T.C.

ALTINBAŞ ÜNİVERSİTESİ

Lisansüstü Eğitim Enstitüsü

Kamu Hukuku

KİŞİSEL VERİLERİN KORUNMASI KANUNU BAKIMINDAN AYDINLATMA YÜKÜMLÜLÜĞÜNÜN YERİNE GETİRİLMEMESİ KABAHATİ

Ramazan DEDE

Yüksek Lisans Tezi

Danışman

Doç. Dr. Hasan SINAR

İstanbul, 2022

KİŞİSEL VERİLERİN KORUNMASI KANUNU BAKIMINDAN AYDINLATMA YÜKÜMLÜLÜĞÜNÜN YERİNE GETİRİLMEMESİ KABAHATİ

Ramazan DEDE

Kamu Hukuku

Yüksek Lisans Tezi

ALTINBAŞ ÜNİVERSİTESİ
2022

"Ramazan DEDE" tarafından hazırlanmış ve 20/05/2022 tarihinde sunulmuş "KİŞİSEL VERİLERİN KORUNMASI KANUNU BAKIMINDAN AYDINLATMA YÜKÜMLÜLÜĞÜNÜN YERİNE GETİRİLMEMESİ KABAHATİ" başlıklı tez Kamu Hukuku Anabilim Dalında Yüksek Lisans Tezi olarak **oy çokluğu** ile kabul edilmiştir.

Doç. Dr. Hasan SINAR
Danışman

Tez Savunma Sınavı Jüri Üyeleri:

Doç. Dr. Hasan SINAR	Hukuk Fakültesi, Altınbaş Üniversitesi	_____
Prof. Dr. Zeynel KANGAL	Hukuk Fakültesi, Üniversite	_____
Dr. Öğr. Üyesi Fulya EROĞLU	Hukuk Fakültesi, Üniversite	_____

Bu tezin Yüksek Lisans. tezi olarak bütün şartları sağladığını beyan ederim.

Tezin Lisansüstü Eğitim Enstitüsüne teslim
tarihi: 20/06/2022

Bu tezdeki tüm bilgilerin akademik kurallara ve etik davranışlara uygun olarak edinildiğini ve sunulduğunu beyan ederim. Ayrıca, bu kuralların ve davranışların gerektirdiği şekilde, bu çalışmada, orijinal olmayan tüm materyalleri ve sonuçları tamamen alıntı yaptığımı ve referans gösterdiğimi de beyan ederim.

Ramazan DEDE
İmzası

____/____/____

İTHAF

Üzerimdeki emeklerini kelimelerle anlatmanın güç olduğu, Kıymetli Annem, Babam, Sevgili Eşim ve Oğlum Eyüp Faruk'a…

TEŞEKKÜR

Keyifli ve uzun bir yol olduğunu düşündüğüm bilim ve ilim sahibi olma sürecinde her zaman yanımda olan, yüksek lisans tez öneri sürecimde fikirleriyle ve görüşleriyle tez konumu şekillendiren, bana yol gösteren, sabrı, hoşgörüsü, ilgisi, anlayışı ve tez araştırmama sağladığı destek ve katkılarından dolayı sayın hocalarım, danışmanım, Doç. Dr. Hasan SINAR'a ve Arş. Gör. Batuhan AKTAŞ'a minnettarım.

Tez konumun araştırma ve veri toplama aşamalarında, birebir tanışma fırsatı yakaladığım, bana arkadaşça davranan meslektaşlarıma, Marmara Üniversite kütüphanesi yöneticilerine ve kütüphanecilerine tüm destek ve yardımları için şükranlarımı sunarım.

Hayat yolumu çizmemde her zaman benim yanımda duran, sahip olduğum kültürü, bilgiyi ve deneyimi bana kazandıran, her zaman beni destekleyen ve bana gösterdikleri sevgi ve saygıdan dolayı anneme ve babama çok teşekkür ederim.

Ayrıca süresiz devam eden öğrencilik hayatıma maddi manevi desteğini esirgemeyen özveriyle her zaman yanımda olan sevgili eşim Nurcan'a ayrıca çok teşekkür ederim. Son olarak 27 Ağustos tarihinde dünyaya gelen canım oğlum Eyüp Faruk, ailemize kattığın mutluluk için teşekkür ediyorum.

ÖZET

KİŞİSEL VERİLERİN KORUNMASI KANUNU BAKIMINDAN AYDINLATMA YÜKÜMLÜLÜĞÜNÜN YERİNE GETİRİLMEMESİ KABAHATİ

DEDE Ramazan

Yüksek Lisans, Kamu Hukuku Anabilim Dalı, Altınbaş Üniversitesi

Danışman: Doç. Dr. Hasan SINAR

Tarih: Mayıs, 2022

Sayfa: 202

Ticari kuruluşlar bakımından pek önemli değer haline gelen kişisel veriler, günümüzde bu kuruluşlar tarafından adeta ekonominin yeni yakıtı olarak ifade edilmeye başlanmıştır. Bireylerin kişilik hakkı sınırları içerisinde kendisine yer bulan kişisel verilerin, ticari bir araç olma tehlikesine karşı korunması elbette çok önemlidir. Kişisel verilerin metalaşma tehlikesine karşı kişisel verilerin korunmasını talep etme hakkı, diğer ülkelerde olduğu gibi ülkemizde de temel insan hakkı olarak kabul edilmektedir.

Kişisel Verilerin Korunması Kanunu m.10'da veri sorumlusu veya yetkilendirdiği kişinin, kişisel verilerin elde edilmesi esnasında ilgili kişiyi aydınlatma yükümlülüğünü düzenlemektedir. Kişisel Verilerin Korunması Kanunu m.18'de aydınlatma yükümlülüğünün yerine getirilmemesi kabahati düzenlenmektedir. Bu düzenlemeye göre, aydınlatma yükümlülüğünü yerine getirmeyenler hakkında çeşitli cezaların uygulanması öngörülmektedir.

Yapmış olduğumuz çalışmanın ilk bölümünde, kişisel verilerin korunması ihtiyacının ortaya çıkışı, tarihsel gelişimi, kişisel verilerin korunması kavramının hukuki niteliği, uluslararası hukukta kişisel verilerin korunmasına ilişkin temel metinlerden kısaca bahsedilmiştir. Zira bahse konu bilgilerin ayrıntılarına, çalışmamın sınırlarını aşacağı endişesiyle yer verilmediğini belirtmek isterim. İkinci bölümde ise, kişisel verilere ilişkin genel tanımlar ve kişisel verilerin korunmasında temel unsurlar hakkında bilgilere yer verilmiştir. Üçüncü bölümde ise, kişisel verilerin ceza ve kabahatler hukuku bakımından incelenmesi ve aydınlatma yükümlülüğünün ilkeleri hakkında açıklamalar yapılmıştır. Son olarak aydınlatma yükümlülüğünün yerine getirilmemesi kabahati yapısal unsurları ve yaptırım usulü yönünden incelenmiştir.

Anahtar kelimeler: (Kişisel Verilerin Korunması, Aydınlatma Yükümlülüğü, İdari Yaptırım, Kişisel Veri.)

ABSTRACT

THE MISDEMEANOR OF NOT FULFILL THE LIGHTING INFORMATION IN TERMS OF THE TURKISH PERSONAL DATA PROTECTION LAW

DEDE Ramazan

M. A, Public Law Department, Altınbaş University

Supervisor: Doç. Dr. Hasan Sınar

Date: May 2022

Pages: 202

Personal data, which has become a very important value for commercial organizations, today has started to be expressed by these organizations as the new fuel of the economy. Of course, it is very important to protect the personal data within the boundaries of individual personal rights against the danger of being a commercial tool. The right to demand the protection of personal data against the danger of commodification of personal data is accepted as a fundamental human right in Turkey, as in other countries.

Article 10 of Turkish Personal Data Protection Law regulates the obligation of the data controller or the person authorized by him to inform the person concerned during the acquisition of personal data. In Article 18 of the Turkish Personal Data Protection Law, the fault of not fulfilling the obligation to inform is regulated. According to this regulation, various punishments are envisaged for those who do not fulfill their obligation to inform.

In the first part of our study, the emergence of the need for personal data protection, its historical development, the legal nature of the concept of personal data protection, the basic texts on the protection of personal data in international law are briefly mentioned. Because, I would like to state that the details of the aforementioned information are not included because of the concern that it would exceed the limits of my study. In the second part, general definitions of personal data and information about the basic elements of personal data protection are given. In the third part, explanations are given about the examination of personal data in terms of criminal and misdemeanor law regulations and the principles of the obligation to inform. Finally, the fault of not fulfilling the obligation to inform is examined in terms of its structural elements and sanction procedure.

Keywords: (Personal Data Protection, Clarification Obligation, Administrative Sanction, Personal Data.)

İÇİNDEKİLER

Sayfa

ÖZET ..... **vii**

ABSTRACT ..... **ix**

KISALTMALAR ..... **xiv**

1. GİRİŞ **1**

2. BİRİNCİ BÖLÜM **5**

KİŞİSEL VERİLERİN KORUNMASI İHTİYACININ ORTAYA ÇIKIŞI, TARİHSEL GELİŞİMİ, KİŞİSEL VERİLERİN KORUNMASI KAVRAMININ HUKUKİ NİTELİĞİ, ULUSLARARASI HUKUKTA KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN TEMEL METİNLER **5**

2.1. KİŞİSEL VERİLERİN KORUNMASI İHTİYACININ ORTAYA ÇIKIŞI 5

2.2. TARİHSEL GELİŞİMİ 8

2.3. GENEL ANLAMDA KİŞİSEL VERİLERİN KORUNMASI HUKUKU 14

2.4. ULUSLARARASI HUKUKTA KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN TEMEL METİNLER 17

2.4.1 Birleşmiş Milletler 17

2.4.2 OECD 19

2.4.3 Avrupa Konseyi 21

2.4.3.1 108 sayılı sözleşme 23

2.4.3.2 Avrupa insan hakları sözleşmesi 32

2.4.4 Avrupa Birliği 35

2.4.4.1 95/46/AT sayılı kişisel verilerin korunması yönergesi 37

2.4.4.2 AB temel haklar koşulu 39

2.4.4.3 Avrupa birliği genel veri koruma tüzüğü 41

2.4.4.4 Elektronik veriyi koruma kapsamında 2002/58/EC sayılı Avrupa Birliği direktifi 49

2.4.4.5 Avrupa Birliği vatandaşlık hakkı direktifi 49

2.4.4.6 Europol antlaşması ve kişisel verilerin korunması 49
2.4.4.7 Eurojust 50
2.4.4.8 Schengen antlaşması ve kişisel verilerin korunması 51
2.5. YABANCI HUKUKTA KİŞİSEL VERİLERİN KORUNMASI 51
2.5.1. Genel Olarak 51
2.5.2. Fransa 52
2.5.3. Almanya 53
2.5.4. İtalya 56
2.5.5. Amerika Birleşik Devletleri 57
2.5.6. İngiltere 59
3. İKİNCİ BÖLÜM 62
KİŞİSEL VERİLERE İLİŞKİN TERMİNOLOJİ, HUKUKİ NİTELİĞİ, KİŞİSEL VERİLERİN KORUNMASI HAKKININ DİĞER TEMEL HAK VE ÖZGÜRLÜKLERLE İLİŞKİSİ VE TEMEL İLKELER 62
3.1. KİŞİSEL VERİNİN TANIMI, UNSURLARI, KİŞİSEL VERİ TÜRLERİ VE BAZI TEMEL KAVRAMLAR 62
3.1.1 Kişisel Verinin Tanımı 62
3.1.1.1. Bilgi kavramı 63
3.1.1.2. Kimliği belirli veya belirlenmesi mümkün kişi kavramı 63
3.1.1.3. Bilginin kimliği belirli veya belirlenebilir kişiye ait olması 64
3.1.2. Kişisel Veri Türleri 67
3.1.2.1. Hassas - özel nitelikli kişisel veriler 68
3.1.2.2. Anonim nitelikli kişisel veriler 73
3.1.3. Kişisel Verilerin Korunması Hakkının Hukuki Niteliğine İlişkin Görüşler 75
3.1.3.1. Verilerin geleceğini belirleme ve bireysel özerklik kavramı görüşü 76
3.1.3.2. Özel hayatın gizliliği hakkı görüşü 78
3.1.3.3. Mülkiyet hakkı görüşü 81
3.1.3.4. Fikri mülkiyet hakkı görüşü 83

3.1.3.5. Öne sürülen görüşler hakkında değerlendirmelerimiz 85

4. ÜÇÜNCÜ BÖLÜM 88

KİŞİSEL VERİLERİN CEZA VE KABAHATLER HUKUKU BAKIMINDAN İNCELENMESİ VE AYDINLATMA YÜKÜMLÜLÜĞÜNÜN ESASLARI 88

4.1. KİŞİSEL VERİLERİN CEZA VE KABAHATLER HUKUKU BAKIMINDAN İNCELENMESİ 88

4.1.1. Genel 88

4.1.2. Türk Ceza Kanunu'nda Kişisel Verilerin Korunmasına Yönelik İşlenen Suçlar 90

4.1.2.1. Kişisel verilerin hukuka aykırı olarak kaydedilmesi suçu 90

4.1.2.2. Verileri hukuka aykırı olarak verme veya ele geçirme suçu 94

4.1.2.3. Kişisel verilerin yok edilmemesi suçu 95

4.1.3. Kişisel Verileri Silmeme ve Anonim Hâle Getirmeme Suçu 97

4.1.4. Kişisel Verilerin Korunması Kanunu'nda Düzenlenen Kabahatler 99

4.1.4.1. Veri güvenliği bakımından yükümlülüklerin yerine getirilmemesi 99

4.1.4.2. Kişisel verileri koruma kurulu tarafından alınan kararların yerine getirilmemesi 100

4.1.4.3. Veri sorumluları siciline kaydolma yükümlülüğünün yerine getirilmemesi 101

4.1.4.4. Aydınlatma yükümlülüğünün yerine getirilmemesi 102

4.2. AYDINLATMA YÜKÜMLÜLÜĞÜNÜN ESASLARI 103

4.2.1. Kişisel Verilerin İşlenmesinde Açıklık (Şeffaflık) İlkesi 103

4.2.2. Aydınlatma Yükümlülüğü 106

4.2.3. Aydınlatma Yükümlülüğünün Kapsamı 108

4.2.4. Aydınlatma Yükümlülüğünde Amaç 110

4.2.4.1. İlgili kişinin rızası 111

5. DÖRDÜNCÜ BÖLÜM 118

AYDINLATMA YÜKÜMLÜLÜĞÜ KAPSAMINDA KABAHAT VE YAPTIRIMLARI 118

5.1. AYDINLATMA YÜKÜMLÜLÜĞÜ KAPSAMINDA KORUNACAK OLAN HUKUKİ DEĞERLER 118
5.2. KABAHAT EYMENİN MADDİ UNSURLARI 118
5.2.1. Kabahatin Konusu 119
5.2.2. Fiil Unsuru 120
5.2.2.1. Kişiye karşı aydınlatma yükümlülüğünün yerine getirme zamanı 122
5.2.2.2. Aydınlatma yükümlülüğünün yerine getirilmesinde şekil unsurları 125
5.2.2.3. Aydınlatma yükümlülüğü kapsamında yapılan bilgilendirmede bulunması gereken unsurlar 128
5.2.3. Fail 132
5.2.4. Mağdur 136
5.2.5. Manevi Unsurlar 137
5.2.6. Hukuka Aykırılık Unsuru 138
5.2.7. Suçun Unsurları Bakımından Kusurluluk 140
5.2.8. Suçun Özel Görünüş Biçimleri 141
5.2.8.1. Teşebbüs 141
5.2.8.2. İştirak 142
5.2.8.3. İçtima 143
5.2.9. Kişisel Verilerin Korunmasında Denetim Ve Yaptırım Yöntemleri 147
5.2.9.1. Veri sorumlusuna başvuru yoluyla koruma 147
5.2.9.2. İdari yaptırım yoluyla koruma 148
5.2.9.3. İhlal durumunda kişisel verileri koruma kuruluna şikâyet 156
5.2.10. Kişisel Verilerin Korunmasında Zamanaşımı 160
5.2.10.1. Soruşturma zamanaşımı 160
5.2.10.2. Yerine getirme zamanaşımı süresi 162
6. SONUÇ 165
REFERANSLAR 180

KISALTMALAR

ABAD : Avrupa Birliği Adalet Divanı
AK : Avrupa Konseyi
a.g.e. : Adı geçen eser
AB : Avrupa Birliği
ABTHŞ : Avrupa Birliği Temel Haklar Şartı
AİHM : Avrupa İnsan Hakları Mahkemesi
AİHS : Avrupa İnsan Hakları Sözleşmesi
AÜEHFD : Atatürk Üniversitesi (Erzincan) Hukuk Fakültesi Dergisi
AÜHFD : Ankara Üniversitesi Hukuk Fakültesi Dergisi
AÜSBF : Ankara Üniversitesi Siyasal Bilgiler Fakültesi
AÜSBFD : Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi
AYM : Anayasa Mahkemesi
AYMK : Anayasa Mahkemesi Kararı
B. : Bölüm
BM : Birleşmiş Milletler
bas.no. : Başvuru no
BEHK : Bilgi Edinme Hakkı Kanunu
BK : Borçlar Kanunu
Bkz. : Bakınız
C. : Cilt
CCTV : Close Circuit Television (Kapalı Devre Televizyon)
CMK : Ceza Muhakemesi Kanunu
Çev. : Çeviren
DEÜHFD : Dokuz Eylül Üniversitesi Hukuk Fakultesi Dergisi
E. : Esas sayısı
ECJ : European Court of Justice (Avrupa Adalet Divanı)
EHK : Elektronik Haberleşme Kanunu
ETDK : Elektronik Ticaretin Düzenlenmesi Hakkında Kanun
HD : Hukuk Dairesi
İHEB : İnsan Hakları Evrensel Beyannamesi

İÜHFM : İstanbul Üniversitesi Hukuk Fakültesi Mecmuası

K. : Karar sayısı

k.t. : Karar tarihi

KVKK : Kişisel Verilerin Korunması Kanunu

m. : Madde

MERNİS : Merkezi Nüfus İdaresi Sistemi

MK : Medeni Kanun

MÜHF : Marmara Üniversitesi Hukuku Fakültesi Dergisi

N.Y.U. L. Rev. : New York University Law Review

no. : Numara

OECD : Organisation for Economic Co-operation and Development (Ekonomik İşbirliği ve Kalkınma Teşkilatı)

RG. : Resmî Gazete

s. : Sayfa

S. : Sayı

T. : Tarih

TBB : Türkiye Barolar Birliği

TBBD : Türkiye Barolar Birliği Dergisi

TCK : Türk Ceza Kanunu

TDK : Türk Dil Kurumu

TMK : Türk Medeni Kanunu

TTK : Türk Ticaret Kanunu

vb. : Ve benzeri

vd. : Ve devamı

Y. : Yıl

yy. : Yüz yıl

GDPR : Avrupa Birliği Veri Koruma Tüzüğü

AB Veri Koruma Yönergesi : 95/46/AT sayılı Yönerge

AK 108 sayılı Sözleşmesi : Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

1. GİRİŞ

Ülkemizde kişisel verilerin korunması hususunun önemi yeni yeni anlaşılmaya başlanmıştır. Kişisel verilerin korunması konusunu tartışmaya başladığımızda tartışmaların siyasal, sosyal, hukuksal ve teknik boyutlarda şekillendiğini görmekteyiz. Ülkemizde yeni sayılabilecek bu alan, gelişmiş dünya ülkelerinde uzun yıllar çok farklı boyutlardaki tartışmaların konusunu oluşturmuştur. Bu uzun süreç içerisinde kişisel verilerin korunmasını korunaklı hale getiren çeşitli düzenlemeler yapılmıştır. Diğer ülkelerde 1970'li yıllarda başlayan düzenlemeler, Türkiye'de 2005 yılında TCK'da KVK kapsamında yapılan ilgili özel düzenleme ile karşımıza çıkmaktadır. Türkiye'de kanun koyucu tarafından yapılan düzenlemelerde çeşitli hükümler yer alsa da kişisel verilerin korunmasını sağlayıcı normların Avrupa standartları ile uyumlu hale getirilmesi süreci devam etmektedir. Kişisel verilerin korunması, temel hak ve özgürlükler kapsamında yer aldığından kişilerin karşılaşabileceği ihlallere karşı elbette bir güvence sağlamaktadır. Bu bağlamda kişisel verileri koruma konusunda ciddi yol kat eden ülkeler ile ülkemizi karşılaştırdığımızda Anayasa seviyesinde *"insan haklarına saygılı, demokratik bir devlet"* bir koruma idealini ortaya koyması açısından elbette çok önemlidir.

Bu anlamda yapmış olduğum çalışmada özellikle üç sorunun yanıtını bulmaya çalıştım. Birinci bölümde kişisel verilerin korunmasının neden gerekli olduğu, kişisel verileri koruma hukuku ile anlatılmak istenen ve bu alana ilişkin tarihsel gelişim süreçleri, bunların yanı sıra "*kişisel veri*" mefhumunun uluslararası metinlerde kayda geçen düzenlemelerinin neler olduğu, uluslararası metinlerde kronolojik sıralamayı takip ederek kişisel veri hakkının nasıl doğduğu, ülkelerdeki teknolojik gelişmelerin söz konusu hakkın oluşmasında nasıl katkılar sunduğu ve bu anlamda kişisel verilerin korunmasına yönelik sağlanmış olan hukuki korumaların neler olduğu, uluslararası metinlerde kişisel verileri koruma hukukunun; amaç bakımından, ortaya konuluş şekli bakımından, metinlerin ayırt edici özellikleri ve prensipler bakımından neler içerdiği irdelenmeye çalışılmıştır.

Çalışmamızın ikinci bölümünde; kişisel verilerin korunması hukukunda bilinmesi gereken temel tanımların içeriği, kişisel verilerin korunması hakkının diğer temel hak ve

özgürlüklerle ilişkisi ve temel prensiplerinin neler olduğu soruları cevaplanmaya çalışılacaktır.

Çalışmamızın üçüncü bölümünde özellikle kişisel verilerin korunmasına ilişkin cezai ve idari yaptırımların neler olduğu ve bu bağlamda aydınlatma yükümlülüğünün yerine getirilmemesi halinde kabahat özelinde hangi esasların söz konusu olduğu soruları cevaplanacaktır.

Çalışmamızın dördüncü ve son bölümünde ise aydınlatma yükümlülüğünün yerine getirilmemesi kabahatinin konusunun ve yapısal unsurlarının neler olduğu, bunun yanı sıra aydınlatma yükümlülüğünün yerine getirilmemesi kabahati, korunan hukuki değer, maddi-manevi unsurlar, hukuka aykırılık unsuru ile kusurluluk, özel görünüş biçimlerinin neler olduğu, son olarak aydınlatma yükümlülüğünün yerine getirilmemesi durumunda yaptırım usulü ve zamanaşımı soruları cevaplanmaya çalışılacaktır. Bu sorulara ilişkin olarak çalışma içerisinde yeri geldikçe detaylı açıklamalar yapılacaktır. Ancak bu çalışmanın konusunu oluşturan kişisel verilerin korunmasının neden bu kadar önemli olduğu konusu üzerinde durmakta yarar olabileceğini düşünüyorum.

Bilginin tarihin hiçbir döneminde olmadığı kadar değerli hale geldiğini rahatlıkla ifade edebiliriz. Bu kadar önemli olmasından dolayı adeta devletlerin ekonomisinin yeni yakıtı haline geldiğini söyleyebiliriz. Dolayısıyla bu çağda bilgiyi elinde bulunduranların her anlamda güç kazandıklarını söyleyebiliriz.

Kişisel verilerden bahsederken, özellikle geleceğimizden bahsettiğimizin bilincinde olarak, bizi belirli kılan kimlik numaramız, ismimiz, soyadımız, eğitim bilgilerimiz, telefon numaramız, araç plakamız, beğenilerimiz hatta yaşam içerisindeki tercihlerimize kadar geniş bir çeşitliliğe sahip olan kişisel verilerimizin bulunduğunu anlamaktayız. Aslında burada dikkat edilmesi gereken, hangi verimizden bahsedersek bahsedelim sonuç itibariyle “biz” kavramının etrafında bir nitelemenin yapıldığı gerçeğidir. Dolayısıyla özellikle bu nedenle kişisel veriler oldukça önemlidir. Bu nedenle bizi belirli kılan verilerimiz üzerindeki hakimiyetimizi kaybettiğimiz durumlarda bireysel özerkliğimizi korumamız ve kişinin kendi olması olanaksız hale gelecektir. Kişisel verileri korunaksız hale gelen kişinin sürekli

izlenmesi, gözlemlenmesi ve davranışlarının yönlendirilmesi kaçınılmaz bir sondur. Dolayısıyla bu durumdaki bir kişinin elbette özgürlüğünden bahsedilemez. Her ne kadar her dönemde kişilerin başkalarının hayatlarını merak etme, bilgi toplama gibi davranışları olsa da "*kişisel verilerin korunması*" kavramı bakımından değerlendireceğimiz hukuksal gelişmelerin bütün dünyada yeni olduğunu ifade edebiliriz. Kişisel verilerin her geçen gün öneminin artması veya daha ciddi bir sorun olarak görülmesi elbette 1970'li yıllardan itibaren gelişen teknolojinin son derece büyük etkisi olmuştur. Bu bağlamda bilgisayarların ortaya çıkışı ile birlikte bilginin çok daha hızlı, kolay bir şekilde depolanması, işlenmesi, bu bilgilerin çok daha kısa sürelerde paylaşılabilmesi ve belki de kişisel veriler bakımından en önemlisi, depolanan bu verilerin ilişkilendirilebilir duruma gelmesi kişilerin özel yaşamlarında ciddi risklerin oluşmasına sebebiyet vermiştir. Bu anlamda 1970'li yıllardan itibaren gelişen teknoloji ile birlikte hayatımız tahmin edemeyeceğimiz büyüklükte bir dijital dönüşüme maruz kalmıştır. Hayatımızda gerçekleşen dijital dönüşümün hayatımızın her noktasına temas ettiği elbette inkâr edilemez ancak bu, bazen olumlu anlamda olmakta bazen de olumsuz durumlara sebebiyet vermektedir. Kişisel verilerin korunması yalnızca teknoloji bağlamında değerlendirilmemelidir. Hayatımızın olağan akışı içerisinde manuel olarak işlenen verilerimizin teknolojiden bağımsız olarak da korunma ihtiyacı bulunmaktadır. Bütün dünyada yaşanan teknolojik gelişmelerin kişisel veriler ile ilgili bir dönüşüm süreci başlattığını bilmekteyiz. Dönüşüm sürecinin bu seviyede olması kişilerin verilerinin korunmasının öneminin fark edilmesini sağlamıştır.

Bir taraftan bilgiye ulaşılması, depolanması, işlenmesi ve elde edilen bilginin özgürce akışından kaynaklanan menfaatlerimiz, diğer taraftan kişisel özerkliğin gerektirdiği bilgi üzerinde kişinin denetim hakkının süre gelen çatışma halinde olduğunu bilmekteyiz. Böyle çatışma durumlarında yapılması gereken mutlaka dengenin göz önünde bulundurulmasıdır. Kişisel verilerin konu olduğu alanlara baktığımızda özellikle devletlerin kendi vatandaşlarına yönelik planlama, yönetim ve özellikle güvenliğin sağlanması gibi sorumluluklarını yerine getirmek; kurum ve kuruluş paydaşlarına daha kaliteli hizmet sağlayabilmek, kar oranlarını arttırmak adına kişisel verilere ihtiyaç duyarlar. Bu gereksinimler karşısında kişisel verilerin korunması hakkı ise verilerin aktarılmasını tamamen ortadan kaldırmayı değil, kişisel verileri üzerinde hâkimiyetini kaybetmiş kişiye, kaybetmiş olduğu hakimiyeti yeniden vermeyi amaç edinmiştir. Dolayısıyla görüldüğü üzere

kişisel verilerin korunması bir denge olarak görülebilir. Gelişen teknoloji karşısında, kişisel hak ve özgürlüklerin zarar görebilme durumları değerlendirilip var olan terazinin uygun bir seviyede tutulması sağlanmaktadır.

Kişisel verilerin korunmasından bahsettiğimiz bütün metinlerde çoğu zaman teknolojinin hızlı değişiminden bahsetmekteyiz. Ancak şunu açık ve net olarak belirtmek zorundayız: Teknoloji, kişisel verileri kullanılan bireylerin düşmanı değildir. Teknolojinin hayatımızı her geçen gün kolaylaştırmasıyla birlikte hayatımızın bir parçası haline geldiğini de görmekteyiz. Dolayısıyla günlük yaşantımızla bu kadar iç içe geçmiş bir teknoloji dünyasından kendimizi soyutlamamız mümkün olmadığı gibi bu yaklaşımda ısrarcı olduğumuzda da yanlışlıklar söz konusu olacaktır. Kişisel verilerin korunması bağlamında teknolojinin getirdiği tehlikelerden kişiyi koruyabilmek için, var olan sorunlara karşı farkındalığı arttırmak, çözüm geliştirmek var olan düzenlemeleri birçok açıdan değerlendirmek önemli olacaktır. Gelişen teknolojinin bireylere sağladığı söz konusu kolaylıklar, kişisel verilerimizden ya da bireysel özerkliğimizden ödün vermemiz anlamına gelmemektedir.

Teknolojinin yükselen ivmesi ile birlikte bilginin her geçen gün büyük önem kazandığı muhakkaktır. Önemi artan bu bilgiyi kullanmak istiyorsak bilgilerimizin her alanda kullanılmasına izin vermemiz gerektiğini düşünebiliriz. Ancak böyle bir düşüncenin kişinin hakları bakımından hem gerekli olmadığı hem de yanlı olduğunu net olarak ifade edebiliriz. Hatta yukarıda bahsetmiş olduğumuz teknolojik gelişmelerden tam manasıyla faydalanabilmemiz için bireysel özgürlüklerimizi koruyabilmek oldukça önemlidir. Kişisel verilerin korunması konusu ile ilgili yapmış olduğum çalışmada asıl amacımız; gelişmiş devletlerde neredeyse elli yıldır tartışılan, bu alanda düzenlemeler yapılan ve gelişmiş olan devletlerin neredeyse tamamında güvence altına alınan kişisel verilerin korunmasına ilişkin açıklamalarda bulunmak, bu açıklamalar doğrultusunda Türkiye'deki güncel duruma ilişkin olarak değerlendirmede bulunmaktır. Bu anlamda konusu çok geniş olan bu çalışma kapsamında belirli sınırlamalar yapılarak işbu konu aktarılmaya çalışılacaktır.

2. BİRİNCİ BÖLÜM

KİŞİSEL VERİLERİN KORUNMASI İHTİYACININ ORTAYA ÇIKIŞI, TARİHSEL GELİŞİMİ, KİŞİSEL VERİLERİN KORUNMASI KAVRAMININ HUKUKİ NİTELİĞİ, ULUSLARARASI HUKUKTA KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN TEMEL METİNLER

2.1. KİŞİSEL VERİLERİN KORUNMASI İHTİYACININ ORTAYA ÇIKIŞI

Toplumların tarihsel süreçleri incelendiğinde bireylerin kendilerine ait olan verilerin, tüm zamanlarda çok değerli bir kavram olduğunu görmekteyiz. Bireylerin kişisel bilgilerine tarih boyunca toplum tarafından önem verilmiştir[1]. Toplum tarafından gösterilen bu ilginin nedeninin birçok farklı sebebi olsa da asıl neden bireye ait bilgilerin toplum tarafından bilinme arzusu olmuştur[2]. Bireyler kendileri veya yakınları hakkında belirli bilgileri paylaşabilmek için güven duymak isterler. Bu sebeple bireylere ait veriler ile gizlilik kavramlarının birbiriyle her anlamda ilişki içerisinde olduğunu net bir şekilde ifade edebiliriz. Nitekim tarihi Antik Yunan'a gidecek kadar eski olan, hasta-doktor mahremiyeti çerçevesinde hasta kişilere ait olan bilgilerin gizlilik içerisinde kalması bu bilgilerin asla üçüncü kişilere açıklanmaması temelini oluşturan Hipokrat yemini, gizlilik kavramı içerisinde şekillenmiş ve tarih boyunca güncelliğini koruyarak sır saklama yükümlülüğünün temelini oluşturmuştur. Bireyler tarafından merak edilen bilgiler aynı şekilde özel şirketler ve kuruluşlar tarafından da merak konusu olmuştur. Bu kuruluşlar ticari faaliyetlerini yürütebilmek ve muhatap oldukları bireylerin tercihlerini öğrenebilmek için özellikle bireyleri yönlendirebilmek adına veri toplamaya gereksinim duymuşlardır[3]. Çeşitli sektörlerden yola çıkarak sır saklama yükümlülüğünün bütün meslek grupları için söz konusu olabileceğini ifade edebiliriz. Sır saklama yükümlülüğünün nedeni paylaşılan bilgiler açısından gizliliğin sağlanarak güvenli ilişkilerin kurulmasını sağlamaktır. Özel

[1] Elif, Küzeci, Kişisel Verilerin Korunması, 3. Baskı, Ankara, Turhan Kitabevi, 2019, s. 17.
[2] Küzeci, a. g. e.
[3] Aydın Akgül, Kişisel Verilerin Korunması Açısından İdarenin Hukuki Sorumluluğu ve Yargısal Denetimi, Doktora Tezi, Kocaeli, 2013, s. 24.

kuruluşların ve kamu hizmetlerinin uygulanabilmesi ayrıca özellikle kamu hizmetlerinin sürekliliğini sağlayabilmek için bireylerin verilerine ihtiyaç duyulmuştur[4]. Bireylerin kişisel bilgilerine ihtiyaç duyan kamu ve özel sektörlerin talebine karşı, kişilerin kendilerine ait olan, özellikle gizli kalması ya da mutlaka kullanılması gereken kişisel bilgilerin kullanılırken bireylerden rıza alınma imkânı söz konusu olmalıdır[5].

Gerek dünyada gerek ülkemizde bireylerin kişisel verilerinin korunmasına dair yasal düzenlemelere gereksinim duyulmasının nedenlerine baktığımızda sayısal elektronik sistemlerinin gelişmesi ve bunun sonucunda bilgisayarların yaygınlaşması ile birlikte kişisel verilerimizin bu sistemlerde depolanması söz konusu olmuştur. Dolayısıyla aslında kişisel verilerin korunmasına duyulan ihtiyaç bir anlamda teknolojinin bütün topluma sirayet etmesine neden olmuştur. Bilgisayarların icadı ve teknolojik gelişmeler sonucunda verilerin depolandığı sanal veri bankaları oluşmaya başlamıştır. Tüm bu gelişmeler yaşanırken kişisel verilerimizin geçen zaman içerisinde çok daha değerli hale geldiği görülmektedir[6].

Günümüz teknoloji dünyasında bilgi ve veri toplumlar için güç anlamına gelmektedir[7]. Bireylerin bilgilerini bünyelerinde toplayan Linkedln, Instagram, Facebook, Google, Telegram, Whatsapp, Bip ve diğer sosyal medya uygulamaları her toplum için ekonomik, siyasi, güvenlik ve daha birçok alanda stratejik öneme sahiptir. Verinin stratejik öneme sahip olduğu ile ilgili olarak, Facebook – Cambridge Analytica veri skandalı olarak ifade edilen; yaklaşık 50 milyon bireyin Facebook profilinde bulunan kişisel verilerinin, rızaları olmadığı halde ekonomik ve siyasi amaçlarla kullanılarak, Amerika Birleşik Devlet'inde seçmenlerin iradelerini manipüle etmek gayesiyle sonuçlara nasıl etkide bulunduğu ifade edilmektedir[8]. Dolayısıyla yukarıda isimlerini zikrettiğimiz uygulamaların nasıl bir etki gücüne sahip olduğunu anlayabiliyoruz. Bu gücün kanuni düzenlemeler ile kontrol altında tutulmadığında nelere sebebiyet verebileceği net olarak görülmektedir.

---

[4] Oğuz Şimşek, Anayasa Hukukunda Kişisel Verilerin Korunması, İstanbul, Beta Yayınları, 2008, s. 3; Akgül, a. g. e., s. 25, 115.
[5] Akgül, a. g. e., s.25,115.
[6] Mesut Serdar, Çekin, Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku, 2. Baskı, On İki Levha Yayıncılık, İstanbul 2019, s. 5.
[7] Akgül, a. g. e., s. 24.
[8] (Çevrimiçi), https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election , (Erişim Tarihi: 01/03/2022)

Günümüzde yapay zekanın ve teknolojideki hızlı gelişmelerin sonucunda kişisel verilerin toplanıp işlenmesi ile ilgili imkanlar artmıştır. Yapay zekâ ve teknolojinin hızla gelişmesi kişisel verilerin her alanda kullanılması neticesinde kişisel verilerin işlenmesine ilişkin olanaklar artmıştır. Kişisel verilerin işlenmesi ile ilgili, gelişen her teknoloji bu verilerin farklı bir boyutta işlenmesine olanak tanımıştır[9]. Yapay zekâ teknolojisinin gelişmesiyle kişisel verilerin toplanması, depolanması ve birbiriyle anlamlı bir bütün olarak ilişkilendirilmesi çok daha kolay ve ekonomik hale gelmiştir[10]. Bahsettiğimiz teknolojiler sayesinde bireylerin temel hak ve özgürlüklerinin sınırlandırılması hukuk düzeni bakımından gerçekçi bir yaklaşım olmayacaktır[11]. Dolayısıyla bireyin temel hak ve özgürlüklerini hiçbir endişe duymadan kullanabilmesi ve geliştirebilmesi, kişisel verilerinin hukuk düzeninde korunmasına bağlıdır[12].

Kanun koyucunun bu gelişmeler karşısında kişilerin verilerini güvende olmasını sağlayacak ve kendilerinin güvende olduklarını hissettirecek çalışmalar yapması kaçınılmazdır. İktisadi İş birliği ve Gelişme Teşkilatı ve Birleşmiş Milletler gibi kuruluşlar kişisel verilerin korunması ile ilgili çeşitli kararlar almışlardır. Bunun yanında Avrupa Birliği ülkelerinde kişisel verilerin korunması ile ilgili yeterli olmasa da çeşitli düzenlemelerin yapıldığı görülmektedir. Bahsettiğimiz ülkeler gibi Türkiye de kişisel verilerin korunması ile ilgili çeşitli düzenlemeler yapmıştır. Ancak bu düzenlemeler diğer ülkelere kıyasen çok daha sonra yapılabilmiştir. 2010 yılı Anayasa değişikliği ile bireylerin kişisel verilerinin korunmasını talep hakkı kanun koyucu tarafından düzenlenmiştir. Anayasa da yapılan bu değişiklikten sonra 2016 yılında ise 6698 sayılı Kişisel Verilerin Korunması Kanunu yürürlüğe girmiştir.

Kişisel verilerin korunması ile ilgili kanun koyucunun amacı, bireylerin kişisel veri niteliğindeki her türlü bilgilerinin toplanması, depolanması, işlenmesi, aktarılması ve silinmesi gibi işlemlerinin nasıl yapılacağı ve bu işlemler yapılırken amacın önceden belirlenip hangi araçlarla yapılması gerektiğinin seçilmesi amaçlanmaktadır. En önemlisi bu

[9] Küzeci, a. g. e., s. 28.
[10] Küzeci, a. g. e., s. 29; Şimşek, a. g. e., s. 3.
[11] Nilgün Başalp, Kişisel Verilerin Korunması ve Saklanması, Ankara, Yetkin Yayınları, 2004, s. 23.
[12] Şimşek, a. g. e., s. 3.

işlemler yapılırken öncelikle ihlalin önlenmesi veya bir ihlal söz konusu olmuş ise hangi kanuni düzenlemelerin yapılması gerektiğini amaç edinmiştir[13]. Bireylerin kişisel verilerinin bahse konu kanuna aykırı olarak işlenmesi durumunda kişiler ciddi hak kayıpları yaşayacaklardır[14] (6698 sayılı Kanun m. 11/1-ğ).

2.2. TARİHSEL GELİŞİMİ

Kişisel verilerin korunmasına ilişkin dünyadaki ilk kanuni düzenleme, 30 Eylül 1970 tarihinde Almanya'nın Hessen eyaletinde oluşturulmuştur[15]. Yıllar içinde diğer eyaletler de Hessen'de yapılan düzenlemeyi takip etmiş ve Almanya'da kişisel verilerin korunmasına ilişkin federal anlamda ilk yapılan düzenleme olan Federal Almanya Veri Koruma Kanunu[16], 1 Ocak 1978 tarihinde yürürlüğe girmiştir[17]. Bu alanda ülke çapında yapılan ilk kanun ise, 1973 yılında İsveç'te çıkarılmıştır. Veri koruma hukukunun ortaya çıktığı yer Avrupa olsa da Amerika'da bu alanda yaşanan gelişmelere kayıtsız kalmamış; 1974 yılında özel hayatın korunmasına yönelik olarak Özel Yaşamın Gizliliği Yasası[18] çıkarılmıştır, ancak Amerika'da günümüzde dahi Avrupa'daki gibi oturmuş bir veri koruma hukuku anlayışının oluştuğu söylenemez. Nitekim Amerika'da bireyin özel hayatının gizliliği ve mahremiyet kavramlarından çok, verinin ekonomik boyutuna önem verildiği söylenebilir.

