 07.06.2018.

ve daha evvel değinilen kararlardaki gerekçeleri esas alarak karşılandığını belirtmiştir. Kararda,

“ceza mahkumiyetine esas olan hırsızlık suçunun Yönerge'nin 9/(b). Maddesinde yer alan suçlar arasında olduğu görülmektedir. Bu verilerin polis ve idari merciler tarafından kullanılmasının gizlilik kurallarına tabi olduğu, açık şekilde belirlenmiş durumlarla sınırlı tutulduğu, ilgili bilgilerin toplanma, paylaşım, kullanım ve silinmesine ilişkin hususların ayrıntılı olarak düzenlendiği anlaşılmaktadır.”

denilmiş ve 6698 sayılı KVKK'nın

“Kişisel verilere ilişkin suçlar bakımından 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununun 135 ila 140 ıncı madde hükümleri uygulanır.

Bu Kanunun 7 nci maddesi hükmüne aykırı olarak; kişisel verileri silmeyen veya anonim hâle getirmeyenler 5237 sayılı Kanunun 138 inci maddesine göre cezalandırılır.”

hükmünü içeren 17. maddesi de temel alınarak eldeki verilerin amacı dışında kullanılmasını önleyecek ve kişisel verilerin ifşa edilmesinin önüne geçecek güvencelerin sağlandığı dile getirilmiştir. Ek olarak

“söz konusu verilerin toplanması, muhafazası ve kullanımı hususunda tespit edilen amaç dışında yararlanıldığına yahut (başvurucunun iddia ettiği) özel yaşamı ve çalışma hayatı bakımından olumsuz sonuçlar doğurduğuna ilişkin somut olgulara dayalı herhangi bir delil başvuru tarafından ortaya konulamamıştır. Bu nedenlerle müdahalenin demokratik toplumda gerekli ve ölçülü olmadığı söylenemez.”

denilerek Anayasa'nın 20. maddesine bir aykırılık tespit edilmemiştir.

Bu karar özelinde belirtilmelidir ki, tıpkı *Bülent Kaya Başvurusu*'nda olduğu gibi, Genel Bilgi Toplama Sistemi'ne kayıtlanacak veriler için her ne kadar AYM çoğunluk görüşü,

“Bu verilerin polis ve idari merciler tarafından kullanılmasının gizlilik kurallarına tabi olduğu, açık şekilde belirlenmiş durumlarla sınırlı tutulduğu, ilgili bilgilerin toplanma, paylaşım, kullanım ve silinmesine ilişkin hususların ayrıntılı olarak düzenlendiği anlaşılmaktadır.”

şeklinde hüküm kurarak uygulamaya temel oluşturan 2559 sayılı Kanun'un 7. maddesine dayanılarak hazırlandığı belirtilen Yönerge'nin 9. ve ilgili maddelerinin kişisel verilerin korunmasına dair yeterli güvenceyi sağladığını ifade etse de, anılan düzenlemeye dair *Bülent Kaya Başvurusu*'nda yaptığımız değerlendirme doğrultusunda yeniden belirtmeliyiz ki, bu düzenlemede bilgilerin toplanma koşulları, amacı, süresi ve silinmesi gibi hususlar eksik olduğu için 6698 sayılı KVKK'nın kişisel verilerin işlenmesinde uyulacak ilkeleri içeren 4. maddesine ve dolayısıyla Anayasa'nın 20. maddesine aykırılık teşkil ettiği söylenebilir.

III. AVRUPA VERİ KORUMA HUKUKUNUN ULUSAL HUKUKA ETKİLERİNİN DEĞERLENDİRİLMESİ

Avrupa'da 1970'lerden itibaren gelişim gösteren veri koruma hukuku, Türkiye özelinde benzer biçimde ilerlememiştir. Türkiye her ne kadar 28 Ocak 1981 tarihinde imzaya açılmış olan Avrupa Konseyi'nin 108 Numaralı Kişisel Verilerin Otomatik İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşmesi'ni aynı gün imzalamışsa da devamında oldukça uzun bir süre ulusal hukuk düzenini veri koruma hukukundan uzak tutmuştur. Bu süre zarfında Avrupa veri hukukunda teknolojik gelişmelerin de etkisiyle, yukarıda bahsedilen birçok anayasal, yasal değişiklik ve düzenlemeler, ayrıca AB alanında geçerli olan bir Direktif ve en nihayetinde tüm AB veri koruma hukukunu yeknesaklaştıran bir Tüzük hazırlanmış ve uygulanmıştır.

Türkiye bakımından ilgili kanuni düzenlemenin yapılması uzun sürdüğü için uygun bulma kanunu ancak 30 Ocak 2016'da kabul edilmiştir. Bilindiği üzere bu tarihten önce 12.09.2010 tarihindeki referandum ile, 07.05.2010 tarih ve 5982 sayılı Türkiye Cumhuriyeti Anayasasının Bazı Maddelerinde Değişiklik Yapılması Hakkında Kanun kabul edilmiştir. Ulusal veri koruma hukuku bakımından ilk önemli ve sonuç doğuran bir

adım ile bu değişiklikler neticesinde “Kişisel Verilerin Korunması Hakkı” Anayasa’nın 20/3. maddesine eklenmiştir. Bu durum neticesinde kişisel verilerin korunması hakkı kural olarak Anayasanın üstünlüğü ilkesi gereğince hiçbir kanun ya da başka bir düzenleyici işlem ile çiğnenemeyecektir. Bu hakkın Anayasa’nın 20/3. maddesi altında düzenlenmesi ile artık bireyin verilerine ilişkin karar verme özgürlüğü söz konusudur ve bu hakka yönelik tehlikeler karşısında birey savunmasız değildir. Elbette ki 12 Eylül 2010 tarihinden evvel bireyler bütünüyle savunmasız değildi. Kişinin verileri üzerindeki koruması ve verilerinin hukuksuz biçimde işlenmesinin önüne geçilebilmesi, kişisel verilerin korunması hakkının çıkış noktaları olarak görülen başka anayasal hakları gündeme getirmekteydi. Bu bağlamda kişisel verilerin korunması hakkı anayasal olarak açıkça kabul edilmeden evvel, insan onuru ve kişiliğin serbestçe geliştirilmesi ile özel hayatın gizliliği haklarının korunması altındaydı. Yukarıda görüleceği üzere anayasal içtihat bu biçimde şekillenmiş ve birey bütünüyle korumasız kalmamıştır. Ancak kişisel verilerin korunmasının, insan onuru ve kişiliğin serbestçe geliştirilmesi ile özel hayatın gizliliği haklarından çıkartılarak bağımsız bir hak olarak anayasal bir temele oturtulması ile bireyler günden güne gelişen ve tehditlerin çapının çok daha büyüdüğü bir alanda çok daha güçlü bir korumaya sahip olmuşlardır.

Anayasa’nın 20/3. maddesine göre bilinmektedir ki kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenmelidir. Bu doğrultuda kişisel verilerin korunması 7 Nisan 2016 tarihinde 6698 sayılı Kişisel Verilerin Korunması Kanunu’nun Resmi Gazete’de yayımı neticesinde yürürlüğe girmesi ile kanuni olarak da düzenlenmiş olmaktadır. Özellikle bu noktada, yukarıda ele alınmış Anayasa Mahkemesi kararları düşünüldüğünde Mahkeme’nin kişisel verilerin korunması hakkına bakış açısının henüz hala bütünüyle “veri koruma” çizgisine oturamadığı söylenebilecektir. Daha açık bir ifadeyle AYM, anayasal bir hak olan kişisel verilerin korunmasına dair meselelerde her ne kadar İHAM çizgisini takibe çalışıyorsa da kimi zaman bu görünümünden çıkarak hakkı sınırlandıran bir tutum takınabilmektedir. AYM kararlarının içerisinde genellikle KVKK’yı nispeten aktif bir şekilde kullanmamakta, çoğunlukla Anayasa hükmü ve İHAM kararları bazlı bir inceleme yürütmektedir. Veri koruma hukukunun giderek

bağımsızlaşan yapısı ile Mahkeme'nin temel hak ve özgürlükleri korumak misyonu birlikte düşünüldüğünde, AB Adalet Divanı'nın kişisel verilerin korunması hakkını koruyucu kararlarını gözlemlemek de hakkın korunması için fayda sağlayabilecektir.

Belirtildiği üzere KVKK, 95/46/AT sayılı Direktif'in esas alınması suretiyle hazırlanmıştır. Ancak KVKK'nın Direktif'teki düzenlemeler düşünüldüğünde önemli farklılıkları bulunmaktadır. Gerekçe'de belirtildiği üzere, her ne kadar Kanun'un yapılış amaçlarından biri AB mevzuatına uyum olsa da KVKK'nın hazırlanışında Direktif'in bazı hükümlerini izlemediği görülmektedir. Direktif, kamu kurum ve kuruluşlarına oldukça sınırlı istisnalar tanımış ve bu istisnaları denetime tabi tutmuştur. Fakat KVKK, yukarıda belirtildiği üzere kolluk kuvvetlerine ve istihbarat kurumlarına oldukça geniş istisnalar tanımış ve Kanun kapsamından çıkarmıştır⁸⁵⁸.

Veri Koruma Hukuku alanında ulusal düzlemde Nisan 2016'da kabul edilen bu Kanun ile aynı zamanlarda AB bakımından ise oldukça mühim bir dönüşüm gerçekleşmekte, 95/46/AT sayılı Direktif tarih olmakta ve yerine, tüm üye devletlerde yeknesak, daha kapsamlı ve koruyucu hükümleri 25 Mayıs 2018'de yürürlüğe sokacak olan GVKT kabul edilmekteydi. AB Veri Koruma Hukuku bu Tüzük ile, daha belirsiz bir çerçeveden sınırları daha net ve koruyucu bir alana geçmiştir. Her ne kadar bazı üye ülkeler bakımından iç hukuklarında GVKT ile çelişik hükümlerin düzeltilmesi uzun zaman almış olsa da ya da hala belirsizlik hâkim olabilmekteyse de çoğunluk bakımından yüksek oranda bir uyum sağlanmıştır.

Türkiye bakımından ise durum biraz daha farklı seyretmektedir. Avrupa veri koruma hukukunun Türkiye'deki yansıması bakımından açıktır ki GVKT ile önemli ölçüde bir uyum gerekmektedir. Bu durum yalnızca KVKK'nın Gerekçe'sinde belirtildiği üzere, AB ile uyum süreci açısından veya ekonomik bakımdan yabancı sermayenin ülkeye çekilmesi için değil, ayrıca kişisel verilerin korunması alanını bütüncül biçimde düzenleyen alanın bu korumayı tam anlamıyla gerçekleştirebilmesi için de

⁸⁵⁸ DÜLGER, "Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması", *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi*, s. 114.

gerekmektedir. Buna göre GVKT ile KVKK'nın genel bir deęerlendirmesinin yapılması, AB veri koruma hukukunun iç hukuka ne şekilde yansıdığını ortaya koyacaktır.

İlk olarak belirtilmelidir ki, GVKT'de kişisel veri ihlallerinde sorumluluk hem veri denetleyicisi hem de veri işleyene aittir. Fakat KVKK'da veri sorumlusu ve veri işleyen arasındaki ilişkinin ne şekilde olacağını içeren detaylı bir hüküm bulunmamakta, idari cezalarının uygulaması bakımından yalnızca veri sorumlusu yaptırımı maruz kalmaktadır. Ayrıca Veri Sorumluları Sicili'ne kayıt yalnızca veri sorumluları bakımından zorunlu tutulmaktadır.

Bir dięer önemli farklılık da unutulma hakkı bakımından kendini göstermektedir. GVKT'nin getirdiğı önemli yeniliklerden biri de unutulma hakkının bir metinde düzenlenmiş olmasıdır. KVKK'da ise böyle bir hak ayrıca tanınmamıştır. Hal böyle olmakla birlikte, yukarıda ifade edildiğı üzere, unutulma hakkı ilk defa Yargıtay HGK tarafından tartışılmış ve bir hak olarak açıkça AYM'nin 3 Mart 2016 tarih ve 2013/5653 sayılı kararında yer almıştır. Bu sebeple anılan hakka dair kanuni bir düzenleme mevcut olmasa da bir emsal kararı bulunmaktadır.

GVKT ile KVKK arasında bir dięer farklılık da idari para cezalarına ilişkindir. Bilinmektedir ki GVKT'nin temel özelliklerinden biri de veri ihlali halinde hükmedilen para cezalarının miktarının 95/46/AT sayılı Direkt'e göre oldukça yükselmiş olmasıdır. Miktarlar belirlenirken de şirketlerin yıllık gelirleri gibi oldukça adaletli bir belirleme noktası seçilmiştir. KVKK bakımından ise öncelikle idari para cezaları yalnızca aydınlatma yükümlülüğünün ihlali, veri güvenliğine ilişkin yükümlülüklerin ihlali, Kişisel Verileri Koruma Kurulu tarafından verilen kararların yerine getirilmemesi ve Veri Sorumluları Sicili'ne kayıt ve bildirim yükümlülüğüne aykırı hareket biçimindeki dört eylem için kabul edilmiş, bunlar harici eylemler bakımından idari para cezası yolu kapalı tutulmuştur. Ayrıca GVKT'nin adaletli sonuç doğuracak şirketin yıllık cirosu üzerinden bir ceza belirleme usulü yerine, miktarlar arası makas çok geniş tutularak verilecek cezanın belirlenmesine dair daha muğlak olabilecek bir yol seçilmiştir.

GVKT ile getirilen diğer bazı yeni düzenlemeler ise, veri taşınabilirliği hakkı, zorunlu veri koruma görevlisi ve zorunlu veri koruma etki değerlendirmesidir. Değinildiği üzere veri taşınabilirliği hakkı bakımından veri öznesi kendisine ilişkin verisini bir veri denetleyicisinden ötekine taşıyabilecektir. Ayrıca hassas verilerin işlenmesi durumunda zorunlu veri koruma görevlisi belirlenmesi ve riskli veri işleme hallerinde zorunlu veri koruma etki değerlendirmesi yapılması gerekmektedir. Bahis konusu olan bu üç düzenleme de KVKK'da bulunmamaktadır. Bu bakımdan daha korunaklı bir alan sunan Avrupa Veri Koruma Hukukunun gerisinde kaldığı söylenebilecektir.