Teknoloji ilerledikçe, gizlilik ile ilgili yasal sorunlar ortaya çıkıyor. Bu durum bireylerin kişisel bilgilerini gizli tutmayı istediği fikrini güçlendirmektedir. Kişisel verilerin otomatik olarak işlenmesi, bu konunun önemini her zamankinden daha fazla ortaya koymaktadır.

---

[13] Akgül, a. g. e., s. 119.
[14] Aksoy, Hüseyin Can, Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması, Ankara 2010, s. 19.
[15] (Çevrimiçi) https://datenschutz.hessen.de/ueber-uns/geschichte-des-datenschutzes , (Erişim Tarihi: 01/03/2022).
[16] (Çevrimiçi) Rudolf, Schomerus, Bundesdatenschutzgesetz Kommentar, Beck, Almanya, 2007, s. 77. http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl177007.pdf, (Erişim Tarihi: 01/03/2022).
[17] Vondem Bussche, Axel Freiherr/ Voigt, Paul, Data Protection in Germany, 2nd Edition, Almanya 2017, s. 1.
[18] Henderson, Harry, Privacy in the Information Age, Revised Edition, ABD 2006, s. 273-275.

Kişisel bilgilerin güvenlik sistemleri ile korunması sorunu diğer sektörlerde de dile getirilmektedir[19].

Milattan önce 5. yüzyılda ortaya çıkan Hipokrat Yemini hala geçerlidir ve doktorlar elde ettikleri verileri saklamak ve gizli bilgilerini açan hastaların bilgilerini açıklamamakla yükümlüdür. Bu yükümlülüğün amaçlarından biri de bireylerin toplumda zarar görmesini önlemektir.

Kişisel verilerin korunması ile ilgili düzenlemeler yapan tüm devletler, sanayi devriminin de bir ürünü olan sosyal devlet ilkesini hayata geçirebilmek için, kamu hizmetlerinin sağlıklı, hızlı ve güvenli sunabilmek için bireylerin kişisel verilerine ihtiyaç duymaktadırlar[20]. Devletler politikalarını belirlerken depoladıkları bu verileri işleyerek ülkenin yönetim, güvenlik, ekonomik ve planlama faaliyetlerini çok daha verimli bir hale getirmişlerdir[21]. Politika belirleme faaliyetlere örnek olması bakımından devletlerin iktisadi ve ekonomik politikalarının belirlenmesi için belirli çalışmaların yapılarak önceden bütün paydaşlara dair hesaplamaların yapılması gerekir[22]. Bu anlamda yukarıda bahsettiğimiz politikaların oluşturulmasında kişisel veriler, planlama ve yönetim organizasyonlarında bireylerin ihtiyaçlarını belirleme konusunda yol gösterici olmaktadır.

Yaşadığımız teknoloji dünyasında bilgiye ulaşmak her birey için oldukça kolay hale gelmiştir[23]. Ancak zamanla bilgiye ulaşım sürecinde bireylerin kendi kişisel verilerini ne ölçüde koruyabileceklerine ilişkin yeterli hukuki korumanın bulunmadığı hususu gün yüzüne çıkmıştır. Zira bilgi güvenliği konusu, bilginin internet aracılığıyla dünyanın her yerine ulaşır nitelikte olmasından dolayı ulusal bir konu olmaktan çıkmış uluslararası bir konu haline gelmiştir. Böylece bilgilere erişimin kolaylaşmasıyla kişilerin menfaatlerinin

---

[19] Yasemin, Avcı, Kişisel Verilerin Korunması, Yüksek Lisans Tezi, Konya 2019, s. 13; Şehriban İpek Aşıkoğlu, Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri**,** 1. Baskı, İstanbul, On İki Levha Yayıncılık, 2018, s. 11.

[20] (Çevrimiçi), https://edpb.europa.eu/about-edpb/more-about-edpb/article-29-working-party_en, Consept of Personal Data, s. 11, (Erişim Tarihi: 01/03/2022).

[21] Cemil, Kaya, Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi, İÜHFM, Y: 2011, C: 69, S: 1-2, s. 318.

[22] Kaya, a. g. e., s. 322.

[23] A. g. e., s. 323, Carey, Peter, Data Protection A Practical Guide to UK And EU Law, 5. Baskı, Oxford University Press, İngiltere 2018.; Küzeci, a. g. e., s. 244.

zedelenmesi söz konusu olmuş ve maddi ve manevi zararlar oluşmaya başlamıştır. Bu sebeple hem devletler kendi iç hukuklarında çeşitli düzenlemelere yer vermeye başlamış hem de uluslararası kuruluşlar bu konuda çalışmalara başlamıştır[24]. Bu bakımdan dünya kamuoyunda çokça konuşulan Facebook-Cambridge Analytica Skandalı olarak ifade edilen ve kişilerin Facebook kullanıcı verilerinin çeşitli uygulamalar kullanılarak sızdırılmasıyla başlayan süreç, sadece siyasetin değil teknolojik imkanların sınırlarını da tartışır hale getirmiştir.

Sosyal medyada hesapları bulunan bireylere kişiselleştirilmiş içerikler göndermeyi amaçlayan Cambridge Analytica "*dünyayı alt üst eden veri kampanyası*" ile dünya kamuoyunda birçok ülkenin siyasal seçimlerine doğrudan etkide bulunulmuştur. Bu bakımdan ülkelerin kamuoyunda oluşturduğu etki itibariyle Amerika Birleşik Devletleri'nde 2016 yılında gerçekleştirilen başkanlık seçimlerinin özellikle dikkat çektiğini ifade edebiliriz. Cambridge Üniversitesi'nde doktora eğitimi sürdüren Michal Kosinski ve David Stillwel'in "*büyük beşli"* olarak ifade edilen davranış teorisini Facebook hesapları bulunan kullanıcılar üzerinde yapılan denemelerle start verilen süreç birçok alana yayılmıştır. Bu alanların başında gelen siyaset ve teknoloji dünyasından birçok önemli kişiyi öne çıkarırken, verinin ne denli önemli bir araç olduğunun da anlaşılmasına sebep olmuştur.

Amerika Birleşik Devlet'inde 2016 yılında yapılan seçimlerin sonucunda Donald Trump'ı başkanlığa taşıyan siyasal sürecin seçim kampanyasını organize eden Cambridge Analytica, Facebook kullanıcı verilerini kişilerin ve şirketin herhangi bir izni olmadan kullanmakla suçlanmıştır. Facebook şirketinin kullanıcı verilerini üçüncü taraf uygulamaların sızdırmasına elverişli şekilde muhafaza edilmesiyle eleştirildiği süreç, Cambridge Analytica şirketinin iflasını ilan edip şirketin kapısına kilit vurulmasıyla sonuçlanmıştır. Diğer taraftan Facebook şirketinin kurucusu ve CEO'su Zuckerberg bu olay nedeniyle, ABD Kongresi'nde ifade vermek zorunda kalmıştır.

Cambridge Analytica'nın özellikle Donald Trump'ın Amerika Birleşik Devleti'nin Başkanlık seçim yarışını kazandığı süreç ile İngiltere'nin Avrupa Birliği'nden ayrılmasının

[24] Sadullah, Çelik, Büyük Veri Teknolojilerinin İşletmeler İçin Önemi, Social Sciences Studies Journal, C: 2, S: 6, s. 873.

referanduma taşındığı Brexit döneminde yaptığı katkılar ve oynadığı rol tartışılmaya ve sorgulanmaya devam edilmektedir. Bu süreç içerisinde şirkete karşı ABD ve İngiltere'de açılmış olan davalar bulunmaktadır. Cambridge Analytica'da çalışan Kanadalı veri danışmanı olan Wyli'ın, "*Facebook beğenileri kullanıcılar hakkında ne kadar bilgi verir?*" seviyesindeki çalışmalarını, ülkelerin siyasal kaderlerini belirleyecek düzeyde veri algoritmasına dönüştürmüştür. Cambridge Analytica şirketi yaklaşık 270 bin kullanıcının verilerini 1 milyar dolar karşılığında elde etmiş ve elde ettiği bu verilerden 32 farklı "*kişilik tipi*" elde etmiştir[25].

2018 yılında İngiliz yayın kuruluşu olan Channel 4 haber kanalı tarafından yürütülen gizli bir araştırma neticesinde, ABD başkanı Trump'ın 2016 yılındaki seçim kampanyasında veri analiz firması olarak faaliyet gösteren İngiltere merkezli Cambridge Analytica şirketi tarafından veri ihlali gerçekleştirildiği ve söz konusu ihlal neticesinde 87 milyona yakın ABD vatandaşının etkilendiği ortaya çıkarılmıştır[26]. Söz konusu bu araştırmada Facebook sosyal medya platformunda yer alan anket temelli kişilik testi uygulamasıyla Amerika Birleşik Devleti'nde bulunan yetişkinlerden elde edilen kişisel veriler ile bu kişilerin karakter özellikleri, siyasi düşüncesi ve yaşam tarzları analiz edilmek suretiyle[27] seçmen profili oluşturulmuştur. Bu yönde bir profilin oluşturulmasıyla karşıt görüşlü olan seçmenlerin oy rengini değiştirecek, kendi taraftarlarına ise seçimlerini pekiştirecek içerikte seçmenlerin karakter özelliklerine uygun özel dijital video içerikleri üretildiği ve sonuç itibariyle yapılan seçim kampanyasının bu biçimde kazanıldığı ifade edilmiştir.

Facebook-Cambridge Analytica şirket ortaklığında patlak veren veri sızıntısı olayının ardından Facebook ve Cambridge Analytica şirketleri için oldukça zorlu bir süreç başlamış oldu. Facebook kurucusu ve CEO'u Mark Zuckerberg, ABD Senatosu'nun düzenlediği

[25] Jo-Ida C. Hansen, Cross-Cultural Research on Vocational Interests , (Çevrimiçi), https://www.tandfonline.com/doi/abs/10.1080/07481756.1987.12022837 , (Erişim Tarihi: 04/03/2022).
[26] (Çevrimiçi), https://www.dw.com/tr/facebook-87-milyon-kullan%C4%B1c%C4%B1-etkilendi/a-43258048 , (Erişim Tarihi: 04/03/2022).
[27] Veri Madencisi Michal Kosinski adlı araştırmacı (Çevrimiçi), https://www.researchgate.net/profile/Ahmet-Oezker/publication/330703883_Financial_Performance_Objective_of_Public_Expenditures_in_Last_Period_and_Its_in_Connected_with_Economic_Budget_in_Turkey/links/5c503e9192851c22a3989c81/Financial-Performance-Objective-of-Public-Expenditures-in-Last-Period-and-Its-in-Connected-with-Economic-Budget-in-Turkey.pdf#page=16 , (Erişim Tarihi: 04/03/2022).

"*Facebook, Sosyal Medya Gizliliği ve Veri Kullanımı ve Suistimali*" isimli oturumda ABD Senatosunda ifade vermiştir. Yaşanan olayla ilgili şirketi ve kendisine yönelik eleştiriler yöneltilen Zuckerberg, veri sızıntısını önlenmesine ilişkin olarak Facebook'un yeterli çaba sarf etmediğini ve şirketin yarattığı araçların zarar verici biçimde kullanıldığına, bu zararların arasında da nefret konuşmalarının artması, sahte haber içeriklerinin ve kritik seçimlere yabancı müdahalesi gibi unsurların yer aldığını ifade etmiştir[28].

Cambridge Analytica skandalında ifade veren Zuckerberg insanların kişisel veri ve bilgilerini korumakta başarısız olduklarını itiraf edip, "*Bu büyük bir hataydı. Benim hatamdı ve özür dilerim*" itirafında bulunmuştur. Zuckerberg, sosyal paylaşım sitesinde yaşanan veri skandalından hemen sonra büyük verilere erişimi olan bütün uygulamaları inceleyip soruşturma başlattığını dile getirmiştir.

Facebook'un kurucusu Mark Zuckerberg, kullanıcılara ait bilgilerin izinsiz paylaşılmasıyla ilgili olarak Amerika Birleşik Devletleri Kongresi'ne ifade vermiştir. Bu ifade esnasında veri sızıntısıyla ilgili soruları yanıtlayan Mark Zuckerberg, veri skandalını kabul eden itiraflarına şunu da eklemiştir; "*Cambridge Analytica 2015'te verileri sildiğini söylediğinde, bu durumu kapanmış sandık. Ama onların sözüne güvenmemeliydik. Bu yüzden Federal Ticaret Komisyonuna bu konuda haber vermedik*" şeklinde beyanda bulunmuştur. Senatör Whip Durbin, sorularının devamında Zuckerberg'e; "*dün gece kaldığınız otelin adını bizimle paylaşır mısınız*?" sorusunu yöneltti. Zuckerberg'in gülerek "*hayır*" cevabını vermesinin ardından Senatör Durbin "*geçen hafta kimlere mesaj attığınızı söyleyebilir misiniz*?" sorusunu yöneltti. Zuckerberg'in "*hayır*" yanıtını vermesi üzerine Senatör Durbin, "*Sanırım her şey bundan ibaret, gizlilik hakkınız*." ifadelerini kullanmıştır[29]. Facebook- Cambridge Analytica skandalı hakkındaki kararını veren ABD Senatosu, kullanıcılara ait verileri izinsiz ve usulsüz kullandığı gerekçesiyle Facebook'a 5 milyar dolar tutarında rekor bir ceza kesti. Bu ceza aynı zamanda 2012'de Google için kesilen 22 milyon dolarlık ceza sonrası, bir teknoloji firmasına verilen en yüksek miktardaki para cezası olarak tarihe geçmiştir[30].

---

[28] (Çevrimiçi), https://www.ntv.com.tr/galeri/teknoloji/facebook-skandalinin-merkezinde-yer-alan-cambridge-analytica-sirketi-kapanacagini,gHYfdIZ7rkmn2NcnJW9q7A , (Erişim Tarihi: 04/03/2022).

[29] (Çevrimiçi), https://www.aa.com.tr/tr/dunya/facebookun-ust-yoneticisi-zuckerberg-abd-senatosunda-ifade-verdi/1114367 , (Erişim Tarihi: 04/03/2022).

[30] (Çevrimiçi), https://haber.sol.org.tr/dunyadan/google-225-milyon-dolar-ceza-odeyecek-haberi-56851 , (Erişim Tarihi: 01/03/2022).

Facebook-Cambridge Analytica skandalı bize şunu göstermiştir ki, bazı kötü aktörler popülist otoriteler adına kişilerin verilerini sömürürken, Facebook sosyal medya platformunun gizliliği ve kontrol edilebilmesi konusunda oldukça yetersiz kaldığı anlaşılmıştır[31].

Modern anlamda kişisel verilerin korunmasının gündeme gelişi ilk olarak Amerika Birleşik Devletleri'nde 20. yüzyılın ortalarını bulmuştur[32]. ABD'de 1960'lı yıllarda kişilerin kredi verilebilirliği önemli bir konuydu. Kişilerin kredi verilebilir olup olmadıkları konusunda bilgisayarın hata yapması sonucu ülke çapında bütün vatandaşların verilerinin bir merkezde kayıt altına alınması hususu önerilmişti. Yaşanan bu sürecin ardından bireyin özel yaşamının korunmasına ilişkin tartışmalar gündeme gelmiştir. Takip eden dönemde, diğer gelişmelerle birlikte özel yaşamın güvence altına alınması maksadıyla 1974 tarihli "*Özel Yaşamı Koruma Kanunu"*[33] kabul edilmiştir. Bu anlamda önerilerden biri olan merkezi veri bankalarının kurulması önerisi, vatandaşların özel alanlarının ihlal edilmesi olasılığı karşısında kabul edilmemiştir[34]. Orwell'dan bu yana gelişen kitle iletişim araçlarının kullanımının birey üzerindeki kontrol korkusu kişisel verilerin korunması hukukunun gelişimini sağlamıştır[35].

Günümüz dünyasında hem devlet kurumları hem de özel kuruluşlar, bünyelerinde topladıkları veriler vasıtasıyla kişilerin çeşitli bilgilerine ulaşmaları çok kolay olabilmektedir. Kurum ve kuruluşlarda depolanan veriler, teknoloji alanında yaşanan hızlı gelişmelerin etkisiyle, kolaylıkla birçok amaçla kullanılabilmektedir. Toplanan veriler arasında özellikle kişisel verilerin bulunması nedeniyle, bu verilerin korunması gerekliliğini tartışmaya açmıştır[36].

---

[31] (Çevrimiçi), https://www.newyorker.com/books/double-take/sunday-reading-the-world-of-adrian-chen , (Erişim Tarihi: 04/03/2022).

[32] Cenk, Derinözlü**,** Büyük Veri ve Mahremiyet, TÜBİTAK 1.Ulusal Bulut Bilişim ve Büyük Veri Sempozyumu B3S17 Sempozyumu Bildiri Kitabı, 2017, s. 1; Necmi, Gürsakal, Büyük Veri, Genişletilmiş 3. Baskı, Dora Yayıncılık, Bursa 2017, s. 7.

[33] Derinözlü**,** a. g. e., s. 1; Gürsakal, a. g. e., s. 7.

[34](Çevrimiçi),https://www.forbes.com/sites/matthewherper/2015/02/17/how-pfizer-is-using-big-data-to-power-patient-care/#60a23635ceb4, (Erişim Tarihi: 01/03/2022).

[35] (Çevrimiçi), https://finland.fi/business-innovation/medicine-world-needs-great-data-finlands-got/, Erişim Tarihi: 01/03/2022).

[36] Ender Ethem, Atay, Hukuk Başlangıcı, 1.Baskı, Ankara, 2013, s. 123.

2.3. GENEL ANLAMDA KİŞİSEL VERİLERİN KORUNMASI HUKUKU

Bireye ait kişisel verilerin toplanması, muhafaza edilmesi, işlenmesi ve belirli ihtiyaçlar için kullanmak maksadıyla yapılacak olan işlem ve eylemlere ait yöntem ve esasların belirlenmesi, kişisel verilerin korunması hukukunun esas amacını oluşturmaktadır. Kişisel verilerin korunması yasasının, bireyin her alanda etkileşimi düşünüldüğünde birçok hukuk dalı ile iç içe girmiş olduğunu rahatlıkla ifade edebiliriz. Toplumsal yaşamı ve bu yaşamdaki insan ilişkileriyle davranışlarını düzenleyen ve devlet yaptırımıyla güçlendirilmiş bulunan kurallar bütünü olarak ifade edilen hukukun, sınıflandırılması söz konusu olduğunda, kamu hukuku ve özel hukuk olarak ayrılması, Roma Hukukunun oluşmasından bu yana kabul edilen sınıflandırma yöntemi olarak kabul görmüştür[37]. Ancak zaman içerisinde teknoloji alanında yaşanılan gelişmelere paralel olarak, toplumsal yapının ve devlet yapılanmalarının değişmesi, özellikle teknolojik gelişmeler olarak ifade edilen sayısal sitemler, dijital, bilişim, yazılım konularındaki ilerlemeler ile birlikte bilgisayar teknolojisinde yaşanan hızlı değişimler dikkate alındığında hukuki olarak artık bu ayrımın yeterli olmadığı bu alandaki tartışmalarda sıklıkla dile getirilmektedir. Yapılan ayrımların yeterli olmadığını öne süren yazarların görüşleri baz alındığında, özellikle bazı yazarların, kamu hukuku ve özel hukuk özelliklerini içerisinde barındıran karma hukuk olarak ifade edilen yeni bir alanı yapılan ayrıma ilave ettikleri görülmektedir[38].

Kişisel verileri koruma hakkı, 1982 Anayasasının orijinal halinde olmaması ile birlikte daha sonra 13/05/2010 tarih ve 27580 sayılı Resmî Gazete'de yayımlanarak 1982 Anayasasının 20. maddesinde, temel haklar kısmının, kişi hakları bölümünde düzenlenmiştir. Bu düzenlemenin bir gereği olarak kamu hukuku öznesi gibi görünse bile kişiler hukuku ile olan bağlantısı dikkate alındığında hem medeni hukuktan hem de özel hukuktan izler taşıdığı görülmektedir. Kanun koyucu tarafından yapılan bu düzenlemenin hem anayasal bir kamu hakkı olarak Anayasaya eklenmesi, hem de TCK ile bu hakka uygun hareket edilmemesinin belirli yaptırımlara bağlanması, bunun yanında, 6698 sayılı yasa ile kurulan "*Kişisel Verilerin Korunması Kurumu*" nun kamu gücünü kullanan bağımsız idari otorite şeklinde

[37] Şeref, Gözübüyük, Hukuka Giriş ve Hukukun Temel Kaynakları, 35. Baskı, Ankara, 2013, s. 23.
[38] Atay, a. g. e., s. 123.

örgütlenmesi gibi nedenler dikkate alınıp değerlendirildiğinde, bireyin verilerini koruyan yasal düzenlemenin kamu hukuku alanıyla daha fazla ilgisinin bulunduğunun söylenebileceği kanaatindeyiz[39].

Kamu gücünü bünyesinde barındıran devletlerin vatandaşları ile olan münasebetlerinin yanında devlet organlarının kendi aralarında olan münasebetlerini düzenleyen hukuk dalı, kamu hukuku olarak ifade edilmektedir. Kamu hukuku, özel hukuk veya karma hukuk ayrımını ortaya koymak için görüşleri incelediğimizde: "*çıkar teorisi"* ne göre söz konusu uyuşmazlık kamu ile ilgili ise; "*alt-üst ilişkisi*" görüşüne göre taraflardan biri devletin gücünü kullanıyor ise; "*özel hukuk*" görüşüne göre, ilgili düzenleme sınırlı olarak devlet otoritesine sorumluluk ve yetkiler yüklüyor ise, bu şartlarda kamu hukukunun varlığından bahsedildiği görülmektedir[40]. Tüm bu teori ve incelemeler ışığında, kişisel verileri koruma hukukunun kamu hukuku alanında incelenmesi gerektiği kanaatindeyiz. Kanaatimizin bu yönde oluşmasının temel nedenlerine baktığımızda; kişisel verilerin korunması hakkının anayasanın temel haklar kısmında düzenlenmesi, temel ceza yasalarında yapılan düzenlemelerde görüleceği üzere devlet veya başka kişilerce bu hakka müdahalelerin olması durumunda devlet adına yaptırımların uygulanması düşüncemizin bu yönde oluşmasına katkı sağlamıştır.

Anayasa hukuku bakımından, sosyal devlet olmanın yüklediği sorumluluk gereğince güvenliğin sağlanması ve kamu otoritesinin yönetime ilişkin karar alabilmesinin gereği olarak, devletler, kendi vatandaşının ayırt edici kişisel verilerini elde edip, bunları ihtiyacı doğrultusunda derleme ve sınıflandırabilmektedir.

Bahsetmiş olduğumuz hususlar, anayasa hukuku açısından, kişilerin verilerinin korunmasının anayasal hak olarak tanınmasındaki düzenlemenin de temelini oluşturduğu görülmektedir[41]. Tüm bu düzenlemeler bağlamında Anayasa'da tanımlanan bir hukuk devletinden bahsedilebilmemiz için, bireylerin kişisel bilgilerinin toplanması ve kullanılması gibi konularda hukuki öngörülebilirliğe mutlaka sahip olmaları gerekmektedir.

---

[39] Furkan Güven, Taştan, Türk Sözleşme Hukukunda Kişisel Verilerin Korunması, 1. Baskı, İstanbul, 2017, s. 8.
[40] (Çevrimiçi), https://www.turkcebilgi.com/kamu_hukuku, (Erişim tarihi 01/03/2022).
[41] Şimşek, a. g. e., s. 4.

Anayasa'da düzenlenen bu temel ilkenin sonucu olarak yürürlükte bulunan 1982 Anayasası'nda kişilerin verilerinin korunmasını isteme hakkı, temel kişi hak ve hürriyetleri kapsamında değerlendirilmiştir.

Günümüzde kişisel veriler devlet tüzel kişisi, kamu tüzel kişileri, özel hukuk tüzel kişileri ve gerçek kişiler tarafından ihtiyaçlarına uygun olarak işlem görmektedir. Bu bakımdan kişisel verilerin korunması konusu tartışmalarda alan kazandığı görülmektedir. Bireylerin verilerine erişim konusu ve kötüye kullanılması ile ilgili endişeler, hayatımızın her alanında olan internet, sosyal medya hesapları ve bunların yanında verilerin depolanmasındaki yazılımsal kolaylıklar ile arttığı görülmektedir. Bu bağlamda alanda yaşanan gelişmeler güvenlik politikaları ile desteklenmediği sürece vatandaşların endişelerinin artacağı kanaatindeyiz.

Bireylere ait kişisel verilerin teknolojinin gelişmesi ve dinamik yazılımlar ile otomatize edilmiş sistemler kullanılmaya başlanması ile birlikte verilere ulaşmadaki kolaylığın artması göz önüne alındığında, devlet kamu tüzel kişisi, kamu tüzel kişileri ve gerçek kişilerin bu verilerin kullanılması noktasında hukuki sınırlandırmaların yapılması son derece önemli hale gelecektir.

Bütün dünyada olduğu gibi bizim ülkemizde de dijital ortamda yapılan işlem sayısı her geçen gün artmakta ve vatandaşların verilerinin korunması ile ilgili alınacak önlemlere ilişkin yasal düzenlemelerin yapılma zorunluluğu bulunmaktadır. Bu anlamda, kişisel verilerin korunmasını geniş anlamda ele aldığımızda, asıl amacın salt verinin korunmasını sağlamak değil, bu verinin korunmaması neticesinde doğabilecek temel hak ve özgürlük ihlallerini engellemeye çalışmak olduğunu söyleyebiliriz[42].

Kişisel verilerin korunması hukukunun dar ve geniş anlamda değerlendirmeleri göz önüne alındığında, bireyin kişisel verilerinin korunması talebi ve talebin kamu otoritesi tarafından korunması, hukuki güvenliğe sahip toplumların var olmasında önemli olduğu kanaatindeyiz. Kişisel verilerin korunması ile ilgili kanun koyucu tarafından yapılan düzenlemelerin hem ulusal boyutta hem de uluslararası boyutta ifade özgürlüğü, özel hayat, devletlerin aralarında

[42] Şimşek, a. g. e., s. 3.

yaptığı ticari faaliyetler ve en önemlisi kamu düzeni ile ilişkili olarak her geçen gün önemi artmaktadır[43]. Bireylerin verilerini korumaya yönelik düzenlemeler; müşteri, vatandaş ve çalışan bağı kamu otoritesine bağlı olan bireylerin verilerinin toplanması, depolanması, aktarılması, kısıtlanması, kullanımı ve sınırlandırılması ile ilgili düzenlemelerin uygulanmasını hedeflemektedir[44].

Kişisel veri koruma hukukunda dünyadaki yaklaşımları incelediğimizde "108 sayılı Sözleşme", "95/46/AT sayılı Yönerge", "2016/ 679/ AT sayılı Genel Veri Koruma Tüzüğü"nün, çeşitli Avrupa Birliği ülkelerindeki hukuki düzenlemelerini dikkate alarak tüzel kişiden daha çok, gerçek kişiyi koruduğunu söyleyebiliriz. Bununla birlikte tüm dünyada gerçek kişilerin korunmasının yanında tüzel kişilerin daha çok korunması gerektiğine dair tartışmalarında olduğu görülmektedir. Bu tartışmaların sonucunda özellikle İtalya ve Lüksemburg gibi ülkelerin iç hukuk düzenlemelerinde, talepler doğrultusunda tüzel kişiliklerin korunması ile ilgili adımlar attıkları görülmektedir[45]. Ülkemizin bahse konu tartışmalar ile ilgili düzenlemeleri incelendiğinde ise gerçek kişilerin yasal ve anayasal çerçevede korunduğunu görmek mümkün olacaktır.

2.4. ULUSLARARASI HUKUKTA KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN TEMEL METİNLER

2.4.1 Birleşmiş Milletler

Birleşmiş milletler, İkinci Dünya Savaşı'ndan sonra, dünya barışını, güvenliğini korumak ve uluslararasında ekonomik, toplumsal ve kültürel bir iş birliği oluşturmak için 24 Ekim 1945'te tarihinde kurulmuştur. Ülkemiz de bu kuruluşa üye olup toplamda 193 ülkenin üye olduğu geniş katılımlı bir kuruluştur[46].

Birleşmiş Milletler, bireyi gerçek kişilere ve özellikle de devlet tüzel kişisine karşı korumayı başından itibaren amaç edinmiştir. Bu amaçla Birleşmiş Milletler, 10 Aralık 1948 tarihli İnsan Hakları Evrensel Beyannamesi (İHEB) yürürlüğe konulmuştur. İnsan Hakları Evrensel

[43] Steven, S. McCarty-Snead; Anne, Titus Hilby, Research Guide to European Data Protection Law, 42 Int'l J. Legal Info. 2014, s. 350.
[44] Peter, can, Privacy and Data Protection, 2009, Volume 10, Issue 1, November, Articles / Data Protection: Backto Basics, s. 2.
[45] Aksoy, a. g. e., s. 19.
[46] (Çevrimiçi), https://www.un.org/en/about-un/ , (Erişim tarihi: 01/03/2022).

Beyannamesi m.12'de bulunan "*özel yaşamın gizliliği*" başlığı düzenlenerek aile hayatının da korunması net bir biçimde ifade edilmiştir. Düzenlenen bu maddenin gereği olarak, hiç kimsenin, ailesi, özel yaşamı, konutu ya da haberleşmesi gibi özel alanlarına asla keyfi müdahalede bulunulmayacağı belirtilmiştir. Bahse konu özel alanlara karşı yapılacak olan saldırılara karşı korumanın hukuki olarak güvence altına alınması bütün ülkeler için yasal yükümlülüktür. Düzenlenen bu maddenin kanaatimizce temel ayırt edici özelliği, kişinin korunması gereken alanları ile ilgili olarak uluslararası ve ulusal alanda düzenlenmesi gereken hukuki metinlerin gerekliliğinin keyfilikten öte ihtiyaç olduğu anlaşılmıştır. Bu konuda, BM'nin insan hakları ile ilgili yaptığı çalışmalar devlet tüzel kişisi ve uluslararası kuruluşlar ile birlikte tüm dünya kurumlarını temel haklar bağlamında düzenleme yapma konusunda olumlu anlamda etkileyerek teşvik etmiştir[47].

Tarih 1966 yılını gösterdiğinde Birleşmiş Milletler tarafından hazırlanan Medeni ve Siyasi Haklar Sözleşmesi tüm üye ülkelerin imzasına sunulmuştur. İmzaya sunulan sözleşme m.17'de,

"1. *Hiç kimsenin özel ve aile yaşamına, konutuna veya haberleşmesine keyfi veya hukuka aykırı olarak müdahale edilemez; onuru veya itibarı hukuka aykırı saldırılara maruz bırakılamaz.*
2.*Herkes bu tür saldırılara veya müdahalelere karşı hukuk tarafından korunma hakkına sahiptir."*

Denilerek insan hakları evrensel beyannamesi ile iç içe geçmiş bir düzenleme yapıldığı görülmektedir. Yapılan bu düzenleme ile veri koruma hukuku bağlamında, BM İnsan Hakları Komitesinin getirmiş olduğu düzenleme ile kişisel verilerin gizliliği konusunun özel yaşamın korunması hakkı ile ilişkilendirilerek koruma alanına alınması yönünde görüş bildirmiştir[48].

[47] Council of Europe, Handbook on European Data Protection Law, European Union Agency for Fundamental Rights, 2014, s. 14.
[48] Mehmet Semih, Gemalmaz, Ulusalüstü İnsan Hakları Hukukunun Genel Teorisine Giriş, 2013, Cilt:1, s. 434.

Kişisel verilerin korunması alanında Birleşmiş Milletler tarafından yapılan belki de en önemli düzenleme, 1990 yılında Genel Kurulun "*Bilgisayara Geçirilmiş Kişisel Veri Dosyalarının Düzenlenmesi Rehber İlkeleri*" isimli BM kılavuzunu kabul etmiş olmasıdır. Hazırlanan Rehber tavsiye niteliğinde olup, dokuz temel ilkeden oluşmaktadır.

i. Hukuka uygun ve dürüst yollardan verilerin toplanması ve işlenmesi ilkesi,
ii. Doğruluk ilkesi,
iii. Amaç-özellik ilkesi,
iv. İlgili kişinin erişiminin sağlanması ilkesi,
v. Bireyler arasında ayrımcılık yapılmaması ilkesi,
vi. İstisna yapma yetkisi,
vii. Güvenlik ilkesi,
viii. Denetim ve yaptırımlar,
ix. Sınır ötesi veri akışı, şeklinde belirlenmiştir[49].

Bahse konu bu ilkelerin uygulanıp uygulanmadığını denetlemek için bağımsız bir yapıya sahip olan kuruluşun var olmasını öngören ilk belge olması nedeni ile rehber ilkeler kılavuzu çok büyük öneme sahip olduğu söylenebilir[50].

Kişisel verilerin korunması hukuku ile ilgili olarak, İkinci Dünya Savaşı'ndan sonraki tüm süreçler irdelendiğinde geçen zaman içerisinde, Birleşmiş Milletler'in kişilik haklarının korunması, özel hayatın gizliliği ve kişilerin sayısal sistemlere aktarılmış olan verilerinin korunması konularında göstermiş olduğu özenin teknolojik gelişmeler doğrultusunda arttırılma çabası içerisinde olduğu söylenebilir.

2.4.2 OECD

Ekonomik İş birliği ve Kalkınma Örgütü 14 Aralık 1960 tarihinde imzalanan "Paris Sözleşmesi" dikkate alınarak 1961 yılında kurulmuştur. OECD'nin kuruluş gayesi ekonomik iş birliği, finansal istikrar, demokrasi ve insan hakları kavramları üzerine inşa edilmiş bir kuruluştur[51]. Ekonomik işbirliği kapsamında ülkelerin birbirleri ile olan ilişkilerinin

[49](Çevrimiçi), https://www.refworld.org/docid/3ddcafaac.html , (Erişim tarihi, 01/03/2022).
[50] Küzeci, a. g. e., s. 136.
[51] (Çevrimiçi), https://www.oecd.org/ , (Erişim tarihi: 01/03/2022).

güçlendirilmesi ve uluslararası ticaretin gelişmesini savunan bir kuruluş olmanın yanında, OECD bağlamında kişisel verilerin korunması mutlak olarak ele alınması gereken konulardandır.

Bu bağlamda, OECD'nin 1980 yılında yayımladığı, **"***Kişisel Verilerin Sınır Aşan Trafiği ve Kişisel Verilerin Korunmasına İlişkin Kılavuz İlkeler***"**, kişisel verilerin korunması hukuku alanında düzenlenmiş ilk uluslararası metindir. Düzenlenmiş olan belgenin hukuki niteliğini incelediğimizde metnin bağlayıcılığının bulunmadığı, dolayısıyla bir tavsiye kararından öteye gidemediği görülmektedir. Bu anlamda belgenin yasal olarak bağlayıcı olmadığını net olarak ifade edebiliriz. Ancak tüm bunlara rağmen düzenlenen belgenin temel ilkeleri barındırması hasebiyle kişisel verileri korunması bakımından hiçbir düzenlemenin bulunmadığı devletler için referans niteliğinde olduğunu söyleyebiliriz[52].

OECD üye ülkeleri tarafından hazırlanan rehber de çeşitli temel ilkeler belirlenmiştir. Bunları sıralayacak olursak[53],

i. Bireye ait verilerin toplanmasının sınırlı olması ilkesi,
ii. Yapılan işlemde amacın belirliliği ilkesi,
iii. Yapılan işlemlerin her adımında şeffaf olunması ilkesi,
iv. Toplanan verilerin kaliteli olması ilkesi,
v. Depolanan veri kullanımın sınırlanması ilkesi,
vi. Veri güvenliğini sağlama ilkesi,
vii. Bireyin süreçlere katılımı ilkesi,
viii. Hesap verilebilirlik ilkesi,

Yukarı da saymış olduğumuz temel ilklerin, OECD üye ülkelerine kişisel verilerin korunması hakkında düzenleme yaparken referans olduğunu ifade edebiliriz. Bu sekiz temel ilkeyi referans alan ülkelerde de tartışılmaya başlanması ile kişisel veriler hukukunun ulusal

[52] Gürsel, İlke, Protection of Personal Data in International Law and The General Aspects of TheTurkish Data Protection Law, DEÜHF Dergisi, C. 18, S. 1, 2016, (Basım Yılı: Ekim 2016), s. 4.
[53] (Çevrimiçi), https://www.oecd.org/digital/ieconomy/oecdguidelinesontheprotectionofprivacyandtransbor%20derflowsofpersonaldata.html , (Erişim tarihi: 01/03/2022).

alandan çıkarak uluslararası alanda tartışılmaya başlandığını her anlamda bizlere göstermektedir. OECD kuruluşuna üye olan ülkeler göz önünde bulundurulduğunda, kabul edilen metnin içerisinde bu türden temel ilkelerin belirlenmesinde geniş katılım ile özellikle objektif bir bakış açısıyla hazırlandığı görülmektedir. Bahse konu belgenin dünya genelinde ekonomik refah ve demokrasi açısından ileri gitmiş olan ülkelerin katılımı ile hazırlandığı için belgenin saygınlığını ve niteliğini arttırdığını söyleyebiliriz.

Teknoloji ve iletişimin hızlı gelişimi ile bu belgenin yüksek derecede koruma gerektiren günümüz dünyasına uyumlaştırılması kaçınılmazdır. Teknolojinin getirdiği güvenlik zafiyetlerinden kaynaklı olarak OECD, var olan bu düzenlemeyi 2013 yılında güncelleme gereksinimi duymuştur. Bütün üye ülkelerce hazırlanan OECD rehber ilkleri bugün bile OECD üyesi olsun veya olmasın tüm dünya devletleri için özel bir öneme sahip olup bu anlamda azımsanmayacak etkiler yaratmaktadır[54].

Bu nedenle, uluslararası alanda, OECD gibi çok paydaşlı ve devletlerin birbirleri ile olan entegrasyonunu ticari alanda savunan bir kuruluşun, kişisel verileri koruma hukukuna özellikle temel ihtiyaç olduğunu bildiren, ilgili alan bağlamında genel bir çerçeve belirleyerek kritik prensipleri belirleyen tavsiye niteliğinde rehber ilkeleri yayımlaması, bu alanı tüm dünyada tartışmaya açarak gerek küresel çapta gerekse de devletlerin iç hukukunda farkındalığın artmasına neden olmuştur.

2.4.3 Avrupa Konseyi

Avrupa genelinde demokrasi, hukukun üstünlüğü ve insan haklarını savunmak amacıyla 1949'da inşa edilmiş hükümetler arası bir kuruluştur. Türkiye, Avrupa Komisyonu (AK)'un kurucu üyeleri arasında bulunup 1949 yılında ilk imzalayan ülkeler arasında yer almıştır. Avrupa Komisyonu tarih 1950'li yılları gösterdiğinde bireylerin özel yaşamına ilişkin hakları içerisinde barındıran düzenlemelerin olduğu Avrupa İnsan Hakları Sözleşmesi'ni kabul etmiştir[55].

[54] (Çevrimiçi), https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf , (Erişim tarihi, 01/03/2022).
[55] McKay, Cunningham, Complying with International Data Protection Law, 84 University of Cincinnati Law Review, 421, 2016, s. 426.

Avrupa İnsan Hakları Sözleşmesi m. 8'de "*özel yaşam ve aile hayatına saygı*" hakkı kendisine yer bulmaktadır. Ancak kişisel verilerin korunması hakkı bağlamında açık bir düzenlemenin sözleşmede bulunmadığını ifade edebiliriz. Elbette düzenleme sade bir haliyle incelendiğinde bir eksiklik olarak görülebilir, ancak gelişen teknolojiyle artan güvenlik endişeleri Avrupa Konseyine bağlı olan Avrupa İnsan Hakları Mahkemesi'nin kararlarını bu maddeyi geniş anlamda yorumlayarak kişisel verilerin kötüye kullanılmasını engellemeyi amaç edinmiştir.

Avrupa Konseyi Bakanlar Komitesi kişisel verilerin korunması ile ilgili olarak birçok tavsiye niteliğinde kararlar almıştır. 1980 tarihli tavsiye niteliğinde verdiği kararlar neticesinde, "*108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireyin Korunması*" ismi verilen sözleşmenin düzenlenmesine ve üye ülkeler nezdinde imzalanmasına yol açmıştır. Bu sözleşme veri koruma hukuku bağlamında çok büyük öneme sahiptir. Çünkü yasal olarak bağlayıcılığı bulunan tek uluslararası metindir. Bu metnin düzenlenmesindeki asıl neden, Avrupa İnsan Hakları Sözleşmesi m. 8'de düzenlenen kısımları uygulamak ve özellikle daha koruyucu güvenceler sağlamak olduğunu söyleyebiliriz. Bahse konu sözleşmenin kişisel verilerin korunması bağlamında hangi durumlarda kısıtlamanın yapılabileceği de düzenlenmiştir. Devletin güvenliği, kamu güvenliği ve kamu sağlığı gibi sebeplerin olması durumunda bir sınırlandırma söz konusu olabilecektir.

108 sayılı sözleşme metnini tüm AB üyeleri imzalamışlardır. Ayrıca Avrupa Komisyonuna üye olmayan katılımcı ülkelerin de imzasına açıktır. 108 sayılı sözleşmenin esas amacı, devlet tüzel kişinin korunması değil gerçek kişilerin korunmasıdır. Bunun yanında, ilgili sözleşme, her ülkenin hukuk düzeninde gerçek kişilerin yanı sıra tüzel kişiler açısından da uygulanmaya engel değildir. Kişisel verilerin korunması ile ilgili yaşanan sorunlara yalnızca gerçek kişilerin muhatap olacağı elbette düşünülemez. Buradaki korumanın hem gerçek kişiler anlamında hem de tüzel kişiler anlamında uygulanması gerektiği bilinmektedir. Bu anlamda çeşitli görüşler olmakla birlikte tek kişilik bir şirketin verilerin daha az korunması gerektiği bunun yanında sendikal örgütlenmelerin, dini yapıya haiz oluşumların, politik kuruluşların daha fazla korunması gerektiğini açıkça ifade edebiliriz. Dolayısıyla verilerin

hangi türden veriler olduğu belirlenip ardından verilerin güvenliğinin bu bağlamda alınması gerektiği kanaatindeyiz.

2.4.3.1 108 sayılı sözleşme

2.4.3.1.1 Tarihi

Tarih 1960'lı yılları gösterdiğinde Avrupa Komisyonu'nda kişisel verilerin korunması kanunu tartışmaya açılmıştır. Bu tartışmaların temelinde hızlı bir biçimde gelişen teknoloji ve bunun karşısında korumasız olan verilerin güvenliğinin nasıl sağlanacağı endişesi her geçen gün artmıştır. Artan bu endişenin nedenlerini incelediğimizde bir diğer sebep olarak kişilerin verilerinin hem devlet tüzel kişisi tarafından hem de tüzel kişiler tarafından sistematik bir şekilde neredeyse sınırlamanın olmadığı bir biçimde işlenmesinden kaynaklandığı görülmektedir[56]. Avrupa Komisyonu'nda bahse konu tartışmalarda dile getirilen kaygıların sonucu olarak Bakanlar Komitesi, 1968[57] yılında kişisel verilerin korunmasını[58] çok yönlü olarak ele almak ve yapılması gerekenleri yapmak üzere toplanmıştır. 1968 yılından itibaren Bakanlar Komitesi, gündeme getirilen özel hayat ve bireylerin verilerinin korunması adına çalışmalar başlatmıştır. 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 hazırlamaktır[59]. Özel hayatın ve kişisel verilerin korunması için harcanan mesailerin sonucu olarak, kişisel verilerin güvenliğinin daha korunaklı hale nasıl getirileceği ile ilgili alt komisyon olarak uzmanlar komitesi düzenlenmiştir. Oluşturulan Uzmanlar Komitesi'nin üzerinde eğilim gösterdiği çalışmaları sonucunda, Bakanlar Komitesi bu çalışmalar ile ilgili "*Özel Sektörde Elektronik Veri Bankalarına Karşı Kişisel Mahremiyetin Korunması Hakkında 73/22 sayılı Karar*" ve "*Kamu Sektöründe Elektronik Veri Bankalarına Karşı Bireylerin Korunması Hakkında 74/29 sayılı Karar*" olmak üzere bu anlamda iki düzenleyici kararı onaylamıştır. Yapılan bu çalışmaların muhteviyatını incelediğimizde dijital banka

[56] Graham, Pearce / Nicholas, Platten, Achieving Personal Data Protection in the European Union, Journal of Common Market Studies, S. 36, December 1998, s. 531.
[57] Evans, A.C., European Data Protection Law, American Journal of Comparetive Law, Cilt:29, Yıl: 1981, s. 572.
[58] Fritz H. Grupa / William Kuechler / ScottSweeney, Dealing with Data Privacy Protection: An Issue for the 21st Century, LawInvestigations andEthics, January / February 2002, s. 46.
[59] Hondius, The Council of Europe's Work in the area of Computers and Privacy, s. 8.

işlemlerinin güvenlik bağlamında yapılması gerekenleri anlatmaktadır. Bakanlar Komitesi tarafından düzenlenen bu kararların, belki de en önemli özelliği 108 Sayılı Sözleşme için ön hazırlık niteliğinde olduğu kabul edilmektedir[60].

Uzmanlar komitesi tarafından hazırlanan taslak sözleşme metinleri Bakanlar Komitesi tarafından kabul edilip "*Kişisel Verilerin Otomatik İşlenmesine İlişkin 108 sayılı Sözleşme*" olarak isimlendirilmiştir. Akabinde imzaya sunulmuştur. Kabul edilen bu sözleşmenin yürürlüğe girebilmesi için en az 5 ülke tarafından resmi olarak onaylanması gerekmektedir. Dolayısıyla 5 ülkenin imzalarının tamamlanmasıyla 1985 yılında 108 sayılı sözleşme yürürlüğe girmiştir. Sözleşme bağlayıcılık unsuru bakımından ciddi düzenlemeler içermemekle birlikte uluslararası düzeyde ilk hukuki metin olması açısından oldukça önemli olduğunu belirtmek gerekir[61].

Uluslararası düzeyde ilk hukuki metin olan sözleşmeyi bütün Avrupa Komisyonu üyesi ülkeler onaylamışlardır. Bunun yanında Avrupa Komisyonu üyesi olmayan bazı ülkeler sözleşmeyi imzalamışlardır[62].

2001 yılında 108 Sayılı Sözleşmeye ek protokol düzenlenip taraf devletlerin onayına sunulmuştur. Ek Protokole uygun olarak sözleşmeye taraf bütün devletlerin, kişisel verilerin sözleşmenin öngördüğü biçimde korunup korunmadığı ile ilgili kendi iç hukuklarında denetleyici otoritelerin oluşturulması gerekmektedir. Söz konusu bu denetleyici otoritelerin ihdas edilmemesi veya gerektiği gibi denetimlerin yapılmaması durumunda herhangi bir ülkeye veya kuruluşa veri akışının sağlamasını zorunlu olarak yasaklamaktadır. Dolayısıyla şöyle bir çıkarımda bulunmamız zor olmayacaktır; 108 sayılı Sözleşme'nin yürürlüğe girmesiyle bütün taraf ülkelerin denetleme kurumlarını oluşturmaları zorunlu hale gelmiştir. İhdas edilen denetleme otoriteleri, 108 sayılı sözleşme uyarınca yeknesaklığın sağlanması

[60] Colin J. Bennett / Charles D. Raab, TheGovernance of Privacy Policy Instruments in Global Perspective, Ashgate Publishing Company, England, 2004, s. 72.
[61](Çevrimiçi), https://www.coe.int/t/e/legal_affairs/legal_cooperation/data_protection/Default_DP_Day_en.asp#TopOfPa.g.e , (Erişim tarihi: 01/03/2022).
[62](Çevrimiçi),https://www.coe.int/en/web/conventions/full-list/conventions/treaty/108/signatures?p_auth=gXtFjq5a , (Erişim tarihi: 01/03/2022).

adına aynı ilkeler ve standartlar çerçevesinde görevlerini ifa etmelidirler[63]. Türkiye' de bu ek protokole onay veren ülkeler arasında bulunmaktadır. Onay vermenin gereği olarak denetleme otoritesi olarak "*Kişisel Verileri Koruma Kurumu*" Adalet Bakanlığının ilgili kuruluşu olarak faaliyet göstermektedir[64].

108 Sayılı Sözleşmenin Amaç ve Kapsamı, vatandaşlık veya mukim olma hususunu gözetmeksizin Sözleşmeye taraf olan devletlerin egemenliği altında bulunan bireylerin, verilerini koruma altına almanın yanı sıra; kişisel verilerin sistemler vasıtasıyla otomatik biçimde işlenmesi esasında temel hak ve hürriyetlere bunun yanında belki de esas olarak kişisel verilerin gizliliklerine saygı göstermek şeklinde düzenlenmiştir[65]. Onaylanan sözleşmede açıkça görüleceği üzere, taraf olan ülkelerde ikamet eden bütün kişilerin, otomatik olarak yapılacak işlemlerde verilerinin korunması ile ilgili güvence verilmektedir. Dolayısıyla, dijital herhangi bir sistem kullanmayarak işlenen veriler düzenleme dışında kalmaktadır. Burada belki de son olarak şunu belirmekte fayda olacaktır; İlgili sözleşmede verilerin otomatik işlenmesinden kasıt bütün süreçlerin otomatik işlenmesi değildir. Veri işlemenin herhangi bir aşamasında otomatik bir işlemin söz konusu olması yeterlidir[66].

Bahse konu sözleşmenin diğer bir önemli amacını şu şekilde ifade edebiliriz; Taraf bulunan ülkelerin sözleşmede bulunan temel ilkeleri göz önünde bulundurarak iç hukuklarında gerekli tüm düzenlemeleri yaparak akabinde denetim mekanizmasının kurulması amaçlanmaktadır (108 s. söz. m. 4). Dolayısıyla kişisel verilerin korunması ile ilgili yapılan bu düzenlemelerin aslında sadece amaç olarak değil birer yükümlülük olarak ifade edilmesi söz konusu olabilecektir.

Esas olarak 108 sayılı sözleşme kişisel verilerin toplanması, depolanması, işlenmesi ve aktarılması ile ilgili tüm süreçleri düzenlemek bunun yanında işlenen verilerin yanlış kullanılmasının önüne geçmek için üst seviyede korumayı amaçlamaktadır. Yine sözleşmedeki bir diğer amaç, verilerin toplanmasını gerektiren hukuki neden ve bu nedene

[63] Handbook on European Data Protection Law, s. 14. s. 115.
[64] (Çevrimiçi), https://kvkk.gov.tr/ , (Erişim tarihi: 01/03/2022).
[65] (Çevrimiçi), https://inhak.adalet.gov.tr/ , 108 s. söz. m.1, (Erişim Tarihi:01/03/2022).
[66] Atak, Songül, Avrupa Konseyi'nin Kişisel Veriler Açısından Sağladığı Temel Güvenceler, TBBD, S. 87, 2010, s. 95.

uygun bir biçimde toplanması, işlenmesi ile ilgili süreçlerin usul ve esaslarının belirlendiği görülmektedir. Sözleşmede açıkça düzenlendiği üzere, yasal güvencelerin bulunmadığı durumlarda hassas kişisel verilerin toplanması kesinlikle yasaklanmaktadır. Sözleşme bireyin kendisine ait olan verinin her zaman düzeltilmesini talep edebilme hakkına sahiptir.

Sözleşme, bireylerin kişisel verilerinin işlenmesi konusunda, gerçek kişilerin verilerinin hem kamu sektöründe hem de özel sektörde işlenmesi işlemlerini barındırmaktadır. Dolayısıyla buradan anlaşılacağı üzere uygulama alanının gerçek kişilerden ibaret olduğunu görebilmekteyiz. Dijital elektronik sistemlerle otomatik olarak işlenmeyen veriler, sözleşme gereği korunması gereken veriler olarak dikkate alınmamaktadır. Ayrıca belirtmek gerekir ki, sözleşmeye taraf bulunan devletler, kendi iç hukuklarında düzenlemeler yaparken veri güvenliğine ilişkin daha kısıtlayıcı ve daha nitelikli koruma içeren çalışmalar yapabilirler[67]. Sözleşmede gerçek kişiler dikkate alınırken taraf olan devletler kendi iç hukuklarında tüzel kişilere ait verilerinin korunması ile ilgili düzenlemeler yapabilirler. Bu bağlamda herhangi bir kısıtlayıcı durum söz konusu değildir[68].

2.4.3.1.2 108 Sayılı Sözleşmede bahsedilen ilkeler

Kişisel verilerin işlenmesine ile ilgili temel ilkeler sözleşme m. 5'de düzenlenmiştir. Yapılan bu çalışmalar kapsamında otomatik olarak işlenen kişisel veriler;

i. Veriler depolandığı amaç ile orantılı olarak gerektiği kadar muhafaza edilmelidir,
ii. Kişisel verilerin toplanması söz konusu olduğunda, amaç belirlenmeli ve bu amaç ile ölçülü olacak biçimde toplanması gerekmektedir,
iii. Toplanan kişisel veriler adil ve hukuk çerçevesinde işlenmelidir,
iv. İşlenen kişisel veriler doğru ve güncel olmalıdır,
v. Düzenlemede ifade edilen meşru amaçlarda depolanması ve yine yasal zeminde amaç ile paralel olarak kullanılmalıdır.

Hassas verilere ilişkin olarak, m. 6'da yapılan düzenlemeye göre, ırk, köken, siyasi görüş, dini inanç, cinsel yaşam, sağlıkla ilgili verilerin yanı sıra cezai yaptırımlarla ilgili verilerin

[68] Colin, Tapper, New European Directions in Data Protection, Journal of Law, Information and Science, Sayı: 9, 1992, s. 11.

toplanması ve saklanmaması hükmünün amir olduğunu ifade edebiliriz (108 s. söz. m.11). Ancak yapılan bu düzenlemenin yanında her ülkenin iç mevzuatı değişkenlik gösterebilir. Hassas verilerin toplanması ve saklanması ile ilgili iç hukuklarında yeterli koruma sağlandığı düşünülüyorsa, o halde bu hassas verilerin işlenmesi söz konusu olabilecektir. 108 Sayılı Sözleşme'de kişisel verilerin korunması bakımından taraf olan devletlerin iç hukuklarında yapacakları düzenlemelerle önlem alınması beklenmektedir. Dolayısıyla otomatik olarak veri dosyalarında saklı bulunan verilerin yetkisiz kişiler tarafından imha edilmesi, yanlışlıkla silinmesi, kaza sonucu kaybolması, yetkisiz erişimi, değiştirilmeye veya yayılmaya karşı korunması için gerçek anlamda önlemler alınmak zorundadır. 108 Sayılı Sözleşme'de düzenlenen güvencelere ilişkin istisna ve kısıtlamalar, AİHS m.8'le benzer olduğu söylenebilir. Bunun yanında herhangi bir mahremiyeti bulunmayan, bilimsel araştırma yürütme veya istatistik tutmak gibi amaçlar için kullanılan otomatik kişisel veri dosyalarının kullanılması ile ilgili de sözleşmeye taraf olan devletlerin kendi iç hukuklarında yapacakları düzenleme ile uygun görülmesi mümkün olabilecektir. 108 Sayılı Sözleşme'ye taraf ülkeler sözleşme ile uyumlu olan temel ilkelerin korunmasında sorumlulukları bulunmaktadır. Dolayısıyla her devlet, kişisel verilerin korunması anlamında bir ihlal söz konusu olduğunda iç hukuklarında yapılan düzenlemelerden yola çıkarak yaptırım ve yapılan ihlalin giderilmesi için harekete geçmek zorundadır (108 s. söz. m.10). Aslında 108 Sayılı Sözleşme'nin taraf olan devletlerin iç hukukuna uygulanabilme imkânı bulunmamaktadır. Söz konusu sözleşmeyi taraf olan devletler doğrudan kendi iç hukuklarına uygulayamadığından, sözleşmeyi ana çerçeve kabul edip her bir maddesinin ayrı ayrı incelenerek yasalaştırılması gerekmektedir[69]. Bu anlamda sözleşmeye taraf olan devletlerin kişisel verilerin korunması ile ilgili olarak yapacakları yasal çalışmalar ile iç hukuklarında daha etkin koruma ve ortak temel güvencelerin oluşabileceği düşünülmektedir[70]. Sonuç olarak, kanun koyucu tarafından çıkarılan 6698 sayılı Kişisel Verilerin Korunması Kanunu 108 Sayılı Sözleşme'nin getirmiş olduğu temel ilkeler neticesinde yürürlüğe girmiştir.

[69] Tekin, Akıllıoğlu, İdari Usul ve Kişisel Verilerin Korunması, https://www.idare.gen.tr/akillioglu.htm , s. 6, (Erişim tarihi: 01/03/2022).

[70] Paul M., Schwartz, European Data Protection Law and Restrictions on International Data Flows, IOWA LawReview, S. 80, March 1995, s. 477.

2.4.3.1.3 108+ Sayılı Sözleşme Revizyonu

Taraf olan ülkelerin hukuk sistemlerini bu Sözleşme'ye uygun hale getirmelerini arayan 108 Sayılı Sözleşme, 1 Ekim 1985 tarihinde yürürlüğe girmiştir[71]. 108 Sayılı Sözleşme'nin yürürlüğe girmesi ile İHAS'a bir hüküm konulmasına gerek duyulmamıştır[72]. Bahse konu Sözleşme, Avrupa Topluluğu'na da açılacak şekilde 1999 yılında değişikliğe uğramıştır. Tarih 2001 yılını gösterdiğinde, Sözleşme düzenini Avrupa Topluluğu'na yakın hale getiren Ek Protokol imzaya açılmıştır[73]. Tarih 2011 yılını gösterdiğinde, 108 Sayılı Sözleşme yeniden ele alınıp değerlendirilmeye alınmıştır. Bu aşamada "*Kişisel Verilerin Korunması Hakkı*"na açıkça atıfta bulunma ihtimali dile getirilmeye başlanmıştır. Yine tarih 2016 yılını gösterdiğinde, 108 Sayılı Sözleşme'nin ele alınıp değerlendirilmesi ve yenilenme sürecinin ikinci aşaması başlatılmıştır. Yenilenme süreciyle birlikte Sözleşme'de yer alan düzenlemelerin hem tavsiye hem de yönergeler aracılığıyla daha kapsamlı kurumsal metinlerle tamamlanacak ilkesel düzenlemeler haline gelmeleri sağlanmakta ve AB yasal düzenlemeleriyle uyum içerisinde olması amaçlanmaktadır. Yapılan tüm çalışmaların sonunda Sözleşme'nin evrensel olması bakımından bir standart oluşturduğunu ifade eden bir taslak ortaya çıkmıştır[74]. AB Genel Veri Koruma Tüzüğü'nün yürürlüğe girmesinden sonra 18 Mayıs 2018'de Avrupa Konseyi Bakanlar Komitesi, Avrupa Konseyi'nin 108 Sayılı Sözleşmesi'ni modernize eden Protokol'ü yani 108+ Sözleşmeyi kabul etmiştir[75]. 108+ Sözleşme'nin yürürlüğe girmesi iki durumun oluşması durumunda gerçekleşecektir: Birincisi mevcut tüm tarafların Sözleşme 108+'ı kabul etmesi durumunda bir diğer durum ise Sözleşme'nin imzaya sunulmasından beş yıl sonra toplamda 38 taraf ülkenin Sözleşme 108+'ı onaylaması durumunda Sözleşme 108+ yürürlüğe gireceği kabul edilmiştir[76].

---

[71] 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 , (Erişim Tarihi: 04/03/2022)

[72] Fuster, The Emergence of Personal Data Protection as a Fundamental Right of the EU, s. 91

[73] 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 , (Erişim Tarihi: 03/03/2022).

[74] Modernisation of the Data Protection Convention 108, https://www.coe.int/en/web/portal/28-january-data-protection-day-factsheet , (Erişim Tarihi: 04/03/2022).

[75] 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/16808b36f , (Erişim Tarihi: 04/03/2022).

[76] 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.

108 Sayılı Sözleşme'nin modernize edilmesi ile düzenlenen 108+ Sözleşme ile bilişim teknolojilerindeki yaşanan gelişmeler gözönünde bulundurularak daha nitelikli bir veri koruma sistemi düzenlenmiştir. Bu bakımdan 108+ Sözleşme, GVKT'de bulunan en önemli yenilikleri tanımaktadır (GVKT). Söz konusu düzenlemenin amacı insan onuru ve bireysel özerklik özellikle vurgulanmış, uluslararası kuruluşların Sözleşme'ye taraf olabileceklerine değinilmiş, yeni tanımlamalar yapılmış, kişisel verilerin işlenmesi aşamalarında maksimum şeffaflığın olması için yeni kurallar belirlenmiş ve veri koruma otoritelerinin görev ve yetkileri yeniden düzenlenmiştir. Bunların yanında özel nitelikli kişisel veriler kategorisi geniş tutularak genetik ve biyometrik veriler de GVKT'de olduğu gibi düzenlemeye dahil edilmiştir[77]. GVKT'de bulunan, tasarımla veri koruma ve varsayılan ayarlarla veri koruma gibi güncel uygulamalar ile kişisel veri öznesinin temel hak ve özgürlüklerine ciddi müdahale oluşturabilecek veri sızıntılarının derhal bildirilmesi yükümlülüğü düzenlenmiştir. Modernize edilen Sözleşme 108+ ile taraf olan devletler bu düzenlemeden sonra bazı alanları istisna olarak tutmak gayesiyle bildirimde bulunamayacaktır. Sözleşme 108+ hükümlerinin gerçek ve ciddi bir ihlal durumu yoksa üye devletler arasında sınır ötesi veri aktarımı serbest tutulmuştur[78]. Sözleşme 108+, GVKT'nin bütün yeniliklerini içermemektedir. Bu nedenle doktrinde GVKT'de bulunup Sözleşme 108+'da bulunmayan düzenlemelerin oluşturacağı farklılığın nelere sebep olabileceği belirsiz olduğu; ancak Sözleşme 108+ düzenlemesinin 2023 yılına dek yeni küresel ilkeler olarak kabul edilebileceği ifade edilmektedir[79].

Genel Veri Koruma Tüzüğü yürürlüğe girdikten sonra kısa bir süre sonra uluslararası alanda kişisel verileri koruma ihtiyacı hasıl olmuş ve Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi ihtiyaçlar doğrultusunda yenilenmiştir. Avrupa Konseyi üyesi olmayan ülkelerin de imzalamasına imkân sağlayan

[77] Sezen, Kama Işık, Avrupa Veri Koruma Hukukuna Anayasal Bir Bakış, Doktora Tezi, Marmara Üniversitesi, Sosyal Bilimler Enstitüsü, Kamu Hukuku Anabilimdalı İstanbul 2019, s. 75.

[78] 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/16808b36f , (Erişim Tarihi: 04/03/2022); Elif Küzeci, Avrupa Konseyi'nin 108 sayılı Kişisel Verilerin Korunması Sözleşmesi Yenilendi! Sözleşme 108+, Carpenter Kararı ve diğer bazı gelişmelere ilişkin değerlendirme, https://medium.com/@elfkzc/avrupa-konseyinin-108-say%C4%B1l%C4%B1-ki%C5%9Fisel-verilerin-korunmas%C4%B1-s%C3%B6zle%C5%9Fmesi-yenilendi-bc8daad9decc , (Erişim Tarihi: 06/03/2022).

[79] Greenleaf, Convention 108+ and the Data Protection Framework of the EU, Conference on Convention 108+ Tomorrow's Common Ground for Protection, s. 4.

108+ sözleşmesi evrensel bir çerçeve çizmiş ve dünyanın herhangi bir ülkesi tarafından imzalanabilir bir hale getirilmiştir[80]. Türkiye 108+ sayılı sözleşmeyi imzalamayan ülkeler arasındadır. Avrupa Konseyi üyesi olsun veya olmasın bütün ülkelerin imzasına sunulan sözleşmede düzenlenen yenilikler:[81]

i. Veri koruma otoritelerinin yetki alanları genişletilmiş ve veri otoriteleri arasında daha fazla işbirliği yapılması öngörülmüştür.
ii. 108+ Sayılı Sözleşmenin yargı yetkisi kapsamında olan kişi hangi ülke vatandaşı olduğuna bakılmaksızın koruma altına alınması öngörülmüştür.
iii. Düzenlenen bu sözleşmeye taraf olan ülkeler arasında veri akışının serbest olması hüküm altına alınmıştır. Kabul edilebilir güvenlik risklerinin olduğu durumlarda bu hüküm uygulanmayacaktır.
iv. Hassas kişisel veri kapsamı genişletilmiş olup, bu kategoriye biyometrik veriler, etnik köken ve sendika üyeliği de eklenmiştir.
v. Kişisel veri sahiplerine yeni haklar tanınmış olup, profilleme ve otomatik karar sistemlerine rıza verilmeden dahil edilmemesi hükmü getirilmiştir.
vi. Veri sızıntılarının derhal bildirilmesiyle alakalı hüküm getirilmiştir.

2.4.3.1.4 Sınır ötesi veri transferi

Sınır ötesi veri akışını, kişisel verilerin yabancı bir ülkenin iç hukukuna tabi kılınan bir alıcıya aktarılması şeklinde tarif edebiliriz[82]. Bilgi sistemleri ve veri işleme mekanizmalarında meydana gelen gelişmelerden dolayı, vatandaşların verilerinin yurt dışına aktarılmasına ilişkin ulusal veya uluslararası düzeyde düzenlemelerin yeniden ele alınıp yorumlanmasına ve bu bağlamda konu ile ilgili en güncel düzenlemelerin yapılmasına ihtiyaç duyulmaktadır. Dolayısıyla günümüzde neredeyse toplumun her ferdinin bir şekilde internet dünyasında kendisine yer bulduğu, özellikle sosyal medyada bulunan platformları kullanarak, verilerinin depolanması ve işlenmesi söz konusu olmaktadır. Söz konusu sosyal medya platformlarının yurt dışı kaynaklı olması nedeniyle, devletler vatandaşlarının

[80] Yılmaz, Sabire Sanem, Tıp Alanında Kişisel Verilerin Korunması, 2021, s. 133.
[81] (Çevrimiçi), https://search.coe.int/cm/pages/result_details.aspx?Objectld=090000016807c65bf, (Erişim Tarihi: 02/03/2022)
[82] Handbook on European Data Protection Law, a. g. e., s. 130.

verilerini korumak, bu alanda güvenliği veya korumayı üst seviyelere çıkarabilmek için sınır ötesi veri akışı konusunun mutlak suretle ele alınıp değerlendirilmesi gerekmektedir[83].

Sözleşmeyi imzalayan taraf ülkeler arasında sözleşme gereği kişisel verilerin serbest dolaşımı kabul edilmiştir. Serbest dolaşım kararının sonucu olarak özel hayatın gizliliğinden dolayı devletlerin veri aktarım sınırlaması söz konusu olmayacaktır. Ancak bu duruma rağmen taraf devletler arasında iki istisna durum belirlenmiştir. Sözleşmeye taraf olan ülkelerin birinde kişisel verilerin korunması hakkında getirilen farklı koruma tedbirlerinin varlığı halinde, sınır ötesi veri akışı yapılacak devletin bu özel koruma tedbirini benimsememesi durumunda, kişisel verilerin aktarılmaması seçeneği seçimlik bir hak olarak veri aktarımında bulunacak ülkeye tanınmıştır. Bir diğer istisna kapsamında Ek Protokol m.2'de yapılan düzenlemeye göre; sözleşme imzacısı olmayan bir devletin veya uluslararası kuruluşa veri aktarılmasının şartı, zorunlu olarak iç hukuklarında eşit düzeyde korumanın sağlanması durumunda izin verilebileceği çok net bir biçimde ifade edilmiştir (108 s. söz. m. 12).

108 Sayılı Sözleşmede görüleceği üzere veri aktarımının gerçekleşeceği devlet veya uluslararası kuruluşun, yeterli bir koruma sağlaması koşulu ile yapılan düzenlemenin, imzacı olmayan yani taraf olmayan ülkelere serbest veri aktarılmasına izin verdiği görülecektir. Bu bağlamda, sözleşmeyi imzalayan taraf devletlerin, hukuk düzeni tarafından, veri aktarılan taraf olmayan bir ülkede veri koruma seviyesinin değerlendirilmesinin nasıl ve kimler tarafından yapılması gerektiği konusunda karar merci olduğu anlamı taşımaktadır[84].

Avrupa Komisyonu'nun veri koruma yasasına yönelik olarak yaptığı çalışmaları incelediğimizde, yukarıda detaylı olarak açıkladığımız üzere ilk olarak 1961 yılında çalışmaların olduğunu görmekteyiz. Bu çalışmalar toplumda uzun yıllar tartışmalara konu olmuştur. Tarih 1973 yılını gösterdiğinde bu konuya eğilimin üst seviyelere ulaştığı görülmektedir. Kişisel verilerin korunması ile ilgili hukuki anlamda bir düzenleme ilk defa 1981 yılında 108 Sayılı Sözleşmenin kabulü ile gerçekleşmiştir. 1981 yılında Avrupa Komisyonu'na üye devletlerce onaylanan 108 Sayılı Sözleşme sadece üye devletlerce

[83] Mckay, a. g. e., s. 422.
[84] Handbook on European Data Protection Law, a. g. e., s.133.

uygulanmayıp üye olmayan devletlerin referans olarak kullanabileceği dolayısıyla üye olması veya üye olmaması fark etmeksizin yararlanabilmesi bakımın çok önemli bir sözleşmedir. Bu anlamda 1961 yılından itibaren yapılan çalışmaların, bilginin ve tecrübenin üye olmayan bütün devletlerin hukuk sistemlerine ulaşma fırsatı sunmuştur. Sonuç olarak sözleşme çerçevesinde üye devletleri sorumluluk altına sokarak kişisel verilerin korunması hukuku temelinde bağlayıcı bir metin olması ve buna ilave olarak ilerleyen yıllarda ek protokol ile bağımsız denetim otoritelerinin oluşturulması ve belki de en önemlisi tüm bu çalışmaların Avrupa İnsan Hakları Sözleşmesi ile paralel bir koruma mekanizması benimsemesi bütünlük açısından 108 Sayılı Sözleşmenin ne kadar önemli olduğu konusunda bize bilgi vermektedir.

2.4.3.2 Avrupa insan hakları sözleşmesi

1982 Anayasası'nda ve Avrupa İnsan Hakları Sözleşmesi'nde kişisel verilere ilişkin bir tanım bulunmamasına rağmen, hem Avrupa İnsan hakları Mahkemesi kararlarında, hem de Anayasa Mahkemesi bireysel başvuru kararlarında, kişisel verilerin, 108 sayılı Avrupa Konseyi Sözleşmesi'ndeki yapılan tanım ile uyumlu bir şekilde tanımlandığı ifade edilebilir[85]. Avrupa İnsan Hakları Mahkemesi de kişisel verilere yönelik olarak teknolojinin neden olduğu tehditlere karşı kayıtsız kalmamış ve kişisel verilerin devlet tarafından bireyin rızası dışında ya da rızası olsa bile belirlenen ölçütlere aykırı olarak toplanmasının özel hayat kapsamında değerlendirileceği ifade edilmiştir[86]. Zira Avrupa İnsan Hakları Mahkemesi'nin çeşitli kararlarına göre, kişilerin özel yaşamına ilişkin bilgilerin kaydedilmesi m. 8 kapsamında olup bilgilerin kullanılmasına gerek olmadığına karar verilmiştir[87]. Mahkeme bir başka kararında; kişisel verilere ilişkin olarak devletin özel hayat bahsinde olduğu gibi

[85] Börekçi, Eşref Barış, Kişisel Verileri Verme, Yayma veya Ele Geçirme Suçu, Yükseklisans Tezi, Yeditepe Üniversitesi, Sosyal Bilimler Enstitüsü, Kamu Hukuku Anabilimdalı, İstanbul 2019, s. 26.

[86] Tezcan, Durmuş, Erdem, Ruhan Mustafa, Sancakdar, Oğuz ve Önok, Rifat Murat, İnsan Hakları El Kitabı Ankara, Seçkin Yayınevi, 2014; Salihpaşaoğlu, Yaşar, Özel Hayatın Kapsamı: Avrupa İnsan Hakları Mahkemesi İçtihatları Işığında Bir Değerlendirme, Gazi Üniversitesi Hukuk Fakültesi Dergisi, Cilt- 17, Sayı 3, Ankara – 2013, s. 228.

[87] Case of Amann v. Switzerland, App. No: 27798/95, (Çevrimiçi), https://hudoc.echr.coe.int/fre#{%22fulltext%22:[%22Amann%20v.%20Switzerland%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-58497%22]} , (Erişim Tarihi: 04/03/2022).

hem negatif[88] hem de pozitif yükümlülüklerinin devletin, tıpkı özel hayat gibi kişisel verilere ilişkin olarak hem negatif hem de pozitif yükümlülüklerinin[89] olduğunu ve bu yükümlülüklere aykırı olarak gerçekleştirilen keyfi müdahalelerin 8. maddeyi ihlal anlamı taşıyacağını belirtmiştir[90].

Avrupa Konseyi'nin kuruluş amaçlarından birisi de üye devletlerin, temel insan haklarını kurumsal ve korunması gereken bir hukuk alanı olarak kendi iç hukuklarında ilgili düzenlemeleri yapmak ve insan hakları ihlallerini engellemek için bir araya getirmektir. Bu amacı gerçekleştirmek için, 1950 tarihli Avrupa İnsan Hakları Sözleşmesi kabul edilmiştir. Altı yıl sonra, üye ülkelerin Avrupa İnsan Hakları Sözleşmesi kapsamındaki yükümlülüklerini yerine getirmelerini garanti altına almak için, Strasburg'da Avrupa İnsan Hakları Mahkemesi kurulmuştur[91]. Avrupa İnsan Hakları Sözleşmesi, insan hakları hukuku ve bu hakların korunması mekanizması içerisinde dünyada en önemli uluslararası metinlerin başında gelmektedir.

Avrupa İnsan Hakları Sözleşmesi'nde, kişisel verilerin korunması ile ilgili herhangi bir hakkın özellikle sayılmadığı görülmektedir. Konu ile ilgili uygulama, içtihat ve sözleşmeler incelendiğinde, AİHS'de kişisel verilerin haksız ve ölçüsüz müdahalelerden korunması için hususi bir hükmün olmadığı görülecektir. Avrupa İnsan Hakları Mahkemesi, kişilerin verilerinin korunması ile ilgili düzenlemeyi, özel hayat hakkı olarak m. 8 kapsamında düzenlemiştir. Bu sebeple, yapılacak yorumlar yardımıyla, kişisel veriler alanında yasa çıkaran ya da yasa çıkarmayan ülkelerin vatandaşları aynı koruma kapsamından yararlanmaktadırlar. Kişisel verilere ilişkin müdahalenin m. 8 kapsamında olup olmadığı konusunu Avrupa İnsan Hakları Mahkemesi değerlendirmektedir. Avrupa İnsan Hakları Mahkemesi konu ile ilgili değerlendirmeyi yaparken, kişilerin verilerine yönelik yapılan

[88] Leander v. Switzerland, App. No: 9248/81, (Çevrimiçi), https://www.legislationline.org/download/id/3521/file/Case_of_Leander_v_Sweden_1987_en.pdf , (Erişim Tarihi: 04/03/2022).
[89] Gaskin v. United Kingdom, App. No: 10454/83, (Çevrimiçi), https://ips.ligazakon.net/document/ES015218 , (Erişim Tarihi: 04/03/2022).
[90] Hasan Sınar, Kişisel Verileri Hukuka Aykırı Olarak Verme, Yayma veya Ele Geçirme Suçu (TCK Md. 136), Kişisel Verileri Koruma Dergisi, C.2, S.1, 2020, s. 37; Aktaş, Batuhan, (2017), İnsan Hakları Avrupa Mahkemesi ve Yargıtay Kararları Açısından Özel Hayatın Gizliliğini İhlal Suçu, İstanbul: Der Yayınları.
[91] Handbook on European Data Protection Law, a. g. e., s.14.

müdahalelerin, iç hukuka ve 108 sayılı sözleşmeye uygun olarak yapılıp yapılmadığını m. 8 kapsamında incelemektedir.

Avrupa İnsan Hakları Mahkemesi'nin Z/Finlandiya Kararında[92], davaya konu olayda başvuran kişinin eşi HIV virüsü taşımaktadır. Başvurucunun daha önce birlikte yaşamış olduğu eski eşine hem tecavüz hem de kasten HIV virüsü bulaştırmak suçlamasıyla açılan ceza davasında, delil olarak kullanmak suretiyle başvurucunun tetkiklerini yaptırmış olduğu sağlık kuruluşundan sağlık bilgileri talep edilmiştir. İstenilen sağlık bilgileri dava dosyası içerisine alınmış, sağlık kuruluşunda çalışan doktorlar da tanık olarak dinlenmiştir. Avrupa İnsan Hakları Mahkemesi dava dosyası kapsamında bütün delilleri değerlendirdikten sonra vermiş olduğu kararda, Avrupa Konseyi Bakanlar Komitesi'nin Sağlık Hizmetlerinde ve Sosyal Alanlarda HIV virüsüne ilişkin Etik Konular Hakkında Tavsiye Kararı'na ve Avrupa Konseyi'nin 108 numaralı sözleşmesine atıfta bulunarak, HIV virüsü taşıyan bireylerin söz konusu hastalığa ilişkin bütün bilgilerinin gizlenmesi gerektiği ve bu türden sağlık verilerin açıklanmasının hayatın olağan akışı içerisinde bireyin aile yaşamından tüm iş yaşamına bütün sosyal ve ekonomik hayatını etkileyebileceği, özel ilişkilerinden mahrum kalacağı ve kişinin hayatı içerisinde yaşayabileceği tüm aktivitelerden soyutlanmasına yol açacağı konularına değinmiştir. HIV virüsü taşıyan kişinin bu korkularından dolayı tedavi olmak istemeyeceği ve bunun sonucunda bulaşıcı hastalıkların artış gösterip toplum yararını olumsuz yönde etkileyen bir durumun oluşacağına, bu türden sağlık verilerinin kamu yararı olduğu durumlarda açıklanmasının daha uygun olacağı ifade edilmiştir. Söz konusu olayda soruşturma devam etmekte olup sağlık verileri mahkeme tarafından soruşturma kapsamında istenmiştir. Mahkeme ilgili olayda soruşturma yararının, kişinin sağlık verilerinin açıklanmamasından elde edilecek yarardan daha üstün olacağını bu nedenle sağlık verilerinin soruşturma dosyasına girmesinin bir ihlal oluşturmayacağına karar vermiştir. Mahkemenin ihlal verdiği husus: Temyiz mahkemesinin HIV virüsü taşıyan hastanın verilerini açık bir şekilde herkesin göreceği gibi soruşturma dosyasına alınması ve 10 yıl sonra da herkese açıklanacağına ilişkin kararının orantısız olduğuna hükmetmiştir.

[92] 25/02/1997 tarih ve 22009/93 Başvuru Numaralı, Z / Finlandiya Karar, (Çevrimiçi), https://hudoc.echr.coe.int/tur#{%22fulltext%22:[%22\%2222009/93\%22%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-58033%22]}, (Erişim Tarihi: 02/03/2022).

Avrupa İnsan Hakları Mahkemesi L.H. Letonya Kararında da, başvuran kişinin, bir kamu kurumu tarafından kendisinin rızası olmadan sağlık verilerinin işlenmesi nedeniyle Avrupa İnsan Hakları Mahkemesi'ne m. 8'in ihlali kapsamında başvuruda bulunmuştur. Mahkeme, devletin takdir hakkını sınırsız kullanamayacağı, takdir hakkını gerekçelendiremediği ve yasal düzenlemelerde yer almaksızın yedi yıl gibi uzun zaman başvurucunun sağlık verisinin toplanmasını m. 8'in ihlali olarak değerlendirmiştir[93].

Konu kapsamında yapılan çalışmalar ve Avrupa İnsan Hakları Mahkemesi'nin kararları değerlendirildiğinde, m.8 kapsamında yapılan denetim önemli olmakla birlikte, kişilerin verilerinin korunması ile ilgili olarak uygulama alanının giderek genişlemesi, her ülkenin kendi iç mevzuatında özellikle anayasalarında söz konusu hakka temel hak olarak yer vermeleri dikkate alındığında, uygulamada birliğin sağlanması adına ayrı ve hususi bir düzenleme yapılarak AİHS kapsamında koruma altına alınması sağlıklı olacaktır. Böyle bir düzenlemenin yapılmaması durumunda sınırlama rejiminde, veri koruma hukuku ile özel yaşamın korunması arasında farklılıklar söz konusu olabilmektedir[94]. Düzenleme kapsamında, ek hükümlerin kabul edilmesine ilave olarak bu hakka getirilecek sınırlamaların açık şekilde bu hakkın ihtiyaçları ile orantılı olarak sözleşmeye eklenmesinin yerinde olacağı kanaatindeyiz.