Nihayetinde GVKT ile karşılaştırılması gerekli olan bir başka düzenleme de önleyici veri koruma yolları olan tasarımla veri koruma ve varsayılan ayarlarla veri koruma hususlarıdır. Teknolojik gelişmelerin olası gidebileceği noktaların da göz önünde bulundurulması ile Tüzük kapsamında alınabilecek bazı teknik ve idari önlemler bakımından düşünülebiyecek ve yukarıda açıklanan bu yenilikler ise KVKK bakımından mevcut değildir.

KVKK'nın GVKT bağlamında değerlendirilmesi gereken bir diğer noktası da AB Veri Koruma Hukuku'nun en temel özelliklerinden biri olan bağımsız ve tarafsız veri koruma otoritesinin seçimi ve üyelerinin atanması hususudur. GVKT'nin "*Denetim makamının kurulmasına ilişkin kurallar*" başlıklı 54. maddesi bağlamında KVKK'ya bakıldığında, Kişisel Verilerin Korunması Kurulu'na ilişkin tüm seçim, atanma, süre gibi usulleri içeren 21. maddesinin uyumlu bir örnek olduğu dile getirilebilecektir. İlaveten Kişisel Verileri Koruma Kurumu, KVKK'nın 19 ve 21. maddelerinde belirtildiği üzere mali ve idari yönden özerktir ve ayrı bir kamu tüzel kişiliğe sahiptir. Dolayısıyla Kurul'a ilişkin düzenlemelerin Avrupa veri koruma standartları ile uygunluk gösterdiği söylenebilecektir. Fakat Kurul'un çoğunluk üyelerinin TBMM'de çoğunluğa sahip siyasi iktidar ve partili bir Cumhurbaşkanı tarafından belirlenmesi durumu, özellikle tarafsızlık

ilkesi bakımından soru işareti yaratabilecektir⁸⁵⁹. Bu bakımdan Kurum uygulamaları bu tespiti olumlu yöne çevirmek bakımından oldukça kilit bir role sahiptir.

Tüm bu eksiklere rağmen belirtilmelidir ki özellikle 12 Eylül 2010 tarihinden önce ayrı bir anayasal hak olarak dahi düzenlenmemiş kişisel verilerin korunması için yaklaşık son 10 yılda atılan adımlar oldukça önemlidir. KVKK'nın yürürlüğe girdiği 7 Nisan 2016 tarihi sonrası ise, özellikle Kişisel Verileri Koruma Kurumu'nun alandaki yol gösterici çalışmaları da düşünüldüğünde, veri koruma bilincinin oldukça arttığı gözlemlenmektedir. Bu noktada belirtilmelidir ki, Avrupa Veri Koruma Hukuku'nun son ve şimdiye kadar ki en önemli halkası olan GVKT'nin Türkiye bakımından anlaşılması ve özümstenmesi oldukça elzemdir. Bu bakımdan, 95/46/AT sayılı Direktif'i esas alıp bundan "Türk tipi bir kişisel verilerin korunması kanunu"⁸⁶⁰ çıkaran kanun koyucunun, Direktif'in çok daha ilerisinde olan Tüzük'te ele alınan ve KVKK'da bulunmayan düzenlemelere ilişkin olarak bir kısım kanuni değişikliklere gidilebileceği, bazı durumlarda ise Kişisel Verileri Koruma Kurulu'nun yapacağı düzenlemeler ve uygulamaları ile durumun değişebileceği değerlendirilmektedir.

⁸⁵⁹ DÜLGER, "Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması", *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi*, s. 162- 163.

⁸⁶⁰ İlgili tanımla ve gerekçeleri için bkz. DÜLGER, "Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması", *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi*, s. 114.

SONUÇ

Dördüncü kuşak haklar, teknolojinin yarattığı tehlikelere karşı insanın onurunu korumak amacıyla ortaya çıkmıştır. Bu kuşakta yer alan kişisel verilerin korunması hakkının ortaya çıkışı da en genel anlamıyla, bilişim teknolojileri karşısında kişinin mahremiyetini korumaktır. Mahremiyet olmaksızın kişi, herkes için bütünüyle görünür hale gelmekte ve bu durum kişinin özgürce maddi-manevi varlığını geliştirme imkanını ileri ölçüde sınırlandırmaktadır. Bu sebeple kişisel verilerin korunması önceleri özel yaşamın korunması altında, devamında ise ayrı bir temel hak ve özgürlük olarak ortaya çıkmıştır. Bu çalışma kapsamında kişisel verilerin korunması insan hakları perspektifinden temel bir anayasal hakka evrilen şekli ile ele alınmıştır.

Veri koruması, bir insan hakları sorunu olarak, bir kişinin belirli ya da belirlenebilir tüm bilgilerine yönelik teknolojik tehditler sonucunda gelişen bir alan olarak karşımıza çıkmaktadır. Bu bağlamda 1970'lerden günümüze dek özellikle Avrupa'da süregelen veri koruma sistemi bünyesinde pek çok hukuki gelişme geçirmiştir. İlk başlarda her ne kadar başka bir hak içerisinde korunmuş olsa da belli bir süre sonra bilgisayar ve teknoloji dünyasındaki gelişmelerin de etkisiyle içerisinde doğduğu ve geliştiği alandan bağımsız hale gelmiştir.

Bu çalışma kapsamında Avrupa Veri Koruma Hukuku kapsamında görülmüştür ki kişisel verilerin korunması, Avrupa Konseyi'nin yargı organı olan İnsan Hakları Avrupa Mahkemesi içtihatları bağlamında özel yaşamın korunması hakkı içerisinde genel bir biçimde değerlendirilmektedir. Bu sebeple koruma, kişisel verilerin korunması hakkının temel unsurları bakımından sınırlı kalmaktadır. İHAM elindeki somut olayda ilk olarak her zaman durumun özel alan içerisinde olup olmadığını incelemektedir. Bu sebeple özel alan dışında kalan konulara ilişkin belirli bir kural mevcut değildir. Mahkeme, İnsan Hakları Avrupa Sözleşmesi ile taraf devletlerin organlarının işlediği veriler bakımından bir koruma sağlarken, özel sektör tarafından işlenen verilerin Sözleşme tarafından koruma altında olup olmadıkları belirsizdir. Devletlerin pozitif yükümlülükleri bağlamında, özel sektöre ilişkin veri işleme durumlarında hukuka

aykırılıkları önleyecek hukuki düzenlemeleri ihmal etmesi halinde doğrudan sorumlu tutulması mümkündür. Ancak Mahkeme içtihatlarında henüz bu duruma ilişkin tüm ihtimallere yönelik kapsamlı cevaplar verilmemiştir.

Öte yandan Avrupa Birliği alanındaki hukuki düzenleme ve içtihatlarda gerek Birlik bünyesinde gerekse ulusal hukuklarda kişisel verilerin korunması için kapsamlı düzenlemelerin mevcut olduğu görülmüştür. AB bünyesinde kişisel verilerin korunması hakkı bağımsız olarak gelişmiştir. 1 Aralık 2009'da Lizbon Antlaşması'nın onayı ile kişisel verilerin korunması hakkının ayrı bir hüküm olarak düzenlendiği AB Temel Haklar Şartı'nın hukuken bağlayıcı hale gelmesi neticesinde Birlik kapsamında veri koruma daha korunaklı hale gelmiştir. Bu bağlamda çalışmada özellikle hem AB Temel Haklar Şartı, hem de 95/46/AT Sayılı Direktif, kişisel verilerin korunması açısından Adalet Divanı kararları ışığında incelenmiştir. Buna göre Divan'ın kişisel verilerin korunması hakkını bağımsız ve temel bir hak olarak ele alan Şart'ı henüz yeterince çözümleyemediği görülse de, yenilikçi ruhunun ileriye dönük umut verdiği tespit edilmiştir.

Çalışmada, Birlik kapsamında 2010'lu yıllardan itibaren veri koruma hukukunda yenilik arayışlarının 2016 yılından bu yana sonuçları olarak görülen Veri Koruma Reformu'nun getirileri incelenmiştir. Buna göre Genel Veri Koruma Tüzüğü'nün eski Direktif'e kıyasla teknolojik ihtiyaçlara ve doğan yeni tehlikelere ne kadar cevap verdiği sorusu cevaplandırılmaya çalışılmıştır. Öncelikle söz konusu metin Tüzük olması sebebiyle artık tüm üye devletlerde doğrudan uygulanabilmektedir. Böylece üye devletlerdeki farklı uygulamalar yeknesaklaştırılmıştır. Ayrıca her ne kadar GVKT'den önceki tüm metinler Avrupa dışındaki ülkeleri bir şekilde etkilemişse de (söz gelimi Türkiye'de 6698 Sayılı Kişisel Verilerin Korunması Kanunu, 95/46/AT Sayılı Direktif'i temel almıştır.) AB alanında ilk defa bir metin ülke dışılık prensibi ile AB dışındaki ülkelere de belli şartlar dahilinde uygulanabilir hale gelmiştir.

Kapsamı giderek genişleyen ve disiplinler arası teknik bir konu olan kişisel verilerin korunması meselesi hem anayasal, hem yasal olarak yeterince geniş ve çok

boyutludur. Bu bağlamda Türkiye’deki anayasal hükümler ve temel kanuni düzenlemeye bakıldığında Avrupa Veri Koruma Hukuku’nun yansımalarının ulusal düzeyde oldukça geç gerçekleştiği görülmektedir. 1970’lerden beri mahremiyetin korunması ve özel yaşam hakkı bağlamında Avrupa’da gelişip bağımsızlaşan bu alanın öneminin anlaşılması Türkiye’de daha ziyade 2000’lerden sonra olmuştur. Bu süre içerisinde Avrupa’da teknolojik gelişmelerin de etkisiyle birçok anayasal ve kanuni değişiklik ve düzenlemeler, ayrıca AB alanında geçerli olan bir Direktif ve en nihayetinde tüm AB veri koruma hukukunu yeknesaklaştıran ve bu hukuku AB dışında da uygulayan bir Tüzük yapılmıştır.

Her ne kadar gerek Anayasa’daki diğer bazı hak kategorileri (insan onuru ve kişiliğin serbestçe geliştirilmesi ile özel hayatın gizliliği gibi.) ile gerekse farklı hukuk dallarındaki bazı düzenlemelerle korunmaya çalışılsa da kişisel verilerin korunmasının anayasal bir hak olarak kabul edilmesinden önce bütünüyle korunması mümkün olamamıştır. 12.09.2010 tarihindeki referandum ile, 07.05.2010 tarih ve 5982 sayılı Türkiye Cumhuriyeti Anayasasının Bazı Maddelerinde Değişiklik Yapılması Hakkında Kanun kabul edilmiştir. Ulusal veri koruma hukuku bakımından önemli ve sonuç doğuran bu değişiklikler neticesinde “Kişisel Verilerin Korunması Hakkı” Anayasa’nın 20/3. maddesine eklenmiştir. Açıktır ki kişisel verilerin korunmasının, insan onuru ve kişiliğin serbestçe geliştirilmesi ile özel hayatın gizliliği haklarından bağımsız bir hak olarak anayasal bir temele oturtulması ile bireyler günden güne gelişen ve tehditlerin çapının çok daha büyüdüğü bir alanda daha güçlü bir korumaya sahip olmuşlardır. Ancak 2010 yılında bağımsız bir anayasal hak olarak kabul edilse de Avrupa Veri Koruma Hukuku’nun geldiği seviyeden ve Anayasa’nın 20/3. maddesinde belirtildiği üzere, kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenlenmesi gerekliliğinden dolayı 7 Nisan 2016 tarihinde Resmî Gazete’de yayımlanarak 6698 sayılı Kişisel Verilerin Korunması Kanunu kabul edilmiştir.

Çalışma kapsamında görülmüştür ki, Türkiye’de kişisel verilerin korunmasına ilişkin olarak 2016 yılında özel bir kanunun ortaya çıkışı önemli bir adım olsa da yeterli değildir. Avrupa Veri Koruma Reformu öncesinde var olan 95/46/AT Sayılı Direktif’i

esas alan 6698 Sayılı Kişisel Verilerin Korunması Kanunu bu sebepten ötürü eski kalmıştır. Üstelik KVKK'nın Direktif'ten önemli farklılıkları bulunmaktadır. Ayrıca Reform'un ana metni olan ve eski Direktif'in yerine geçen GVKT ile karşılaştırıldığında, KVKK birçok noktada günümüz ihtiyaçlarını karşılayamamaktadır. Bu bakımdan Kanun'un hem Direktif, hem Tüzük'ten temel dört noktada eksikliği bulunduğu tespit edilmiştir.

- Kamu kurum ve kuruluşlarına, özellikle kolluk kuvvetleri ve istihbarat kurumlarına oldukça geniş istisnalar tanınarak bu tarz faaliyetlerin Kanun kapsamı dışında tutulması.
- Kişisel Verileri Koruma Kurulu'nun çoğunluk üyelerinin TBMM'de çoğunluğa sahip siyasi iktidar ve partili bir Cumhurbaşkanı tarafından belirlenmesi.
- Kişisel Verileri Koruma Kurulu kararlarının KVKK 24/3(b) hükmü uyarınca tebliği ve bu kararların Kurulca gerekli görülenlerinin kamuoyuna duyurulmasının sağlanması ve uygulanmalarının izlenmesi görevinin Başkan'a ait olması.
- Kanun kapsamında idari para cezalarının yalnızca dört eylem için⁸⁶¹ kabul edilmesi, bunlar dışındaki eylemler bakımından idari para cezası yolunun kapalı tutulmuş olması ve idari para cezaları arasındaki makasın oldukça geniş tutulması.

Kanun'da genel hatlarla bu şekilde yer alan eksikliklerin bir kısmının kanuni değişikliklerle giderilebileceği, bazı durumlarda ise Kişisel Verileri Koruma Kurulu'nun yapacağı düzenlemeler ve uygulamalar ile durumun değişebileceği tespit edilmiştir. Buna göre:

⁸⁶¹ Bu dört hareket şunlardır: "Aydınlatma yükümlülüğünün ihlali, veri güvenliğine ilişkin yükümlülüklerin ihlali, Kişisel Verileri Koruma Kurulu tarafından verilen kararların yerine getirilmemesi ve Veri Sorumluları Sicili'ne kayıt ve bildirim yükümlülüğüne aykırı hareket."

- Öncelikle KVKK da tıpkı Direktif’de olduğu gibi, kolluk güçlerinin faaliyetleri ve istihbarat faaliyetleri Kanun kapsamına alınmalı, kamu kurum ve kuruluşlarına sınırlı istisnalar tanınmalı ve tüm bu istisnalar denetime tabi tutulmalıdır.
- Veri koruma otoritesinin oluşumu her ne kadar GVKT’ye uyumlu olsa da Kurul’un çoğunluk üyelerinin TBMM’de çoğunluğa sahip siyasi iktidar ve partili bir Cumhurbaşkanı tarafından belirlenmesi durumu tarafsızlık ilkesi bakımından soru işareti yaratabilecektir. Dolayısıyla Kişisel Verileri Koruma Kurulu’nun uygulamalarının dikkatle takip edilmesi gerekmekte ve görünüşte dahi olsa tarafsızlığa leke düşürecek karar ve uygulamalardan kaçınılmalıdır.
- Kişisel Verileri Koruma Kurulu’nun kararlarından Kurul tarafından gerekli görülenlerin Başkan tarafından kamuoyuna duyurulması görevi ile Kurul’a kamuoyu ile paylaşılacak kararlar hususunda ilk elden belirleme yetkisi verilmiştir. Bu durumda KVKK’nın uygulaması bakımından bazı Kurul kararlarının yayınlanmayacak olması durumu ortaya çıkmaktadır. Bu ise, kişisel verilerin korunması hukukunun gelişimi açısından olumsuz bir gelişme olarak değerlendirilebilecek ve alanın pratikteki uygulamasının tüm hatları ile görmeye engel olabilecektir. Dolayısıyla söz konusu kararların tümünün erişime açık olması bu hukuk alanının gelişimi için oldukça önem arz etmektedir.
- İdari para cezalarının yalnızca belli haller için söz konusu olması ve diğer tüm hallerin kapsam dışında olması hukuki belirlilik ilkesine zarar verebileceğinden Kanun’da idari açıdan yaptırımsız düzenleme bırakılmamalıdır.
- İdari para ceza miktarları kararlaştırılırken dikkate alınacak somut ölçütler belirlenmesinin veya GVKT’de olduğu gibi, şirketlerin yıllık cirosuna göre ceza verilmesinin daha hakkaniyetli sonuçlar doğuracağı düşünülmektedir.

Kişisel verilerin korunmasına ilişkin ele alınan Anayasa Mahkemesi kararlarına bakıldığında ise görülmüştür ki, Mahkeme’nin bakış açısı henüz bütünüyle “veri koruma”

çizgisine oturmamıştır. Daha açık bir ifadeyle AYM, anayasal bir hak olan kişisel verilerin korunmasına dair meselelerde her ne kadar İHAM çizgisini takip etmeye çalışsa da özellikle son yıllarda kimi zaman bu görünümünden de çıkarak daha sınırlandırıcı bir tutum takınabilmektedir. AYM kararlarında göze çarpan bu durum KVKK'da da (özellikle istihbari faaliyetler bağlamında) görülmektedir. Bu ise veri korumanın varlık sebebini tehlikeye düşüren bir anlayıştır. Ayrıca görülmüştür ki AYM, kararlarında KVKK'yı aktif bir şekilde kullanmamakta (Kanun metninin Anayasa'ya aykırılığının konu edildiği karar ve genelde karşı oylar hariç), çoğunlukla Anayasa hükmü ve İHAM kararları bazlı bir inceleme yürütmektedir. Bu durumun gerekçesi içtihat incelemesinden doğrudan anlaşılsa da meselenin Kanun'a ilişkin teknik bilgi eksikliğinden kaynaklanıyor olabileceği düşünülmektedir. Mahkeme'nin konuya dair özel bir düzenleme olan ve normlar hiyerarşisi çerçevesinde Anayasa hükmünden çok daha detaylı düzenlemeler içeren Kanun'u kararlarında çok daha işler hale getirmesi, konuya dair içtihatların çeşitlenmesi ve hakkın koruma alanının genişlemesi açısından önemli görülmektedir. Bu noktada bir diğer öneri de veri koruma hukukunun giderek bağımsızlaşan yapısı ile Mahkeme'nin temel hak ve özgürlükleri korumak misyonu birlikte düşünüldüğünde sadece kişisel verilerin korunması hakkına ilişkin başvuruları özel yaşama saygı hakkı nezdinde inceleyen İHAM kararlarına atıf yapılmasının yanında, kişisel verilerin korunması hakkının koruma alanını genişletebilmek amacıyla kişisel verilerin korunması hakkının bağımsız olarak düzenlendiği Temel Haklar Şartı'nın ve GVKT hükümlerinin konu edildiği Adalet Divanı'nın konuya dair kararlarının da ele alınmasının yerinde olacağı biçimindedir.

Görülmüştür ki Kişisel Verilerin Korunması Kurulu, özellikle üyesi bulunduğumuz Avrupa Konseyi ve aday statüsünde bulunduğumuz AB'deki hukuki gelişmeleri Anayasa'nın 90. maddesi uyarınca takip etmeye ve bu bağlamda elindeki Kanun metnini mümkün olduğunca ilerici şekilde kullanmaya çalışmaktadır. Mayıs 2019'da vermiş olduğu Facebook Kararı ile de bu tespiti doğrulamaktadır. Ancak doktrinde çok defa en büyük veri tekeli olarak adlandırılan ve ancak günümüzde

şirketlerin giderek bu özelliği elinden aldığı kamu kurumlarına ilişkin meselelerde Kurul'un nasıl bir tutum takınacağı merakla beklenmektedir.

Tüm bu eksiklere rağmen belirtilmelidir ki özellikle 12 Eylül 2010 tarihinden önce ayrı bir anayasal hak olarak dahi düzenlenmemiş kişisel verilerin korunması için son 10 yılda atılan adımlar olumlu olarak değerlendirilmelidir. Ancak bu noktada bir kez daha altı çizilmelidir ki, Avrupa Veri Koruma Hukuku'nun son ve şimdiye kadar ki en önemli halkası olan GVKT'nin Türkiye bakımından anlaşılması ve özümsemişi konunun gelişimi ve gelecekte erişeceği nokta açısından oldukça önemlidir. Bu ise ilk planda 6698 Sayılı Kişisel Verilerin Korunması Kanunu'nun belli başlı hükümlerinin değiştirilmesi ile mümkün olabilecektir.

KAYNAKÇA

Kitap, Makale ve Bildiriler

ABADAN, Yavuz, “Tanzimat Fermanı’nın Tahlili”, *Tanzimat: Değişim Sürecinde Osmanlı İmparatorluğu*, Halil İNALCIK, Mehmet SEYİTDANLIOĞLU, Türkiye İş Bankası Kültür Yayınları, ss. 31- 59, 2014.

ACEMOGLU, Daron, James A. ROBINSON, *Why Nations Fail – The Origins of Power Prosperity and Poverty*, Profile Books, 2013.

AKAD, Mehmet, Bihterin VURAL DİNÇKOL, Nihat BULUT, *Genel Kamu Hukuku*, Gözden Geçirilmiş 14. Baskı, Der Yayınları, İstanbul, 2018.

AKGÜL, Aydın, “Kişisel Verilerin Korunmasında Yeni Bir Hak: ‘Unutulma Hakkı’ ve AB Adalet Divanı’nın ‘Google Kararı’”, *TBB Dergisi*, Y. 2016, S. 116, ss. 11- 38.

AKGÜL, Aydın, *Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması*, Beta, İstanbul, 2014.

AKILLIOĞLU, Tekin, *İnsan Hakları: Kavram, Kaynaklar ve Koruma Sistemleri*, İmaj, Ankara, 2010.

AKSOY, Hüseyin Can, *Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması*, Çakmak Yayınevi, Ankara, 2010.

ALEXY, Robert, *A Theory of Constitutional Rights*, Oxford University Press, 2010.

ALGAN, Bülent, “Rethinking ‘Third Generation’ Human Rights”, *Ankara Law Review*, Vol. 1, No: 1, Y. 2004, ss. 121- 155.

- AMAR, Akhil Reed, *The Bill of Rights- Creation and Reconstruction*, Yale University Press, 1998, New Haven& Londra.
- ANDRIULLI, Laura, *Online Privacy Law: Italy Country Report*, June 2012, Library of Congress, <https://www.loc.gov/law/help/online-privacy-law/2012/italy.php> , E.T. 02.05.2019.
- ARASLI, Oya, *Özel Yaşamın Gizliliği Hakkı ve T.C. Anayasasında Düzenlenişi*, Ankara, 1979, (Yayımlanmamış Doçentlik Tezi).
- ARSLAN ÖNCÜ, Gülay, *Avrupa İnsan Hakları Sözleşmesinde Özel Yaşamın Korunması Hakkı*, Beta, 2011.
- ARZT, Clemens, “Data Protection Versus Fourth Amendment Privacy: A New Approach Towards Police Search and Seizure”, *Criminal Law Forum*, Vol. 16 (3-4), Y. 2005, ss. 183- 230.
- ASHFORD, Warwick “New UK Data Protection Act not welcomed by all”, *Computer Weekly*, 24.05.2018, <https://www.computerweekly.com/news/252441814/New-UK-Data-Protectio-Act-not-welcomed-by-all> , E.T. 01.05.2019.
- ASSCHER, Lodewijk F., Judith VAN ERVE, *Regulating Spam: Directive 2002/ 58 and Beyond*, The Institute For Information Law- University of Amsterdam, 2004.
- ATWILL, Nicole, *Online Privacy Law: France Country Report*, Library of Congress, June 2012, <https://www.loc.gov/law/help/online-privacy-law/2012/france.php> , E.T. 03.05.2019.
- AYBAY, Rona, *Açıklamalı İnsan Hakları Evrensel Bildirisi*, TBB, Ankara, 2006.

AYBAY, Rona Fazıl SAĞLAM, Süheyl BATUM, Oktay UYGUN, Korkut KANADOĞLU, Ece GÖZTEPE, Faruk BİLİR, Teoman ERGÜL, *Türkiye Cumhuriyeti Anayasa Önerisi*, Türkiye Barolar Birliği, Geliştirilmiş Gerekçeli Yeni Metin, 2011, 5. Baskı.

AYDIN, Devrim, “Ceza Kanunlarının Yer Yönünden Uygulanması”, *TBB Dergisi*, Y. 2011, S. 94, s. 133, ss. 131- 148.

BARRY, Norman P., *Modern Siyaset Teorisi*, Çev: Mustafa ERDOĞAN- Yusuf ŞAHİN, Liberte, Ankara, 2003.

BASDEVANT, Adrien, Jean-Pierre MIGNARD, *L’Empire des Données: Essai sur la Société, les Algorithmes et la Loi*, Don Quichotte éditions, Paris, 2018.

BAŞALP, Nilgün, *Kişisel Verilerin Korunması ve Saklanması*, Yetkin Yayınevi, Ankara, 2004.

BAŞGİL, Ali Fuat, “Hakkı ve Hukuku Devlet mi Yaratır ve Yapar?”, *Ordinaryüs Prof. Dr. Tahir TANER’e Armağan’dan Ayrı Bası*, İsmail AYGÜN Matbaası, İstanbul, 1956.

BEAUMONT, Samantha, "The Data Protection Directive versus the GDPR: Understanding key changes", *Synopsys Software Integrity Blog*, 18.01.2018, <https://www.synopsys.com/blogs/software-security/dpd-vs-gdpr-key-changes/>, E.T. 27.02.2019.

BEITZ, Charles R., *The Idea of Human Rights*, Oxford University Press, New York, 2009.

BENNETT, Colin J., *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*, Cornell University Press, Ithaca & London, 1992.

- BENNETT, Colin, J. Charles D. RAAB, *The Governance of Privacy: Policy Instruments in Global Perspective*, The MIT Press, 2006.
- BERKES, Niyazi, *Türkiye’de Çağdaşlaşma*, Haz: Ahmet KUYAŞ, YKY Yayınları, 7. Bası, İstanbul, 2004.
- BEVERLEY- SMITH, Huw, Ansgar OHLY, Agnes LUCAS- SCHLOETTER, *Privacy, Property and Personality- Civil Law Perspectives on Commercial Appropriation*, Cambridge University Press, New York, 2005.
- BIGLINO, Irene, Christophe GOLAY, *The Optional Protocol to the International Covenant on Economic, Social and Cultural Rights*, Academy in-Brief, No: 2, Geneva Academy of International Humanitarian Law and Human Rights, 2013, Geneva, <http://www.geneva-academy.ch/docs/publications/The%20optional%20protocol%20In%20brief%202.pdf> , E.T. 31.10.2016.
- BLUME, Peter, *Nordic Studies in Information Technology and Law*, Kluwer Law and Taxation Publishers, 1991.
- BLUME, Peter, *Protection of Informational Privacy*, International Specialized Book Service Incorporated, DJOF Publishing, 2002.
- BORING, Nicolas, *Online Privacy Law: France Country Report*, Library of Congress, December 2017, https://www.loc.gov/law/help/online-privacy-law/2017/france.php#_ftn1 , E.T. 03.05.2019.
- BOYAR, Oya, “Devletin Pozitif Yükümlülükleri ve Dolaylı Yatay Etki”, *İnsan Hakları Avrupa Sözleşmesi ve Anayasa*, Ed. Sibel İNCEOĞLU, Avrupa Konseyi, Ankara, 2013.

- BREITBARTH, Paul, “The GDPR Implementation Act in The Netherlands”, *National Adaptations of the GDPR*, E-Conference, Blog Droit Europeen, June 2018, <https://blogdroiteuropeen.files.wordpress.com/2018/06/paul-1.pdf> , E.T. 02.05.2019.
- BULUT, Nihat, *Sanayi Devriminden Küreselleşmeye Sosyal Haklar*, On İki Levha Yayıncılık, İstanbul, 2009.
- BYGRAVE, Lee A., *Data Protection Law: Approaching its Rationale, Logic and Limits*, Kluwer Law International, 2002.
- CADWALLADR, Carole, Emma GRAHAM- HARRISON, “Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach”, The Cambridge Analytica Files, 17.03.2018, <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-face-book-influence-us-election> , E.T. 01.03.2019.
- CAREY, Peter, *Data Protection: A Practical Guide to UK and EU Law*, Oxford University Press, 2004,
- CHARLESWORTH, Andrew, “CCTV, the GDPR and the Third Wave of Data Protection”, *The Watching The Watchers, A Cloudview White Paper*, 2017, ss. 1- 20.
- CHESTER, Jeff, “Cookie Wars: How New Data Profiling and Targeting Techniques Threaten Citizens and Consumers in the ‘Big Data’ Era”, *European Data Protection: In Good Health?*, Eds. Serge GUTWIRTH, Ronald LEENES, Paul DE HERT, Yves POULLET, Springer, 2012, ss. 53- 78.
- CHRISTOPHER, Warren, *In the Stream of History- Shaping Foreign Policy for a New Era*, Stanford University Press, 1998.