2.4.4 Avrupa Birliği

13 Haziran 1990'da Berlin Duvarının yıkılmasından sonra 3 Kasım 1990'da Doğu ve Batı Almanya'nın birleşmesi ve ardından Aralık 1991'de Sovyetler Birliği'nin dağılması sonucunda Avrupa'nın siyasi yapısı baştan aşağı değişmiştir. Avrupa ülkeleri, temel kriterleri belirlemek için 1991 yılında Maastricht'te bir araya gelen Avrupa Birliği Zirvesi ile belirlenen yeni bir antlaşma yapılması için görüş alışverişlerinde bulunmuşlardır. Bu görüşmeler sonucunda Avrupa Birliği Antlaşması olarak da zikredilen Maastricht Antlaşması, 1 Kasım 1993 tarih itibari ile yürürlüğe girmiştir. 1995'te siyasi ve ekonomik bir birlik olarak anılan AB'nin asıl gayesi, üye devletler arasında uygulanabilecek yasama

[93] L. H. v. Letonya, para, Başvuru No: 52019/07, T.29/04/2014, (Çevrimiçi), https://hudoc.echr.coe.int/tur#{%22fulltext%22:[%2252019/07%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-142673%22]} , (Erişim Tarihi: 02/03/2022)

[94] Christoph Sobotta, Juliane Kokott, The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR, International Data Privacy Law, 2013, S. 3, s. 222.

çalışmalarında bulunabilmektedir. Ancak her üye devletin bağımsız olması ve dış politikada kendilerini temsil edebilmeleri göz önünde bulundurulduğunda tipik federal devletten ayrıldığı görülmektedir.

Kişisel verilerin korunması konusu 1960'ların başından itibaren Avrupa'da tartışma alanında kendisine yer bulmuştur. Bu tartışmalar neticesinde özellikle bu tarihlerde, kişisel verilerin korunmasının hukuki zeminde düzenlenmesiyle ilgili önemli adımlar atılmıştır. Bu anlamda ilk olarak, Almanya'nın Hessen eyaleti, 1970 yılında dünyada ilk olarak kişilerin verilerinin korunması ile veri koruma yasasını kabul etmiştir[95]. Avusturya, Danimarka, İsveç ve Fransa gibi ülkeler de aynı yöntemleri izleyerek 1970'li yıllarda iç hukuklarında düzenlemeler yaparak verilerin korunmasına ilişkin yasalar çıkarmışlardır[96]. Bu kapsamda, devletler vatandaşlarının verileri ile ilgili kişisel verilerin korunması hakkının 1976'lı yıllarda Portekiz Anayasasında, 1978'li yıllarda İspanya Anayasasında ve ayrıca 1983 tarihli Hollanda Anayasasında düzenlendiğini görmekteyiz[97]. 1970'li yıllarda veri koruma yasasını kabul eden Alman Anayasa Mahkemesi, kişisel verilerin korunması ile ilgili olarak Kıta Avrupa'sına büyük katkıda bulunduğu kabul edilen ve aynı zamanda "Nüfus Sayımı Kararı" olarak dile getirilen kararında; kişilerin kendisi hakkında tutulan bilgilere erişimine ek olarak kişinin kendisine ait olan veriler üzerinde tasarruf yetkisini kabul eden ve kişilerin verilerinin kaderini tayin hakkı kararına imza atmıştır[98]. Tüm bu gelişmeler değerlendirildiğinde Avrupa Hukukunda, 95/46/AT sayılı AB Yönergesinin yürürlükte olmasından önce, kişilerin verilerinin korumasının öneminin farkına varıldığı ve pek çok ülkenin Anayasasında bir anayasal hak olarak düzenlendiği görülmektedir.

Tarihsel gelişim sürecinde, Avrupa hukukunun genel anlamda veri koruma hukukuna, daha özelde ise kişisel verilerin korunması hukukuna verdiği katkının ne kadar önemli olduğu yadsınamaz bir gerçektir. Hususiyetle 1960'lı yıllarda başlayan süreç ile ilk olarak, özellikle

[95] Sandra C. Henderson, Charles Asynder, Personal Information Privacy: Implicationsfor MIS Mana. g. ers, Information & Mana. g. ement, S. 36, 1999, s. 214.
[96] Krause, Rüdiger, New Developmentsin Data Privacy for Employees in German Law, The Law in the Information and Risk Society, (Ed. GunnarDuttge/SangWon Lee), Universitats verlag Göttingen, 2011, s. 89.
[97] Kuner, Christopher European Data Protection Law, Corporate Compliance and Regulation, Second Edition, Oxford University Press, United Kingdom 2007, s. 18.
[98] Lothar Determann / Robert Sprague: Intrusive Monitoring: Employee Privacy Expectations are Reasonable in Europe, Destroyed in the United States, Berkeley Technology Law Journal, S.26, 2011, s. 1025.

Avrupa'daki devletlerin bu konuya önem verdikleri bilinmektedir. Yaşanan bu gelişmelere paralel olacak şekilde, Avrupa merkezli olan AK ve onun peşi sıra AB'nin kişisel verilerin korunması alanında hukuki düzenlemeler yaptığını görmekteyiz. Tüm bunların sonucunda kişisel verilerin korunması hukuku alanında belki de en büyük katkısı olan 95/46/AT sayılı Yönerge ve onun hemen akabinde yine GDPR'nin bu alanda en gelişmiş düzeyde koruma içeren ve diğer ülkelerle ve uluslararası kuruluşlara esin kaynağı olabilecek evrensel bir metin halinde AB tarafından yürürlüğe konulduğunu görmekteyiz.

2.4.4.1 95/46/AT sayılı kişisel verilerin korunması yönergesi

Kişisel verilerin korunmasına ilişkin en temel metinlerden bir diğeri "*Kişisel verilerin işlenmesi ve bu türdeki verilerin serbest dolaşımı bağlamında bireylerin korunmasına ilişkin 24 Ekim 1995 tarihli ve 95/46/AT sayılı Avrupa Parlamentosu ve Konseyi Yönergesi*" olduğunu net olarak ifade edebiliriz. Bahse konu Yönerge, 1990'lı yılların başında düzenlenerek 24 Ekim 1995'te resmi olarak yürürlüğe girmiştir[99]. Resmi olarak onaylanan bu metnin, doktrin tarafından o zamana kadar olan en etkili ve referans olarak kabul edilen uluslararası belge olarak değerlendirildiği görülmektedir. Bu yönergenin asıl amacına baktığımızda Avrupa Birliği'ne üye devletlerin veri akışını düzenlemek için hazırlanmış olmasına karşın, resmi olarak onaylandığı dönemde dünyanın her yerinde referans olarak kabul edilen bir metin halini almış olmasıdır. Bunun yanında, yönergenin bir diğer ayırt edici özelliği ise AB üye devletlerinde bu yönergenin bağlayıcı ve zorlayıcı bir hukuksal metin olarak kabul edilmesidir[100]. Bu yönerge, dünya çapında etkisini her gün artıran sınır ötesi veri transferleri için sağladığı sistemin bir parçası olarak ön plana çıkmaktadır. Yönerge, AB üyesi olmayan ülkeleri, AB üyesi ülkelerle ticari ve benzeri faaliyetler için anlaşmalar uygulayarak kişisel verilerin güvenliğini sağlamaya teşvik etmektedir. Bu anlamda her alanda kapsayıcı bir yaklaşım sergilemesi nedeniyle, 95/46/AT sayılı Yönergeye olan ilginin dünya çapında arttığını ifade edebiliriz[101].

Esasında Yönergenin amacı, AB üye devletleriyle eş güdümlü olarak yüksek veri koruma standartları oluşturabilmek ve AB üye devletleri arasında kişilerin verilerinin korunması

[99] Daniel J. Solove / Marc Rotenberg / Paul M. Schwartz, Information Privacy Law, Apsen Publishers, New York, 2006, s. 900.
[100]Cunningham, a. g. e., s. 427.
[101] Cunningham, A. g. e. s. 427.

bakımından uygulamayı uyumlu hale getirmek suretiyle, AB üye ülkeleri arasındaki kişisel verilerin serbest dolaşımını kolay hale getirmektir[102]. AB üye devletleri arasındaki kişisel veriler ile ilgili veri ve bilgi akışı, amaçlanan ortak Avrupa pazarı hedefine engel olmaması bakımından çok büyük önem arz etmektedir[103]. Dolayısıyla, yönergenin amaçlarını, kişisel bilgilerin işlenmesi ile ilgili olarak veri sahiplerinin mahremiyetinin korunması ve buna ilave olarak, AB üye ülkelerinin iç hukuklarında verilerin korunmasına dair düzenlemelerin AB yasaları ile uyumlaştırılması olarak özetleyebiliriz[104].

95/46/AT Yönerge m. 3'de ifade edilen kapsama göre, otomatik olarak oluşturulan veya otomatik olarak oluşturulmasa bile dosyalama mekanizmasında depolanan veriler bakımından yönerge uygulama alanı bulmaktadır. Modern dünyada neredeyse verilerin tamamı bilgisayar sistemleri kullanılmak suretiyle otomatik olarak kaydedilmektedir. Diğer taraftan eskiden var olan birtakım manuel tutulan kişisel verilerin ise hızlıca otomatik veri işletim mekanizmalarına taşındığı görülmektedir. Bu nedenle, yönergenin kapsamının ister otomatik yollar ile tutulan veriler olsun isterse de klasik metotlar ile tutulan veriler olsun, otomatik sistemlere aktarıldıklarında tüm verileri kapsayacak şekilde yorumlanması yanlış bir işlem olmayacaktır[105].

95/46/AT Yönergesi kapsamında temel ilkeleri aşağıdaki şekilde sıralayabiliriz[106];

i. Kişinin yanlış verilerinin düzeltilmesi hakkı
ii. Hukuka aykırı işlemelere karşı başvuru hakkı
iii. Kişinin verilerinin kaynağını bilme hakkı
iv. Ticari hususlarda kişisel verilerin kullanılmasına izin vermeme hakkı.

Bunların yanında bir istisna olarak 95/46/AT Sayılı Yönerge'nin m. 3/2'ye göre, milli savunma, kamu güvenliği, ceza hukuku ve devletin güvenliği alanında devletin faaliyetlerinde işlediği kişisel verilere ilişkin uygulama alanı bulamayacağını söyleyebiliriz[107]. Yine ikinci bir istisna olarak da gerçek bireyler tarafından salt kişisel ya da

[102] Rotenberg /Solove/Schwartz A. g. e., s. 900.
[103] Bainbridge, David, Introduction to Informaion Technology Law, Six Edition, Pearson Longman, 2007, s. 499.
[104] Carey, a. g. e., s. 6.
[105] Şimşek, a. g. e., s. 43.
[106] (Çevrimiçi), https://kisiselveri.com/9546ec-turkce , (Erişim tarihi: 13.02.2021).
[107] Küzeci, a. g. e., s. 181.

bireylerin ailelerine yönelik etkinlikleri ile ilgili verilerin işlenmesinde yönerge hükümlerinin uygulanmayacağını ifade edebiliriz. Bu direktif, profesyonel ve ticari olmayan veri işleme kategorisini dikkate almaktadır. Bu anlamda örnek üzerinden hareket edeceksek olursak bireyin telefon kayıt defteri yönerge kapsamında değerlendirilmeyecektir. Yönerge kapsamında değerlendirme konusu olan, bireylerin sosyal medya hesaplarında tuttukları datalar ile ilgili olduğunu net olarak söyleyebiliriz. Bu anlamda bir değerlendirmenin yapılmasının esas nedeni ise bireylerin aktif olarak kullandıkları instagram, linkedin, facebook, twitter gibi uygulamalarda, uygulamayı kullanan kişinin ağında bulunan kişiler ile ilgili konum, ses, resim, görüntü, lokasyon bilgilerini bu hesaplar üzerinde kaydederek her an verileri paylaşarak bu bilgileri alenileştirebilmektedir[108].

95/46/AT sayılı Yönerge m. 29'a göre, kişisel verilerin işlenmesi ile ilgili olarak bir çalışma grubu kurulmuştur. Bu çalışma grubunun gayretleri sonucunda, özel hayatın korunması hakkı üye ülkeler tarafından temel bir hak olarak dikkate alınmış, AB'nin Temel Haklar Şartı'nda verilerin korunması hakkı olarak bu esas üzerine düzenlenmiştir[109].

Bu yönergeye yönelik olumlu eleştiriler arasında bir yandan kişisel verilerin serbest akışının sağlanması, diğer yandan bireylerin temel haklarının korunması ilkeleri yer almaktadır[110].

2.4.4.2 AB temel haklar koşulu

AB Temel Haklar Şartı 07 Aralık 2000 yılında imzalanarak AB devletlerinde vatandaş olmasa dahi mukim olan ve AB vatandaşlığına sahip olan kimselerin; kişisel, siyasi ve ekonomik hakları ilk defa olmak üzere tek bir metinde bir araya getirilmiştir.

Avrupa Birliği Temel Haklar Şartı 7 Aralık 2000 tarihinde imzalanmış olup üye ülkelerde ikamet eden bunun yanında AB üye ülkelerinin vatandaşlığına sahip olan kişilerin; Kişisel,

[108] Küzeci, Elif, Kişisel Verilerin Korunması, Doktora Tezi, Ankara Üniversitesi, Sosyal Bilimler Enstitüsü, Kamu Hukuku Anabilimdalı, Ankara 2010, s. 181-182.
[109] Lucas,Bergkamp, EU Data Protection Policy, The Privacy Fallacy: Adverse Effects Of Europe's Data Protection Policy İn An Information-Dirven Economy, Computer Law and Security Report, Sayı: 18, Yıl: 2002, s. 33.
[110] Gutwirth S., / Poullet, Y., The Contribution of the Article 29 Working Party to the construction of a harmonised European data protection system: an illustration of reflexive governance?, Brussels, 2008, s. 570-580.

siyasi ve ekonomik hakları ilk kez tek bir metinde bir araya getirilmiştir. Tarih 2009 yılını gösterdiğinde bu şart Lizbon Antlaşmasının imzalanması ile tüm üye ülkeler için bağlayıcı bir metin halini gelmiştir. Avrupa Birliği Temel Haklar Şartı m. 8 kişisel verilerin korunması başlığını içermekte olup aşağıdaki gibi düzenlenmiştir[111].

1- "*Herkes, kendisini ilgilendiren kişisel verilerin korunması hakkına sahiptir.*
2- *Bu veriler, dürüst bir şekilde belirli amaçlar için ve ilgili kişinin rızasına veya yasa ile öngörülmüş diğer meşru bir temele dayanılarak işlenir. Herkes kendisi hakkında toplanmış verilere erişme ve bunları düzelttirme hakkına sahiptir.*
3- *Bu kurallara uyulması bağımsız bir makam tarafından denetlenir*."

Bu düzenlemede özellikle dikkat edilmesi gereken husus "herkes" kelimesinin bilinçli olarak tercih edilmesi olmuştur. Bu ifadenin özellikle doktrinde, tercih edilmesine rağmen, düzenlemede korunması amaçlanan kişilerin gerçek kişiler olduğuna dair görüşlerin bulunduğu gözlemlenmektedir[112]. Temel Haklar Şartı'nın kabulünden önce yürürlüğe giren 95/46/AT sayılı Yönergede gerçek kişi ifadesinin açık bir şekilde kullanıldığı görülmektedir. Ancak düzenlemede herkes ifadesinin tüzel kişileri de kapsayabileceği ilgili maddenin lafzi yorumundan anlaşılabileceği düşüncesinde olmamızla birlikte sistematik ve tarihsel yorum geliştirilerek düşünüldüğünde korumanın sadece gerçek kişiler ile sınırlı olabileceğini söylemenin daha gerçekçi olacağı kanaatindeyiz.

AB üye ülkelerinde Lizbon Antlaşmasının 01/12/2009 tarihinde yürürlüğe girmesi ile Temel Haklar Şartı bağlayıcı bir araç halini almıştır[113]. Bu antlaşma ile bireylerin kişisel verilerinin işlenmesini hukuki ve idari yönden denetleyecek olan bir bağımsız kuruma ihtiyaç olduğu kesin olarak anlaşılmıştır.

[111] Küzeci, a. g. e., s. 170-174.
[112] Şimşek, a. g. e., s. 73.
[113] Alina, Kacrorowska, European Union Law, Routledge.Cavendish, Taylor and Francis Group, London and New York, 2009, s. 43.

2.4.4.3 Avrupa birliği genel veri koruma tüzüğü

Teknoloji ve küreselleşmenin hızla gelişmesi sonucunda, 2012 yılında Avrupa Komisyonu tarafından var olan düzenlemelerin tekrardan ele alınması gerektiği düşüncesiyle bir reform önerisi sunuldu. Bu önerinin esas amacı, komisyon tarafından, Genel Veri Koruma Tüzüğünün, kolluk yetkisinin kullanımı ve adli iş birliği konularında 95/46/AT sayılı Yönergenin yerine yürürlüğü girmesidir[114]. Bundan sonraki süreçte tarih 2015 Aralık ayını gösterdiğinde, düzenlenen bu tüzük hakkında AB Komisyonu, Konsey ve Avrupa Parlamentosu arasında bir anlaşmaya varıldı. 2016 Nisan ayında Genel Veri Koruma Tüzüğünün en son sürümü, Avrupa Birliği Konseyi ve Avrupa Parlamentosu tarafından kabul edilerek onaylanmıştır. Daha sonra üye ülkelerce onaylanan, GDPR 04 Mayıs 2016 tarihinde yayınlandı. 24 Mayıs 2016 tarihinden itibaren, üye devletler için geçerli olan düzenlemelere yönelik hazırlıklarını tamamlamaları için iki yıllık bir geçiş dönemi öngörüldü (GDPR, m. 99).

Tüzüğün esas amacının, bireylerin kişisel verilerin korunması anlamında, daha korumacı kriterler belirleyerek AB ülkelerinin bu alanda yapılan düzenlemelere entegrasyonunu hızlandırmak ve AB üyesi olmayan ülkelerde bir şekilde faaliyette bulunan ancak AB üyesi ülkelerle ticari ilişkilerde bulunan şirketlerin bu düzenlemelere entegrasyonunu sağlamak olduğu görülmektedir[115]. AB'nin veri koruma yönergesinden vazgeçerek kişisel verilerin korunması hukukunu tüzük ile düzenlenmesinin esas nedeni tüzüklerin üye devletlerde olduğu şekliyle uygulanması gerektiği ve özellikle hukuken bağlayıcı bir metin olmasından kaynaklanmaktadır[116]. Bu türden bir düzenlemenin yapılmaması durumunda var olan yönerge ancak tavsiye niteliğinde olacaktır. Tüzüğün tüm üye ülkelerce onaylanması veri koruma hukuku bakımından çok önemli bir adım olup yeknesaklığı sağlaması bakımından ayrıca önemlidir. AB üye ülkeleri ile bir şekilde ticaret yapan, ancak AB üyesi olmayan ülkelerin şirketlerinin tek bir hukuki düzenlemeye tabi olması tüzüğün sağlamış olduğu kolaylıklardan biri olarak göze çarpmaktadır. Genel Veri Koruma Tüzüğünün kapsamı,

[114] European Commission (2012), Proposal For A Regulation Of The Europeanparliament And Of The Council On The Protection Of İndividuals With Regard To The Processing Of Personal Data And On The Free Movement Of Such Data (General Data Protection Regulation), COM (2012) 11 Final, Brussels, 25 January 2012.
[115] Taştan, a. g. e., s. 15.
[116] Sanem Baykal, İlke Göçmen, Avrupa Birliği Hukukunun Kaynakları Bakımından Normlar Hiyerarşisi, Prof. Dr. Erdal Onar'a Armağan, Cilt- II, Ankara – 2013, s. 325.

yönergeye göre daha kapsayıcı olarak, Tüzük m. 3'e göre AB hukukuna tabi kuruluşların yanında tabi olmayan, fakat AB üyesi ülkelerin vatandaşlarına mal ve hizmet sunan kuruluşların da yeknesaklık anlamında kapsam dahiline alındığı görülmektedir.

Kişisel verilerin işlenmesine ilişkin ilkeler ise Genel Veri Koruma Tüzük m. 5'de şu şekilde düzenlenmiştir;

i. Kanunilik ilkesine göre veri sahiplerine ilişkin kişisel verilerin hukuka uygun, adil ve şeffaf bir şekilde işlenmesi gerekmektedir.
ii. Amacın belirli olması ilkesine uygun olarak, kişisel veriler belirli, açık ve meşru amaçlar için toplanmalı ve bu amaçlar doğrultusunda işlenmelidir. Ayrıca toplanan veriler işlenirken uyulması gereken hedefler şunlardır:
    a. Kamu yararı gözetilerek arşivleme,
    b. Bilimsel bir gaye için verilerin işlenmesi,
    c. Tarihi araştırmaların yapılması amacıyla verilerin işlenmesi,
    d. İstatistiki amaç güdülerek veri işlenmesi.
iii. İşlenecek verilerin güncel, yeterli ve gerekli olmasının gereği olarak, kişisel veriler mutlaka işlendikleri amaçlarla ilgili olmalıdır. Bunun yanında veri işlemenin yeterli, uygun ve gerekli olanla sınırlı olması gerekmektedir. Veri işlemenin gerektiği şekilde yapılabilmesi için özellikle tutulan verilerin güncel olması büyük önem taşır. Güncel veya doğru olmayan kişisel verilerin derhal silinmesi ve bu anlamda gerekli tüm tedbirlerin alınması ayrıca önem taşımaktadır.
iv. Verilerin belirli bir süre saklanması ilkesinin gereği olarak, kişilerin verilerinin sadece işlenme amaçlarının zorunlu kıldığı süre zarfında teşhis edilmesi gerekmektedir. Bununla birlikte, GDPR'de ifade edildiği üzere, kişisel veriler, verilerin kamu yararı, bilimsel veya tarihi araştırmalar veya istatistiksel faaliyetler için geçerli olduğu ölçüde işlenmesi ve teknik önlemlerin sağlanması halinde uzun süreler boyunca saklanabilir.
v. Gizlilik ve bütünlük ilkelerine uygun olarak, kişisel verilerin yetkisiz veya yasa dışı veri işleme, kaza sonucu kaybolma ve veri imha veya imhasına karşı koruma dahil olmak üzere uygun ve teknik yollarla güvenli bir şekilde işlenmesi gerekir.

Resmi olarak onaylanan tüzük m. 7 "*ilgilinin rızasını*" düzenlemektedir. Bahse konu düzenlemede yer bulan maddenin amaçlarından bir tanesi, bireyin kendi verilerinin toplanması ile alınmış olan rızadan kişinin istediği anda vazgeçebilmesidir. İlgili madde kapsamında verileri depolamak ve bu veriyi güvenli bir şekilde muhafaza etmek ile görevlendirilen veri sorumlusunun istenildiği anda verilerin rıza çerçevesinde hareket edilip edilmediği noktasında ispat görevi bulunmaktadır. Yine bu maddeye göre, kişisel verileri tutmak ve onları muhafaza etmek ile görevli olan veri sorumluları veriyi rızaya uygun olarak topladıklarını ispat ile mükelleflerdir.

Tüzük m. 8'e göre, önleyici hizmetler ve yönlendirme hizmetleri dışında, 16 yaşın altındaki bireylerin bilgilerini toplamak ve internet profili oluşturup kullanmak için ebeveyn izni gereklidir. AB üye ülkelere bu yaş sınırlamasını 13'e kadar çekebilme esnekliği sağlanmıştır.

GDPR'nin getirdiği öncü yeniliklerden biri de kuşkusuz "*unutulma hakkı*"nın[117] tanınmasıdır. Hiçbir üye devlet bu hakkı görmezlikten gelemeyip tanımak zorunda kalmıştır[118]. Verisi işlenen birey, kendisiyle ilgili kişisel verilerin hiçbir sebep göstermeksizin silinmesini veri sorumlusundan talep etme hakkına sahiptir. Tüzüğün onaylanmasından önce çeşitli kararlar olmakla birlikte özellikle ABAD'ın vermiş olduğu karar ilk olmasından kaynaklı olarak unutulma hakkını gündeme taşımıştır[119].

Yukarıda bahsedilen 95/46 EC Sayılı Direktif'in esas alınarak oluşturulduğu ABAD'ın 13/05/2014 tarihli Mario Costeja Gonzalez kararı, unutulma hakkını konu alan ilk karar olması nedeniyle konumuz bakımından oldukça önemli olduğunu söyleyebiliriz.

Dava konusu olayda,[120] Mario Costeja Gonzalez adında İspanyol bir avukatın sosyal güvenlik borçlarını ödeyememesi nedeniyle İspanya Sosyal Güvenlik ve Çalışma

[117] TBBD, 2015, C. 27. S. 116, s. 16.
[118] Taştan, a. g. e., s. 17.
[119] ABAD, C-11/12 sayılı T.13/05/2014 kararı, (Çevrimiçi), https://rm.coe.int/ozelyasam-aile-ceza/16808e940d , (Erişim Tarihi: 04/03/2022).
[120] ABAD, C-11/12 sayılı T.13/05/2014 kararı, (Çevrimiçi), https://curia.europa.eu/juris/liste.jsf?td=ALL&language=en&jur=C,T&num=c-131/12 , (Erişim Tarihi: 04/03/2022).

Bakanlığınca açık artırma usulü ile kendisine ait konutu satılmıştır. La Vanguardia Ediciones SL gazetesi de bu açık artırmaya ilişkin satışı ilan biçiminde yayınlamıştır. Davacı olan Mario Costeja Gonzales'in belirli bir süre sonra kendi ismini arama motoru olan Google'da aratması sonucunda kendi ismiyle ilintili olarak La Vanguardia gazetesinin ilanlarını içeren bağlantı sonuçlarını görmüştür.

Mario Costeja Gonzalez, arama motorunda çıkan haber içeriklerinin gerçeği yansıtmadığını, işlerinin ve maddi durumunun düzeldiğini dolayısıyla bu haberlerin güncelliğini yitirdiğini belirterek haberlerin yer aldığı bağlantı sayfalarının kaldırılmasını, gizlenmesini veya değiştirilmesini istemiştir. Bu sebeple 5 Mart 2010 tarihinde La Vanguardia gazetesini, Google İspanya'yı ve Google Merkez'i İspanyol Veri Koruma Otoritesi'ne şikâyette bulunmuştur. İspanyol Veri Koruma Otoritesi tarafından La Vanguardia'ya ilişkin olan talep, İspanya Sosyal Güvenlik ve Çalışma Bakanlığı'nın zamanında yaptığı açık artırmanın kamuoyu tarafından biliniyor olması ve açık artırmaya katılacak olan kişi sayısını artırma olduğu gerekçesi ile reddedilmiştir. Google İspanya ve Google Merkez'e yapılan başvuruda ise arama motorlarının veri koruma düzenlemeleri çerçevesinde veri işlemekle sorumlu olduklarını ve veri öznesinin isteği halinde verilerin kaldırılmasını ya da erişime engellenmesinin mümkün olabileceği gerekçesiyle kabul etmiştir. Bu sırada Google İspanya ve Google Merkez tarafından İspanyol Veri Koruma Otoritesi kararını İspanya Ulusal Yüksek Mahkemesine taşımıştır. İspanya Ulusal Yüksek Mahkemesi yapılan her iki başvuruyu birleştirerek bazı sorularla birlikte ABAD'a havale etmiştir.

ABAD'a havale edilen hukuki problem; arama motorlarının veri işlemesi bakımından sorumluluğunun olup olmadığıdır. Diğer taraftan yukarıda açıkladığımız, Mahkeme tarafından ABAD'ın Direktif'te yer alan düzenlemeler doğrultusunda cevaplamasını istediği soruların unutulma hakkına ilişkin olarak;

i. Arama motorlarının veri işleyen kabul edilmesi durumunda işlenen veriler üzerinde sorumluluğunun olup olmadığı,
ii. Arama motorlarında yer alan bilgilerin veri öznesinin rızası alınmaksızın ancak hukuka uygun biçimde işlenmesi durumunda verilerin engellenmesi, silinmesi veya düzeltilmesinin istenip istenmeyeceği,

iii. Direktif m.12 (b) ve m.14 (a) hükümleri doğrultusunda veri öznelerinin unutulma hakkı isteyip istemeyeceği,

Sorularını yöneltmiştir. ABAD, ise sonuç olarak vermiş olduğu kararda Direktif'in m. 12 (b) ve m.14 (a); yürürlüğe girdiği tarihte hukuka uygun ve doğru olsa bile geçen zaman içerisinde dava konusu haberlerin üzerinden on altı yıl geçtiğini bu nedenle söz konusu haberlerin hem güncelliğini hem de doğruluğunu yitirdiğini, toplumun bahse konu haberlere erişmesinde menfaatinin olmadığını ve haber içeriklerinin dava açan kişinin özel hayatına ilişkin olduğunu belirterek haberlerin bağlantılı olduğu bütün linklerin kaldırılması gerektiği kanaatine varmıştır[121]. Davacının davasının kabul edilmesi unutulma hakkının ortaya çıkışı için oldukça önemlidir. Haber içeriklerinin kaldırılmasında yukarıda açıkladığımız ve dikkate alınan hususlar aynı zamanda unutulma hakkının ölçütlerini oluşturması bakımından son derece önemlidir. Söz konusu ölçütler, haber içeriğinin doğruluğu, güncelliği, aradan geçen zamanın süresi, haber içeriğine ulaşmada kamu menfaati, çatışan haklar ve ilişkili hakların ilişkisi yönünden önem arz eder.

ABAD, uyguladığı hukuk bakımından Direktif'in 12 (b) "*veri öznesinin erişim hakkı*" ve 14 (1)(a) (95/46 EC Sayılı Direktif m.12(b)) "*veri öznesinin itiraz hakkı*" maddeleri doğrultusunda davacının haber içeriklerinin bulunduğu bağlantıların, arama motorları tarafından kaldırılması gerektiği kararına hükmetmiştir.

Diğer taraftan kararın başında ifade edildiği üzere ABAD, verilen kararın uygulanmasında işaret ettiği Direktif hükümlerinin temelini Avrupa Birliği Temel Haklar Şartı m. 7 ve m. 8 (Avrupa Birliği Temel Haklar Şartı m. 7, m. 8) dayandırmıştır. Avrupa Birliği Temel Haklar Şartı m.7'de "*özel ve aile yaşamına saygı*" ve m. 8 "*kişisel bilgilerin korunması*" hükümleri iki bakımdan önemlidir. Öncelikle her iki hakkın da ayrı biçimde kararda zikredilmesi, kişisel verilerin korunması hakkının, özel hayatın gizliliği hakkından ayrıştırılarak farklı bir hak olarak dikkate alındığını

[121] ABAD, C-11/12 sayılı T.13/05/2014 kararı, (Çevrimiçi), https://curia.europa.eu/juris/liste.jsf?td=ALL&language=en&jur=C,T&num=c-131/12 , paragraf 98.

göstermektedir[122]. Diğer taraftan Direktif hükümlerinde m. 7'de esas teşkil etmesi; mahremiyet hakkının ve özel hayatın korunması hakkının önemini özellikle yineleyerek kişisel verilerin korunması hakkının her ne kadar ayrı bir hak kapsamında değerlendirilse de kişilik hakları ile olan ayrılmaz ilişkisini ortaya koymaktadır.

ABAD, söz konusu davayla ilgili kararını verirken davacıyı koruyucu Avrupa Birliği Temel Haklar Şartı'nın m. 7 ve m. 8 düzenlemeleri ile kamunun çıkarlarını oluşturan toplumun bilgi edinme hakkı ve arama motorlarının ekonomik çıkarları arasında oluşan dengenin dikkatli olunması gerektiğini belirtmiştir[123]. Bu açıdan ABAD tarafından davacının kişilik haklarını önceleyerek kamu çıkarları ve arama motorlarının ekonomik çıkarlarına göre daha ağır basmıştır. ABAD'ın birey eksenli vermiş olduğu bu karar, haklar arasında gözetilecek dengenin adil olmadığı nedeniyle çeşitli eleştirilere maruz kalmış olsa da[124] unutulma hakkının uygulanmasına neden olan ölçütler belirlenmiş olup çatışan haklar dengesinde kişilik hakkının daha ön planda tutulması gerektiği sonucuna ulaşabiliriz[125]. Unutulma hakkı ile ilgili olarak elbette çok daha detaylı sonuçlar ortaya konulabilir ancak tezimizin sınırlarını aşacağı kaygısıyla karar bilgisi vermekle yetinilmiştir. (Melvin v. Reid Kararı[126], Briscoe v. Reader's Digest Kararı[127], Lebach Kararı[128], ünlü bir oyuncu olan başvurucunun haklarında geçmişte hükmedilen hapis cezası haber içeriklerinin kaldırılması kararı[129], unutulma hakkına yer veren ilk Anayasa

[122] Dülger, Murat Volkan, Kişisel Verilerin Korunması Hukuku, Hukuk Akademisi, 2.Baskı, Hukuk Akademisi Yayınları, İstanbul 2019, s. 35-36.
[123] ABAD, C-11/12 sayılı T.13/05/2014 kararı, (Çevrimiçi), https://curia.europa.eu/juris/liste.jsf?td=ALL&language=en&jur=C,T&num=c-131/12 , Pragraf 81, (Erişim Tarihi: 04/03/2022).
[124] Sözüer, s.134.
[125] Hande, Mahmutoğlu, Kişilik Hakkı Çerçevesinde Unutulma Hakkı, Bahçeşehir Üniversitesi Sosyal Bilimler Enstitüsü, Yükseklisans Tezi, İstanbul, 2021, s.77.
[126] Melvin v. Reid, Court of Appeal of California, Fourth District, 112 Cal.App. 285, February 28, 1931, (Çevrimiçi), https://casetext.com/case/melvin-v-reid , (Erişim Tarihi: 03/05/2022).
[127] Briscoe v. Reader's Digest Association, Inc., Supreme Court of California, L.A. 29813, April 02, 1971, (Çevrimiçi), https://law.justia.com/cases/california/supreme-court/3d/4/529.html , (Erişim Tarihi: 03/05/2022).
[128] BVerfG, l BvR 536/72, 05.06.1973, (Çevrimiçi), https://opinioiuris.de/entscheidung/3331 , (Erişim Tarihi: 03/05/2022).
[129] AİHM M.L. ve W.W. v. Almanya, B. No: 60798/10 ve 65599/10, Tarih: 28.09.2018, (Çevrimiçi), https://hudoc.echr.coe.int/tur#{%22fulltext%22:[%2265599/10%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-183947%22]} , Erişim Tarihi: 03/05/2022.

Mahkemesi kararı 03.03.2016 tarihli N.B.B. Kararı[130], cinsel taciz suçu kapsamında mağdurun isminin gizlenmeden, bilimsel bir eserde yer almış olması kararı[131], "Kim Bu Cinsel İstismarcı" başlığıyla yer alan yazının hakaret içermesi iddiasıyla, yazı sahibinin şikâyet edilmesi ile ilgili olan karar[132], silahlı terör örgütüne üye olma suçundan yargılanması ile ilinti olan karar[133], internette çıkan haberlere yönelik erişimin engellenmesi talebine ilişkin karar[134], geçmişlerindeki olumsuz deneyimleri içeren haberlere ilişkin kararı[135].)

GDPR m. 17'ye göre[136] veri sahibi, veri sorumlusundan kendisiyle ilgili kişisel verilerinin gecikmeksizin silinmesini talep etme hakkına sahiptir ve aşağıdaki koşullardan birinin oluşması durumunda veri sorumlusu kişisel verileri gecikmeksizin silmekle yükümlüdür:

(a) *kişisel verilerin toplanma veya işlenme amaçlarıyla ilişkili olarak artık gerekli olmaması*;

(b) *veri sahibinin 6(1) maddesinin (a) bendi veya 9(2) maddesinin (a) bendine göre işleme faaliyetinin dayandığı izni geri çekmesi ve işleme faaliyetiyle ilgili başka bir yasal gerekçe bulunmaması;*

(c) *veri sahibinin 21(1) maddesi uyarınca işleme faaliyetine itirazda bulunması ve işleme faaliyetine yönelik ağır basan meşru bir gerekçe bulunmaması ya da veri sahibinin 21(2) maddesi uyarınca işleme faaliyetine itirazda bulunması;*

(d) *kişisel verilerin yasa dışı biçimde işlenmiş olması*;

(e) *kontrolörün tabi olduğu Birlik veya üye devlet hukukundaki bir yasal yükümlülüğe uygunluk sağlanması amacı ile kişisel verilerin silinmesinin zorunlu olması;*

(f) *kişisel verilerin 8(1) maddesinde atıfta bulunulan bilgi toplumu hizmetlerinin sağlanması ile ilgili toplanmış olması."*

---

[130] Anayasa Mahkemesi N. B. B. Kararı, Başvuru No: 2013/5653, Karar Tarihi: 03.03.2016, (Kazancı)
[131] Yargıtay Hukuk Genel Kurul Kararı, T. 17.06.2015, E. 2014/56, K. 2015/1679, (Kazancı).
[132] Yargıtay Ceza Genel Kararı, T. 30.10.2018, E. 2016/18-1169, K. 2018/490, (Kazancı).
[133] Yargıtay, 16. CD. T. 07.06.2016, E. 2016/927, K. 2016/3874, (Kazancı).
[134] Yargıtay, 19. Ceza Dairesi, T. 11.03.2019. E. 2018/8285, K. 2019/5447, (Kazancı).
[135] Yargıtay, 19. Ceza Dairesi, T. 19.10.2020, E. 2019/28149, K. 2020/13099, (Kazancı).
[136] (Çevrimiçi), https://www.kisiselverilerinkorunmasi.org/wp-content/uploads/2017/09/GDPR-T%C3%BCrk%C3%A7e-%C3%87eviri-AB-Bakanl%C4%B1%C4%9F%C4%B1.pdf , (Erişim tarihi, 01/03/2022).

Yukarıda bahsedilen durumların oluşması durumunda ilgili kişinin kişisel verileri herhangi bir gecikme olmaksızın silinmesi gerekmektedir. Ancak bu hükümlerin istisnası olarak, kamu düzeni, kamu yararı, kamu sağlığı gibi nedenlerin olması halinde silme talebi ilgili Tüzük m. 17/3 uyarınca kabul edilmeyecektir (GDPR, m. 17/3). Yukarıda sayılan koşullardan herhangi birinin gerçekleşmesi silme işlemi için yeterli olacaktır. Dolayısıyla veri sorumlusu bu sayılan koşulların dışındaki gerekçelerle gelen silme talebini kabul etmeyecektir.

GDPR'nin getirdiği en önemli yeniliklerin bir diğeri ise "Tasarımla Veri Koruma" (Privacy by design) ve "Varsayılan Ayarlarla Veri Koruma" (Privacy by Default) ilkelerinin benimsenmesi olmuştur. Tasarım ile veri koruma deyiminden kasıt, veri işleyen veya bu hususa ilişkin teknoloji üreten-kullanan kimselerin ürünlerinin tasarım aşamasındayken yüksek güvenlikli olması gerekliliğidir[137]. Varsayılan ayarlar ile korumadan kasıt ise, alınan ürün ve hizmetin kişisel verilerin korunmasına ilişkin gerekli olabilecek şekilde gizlilik politikalarına ve ayarlarına riayet etmesidir. Örneğin, Facebook adlı sosyal paylaşım sitesine üye olunduğunda ilgili sitenin, yani şirketin varsayılan ayarlarında, üyenin her türlü bilgisinin üçüncü kişilerin müdahalesine ve erişimine kapalı olması gereklidir. Üye eğer ayarları değiştirirse bu "rıza" kapsamında değerlendirilerek ihlal oluşmayacaktır[138]. Örneğin, Apple, güvenlik rehberinde[139] kişisel verilerin korunmasına ilişkin azami ölçüde dikkat edildiğini belirtmiştir. Burada hukuk tekniği bakımından adı geçen ilkelerin kabulünde bir beis olmasa dahi bu ilkelerin pratikte, yani hayatın içinde, nasıl uygulanacağına ilişkin ciddi sorunlar olduğu görülmektedir[140].Zira bu sistemlerin kurulumu, denetimi hukuk tekniğinden ziyade bilişim teknolojisi ile çözülebilecek bir sorun olarak göze çarpmaktadır. Ancak yine de GDPR'nin, günümüz teknolojisinin geldiği noktayı gözeterek almış olduğu bu tedbirler olumlu mütalaa edilmelidir. Gündelik hayatımızda ve rutin eylemlerimizde, kişisel verilerimizin rızamız dahilinde olsun veya olmasın en çok kaydedildiği, kullanıldığı alan olarak internet bazlı uygulamaların olduğunu söylemek yanlış olmayacaktır. Bu nedenle

[137] Nilgün, Başalp, Avrupa Birliği Veri Koruması Genel Regülasyonu'nun Temel Yenilikleri, MÜHF, Cilt: 21, Sayı: 1, s. 92.
[138] Taştan, a. g. e., s. 19.
[139] (Çevrimiçi), https://support.apple.com/tr-tr/guide/security/welcome/web , s. 19, (Erişim tarihi: 01/03/2022).
[140] Gerrit, Hornung, "A general data protection regulation for Europe? Light and Shade in the Commission's Draft of 25th January 2012.", Script-ed 9, No:1, s. 75.

Facebook, Youtube, Twitter ve İnstagram gibi bazı popüler sosyal medya uygulamalarının GDPR'de kendisine yer bulan "varsayılan ayarlar" ile kullanıcılarına asgari düzeyde kişisel verilerinin korunduğuna dair taahhütte bulunması gerekmektedir. Böylelikle kişisel verileri daha kaynağında iken bir sözleşme ile kişiler koruma altına almaktadır.

"*Veri koruma görevlisi*" kavramı, GDPR ile kişisel verileri koruma hukuku literatürüne kazandırılmıştır[141]. Veri koruma görevlisi unvanı ile görevlendirilen kişi, kişisel verilerin, hangi amaçla işlendiği ile ilgili hususlarda ve bu işleme işlemi gerçekleştirilirken hangi araçların kullanılacağına ilişkin takdir hakkı bulunan kişiyi ifade eder. Bu kişi yasal olarak gerçek veya tüzel kişi olabilmektedir. Görevlendirilen bu kişilere yasal olarak birtakım sorumluluklar verilebilir. Bu yükümlülükler; aydınlatma, gizlilik vs. şeklinde ifade edilebilir[142].

2.4.4.4 Elektronik veriyi koruma kapsamında 2002/58/EC sayılı Avrupa Birliği direktifi

Avrupa Parlamentosu ve Avrupa Konseyi 12 Temmuz 2002 tarihinde "*Elektronik Veriyi Kullanmaya İlişkin İlişkin Direktifi"* kabul etmişlerdir. 2002/58/EC sayılı bu direktifin esas amacı teknolojik gelişmeler doğrultusunda elektronik telekomünikasyon alanında temel hak ve özgürlükleri koruyabilmektir[143].

2.4.4.5 Avrupa Birliği vatandaşlık hakkı direktifi

Avrupa Birliği Vatandaşlık Hakkı Direktifi olarak da bilinen 2009/136/EC sayılı yönerge, 2002/58/EC sayılı Elektronik Veri Koruma yönergesindeki kişisel verilerin güvenirliliği ile ilgili bulunan noksanlıkları gidermek için kabul edilen bir yönergedir[144].

2.4.4.6 Europol antlaşması ve kişisel verilerin korunması

AB'nin kolluk birimi olarak kurulan ve Hollanda'nın Lahey şehri olan Europol 1998 senesinde resmi faaliyetlerine başlamıştır. Europol'ün misyonu, organize suçların

[141] Taştan, a. g. e., s. 20.
[142] (Çevrimiçi), https://www.kvkk.gov.tr/Icerik/2032/Veri-Sorumlusu-Kimdir , (Erişim Tarihi: 01/03/2022)
[143] Hayrunisa, Özdemir, Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Doktora Tezi, Ankara, 2009, s. 43.
[144] Baykal, Göçmen, a. g. e., s. 44.

önlenmesine, soruşturulmasına ve kovuşturulmasına yardımcı olmak, iki veya daha fazla üye devleti etkileyen terörizm ve diğer ciddi suç türleriyle mücadele etmede gerekli desteği sağlamaktır. Uluslararası alanda faaliyet gösteren siber suç örgütleriyle yaşanan yeni gelişmeler sonucu, 1 Ocak 2013 tarihinde resmi olarak Europol'de Avrupa Siber Suç Merkezi üye devletlerin katkılarıyla kurulmuştur.

Üye ülkeler tarafınca onaylanan Europol Antlaşması'nın maddeleri incelendiğinde kişisel verilerin işlenmesi ile ilgili çok önemli düzenlemelere yer verilmiş, bu düzenlemeler doğrultusunda üye ülkelerin veri değişim sistemine entegre olabilmesi için Avrupa Konseyi'nin 108 sayılı Sözleşmesi'ni kabul etmek şartıyla ulusal hukuklarında kişisel verilerin korunması ile ilgili farklılıkların oluşmaması için standart oluşturulması gerektiği ifade edilmiştir[145].

2.4.4.7 Eurojust

Eurojust 2002 yılında Lahey'de kurulmuştur. Avrupa Birliğine üye olan devletlerin kendi aralarında anlaşarak, nitelikli suçların soruşturma ve kovuşturma safhasında adli olarak her türlü işbirliği yapılmasını özellikle teşvik eden Avrupa Birliği organıdır[146].

Eurojust kapsamında nitelikli ve ağır suçların soruşturulması, kovuşturulması aşamalarında kişisel verilerin toplanması ve işlenmesi yapılabilmektedir. Ancak kişisel verilerin işlenmesinde birtakım sınırlamalar bulunmaktadır. Eurojust kapsamında, suç işleyen veya suç işlediğine dair ciddi şüphelerin bulunduğu ya da hüküm giyen bireylerin bilgilerine ulaşılabilecektir. Ayrıca Eurojust kapsamında herhangi bir şekilde tanıklıkta bulunan veya bu tür suçların mağduru olan kişisel verilerinin de işlenmesi mümkün olacaktır[147]. Kişisel verilerin paylaşılması söz konusu olduğunda Eurojust Veri Koruma esasları, konsey kararları ve ikili anlaşmalarda düzenlenen kurallar ve sınırlamalara uygun olarak işlemler yapılması gerekmektedir[148].

[145] Şimşek, a. g. e., s. 75.
[146] Avrupa Birliği Konseyi, 28 Şubat 2002 tarihli ve 2002/187/JHA sayılı Kararı.
[147] Avrupa Veri Koruma Hukuku El Kitabı s. 108.
[148]Avrupa Veri Koruma Hukuku El Kitabı, s. 110.

2.4.4.8 Schengen antlaşması ve kişisel verilerin korunması

Schengen Anlaşması 1986 yılında yürürlüğe girmiştir. Antlaşmanın esas amacı, taraf olan ülkelerin sınır kontrollerinin kaldırılmasıdır. Yapılan bu antlaşmaya göre, taraf olan devletlerin SIS II isimli otomatik sisteme, bireyin kişisel verisi olan parmak izi ve fotoğraf veya ulaşım araç bilgilerini, dolayısıyla bireylere ve objelere ilişkin her türlü uyarıcı nitelikli bilgilerini; soruşturma ve kovuşturma kapsamında tutuklama, iade, teslim için aranan kişilere ait verilerin sisteme girilmesi vazifeleri bulunmaktadır. Ancak girilen sistemdeki verilere sadece taraf olan devletler ulaşabilecektir. Sisteme kaydedilen tüm bu kategorik verilerin güvenliğinden var olan sisteme işleyen ulusal idarelerin sorumlulukları bulunmaktadır[149].

2.5. YABANCI HUKUKTA KİŞİSEL VERİLERİN KORUNMASI

2.5.1. Genel Olarak

Avrupa ülkelerinde kişisel verilerin korunmasına ilişkin ilk olarak 1970'li yıllarda başlayan tartışmalar, kişisel verilerin korunması hukukunun gelişmesini ve uluslararası ve ulusal düzeyde mevzuat çalışmalarını yapılmasını sağlamıştır. Yaşanan bu gelişmeler, tartışmayı farklı bir noktaya taşıyarak özellikle 1995 yılında kabul edilen 95/46/AT sayılı Avrupa Birliği Yönergesi'nin kişisel verilere yönelik eşdeğer koruma sağlamayan ülkelere veri transferini yasaklamasıyla, zaman içerisinde Avrupa Birliği üyesi olmayan ülkelerde de tartışılmaya başlanmış ve bu ülkelerde kişisel verilerin korunması düzenlemelerini Avrupa Birliği standartlarıyla birebir aynı olmasa da bu alanda çeşitli iyileştirmelerde bulunmuşlardır. Avrupa Birliği standartlarıyla uyumlu hale getirme sürecinde özellikle ABD'deki ticari kuruluşlar kişisel verilerin aktarımı konusunda çeşitli sorunlar yaşamışlar ve yapılan düzenlemelerle bu sorunların giderilmesi içim adımlar atılmıştır. Bu bağlamda bahse konu tarihlerde ülkemiz, yaşanan gelişmelerin gerisinde kalmıştır[150]. 1981 yılında 108 sayılı Avrupa Konseyi Sözleşmesi'ni imzalamasından sonra bu Sözleşme'yi iç hukukuna uyarlamayarak fiili olarak onaylamamıştır. Tarih 7 Nisan 2016 tarihini gösterene kadar kişisel verilerin korunmasına ilişkin herhangi bir özel kanun çıkarılmamıştır. Gelinen

[149] Avrupa Veri Koruma Hukuku El Kitabı, s. 11.

[150] Korkmaz, İbrahim, Kişisel Verilerin Ceza Hukuku Kapsamında Korunması, Doktora Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku (Ceza ve Ceza Usul Hukuku) Anabilim Dalı, Ankara 2017, s. 233.

noktada, Avrupa Birliği ülkeleri ve iç hukuklarında AB veri koruma standartlarına sahip olan ülkeler açısından, ülkemizi eşdeğer veri koruma standardı olmayan ülke durumuna düşürmekteydi.

1995 yılından kabul edilen 95/46/AT sayılı Avrupa Birliği Yönergesi, kişisel verilerin korunması ile ilgili yapılan düzenlemelerin iç hukuklarında uygulanmasını zorunlu kılmakta ise de, nasıl ve ne şekilde uygulayacakları konusunda taraf olan ülkelere bir özgürlük alanı tanımıştır[151]. Bu sebepten Avrupa Birliği üye devletleri arasında kişisel verilerin korunması ile ilgili düzenlemelerde bazı farklılıkların bulunması kaçınılmazdır. Çalışmamızın bu bölümünde bahse konu devletlerde, kişisel verilerin korunması hukukuyla ilgili önemli gördüğümüz düzenlemeleri incelemeye çalışacağız.

2.5.2. Fransa

1958 tarihli Fransa Anayasası'nda Özel hayatın gizliliği hakkı ve kişisel verilerin korunması hakkı özel olarak düzenlenmiştir. Bunun dışında Fransa Anayasa Mahkemesi, 1994 yılında vermiş olduğu bir kararda özel hayatın gizliliği hakkının Anayasa'da örtülü şekilde bulunduğunu ifade etmiştir[152]. Kişisel veriler Fransa'da ilk olarak 1978 tarihli Bilgi Teknolojisi, Veri Dosyaları ve Bireysel Özgürlükler Kanunu[153] ile koruma altına alınmıştır.

1978 tarihinde düzenlenen veri koruma hukuku diğer Avrupa ülkelerine kıyasla daha önce ele alınmasına rağmen Avrupa Birliği Veri Koruma Yönergesi'nin Fransa'da kanun haline getirilmesinin 2004 yılına kadar yapılmadığını görmekteyiz. 1978 tarihli Kanun 6 Ağustos 2004 tarihli Kişisel Verilerin İşlenmesinde İlgili Kişilerin Korunması Kanunu[154] ile büyük bir kısmı değiştirilmek suretiyle 95/46/AT sayılı Avrupa Birliği Yönergesi Fransa'da kanun haline getirilmiştir. 1978 tarihinde kabul edilen Kanun, yalnızca gerçek kişiler için bağlayıcı olup, tüzel kişiler bakımından kapsam dışında bırakılmıştır[155]. 1978 tarihli yapılan

[151] Klosek, Jacqueline, Data Privacy in the Information Age, Quorum Books, 2000, s. 51.
[152] Fransa Anayasa Mahkemesi'nin 94-352 numaralı ve 18 Ocak 1995 tarihli kararı.
[153] 1978 tarihli Bilgi Teknolojisi, Veri Dosyaları ve Bireysel Özgürlükler Kanunu, (Çevrimiçi), https://www.cnil.fr/ , (Erişim Tarihi: 03/05/2022).
[154] Kişisel Verilerin İşlenmesinde İlgili Kişilerin Korunması Kanunu, https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000441676/ , (Erişim Tarihi: 03/05/2022).
[155] 1978 tarihli Bilgi Teknolojisi, Veri Dosyaları ve Bireysel Özgürlükler Kanunu madde 2.

düzenlemeye göre veri sorumluları, işledikleri kişisel verilere ilişkin Fransa Veri Koruma Komisyonu (CNIL)'a bir bildirimde bulunmak zorundadırlar[156].

Fransız kişisel verileri koruma hukukunun büyük bir bölümü Fransız Ceza Kanunu'nda[157] düzenlenmiştir. 1978 tarihli Bilgi Teknolojisi, Veri Dosyaları ve Bireysel Özgürlükler Kanunu'nun ihlali durumunda ceza hukuku kapsamında uygulanan yaptırımlar, Fransa Ceza Kanunu'nun Kişilere Karşı Suçlar isimli İkinci Kitabı'nın, İnsana Karşı İhlaller isimli İkinci Başlığı'nın, Kişilere Karşı İhlaller isimli altıncı bölümünde, 226-16–226-24 maddeleri arasında gerekli düzenlemeler yapılmıştır.

Yapılan düzenlemeler incelendiğinde Fransız Ceza Kanunu'nda, kişisel verilerin korunması bağlamında düzenlenen suçlar için ağır cezaların öngörüldüğü görmekteyiz. Bu açıdan Türk Ceza Kanunu'nda düzenlenen suçlarla mukayese edildiğinde, Türk Ceza Kanunu'nda düzenlenmiş olan cezaların daha hafif olduğu görmekteyiz[158]. Fransız Ceza Kanunu diğer ülkelerin ceza kanunu ile karşılaştırıldığında, kişisel verilerin hukuka aykırı olarak kaydedilmesi ve saklanması konusunda, hassas nitelikli kişisel veriler bakımından herhangi bir ayrımın yapılmamış olması dikkat çekmektedir[159].

2.5.3. Almanya

Alman Anayasası'nda[160] kişisel verilerin korunması konusunda hususi bir yasal düzenleme bulunmayıp, Özellikle Doğu ve Batı Almanya'nın birleşmesinden sonra, Alman Anayasası'nın değiştirilmesi sürecinde kişisel verilerin korunmasıyla ilgili özel bir yasal

---

[156] Fransa Bilgi Teknolojisi, Veri Dosyaları ve Bireysel Özgürlükler Kanunu madde 22; Topaloğlu, Mustafa, Bilişim Hukuku, Karahan Kitabevi, Adana 2005, s. 166.

[157] Fransız Ceza Kanunu'nun İngilizce metni için bakınız. (Çevrimiçi), https://www.legislationline.org/download/id/3316/file/France_Criminal%20Code%20updated%20on%2012-10-2005.pdf , (Erişim Tarihi: 03/05/2022).

[158] Gültekin, Nil Melek, Kişisel Verilerin Ceza Hukuku Yönünden Korunması, Yüksek Lisans Tezi, Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, İstanbul 2012, s.39.

[159] Gültekin, a. g. e., s.39.

[160] Almanya Anayasası'nın (Almanca, Grundgesetz) İngilizce metni için bakınız. (Çevrimiçi), https://www.gesetze-im-internet.de/englisch_gg/ , (Erişim Tarihi: 03/05/2022).

düzenlemenin ilgili metinde yer alması için çaba gösterilse de, siyasi iktidar mensupları tarafından sürekli reddedildiğini görmekteyiz[161].

Almanya'nın kişisel verileri koruma konusunda Avrupa Birliği ülkeleri arasında en kısıtlayıcı kanuni düzenlemelerinden birine sahip olduğunu söyleyebiliriz. Dünya genelinde ilk veri koruma düzenlemesi 1970'te Almanya'nın Hessen eyaletinde yürürlüğe girmiştir[162]. Tarihler 1977 yılını gösterdiğinde ise, Almanya genelinde kişisel verilerin korunmasını amaçlayan Federal Veri Koruma Kanunu[163] yürürlüğe girmiştir. Kişisel verilerin korunması bakımından Almanya'da üç temel kanuni düzenlemenin olduğunu söyleyebiliriz. Bunlardan ilki Alman Ceza Kanunu, ikincisi Alman Ceza Muhakemesi Kanunu, üçüncüsü ise hususi bir kanuni düzenleme niteliğinde olan Alman Veri Koruma Kanunu'dur.

Avrupa Topluluğu içerisinde düzenlenen yasal düzenlemelerin uygulanmadığı ülkelere, Kişisel verilerin uluslararası kuruluşlara taşınması söz konusu olduğunda, şayet bu kuruluşlar gerekli ve yeterli koruma seviyesini (BDSG m. 4b-3) sağlayamıyorlarsa ve transferin yapılmaması için ilgili kişinin transferin yapılmasından daha üstün yararı varsa kişisel veriler transfer edilmemelidir. Almanya devletinin güvenliği, uluslararası düzeyde yükümlülüklerin yerine getirilme zorunluluğunun bulunması, kriz yönetimi, çatışmaların önlenmesi ya da insani yardım nedenleriyle kişisel verilerin transferi istisna kapsamında gerçekleştirilebilir. İfade edilen bu durumlarda kişisel verilerin transfer edildiği ülkelerde yeterli koruma seviyesi olmasa bile veriler transfer edilebilir (BDSG m. 4b-2).

Almanya Federal Veri Koruma Kanunu m. 43'te yasal düzenlemeye aykırı davranışlar olması durumunda uygulanacak idari cezalar, m. 44'te ise adli cezalar düzenlenmiştir[164]. Bu

[161] Akıllıoğlu, Tekin, İdari Usul ve Kişisel Verilerin Korunması, Maltepe Üniversitesi Hukuk Fakültesi Dergisi, Özel Sayı 2008, s. 15; KÜZECİ, Elif, Kişisel Verilerin Korunması, Turhan Kitabevi, Ankara 2010, s. 49.

[162] Kuner, Cristopher, European Data Privacy Law, 13; Topaloğlu, Mustafa, Bilişim Hukuku, Karahan Kitabevi, Adana 2005, s. 166; Dağ, Güray, Kişisel Verilerin Ceza Muhakamesi Hukukunda Delil Olarak Kullanılması, Doktora Tezi, Marmara Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, İstanbul 2011, s. 13; CATE, Fred H., Privacy in the Information Age, Brookings Instution Press, ABD. 1997, s. 32.

[163] Almanya Federal Veri Koruma Kanunu'nun (Almanca, Bundesdatenschutzgesetz) İngilizce metni için bakınız. (Çevrimiçi), https://germanlawarchive.iuscomp.org/ , (Erişim Tarihi: 03/05/2022).

[164] Güven, Bilhan, Hasta Bilgilerinin Gizliliği Prensibi, Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, 2010, s. 48.

bakımdan kişinin bilerek ya da ihmalle Kanun'un 43/1. maddesinde sıralanan eylemlerden birisini gerçekleştirmesi halinde bir idari kabahat söz konusu olacaktır[165] (BDSG m. 43/1). Madde 43/2'de yapılan düzenlemede ise diğer idari kabahatlerin düzenlendiğini görmekteyiz. İlgili Kanuni düzenlemesinin (BDSG) m. 43/1'de idari kabahatlerin işlenmesi halinde 50,000 €'a kadar, m. 43/2'de ise idari kabahatlerin işlenmesi durumunda 300,000 €'a kadar para cezası verilebileceği ifade edilmiştir. Karar verilen para cezası miktarı failin kabahati işlemesinden elde ettiği finansal kazançtan daha büyük olmalıdır. Bu durumda para cezası limitleri daha düşük olursa bu limitler arttırılabilmesi söz konusu olacaktır (BDSG m. 43/3).

Alman Ceza Kanunu[166] kişisel verilere karşı suçlar, Kanun'un Kişisel Yaşam ve Gizli Alanın İhlali başlıklı 15. Kısmında yer alan m. 201, m. 202-a ve m. 205'te yer almaktadır[167]. İlgili Ceza Kanunu'nda veri casusluğu başlıklı m.202-a'nın birinci fıkrasında, yetkisiz erişime karşı korunan verileri, hukuka aykırı bir biçimde kendisi ya da bir başkası için ele geçirirse, üç yıla kadar hapis ya da para cezası cezalandırılabileceği düzenlenmiştir. m. 202-a'nın İkinci fıkrasında ise bahse konu verilerin yalnızca elektronik veya manyetik olarak saklanan ve transfer edilen veriler olduğu ifade edilmiştir[168]. Bahse konu düzenleme, bireylerin kişisel yaşamları, gizli alanları, özel hayatlarını korumak dışında, depolanan ve açıklanan kişisel verilerin gizli tutulmasındaki kişinin üstün yararını da güvenceye alabilmektedir[169]. Tanımlanan düzenlemeyle ileride mağdur olabilecek kişilere ilişkin saklanmış ve hususi olarak güvenceye alınmış kişisel veriler korunmaktadır.

Alman Ceza Kanunu (StGB) m. 202-a düzenlemesinde bilinçli olarak veri kavramının tanımlanmadığını görmekteyiz. Burada özellikle dikkat edilmesi gereken verilerin hangi araçlarla ve nasıl depolanmış olduğudur. Hatta bu bağlamda verinin içeriğinin bile önemi yoktur[170].

---

[165] Güven, s. 49.
[166] Alman Ceza Kanunu (Almanca, Strafgesetzbuch, StGB) Tarihi: 13 Kasım 1998, Federal Hukuk Gazetesi [Bundesgesetzblatt] I p. 3322, (Çevrimiçi), http://www.gesetze-im-internet.de/englisch_stgb/ , (Erişim Tarihi: 03/05/2022).
[167] Ünver, Yener, Kişisel Verilerin Korunması, Galatasaray Üniversitesi Hukuk Fakültesi, S.1, 2008, s. 175.
[168] Ünver, Yener, Kişisel Verilerin Korunması, Galatasaray Üniversitesi Hukuk Fakültesi, S.1, 2008, s. 176.
[169] Ünver, a. g. e., s. 177.
[170] Ünver, a. g. e., s. 177.

Alman Ceza Kanununa göre suç oluşturan eylem, failin kişiye ait verileri kendisi ya da başkası için elde etmesidir. Fail bahse konu eylemi gerçekleştirirken yetkisinin bulunmaması gerekir[171]. Bunun dışında ilgili kişinin rızasının bulunmaması gerekir. İlgili kanuni düzenlemeye göre bu suç kasten işlenebilir olup, failin bu eylemlerini hangi amaçla işlediğinin bir önemi yoktur. Ayrıca suç içtima hallerinin uygulanmasına elverişlidir[172].

2.5.4. İtalya

Bir diğer Avrupa Birliği ülkesi olan İtalya, 108 sayılı Avrupa Konseyi Sözleşmesi'ni 1981 yılında onaylamasına rağmen, 1996 yılında 675 sayılı Bireylerin ve Diğer Kişilerin Kişisel Verilerinin İşlenmesine Karşı Korunması Kanunu'nu[173] kabul edilmesine kadar kişisel verilerin korunması konusunda bir düzenleme yapılmamıştır. 675 sayılı düzenleme aynı zamanda 95/46/AT sayılı Avrupa Birliği Yönergesi'ni İtalya'da yürürlüğe sokmuştur. 2003 tarihinde yapılan Kanuni düzenleme ile 1996 yılından itibaren kişisel verilerle ile ilgili olarak yapılmış tüm düzenlemeleri tek bir düzenlemede birleştirmiştir. İtalya'da kişisel verilerin korunmasından sorumlu kurum İtalya Veri Koruma Komisyonu'dur[174].

Veri Koruma Kanuni düzenlemesinde kişisel verilerin korunmasına ilişkin hukuk dışı eylemlere karşı uygulanacak yaptırımlar m. 161 ve m. 172 arasında düzenlenmiştir. İdari kabahatler m. 161 ile m. 166 arasında düzenlenmiştir. İtalya Veri Koruma Komisyonu m. 166'a göre söz konusu yaptırımların uygulanması bakımından yetkili ve sorumludur.

İtalyan Veri Koruma Kanunu'nda m. 167 ve m. 172. arasında kişisel veri suçları düzenlenmiştir.

---

[171] Ünver, a. g. e., s. 179.
[172] Ünver, a. g. e., s. 120.
[173] Bireylerin ve Diğer Kişilerin Kişisel Verilerinin İşlenmesine Karşı Korunması Kanunu, Kanun Numarası: 675/1996, Yürürlüğe Giriş Tarihi: Mayıs 1997, (Çevrimiçi), https://www.dataguidance.com/notes/italy-data-protection-overview , (Erişim Tarihi: 03/05/2022).
[174] İtalya Veri Koruma Komisyonu'nun (İtalyanca, Garante per la protezione dei dati personali) resmi web sitesi (Çevrimiçi), https://www.garanteprivacy.it/web/garante-privacy-en/home_en , (Erişim Tarihi: 03/05/2022)

2.5.5. Amerika Birleşik Devletleri

Amerikalıların özel hayatın korunması bakımından Avrupalı ülkelerden farklı bir bakış açısı içinde olduklarını ifade edebiliriz. Zira Amerikalılara göre özel hayat devletin kişiyi kendisiyle baş başa bırakması ve hiçbir müdahalesinin olmaması ile korunabileceği düşünülmektedir. Dolayısıyla bu durumda kişinin özel hayatının korunması için devletin bir tedbir almasına gerek yoktur. Amerika Birleşik Devletleri'nde kişisel veriler, federal kanunlar, ABD Anayasası, eyalet kanunları, teamül hukuku ve bazı eyalet anayasaları tarafından oluşan bir yasal düzenleme koruma sistemi aracıyla korunmaktadır. Bu sebeple mevcut durum, Avrupa Birliği'ndeki uygulanan tekdüze koruma siteminden ayrılmaktadır[175]. Amerika'daki bu dağınık koruma düzeni, çeşitli yasal düzenlemelerin kişisel verilerin korunmasına farklı yaklaşımları sebebiyle kişisel verilerin korunması bakımından zayıflık oluşturmaktadır[176]. Bunun dışında ABD Anayasası kişisel verilerin korunması konusunda açık hükümler içermez, bu sebeple yeterince koruma sağlamadığını ifade edebiliriz[177]. Avrupa Birliği ülkeleri ile ABD arasında kişisel verilerin korunması bakımından bir diğer fark, 95/46/AT sayılı Avrupa Birliği Yönergesi'nin pazar ekonomisi üzerinde daha kısıtlayıcı düzenlemeler barındırmasıdır.

Amerika Birleşik Devletleri'nde süreç içerisinde oluşan anlayışa göre, teknolojik gelişmelerin kişisel verileri daha kolay ulaşılabilir hale getirmesinin, kişilerin bu alanda kendilerine ait olan veriler ile ilgili olarak karar almalarını, böylece kişisel verilerin bireylerin sorumluluğunda olmasını sağlayacağı kabul edilmiştir. Bu bağlamda Amerika Birleşik Devleti özel düzenlemelerin daha iyi koruma sağlayacağı esasını benimseyerek, merkezi olmayan, bölünmüş ve dar kapsamlı özel kanuni düzenlemelerle bahse konu alanı düzenlediğini ifade edebiliriz.

---

[175] Cate, Fred H., Privacy in the Information Age, Brookings Instution Press, ABD. 1997, s. 49,50.

[176] Heısenberg, Dorothee, Negotiating Privacy; The European Union, the United States and Personal Data Protection, Lynne Rienner Publishers, London 2005, s. 65

[177] Topaloğlu, s. 174; Ersoy, Uğur, Bir İnsan Hakları Kavramı Olarak "Kişisel Verilerin Korunması", Yüksek Lisans Tezi, Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Kamu Yönetimi Anabilim Dalı, Ankara 2009, s. 79; Heısenberg, s.33.

Amerika Birleşik Devletleri'nde 1966 yılında çıkarılan Bilgi Edinme Özgürlüğü Kanunu[178] ile bireylere, devlet tarafından kendileri ile ilgili olarak toplanmış olan kişisel verilere ulaşabilmeleri hakkı tanınmış, ardından 1974 yılında Özel Hayatın Gizliliği Kanuni düzenlemesi[179] çıkarılarak, devletin vatandaşları ile ilgili kişisel verilerini toplamalarına sınırlama getirilmiştir[180]. Bu iki kanuni düzenleme birlikte değerlendirildiğinde, esas amacın devlet kurumları tarafından toplanmış olan kişisel verilerin devlet ve üçüncü kişiler tarafından hukuka aykırı kullanılmasının engellenmesi olduğu görülmektedir. Bu düzenlemelerin yanında ABD özel sektör için kapsayıcı bir kanuni düzenleme yapmaktan özellikle kaçınarak, bu sektörde kişisel verilerin korunmasını rehber ilkelere ve özel düzenlemelere bırakmıştır[181].

Amerika Birleşik Devletleri'nde var olan sistem uyarınca, anayasal haklar bir bakımından devletin kişilerin haklarına müdahalesini engellemekte diğer bakımdan da kişilerin haklarını özel sektöre karşı koruduğunu söyleyebiliriz. Dolayısıyla, genel koruma sağlayan bir kanuni düzenleme yerine, kişisel verilerin çeşitli sektörlerde korunması konusunda çeşitli konuları düzenleyen birçok federal kanuni düzenleme yürürlüğe konulmuştur[182].

Avrupa Birliği ülkelerinde kişisel verilerin korunmasına yönelik önemin artması ve bu alanda somut adımlar atılarak Rehber İlkeler ve sözleşmelerin yürürlüğe girmesi, özellikle 95/46/AT Sayılı Yönerge'nin yürürlüğe girmesinden sonra bu sözleşmeleri imzalayan ülkelerin de iç hukuklarında gerekli düzenlemeleri yaparak ortak koruma kararlarına uyum sağlamaları neticesinde, kişisel verilere yönelik eşdeğer korumadan yoksun diğer ülkelere aktarılmamasıyla ilgili mevcut kararlar ABD'nin kişisel verilerin korunması alanında daha koruyucu bir kanuni düzenleme yapma gereksinimini ortaya çıkarmıştır[183]. ABD'nin kişisel verilerin korunması alanında diğer Avrupa ülkelerine kıyasla güven vermeyen bir koruma

[178] US Freedom of Information Act (FOIA), kanunun tam metni, (Çevrimiçi), https://www.thoughtco.com/us-government-4133021 , (Erişim Tarihi:03/05/2022).
[179] The Privacy Act of 1974, Kanunu, (Çevrimiçi), https://www.justice.gov/opcl/privacy-act-1974 , (Erişim Tarihi: 03/05/2022).
[180] Gültekin, Nil Melek, Kişisel Verilerin Ceza Hukuku Yönünden Korunması, Yüksek Lisans Tezi, Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, İstanbul 2012, s. 57.
[181] Gültekin, a. g. e., s. 57.
[182] Yıldız, Esra Tekil, İnternet Üzerinde Kişisel Verilerin Korunması, Marmara Üniversitesi Hukuk Fakültesi, Beta Basım, İstanbul 2003, s. 817.
[183] Gültekin, a. g. e., s. 57.

sağladığı gerekçesiyle verilerin aktarılması bakımından ciddi tereddütler söz konusu olmuştur. Gelinen noktada kişisel verilerin ABD'ye gönderilmemesi üzerine özel kuruluşlarda işletme maliyetlerinde ciddi artışlar söz konusu olmuştur[184]. Avrupa genelinde kişisel verilerin korunmasına yönelik sağlanan korumanın ve farkındalığın artması sonucunda 1999 yılında, sektördeki müşterilerin finansal alandaki verilerinin korunması maksadıyla federal düzeyde asgari koruma sağlayan ve ABD tarihinin özel hayatın gizliliğini koruyan en kapsamlı federal kanunu olan Finansal Hizmetleri Modernleştirme Kanunu[185] çıkarılmıştır.

Amerika Birleşik Devletleri'nin kişisel verilerin korunması ile ilgili olarak benimsediği yöntem incelendiğinde, verilerin kamu alanında korunmasını düzenleyen alanın, federal seviyede, tek elden ve bütünü kapsayan bir yaklaşımla kanuni düzenlemelerin yapıldığı görülürken, özel sektör bakımından bunu söylemenin mümkün olmadığı hatta tam zıttı bir yaklaşımın olduğu, özel sektördeki alanların ayrı ayrı düzenleyen kanunlar bulunmaktadır. Dolayısıyla, Avrupa Birliği'nin yürürlüğe soktuğu düzenlemelere ve AB üyesi ülkelerin bunu iç hukuklarına uyumlu hale getirme iradelerine bakıldığında, ABD'deki kişisel verileri koruma hukukunun kamu sektöründe 95/46/AT Sayılı Yönergesinin üçüncü ülkelere aktarım için talep ettiği eşdeğer korumayı gerçekleştirebildiği, ancak aynı şeyleri özel sektör için söyleyebilmenin mümkün olmadığını ifade edebiliriz. Zira özel sektör bakımından kişisel verilerin korunmasında kanuni düzenlemeler bakımından bu denli dağınık ve belirsiz bir düzenin benimsenmiş olmasının getirdiği sorunlar zorunlu olarak arayışa sürüklemiş bunun neticesinde Safe Harbor Antlaşması ile önemli oranda sorunlar giderilmeye çalışılmıştır.

2.5.6. İngiltere

İngiltere kişisel verilerin korunmasına ilişkin ilk olarak 1960'ların sonları ve 1970'lerin başlarında çeşitli düzenlemeler yapmıştır[186]. Bu alanda yapılan ilk düzenleme 1975 tarihli Cinsel Ayrımcılık Kanunu[187] ve 1968 tarihli Irkların İlişkileri Kanunu içerisinde

[184] Gültekin, a. g. e s. 58.
[185] Gültekin, a. g. e s. 58.
[186] Jay, Rosemary – Hamilton, Angus, Data Protection Law and Practice, Second Edition, Thomson, 2003, s. 2;
[187] İngilizce, The Sex Discrimination Act 1975, (Çevrimiçi), https://www.legislation.gov.uk/ukpga/1975/65/pdfs/ukpga_19750065_en.pdf , (Erişim Tarihi: 03/05/2022).

bulunmaktadır[188]. 1982 Nisan ayında İngiltere Hükümeti, kişisel verilerin korunması konusunda bir kanuni düzenleme oluşturmak için Lordlar Kamarası'na bir öneride bulunmuştur. Bu öneri neticesinde 1984 tarihli Veri Koruma Kanunu yürürlüğe girmiştir. 1984 tarihli Veri Koruma Kanunu, OECD ve Avrupa Konseyi Veri Koruma ilkelerini benimsemiş[189] ve Avrupa Birliği standartlarını da karşılayan bir düzenleme olarak mevzuatta yerini almıştır [190]. Tarih 2007 yılını gösterdiğinde, gelişen teknoloji ile birlikte kişisel verilerin korunması ile ilgili tartışmalar ve yapılan ihlallerin sayısında ciddi artış gözlemlenmiştir. Zira 2007 yılında yapılan bir açıklamada; "2007 senesi boyunca açıkçası korkunç bir ihlal listesi" olduğunu açıkça söylemiştir[191]. Kişisel verilerin korunmasına yönelik farkındalığın artması sonucunda hükümetin yeni tedbirler alması kaçınılmaz olmuştur. Bu bakımdan Adalet Bakanlığı, mahkemelere göndermiş olduğu uyarı yazısında, kişisel verilerin korunması hukukunu ihlal edenlerin cezalandırılmasında, bu tür suçları işleyenlere hapis cezası verilmesinde takdir yetkisi dahil olmak üzere, daha geniş yetkiler verileceğini açıkça ifade etmiştir[192].

Kişisel verilerin korunmasına yönelik ilgili Kanun düzenlemesinin cezai hükümleri ise, m. 55 ve devamında düzenlenmiş, ancak bu düzenlemede sadece hangi fiillerin ihlal oluşturacağı belirtilmiş ve bu fiillerin işlenmesi durumunda para cezası öngörülmüştür. İngiltere'de diğer ülkelerin aksine, ilgili Kanun'da kişisel verilerin hukuka aykırı olarak ele geçirilmeleri, ifşa edilmeleri, aktarılmaları gibi eylemlere hapis cezası yaptırımı düzenlenmemiştir. Bunun dışında, kişisel verilerin kasten ya da taksirle veri sorumlusunun izni olmadan ele geçirilmesi ya da ifşa edilmesi ya da kişisel verinin içerdiği bilginin üçüncü kişilere tedarik edilmesi ihlal teşkil eden fiiller olarak sıralanmıştır. İhlal teşkil eden fiiller sıralandıktan sonra kişisel verilerin korunmasına yönelik düzenlemelerin ruhuna aykırı olan

[188] İngilizce, The Race Relations Act of 1968, (Çevrimiçi), https://www.parliament.uk/about/living-heritage/transformingsociety/private-lives/relationships/collections1/1968-race-relations/1968-race-relations-act/#:~:text=On%2025th%20October%201968%2C%20the,promoting%20racial%20hatred%20a%20crime. , (Erişim Tarihi: 03/05/2022).

[189] Jay, Rosemary – Hamilton, Angus, Data Protection Law and Practice, Second Edition, Thomson, 2003, s. 3;

[190] Grant, Hazel, "Data Protection 1998 - 2008", Computer Law & Security Review, Vol. 25, Issue 1, 2009, (Çevrimiçi), https://www.sciencedirect.com/science/article/pii/S0267364908001696 , s. 44, (Erişim Tarihi:03/05/2022).

[191] Grant, a. g. e., s. 45.

[192] Grant, a. g. e., s. 47.

çok geniş istisnalar getirilmiştir. Ele geçirme, ifşa ya da tedarik etme eylemlerinin bir suçun önlenmesi ya da tespit edilmesi için veyahut kanun hükmü ya da mahkeme emriyle yapılması, kişinin bu eylemleri yapmakta hukuken yetkili olduğu inancının makul olması, kişide veri sorumlusunun bu eylemlerden haberdar olması durumunda bunlara izin vereceği inancının bulunması ve bu inancın makul olması ve bu eylemlerin kamu menfaatleri dolayısıyla yapılmış olması durumunda, yapılan eylemler ihlal oluşturmazlar.

3. İKİNCİ BÖLÜM

KİŞİSEL VERİLERE İLİŞKİN TERMİNOLOJİ, HUKUKİ NİTELİĞİ, KİŞİSEL VERİLERİN KORUNMASI HAKKININ DİĞER TEMEL HAK VE ÖZGÜRLÜKLERLE İLİŞKİSİ VE TEMEL İLKELER

3.1. KİŞİSEL VERİNİN TANIMI, UNSURLARI, KİŞİSEL VERİ TÜRLERİ VE BAZI TEMEL KAVRAMLAR

3.1.1 Kişisel Verinin Tanımı

Kişisel veri kavramı ile ilgili tanımlamaya başlamadan önce, "kişisel veri" kelime grubunun ana unsurunu oluşturan veri kavramının açıklığa kavuşturulması faydalı olacaktır. Türk Dil Kurumu'nun yaptığı tanımlamaya baktığımızda verinin[193], "*bilgi – data*" ve "*olgu, kavram veya komutların, iletişim, yorum ve işlem için elverişli biçimli gösterimi*" biçiminde tanımlandığını görmekteyiz. Verileri bir bütün olarak düşündüğümüzde verilere ait kırıntıların bir araya gelmesiyle bilgi denen kavram oluşmaktadır. Bundan dolayı veriler bilgi kavramının en küçük yapı taşı olarak görülmektedir[194]. Tüm bunlardan hareketle genel olarak, bireyleri elektronik veya manuel olarak tanımlayan verilere kişisel veri denilmektedir. Bu anlamda bireye özgü; telefon numarası, mail adresi, adı, soyadı, adresi, sağlık bilgileri, eğitim bilgileri, banka bilgileri, sigorta bilgileri gibi bilgiler kişisel bilgiler olarak ifade edilebilir. Kişisel veriler sadece bilgisayar ortamlarında depolanmamakta, ayrıca bireyin tanınmasını sağlayan konuşmaları hatta bilgisayar dışı ortamlara örnek verebileceğimiz kapalı devre video sistemlerinde de veriler işlenebilmektedir[195]. Kişisel veriler ile ilgili özgün bir tanımlamayı İngiliz Yüksek Mahkemesi'nin yaptığını görmekteyiz. Bu tanımlamaya göre "*kişisel veri*", "*bireylerin kişisel ya da aile yaşantıları,*

[193] (Çevrimiçi), http://sozluk.gov.tr/ , (Erişim Tarihi: 02/03/2022).
[194] Ruiter, Leslie/Van Belle, Gerald, Data and Law: Beyond the Sweat of the Brow: Who Owns Published Data? And What Is Data?, April, 2014, Journal of Significance, S.11, s. 29.
[195] A. g. e., s. 26.

iş veya meslekî kapasiteleri yönünden özel hayatını etkileyen bilgi" olarak ifade edilmektedir[196].

3.1.1.1. Bilgi kavramı

Kişisel veri kavramının unsurlarından birincisi bilgidir[197]. Gerek AB 95/46/AT sayılı Yönergede gerekse de KVKK m. 3'te, kişisel veri, "*belirli veya kimliği belirlenebilir olmak şartıyla -gerçek- bir kişiye ilişki her türlü bilgi*"[198] şeklinde tanımlanmıştır. İçerikten bağımsız olarak, belirli veya belirlenmesi mümkün bir şahsa ait olan objektif veya sübjektif nitelikli her türlü bilgi, kişisel verilerin unsurlarını oluşturur[199].