CRAIG, Paul, Grainne DE BURCA, *EU Law- Text, Cases and Materials*, Oxford University Press, 2007.

ÇAĞLAR, Selda, Küreselleşme Sürecinde Sosyal Hakları Yeniden Düşünmek”, *Maltepe Üniversitesi Hukuk Fakültesi Dergisi*, Vol. 1, Y: 2010, Maltepe Üniversitesi Yayınları, İstanbul, ss. 211-226.

ÇAĞLAR, Selda, *Disiplinlerarası Yaklaşımla İnsan Hakları*, Ed., Beta, İstanbul, 2010.

ÇAĞLAR, Selda, “Hukuk Devleti Açısından Hukuki Belirlilik- Hukuk Güvenliği İlişkisi”, *Hukuk Güvenliği*, Kamu Hukukçuları Platformu, Türkiye Barolar Birliği Yayınları, 2015, ss. 25- 138.

ÇAĞLAR, Selda, *Hukuk Devletin Hukuki Belirlilik İlkesi Üzerinden Değerlendirilmesi*, Beta, 2013.

ÇEKİN, Mesut Serdar, “6698 sayılı Kişisel Verilerin Korunması Kanunu’nun Big Data (Büyük Veri) ve İrade Serbestisi Açısından Değerlendirilmesi”, *İÜHFM*, C. LXXIV, S. 2, Y. 2016, ss. 629- 644.

ÇEKİN, Mesut Serdar, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu*, On İki Levha Yayıncılık, 2018.

DE HERT, Paul, Vagelis PAPAKONSTANTINOU, “The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?”, *Computer Law& Security Review: The International Journal of Technology Law and Practice*, 2016, ss. 1- 16.

DE HERT, Paul, *Citizen’s Data and Technology: An Optimistic Perspective*, The Hague Dutch Data Protection Authority, 2009.

- DE HERT, Paul, Serge GUTWIRTH, “Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action”, *Reinventing Data Protection*, Serge GUTWIRTH, Yves POULLET, Paul DE HERT, Cecile DE TERWANGNE, Sjaak NOUWT (Ed.), Springer, 2009, ss. 3- 44.
- DE HERT, Paul, Serge GUTWIRTH, “Privacy, Data Protection and Law Enforcement-Opacity of the Individual and Transparency of Power”, *Privacy and the Criminal Law*, Erik CLAES, Anthony DUFF, Serge GUTWIRTH (Ed.), Antwerp/Oxford, Intersentia, 2006.
- DE SCHUTTER, Olivier, *International Human Rights Law*, Cambridge University Press, 2010.
- DE SOUSA GONÇALVES, Anabela Susana, “The Cross Border Regulation of Online Data Privacy and the Judicial Cooperation”, *Jusletter IT*, 26.02.2015.
- DEMPEGIOTIS, Sotiris I., Eirini G. CHAGIOU, “Personal Data Protection”, *Greek Law Digest*, 05.03.2019, <http://www.greeklawdigest.gr/topics/data-protection/item/111-personal-data-protection> , E.T. 30.04.2019.
- DINAN, Desmond, *Europe Recast: A History of European Union*, Lynne Rienner Publishers, 2014.
- DİNÇKOL, Abdullah, “Bir Pozitif Hukuk Kaynağı Olarak Avrupa Birliği Hukuk Sistemi”, *Hukuk Felsefesi ve Sosyolojisi Arkivi*, S. 22, İstanbul Barosu Yayınları, 2010, ss. 189- 214.
- DİNÇKOL, Abdullah, “Teknoloji ve Hukuk”, *Hukuk Felsefesi ve Sosyolojisi Arkivi*, S. 19, İstanbul Barosu Yayınları, 2010, ss. 248- 279.
- DİNÇKOL, Abdullah, “Küreselleşme ve İnsan Hakları”, *Doç. Dr. Mehmet SOMER’e Armağan*, Marmara Üniversitesi Hukuk Fakültesi Yayını, 2006, ss. 879- 919.

- DOBSON, Deborah, “The 4 Types of Blockchain Networks Explained”, International Legal Technology Association, 2018, <https://www.iltanet.org/blogs/deborah-dobson/2018/02/13/the-4-types-of-blockchain-networks-explained> , E.T. 06.05. 2019.
- DOĞAN, İlyas, “İnsan Hakları Hukukunun Temel Kavramları ve Özellikleri”, *İnsan Hakları Hukuku* (Ed.: İlyas DOĞAN), Astana Yayınları, Ankara, 2015.
- DONNELLY, Jack, *Teoride ve Uygulamada Evrensel İnsan Hakları*, Çev: Mustafa ERDOĞAN- Levent KORKUT, Yetkin, 1995, Ankara.
- DOSWALD-BECK, Louise, “The Meaning of the ‘Right to Respect for Private Life’ under the European Convention on Human Rights”, *Human Rights Law Journal*, Vol. 4, No: 3.
- DUGHI, Paul, “A Simple Explanation of How Blockchain Works”, *Medium*, <https://medium.com/the-mission/a-simple-explanation-on-how-blockchain-works-e52f75da6e9a> , E.T. 04.05.2019.
- DUNCAN, Bob, “Can EU Data Protection Regulation Compliance be Achieved When Using Cloud Computing?”, *Cloud Computing 2018: The Ninth International Conference on Cloud Computing, GRIDs, and Virtualization*, Eds. Bob DUNCAN, Yong Woo LEE, Aspen OLMSTED, 18- 22 February 2018, ss. 1- 6.
- DÜLGER, Murat Volkan, “Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması”, *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi*, C. 3(2), Y. 2016, ss. 101- 167.
- DÜLGER, Murat Volkan, *Bilişim Suçları ve İnternet İletişim Hukuku*, Seçkin Yayıncılık, Ankara, 2015.
- DÜLGER, Murat Volkan, *Bilişim Suçları*, Seçkin Yayınevi, Ankara, 2004.

- DÜLGER, Murat Volkan, *Kişisel Verilerin Korunması Hukuku*, Hukuk Akademisi, İstanbul, 2019.
- DWORKIN, Ronald, *Taking Rights Seriously*, Harvard University Press, 1977.
- EBERLE, Edward J., “Human Dignity, Privacy and Personality in German and American Constitutional Law”, *Utah Law Review*, No:4, Y: 1997, ss. 963- 1056.
- ENGELS, Barbara, “Data Portability among Online Platforms”, *Internet Policy Review-Journal on Internet Regulation*, Vol. 5, Issue: 2, Y. 11.06.2016, ss. 1-17.
- ERDOĞAN, Mustafa *İnsan Hakları Teorisi ve Hukuku*, Orion Kitabevi, Ankara, 2015.
- ERMAN, R. Barış, “Adli Yargı Sisteminde DNA Örnekleri ve Profilleri- S. ve Marper-Birleşik Krallık Davası”, *Fasikül Hukuk Dergisi*, C. 2, S. 11, Y: 2010, ss. 20-23.
- FABBRINI, Federico, *The EU Charter of Fundamental Rights and the Rights to Data Privacy: The EU Court of Justice as a Human Right Court*, iCourts Working Paper Series, No: 19, 2015.
- FLAHERTY, David H., *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweeden, France, Canada and the United States*, University of North Carolina Press, 1989.
- FUSTER, Gloria Gonzales, Raphael GELLERT, “The Fundamental Right of Data Protection in the European Union: In Search of an Unchartered Right”, *Review of Law, Computers & Technology*, Vol. 26, No: 1, 2012, ss. 73- 82, <https://www.researchgate.net/publication/254294660/download> , E.T. 05.09.2018.

- FUSTER, Gloria Gonzales, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Law, Governance and Technology Series 16, Springer International Publishing, 2014.
- GALETTA, Antonella, Paul DE HERT, “A European Perspective on Data Protection and Access Rights”, *Increasing Resilience in Surveillance Societies (IRISS) Project*, Vrije Universiteit Brussels- Belgium, 2014, <http://irissproject.eu/wp-content/uploads/2014/06/European-level-legal-analysis-Final1.pdf> , E.T. 03.09.2018.
- GASSMANN, Hans Peter, *30 Years After: The Impact of the OECD Privacy Guidelines, Joint Roundtable of the Committee for Information, Computer and Communications Policy (ICCP), and its Working Party on Information Security and Privacy (WPISP)*, 10 Mart 2010.
- GAVISON, Ruth, “Privacy and the Limits of Law”, *The Yale Law Journal*, Vol. 89, No: 3, ss. 421- 471.
- GERARDS, Janneke, *General Principles of the European Convention on Human Rights*, Cambridge University Press, 2019.
- GESLEY, Jenny, *Online Privacy Law: Germany Country Report*, December 2017, Library of Congress, <https://www.loc.gov/law/help/online-privacy-law/2017/germany.php> , E.T. 01.05.2019.
- GÖREN, Zafer, “Avrupa Birliği Temel Haklar Şartı’nın Ana İlkesi: Dokunulmaz İnsan Onuru”, *İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi*, Y: 6, S. 12, Güz 2007/2, ss. 21- 37, 2007.
- GÖREN, Zafer, *Temel Hak Genel Teorisi*, Dokuz Eylül Üniversitesi Yayını, İzmir, 2000.
- GÖZLER, Kemal, *Türk Anayasa Hukuku Dersleri*, Ekin Yayınevi, 2016, Bursa.

GÖZLER, Kemal, *Türk Anayasa Hukuku*, Ekin Yayınevi, Bursa, 2000.

GÖZÜBÜYÜK, A. Şeref, *Anayasa Hukuku*, Turhan Kitabevi, Ankara, 1998.

GREENLEAF, Graham, “Convention 108+ and the Data Protection Framework of the EU”, *Conference on Convention 108+ Tomorrow’s Common Ground for Protection*, Council of Europe, Strasbourg, 21.06.2018, *University of New South Wales Law Research Paper*, No. 18-39, ss. 1-7.

GREENLEAF, Graham, “‘Modernised’ Data Protection Convention 108 and the GDPR”, *Privacy Laws & Business International Report*, Vol. 154, No: 22, Y: 2018, *University of New South Wales Law Research Paper*, No: 19-3, Y: 2019, ss. 1-2.

GUEGAN, Dominique, “Public Blockchain versus Private Blockchain”, *Centre de Economie Sorbonne (CES) Working Papers*, 2017, ss. 1-6.

GUILD, Elspeth, Evelien BROUWER, “The Political Life of Data: The ECJ Decision on the PNR Agreement between the EU and the US”, *Centre for European Policy Studies Policy Brief*, No: 109, July 2006, <https://www.files.ethz.ch/isn/24402/PB110.pdf>, E.T. 17.01.2019.

GUTWIRTH, Serge, *Privacy and the Information Age*, For the Rathenau Institute, Raf CASERT (Çev.), Rowman & Littlefield, 2002.

GÜMÜŞ, Ali Tarık, *Türk Anayasasında Kişinin Maddi ve Manevi Varlığını Koruma ve Geliştirme Hakkı*, Eğitim Akademi Yayınları, 2010.

GÜNDÜZÖZ, İlker, “Yeni Kuşak İnsan Hakları Çerçevesinde Türkiye’de Mülki İdare Amirliğine Analitik Bir Yaklaşım”, *İnsan Hakları Yıllığı*, C.: 33, 2015, ss. 19- 33, s. 25.

- HAKYEMEZ, Yusuf Şevki, “Temel Hak ve Özgürlüklerin Sınırlandırılmasında Ölçülülük İlkesi”, *Prof. Dr. Hayri DOMANIÇ’e 80. Yaş Günü Armağanı*, C. II, İstanbul, 2001, s. 1287- 1337.
- HAMAMCI, Can, “Üçüncü Kuşak İnsan Hakları”, *Yeni Kuşak İnsan Hakları*, Ed. Ertan Kuvılcım AKKOYUNLU, 2013, TODAİE Yayın No: 371, ss.1-237.
- HARARI, Yuval Noah, *Homo Deus- A Brief History of Tomorrow*, Harper Collins Publishers, 2017.
- HARRIS, David, Michael O’BOYLE, Colin WARBRICK, *Law of the European Convention on Human Rights*, 2nd Ed., Oxford University Press, 2009.
- HAYEK, Friedrich, *Kanun Yasama Faaliyeti ve Özgürlük: Sosyal Adalet Serabı*, Çev: Mustafa ERDOĞAN, Türkiye İş Bankası Yayınları, 1995, İstanbul.
- HEKİMOĞLU, Mehmet Merdan, “İnsan Haklarının Temelini Oluşturan ‘İnsan Onuru’ Kavramının Anayasal Boyutları: Federal Almanya Örneği”, *Kazancı Hakemli Hukuk Dergisi*, N: 71- 72.
- HELVACI, Serap, *Türk ve İsviçre Hukuklarında Kişilik Hakkını Koruyucu Davalar*, Beta, İstanbul, 2001.
- HELVACI, Serap, *Gerçek Kişiler*, Legal Yayıncılık, İstanbul, 2016.
- HENKOĞLU, Türkay, *Bilgi Güvenliği ve Kişisel Verilerin Korunması*, Yetkin Yayınları, Ankara, 2015.
- Elin HOFVERBERG, *Online Privacy Law: Sweeden Country Report*, Library of Congress, June 2012, <https://www.loc.gov/law/help/online-privacy-law/2012/sweden.php> , E.T. 01.05.2019.

- HOFVERBERG, Elin, *Online Privacy Law: Sweeden Country Report*, Library of Congress, December 2017, <https://www.loc.gov/law/help/online-privacy-law/2017/sweden.php> , E.T. 01.05.2019.
- HONDIUS, Frits W., *Emerging Data Protection in Europe*, North Holland Publishing Company, 1975.
- HONDIUS, Frits W., *The Council of Europe's Work in the area of Computers and Privacy*, Discussion Paper on the Use of Data Processing, Parliamentary Assembly of the Council of Europe, 18- 19 May 1978.
- HORNUNG, Gerrit, Christoph SCHNABEL, "Data protection in Germany I: The population census decision and the right to informational self-determination", *Computer Law & Security Report*, Vol.: 25, Issue 1, 2009, ss. 84-88.
- HUSTINX, Peter, "EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation", *Collected Courses of the European University Institute's Academy of European Law*, 24th Session on European Union Law, 1-12 July 2013, https://edps.europa.eu/data-protection/our-work/publications/speeches-articles/eu-data-protection-law-review-directive_en , E.T. 04.11.2018.
- INGRAM, David, "Of Sweatshops and Subsistence: Habermas on Human Rights", *Ethics & Global Politics*, Vol. 2, No: 3, Y: 2009, ss. 193, 217.
- İLKİZ, Fikret, "Kişisel Verilerin Korunmaması Kanunu", <http://bianet.org/bianet/insan-haklari/174173-kisisel-verilerin-korunmamasi-kanunu> , E.T. 04.04.2019.
- İLKİZ, Fikret, "Kişisel Verilerin Korunması ve Kanun Tasarısı", *Güncel Hukuk*, 2009, S. 7- 67, ss. 12- 23;
- İNCEOĞLU, Sibel, *Anayasa Mahkemesi'ne Bireysel Başvuru- Türkiye ve Latin Modelleri*, On İki Levha Yayıncılık, İstanbul, 2017.

- İNCEOĞLU, Sibel, “Hak ve Özgürlükleri Sınırlama ve Güvence Rejimi”, *İnsan Hakları Avrupa Sözleşmesi ve Anayasa*, Ed. Sibel İNCEOĞLU, Avrupa Konseyi, Ankara, 2013, ss. 23- 52.
- KABOĞLU, İbrahim Ö., “Pozitif Anayasa Hukukunda Düşünce Özgürlüğünün Sınırları”, *Hukuk Felsefesi ve Sosyolojisi Arkivi*, Ed. Hayrettin ÖKÇESİZ, İstanbul, 1998.
- KABOĞLU, İbrahim Ö., *Özgürlükler Hukuku*, İmge Kitabevi, Ankara, 2002.
- KAMA, Sezen, “Parlamente Hükümet Sistemi Olarak ‘Westminster Modeli’ - Britanya Örneği Üzerine Bir Deneme”, *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, C. 22, S. 2, ss. 161- 201.
- KAPANİ, Münci, *Kamu Hürriyetleri*, Ankara, Ankara Üniversitesi Hukuk Fakültesi Yayını, Ankara, 1981.
- KAPANİ, Münci, *Kamu Hürriyetleri*, Yetkin Yayınları, Ankara, 2013.
- KAYA, Cemil, “Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi”, *İÜHFM*, C. LXIX, S. 1-2, Y. 2011, ss. 317- 334.
- KAYA, Cemil, *İdare Hukukunda Bilgi Edinme Hakkı*, Seçkin Yayıncılık, Ankara, 2005.
- KAYA, Mehmet Bedii, *Teknik ve Hukuki Boyutlarıyla İnternete Erişimin Engellenmesi*, On İki Levha Yayıncılık, İstanbul, 2010.
- KELLER, Daphne, “The Right Tools: Europe’s Intermediary Liability Laws and the EU 2016 General Data Protection Regulation”, *Berkeley Technology Law Journal*, Vol. 33, 2018, ss. 297- 377.

- KELLY, Heather, “Facebook will push privacy alert to users outside EU ahead of GDPR”, *CNN Money*, 24.05.2018, https://money.cnn.com/2018/05/24/technology/facebook-gdpr-us/index.html?utm_content=2018-05-24T12%3A36%3A40&utm_source=twmoney&utm_term=image&utm_medium=social , E.T. 01.03.2019.
- KEYTON, Andrew T., “Defamation and Privacy in an Era of ‘More Speech’”, *Comparative Defamation and Privacy Law*, Ed. Andrew T. KEYTON, Cambridge University Press, 2016.
- KIRBY, Michael, “The History, Achievement and Future of the 1980 OECD Guidelines on Privacy”, *International Data Privacy Law*, Vol. 1, No: 1, Y.: 2011, ss. 6-14.
- KLATT, Matthias, “Positive Rights: Who decides? Judicial Review in Balance”, *International Journal of Constitutional Law*, Vol. 13, No: 2, Y: 2015, ss. 354-382.
- KLEKOVIC, Ivan, “EU GDPR vs. European Data Protection Directive”, *EU GDPR Academy*, 30.10.2017, <https://advisera.com/eugdpracademy/blog/2017/10/30/eu-gdpr-vs-european-data-protection-directive/> , E.T. 26.02.2019.
- KORFF, Douwe, *Comparative Study on Different Approaches to New Privacy Challenges in Particular in the light of Technological Developments, Country Studies: Germany*, European Commission, 2010.
- KOSTA, Eleni, *Consent in European Data Protection Law*, Martinus Nijhoff Publishers, Leiden- Boston, 2013.
- KRANENBORG, Herke “Access to Documents and Data Protection in the European Union: On the Public Nature of Personal Data”, *Common Market Law Review*, Vol. 45, Issue: 4, 2008, ss. 1079-1114.

- KRISHNA, Prasad, “Comparison Table of GDPR- DPD”, *The Centre for Internet and Society*, 07.02.2017, <https://cis-india.org/internetgovernance/files/comparison-table-gdpr-dpd> , E.T. 04.03.2019.
- KUNER, Christopher, *Regulation of Transborder Data Flows Under Data Protection and Privacy Law: Past, Present and Future*, OECD Digital Economy Papers No: 187, OECD Publishing, 2011, s. 14.
- KUNER, Christopher, Fred H. CATE, Christopher MILLARD, Dan Jerker B. SVANTESSON, “The Challenge of ‘Big Data’ for Data Protection”, *International Data Privacy Law*, Vol. 2, No: 2, Y: 2012, ss. 47- 49.
- KÜZECİ, Elif, “Anayasal Bir Hak: Kişisel Verilerin Korunması”, *Bilişim Dergisi*, S. 128, Ocak 2011, Türkiye Bilişim Derneği, Ankara, ss. 142- 148.
- KÜZECİ, Elif, “Avrupa Konseyi’nin 108 sayılı Kişisel Verilerin Korunması Sözleşmesi Yenilendi! Sözleşme 108+, Carpenter Kararı ve diğer bazı gelişmelere ilişkin bir değerlendirme”, *Medium*, <https://medium.com/@elfkzc/avrupa-konseyinin-108-sayili-kisisel-verilerin-korunmasi-sozlesmesi-yenilendi-bc8daad9decc> , E.T. 18.05.2019.
- KÜZECİ, Elif, *Kişisel Verilerin Korunması*, Gözden Geçirilmiş ve Yenilenmiş 2. Baskı, Turhan Kitabevi, 2018.
- KÜZECİ, Elif, *Kişisel Verilerin Korunması*, 3. Baskı, Turhan Kitabevi, Ankara, 2019.
- LEENKNEGT, Gert- Jan, “The Protection of Fundamental Rights in Digital Age”, *Electronic Journal of Comparative Law*, Vol. 6.4, Netherlands Comparative Law Association, Aralık 2002.

- LEHNER, Andreas, “The Protection of Personal Data by the Austrian Constitutional Court”, *ICL Journal- Vienna Journal on International Constitutional Law*, Vol. 2, Issue: 3, 2017, <https://doi.org/10.1515/icl-2008-0304> , E.T. 07.09.2017.
- LERNER, K. Lee, Brenda WILMOTH LERNER, Adrienne WILMOTH LERNER (Ed.), *Human and Civil Rights: Essential Primary Sources*, Thomson Gale, 2006, Michigan.
- LETA JONES, Meg, *Ctrl + Z: The Right to Be Forgotten*, New York University Press, New York, 2016.
- LEWIS, Bernard, *Modern Türkiye'nin Doğuşu*, Türk Tarih Kurumu, 8. Bası, İstanbul, 2000.
- LIEW, Anthony, “Understanding Data, Information, Knowledge and Their Inter-Relationships”, *Journal of Knowledge Management Practice*, C. 8, No: 2, June 2007.
- MACENAITE, Milda, Eleni KOSTA, “Consent for Processing Children’s Personal Data in the EU: Following in US Footsteps?”, *Information & Communications Technology Law*, 2017, Vol. 26, No: 2, ss. 146- 197.
- MALDOFF, Gabe, “Top 10 operational impacts of the GDPR: Part:8-Pseudonymization”, *The International Association of Privacy Professionals*, 12.02.2016, <https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-8-pseudonymization/> , E.T. 07.03.2019.
- MARCELLA, Albert J., Carol STUCKI, *Privacy Handbook- Guidelines, Exposures, Policy Implementation and International Issues*, John Wiley & Sons Inc., 2003.

- MCCRUDEN, Christopher, “Human Dignity and Judicial Interpretation of Human Rights”, *The European Journal of International Law*, Vol. 19, No: 4, 2008, ss. 655- 724.
- MEHMOOD, Abid, Iynkaran NATGUNANATHAN, Yong XIANG, Guang HUA, Song GUO, “Protection of Big Data Privacy”, *IEEE Access*, Vol. 4, Y: 2016, ss. 1821- 1834.
- METİN, Yüksel, “Temel Hakların Sınırlandırılması ve Ölçülülük: Ölçülülük Evrensel Bir Anayasal İlke midir?”, *Süleyman Demirel Üniversitesi Hukuk Fakültesi Dergisi*, Vol. 7, No: 1, Y: 2017, ss. 1- 74.
- METİN, Yüksel, *Ölçülülük İlkesi- Karşılaştırmalı Bir Anayasa Hukuku İncelemesi*, Seçkin Yayıncılık, Ankara, 2002.
- MICHAEL, James, *Privacy and Human Rights: An International and Comparative Study with Special Reference to Developments in Information Technology*, UNESCO, 1994.
- MILLARD, Christopher, W. Kuan HON, “Defining ‘Personal Data’ in E-Social Science”, *Information, Communication and Society*, Vol. 15, No:1, February 2012, ss. 66- 84.
- MILLER, Arthur R., *The Assault on Privacy: Computers, Data Bank and Dossiers*, University of Michigan Press, 1971.
- MUMCU, Ahmet, Elif KÜZECİ, *İnsan Hakları ve Kamu Özgürlükleri*, Turhan Kitabevi, 5. Bası, Ankara, 2011.
- NARİN, Bilge, Sevda ÜNAL, “Ünlü Fotoğraflarının Sızdırılmasındaki Etik Sorunlar: Türkiye Medyası Örneği”, *İletişim Hakkı ve Yeni Medya- Tehditler ve Olanaklar*, Eds. Tezcan DURNA, Mutlu BİNARK, Günseli BAYRAKTUTAN, Umag Vakfı Yayınları, 2019, ss. 119- 138.

NISSENBAUM, Helen, *Privacy in Context: Technology, Policy and the Integrity of Social Life*, Stanford University Press, 2010.

NIXON, Richard, “Address on the State of the Union Delivered Before a Joint Session of the Congress”, 30.01.1974, <http://www.presidency.ucsb.edu/ws/?pid=4327> , E.T. 05.12.2016.

NOWAK, Manfred, *Introduction to the International Human Rights Regime*, The Raoul Wallenberg Institute Human Rights Library, Vol. 14, Brill- Martinus Nijhoff Publishers, 2003.

OĞURLU, Yücel, *Karşılaştırmalı İdare Hukukunda Ölçülülük İlkesi*, Seçkin Yayıncılık, Ankara, 2002.

OVEY, Clare, Robin WHITE, *European Convention on Human Rights*, 3rd Ed., Oxford University Press, 2002.

ÖZBUDUN, Ergun, *Türk Anayasa Hukuku*, 17. Basım, Yetkin Yayınları, Ankara, 2017.

ÖZDEMİR, Hayrunnisa, “Haberleşmenin Gizliliği ve Kişisel Veriler”, *Erzincan Üniversitesi Hukuk Fakültesi Dergisi*, C. XIII, S. 1-2, Y. 2009, ss. 285- 303.

ÖZTÜRK, Bahri, Elif ALTINOK ÇALIŞKAN, “Kişisel Verilerin Korunması Kanunu Hakkında Genel Değerlendirmeler ve Anayasaya Aykırılık Sorunu”, *Fasikül Hukuk Dergisi*, Mart 2018, ss. 277- 336.

PACKARD, Vance, *The Naked Society*, Penguin Books, Harmondsworth, 1971.

PALMER, Edith, *Online Privacy Law: Germany Country Report*, June 2012, Library of Congress, <https://www.loc.gov/law/help/online-privacy-law/2012/germany.php> , E.T. 01.05.2019.

- PATTERSON, John, *The Bill of Rights Politics Religion and the Quest for Justice*, iUniverse Inc., 2004.
- PAULSEN, Michael Stokes, Luke PAULSEN, *The Constitution- An Introduction*, Basic Books, New York, 2015.
- PERNICE, Ingolf, “The Treaty of Lisbon and Fundamental Rights”, *The Lisbon Treaty- EU Constitutionalism without a Constitutional Treaty*, Stefan GRILLER, Jacques ZILLER (Ed.), European Community Studies Association of Austria (ECSA Austria) Publication Series, Vol. 11, SpringerWienNewYork, 2008.
- PETERSEN, Kyle, “GDPR: What (and Why) You Need to Know about EU Data Protection Law”, *UTAH Bar Journal*, Vol. 31, No:4, ss. 12- 16.
- PRAKKE, Lucas, Constantijn A. J. M. KORTMANN, *Constitutional Law of 15 EU Member States*, Kluwer Law International, 2005.
- PROSSER, William L., “Privacy”, *California Law Review*, Vol. 48, Y: 1960, No: 3, ss. 383- 423.
- RICCARDI, J. Lee, “The German Data Protection Act of 1977: Protecting the Right to Privacy?”, *Boston College International and Comparative Law Review*, Vol. 6, Issue: 1, 12.01.1983, ss. 243- 271.
- RICHARDSON, Megan, *The Right to Privacy Origins and Influence of Nineteenth-Century Idea*, Cambridge University Press, 2017.
- ROCA, Javier Garcia, “The Preamble, The Convention’s Hermeneutic Context: A Constitutional Instrument of Public Order”, *Europe of Rights: A Compendium on the European Convention on Human Rights*, Eds. Javier Garcia ROCA, Pablo SANTOLAYA, Martinus Nijhoff Publishers, 2012, ss. 1- 26.