3.1.1.2. Kimliği belirli veya belirlenmesi mümkün kişi kavramı

Kişisel verinin birinci unsurunu bilgi olarak ifade etmiştik. Elde edilen bilginin kimliğinin belirli olması veya belirlenebilecek bir kişiyle irtibatlandırılması verinin ikinci unsurunu oluşturmaktadır. Kimliğin belirli olmasından kasıt bahse konu kişinin bulunduğu ortamdaki diğer bireylerden ayırt edilmesidir. Aynı şekilde kişinin kimliğinin belirlenebilir olmasından maksat kişinin ayırt edilmemiş olması ile birlikte ayırt olabileceği anlamını taşımaktadır[200]. Dolayısıyla elde edilen veri kimliği belirli veya belirlenebilir bir kişi ile irtibatlandırılmadığı sürece kişisel veri olarak kullanılamaz.

Elde edilen veriler belirli bir kişi ile doğrudan irtibatlandırılabiliyorsa bu verilere kişisel veri denilmektedir. Bunun yanında elde ettiğimiz verilerde ek bilgilere ihtiyaç duyuluyorsa ve bunun için belirli bir çaba harcanıyorsa birey ile irtibatlandırılabiliyorsa belirlenebilir bir kişinin kişisel verisinden bahsedilebilir. Bireyin sağlık verileri, eğitim bilgileri, banka bilgileri, kimlik numarası, sosyal ve kültürel özellikleri kullanılmak suretiyle bahse konu kişi belirli ya da belirlenebilir olabilmektedir. Yaptığımız açıklamayı bir örnekle açıklayacak olursak Altınbaş Üniversitesinin kamu hukuku programına kayıt olan bir öğrencinin adını

---

[196] Şimşek, a. g. e., s. 13.
[197] (Çevrimiçi), http://sozluk.gov.tr , (Erişim tarihi: 02/03/2022)
[198] (Çevrimiçi), https://ec.europa.eu/info/policies/justice-and-fundamental-rights_en , (Erişim tarihi: 02/03/2022)
[199] ARTICLE 29 DATA PROTECTION WORKING PARTY, s. 6.
[200] Informatıon Commıssıoner's Office; Data Protection Technical Guidance- Determining What İs Personal Data, s, 7, (Çevrimiçi), https://ico.org.uk/media/fororganisations/documents/1554/determining-what-is-personaldata.pdf , (Erişim tarihi: 02/03/2022).

bilmediğimizi varsayarak, kişinin hukuk fakültesi mezunu olduğunu, kaç yaşında olduğunu, lisanstan nereden mezun olduğunu, nerede çalıştığı ile ilgili verilerin kaydedilmesi, bireyin özellikleri kullanılarak belirlenebilir olması söz konusu olacaktır[201].

Bireyin "*belirli veya belirlenebilir olma*"sı, GDPR' da yapılan düzenlemede görüleceği üzere, kimlik numarası, adres bilgisi, sosyal medya hesap bilgileri yardımıyla doğrudan ya da dolaylı olarak kişinin belirlenebilir olması olarak ifade edilmiştir[202]. Kişiyle ilişkilendirilebilecek bilgiler dışında istatistiksel verilerin kişinin tanınabilirliği ile ilgili herhangi bir sonuca götürmediği için *"kişisel veri"* olarak ele alınması söz konusu olmayacaktır[203].

3.1.1.3. Bilginin kimliği belirli veya belirlenebilir kişiye ait olması

Kişisel veri kavramının en önemli unsurlarından biri olan "*bilginin kimliği belirli veya belirlenmesi mümkün kişiye dair olması*" hususu ifade edildiğinde "*kişi*" kavramının özellikle incelenmesi gerekmektedir. Kişi kavramı ifadesi incelendiğinde; bu ifadenin hem gerçek kişiler hem de tüzel kişiler için kullanıldığını söyleyebiliriz, ayrıca hak ve borçlara sahip olan anlamında da kullanıldığını görmekteyiz. Kişi kavramı her ne kadar hem gerçek kişiler hem de tüzel kişiler için ifade edilse de KVKK kapsamında değerlendirildiğinde gerçek kişiler için mi yoksa tüzel kişiler için mi kullanıldığı tartışmalı bir konudur. Bu anlamda ulusal ve uluslararası düzenlemelerde farklılıklar olduğu görülmektedir. KVKK kapsamında, uluslararası düzeyde kabul gören metinlerde gerçek bireylerin verilerinin korunmasına yönelik esaslı düzenlemelerin yapıldığı görülmektedir. Uluslararası düzenlemelerden olan 108 sayılı Sözleşme'nin muhteviyatı incelendiğinde kişisel verilerin geçerlilik alanının, gerçek kişilerle sınırlandırıldığını görmekteyiz (108 s. söz. m. 2/a). Uluslararası düzenlemelerden olan 108 sayılı sözleşme'ye taraf olan devletlerin iç hukuktaki uygulamalarına baktığımızda gerçek kişilerden oluşan kişi toplulukları bakımında 108 sayılı Sözleşme'nin uygulanabildiği görülmektedir (108 s. söz. m.3/2-b). Bir diğer uluslararası kuruluş olan OECD'nin kişisel verilerin korunması ile ilgili düzenlemelerinde kişisel

[201] Şimşek, a. g. e., s. 143.
[202]Sümeyye Hilal, Üçüncü, Medeni Yargılama Hukukunda Kişisel Verilerin ve Sırların Korunması, Doktora Tezi, Ankara 2018, s. 7.
[203] Çetin, Arslan, Avrupa Birliği Hukukunda Kişisel Verilerin Üçüncü Ülkelere Aktarılması, (Kazancı), Hakemli Hukuk Dergisi, Yıl: Mart-Nisan 2011.s. 32-35.

verilerin korunması kanununun gerçek kişilerle sınırlandırıldığı bunun dışında tüzel kişilerin ve kişi topluluklarının uygulama alanında değerlendirilip değerlendirilmeyeceği konusu üye devletlerin takdirine bırakılmıştır.

Bir diğer uluslararası düzenleme olan Avrupa Birliği'nin kişisel verilerin korunması yönergesinde de (95/46/AT) diğer düzenlemelerde olduğu gibi sadece gerçek kişileri koruma kapsamına aldığını görmekteyiz. Söz konusu yönergenin uygulama alanının düzenlendiği m.3'te veri işleme faaliyetlerini sadece gerçek kişilerle sınırlandırıldığı açıkça ifade edilmiştir. Bu düzenlemelerin yanında gerek Avrupa ülkelerinin gerek diğer ülkelerin kişisel verilerin korunmasına ilişkin yapılan düzenlemelerde tüzel kişileri de kapsam alanına aldıkları az da olsa görülmektedir[204].

Türk hukukunda yapılan düzenlemeler incelendiğinde, hem Anayasamızın 20. maddesinde hem de kişisel verilerin korunması kanunu kapsamında yalnızca gerçek kişilerin verilerinin koruma altına alındığı görülmektedir[205]. Kişisel verilerin korunması hakkının temel haklar kapsamında olduğu, özünde bireyin kişiliğini ve onun özel alanını korumayı amaçladığı göz önünde bulundurulduğunda, kişisel verilerin korunması hakkının tüzel kişiler bakımından uygulama alanı bulamayacağı, bireyin kişiliği ile ilgili olduğu, kişinin özel alanda korunması amaçlandığı düşünüldüğünde kişisel verilerin korunması kanununun tüzel kişilere uygulanamadığı çıkarımında bulunularak yasal düzenlemelerin yapıldığını görmekteyiz. Bireye ait kişisel veriler ile tüzel kişilere ait verilerin bazen iç içe geçtiği durumlar söz konusu olabilir. Bu tür durumlarda gerçek kişilere ait veriler kapsamında değerlendirilir ve Kişisel Verilerin Korunması Kanunu kapsamında korunurlar[206].

Yapılan açıklamalar doğrultusunda Türk hukukunda yaygın olan uygulamaya göre kişisel verilerin korunması temel hakkının sahibinin gerçek kişiler olduğunu açıkça ifade edebiliriz. Dolayısıyla Kişisel Verilerin Korunması Kanunu kapsamında kişilik haklarının korunmasının temel bir insan hakkı olduğuna dair şüphe yoktur. Bu nedenle, hak sahibinin yaşayan gerçek kişi olması gerekliliği, kişisel verilerin korunması hakkının aslında kişinin,

[204] Şimşek, a. g. e., s. 122.
[205] (Çevrimiçi), https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6698&MevzuatTur=1&MevzuatTertip=5 , (Erişim Tarihi:02/03/2022)
[206] Şimşek, a. g. e., s. 123; Başalp, a. g. e., s. 35.

kendi kişisel verilerinin geleceğini belirleme hakkını korumasından kaynaklandığı, dolayısıyla bireyin hayatı sona erdiğinde kişisel verilerinin korunması hakkının doğrudan sahibi olamayacağını söyleyebiliriz[207].

Tüzel kişilere ait kişisel verilerin korunması, Kişisel Verilerin Korunması Kanunu bağlamından ziyade, özel hukuk yaklaşımı ile irdelenmektedir. Özel hukuk bakımından incelendiğinde ticari sır niteliği taşımakta olup korumanın bu anlamda sağlanması gerektiği düşünülmektedir[208]. Ancak bu görüş tüzel kişilerin verilerinin korunması bakımından yetersiz kalmaktadır. Bu bakımdan gerek kamu tüzel kişisi olsun gerekse özel hukuk tüzel kişisi olsun, tüzel kişilerin faaliyet alanlarının sadece ticari hayatla sınırlı olmadığını biliyoruz. Bu nedenle ifade edilen görüşe katılmak mümkün değildir[209].

Kişisel verinin bir diğer unsuru ifade edilmeye çalışılırken, değerlendirilmesi gereken hususun, bilginin, kimliği belirli veya belirlenmesi mümkün bireye "ilişkin olması" gerekliliği söz konusudur. Veri ile kişi arasındaki bağlantı, birçok biçimde ortaya çıkabilir. Dolayısıyla elde edilen bilgi; içerik, amaç veya sonuç bakımından kişiyle bağlantılı olabilir[210].

Kişi ile bilgi arasında açıkça bir bağlantı tespit edilebiliyorsa bu bilginin bireyin kişisel verileri olduğu kabul edilebilir; ancak çoğu zaman kişi ile bilgi arasında bir ilişki açıkça tespit edilemediğinden kişinin kimliği tespit edilemez. Bazı durumlarda ise elde edilen verinin bir kişiye ait değil bir nesneye ait olduğu tespit edilebilir[211]. Dolayısıyla kaydedilen veriler mutlaka kişi ile ilgili olmak zorunda değildir, kişinin yaşadığı olaylarla veya faaliyet alanı ile bağlantı kurulabilir[212]. Elde edilen bilgilerin amaç bakımından kişiyle ilişkili olması söz konusu olabilir. Kaydedilen veriler neticesinde bireyin davranış biçimleri hakkında bilgi

---

[207] Şimşek, a. g. e., s. 123.
[208] İbrahim, Korkmaz, Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme, Türkiye Barolar Birliği Dergisi, Sayı: 124, Yıl: 2016, s. 89.
[209] Başalp, a. g. e., s. 35; Şimşek, a. g. e., s. 123.
[210] Çevrimiçi), https://edpb.europa.eu/about-edpb/more-about-edpb/article-29-working-party_en , s. 9, (Erişim Tarihi: 02/03/2022).
[211] (Çevrimiçi), https://edpb.europa.eu/about-edpb/more-about-edpb/article-29-working-party_en , a. g. e., s. 9, (Erişim Tarihi: 02/03/2022).
[212] (Çevrimiçi), https://ico.org.uk/media/about-the-ico/policies-and procedures/1873/section_10_guidance_for_staff.pdf , a. g. e., s. 10, (Erişim Tarihi: 02/03/2022).

sahibi olmak ve bu doğrultuda kişiye belirli bir biçimde davranmak için kullanılabiliyorsa, kullanılan bilginin amaç itibarıyla kişiyle bağlantılı olduğu söylenebilir[213].

Bilginin amaç bakımından nasıl kişi ile ilişkisi olabiliyorsa sonuç anlamında da kişiye ilişkin olabilmektedir. Somut olayın niteliğine göre elde edilen verinin kullanılması ile kişinin hak ve menfaatlerinin etkilenmesi söz konusu ise, bu bilginin sonuç itibariyle kişiye ilişkin olduğu ifade edilebilir. Sonuç bağlamında elde edilen muhtemel sonucun doğurmuş olduğu etkinin büyüklüğünün hiçbir önemi yoktur. Elde edilen verilerin analizleri sonucunda, kişiye toplumdaki diğer kişilerden farklı bir davranış biçiminin sergilenmesi yeterli olacaktır[214].

Bu değerlendirmelerimiz göz önüne alındığında, verinin kişiye ilişkin olup olmadığının tespitinde kullanılan amaç, içerik ve sonuç unsurlarının birbirlerine seçenek olabilecekleri yargısı çıkarılabilir. Dolayısıyla bilgi içerik olarak bireye ait ise aynı zamanda amaç ve sonuç olarak da o birey ile bağlantılı olması zorunlu değildir. Elde edilen bir bilgi içerik, amaç ve sonuç itibariyle birbirinden farklı kişilere ilişkin olabilir[215]. Sonuç itibariyle bu gibi durumlar söz konusu olduğunda özellikle somut olayın özelliklerine göre bilginin ilgili kişiyi belirli veya belirlenebilir kılıp kılmadığına özen gösterilmelidir[216].

Bir bilginin kişisel veri olup olmadığı konusundaki tespit çalışmasında veri çeşidinin ve özelliklerinin bir önemi yoktur. Bu bilgi çok hassas bir veri olabileceği gibi çok sıradan bir veri de olabilir. Burada değerlendirilmesi gereken önemli unsur elimizdeki verinin sahibi ile ilişkilendirilmesi ve somut bir kişinin tespit edilmesidir

3.1.2. Kişisel Veri Türleri

Kişisel verilerimiz etkiledikleri alanlar bakımından genel nitelikli ve özel nitelikli kişisel veriler olmak üzere farklı iki grupta incelenmektedir.

---

[213] Aksoy, a. g. e., s. 29.
[214] Aksoy, a. g. e., s. 29.
[215] (Çevrimiçi), https://edpb.europa.eu/about-edpb/more-about-edpb/article-29-working-party_en , a. g. e., s. 12, (Erişim Tarihi: 02/03/2022).
[216] Üçüncü, a. g. e., s. 10.

3.1.2.1. Hassas - özel nitelikli kişisel veriler

3.1.2.1.1. Genel olarak

Çeşitli veri türleri bulunmakla birlikte, bunların içerisinden bazıları karşıladıkları bilgi bakımından hassas veri olarak ifade edilmektedir. Bu veri türlerine baktığımızda siyasi görüşü, dini görüşü, ahlaki eğilimi, cinsel yaşamı, felsefi düşüncesi, etnik kökeni, sağlık bilgileri ve sendikal bilgileri kişiler hakkında ciddi derecede önemli bilgiler sunan verilerin başında gelmektedir. Hassas verilerin neler olduğu ile ilgili uluslararası sözleşmelerde hem de uluslararası belgelerde gerçek anlamda bir yeknesaklık bulunmamaktadır. Elde edilen verilerin hassas olup olmadıkları konusunda çoğunluk görüşüne göre, bu verilerin hangi amaçla toplandıklarının ve hangi amaçla işlendiklerinin somut olayın özelliklerine göre belirlenmesi gerektiği düşünülmektedir. Aslında yukarıda saymış olduğumuz hassas veri tipleri, bu görüş doğrultusunda somut olayın özelliğine göre değerlendirilmeden verinin hassas olup olmadığı kanaatine varılamaz[217]. Kişisel verilerin korunması konusu sürekli değişen ve dinamik bir hukuk alanı olduğundan bunun pek uygun bir yaklaşım olmadığı düşünülse de hukuki öngörülebilirlik, yargı ve idare makamlarının uygulamalarında yeknesaklık sağlanması, hassas verilerin içeriğine ve işlenmesine ilişkin yapılabilecek olan değerlendirmelerin objektif bir biçimde yapılabilmesi için kişisel veriler ile ilgili olarak tahdidi bir sayım yapılması gerektiğinin daha doğru olacağı kanaatindeyiz.

Hassas kişisel veriler ile ilgili yapılan ulusal ve uluslararası düzenlemelere bakıldığında, bu tür verilerin temel hak ve hürriyetlerle ilişkisi göz önüne alındığında özel bir koruma gerektiren veriler olduğunu açıkça ifade edebiliriz[218]. Özel koruma gerektiren hassas kişisel verilerin 95/46/AT sayılı Yönerge kapsamında özel olarak koruma altına alındığını görmekteyiz. Ulusal düzenlemeler bakımından hassas kişisel veriler GDPR m. 9'da düzenlenmiştir[219].

95/46/AT sayılı düzenlemede bahsedilen, hassas veriler nitelikleri itibariyle ve özel yaşama ilişkin oldukları için diğer veriler bakımından ihlal edilmeye çok daha müsaitlerdir. Bu

[217] Karen, Mccullagh, Data Sensitivity: resolving the conundrum, Journal of International Commercial Law and Technology C. 2, S. 4, 2007, s. 12.
[218] Akgül, a. g. e., s. 18.
[219] Çiğdem, Ayözger Öngün, Kişisel Verilerin Korunması Hukuku: Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil, Beta Yayıncılık, İstanbul 2019, s.27.

nedenle hem ulusal hem de uluslararası düzenlemeler de bu verilerin daha fazla korunması gerektiği belirtilmiştir[220]. Bu bağlamda ilgili Yönerge m. 8'de, yapılan düzenlemede üye ülkelerin, kişilerin sağlık bilgileri ya da cinsel tercihlerine yönelik verilerin işlenmesi, sendika bilgilerini, dini inanışları, siyasi görüşleri, etnik kökenleri ve felsefi inançlarına dair bilgiler veren kişisel verilerin işlenmesini yasaklayarak hassas veri tanımlaması yapıldığı görülmektedir[221].

Yaptığımız incelemeler doğrultusunda, Uluslararası düzenlemelerde, hassas veriler konusunda bir fikir birliği bulunmadığı tespit edilmiştir. Elde edilen verilerin kişilerin özel yaşam alanı ile ilgili olarak, diğer bireylerin arzularını, düşünce yapılarını, sağlık durumlarını, cinsel yönelimlerini tespit etmemizi sağlıyor ise bu tür verilerin hassas olduğunu ve özel nitelikli veri olarak ifade edildiğini söyleyebiliriz[222]. Dolayısıyla kişisel veri niteliğinde olmasına rağmen bu kişisel verilerin kullanıldıkları amaçlar düşünüldüğünde daha fazla korumaya ihtiyaç duyulan kişisel veriler "h*assas kişisel*" veri olarak ifade edilmektedir[223].

Kişisel verilerin küçük bir grubunu oluşturan hassas veriler açıklanmaları durumunda ait olduğu kişinin ciddi zarar görmesini veya bu kişi aleyhine ayrımcılık yapılmasına neden olabilecek kişisel verilerdir. Yukarıda da bahsettiğimiz üzere hassas verilerin kapsama alanına giren veriler, kişinin politik düşüncesine ait veriler, dini düşüncesine ait veriler, cinsel yaşantısına ait veriler yani kişinin hayatının özel alanına ait olan verilerdir[224]. Kişinin hassas verilerinin ortak özelliği risk faktörü olarak değerlendirilebilecek "ayrımcılık tehlikesi" bulundurması bakımından ifade edilebilir[225].

Hassas veriler çoğunlukla kişilik değerleri içinde bulunduğundan ve toplanıp işlenmesi durumunda ait oldukları kişi hakkında ayrımcılık yapılmasına neden olma gibi bir durumla

[220] Angel, John/Reed, Chris, ComputerLaw, The Law and Regulation of Information Technology, Sixth Edition, Oxford University Press 2007, s. 476.
[221] Kaya, a. g. e., s. 318.
[222] Edward J., Bloustein, Privacyas an Aspect of Human Dignity: An Answer to Dean Prosser, 39 N.Y.U. L. Rev. 962 (1964), s. 1023.
[223] Kaya, a. g. e., s. 318.
[224] Şimşek, a. g. e., s. 121.
[225] Başalp, a. g. e., s. 23.

karşılaşabileceğinden diğer verilere oranla daha farklı bir şekilde korunmaları ve bu korumanın sağlanması durumunda kişilik haklarının da korunması söz konusu olabilecektir[226]. Hassas verileri ait olduğu kişi dışındaki birilerinin öğrenmeleri durumunda bu verilerin barındırdıkları bilgiden kaynaklı olarak mağduriyetin oluşmasına sebep olabilecektir. Bununla ilgili olarak örneğin kişinin cinsel tercihlerine yönelik bilgileri veya kendilerine ait bilgilerinin bilinmesi bireyin mahalle baskısına ya da ırkçı saldırılara maruz kalmasına sebep olabilir[227].

Dünya hukuk sistemine baktığımızda neredeyse bütün ülkelerde kişisel verilerin korunmasında yapılan düzenlemelerde çeşitli veri türlerinin hassas olduğunu kabul ederek bu doğrultuda düzenlemeler yapıldığını görmekteyiz[228]. Yapılan düzenlemelerde verilerin bazılarının hassas veri olarak nitelendirilmesinin en önemli sebeplerinden bir tanesi bu verilerin daha hassas korunması gerektiği düşüncesinden kaynaklanmaktadır[229].

Uluslararası hukuk düzenlemeleri bakımından, bir kişisel verinin hassas veri kategorisinde bulunup bulunmadığı ile ilgili değerlendirme, konu ile ilgili oluşturulan yetkili kurulların ve mahkemelerin değerlendirmesine bağlıdır[230].

Ulusal ve uluslararası düzenlemeler bakımından kişinin siyasi görüşü, dini inançları, felsefi düşünceleri, ırki kökenleri bunun dışında sendikal bilgileri, dernek vakıf üyelikleri, beden bütünlüğüne ilişkin bilgileri, kişinin kendisi ile ilgili yargı kararları ve özel hayatı ile ilgili kişisel verileri özel ifadeye sahip olan hassas kişisel veri olarak kabul edilmektedir. Kişiye ait olan bu tür hassas verilerin işlenmesinin yasak olarak düzenlenmesinin kabul gören yaklaşım olduğunu görmekteyiz[231]. Bununla birlikte gerek kamu yararının gerek de ilgili kişinin rızasının olması halinde hassas verilerin işlenmesi söz konusu olabilmektedir[232].

---

[226] Şimşek, a. g. e., s. 88.
[227] Başalp, a. g. e., s. 43.
[228] Ian J., Lloyd, İnformation Tecnology Law, Fifth Edition, Oxford University Pres, Oxford, 2008, s.42 (Aktaran: Kaya, Hassas Veriler, s. 317).
[229] Küzeci, a. g. e., s. 230.
[230] Küzeci, a. g. e., s. 232.
[231] Kaya, a. g. e., s. 320-329.
[232] Döner, Kişisel Verilerin Korunması Hakkında Federal Kanun, s. 1-13.

Kanun koyucu tarafından kişisel verilerin korunması amacıyla yapılan düzenlemede, diğer ülkelerin yaklaşımından farklı olarak "*hassas veriler*" terimi yerine "*özel nitelikli kişisel*" veriler' terimi kullanılmıştır. Söz konusu düzenlemede "*Özel Nitelikli Kişisel Veriler*" başlığı altında bulunan ceza ve güvenlik tedbirleri ile ilgili veriler, kişilerin cinsel tercihleri, sağlık verileri, dini ve mezhebi verileri, dernek ve vakıf üyelik bilgileri, biyometrik ve genetik verileri, felsefi ve siyasi düşüncesi, etnik kökeni ve kişilerin ırkı olmak üzere çeşitli verileri kapsar. Demokratik bir hukuk devletinin gereği olarak özel nitelikli kişisel verilere kişinin rızası dışında asla dokunmaması gerekmektedir. Çünkü demokratik hukuk Devleti'nde temel hakları ancak ve ancak zorunluluk hallerinde kanunla sınırlanabileceği düzenlenmiştir[233].

3.1.2.1.2. Hassas kişisel veriler

Kişisel verilerin korunmasına dair hem uluslararası hem de ulusal düzenlemeler incelendiğinde sair ekseriyette veri türleri arasında ayrım yapıldığı görülmektedir. Hassas verilerin işlenmesi ile ilgili çok daha sıkı kurallar uygulanarak veriler koruma altına alınmıştır[234].

Doktrinde farklı görüşler bulunmakla birlikte, uluslararası ve ulusal hukuki düzenlemelerde hassas kişisel verilerin sınırlı sayıda ifade edilmesine karşı çıkıldığı görülmektedir. Hassas verilerin sınırlı sayıda sayılmasına karşı çıkan görüşlerde ise "*bağlamsal*" ve "*amaçsal*" görüşlerin savunulduğu görülmektedir. Görüşlerden biri olan bağlamsal yaklaşımı destekleyenler, kişisel verilerin kendi aralarında gruplandırılarak bazılarının mutlak anlamda hassas veri olarak ifade edilmesinin kabul edilmeyeceğini belirtmektedirler[235]. Gerekçe olarak, hassas olmayan bir verinin işlenmesi sonucu, içinde bulunduğu durumun şartlarına göre hassas kişisel veri durumuna dönüşmesi söz konusu olabilecektir[236]. Dolayısıyla bu görüş özelinde, kişisel verinin hassas veri olup olmadığına ilişkin çıkarsama yapmadan önce, elde bulunan bu verinin toplanmasındaki amaç, ait olduğu kişinin çıkarları ve en önemlisi elde bulunan verinin işlendiğinde bahse konu kişiler bakımından doğabilecek olası sonuçları

[233] Ersan, Şen, Kişisel Verilerin Korunması Kanunu Tasarısı'nın Anayasa ve Türk Ceza Kanunu Hükümleri Çerçevesinde Değerlendirilmesi, İstanbul Barosu Dergisi, Cilt: 83, Cilt: 3, Yıl:2009, s. 1206.
[234] David Towned, Segolene/Deryck, Beyleveld/Rouille Mirza and Jessica Wright, The Data Protection Directive and Medical Research Across Europe, Burlington: Ashgate Publishing Limited, 2004, s. 28.
[235] Prins, a. g. e., s. 33.
[236] Cammilleri Anne/ Clarie Levallois, Data Protection in the European Union, Bruxelles, 2007, s. 26.

değerlendirerek verinin hassas olup olmadığı sonucuna varılması gerekmektedir. Sonuçları bakımından değerlendirmenin ön plana çıkan görüşün birçok uluslararası ülkede benimsenmiş olmasına rağmen sektörel bağlamda uygulanmasının çok maliyet getirmesinden kaynaklı olarak ciddi eleştiriler aldığı bilinmektedir[237].

Kişisel verilerin gruplandırılması ile ilgili bir diğer önemli görüş olan "*amaçsal yaklaşım*" görüşünü savunanlara göre; kişisel verinin hassas veri olup olmayacağı ile ilgili kararın işlenme amacı bağlamında değerlendirme yapılarak karar verilmesi gerekmektedir. Dolayısıyla elde edilen kişisel verinin işlenme amacı net olarak belirlenip, bu amacın hassas verinin açığa çıkartılmasını sağlayıp sağlamadığına bakılmalıdır. Bu görüşün eleştirilmesinin temelinde işlenen verinin hassas veri olup olmadığı yönündeki değerlendirmeyi kimin yapacağı konusu bulunmaktadır[238].

Bu konuda ki bir diğer görüş olan bağlamsal yaklaşımda, verilerin kategorileştirilmesi reddedilerek elde edilen kişisel verinin kendi bağlamında değerlendirilerek, bu değerlendirmenin kişisel veri sahibinin özelinde ve somut olayın özellikleri göz önünde bulundurularak kişisel verinin hassas veri olup olmadığına karar verilmesi gerektiği görüşü öne sürülmüştür. Dolayısıyla bu görüşten hareketle bir kişi için çok alelade olan bir bilginin bir başka kişi için çok hassas bir veri olabilmesi söz konusu olabilmektedir. Yukarıda bahsettiğimiz amaçsal yaklaşımda ise kişisel verinin işlendiği amaç göz önünde bulundurularak, söz konusu veri ait olduğu kişi için alelade ve hassas olmayan bir nitelikte ise, bu verinin hassas veri olarak kabul edilmesi gerektiği görüşü savunulmaktadır.

Açıklamaya çalıştığımız tüm görüşler doğrultusunda bir değerlendirme yapıldığında hukuki öngörülebilirlik özellikle veri işleme noktasında yeknesaklık sağlanması ve verileri işlerken bu işlem sırasında tereddütlerin oluşmaması için hassas kişisel verilerin belirlenmesi hususundaki görüşlerden olan amaçsal yaklaşım görüşünün diğerlerine kıyasla daha uygulanabilir olduğunu ifade edebiliriz. Bunun yanında hassas veriler ile ilgili yapılan düzenlemelerde bu verilerin neler olabileceği ile ilgili objektif değerlendirmelerin yapılması karşılaşılan her olayda farklı değerlendirmelerin önüne geçilmesi anlamına geleceği için

[237] Aksoy, a. g. e., s. 33.
[238] Aksoy, a. g. e., s. 34.

amaçsal yaklaşım görüşünün olabileceği düşünülmektedir. Buna bağlı olarak hem verileri işleyen hem de yargı makamında bulunan otoriteler bakımından hassas verilerin tespitinin daha basit aynı zamanda objektif bir şekilde yapılabileceğini ifade edebiliriz.

Kişisel veri gruplamasının Avrupa hukukundaki düzenlemelerine baktığımızda AK ve AB, kişisel verileri çeşitli gruplara ayırarak verileri birbirinden ayrı tutmaktadır. Bununla ilgili özellikle Avrupa Birliği veri türleri içinde "*hassas kişisel veri*" ismiyle yasa koyucu tarafından hukuksal boyutta düzenlemelerin yapıldığı bilinmektedir[239].

Teknolojik alandaki hızlı gelişmeler ile birlikte 21. yy ihtiyaçları farklılık göstermektedir. Daha önceden düzenlenen ilgili yönerge veya yönetmeliklerde bulunan verileri teknolojik alandaki gelişmelerle birlikte yönerge ve yönetmeliklerde var olan kişisel hassas verilerin bazılarının önemini yitirdiği bazılarının ise hassas kişisel veri olarak kabul edilmediği görülmektedir. Dolayısıyla gelişen teknoloji ile birlikte farlı ülkelerde yaşayan kişilerin yaşam biçimleri, değer yargıları farklılaşabilmektedir. Bunun sonucunda Atlas veri kategorisi değişebilmektedir[240].

3.1.2.2. Anonim nitelikli kişisel veriler

Verinin anonim hâle getirilmesi, "*Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesi*" (KVKK m.3/1-b) şeklinde tanımlanmaktadır. Yapılan bu tanımlamaya göre, istatistik, araştırma, planlama ve süreç yönetimi gibi amaçlarla kayıt altına alınan ve herhangi bir kişiyi belirtmekten ziyade kitlesel bilgi olarak anlam ifade eden bu tür veriler, ilgili kişilerle ilişkilendirilmeleri olanaklı olmadığından kişisel veri sayılmamaktadır[241]. Bu tür durumlarda verinin ait olduğu kişi ile veri arasındaki ilişkilendirme yapılamadığından, bu tip veriler hakkında yapılacak işlemler kişilerin hak ve hürriyetlerinin ihlaline yol açmayacaktır[242].

[239] Cammilleri / Clari, a. g. e., s. 7.
[240] Aksoy, a. g. e., s. 33.
[241] Uğur, Ersoy, Bir İnsan Hakları Kavramı Olarak Kişisel Verilerin Korunması, Yüksek Lisans Tezi, Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Ankara 2009, s. 20.
[242] Başalp, a. g. e., s. 16.

Kişisel bilgilerin en önemli özelliklerinden bir tanesi ait oldukları kişi ile birlikte geçerliliklerini devam ettirebilmesidir. Bunun için bazı kişisel verilere sağlanan koruma ait olduğu kişinin hayatta bulunma süresi ile sınırlıdır[243]. Hayatı sona eren kişinin verileri tamamen korumasız bir hale gelmemektedir. Kişisel verilerin korunması kişiye tanınan temel haklardan olduğu için kişinin hayatının son bulması durumunda bile kişinin bu hakkı belirli ölçülerde korunduğunu biliyoruz. Zira, ölmüş kişiler bakımından kişisel veri kapsamının nasıl değerlendirileceğine ilişkin farklı düzenlemelerin olduğunu görmekteyiz. Kişilerin sağlık verilerinin hayatlarının son bulmasından sonra da saklanacağına ve açıklanması durumundan kişisel verilerin açıklanması suçundan bahsedileceğine dair uluslararası düzenlemeler olduğunu ve bu düzenlemelerde hayatın son bulmasından sonra da verilere ilişkin korumanın devam ettiği bilinmektedir. Uluslararası uygulamalar incelendiğinde konunun farklılık göstermesi, hayatın son bulma zamanı veya hayatın son bulduktan sonra geçen süreyle ilgili olduğunu görüyoruz.

Hayatı sona eren bir kişiye ait olan veriler hayatta olan kişiler hakkında bize bilgi verebilir. Bu nedenle kişinin hayatı son bulsa dahi verisinin açıklanmaması gerekmektedir[244]. Zira, bazı sağlık problemleri genetik olduğundan, hayatı son bulan kişinin verileri kendi ailesinin verileri ile ilişkilendirilebileceği için hayatta olan ailesinin verilerini açığa çıkarabilmektedir. Bu nedenle özellikle sağlık çalışanlarının hayatı son bulan kişinin kişisel verilerini açığa çıkarmama yükümlülükleri bulunmaktadır. Bazı durumlarda hayatı son bulan kişinin kişisel verilerinin açıklanması kendi soyundan gelenlerin hastalıklarının belirlenmesi bakımından bilgi sahibi olunmasını sağladığından, kişisel verilerin açıklanması bu bakımından oldukça tehlikelidir[245]. Bu türden tehlikelerin oluşmasını önlemek için, İngiltere yalnızca hayatta olan kişilerin verilerinin korunacağını düzenlemişken, Kanada hayatı son bulan kişinin hayatı son bulduğu andan itibaren 20 yıllık süre sonunda verilerinin açıklanacağına ilişkin düzenlemeler yapmıştır. "*Örneğin, hemofili, X-kromozomuna bağlı genetik bir hastalık olduğundan, ölmüş bir kimsenin hemofili hastası olduğuna ilişkin bilgi,*

[243] Ahmet, Boz, Kişisel Verilerin Korunması; Türkiye, ABD ve AB Örnekleri, Yüksek Lisans Tezi, Ankara: Polis Akademisi, Güvenlik Bilimleri Enstitüsü, 2014, s. 7-10.
[244] Yılmaz, Sabire Sanem, Tıp Alanında Kişisel Verilerin Korunması, 2021, s. 55.
[245] Aksoy, Hüseyin Can, Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması, 2010, s. 21.

o kişinin olduğunun da aynı hastalığa taşıdığını ortaya koymaktadır. Bu niteliği itibariyle söz konusu bilgi veri koruma yasalarının kapsamı içinde değerlendirilmelidir[246]*."*

Kişinin kimliğinin belirli veya belirlenebilir olması kavramı, kişinin diğer bireylerden ayırt edilmesi[247] anlamına gelmektedir. İlgili düzenlemede belirli veya belirlenebilir kavramının gerekçesi "*Bir kişinin belirli veya belirlenebilir olması, mevcut verilerin herhangi bir şekilde bir gerçek kişiyle ilişkilendirilmesi suretiyle, o kişinin tanımlanabilir hale getirilmesini ifade eder. Bu durum, kişinin fiziksel, ekonomik, kültürel, sosyal veya psikolojik kimliğini ifade eden somut bir içerik taşıması veya kimlik, vergi, sigorta numarası gibi herhangi bir kayıtla ilişkilendirilmesi sonucunda kişinin belirlenmesini sağlayan tüm halleri kapsar*[248]*."* şeklinde ifade edilmektedir. Burada ifade edilen belirlilik kavramının her somut olaya göre değerlendirilmesi gerekmektedir[249].

Sağlık alanında yaşanan gelişmeler, kişisel veri olarak ele alacağımız verilerin çeşitliliği arttırmakta, veri güvenliği açısından yeni tartışmaların yaşanmasına sebebiyet vermektedir[250]. Özellikle sağlık alanında kişisel verilerin korunmasının sağlanabilmesi için bilgilerin anonim hale getirilmesinden bahsetmek mümkündür. Bilgilerin anonim hale getirilmesi, sağlık hizmeti kapsamında alınan verilerin ihlalini minimuma indirebilecek bir yöntem olduğunu söyleyebiliriz[251].

3.1.3. Kişisel Verilerin Korunması Hakkının Hukuki Niteliğine İlişkin Görüşler

Günümüzde teknolojinin hızlı bir şekilde ilerlemesi nedeniyle kişisel verilere yönelik ciddi anlamda tehditler artmakta ve güvenlik zafiyeti doğmaktadır. Gerek ulusal gerekse de uluslararası düzenlemelerde bu tehditlere karşı hukuk düzeni tarafından koruma yolları aranmaktadır[252]. Hukuk düzeni tarafından aranan korunma yollarının temelinde teknolojik

[246] Aksoy, a. g. e., s. 21.
[247] Aksoy, a. g. e., s. 21.
[248] (Çevrimiçi), https://www.kvkk.gov.tr/Icerik/5388/Madde-ve-Gerekcesi-ile-Kisisel-Verilerin-Korunmasi-Kanunu-Bilgi-Notu-ve-Kisisel-Verilerin-Korunmasina-Iliskin-Terimler-Sozlugu ,(Erişim Tarihi:02/03/2022).
[249] Yılmaz, Sabire Sanem, Tıp Alanında Kişisel Verilerin Korunması, 2021, s. 56.
[250] Akyürek, Güçlü, Özel Hayatın Gizliliği İhlal Suçu, 2014, s. 56.
[251] Akyürek, Güçlü, Özel Hayatın Gizliliği İhlal Suçu, 2014, s. 57.
[252] Şimşek, a. g. e., s. 115.

gelişmelere paralel olarak artış gösteren kişisel veri işleme faaliyetleri karşısında kişinin korunması esas alınmaktadır[253].

Devletler tarafından kişilerin verilerine yönelik korumanın nasıl sağlanacağı ile ilgili yapılan düzenlemeler önemli olmakla birlikte, yapılan hukuki düzenlemelerin birbirinden farklı olduğunu görmekteyiz. Bu kapsamda yapılan düzenlemelerde ileri sürülen görüşler alt başlıklar halinde irdelenecektir.

3.1.3.1. Verilerin geleceğini belirleme ve bireysel özerklik kavramı görüşü

Kişisel verilerin korunması ile ilgili yapılan bütün düzenlemeleri incelediğimizde burada amaçlanan, gelişen teknoloji ile birlikte bireylerin kişisel bilgilerinin hiçbir sınırlama olmadan toplanması, toplanan bu verilerin çeşitli amaçlarla kullanılması ve aktarılması ile ilgili kişinin hukuki zeminde korunması hedeflenmektedir. Bu bağlamda kişisel verilerin korunması hakkının öncelikle insan onuru ve bununla bağlantılı olarak bireylerin kişiliklerini özgürce geliştirebilmesi hakkına[254] dayandırıldığı ifade edilebilir[255].

Kişisel verilerin korunmasıyla ilgili olarak 1983 yılında Alman Anayasa Mahkemesi'nin "*Nüfus Sayımı*" kararında Federal Alman Anayasası'nda gerek insan onurunun korunması ile ilgili gerekse de kişiliğin korunması ile ilgili düzenlemeler bir arada değerlendirilerek *"bilgilerin geleceğini belirleme hakkı"* kavramı ilgili konuya kazandırılmıştır[256].

Bilgilerin geleceğini belirleme hakkının ne denli önemli ve vazgeçilmez olduğunu şöyle bir örnekle somutlaştırabiliriz; örneğin, toplantı ve gösteri yürüyüşü faaliyetinde bulunan veya çeşitli sivil toplum örgütlerine üye olmasının kamu gücünü elinde bulunduran makamlarca kaydedildiğini ve bu işlemin çeşitli mağduriyetler yaşanmasına neden olabileceğini düşünen bir birey, bu durumdan endişe ederek bu türden yasal haklarını kullanmak istemeyebilir. Bu durum, "bireyin kendi kişiliğini geliştirme hakkı"nı zedeleyeceği gibi, bunun yanında kamu çıkarlarının zarar görmesine de yol açabilir.

[253] A. g. e., s. 112.
[254] Küzeci, a. g. e., s. 68.
[255] Şimşek, a. g. e., s. 111.
[256] Akgül, a. g. e., s. 87.

Oluşan bu durumda "*bireyin kendi kişiliğini geliştirme hakkı*"nı açıkça zedelenmesi söz konusu olacaktır. Bu nedenle bireyin kişiliğini özgürce geliştirebilmesi ve demokratik toplum yapısının sürekliliğinin sağlanabilmesi için, idare tarafından kişisel verilere yönelik olarak yapılan her türlü işleme karşı kişinin özellikle korunması gerekmektedir. Toplum içerisinde kişinin kurmuş olduğu ilişkilerin alenileştirilmesi ve bu ilişkiler konusunda hangi seviyede aleniliğin sağlanması ile ilgili kişinin karar vermesi gerekmektedir. Dolayısıyla bilginin geleceğini belirleme hakkı kural olarak bireyi kendisine ait olan kişisel verileri üzerinde tasarrufta bulunmayı ifade etmektedir[257].