- RODRIGUEZ-FERRAND, Graciela, *Online Privacy Law: Spain Country Report*, Library of Congress, June 2012, <https://www.loc.gov/law/help/online-privacy-law/2012/spain.php> , E.T. 02.05.2019.
- ROIG, Antoni, “Safeguards fort he Right not to be Subject to a Decision based solely on Automated Processing (Article 22 GDPR)”, *European Journal of Law and Technology*, Vol. 8, No: 3, Y: 2017, <http://ejlt.org/article/view/570/771> , E.T. 01.06.2019.
- ROSENBERG, Matthew, Nicholas CONFESSORE, Carole CADWALLADR, “How Trump Consultants Exploited the Facebook Data of Millions”, 17.03.2018, <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html> , E.T. 01.03.2019.
- ROSIC, Ameer, “What is Blockchain Technology? A Step-by-Step Guide for Beginners”, *Blockgeeks*, <https://blockgeeks.com/guides/what-is-blockchain-technology/> , E.T. 04.05.2019.
- ROTENBERG, Marc, *The Privacy Law Sourcebook 2001: United States Law International Law and Recent Developments*, Electronic Privacy Information Center, Washington, 2001.
- RÖSSLER, Beate, “Privacies: An Overview”, *Privacies*, Ed.: Beate RÖSSLER, Stanford University Press, 2014, ss. 1- 18.
- RUDGARD, Sian, “Origins and Historical Context of Data Protection Law”, *European Privacy*, International Association of Privacy Professionals (IAPP), 2012, https://iapp.org/media/pdf/publications/European_Privacy_Chapter_One.pdf , E.T. 20.09.2018.

- SAĞLAM, Fazıl, *Temel Hakların Sınırlanması ve Özü*, Ankara Üniversitesi Siyasal Bilgiler Fakültesi Yayınları: 506, S.B.F. İnsan Hakları Merkezi Yayınları: 4, Ankara, 1982.
- SALIHPAŞAOĞLU, Yaşar, “Özel Hayatın Kapsamı: Avrupa İnsan Hakları Mahkemesi İctihatları Işığında Bir Değerlendirme”, *Gazi Üniversitesi Hukuk Fakültesi Dergisi*, C. XVII, Y. 2013, S. 3.
- SCHOEMAN, Ferdinand David, *Privacy and Social Freedom*, Cambridge University Press, 2008.
- SENGER, Harovon, “From the Limited to the Universal Concept of Human Rights: Two Periods of Human Rights”, *Human Rights and Cultural Diversity*, Keip Publishing, 1993.
- SEZER, Abdullah, Emrah KIRIT, Oya BOYAR, *Hukuk Devleti*, Toplumsal Katılım ve Gelişim Vakfı, İstanbul, 2003.
- SHESTACK, Jerome J., “The Philosophical Foundations of Human Rights”, *Human Rights Quarterly*, V. 20, N. 2, Mayıs 1998.
- SHIFERAW, Demelash, Yonas TESFA, *Human Rights Law*, The Justice and Legal System Research Institute, 2009.
- SMARTT, Ursula, *Media and Entertainment Law*, Routledge, London & New York, 2011.
- SOARES, Eduardo, *Online Privacy Law: Portugal Country Report*, June 2012, Library of Congress, https://www.loc.gov/law/help/online-privacy-law/2012/portugal.php#_ftn6 , E.T. 02.05.2019.

SOARES, Eduardo, *Online Privacy Law: Portugal*, Library of Congress, December 2017, <https://www.loc.gov/law/help/online-privacy-law/portugal.php> , E.T. 07.09.2017.

SOFSKY, Wolfgang, *Privacy: A Manifesto*, Princeton University Press, 2008.

SOLOVE, Daniel J., “A Taxonomy of Privacy”, *University of Pennsylvania Law Review*, Vol. 154, No: 3, 2006, ss. 477- 564.

SOLOVE, Daniel J., Marc ROTENBERG, Paul M. SCHWARTZ, *Information Privacy Law*, New York, İkinci Baskı, 2006.

SÖZÜER, Eren, *Unutulma Hakkı İnsan Hakları Hukuku Perspektifinden bir İnceleme*, On İki Levha Yayıncılık, İstanbul, 2017.

STAMPFEL, Gerald, Wilfried GANSTERER, Martin ILGER, “Implications of the EU Data Retention Directive 2006/24/EC”, *Sicherheit 2008: Sicherheit, Schutz und Zuverlässigkeit*, 2.-4. April 2008, Saarbrücker Schloss, <https://eprints.cs.univie.ac.at/331/1/ImplicationsEUDR.pdf> , E.T. 08.02.2019.

STEELE, Jonathan, “Data Protection: An Opening Door? The Relationship Between Accessibility and Privacy in Sweeden in an EU Perspective”, *Liverpool Law Review* 24, ss. 19-39.

STRÖMHOLM, Stig, *Right of Privacy and Rights of the Personality- A Comparative Survey*, Working Paper prepared for the Nordic Conference on Privacy, International Commission of Jurists, Stockholm, May 1967.

ŞİMŞEK, Oğuz, *Anayasa Hukukunda Kişisel Verilerin Korunması*, Beta, 2008.

TANÖR, Bülent, Necmi YÜZBAŞIOĞLU, *1982 Anayasasına Göre Türk Anayasa Hukuku*, 12. Baskı, Beta, 2012.

- TANÖR, Bülent, *Osmanlı-Türk Anayasal Gelişmeleri*, YKY, 9. Bası, İstanbul, 2002.
- TEKİN, Nurullah, “Kişisel Verilerin Korunması ile İlgili Türkiye’deki Kanun Tasarısı’nın Avrupa Birliği Veri Koruma Direktifi Işığında Değerlendirilmesi”, *Uyuşmazlık Mahkemesi Dergisi*, S. 4, ss. 222- 262, 2014.
- TEPE, Harun, “İnsan Hakları: Kavram, Kapsam, Ölçüt”, *Disiplinlerarası Yaklaşımla İnsan Hakları*, Ed. Selda ÇAĞLAR, Beta, İstanbul, 2010, ss. 1- 32.
- TEZCAN, Durmuş, “Bilgisayarın Hukukta Kullanılması ve Özellikle Adli Sicil Sisteminin Mekanik Hale Dönüştürülmesi”, *Adalet Dergisi*, 1979, Y: 70, No: 1-2, ss. 53- 79.
- TEZİÇ, Erdoğan, *Anayasa Hukuku Genel Esaslar*, Beta, Gözden Geçirilmiş 14. Baskı, 2012.
- The Bill of Rights with Writings that Formed Its Foundation*, Applewood Books, Bedford, 2016.
- The U.S. Constitution and Other Key American Writings*, Canterbury Classics/ Baker& Taylor Publishing, San Diego, 2015.
- TIKKINEN-PIRI, Christina, Anna ROHUNEN, Jouni MARKKULA, “EU General Data Protection Regulation: Changes and implications for personal data collecting companies”, *Computer Law & Security Review: The International Journal of Technology Law and Practice*, 2017, ss. 1- 20.
- TOMUSCHAT, Christian, *Human Rights: Between Idealism and Realism*, Oxford University Press, 2008.
- TURK, Alexander H., “Lawmaking after Lisbon”, *EU Law After Lisbon*, Ed. Andrea BIONDI, Piet EECKHOUT, Stefanie RIPLEY, Oxford University Press, 2012, ss. 62- 84.

- TURKINGTON, Richard C., Anita L. ALLEN, *Privacy Law: Cases and Materials*, St. Paul West Group, 1999.
- UMAR, Bilge, *Hukuk Başlangıcı*, Dokuz Eylül Üniversitesi Yayınları, İzmir, 1997.
- USTA, Ahmet, Serkan DOĞANTEKİN, *Blockchain 101*, Digital Age- BKM, 2017.
- UYGUN, Oktay, *1982 Anayasasında Temel Hak ve Özgürlüklerin Genel Rejimi*, Kazancı Yayınları, İstanbul, 1992.
- UYGUN, Oktay, *Türkiye’de Demokrasi ve İnsan Hakları*, TODAİE İnsan Hakları Araştırma ve Derleme Merkezi, Ankara, 1996.
- UYGUN, Oktay, “İnsan Hakları Kuramı”, *İnsan Hakları*, Ed.: Korkut TANKUTER, Yapı Kredi Yayınları, İstanbul, 2000.
- UYGUN, Oktay, “İnsan Hakları Açısından Yeni Anayasa Çalışmaları”, *Kamu Hukuku İncelemeleri – İnsan Hakları, Demokrasi, Hukuk Devleti ve Egemenlik*, Oniki Levha Yayıncılık, İstanbul, 2013, ss. 199- 236.
- UYGUN, Oktay, “Çağımızın İnsan Onuruna Yönelttiği Tehditler Karşısında İnsan Haklarının Önemi”, *Kamu Hukuku İncelemeleri*, Oniki Levha Yayıncılık, İstanbul, 2013, ss. 45- 83.
- UYGUN, Oktay, *Devlet Teorisi*, On İki Levha Yayıncılık, İstanbul, 2014.
- UYGUN, Oktay, *Devlet Teorisi*, 2. Baskı, On İki Levha Yayıncılık, İstanbul, 2015.
- ÜÇÖK, Coşkun, Ahmet MUMCU, Gülnihal BOZKURT, *Türk Hukuk Tarihi*, 14. Bası, Ankara, 2010.

ÜNSAL, Burçak, “Facebook/ Cambridge Analytica skandalının veri koruma çabalarına etkisi”, *Digital Age*, 03.05.2018, <https://digitalage.com.tr/facebook-cambridge-analytica-skandalinin-veri-koruma-cabalarina-etkisi/> , E.T. 01.03.2019.

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

VAN DUN, Frank, “Human Dignity: Reason or Desire? Natural Rights versus Human Rights”, *Journal of Libertarian Studies*, C: 15, N: 4, s.14.

VASAK, Karel, *Human Rights: A Thirty-Year Struggle: the Sustained Efforts to give Force of law to the Universal Declaration of Human Rights*, United Nations Educational, Scientific, and Cultural Organization, November 1977.

VINCENT, Andrew, *The Politics of Human Rights*, Oxford University Press, 2010.

VOIGT, Paul, Axel VON DEM BUSSCHE, *The EU General Data Protection Regulation (GDPR)- A Practical Guide*, Springer International Publishing, 2017.

VOSS, W. Gregory, “European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield and the Right to Delisting”, *Business Lawyer*, Vol. 72, No: 1, Winter 2016/ 2017, January 2017.

WACHTER, Sandra, “The GDPR and the Internet of Things: A Three-Step Transparency Model”, *Law, Innovation and Technology Journal*, Vol. 10, S. 2, Y: 2018, ss. 266- 294.

WARREN, Adam P., James DEARNLY, “Data Protection Legislation in the United Kingdom: From Development to Statute 1969-84”, *Information Communication and Society*, 2005, Vol. 8 (2), ss. 238 – 263.

- WARREN, Samuel, Louis BRANDEIS, "The Right to Privacy", *Harvard Law Review*, Vol. 4, No: 5, 1890, ss. 193- 220.
- WEBB, Philippa, "A Comparative Analysis of Data Protection Laws in Australia and Germany", *Journal of Information, Law and Technology*, 2003, Issue: 2, ss. 2-26.
- WESTIN, Alan F. *Privacy and Freedom*, Atheneum, New York, 1970.
- WESTIN, Alan F., Michael A. BAKER, *Databanks in Free Society: Computers, Recordkeeping and Privacy*, Quadrangle Books, New York, 1972.
- WIRTH, Christian, Michael KOLAIN, "Privacy by Blockchain Design: A Blockchain-enabled GDPR- compliant Approach for Handling Personal Data", *ERCIM Blockchain Workshop 2018: Blockchain Engineering: Challenges and Opportunities for Computer Science Research, Reports of the European Society for Socially Embedded Technologies (EUSSET)*, Vol. 2, No: 6, Y: 2018, https://dl.eusset.eu/bitstream/20.500.12015/3159/1/blockchain2018_03.pdf , E.T. 05.05.2019.
- WOLTERS, P.T.J. (Pietr), "The Enforcement by the Data Subject Under the GDPR", *Journal of Internet Law*, Vol.22, No:8, February 2019, ss. 21- 31.
- WONG, Rebecca, "Data Protection Online: Alternative Approaches to Sensitive Data?", *Journal of International Commercial Law and Technology*, Vol. 2, No:1, 2007, ss. 9- 16.
- WU, Caesar, Rajkumar BUYYA, "Cloud Computing", *Cloud Data Centers and Cost Modelling- A Complete Guide to Planning, Designing and Building a Cloud Data Center*, Morgan Kaufmann, 2015, ss. 3- 41.
- YAVUZ, Can, *İnternetteki Arama Sonuçlarından Kişisel Verilerin Kaldırılması: Unutulma Hakkı*, Seçkin Yayıncılık, Ankara, 2018.

YILDIRIM, Turan, “Kamu Görevlilerinin Özel Hayatı: Cinsel Tercih”, *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, C. 24, S. 2, Y: 2018, ss. 453- 481.

YÜCEL, Bülent, *Parlamente Hükümet Sisteminin Rasyonelleştirilmesi ve Türkiye Örneği*, Adalet Yayınevi, 2009, Ankara.

ZELDIN, Wendy, *Online Privacy Law: Netherlands Country Report*, June 2012, Library of Congress, https://www.loc.gov/law/help/online-privacy-law/2017/netherlands.php#_ftn9 , E.T. 02.05.2019.

ZERDICK, Thomas, “European Aspects of Data Protection: What Rights for the Citizen?”, *Legal Issues of Economic Integration*, Vol. 22, Issue: 2, Y. 1995, s. 80- 83.

Hukuki Metinler, Görüşler, Raporlar ve İnternet Kaynakları

“Protecting personal data when being used by police and criminal justice authorities (from 2018)”, *Summaries of EU Legislation*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3A310401_3 , E.T. 24.02.2019.

Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding Supervisory Authorities and Transborder Data Flows, <https://rm.coe.int/1680080626> , E.T. 27.09.2017.

Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, WP 251rev.01, 06.02.2018, s. 8, https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49826 , E.T. 28.04.2019.

Avrupa Komisyonu, Türkiye 2014 Yılı İlerleme Raporu, Komisyon Tarafından Avrupa Parlamentosuna, Konseye, Ekonomik ve Sosyal Komiteye ve Bölgeler Komitesine Sunulan Bildirim, Genişleme Stratejisi ve Başlıca Zorluklar 2014-2015, Brüksel, 08.10.2014.

Avrupa Komisyonu, Türkiye 2018 Yılı İlerleme Raporu, Komisyon Tarafından Avrupa Parlamentosuna, Konseye, Ekonomik ve Sosyal Komiteye ve Bölgeler Komitesine Sunulan Bilgilendirme, AB Genişleme Politikasına İlişkin 2018 Bilgilendirmesi, Strazburg, 17.04.2018.

Charter of Fundamental Rights of the European Union, 2012/C 326/02, 26.10.2012, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT> , E.T. 30.03.2019.

Charter of Fundamental Rights of the European Union, Art. 51, 18.12.2000, C 364/, http://www.europarl.europa.eu/charter/pdf/text_en.pdf , E.T. 25.01.2019.

Commission of the European Communities, *First Report on the Implementation of the Data Protection Directive (95/46/EC)*, COM (2003) 265, Brussels, 15.05.2003, <http://eur-lex.europa.eu/LexUriServ/site/en/com/2003/com20030265en01.pdf> , E.T. 28.05.2019.

Commission of the European Communities, *Communication on the Protection of Individuals in relation to the Processing of Personal Data in the Community and Information Security* (COM) (90) 314 final- SYN 287&288, 13 Eylül 1990, s.4, <http://aei.pitt.edu/3768/1/3768.pdf> , E.T. 04.11.2018.

Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108> , E.T. 19.09.2017.

Convention 108+, Convention for the protection of individuals with regard to the processing of personal data, 18.05.2018, <https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1> , E.T. 18.05.2019.

Council of Europe, *Details of Treaty No.108- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108> , E.T. 27.09.2017.

Council of Europe, *Explanatory Report to the Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data*, <https://rm.coe.int/16800ca434> , E.T. 21.09.2017.

Council of Europe, Factsheet: “Modernisation of the Data Protection ‘Convention 108’”, <http://www.coe.int/en/web/portal/28-january-data-protection-day-factsheet> , E.T. 27.09.2017.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications), <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN> , E.T. 29.10.2018.

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC, L 105/54, <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32006L0024> , E.T. 08.02.2019.

Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to 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, and repealing Council Framework Decision 2008/977/JHA, 04.05.2016, L 119/89, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016L0680> , E.T. 24.02.2019.

Directive 95/ 46/ EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046> , E.T. 12.09.2018.

Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector, Art. 1, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31997L0066&from=EN> , E.T. 26.10.2018.

Encyclopedia Britannica, <https://www.britannica.com/> , E.T. 19.09.2017;

European Commission, “Agreement on Commission’s EU Data Protection Reform will boost Digital Single Market”, *Press Release*, Brussels, 15.12.2015, http://europa.eu/rapid/press-release_IP-15-6321_en.htm , E.T. 23.02.2019.

European Commission, “Joint Statement on the Final Adoption of the New EU Rules for Personal Data Protection”, Brussels, 14.04.2016, http://europa.eu/rapid/press-release_STATEMENT-16-1403_en.htm , E.T. 22.02.2019.

European Commission, “What constitutes data processing?”, *Reform of EU Data Protection Rules*, https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-constitutes-data-processing_en , E.T. 17.05.2019.

European Commission, “*Why do we need the Charter?*”, https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights/why-do-we-need-charter_en , E.T. 01.09.2018.

European Court of Human Rights, *Factsheet- Personal Data Protection*, Press Unit, February 2019, https://www.echr.coe.int/Documents/FS_Data_ENG.pdf , E.T. 19.05.2019.

European Data Protection Supervisor, *Data Protection, Glossary*, https://edps.europa.eu/data-protection/data-protection/glossary_en , E.T. 17.05.2019.

- European Data Protection Supervisor, *Guidelines on the processing of personal data with regard to the management of conflicts of interest in EU institutions and bodies*, 08.12.2014, https://edps.europa.eu/sites/edp/files/publication/14-12-08_coi_guidelines_en.pdf , E.T. 13.09.2018.
- European Data Protection Supervisor, The History of the General Data Protection Regulation, https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en , E.T. 24.02.2019.
- European Union, “Regulations, Directives and other acts”, *EU Law*, https://europa.eu/european-union/eu-law/legal-acts_en , E.T. 20.04.2019.
- First Report on the Implementation of the Data Protection Directive (95/46/EC), COM/2003/0265 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52003DC0265> , E.T. 31.11.2018.
- Handbook on the European Data Protection Law*, European Union Agency for Fundamental Rights and Council of Europe, 2018.
- International Commission of Jurists, “Right to Privacy: Conclusions of the Nordic Conference”, Mayis 1967, Cenevre. <http://www.icj.org/wp-content/uploads/2013/06/Right-to-privacy-seminar-report-conclusions-1967-eng.pdf> , E.T. 11.12.2016.
- International Commission of Jurists, “The Protection of Privacy”, *UNESCO International Social Science Journal*, Vol. XXIV, No: 3, 1972.
- International Commission of Jurists, Committee on Privacy and JUSTICE (The British Section of ICJ), “Privacy and the Law”, Stevens& Sons Ltd., Londra, 1970.
- International Covenant on Civil and Political Rights, United Nations General Assembly, Resolution 2200 A, 16.12.1966, <https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx> , E.T. 30.03.2019.

International Covenant on Economic, Social and Cultural Rights, United Nations General Assembly, Resolution 2200 A, 16.12.1966, <https://www.ohchr.org/en/professionalinterest/pages/cescr.aspx> , E.T. 30.03.2019.

Kişisel Verileri Koruma Kurulu, “Yurtdışına Veri Aktarımında Veri Sorumlularınca Hazırlanacak Taahhütnamede Yer Alacak Asgari Unsurlar”, <https://www.kvkk.gov.tr/Icerik/2053/Yurtdisina-Aktarim> , E.T. 25.04.2019.

Library of Congress, “Online Privacy Law”, *Research& Reports*, <http://www.loc.gov/law/help/online-privacy-law/index.php> , E.T. 23.05.2019.

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 23 Eylül 1980, <https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm> , E.T. 16.09.2017.

Praesidium, *Explanations relating to the Charter of Fundamental Rights of the European Union and Article 7*, document CONVENT 49, http://www.europarl.europa.eu/charter/pdf/04473_en.pdf , 11.10.2000, E.T. 19.01.2019.

Recommendation 509 (1968) Human Rights and Modern Scientific and Technological Developments, <http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=14546&lang=en> , E.T. 19.09.2017.

Register of Commission Expert Groups and Other Similar Entities, E03461- Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, Updated Table GDPR Implementation Member States, 11.04.2019, <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=30306> , E.T. 03.05.2019.

Regulation (EC) No: 45/2001 of the European Parliament and of the Council of 18 December 2000 on the Protection of Individuals with regard to the Processing of Personal Data by the Community Institutions and Bodies and on the Free Movement of Such Data, <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32001R0045> , E.T. 29.10.2018.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 04.05.2016, <https://eur-lex.europa.eu/legalcontent/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504> , E.T. 21.03.2019.

Report of the Special Rapporteur on the Right to Privacy, Advanced Unedited Version, 27.02.2019, Human Rights Council, Fortieth Session, 25.02-22.03.2019, <https://rm.coe.int/40th-hrc-session-report-of-the-special-rapporteur-on-the-right-to-priv/1680933f08> , E.T. 20.08.2019.

Resolution 73 (22) on the Protection of the Privacy of Individuals vis-a-vis Electronic Data Banks in the Private Sector <https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=589402&SecMode=1&DocId=646994&Usage=2> , E.T. 19.09.2017.

Resolution 74 (29) on the Protection of the Privacy of Individuals vis-a-vis Electronic Data Banks in the Public Sector, <https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=590512&SecMode=1&DocId=649498&Usage=2> , Erişim Tarihi: 19.09.2017.

Safe Harbor Privacy Principles Issued by the U.S. Department Of Commerce, 21.07.2000, <https://rm.coe.int/16806af271> , Erişim Tarihi, 06.10.2018.

Treaty establishing the European Community (Amsterdam consolidated version), Art. 286, [https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX: 11997E286](https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:11997E286) , E.T. 29.10.2018.

Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, 13.12.2007, C 306/1, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12007L%2FTXT> , E.T. 17.02.2019.

TÜBA Türkçe Bilim Terimleri Sözlüğü, <http://www.tubaterim.gov.tr> , E.T. 19.05.2019.

Türk Dil Kurumu, *Güncel Türkçe Sözlük*, http://www.tdk.gov.tr/index.php?option=com_gts&view=gts , E.T. 20.05.2019.

U.S. Department of Health, Education and Welfare, Report of the Secretary’s Advisory Committee on Automated Personal Data Systems, “Records, Computers and the Rights of Citizens”, July 1973, DHEW Publication No. (OS) 73- 94, <https://www.justice.gov/opcl/docs/rec-com-rights.pdf> , E.T. 27.11.2016.

UK Department for Digital, Culture, Media and Sport, *Factsheet: Data Protection Act 2018, – Overview*, 23.05.2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/711162/2018-05-23_Factsheet_1_Act_overview.pdf , E.T. 01.05.2019

UK Government’s Analysis, “Charter of Fundamental Rights of the EU Right by Right Analysis”, 05.12.2017, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/664891/05122017_Charter_Analysis_FINAL_VERSION.pdf , E.T. 01.09.2018.

United Press International (UPI), “Electronic Brain: ‘Peril’ to Liberty”, *Sarasota Journal*, 17 Nisan 1961.

Universal Declaration of Human Rights, United Nations General Assembly, Resolution 217 A, 10.12.1948, <https://www.un.org/en/universal-declaration-human-rights/> , E.T. 30.03.2019.

Wex Legal Dictionary/ Encyclopedia, Legal Information Institute, Cornell Law School, https://www.law.cornell.edu/wex/false_light , E.T. 12.12.2016.

Working Party for Information Security and Privacy (WPISP), *The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines*, Directorate for Science, Technology and Industry – Committee for Information, Computer and Communications Policy, 06.04.2011, <http://www.oecd-ilibrary.org/docserver/download/5kgf09z90c31-en.pdf?expires=1516186345&id=id&acname=guest&checksum=DCF492E917A83B087FFCAE3125E7D32F> , E.T. 16.09.2017.

Working Party on the Protection of Individuals with regard to the Processing of Personal Data, Working Document: Transfers of Personal Data to Third Countries : Applying Articles 25 and 26 of the EU Data Protection Directive, Adopted by the Working Party on 24 July 1998, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1998/wp12_en.pdf , E.T. 06.02.2019.

Working Party on the Protection of Individuals with regard to the Processing of Personal Data, Opinion 03/2013 on purpose limitation, 02.04.2013, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf , E.T. 23.04.2019.

Working Party on the Protection of Individuals with regard to the Processing of Personal Data, Guidelines on consent under Regulation 2016/679, 28.11.2017 and Revised 10.04.2018, s. 15- 16, https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51030 , E.T. 25.04.2019.

Council of Europe, <https://www.coe.int/>, E.T. 19.09.2017.

“The Third Ministerial Meeting on Science at OECD”, March 1968, *The OECD Observer*, No: 33, April 1968, s. 15- 17.

Commission Decision of 14 May 2004 on the Adequate Protection of Personal Data Contained in the Passenger Name Record of Air Passengers Transferred to the United States’ Bureau Of Customs and Border Protection, Par. 14, 2004/535/EC, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32004D0535> , E.T. 17.01.2019.

Council Decision of 17 May 2004 on the Conclusion of an Agreement Between the European Community and the United States of America on the Processing and Transfer of PNR Data by Air Carriers to the United States Department of Homeland Security, Bureau Of Customs And Border Protection, Par. 2-3, 2004/496/EC, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32004D0496> , E.T. 17.01.2019.

Article 29 Data Protection Working Party, Opinion 4/2007 on the Concept of Personal Data, 20.06.2007, 01248/07/EN WP136, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf , E.T. 17.05.2019.

Article 29 Data Protection Working Party, Opinion 8/2010 on Applicable Law, 16 December 2010 (WP 179), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp179_en.pdf , E.T. 05.11.2018.

Article 29 Data Protection Working Party, *Opinion 05/ 2012 on Cloud Computing*, WP 196, 01.07.2012, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf , E.T. 24.03.2019.

Article 29 Data Protection Working Party, Opinion 8/ 2014 on the Recent Developments on the Internet of Things, WP 223, 16.09.2014, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf , E.T. 25.03.2019.

OECD, <http://www.oecd.org/>, E.T. 16.09.2017.

Handbook on Data Protection Laws of the World, 10.01.2019, DLA Piper, <https://www.dlapiperdataprotection.com> , E.T. 30.04.2019.

Consolidated Version of the Treaty on European Union, Art. 6, 26.10.2012, C 326/13, https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0023.02/DOC_1&format=PDF , E.T. 25.01.2019.

Draft Charter of Fundamental Rights of the European Union, 11.10.2000, 4473/00, Convent 49, http://www.europarl.europa.eu/charter/pdf/04473_en.pdf , E.T. 21.01.2019.