Tüm bunların yanında kişisel verileri toplanmak suretiyle yaşamına ilişkin her türlü bilgisi kayıt altına alınan ve sürekli izlenen kişinin, kişiliğini serbestçe geliştirebilmesi pek mümkün olmayabilir. Bu bağlamda; kişisel verilerin korunması hakkı, bireyin kendisine ait kişisel verileri hukuka aykırı olarak belirli bir sınırlama olmadan kaydedilmesi, işlenmesi ve paylaşılması durumlarına karşı bir temel hak vererek onu alelade bir "veri nesnesi" olma durumuna karşı korumaktadır. Dolayısıyla bireyin kişisel verilerinin geleceğini belirleme hakkı, kendisine ait olan verilerin üzerinde karar verme hakkını sağlamaktadır[258].

Kişilik hakkının korunması bağlamında ortaya çıkan "*insan onuru*", "*bireysel özerklik*" gibi temel kavramların kişisel verilerin korunması ile ilgili "*bilgilerin geleceğini belirleme hakkı*" nın temel bir unsurunu oluşturduğunu ifade edebiliriz. Bilgilerin geleceğini belirleme hakkının bu denli önemli olmasının sebebi verilerin sadece toplandığı anda değil, elde edilmesinden silinmesine kadar geçen tüm süreçlerde kişinin korunması beklenmektedir. Bu amaçla bilgilerin geleceğini belirleme hakkı, bireyin kişisel verilerinin elde edilmesinden silinmesine kadar her aşamada veri sahibi olan bireye verileri üzerinde haklarını kullanabilme imkânı vermektedir[259].

[257] Küzeci, a. g. e., s. 69.
[258] Şimşek, a. g. e., s. 112.
[259] Metin, Çokmutlu, Türk Ceza Hukukunda Kişisel Verilerin Korunması, Doktora Tezi, Kocaeli Üniversitesi, Sosyal Bilimler Enstitüsü, Kamu Hukuku Anabilimdalı, Kocaeli, 2014, s. 54.

3.1.3.2. Özel hayatın gizliliği hakkı görüşü

Bireylerin kişisel verilerinin korunması hakkı ile ilgili bir diğer önemli görüş ise özel hayatın gizliliği hakkı olarak ifade edilebilir. Kişilerin özel hayatlarının gizliliği hakkı[260] demokratik bir hukuk devletinde vazgeçilmez bir niteliğe ve kişilik hakları içerisinde özel bir ehemmiyete sahip olması nedeniyle toplumdaki bireylerin kişiliğinin en temel öğesi olarak görülmektedir. Çağdaş hukuk düzenlemelerinin olduğu toplumlarda, tüm yönleriyle bir bütün olarak değerlendirildiğinde, özel hayatın gizliliği hakkının, bu bütünlüğün çok önemli bir parçası olarak kabul edilir. Bu bağlamda devletlerin kendi iç düzenlemelerinde bireyin kişiliğini özgürce yaşayabileceği, kendisini geliştirebileceği, sevdikleriyle vakit geçirebileceği, toplumdaki diğer kişiler ve devlet tarafından rahatsız edilmeyeceği özerk alanlar sağlamaları çok büyük önem arz eder[261]. Aslında kişisel verilerin korunması ile ilgili yapılan düzenlemeler; bireye, içerisinde diğer kişiler tarafından gözetlenmediği, kendisiyle baş başa kalabildiği, özgürce dilediği kişiyle iletişim kurabildiği, kendisini geliştirmesine olanak sağlayabildiği kısacası hususi bir alanın korunması anlamında güvence vermektedir[262]. Özel hayatın gizliliği bu denli önemli olmasına rağmen iç hukukumuzda gerekse uluslararası düzenlemelerde net bir tanımlamanın yapılmadığı görülmektedir.

Kıta Avrupa'sı ülkelerinde bireyin kişisel verilerine yaklaşıma bakıldığında, kişisel veriler kişilik hakkının önemli bir parçası olarak görülmektedir. Çünkü 95/46/AT sayılı Yönerge'nin içeriğinde, bireyin kişisel verileri mahremiyet hakkı ile ilişkilendirilerek çekirdek kişilik haklarının korunması amaçlanmıştır[263]. Bu bağlamda 95/46/AT sayılı Yönerge'de "*mahremiyet hakkı*" olarak düzenlenen hak, iç hukukumuz da "*özel hayat hakkı*"na karşılık gelmekte olup Türk Hukukunda, özel hayat hakkı, kişilik hakkının farklı bir görünümü olarak ifade edilmektedir[264]. Bundan dolayı aslında özel hayatın gizliliği hakkı kişisel verilerin korunması hakkından daha kapsamlı olsa bile gelişen teknoloji ile birlikte

---

[260] Tuba, Karahisar, Özel Hayatın Gizliliği ve İnternette İşlenen Suçlar, II. Medya ve Etik Sempozyumu, Medya Kültür İlişkisinde Etik, s. 599.

[261] Behiye Kazancı, Eker, Kişilerin İzinsiz Görüntülerinin Alınmasının TCK m. 134 Çerçevesinde Değerlendirilmesi, DEÜHFD, C. 9, S. 1. 2007, s. 131.

[262] Selen, Uncular, İş İlişkisinde İşçinin Kişisel Verilerinin Korunması, Ankara, Seçkin Yayıncılık, 2014, s. 28.

[263] Korff, Douwe, EC Study on Implementation of Data Protection Directive – Comparative Summary of National Laws, Cambridge, 2002.

[264] Muammer, Ketizmen, "Kişisel Verilerin Korunması" Tebliğ, (Çevrimiçi), http//www.tbd.org.trusrimgcdkamubib14raporlarPDFRP2-2008.pdf , (Erişim tarihi:02/03/2022).

kişisel verilerin korunması hakkının günümüzde önem kazanması sebebiyle, kişisel verilerin korunması hakkı temel unsurlarını özel hayatın gizliliğinden almış olsa bile bu haktan büyük oranda ayrılarak[265] kişisel verilerin korunması için çok ciddi düzenlemelerin yapıldığı görülmektedir[266].

Özel hayatın tanımı ile ilgili olarak yukarıda anlatılanlara paralel olarak Avrupa İnsan Hakları Mahkemesi'de özel hayatın tanımını yapmaktan imtina etmiştir. Bunun yanında özel hayatın önemini vurgulamak adına "özel hayatın" bireyin "*gizli alanı*"ndan daha kapsamlı bir alan olduğunu ifade etmiştir. Avrupa İnsan Hakları Mahkemesi çeşitli bazı kararlarından ve özellikle Niemietz v. Almanya kararında: özel hayatı tanımlamanın olası ve lüzumlu olmadığını belirtmiştir.

Avrupa İnsan Hakları Mahkemesi konuya ilişkin diğer davalarda da benzer yaklaşımı sürdürerek yukarıda bahsettiğimiz karara[267] atıflar yaparak özel hayat kavramının tanımının yapılmayacağını belirtmiştir[268].

Avrupa İnsan Hakları Mahkemesi yerleşik olan kararlarından biri olan, Niemietz - Almanya kararında *"...Özel hayat kavramını, bireyin kişisel hayatını istediği gibi yaşayabileceği bir iç alanla kısıtlamak ve bu alanın dışında kalan dış dünyayı bu alandan tamamen hariç tutmak aşırı sınırlayıcı bir yaklaşımdır. Özel hayata saygı, başka insanlarla ilişki kurmak ve söz konusu ilişkileri geliştirmek hakkını da bir dereceye kadar içermelidir..."*[269] şeklinde önemli saptamalarda bulunmuştur. Verilen bu kararda, kişinin özel yaşamının, yaşamın iç alanıyla sınırlı tutulmaması gerektiği, yaşamın sadece iç alanla sınırlandırılmaması, dış dünyanın iç alandan tamamıyla ayrılamayacağı belirtilerek, kişinin çeşitli ilişkiler kurabilmesi ve bu ilişkileri geliştirme hakkının da özel hayat kavramı içerisinde olduğu ifade edilmiştir.

---

[265] Küzeci, a. g. e., s. 70.
[266] Küzeci, a. g. e., s. 74.
[267] Niemietz, Almanya, Başvuru No: 13710/88, Tarih: 16.12.1992, (Çevrimiçi), http://hudoc.echr.coe.int/eng?i=001-57887 (Erişim tarihi: 02/03/2022).
[268] Yaşar, Salihpaşaoğlu, Özel Hayatın Kapsamı: Avrupa İnsan Hakları Mahkemesi İçtihatları Işığında Bir Değerlendirme, GÜHFD, C. 17, Yıl: 2013, Sayı: 3, s. 234.
[269] Sultan Üzeltürk, 1982 Anayasası ve İnsan Hakları Avrupa Sözleşmesine Göre Özel Hayatın Gizliliği Hakkı, İstanbul, 2004, Beta Yayınevi.

Özel hayat kapsamında nelerin olabileceği ile ilgili bir değerlendirmede bulunduğumuzda, kişinin cinsel tercihleri, farklı ilişkiler içine girebilmesi ve cinsel kimliğini belirleyip bu kimliği benimsemesi, telefon görüşme verileri, haberleşmeye müdahale etmek amacıyla gizli teknolojik cihazların kullanılması, birey hakkında bireyin rızası alınmadan devlet eliyle verilerinin toplanması, zorunlu tıbbî tedaviler, toplumdaki diğer bireylerle ilişki kurup bu ilişkileri geliştirebilme bu kapsamın içine girmektedir[270].

Özel hayat kavramının doktrindeki tanımlarına baktığımızda "*herkes tarafından bilinmeyen, özel araştırma ve bilgi edinmeyle sağlanan kişiye ait hususlar", "kişinin sadece kendisi için saklı tuttuğu ve başkalarının bilgisinden uzak kalmasını istediği yaşam görünümleri", "bireyin kişiliğini geliştirmek ve manevi değerlerine güvence sağlamak için başkaları tarafından bilinmesini istemediği hususların oluşturduğu ve korunması hukuken gerekli görülen hayat üzerindeki hakkı", "kişilerin gizli hayat alanlarında yapmış oldukları faaliyetlerin başkaları tarafından bilinmemesini istedikleri taraflar"* biçiminde tanımlamalar yapıldığını görmekteyiz. Yapılan bu tanımlamaların ortak noktası, yalnızca kişiye ait bir sahanın bulunması ve bu sahanın diğer kişiler tarafından bilinmemesi olarak değerlendirilebilir[271].

Avrupa İnsan Hakları Mahkemesi'nin özel hayat kavramının tanımlanması ile ilgili yaklaşımını açıkça belirtmiştik. Bunun yanında, söz konusu mahkeme birçok içtihadında hangi verilerin kişisel veri niteliğinde olduğuna dair tespitlerde bulunmuştur[272]. Bu bağlamda cinsiyet, medeni durum, doğum yeri, fotoğraf, parmak izi veya bunlara benzer kişisel verilerin kaydedilmesinin; tıbbi verilerin toplanması ve kayıt altına alınması, sağlık hizmetleri ile sosyal hizmetler ve vergi benzeri idari nitelikli konuların düzenlendiği "*bireysel kimlik belirleme sistemi*"nin kişisel veriler olduğuna dair değerlendirmede bulunmuştur. Avrupa İnsan Hakları Mahkemesi'nin yaptığı tespitler ile ilgili olarak özel hayat kapsamında değerlendirilmeyen bazı verilerin kişisel veri olarak değerlendirilip değerlendirilmeyeceği sorunu oluşmaktadır. AİHM'in bu konudaki yaklaşımı, özel hayat

[270] Doğan, Kılınç, Anayasal Bir Hak Olarak Kişisel Verilerin Korunması", Ankara Üniversitesi Hukuk Fakültesi Dergisi,Cilt: 61,Cilt: 3, Yıl:2012, s.1100.
[271] Kılınç, a. g. e., s.1100.
[272] Salihpaşaoğlu, a. g. e., s. 234.

alanında yer almayan diğer kişilerden saklanması gerekmeyen verilerin de kişisel veri olarak ifade edilebileceği şeklinde kararlaştırılmıştır. Bu konu ile ilgili bir örnek verecek olursak kişinin sendika bilgisi özel hayat olarak ifade edilmesi gerekmiyor iken, bu konuda kişinin sendikal bilgisinin hukuka aykırı bir şekilde kaydedilmesi durumunda kaydedilen bu veriler kişisel veri niteliğini haiz olacaktır[273]. Bu konuda kesinleşmiş olan Avrupa İnsan Hakları Mahkemesi'nin Rotaru / Romanya kararında[274] *"Ayrıca kamuya açık bilgiler, düzenli olarak toplandığında ve yetkili makamlar tarafından dosyalarda saklandığında da özel hayat kapsamına girebilir. Bu durum özellikle söz konusu bilgiler kişinin geçmişine aitse daha da geçerlidir…"*[275] şeklinde bir yaklaşımda bulunarak esas olarak özel hayatın gizliliği kapsamında değerlendirilmeyecek verilerin, birey hakkında düzenli olarak toplanıp, depolanması durumunda özel hayatın ihlali kapsamında değerlendirileceği kabul edilmiştir.

Özel hayatın korunması ile ilgi son olarak özetlemek gerekirse; gerek Avrupa İnsan Hakları Mahkemesi kararlarında gerek diğer düzenlemelerde görüleceği üzere bir görüş birliğinin olmadığıdır; ancak bunun yanında özel hayatın gizliliği konusunda birbirinden farklı üç farklı koruma alanının olduğu kabul edilmiştir. Kavramlaştıran bu alanlar, "ortak alan", "*özel alan*" ve "*gizli alan*" olarak ifade edilmektedir.

3.1.3.3. Mülkiyet hakkı görüşü

Kişisel verilerin korunmasının hukuki açıdan değerlendirilmesi ile ilgili öne sürülen bir diğer görüş olan mülkiyet hakkı görüşünün, çoğunlukla Amerika hukuk sistemi kaynaklarında öne sürüldüğünü görmekteyiz. Bu görüşe göre kişisel verilerimiz hem kişiliğimizin bir uzantısı hem de kişiliğimizin bir ürünü olarak ifade edilmektedir. Bu bağlamda bireyin kendisi hakkındaki kişisel verilerinin sahibi olduğu kabul edilmektedir. Bu görüşe göre bireylerin mülkiyetindeki verilerin nasıl ve hangi şartlar altında kullanılacağı kişinin kontrolünde olmasına imkân verilmelidir[276]. Görüş çerçevesinde kişisel verilere ilişkin mülkiyet hakkının korumasının sağlanması halinde mülkiyet hakkı ile sağlanan yasal

[273] Ramazan, Keklik, Özel Hayatın Gizliliğini İhlal Suçları, 2012, Ankara, Adalet Yayınevi, s. 27.
[274] Rotaru, Romania, Başvuru No: 28341/95, Tarih: 04/05/2000, (Çevrimiçi), http://hudoc.echr.coe.int/eng?i=001-58586 , (Erişim tarihi: 02/03/2022).
[275] Keklik, a. g. e., s. 27.
[276] Küzeci, a. g. e., s. 62.

korumalardan kişisel veri sahibi olan kişiler de yararlanacaktır. Dolayısıyla kişinin kendisine ait olan veriler hakkında kapsamlı bir denetim yetkisi söz konusu olacaktır[277].

Amerika hukuk sistemi kaynaklarında karşımıza çıkan bu görüşe göre kişisel veri sahibi olan kişi ya da kişiler verilerinin kullanılması karşılığında çeşitli anlaşmalar yaparak maddi veya manevi karşılığını alması mümkün olabilecektir. Dolayısıyla bu görüşe göre kişiler istemeleri durumunda kendi kişisel verilerini satabilecek ve bu yolla da bu sektörün daha adil işlenmesi sağlanabilecektir. Öne sürülen bu yolla, şirketlerin kişisel verilerin toplanması, işlenmesi ile ilgili katlanmak zorunda oldukları bedeli düşünerek, kişilerin özel hayatının daha güçlü korunacağı savunulmaktadır[278]. Kişisel verileri kötüye kullanılan kişilere direkt mahkemeye başvuru hakkının söz konusu olması veya kişisel verileri ihlal edilen kişinin zararının giderilmesi hakkının verilmesi bu görüşün en önemli noktalarından birini oluşturmaktadır. Bu korumanın daha kapsayıcı olabilmesi için kişinin kendi profili üzerinde denetim olanağı ve bu hakkı ile ilgili mahkemelerden talepte bulunabilmesi sağlanabilirse, profil sahibi olan bireyin izni olmadan bilgilerinin paylaşılması önlenebilecektir[279]. Bu görüşte özellikle kişisel verilerin ticari değerleri ön plana alınmaktadır.

Kişisel verilere ticari değer kazandıran mülkiyet hakkı görüşü birçok açıdan eleştirilmektedir. Yapılan ilk eleştiri, mülkiyet hakkı tanımının niteliğinin kişisel verilerin niteliği ile uyumlu olamayacağı değerlendirilmesinde bulunulmuştur. Mülkiyet hakkının, en önemli niteliklerinden biri, eşyanın ilk sahibi tarafından satışı sonrası, eşya üzerinde yani hak sahibi olanın bu hakkını dilediği gibi kullanabilmesi göz önünde bulundurulduğunda, eşyanın malikine mülkiyet hakkının sağladığı tasarruf yetkisinin, kişisel veriler bakımından söz konusu olabileceğinin kabulü çok zor olacaktır.

Yine bu görüşe göre, tasarruf yetkisinin kişisel verilerin korunması açısından söz konusu olduğunu kabul ettiğimizde, veri sahibinden satın alınan bir kişisel veri, satın alan kişi veya kurumlar veri öznesinin tekrardan rızasını almadan aktarabilecektir. Mülkiyet hakkı

[277] Akgül, a. g. e., s. 73;
[278] Küzeci, a. g. e., s. 62.
[279] Küzeci, a. g. e., s. 62.

görüşüne göre, kişinin kendi kişisel verilerini bir işletme ile paylaşması durumunda, paylaştığı kişisel verilerini bir başka kişi veya işletme ile paylaşmak istememesi durumunda böyle bir yetkisinin olabileceği kabul edilmektedir. Bu bağlamda, kişisel verilerini bir başkasına devreden veri öznesinin, kendisine ait olan kişisel verilerden mutlak surette bir soyutlanması söz konusu olacağından, mülkiyet hakkı görüşünün kişisel verilerin yapısı ile örtüşmediği değerlendirilmektedir[280].

Mülkiyet hakkı görüşü ile ilgili dile getirilen diğer bir önemli görüş, mülkiyet hakkının hukuki anlamda işlevine ilişkindir. Mülkiyet hakkı ile amaçlanan, doğadaki sınırlı kaynakların gerçekçi bir şekilde dağıtılmasının söz konusu olduğu, oysa doğada kişisel veriler ile ilgili bir eksilmenin veya tükenmenin olmadığı düşünüldüğünde; kişisel verilerin hukuki niteliğinin, mülkiyet hakkı bağlamında yapılacak bir değerlendirmenin yanlış olacağı değerlendirilmektedir[281].

3.1.3.4. Fikri mülkiyet hakkı görüşü

Kişisel verilerin hukuki niteliği ile ilgili olarak öne sürülen bir diğer görüş fikri mülkiyet hakkı görüşüdür. Kişisel verilerin korunması açısından bu görüşü savunanlar; amaç noktasından hareketle, kişisel verilerin korunması ve fikri mülkiyet korunmasındaki esas amacın, kişisel verinin korunup, dengeli dağıtılmasından yola çıkılarak, bu iki temel hak arasında benzerlik olduğunu savunmaktadırlar[282]. Bu görüşte olan kaynaklar, kişinin kendisine ait olan veriler üzerindeki hakları ile, fikri mülkiyet hukukunda eser sahibinin meydana getirdiği eser hakları arasında benzerlik bulunduğunu düşünerek böyle bir görüş etrafında birleşmişlerdir[283].

Fikri mülkiyet hakkı görüşünde, söz konusu kişinin sahip olduğu kişisel verilerine ilişkin olarak verilerini hangi şartlarda kimlerle paylaşacağını seçme veya diğer kişilerin elinde bulunsa bile veri öznesi ile ilişkili verilerin bütünlüğünün ve doğruluğunun korunmasını talep etme yetkisi olmalıdır. Bu anlamda veri öznesinin mutlak bir tasarruf yetkisinden bahsedilmektedir. Dolayısıyla bu görüş açısından yapılan değerlendirmede, eserin malikine

[280] Aksoy, a. g. e., s. 64-65.
[281] Aksoy, a. g. e., s. 66.
[282] Prins, a. g. e., s. 1146.
[283] Akgül, a. g. e., s. 74;

sağladığı haklar ile kişisel verilerin veri öznesine sağlamış olduğu haklar arasında bir benzerlik bulunduğu düşüncesi bu görüşün temelini oluşturmaktadır[284].

Bu görüşü savunanlar olduğu gibi diğer görüşlerle benzer şekilde ciddi anlamda eleştirenler de olmuştur. Bu eleştirileri incelediğimizde, fikri mülkiyet hakkının bilgiyi temel alan bir hak olması nedeniyle kişisel verilerin korunmasının fikri mülkiyet hakkı ile korunamayacağı düşünülmektedir. Fikri eserlerde meydana gelebilecek sorunları çözebilmek, fikri mülkiyet hukukunun iktisadi temelini oluşturmaktayken, kişisel verilerin fikir eserleri olarak nitelendirilmesi mümkün olmayacaktır[285].

Fikri mülkiyet hakkı görüşünü savunanlara göre, bilim dünyasına katkı sağlamak, kişisel verilerin korunmasının ve fikri mülkiyet haklarının amacını oluşturmaktadır. Ancak, fikri mülkiyet hukuku esas alınarak öne sürülen bu ortak amaç görüşünün kişisel verilerin korunması ile fikri mülkiyet hakkının doğal yapısı gereği birbirinden farklı olduğunu görmekteyiz. Fikri mülkiyette esasen korunan kişinin emeğidir. Kişinin bilinçli bir biçimde sarf ettiği çalışmanın eseri olarak fikri mülkiyete konu olan değerlerin meydana geldiğini görmekteyiz. Ancak kişisel verilerin meydana gelebilmesi için veri öznesinin herhangi bir çaba içerisinde olmasına gerek yoktur. Kişinin varoluşuyla birlikte yaşamını sürdürmesiyle meydana gelmektedir[286].

Fikri mülkiyet hakkı görüşüne getirilen bir diğer eleştiri hem kişisel verilerin hem de fikri mülkiyet hakkının korunmadığı durumlara ilişkindir. Sonuçları bakımından bir değerlendirme yapıldığında kişisel verilerin korunmadığı durumlarda çok daha ağır sonuçların doğabileceği görülmektedir[287]. Kişisel verilerin korunmaması durumunda kişinin ayrımcılığa maruz kalması, işten çıkarılması, aşağılanması ve ağır insan hakkı ihlalleri gibi durumlar söz konusu olabilecektir. Fikri mülkiyet hakkının korunmadığı herhangi bir durumda böyle ağır bir bedelin ödenmesi söz konusu olmayacaktır. Bu anlamda doğabilecek zarar çoğunlukla maddi zarardan ibaret olacaktır[i].

[284] Aksoy, a. g. e., s. 61.
[285] Küzeci, a. g. e., s. 64.
[286] Prins, a. g. e., s. 296.
[287] Aksoy, a. g. e., s. 66.

3.1.3.5. Öne sürülen görüşler hakkında değerlendirmelerimiz

Yukarıda açıklamaya çalıştığımız görüşlerin tamamının hukuk dalına ciddi anlamda katkı sunduğu net olarak ifade edilebilir. Kişisel verilerin korunmasının hangi hukuki zeminde tartışılması gerektiği ve bu tartışmaların hukuk dünyasında ne gibi sonuçlar doğuracağı önem arz etmektedir. Tartışma ve değerlendirmeler sonucu oluşan temel teori şekillenmeye başladıktan sonra, kişisel verilerin korunması hukukundaki esas müesseseler, şekillenen bu temel teori etrafında oluşacaktır. Dile getirilen görüşlerin tamamı kendilerine özgü bir hukuki gerekçelendirmeye dayanmaktadır. Bu gerekçelerin bazılarının maddi anlamda bazılarının ise manevi anlamda öne çıktığını görmekteyiz.

Yukarıda açıklamaya çalıştığımız ilk görüş çerçevesinde bireysel özerklik, insan onuru ve kişisel verilerin geleceğini belirleme kuramı ile ilgili bir değerlendirmede bulunduğumuzda; doktrinde bu görüşü savunanlar, bireyin sıradan bir veri nesnesi olarak görülmemesi gerektiğini ifade etmektedirler. Çünkü modern hukuk devletlerinde, bireylerin kendileri ile ilgili verilerin toplanması, işlenmesi ve aktarılması işlemlerinde tam bir yetkinin ve sıkı bir denetimin olması gerektiği kabul edilmiştir. Bireyler yalnızca insan olmak ve insanlık onuruna sahip olmakla birlikte, bu hak devredilemez ve vazgeçilemez. Söz konusu görüşte, kişilerin verilerinin toplanması, işlenmesi, aktarılması yani her aşamasında kişinin tasarruf hakkının bulunabilmesi ve kendi verilerinin geleceğini belirleyebilmesi savunulmuştur. Söz konusu görüş özellikle insan hakları yaklaşımından hareketle kişinin manevi varlığını ön plana çıkaran, kişiyi önemseyen hukuki temele dayanmaktadır. Dolayısıyla bireyi önceleyen ve modern hukuk düzenini temel alan bu görüşün çok değerli olduğunu belirtebiliriz.

İkinci önemli bir görüş olan özel hayatın gizliliği hakkı ile ilgili olarak, öncelikle özel hayatın tanımının yapılmasından kaçınıldığı net olarak ifade edilebilir. Zira bu konuda yapılan düzenlemeleri incelediğimizde özellikle uluslararası metinler ve Avrupa İnsan Hakları Mahkemesi tarafından bir tanımlamanın yapılmadığını görmekteyiz. Böyle bir yaklaşımın bilinçli bırakılan bir boşluk olduğunu ifade edebiliriz. Kişisel verilerin korunmasının esası, söz konusu görüşte bireyin özerk alanına dayandırıldığını görmekteyiz. Dolayısıyla kaynağını kişinin özerk alanından almaktadır. Yukarıda kısaca değindiğimiz üzere kişinin özel hayatı; ortak, özel ve giz gibi alanlardan teşekkül etmektedir. Bu bakımdan

kişinin özel hayatı kişisel verilerinden çok daha fazlasını ifade etmektedir. Ortak alanda bulunan kişisel veriler için özel bir koruma gereksinimi sağlanmıyorsa bu tamamen korumasız olduğu anlamına gelmemektedir. Özel alanın ortak alandan kural olarak daha fazla korunması gerekmektedir. Giz alanı ise kesin olarak korunması gereken bir alandır. Kişisel verilerimizden olan hassas veriler giz alanında korunmaktadır. İleri sürülen görüş bir bütün olarak değerlendirildiğinde insan hakları temelli olmasından dolayı insan onuru ve bireysel özerklik görüşüne yakın bulunmaktadır. Ancak kişisel veriler ile ilgili sağlanan korumanın gerekçesini değerlendirdiğimizde bireysel verilerin özel hayatın sadece belirli bir kısmı olması nedeniyle bir önceki görüş karşısında daha dar olduğu ifade edilebilir.

Bir diğer önemli görüş olan mülkiyet hakkı, kişisel verileri kişinin kendisine ait olan bir ürün olarak gördüğü için değerlendirmesini bu bakımdan açıklamaktadır. Bu görüşe göre bireyler kendi verileri üzerinde tasarruf yetkisini kullanarak gelir sağlayacak ve aynı zamanda mülkiyet hakkının korunmasından faydalanmış olacaklardır. Yine bu görüşe göre kişiler için bir zarar söz konusu olduğunda doğrudan yargıdan bu zararlarının giderilmesini talep edebileceklerdir. Bu görüş kişisel verilerin ürün olarak görülmesi nedeniyle bireyi metalaştırdığı ve insan hakları ile bağdaşmadığı gerekçesiyle eleştirilmektedir.

Fikri mülkiyet hakkı görüşüne baktığımızda, kişisel verilerin korunarak denetimli bir şekilde dağıtılmasının, eserlere sağlanan telif hakkındaki gerekçelendirme ile aynı bağlamda savunulduğu dile getirilmektedir. Kişisel verilerin bir fikir olmadığı çok net ortada iken, fikri mülkiyette eserin fikrinin korunması söz konusudur. Yani fikri mülkiyet esasen maddi hakkın korunması ile ilgiliyken, kişisel verilerin korunmasında ise söz konusu olan manevi hakkın korunmasıdır. İlgili görüşün bu açılardan incelendiğinde diğer görüşlere göre daha zayıf olduğunu ifade edebiliriz.

Günümüz hukuk sistemlerine baktığımızda; kişilerin münhasır alanlarının olduğunu ve bu alanlar ile ilgili olarak tercihlerini rahatlıkla hayata geçirebilecekleri ortamların pozitif yükümlülükler çerçevesinde devletler tarafından sağlandığını görmekteyiz. Çağdaş demokrasilerin yaşandığı devletlerde bu hususların doğal sonucu olarak, bireylerin kendileri ile ilgili hususlarda tasarruf hakkı olduğu, hukuki güvenlik, öngörülebilirlik ve geleceklerini kendi seçimleri sonucunda şekillendirebilecekleri artık kaçınılmaz bir gerçektir. Tüm bu

açıklamalardan sonra *"insan onuru, bireysel özerklik ve kişisel verilerin geleceğini belirleme"* teorisine dayanan görüşün öncelikle kişiyi meta olarak görmeden yalnızca insan olmasından kaynaklanan ayrıcalıklara sahip olması gerektiği yaklaşımı temelinde daha isabetli ve uygulanabilir düşüncesini taşımaktayız.

4. ÜÇÜNCÜ BÖLÜM

KİŞİSEL VERİLERİN CEZA VE KABAHATLER HUKUKU BAKIMINDAN İNCELENMESİ VE AYDINLATMA YÜKÜMLÜLÜĞÜNÜN ESASLARI

4.1. KİŞİSEL VERİLERİN CEZA VE KABAHATLER HUKUKU BAKIMINDAN İNCELENMESİ

4.1.1. Genel

Türk Ceza Hukuku'nda suçun konusu, kanuni tipe uygun hareketin üzerinde gerçekleştirildiği maddi şeydir[288]. Bu bağlamda kişisel verileri hukuka aykırı olarak verme, yayma ve ele geçirme suçunun konusu kişisel verilerimiz olacaktır.

Suça ilişkin yapısal unsurlar, bütün suçlar bakımından müşterek olan ve olmadıkları zaman suçun oluşmasını engelleyen, genel nitelikteki unsurlardır. Bir suçun genel ve kurucu unsurlarının nelerden oluştuğu ya da bir diğer ifadeyle suçun hangi yapısal unsurlardan müteşekkil olduğu konusunda ceza hukuku doktrininde bir görüş birliğinin olmadığı bilinmektedir[289]. Bu fikir ayrılığı, suçun yapısal unsurlarının kaç başlık altında incelenmesi noktasında dile getirildiği gibi; suçun aynı sayıda unsurdan oluştuğunu kabul eden yazarlar arasında da bu unsurlara verilen anlam konusunda bir mutabakatın oluşturulabilmesi de mümkün olmamıştır. Bu açıdan suçun yapısal unsurlarının gerek sayısı gerekse anlam ve içeriği yazardan yazara değişkenlik göstermektedir[290]. Kişisel verilerin korunmasına ilişkin suç tipleri inceleme konumuzun kapsamı dışında kaldığı için bu suç tüplerinin yapısal unsurlarına ayrıntılı olarak yer verilmemiş ancak suç tiplerine ilişkin kanundaki genel çerçeve kısaca izah edilmiştir.

[288] Özbek, Veli Özer, Doğan Koray, Bacaksız Pınar ve Tepe İlker, Türk Ceza Hukuku Genel Hükümler, Ankara: Seçkin Yayınevi, 2016.
[289] Hasan Sınar, Kişisel Verileri Hukuka Aykırı Olarak Verme, Yayma veya Ele Geçirme Suçu (TCK Md. 136), Kişisel Verileri Koruma Dergisi, C.2, S.1, 2020, s. 37.
[290] Artuk, Gökcen, Alşahin, Çakır, a. g. e., s.378.

Teknoloji dünyasında yaşanan hızlı gelişmeler daha çok kişisel verilerin işlenmesine sebebiyet vermiş olup bu durum kişisel verisi işlenen bireyin daha etkili bir şekilde korunması gerektiği anlayışını göstermiştir[291].

TCK'da "*Kişilere Karşı Suçlar*" kısmının "*Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar*" başlığının 9. bölümünde kendisine yer bulan 135, 136 ve 138. maddelerinde kişisel veriler hakkında işlenen suçlara dair düzenlemeler yapılmıştır. Kanun koyucunun kişisel verilere dair işlenen suçları neden TCK'daki 9. bölümde düzenlediğine baktığımızda, kişisel verileri, *"özel hayat"* mefhumu kapsamında değerlendirdiğinden dolayı böyle bir düzenlemenin yapıldığı anlaşılmaktadır[292].

Bireye ait kişisel verilerin yukarıda bahsetmiş olduğumuz ulusal ve uluslararası metinlerde düzenlenen temel ilkeler dikkate alınmadan var olan düzenlemelere aykırı bir biçimde işlenmesi neticesinde, ceza yasalarında belirlenen suç tipleri oluşmakta[293] ve bunların karşılığında çeşitli yaptırımlar tatbik edilmektedir. Türk Ceza Kanunu "Ö*zel Hayata ve Hayatın Gizli Alanına Karşı Suçlar*" başlığı altında "*kişisel verilerin kaydedilmesi*" (m. 135), "*verileri hukuka aykırı olarak verme veya ele geçirme*" (m. 136) ve "*verileri yok etmeme*" (m. 138) suçlarının düzenlendiğini bilmekteyiz. TCK'da yapılan düzenlemeler dışında KVKK m. 17'de yapılan düzenlemelere aykırı olarak, verileri işlenen bireyin verilerini silmeyen ya da anonim hâle getirmeyen sorumlular hakkında, *"verileri yok etmeme"* suçu hakkında düzenlenen cezanın tatbik edileceği ifade edilmektedir. Çalışmamızın konu başlığını oluşturan kabahat hakkında KVKK m. 18'de kabahat tiplerinin düzenlendiğini görmekteyiz. Dolayısıyla KVKK bakımından aydınlatma yükümlülüğünü yerine getirmeyen sorumlular hakkında (m. 18/1-a), kişilerin verilerine ilişkin güvenlik yükümlülüklerini yerine getirmeyenler hakkında (m. 18/1-b), Kişisel Verileri Koruma Kurulu'nun vermiş olduğu kararları yerine getirmeyenler hakkında (m. 18/1-c), son kabahat tipi olan Veri Sorumluları Sicili ne kayıt bildirim yükümlülüğünü getirmeyenler hakkında (m. 18/1-ç)

[291] Kuşkonmaz, Elif Mendos, Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması, Yüksek Lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2013, s.126.
[292] Çokmutlu, a. g. e., s. 144.
[293] Aysun, Melike Köse, Kişisel Verilerin Kaydedilmesi Suçu, Yüksek Lisans Tezi, Akdeniz Üniversitesi Sosyal Bilimler Enstitüsü, Antalya, 2018, s.73; Ketizmen, a. g. e., s. 206.

KVKK m. 18'de düzenlenen idari para cezalarının uygulanması öngörülmektedir. Söz konusu kabahat tiplerine ilişkin detaylı açıklamalar alt metinlerde yapılacaktır.

4.1.2. Türk Ceza Kanunu'nda Kişisel Verilerin Korunmasına Yönelik İşlenen Suçlar

Kişisel veri kavramının Türk Ceza Hukuku'nda yorumlanmasına ilişkin olarak her ne kadar 5237 sayılı TCK, kişisel verilerin korunmasına ilişkin kanun seviyesindeki ilk metin olma özelliğini gösterse de, TCK'nın tanımlar başlıklı m. 6'da kişisel veri tanımının yapılmadığını görmekteyiz[294]. Başlıklar kısmında bir tanımlama yapılmamasına rağmen TCK m. 135'de düzenlenen kişisel verilerin kaydedilmesi suçunun gerekçesinde bir tanım yapılmış ve kişisel verini tanımı, "gerçek kişiyle ilgili her türlü bilgi" olarak tanımlanmıştır.

4.1.2.1. Kişisel verilerin hukuka aykırı olarak kaydedilmesi suçu

Kişisel verilerin hukuka aykırı olarak verilmesi ya da ele geçirilmesi suçuyla korunması amaçlanan hukuksal yararın belirlenmesinde öncelikle normlar hiyerarşisine uygun olarak normlar piramidinin en üst basamağında kendisine yer bulan Anayasa'dan başlanmalıdır. Zira normlar hiyerarşisinin en üst basamağında kendisine yer bulan Anayasa hükümleri, diğer alt sıralarda bulunan yasal düzenlemeler bakımından bağlayıcı bir nitelik taşır ve bu düzenlemelerin Anayasa'da zikredilen hususlara aykırı bir hüküm barındırması mümkün değildir. Bu açıdan özellikle temel hak ve özgürlükler bakımından anayasal seviyede bir düzenlemenin yapılmış olması hukuk düzeni içerisinde nedenli bir korumanın sağlandığını ifade etmektedir[295].

Kişisel verilerin hukuka aykırı olarak kaydedilmesi suçunun düzenlendiği TCK m. 135'e göre *"... kişisel verilerin hukuka aykırı olarak kaydedilmesi*" fiili suç olarak düzenlenmiştir. Bu madde kapsamında "*hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir"* olarak ifade edilmektedir.

TCK m. 135'in 2. fıkrasında, *"kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya*

[294] Hasan Sınar, ''Kişisel Verileri Hukuka Aykırı Olarak Verme, Yayma veya Ele Geçirme Suçu (TCK Md. 136)", Kişisel Verileri Koruma Dergisi, C.2, S.1, 2020, s. 38.
[295] Hasan Sınar, ''Kişisel Verileri Hukuka Aykırı Olarak Verme, Yayma veya Ele Geçirme Suçu (TCK Md. 136)", Kişisel Verileri Koruma Dergisi, C.2, S.1, 2020, s. 35.

sendikal bağlantılarına…" bağlantılı olarak kişisel verilerin kaydedilmesi durumunda öngörülen cezanın yarısı oranında artırılacağı düzenlenmiştir. İlgili maddenin gerekçesini incelediğimizde kanun koyucunun, Türkiye'nin de tarafı olduğu 108 Sayılı Avrupa Konseyi Sözleşmesi kapsamında, bireylerin kişisel verilerine ilişkin koruma hükümlerinin düzenlendiği ve bu düzenlemeler sebebiyle gelişen teknoloji ile birlikte artan, verilerin kaydedilmesi işlemleri karşısında, kişilerin haklarının korunmasının asıl hedef olarak ortaya konulduğunu ifade edebiliriz[296].

Bilindiği üzere suçun konusunu oluşturan "kişisel veri"[297] kavramı TCK'da tanımlanmamıştır. Tabi bu durum KVKK düzenlemesi yapılmadan önce çok ciddi sorunlara sebebiyet vermekteydi[298]. Bu dönemde KVKK adına yapılacak olan tespitlerde 95/46/AT sayılı Yönerge ile 108 sayılı Avrupa Konseyi Sözleşmesi gibi uluslararası düzeyde düzenlemelerden faydalanılmaktaydı[299]. Bu süre içerisinde bu alanda yaşanan boşluk KVKK ile aracılığıyla giderilmiş olup[300] KVKK' da *"kimliği belirli veya belirlenebilir gerçek kişiye ait her türlü veriyi ifade eder."* biçiminde bir tanımlamanın yapıldığı görülmektedir.