Kararlar

- Amann v. Switzerland*, Application No: 27798/95, 16.02.2000, <http://hudoc.echr.coe.int/eng?i=001-58497> , E.T. 18.10.2017.
- Benedik v. Slovenia*, Application No: 62357/14, 24.07.2018, <http://hudoc.echr.coe.int/eng?i=001-182455> , E.T. 19.05.2019.
- Bensaid v. United Kingdom*, Par. 47, Application No: 44599/98, 06.05.2011, <http://hudoc.echr.coe.int/eng?i=001-59206> , E.T. 29.09.2017.
- Big Brother Watch and Others v. The United Kingdom*, Application Nos: 58170/ 13, 62322/ 14 and 24960/ 15, <http://hudoc.echr.coe.int/eng?i=001-186048> , E.T. 19.08.2019.
- Centrum for Rattvisa v. Sweeden*, Application No: 35252/ 08, 19.06.2018, <http://hudoc.echr.coe.int/eng?i=001-183863> , E.T. 19.08.2019.
- Copland v. The United Kingdom*, Application No: 62617/00, 03.07.2007, <http://hudoc.echr.coe.int/eng?i=001-79996> , E.T. 29.05.2019.
- Fernandez Martinez v. Spain*, Application No: 56030/07, 12.06.2014, <http://hudoc.echr.coe.int/eng?i=001-145068> , E.T. 25.10.2018.
- Friedl v. Austria*, Application No: 15225/89, 31.01.1995, <http://hudoc.echr.coe.int/eng?i=001-57917> , E.T. 18.10.2017.
- Gaskin v. United Kingdom*, Application No: 10454/ 83, 07.07.1989, <http://hudoc.echr.coe.int/eng?i=001-57491> , E.T. 10.01.2018.
- Gorlov and Others v. Russia*, Application Nos: 27057/06, 56443/09, 25147/14, 02.07.2019, <http://hudoc.echr.coe.int/eng?i=001-194247> , E.T. 18.05.2019.

- Huvig* v. *France*, Application No: 11105/84, 24.04.1990,
[http://cambodia.ohchr.org/sites/default/files/echrsources/Huvig%20v.%20France%20\[24%20Apr%201990\]%20\[EN\].pdf](http://cambodia.ohchr.org/sites/default/files/echrsources/Huvig%20v.%20France%20[24%20Apr%201990]%20[EN].pdf) , E.T. 21.01.2018.
- I* v. *Finland*, Application No: 20511/03, 17.10.2008,
<http://hudoc.echr.coe.int/eng?i=001-87510> , E.T. 15.08.2018.
- Karabeyoğlu* v. *Turkey*, Application No: 30083/10, 17.10.2016,
<http://hudoc.echr.coe.int/eng?i=001-163455> , E.T. 19.05.2019.
- Khelili* v. *Switzerland*, Application No: 16188/07, 08.03.2012,
<http://hudoc.echr.coe.int/eng?i=001-107032> , E.T. 03.11.2018.
- Klass and Others* v. *Germany*, Application No: 5029/71, 06.09.1978,
<http://hudoc.echr.coe.int/eng?i=001-57510> , 29.11.2017.
- Kruslin* v. *France*, Application No: 11801/85, 24.04.1990,
<http://hudoc.echr.coe.int/eng?i=001-57626> , E.T. 21.01.2018
- L.H.* v. *Latvia*, Application No: 52019/07, 29.07.2014,
<http://hudoc.echr.coe.int/eng?i=001-142673> , E.T. 19.05.2019.
- Leander* v. *Sweden*, Application No: 9248/81, 26.03.1987,
<http://hudoc.echr.coe.int/eng?i=001-57519> , E.T. 06.10.2017.
- Lundvall* v. *Sweden*, Application No: 10473/83, 11.12.1985,
<http://hudoc.echr.coe.int/eng?i=001-72432> , E.T. 30.05.2019.
- Malone* v. *United Kingdom*, Application No: 8691/79, 02.08.1984,
<http://hudoc.echr.coe.int/eng?i=001-57533> , E.T. 06.10.2017.

Malone v. United Kingdom, Concurring Opinion of Judge Pettiti, Application No: 8691/79, 02.08.1984, <http://hudoc.echr.coe.int/eng?i=001-57533> , E.T. 06.10.2017.

McGinley and Egan v. The United Kingdom, Application No: 21825/93& 23414/94, 28.11.2000, <http://hudoc.echr.coe.int/eng?i=001-58452> , E.T. 30.05.2019.

Mustafa Sezgin Tanrıkulu v. Turkey, Application No: 27473/06, 18.10.2017, <http://hudoc.echr.coe.int/eng?i=001-175464> , E.T. 19.05.2019.

Niemietz v. Germany, Application No: 13710/88, 16.12.1992, <http://hudoc.echr.coe.int/eng?i=001-57887> , E.T. 29.09.2017.

Peck v. The United Kingdom, Application No: 44647/98, 28.04.2003, <http://hudoc.echr.coe.int/eng?i=001-60898> , E.T. 28.05.2019.

Perry v. The United Kingdom, Application No: 63737/00, 17.10.2003, <http://hudoc.echr.coe.int/eng?i=001-61228> , E.T. 29.05.2019.

R.E. v. The United Kingdom, Application No: 62498/11, 27.01.2016, <http://hudoc.echr.coe.int/eng?i=001-158159> , E.T. 19.05.2019.

Rotaru v. Romania, Application No: 28341/95, 04.05.2000, <http://hudoc.echr.coe.int/eng?i=001-58586> , E.T. 19.10.2017.

S. and Marper v. The United Kingdom, Application Nos: 30562/04 and 30566/04, 04.12.2008, <http://hudoc.echr.coe.int/eng?i=001-90051> , E.T. 03.11.2017.

Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland, Application No: 931/13, 27.06.2017, <http://hudoc.echr.coe.int/eng?i=001-175121> , E.T. 18.01.2019.

Segerstedt-Wiberg and others v. Sweden, Application No. 62332/00, 06.09.2006, <http://hudoc.echr.coe.int/eng?i=001-75591> , E.T. 30.05.2019.

Sinan Isik v. Turkey, Application No: 21924/ 05, 02.05.2010,
<http://hudoc.echr.coe.int/eng?i=001-97087> , E.T. 21.08.2019.

Société Colas Est and Others v. France, Application No. 37971/97, 16.07.2002,
<http://hudoc.echr.coe.int/eng?i=001-60431> , E.T. 30.05.2019.

Tyrer v. United Kingdom, Application No: 5856/72, 25.04.1978,
<http://hudoc.echr.coe.int/eng?i=001-57587> , E.T. 29.09.2017.

X v. Iceland, Application No: 6825/74, 18.05.1976, <http://echr.ketse.com/doc/6825.74-en-19760518/i> , E.T. 28.09.2017.

Z v. Finland, Application No: 22009/93, 25.02.1997, <http://hudoc.echr.coe.int/eng?i=001-58033> , E.T. 08.11.2017.

YHGK, E. 2014/4-56, K. 2015/1679, K.T. 17.06.2015.

AYM Kararı, E. 1963/ 132, K. 1966/29, T. 28.06.1966, AMKD, S. 4.

AYM E. 1979/9, K. 1979/44, K.T. 27.11.1979.

AYM E. 1995/17, K. 1995/16, K.T. 21.06.1995.

AYMK E. 1996/68, K. 1999/1, K.T. 06.01.1999.

AYMK E. 2006/ 167, K. 2008/86, K.T. 20.03.2008

AYMK E. 2006/ 167, K. 2008/86, K.T. 20.03.2008.

AYMK E. 2010/12, K. 2011/135, K.T. 12.10.2011

AYMK E. 2010/12, K. 2011/135, K.T. 12.10.2011.

AYMK E. 2010/12, K. 2011/135, K.T. 12.10.2011.

AYMK E. 2011/150, K. 2013/30, K.T. 14.02.2013.

AYMK E. 2011/150, K. 2013/30, K.T. 14.02.2013.

AYMK E.2013/122, K. 2014/74, K.T. 09.04.2014.

AYMK E.2013/122, K. 2014/74, K.T. 09.04.2014.

AYMK E. 2014/149, K. 2014/151, K.T. 02.10.2014.

AYMK E. 2013/114, K. 2014/184, K.T. 04.12.2014.

AYMK E. 2013/84, K. 2014/ 183, K.T. 04.12.2014.

AYMK E. 2013/84, K. 2014/ 183, K.T. 04.12.2014.

AYMK, E. 2014/180, K. 2015/30, K.T. 19.03.2015.

AYMK E. 2015/32, K. 2015/102, K.T. 12.11.2015.

N.B.B. Başvurusu, Başvuru No: 2013/5653, K.T. 03.03.2016.

Bülent Kaya Başvurusu, Başvuru No: 2013/2941, K.T. 11.05.2016.

AYMK E. 2016/125, K. 2017/143, K.T. 28.09.2017.

AYMK E. 2016/125, K. 2017/143, K.T. 28.09.2017.

E.Ç.A. Başvurusu, Başvuru No: 2014/5671, K.T. 07.06.2018.

Fatih Saraman Başvurusu, Başvuru No: 2014/7256, K.T. 27.02.2019.

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, <https://www.kvkk.gov.tr/Icerik/4110/2018-10> , E.T. 28.04.2019.

Arabulucuların Veri Sorumluları Siciline Kayıt Zorunluluğundan İstisna Tutulması ile ilgili Kişisel Verileri Koruma Kurulunun 05/07/2018 Tarihli ve 2018/75 Sayılı Kararı, <https://www.kvkk.gov.tr/Icerik/5270/2018-75> , E.T. 27.04.2019.

Gümrük Müşavirlerinin Sicile Kayıt İstisnası Hakkında Görüş Talebi ile ilgili Kişisel Verileri Koruma Kurulunun 28/06/2018 Tarihli ve 2018/68 Sayılı Kararı, <https://www.kvkk.gov.tr/Icerik/5269/2018-68> , E.T. 27.04.2019.

Sicile Kayıt Yükümlülüğünün Başlama Tarihleri ile ilgili Kişisel Verileri Koruma Kurulunun 19/07/2018 Tarihli ve 2018/88 Sayılı Kararı, <https://www.kvkk.gov.tr/Icerik/5272/2018-88> , E.T. 27.04.2019.

Google Spain SLand Google Inc. V. Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzalez, 13.05.2014, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131> , E.T. 15.04.2019.

Case C-212/ 13 *František Ryneš v. Úřad pro ochranu osobních údajů*, 11.12.2014, Par. 30, 35, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62013CJ0212> , E.T. 22.04.2019.

Case C-362/14 *Maximillian Schrems v. Data Protection Commissioner*, 06.10.2015, Par. 88-89, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362> , E.T. 21.03.2019.

Case C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, 13.05.2014, Par. 94, 100, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131>, E.T. 19.05.2019.

Joined Cases C-465/00, C-138/01 and C-139/01, *Rechnungshof v Österreichischer Rundfunk and Others and Christa Neukomm and Joseph Lauermann v Österreichischer Rundfunk*, 20 May 2003, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=ecli:ECLI:EU:C:2003:294>, E.T. 01.01.2019.

Joined Cases C-141/12 *Y.S. v. Minister voor Immigratie, Integratie en Asiel* and C-372/12 *Minister voor Immigratie, Integratie en Asiel v. M. and S.*, 17.07.2014, Par. 8, 44, <http://curia.europa.eu/juris/document/document.jsf?docid=155114&doclang=EN>, E.T. 22.04.2019.

Joined Cases C-317/04 and C-318/04 *European Parliament v Council of the European Union and Commission of the European Communities*, 30.05.2006, Par. 54-61, 67- 70, <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A62004CJ0317>, E.T. 17.01.2019.

Case C-342/12 *Worten – Equipamentos para o Lar SA v. Autoridade para as Condições de Trabalho (ACT)*, 30.05.2013, Par. 24, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0342&from=FR>, E.T. 27.04.2019.

Joined Cases C-468/10 and C-469/10 *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECMD) v. Administración del Estado*, 24.11.2011, Par. 37- 38, 49, 51- 55, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62010CJ0468>, E.T. 18.01.2019.

Case C-518/07 *European Commission v. Federal Republic of Germany*, 09.03.2010, <http://curia.europa.eu/juris/celex.jsf?celex=62007CJ0518&lang1=en&type=TEXT&ancre=> , E.T. 26.01.2019.

Case C-553/07 *College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer*, Par. 62, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62007CJ0553&from=EN> , E.T. 27.04.2019.

Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, 08.04.2014, Par. 68, <http://curia.europa.eu/juris/celex.jsf?celex=62012CJ0293&lang1=en&type=TEXT&ancre=> , E.T. 27.01.2019.

Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, 08.04.2014, <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A62012CJ0293> , E.T. 31.01.2019.

Case C-73/07 *Tietosuoja-valtuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy*, 16.12.2008, Par. 44, <https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:62007CJ0073> , E.T. 18.01.2019.

Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen*, 09.11.2010, Par. 30- 44, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62009CJ0092> , E.T. 28.01.2019.

Case C-291/12 *Michael Schwarz v Stadt Bochum*, 17.10.2013, Par. 12, 29- 30, 32- 33, 39, 63- 66, <http://curia.europa.eu/juris/celex.jsf?celex=62012CJ0291&lang1=en&type=TEXT&ancre=> , E.T. 31.01.2019.

Case 486/12 X, 12.12.2013, Par. 20- 23, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0486> , E.T. 04.04.2019.

Case C-288/12, *European Commission v. Hungary*, 08 April 2014, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0288> , E.T. 06.11.2018.

Case C-288/12, *European Commission v. Hungary*, 08 April 2014, Par. 48, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0288> , E.T. 04.04.2018.

Case C-101/01, Criminal proceedings against *Bodil Lindqvist*, 06.11.2003, Par. 47, <https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX%3A62001CJ0101> , E.T. 18.01.2019.

Case C-614/10, *European Commission v. Republic of Austria*, 16 October 2012, Par. 37, <https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX%3A62010CJ0614> , E.T. 06.11.2018.

Case C-288/12, *European Commission v. Hungary*, 08 April 2014, Par. 48, <https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX%3A62012CJ0288> , E.T. 06.11.2018.

Case C-582/14, *Patrick Breyer v Bundesrepublik Deutschland*, 19.10.2019, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0582> , E.T. 04.02.2019.

Griswold v. Connecticut, 381 U.S. 479 (1965), <https://supreme.justia.com/cases/federal/us/381/479/> , E.T. 21.11.2016.

Whalen v. Roe, 429 U.S. 589 (1977), <https://supreme.justia.com/cases/federal/us/429/589/case.html> , E.T. 17.05.2019.

Felix c. O'Connell, Seine Hukuk Mahkemesi, 16.6.1858.

Prince Albert v. Strange, High Court of Chancery, (1849) 1 Mac & G 25, [1849] EWHC Ch J20, 41 ER 1171, (1849) 18 LJ Ch 120, <http://www.bailii.org/ew/cases/EWHC/Ch/1849/J20.html> , E.T. 19.12.2016.