5237 sayılı Türk Ceza Kanunu'nda düzenlenen m. 135'e göre kişisel verilerin kaydedilmesi suçunun varlığından bahsedebilmek için bireyin kişisel verisinin, var olan hukuki düzenlemelere aykırı olarak kaydedilmesi gerekmektedir[301]. Burada önemli olan hangi durumlarda kayıt işleminin hukuka aykırı olup olmayacağı konusunun net olmasıdır. KVKK yürürlüğe girmeden önce bu konunun net olmadığını açıkça ifade edebiliriz. Bu konuda 5237 sayılı Türk Ceza Kanunu'nun 135. maddesinin gerekçesinde de net bir tanımın yapıldığını söyleyemeyiz. Kanunilik ilkesi göz önüne alındığında ciddi belirsizliklere sebep olan böyle bir konuda KVKK'nın yürürlüğe girmesi ile birlikte var olan bu boşluğun giderilmesi elbette önemlidir. TCK'da var olan boşluk Kanun koyucu tarafından KVKK düzenlenmesi

[296] Türk Ceza Kanunu, m. 135 Gerekçesi, s.88.
[297] Veli Özer Özbek, Koray Doğan, Pınar Bacaksız, İlker Tepe, Türk Ceza Hukuku Özel Hükümler, 11. Baskı, Ankara, Seçkin, 2017, s. 570.
[298] Ersan Şen, 5237 sayılı TCK'da Özel Hayata Karşı Suçlar, İstanbul Barosu Dergisi, C.79, S.3, 2005, s. 717-718; Kuşkonmaz, a. g. e., s. 128; Murat Volkan Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, 6.Baskı, Ankara, Seçkin, 2015, s. 679
[299] Sedat Erdem Aydın, AİHM İçtihatları Bağlamında Kişisel Verilerin Kaydedilmesi Suçu, İstanbul, On İki Levha, 2015, s. 1128.
[300] Dülger, a. g. e., s. 679.
[301] Özbek, Koray, Bacaksız, Tepe, a. g. e., s. 574.

esnasında dikkate alınıp kişisel verilerin kaydedilmesi suçuna ilişkin düzenlemeler açıkça ifade edilmiştir. Kişisel verilerin kaydedilmesi suçunun oluşabilmesi için bu verilerin ne şekilde ve nasıl kaydedildiğinin hiçbir önemi bulunmamaktadır[302]. Önemle üzerinde durulması gereken konu, kişisel verilerin hukuka aykırı herhangi bir biçimde kaydedilmesidir[303]. Kişisel veriler kural olarak ilgili kişinin rızasının alınması gereken ya da açık rızasının alınmasına gerek olmayan durumlarda işlenebilir. Kişisel verilerin işlenmesi esnasında ilgili kişinin rızasının arandığı durumlar KVKK m. 5/1'de ilgili kişinin açık rızası alınarak işlenebileceği şeklinde düzenlenmiştir. Bunun yanında KVKK m. 5/2'ye göre de kişisel veriler ilgili kişinin açık rızası olmadan da hukuka uygun olarak işlenebilecektir. Dolayısıyla veri işleme faaliyetinin bir kanuna dayanması durumunda ilgili kişinin rızası olmasa dahi kişisel verisi işlenebilecektir. Kişisel verilerin kaydedilmesi eyleminin, hukuka uygun olarak yapılabilmesi için KVKK'da yer alan düzenlemeler doğrultusunda yapılması gerekmektedir. Bahse konu bu düzenlemeler dışında yapılan her faaliyet hukuka aykırılıkların oluşmasına sebebiyet verecektir. İlgili kişinin kişisel verilerinin kaydedilmesinde asıl olan kaydedilen verilerin sonradan kullanılmak üzere depolanması[304] işlemidir. Kişisel verilerin var olan düzenlemelere uygun olarak kaydedilmesine ilişkin temel ilkeleri göz önünde bulundurduğumuzda hangi fiillerin tipikliği oluşturduğunu bulmamız mümkün olacaktır[305]. Kişisel verilerin kaydedilmesi suçunun oluşabilmesi için verilerin kaydedilmesi yeterli olup bu anlamda verileri alenileştirilmesi veya ilgili kişinin herhangi bir zarara uğratılması gerekmemektedir[306].

TCK m. 135/1'de düzenlenen suç açısından gerçek kişiyle ilgili olan her türlü bilgi kişisel veri olarak kabul edilmektedir. TCK m. 135/2'de düzenlenen suçun konusu ise; kişilerin *"siyasi, felsefi veya dini görüşlerine, ırki kökenlerine, ahlaki eğilimlerine, cinsel yaşamlarına sağlık durumlarına veya sendikal bağlantılarına"* ilişkin bilgilerdir[307]. TCK m.135/2'de sayılan ve daha fazla ceza öngörülen veriler hassas nitelikli kişisel verilerdendir.

[302] Özbek, Koray, Bacaksız, Tepe, a. g. e., s. 574.
[303] Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, s. 680.
[304] Osman Yaşar, Hasan Tahsin Gökcan, Mustafa Artuç, Yorumlu-Uygulamalı Türk Ceza Kanunu, C.III, Ankara, Adalet, 2010, s. 4437.
[305] Küzeci, a. g. e., s. 403; Özbek, Doğan, Bacaksız, Tepe, a. g. e., s.574.
[306] A. g. e., s.575; Dülger, a. g. e., s.681.
[307] Parlar, Ali/ Hatipoğlu, Muzaffer, Türk Ceza Kanunu Yorumu, 2. Baskı, Cilt: 2. Ankara, 2008, s. 2043.

TCK m. 135/2'de düzenlenen hassas veriler arasında ayrıma gidilerek, ilgili kişilerin *"siyasi, felsefi veya dini görüşlerine, ırki kökenlerine ilişkin bilgiler"* salt dokunulmaz veri olarak kabul edilirken; ilgili kişilerin *"ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgiler"* göreceli dokunulmaz veri olarak kabul edilmektedir. Burada ilk kısımda yer verilen kişisel veriler hiçbir koşulda kaydedilmemesi gerekirken, ilgili düzenlemede yer alan *"hukuka aykırı olarak"* ifadesi nedeniyle, ikinci kısımda yer alan kişisel verilerin kaydedilmesi, bu nedenle saymış olduğumuz verilerin işlenmesine izin verilen hükümlerin bulunması durumunda mümkün olabilecektir[308].

Türk Ceza Kanunu'nda düzenlenen kişisel verilerin kaydedilmesi suçunun TCK m. 135/2'de daha detaylı bir biçimde düzenlendiği görülmektedir. Kişisel verinin, hukuka aykırı olarak, ilgili kişinin cinsel yaşamına, sağlık bilgilerine, sendikal bilgilerine ve kişinin ahlaki yönelimlerine ilişkin olması durumlarında birinci fıkrada zikredilen ceza ağırlaştırılacaktır. Buna ilave olarak verinin siyasal, dini, felsefi görüşleri veya ırki kökenine ilişkin olması durumunda yapılan işlemde hukuka aykırılık olsun veya olmasın kişisel verinin kaydedilmesi suçunun oluşacağı ve aynı şekilde cezanın ağırlaşacağı ifade edilmektedir[309]. Buradaki fıkrada ifade edilen kişisel veri türlerinin hukuka aykırı olarak kaydedilmesi haline düzenlenmiş olan cezanın daha ağır bir biçimde uygulanması gerektiği ifade edilmiştir. Dolayısıyla bu durumda söz konusu fıkra ile cezanın ağırlaştıran nitelikli hali öngörülmüştür[310].

KVKK'da düzenlenen özel nitelikli kişisel veriler ile Türk Ceza Kanunu m. 135/2'de düzenlenen özel nitelikli kişisel veriler arasında uyumsuzluk bulunmaktadır. Kişisel Verilerin Korunması Kanunu'nda özel nitelikli kişisel verilerin işlenme şartları başlığı altında özel nitelikli kişisel veriler sıralanırken Türk Ceza Kanunu m. 135/2'de bunlar sayılmamaktadır. Ayrıca kişisel verilerin kaydedilmesi suçu bakımından kişinin ahlaki eğilimlerinin, KVKK bakımından özel nitelikli kişisel veri olarak kabul edilmemesine

---

[308] Özbek, Veli Özer/ Kanbur, Mehmet Nihat/Doğan, Koray / Bacaksız, Pınar/ Tepe, İlker, Türk Ceza Kanunu Özel Hükümler, Ankara, 2013, Seçkin Yayınevi, s. 530.
[309] A. g. e., s.578; Küzeci, a. g. e., s. 403.
[310] Özbek, Doğan, Bacaksız, Tepe, a. g. e., s. 575; Dülger, a. g. e., s. 575.

rağmen Türk Ceza Kanunu bakımından sayıldığı görülmektedir. Dolayısıyla böyle bir karmaşıklığın olmaması için bu uyumsuzluğun giderilmesi elzemdir[311].

4.1.2.2. Verileri hukuka aykırı olarak verme veya ele geçirme suçu

"Kişisel verileri hukuka aykırı olarak verme, yayma veya ele geçirme suçunun" düzenlendiği Türk Ceza Kanunu m. 136'ya göre*, "kişisel verileri hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren iki yıldan dört yıla kadar hapis cezasıyla cezalandırılır*" (m. 136).

Bireylere ait kişisel veriler ister hukuka uygun olsun isterse de hukuka uygun olmayan bir yöntemle kaydedilmiş olsun söz konusu bu kişisel verilerin hukuka aykırı olarak bir başkası ile paylaşılması, yayılması veya ele geçirilmesi durumunda suç oluşacaktır[312]. Çünkü burada bu suç tipi ile amaçlanan, hukuka uygun olacak şekilde toplanan kişisel verilerin daha sonra yine hukuka uygun olacak bir biçimde saklanmasını ve kullanılmasını temin etmektir[313].

Kişisel verilerin, KVKK m. 4'te yapılan düzenlemeler dikkate alındığında belirli, açık ve meşru amaçlar için hukuk ve dürüstlük kurallarına uygun olarak işlenmesi söz konusu olacaktır. Dolayısıyla bu ilkeler göz önünde bulundurularak toplanan kişisel verilerin yine aynı ilke ve kurallara uygun olarak saklanması ve kullanılması gerekmektedir. Bahse konu kural ve ilkeler KVKK hukukuna hâkim olan unsurlardır. Kural ve ilkelerin uygulanmasının ceza hukuku normları ile koruma altına alındığını ifade edebiliriz[314].

Suçun hareket unsurlarını oluşturan fiilleri *"verme, yayma veya ele geçirme"* şeklinde sıralayabiliriz. Toplanan veya depolanan kişisel verilerin ilgili kişinin rızası dışında bir başkasına verilmesi veya yayılması fiilleri aslında bu verilerin aktarılmasını ifade etmektedir[315]. Burada zikredilen "verilmesi" fiili, var olan kişisel verilerin bir başkasına aktarılmasını ifade etmekle birlikte, sınırlı bir etki alanına sahip olduğunu ifade edebiliriz[316].

---

[311] Küzeci, a. g. e., s. 405.
[312] Soyaslan, Doğan, Ceza Hukuku Özel Hükümler, 8. Baskı, Ankara, Yetkin, 2010, s. 345-346.
[313] Küzeci, a. g. e., s. 407.
[314] Kuşkonmaz, a. g. e., s. 152.
[315] Özbek, Doğan, Bacaksız, Tepe, a. g. e, s. 583;
[316] Rezzan İtişgen, ''Türk Ceza Hukukunda Kişisel Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme Suçu'', Y.6 S. 23, Ekim 2015, s. 188.

Fakat "yayılması" fiilinin doğurduğu etki bakımından sonucunda birçok kişiye verinin aktarılması mümkündür[317]. Bunların dışında "ele geçirmek" fiiline baktığımızda ise herhangi bir bilişim sisteminde kayıtlı bulunan kişisel verilerin alınması anlamını taşımaktadır[318]. Kişisel verilerin kaydedilmesi suçunun TCK'da ayrıca düzenlendiğini bilmekteyiz. Kişisel verilerin ele geçirilmesi suçunun oluşması için, kaydetme fiili dışındaki başka hareketlerin varlığı gerekmektedir[319]. Kişisel verileri hukukun çizdiği çerçevenin dışına çıkarak verme, yayma ve ele geçirmek suçlarının kamu görevlisi tarafından ve görevinin sağlamış olduğu yetkiyi kötüye kullanmak suretiyle ya da belirli bir meslek veya sanatın sağladığı kolaylıktan faydalanmak suretiyle işlenmesi durumunda verilecek olan ceza yarı oranında arttırılacaktır (m. 137).

Kişisel verilerin hukuka aykırı olarak bir başkasına verilmesi veya yayılması söz konusu olduğunda TCK m. 136'da düzenlenen suç da ayrıca oluşacağı için, gerçek içtima kuralları dikkate alınarak her iki suçtan ayrı ayrı ceza verilecektir. Kaydedilen kişisel verilerin ifşa edilmesi durumunda ayrıca hakaret suçu da oluşuyorsa, bu durumda da gerçek içtima kuralları söz konusu olacaktır[320].

4.1.2.3. Kişisel verilerin yok edilmemesi suçu

Bahse konu çalışmamızın daha önceki bölümlerinde de anlattığımız üzere, kişisel verilerin işlenmesi, verilerin elde edilmesinden başlayarak, bu verilerin kaydedilmesine, üçüncü kişilere aktarılmasından yok edilmesi de dahil olmak üzere geçen süreçte kişisel veriler üzerinde yapılan her türlü işlemi kapsamaktadır. Bunun gibi KVKK'da bütüncül bir sistem olarak, bu kapsamda sadece kişisel verilerin kaydedilmesini değil, tüm veri işleme aşama ve ihlallerini de korumaktadır.

Kişisel verilerin yok edilmemesi suçunun düzenlenmiş olduğu TCK m.138 gereğince; "*Kanunların belirlediği sürenin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde bir yıldan iki yıla kadar hapis cezası verilir*" denilmektedir.

317 Doğan, a. g. e., s. 345-346; Yaşar, Gökcan, Artuç, a. g. e s. 4126.
318 Kuşkonmaz, a. g. e., s.154; Yaşar, Gökcan, Artuç, a. g. e s. 4126; Dülger, a. g. e., s. 713.
319 Özbek, Doğan, Bacaksız, Tepe, a. g. e, s. 584;
320 Parlar, Ali/ Hatipoğlu, Muzaffer, Türk Ceza Kanunu Yorumu, 2. Baskı, Cilt: 2. Ankara, 2008, s. 2043.

Kişisel verilerin yok edilmemesi suçunda fail, kişisel verileri sistemde yok etmekle yükümlü olan kişilerdir[321]. Bahse konu verileri yok etmek bu kişilerin görev tanımında bulunmak zorundadır[322]. Bu nedenle bu suç tipi özgü bir suçtur[323].

Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hâle Getirilmesi Hakkında Yönetmelik'e göre kişisel verilerin yok edilmesi, söz konusu verilerin herhangi bir kimse tarafından ulaşılamaz ve tekrar kullanılamaz duruma getirilmesi anlamına gelmektedir (m. 9).

Kişisel veriler, KVKK m. 4'e göre ilgili düzenleyici işlemlerde öngörülen süreler dikkate alınarak ve en önemlisi işlendikleri amaç doğrultusunda belirlenen süre kadar muhafaza edilmelidir. Kişisel verileri yok etmeme suçu, KVKK da hâkim olan ilkelere göre koruma sağlamaktadır[324]. Burada verilerin yok edilmemesi ile ilgili olarak KVKK m. 17/f.2'ye göre; KVKK m. 7'de yapılmış olan düzenlemeye aykırı olarak verileri silmeyen veya anonim hâle getirmeyenler hakkında, 5237 Türk Ceza Kanunu'nda yer bulan düzenlemeye göre verileri yok etmeme suçu hükmüyle cezalandırılabileceklerdir. Ayrıca TCK'dan ayrı olarak Ceza Muhakemesi Kanunu gereği, tamamen yok edilmesi gereken bir verinin varlığı söz konusuysa ilgililer hakkında verilecek cezanın ağırlaştırılması gerekmektedir (m.138/2). Dolayısıyla CMK m. 80'de düzenlenen koşulların gerçekleşmesine karşın, ilgili verilerin yok edilmemesi durumunda TCK m. 138/2'de düzenlenen suçun nitelikli hali oluşacaktır.

Önemle belirtmek gerekir ki, kişisel verileri KVKK'nın ilgili maddelerine aykırı olarak yok edilmemesi durumunda, bir zararın oluşup oluşmadığı dikkate alınmadan suçun oluşumundan bahsedilecektir[325].

[321] Özbek, Doğan, Bacaksız, Tepe, a. g. e, s.588; Doğan, a. g. e., s.345-346; Yaşar, Gökcan, Artuç, a. g. e., s. 4133.
[322] Özbek, Doğan, Bacaksız, Tepe, a. g. e, s. 589;
[323] A. g. e., s. 4133;
[324] Küzeci, a. g. e., s. 408.
[325] Özbek, Doğan, Bacaksız, Tepe, a. g. e, s. 589;

4.1.3. Kişisel Verileri Silmeme ve Anonim Hâle Getirmeme Suçu

Kişisel Verilerin Korunması Kanunu m. 17/2'de bu suç tipi ayrıca düzenlenmektedir. Bu düzenleme gereğince "*Bu Kanunun 7'nci maddesi hükmüne aykırı olarak; kişisel verileri silmeyen veya anonim hâle getirmeyenler 5237 sayılı Kanunun 138 inci maddesine göre cezalandırılır*" denilmektedir. Yapılan bu düzenlemede özel bir suç tipi belirlenmiş olup sadece yaptırım açısından TCK'nın ilgili maddesinde işaret edilmiştir. Kişisel verileri, KVKK m. 7'de yer alan düzenlemelere göre silmeyen veya anonim hâle getirmeyenler, Türk Ceza Kanunu m. 138'de yer alan *"verileri yok etmeme"* suçu bakımından cezalandırılırlar.

Hukuk kurallarına uygun olarak işlenmiş olan kişisel veriler, işlenme amacının sona ermesi ile birlikte re'sen ya da ilgili kişinin talebi ile silinebilir, yok edilebilir veya anonim hâle getirilmesi söz konusu olabilecektir. Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hâle Getirilmesi Hakkında Yönetmelik'te yapılan düzenlemeye göre kişisel verilerin silinmesi, kişisel verileri işlenen kullanıcıların ilgili verilere hiçbir biçimde ulaşamamaları yani verileri tekrar kullanamamaları anlamına gelmektedir (m. 8). Kişisel verilerin yok edilmesi ise, ilgili verilerin hiç kimse tarafından kullanılamaz ve ulaşılamaz duruma getirilmesidir (m. 9). Anonim hâle getirme, ilgili verinin hiçbir biçimde kimliği belirlenebilen kişiyle ilgisinin kurulamayacak duruma getirilmesi şeklinde ifade edilebilir (m. 10).

Bahse konu suçun maddi unsurunu KVKK'na aykırı biçimde, kişisel verileri silmemek veya anonim hâle getirmemek oluşturmaktadır. Burada dikkat edilmesi gereken anonimleştirilmiş verilerin yeniden verisi işlenen kişilerle bağlantılı hâle getirilmesi suç olarak düzenlenmemiştir. Dolayısıyla bunun bir eksiklik olduğunu net olarak ifade edebiliriz. Bu eksikliğin giderilebilmesi için iç hukukumuzda ayrı bir suç tipi olarak düzenlenmesinde yarar olacağı kanaatindeyiz.

Kişisel verilerin silinmesine, yok edilmesine veya anonim hâle getirilmesine ilişkin esaslar Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hâle Getirilmesi Hakkında Yönetmelik'te düzenlenmiştir. Söz konusu düzenlemede re'sen ya da talep üzerine verilerin nasıl ve ne zaman silineceğine ilişkin düzenlemeler bulunmaktadır. Bu düzenlemelere aykırı

hareket edilmesi durumunda KVKK m. 17/2'de yer alan suç oluşacak ve ilgili faile, TCK'de düzenlenen verileri yok etmeme suçunun cezası uygulanacaktır.

Kişisel Verilerin Korunması Kanunu m. 7/1 hükümleri gereğince suçun faili veri sorumlusudur. Bundan dolayı özgü suç niteliği taşımaktadır. Kişisel Verilerin Korunması Kanunu m. 3/1-ı'de "*kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi"* ifade eden veri sorumlusunun nitelikleri düzenlenmiştir. İlgili Kanun m. 7'de kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesinden veri sorumlusunun yükümlü olduğu şeklinde düzenlenmiştir. Buna göre suç tipi, anılan maddeler ve atıflar birlikte incelendiğinde suç tipi şu şekilde ifade edilebilir: "*6698 sayılı Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebepleri ortadan kalkan kişisel verilerin resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinmemesi, yok edilmemesi veya anonim hâle getirilmemesi halinde veri sorumlusu gerçek kişi ise bu kişiye, tüzel kişi ise yetkili ve görevli organ ve/veya temsilcilerine ...hapis cezası verilir*[326]*."* Bura da önemle belirtmek gerekir ki tüzel kişiler suçun faili olamazlar dolayısıyla tüzel kişiler bakımından bahse konu işlemlerden kimlerin sorumlu olacağının ilgili kanunda açıkça düzenlenmesi gerekmektedir[327].

Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hâle Getirilmesi Hakkında Yönetmelik'te KVKK m. 7/3'de yer alan düzenlemelerin dışında özel kanunlarda bulunan düzenlemeler mahfuzdur. Örneğin bir üniversite öğrencisinin kişisel verilerinin KVKK dışında ki düzenlemeler dikkate alınarak belirli bir süre saklanabileceğine dair düzenlemeler yapılmış ise de, hukuka uygun olarak işlenmiş bu verilerin belirlenen süre boyunca saklanması yine aynı şekilde hukuka uygun olacaktır. Belirlenen süreler boyunca kişisel verilerin silinmesine dair yapılacak başvurular bu özel düzenlemeler dikkate alınarak reddedilecektir. Bir diğer örneğimizde de Kişisel Verileri Koruma Kurulu'nun 05/12/2018 tarihli kararında; 5411 sayılı Bankacılık Kanunu m. 42'ye göre, alınmış olan yazı ve faaliyetlere ilişkin dokümanların asılları veya kopyaları ile yazılan yazıların tarih ve sıra numarası verilerek on yıl süreyle banka sorumluluğunda saklanır. Kişisel Verileri Koruma

[326] Dülger, a. g. e., s.135.
[327] Dülger, a. g. e., s.136.

Kurulu'na yapılan başvuruda, ilgili kişinin, veri sorumlusu bankaya ait veri kayıt sisteminde bulunan verilerinin silinmesi ile ilgili talebinin değerlendirildiği kararda, kanuni düzenlemede yer alan on yıllık sürenin dolmadığı, bu sebeple ilgili kişinin talebinin veri sorumlusu banka tarafından kabul edilmemesinde herhangi bir hukuka aykırılık bulunmadığı ifade edilmiştir[328].

4.1.4. Kişisel Verilerin Korunması Kanunu'nda Düzenlenen Kabahatler

Çalışmamızın bu bölümünde Kişisel Verilerin Korunması Kanunu'nda bahsedilen kabahatlere değinilecektir. Kişisel verilerin korunmasına yönelik kabahatler, Kabahatler Kanunu'nda düzenlenmeyip Kişisel Verilerin Korunması Kanunu'nda düzenlenmiştir. KVKK m. 18'de, atıfta bulunan yükümlülüklerin ihlali durumunda, yapılan ihlal bakımından farklı miktarda düzenlenen idari para cezalarına hükmedilir.

4.1.4.1. Veri güvenliği bakımından yükümlülüklerin yerine getirilmemesi

Veri güvenliğinin sağlanması ile ilgili yükümlülükler KVKK m. 12'de düzenlenmiştir. Veri sorumlusu veya yetkilendirdiği kişinin, verilerin hukuk kurallarına uygun olarak işlenmesini ve saklanmasını sağlamak, bu bağlamda kişisel verilerin güvenliği için her türlü idari ve teknik tedbirleri alma zorunluluğu bulunmaktadır. Veri güvenliğine ilişkin sorumlulukları "yerine getirmeyenler hakkında 15.000 Türk Lirası'ndan 1.000.000 Türk Lirası'na kadar idari para cezası" uygulanacağı ilgili yasal düzenlemede ifade edilmiştir.

Veri sorumlusu, yetkilendirdiği kişi veya verileri işleyen kişiler bağlı bulundukları kurumdan ayrılsalar bile, görev süresi içerisinde işlemiş oldukları verileri hukuka aykırı olarak başkalarına açıklayamaz veya amacı dışında kullanamazlar. Verilerin veri sorumlusu tarafından yetkilendirdiği kişi tarafından işlenmesi durumunda, veri sorumlusunun sorumluluğu devam etmektedir. Dolayısıyla yetkilendirilen kişi ile birlikte veri sorumlusunun sorumluluğu devam edecektir.

Veri sorumlusu yukarıda bahsettiğimiz üzere veri güvenliğine ilişkin her türlü idari ve teknik tedbiri almak zorundadır ve buna rağmen bir ihlal söz konusu olduğunda bu ihlali en kısa

[328] Kişisel Verileri Koruma Kurulunun 05/12/2018 tarihli ve 2018/142 sayılı Karar, (Çevrimiçi), https://kvkk.gov.tr/Icerik/5424/-Ilgili-mevzuatta-ongorulen-veya-islendikleri-amac-icin-gerekli-olan-sure-kadar-muhafaza-edilme-ilkesi-gereginceKisisel-verilerin-silinmemesi-hakkinda-Kisisel-Verileri-Koruma-Kurulunun , 05-12-2018-tarihli-ve-2018-142-sayili-Karari-Ozeti, (Erişim Tarihi: 02/03/2022).

sürede kişisel Verileri Koruma Kurumu'na bildirmek zorundadır. Burada bildirim süresinin "en kısa sürede" kavramı ile açıklanması hukuki açıdan bir belirsizlik durumunun söz konusu olabileceği kanaatindeyiz. Dolayısıyla bu anlamda bildirim sorumluluğunun suiistimal edebileceğini ifade etmek gerekir. Veri Koruma Tüzüğü m. 33'te veri sorumlusunun, kişisel verilere ilişkin bir ihlal gerçekleştiği durumda gecikmeksizin ve en geç yetmiş iki saat içerisinde söz konusu ihlal bildirimini gerekli birimlere yapması gerektiği ifade edilmektedir. Kurul veri ihlaline ilişkin bildirimleri, gerek görürse durumu kamuoyuna kendi internet sitesinden ya da başka yöntemlerle bildirir[329]. Kurul'un var olan ihlalleri kamuoyu ile paylaşması Kurul'un takdirine bırakıldığı için kanaatimizce burada da keyfilik söz konusu olabilir. Burada yapılması gereken ilgili yasal düzenlemede hangi bildirimlerin kamuoyuyla paylaşılacağının net olarak ifade edilmesidir.

Veri Koruma Tüzüğü'nde düzenlenen en geç yetmiş iki saat düzenlemesi dikkate alınarak bildirim yapılamıyorsa, yapılmış olan gecikmenin nedeni ve ihlal bildirimi Kişisel Verileri Koruma Kurulu'na yapılmak zorundadır. Kurul bu anlamda bu gecikmelere ilişkin çeşitli kararlarında idari para cezalarının uygulanmasına karar vermiştir.

4.1.4.2. Kişisel verileri koruma kurulu tarafından alınan kararların yerine getirilmemesi

Kişisel verileri koruma kurulu gerek şikâyet üzerine gerek re'sen yapacağı incelemede KVKK anlamında herhangi bir ihlal tespit ederse söz konusu ihlalin giderilmesine ilişkin karar alınarak dosyayı ilgili veri sorumlusuna gönderir. Veri sorumlusu ise söz konusu ihlal ile ilgili kararın kendisine tebliğ edildiği tarihten itibaren en geç otuz gün içerisinde kararı yerine getirmek zorundadır. Kararın yerine getirilmemesi durumu ile ilgili kişisel verilerin Korunması Kanunu m. 18/1-c'de düzenleme yapılmıştır. Bu düzenlemeye göre Kişisel Verileri Koruma Kurulu tarafından alınan kararı yerine getirmeyenler için "25.000 Türk Lirası'ndan 1.000.000 Türk Lirası'na kadar idari para" cezasının uygulanacağı ifade edilmiştir.

Kurul ilgili kişinin yapmış olduğu başvuruda veri kayıt sistemindeki mevcut kişisel verilerin silinmemesi amacıyla vermiş olduğu kararda, "*Kurul Kararı 02.07.2018 tarihinde*

[329] (Çevrimiçi), https://www.kvkk.gov.tr/Icerik/5483/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-Pizza-Restaurantlari-A-S-Domino-s-Pizza- , (Erişim Tarihi: 02/03/2022).

veri sorumlusuna tebliğ edilmiştir. Bu kapsamda veri sorumlusunun, Kurul Kararı kapsamında 16.08.2018 tarihinde şikâyetçiye bilgi verdiği, bu hususun da 17.08.2018 tarihli yazı ile Kurula bildirildiği görülmekte olup, Şirket tarafından ilgili mevzuat hükümleri çerçevesinde en geç 01.08.2018 tarihinde yapılması gereken işlemin 16.08.2018 tarihinde yapıldığı; diğer yandan şikâyetçinin, veri sorumlusu nezdinde bulunan kişisel verilerin den asgari saklama süresi tamamlanmış olanlarının kişisel verilerin Silinmesi, Yok Edilmesi veya Anonim Hâle Getirilmesi Hakkında Yönetmeliğin 11 inci maddesinin (1) numaralı fıkrası gereğince ilk periyodik imha işleminde, kalanların da yasal saklama yükümlülüğünün dolmasını müteakiben yapılacak periyodik imha işlemi dönemlerinde silinmesine ve gerçekleşecek silme işlemleri hakkında Şikâyetçiye bilgi verilmesi ayrıca, söz konusu kişisel verilerin saklama amacı dışında işlenmemesi hususunda veri sorumlusunun talimatlandırılmasına karar verilmiş olmasına rağmen Şirketin şikâyetçiyi muhatap 16.08.2018 tarihli yazısında Kurul Kararının bu maddelerine ilişkin herhangi bir açıklamada bulunmadığı tespit edilmiştir." açıklanan kararda kurul tarafından verilen kararın yerine getirilmemesinden dolayı idari para cezası vermiştir[330].

4.1.4.3. Veri sorumluları siciline kaydolma yükümlülüğünün yerine getirilmemesi

Kişisel Verilerin Korunması Kanunu m. 18/1-ç'de yapılan düzenlemeye göre, Veri Sorumluları Siciline kayıt ve bildirim yükümlülüğüne aykırı hareket edenler için "20.000 Türk Lirası'ndan 1.000.000 Türk Lirası'na kadar idari para cezası" verilmesi öngörülmüştür.

Kişisel Verilerin Korunması Kanunu m. 16'da yapılan düzenlemede ise, kişisel verileri işleyen gerçek veya tüzel kişilerin, verileri işlemeye başlamadan önce Kişisel Verileri Koruma Kurumu tarafından aleni olarak tutulan Veri Sorumluları Sicili'ne kaydolma zorunluluğu bulunmaktadır. Yapılacak olan başvuruda, veri sorumlusu ve varsa temsilcisinin kimlik bilgileri, kişisel verilerin hangi amaçlarla işlenebileceği, kişisel veri güvenliğine ile ilgili alınan güvenlik tedbirleri hakkında bilgilerin yer alması gerekmektedir. Veri Sorumluları Sicili Hakkında Yönetmelik'e[331] göre, ilk başta Veri Sorumluları Sicili'ne kayıt yükümlülüğü bulunmayan ancak daha sonra kayıt yükümlülüğü doğan veri

[330] Kişisel Verileri Koruma Kurulunun 14/02/2019 tarihli ve 2019/23 sayılı Karar Özeti, (Çevrimiçi), https://www.kvkk.gov.tr/Icerik/5464/2019/52 , (Erişim Tarihi: 23.07.2021).
[331] Veri Sorumluları Sicili Hakkında Yönetmelik, 30.12.2017 tarihli 30286 sayılı Resmi Gazete.

sorumlularının, bu yükümlülüklerinin doğumundan itibaren otuz gün içerisinde Veri Sorumluları Sicili'ne kayıt olma zorunlulukları bulunmaktadır (m. 8). Düzenlemede bulunan bu süre içerisinde sicile kayıt yaptırmayan veri sorumluları için kabahat fiili söz konusu olacaktır.

4.1.4.4. Aydınlatma yükümlülüğünün yerine getirilmemesi

Kişisel Verilerin Korunması Kanunu m. 10'da veri sorumlusu veya onun yetkilendirdiği kişinin, ilgili kişileri aydınlatma yükümlülüğü düzenlenmiştir. Bu düzenlemeye göre veri sorumlusu ya da görevlendirilen ilgili kişinin, "*veri sorumlusunun ve varsa temsilcisinin kimliği, kişisel verilerin hangi amaçla işleneceği, işlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceği, kişisel veri toplamanın yöntemi ve hukuki sebebi ve kişisel verilerin Korunması Kanunun 11. maddesinde sayılan diğer hakları*" konularında bilgilendirme yükümlülüğü bulunmaktadır (m. 10/1). Kişisel Verilerin Korunması Kanunu m. 10'da yapılan düzenlemeler 95/46/AT sayılı Yönerge dikkate alınarak paralel şekilde düzenlemelerin olduğu görülmektedir.

Kişisel Verilerin Korunması Kanunu m. 11'de ise, kişisel verileri işlenen kişilerin haklarını düzenlemektedir. Bu düzenlemede verileri işlenen kişinin kendisi ile ilgili verilerin işlenip işlenmediği konusunda bilgi sahibi olma, şayet işlenmiş ise buna dair bilgileri talep etme, verilerin işlenme amacı ile bu verilerin işlenme amacına uygun olarak kullanılıp kullanılmadığını öğrenme, verilerinin aktarılıp aktarılmadığını öğrenme, şayet aktarılmış ise kimlere aktarıldığını öğrenme, bunların dışında KVKK m. 7'de düzenlenen koşullar çerçevesinde, verileri işlenen kişinin bu verileri silinmesini, yok edilmesini veya işlenmiş olan verilerinin içeriğinin eksik ya da gerçeğe aykırı olması durumlarında bunların düzeltilmesini isteme hakkına, bunların dışında kişisel verilerin otomatik sistemler aracılığıyla analiz edilmesi sonucunda, ilgili kişinin aleyhine sonuçlar çıkarılmasına itiraz etme hakkı, verilerin ilgili yasal düzenlemelere aykırı olarak işlenmesi ve zarara uğraması durumunda bu zararın giderilmesini talep hakkı bulunmaktadır.

Aydınlatma yükümlülüğünü yerine getirmeyenler için KVKK m. 18/1-a'da "5.000 Türk Lirası'ndan 100.000 Türk Lirası'na kadar idari para cezasına" hükmedileceği düzenlenmiştir.

4.2. AYDINLATMA YÜKÜMLÜLÜĞÜNÜN ESASLARI

4.2.1. Kişisel Verilerin İşlenmesinde Açıklık (Şeffaflık) İlkesi

Kişisel Verilerin Korunması Kanunu bağlamında aydınlatma yükümlülüğünün, kişisel verilerin işlenmesine hâkim ilkeler ile önemli bir ilişki içerisinde olduğunu ifade edebiliriz. Bunlardan belki de en önemlisi, kişisel verilerin hukuka ve dürüstlük kurallarına uygun olarak işlenmesi ilkesinin bir görünümü olan "açıklık (şeffaflık) ilkesi" olduğunu söyleyebiliriz[332].

GDPR m. 5/1-a'da "*hukuka ve dürüstlük kuralına uyma ilkesi"*nin yanı sıra şeffaflık ve adalet kavramları dile getirildiği görülmektedir. Verilerin işlenmesi sırasında hukuka uygun olarak kişisel verilerin toplanarak işlenmesi ilkesi, kişisel verilerin işlenmesi sürecinin neredeyse tamamında, veri toplama ve işleme hususlarında bahse konu kişilerin aldatılmaması veya veri işleme amacıyla bağdaşmayan ya da kişilerin anlamayacakları bir amaç için işlenmemesi başlıklarını kapsamaktadır[333]. Bahsetmiş olduğumuz başlıklar bir bakımdan dürüstlük kuralının temelini de teşkil eden "amaca uygun davranma ve yanıltmama" ilkeleri ile uyuşmaktadır[334].

Kişisel verilerin işlenmesinde, hukuka ve dürüstlük kurallarına uyulması gerektiği KVKK m. 4/2'de bulunan düzenlemede ifade edilmiştir. Bireylerin kişisel verilerinin işlenmesi sürecinin tamamı bu ilkeye uygun olarak yürütülmesi gerekmektedir[335]. Kişisel verilerin hukuk kurallarına uygun olarak, adil ve şeffaf şekilde işlenmesi gerektiği Veri Koruma Tüzüğü m. 5'te de ifade edilmektedir.

Kişisel verilerin hukuk kurallarına uygun olarak işlenmesi, veri işleme faaliyeti sırasında, hem KVKK'na ilişkin genel prensiplerin dikkate alınması hem de yer alan düzenlemelere uygun hareket edilmesi anlamına gelmektedir[336]. Dürüstlük kuralına uygun olarak kişisel verileri işleme, ilgili kişinin menfaatlerinin ve haklı beklentilerinin dikkate alınması, veri

---

[332] Guidelines on Transparency under Regulation 2016/679, 11.04.2018, (Çevrimiçi), https://datenschutz-hamburg.de/assets/pdf/wp260rev01_en.pdf , (Erişim Tarihi: 02/03/2022).
[333] Başalp, a. g. e., s. 37;
[334] Ayözger, a. g. e., s.120.
[335] Özdemir, a. g. e., s.137.
[336] Nafiye Yücedağ, Kişisel Verilerin Korunması Kanunu Kapsamında Genel İlkeler, Kişisel Verileri Koruma Dergisi, C.1, S.1, 47-63, 2019, s. 49.

sorumlusuna duymuş olduğu güvenin kötüye kullanılmaması, yanılgısından yararlanılmaması anlamlarını taşımaktadır[337].

Şeffaflık ilkesi, verilerin işlenmesi bakımından yapılan uygulama, politika ve düzenlemelerin ilgili kişilerce bilinebilir olmasını ifade etmektedir[338]. OECD kapsamında hazırlanan Rehber İlkeleri'nde yer alan düzenlemelerde de kişisel verilerin işlenmesine ilişkin politikalar, uygulamalar ve gelişmeler bakımından şeffaflık bulunması gerektiği; ilgili kişilerin, verilerin işlenme amaçları ile veri sorumluları hakkındaki bilgilere basit bir şekilde ulaşabilmesi gerektiği ifade edilmektedir (m. 12). Kişisel verilerin işlenmesi sürecinin tüm aşamalarının ilgililer tarafından bilinebilir olması şeffaflık açısından oldukça önemlidir. Bu durumda ilgili kişiler, verilerinin hukuk kurallarına ve dürüstlük kurallarına uygun olarak işlenip işlenmediği hakkında detaylı bilgi sahibi olabilirler. Çünkü bireylerin kişisel verilerinin KVKK'na uygun olarak toplanması ve bu kanuna uygun olarak işlenmesi ve bu işlem süreçlerinde ilgililerin yanıltılmaması gerekmektedir[339]. Verisi işlenen kişiler, verilerin işlenme sürecinde hukuki düzenlemelerde kendilerine tanınan hakları kullanmak suretiyle aktif rol alma hakkına sahiptirler. Bu konuda, 108 sayılı Avrupa Konseyi Sözleşmesi m. 8'de ilgili kişiler hakkında ek güvenceleri düzenlenmiştir. İlgili kişinin, kendisi için hazırlanmış olan bir veri dosyasının bulunup bulunmadığını, şayet böyle bir dosya var ise hangi amaçla tutulduğunu, dosya yöneticisi olan kişinin kimliğini, dosya yöneticisinin sürekli olarak kullanmış olduğu ikamet yerini ve işyerini öğrenme hakkı olduğu ifade edilmektedir. Dolayısıyla ilgili kişi hakkında yapılan veri işleme çalışmasına dair bilgi edinen ilgili kişi, maddenin devamında düzenlenen diğer hakları olarak düzenlenen bu verileri gerekli durumlarda düzelttirme ve sildirme haklarını da kullanması mümkün olacaktır. Tüm bu nedenlerden dolayı veri işleme faaliyetinin olabildiğinde şeffaf olması gerektiği ve ilgili kişilerin bu konuda yeterince aydınlatılmaları gerekmektedir.

KVKK bağlamında, şeffaflık ilkesi; ilgili kişinin verilerin işlenmesi ile ilgili veya hukuken kendisine tanıdığı hakların kullanımı ile ilgili konularda aydınlatılması gerektiğini ifade etmektedir. Yine şeffaflık ilkesi veri sorumlusunun veya temsilcisinin, ilgili kişinin

[337] Yücedağ, a. g. e., s.50.
[338] Şimşek, a. g. e., s. 90;
[339] Özdemir, a. g. e., s.137.

kendisine tanınan haklarını aktif olarak kullanabilmesi için kolaylık sağlamasını da ifade etmektedir[340]. Şeffaflık ilkesi aslında kişisel verileri işleme süreci ve ilgili kişilerin bu süreç içerisinde sahip oldukları hakları konularında kolay, kısa, anlaşılır ve açıkça anlaşılabilir biçimde aydınlatılmalarını ifade etmektedir[341]. Dolayısıyla veri sorumluları veya temsilcilerinin aydınlatma yükümlülükleri buradan kaynaklandığını ifade edebiliriz. Veri Koruma Tüzüğü'nün genel gerekçesinde, şeffaflık ilkesinin önemine vurgu yapılmaktadır. Bu anlatımlardan hareketle kişisel veri işleme faaliyetinin hukuk kurallarına uygun ve adil bir biçimde yürütülebilmesi için verilerin toplanması, depolanması, kullanılması ve değerlendirilmesi hakkında ilgili kişilere olabildiğince açık olunması gerekir. Ayrıca şeffaflık ilkesinin gereği olarak yukarıda bahsedilen bilgilerin mutlak surette sade, açık, anlaşılır bir dille ifade edilmeli ve bu bilgilere erişimin basit olması gerekmektedir.

Veri işleme faaliyetine ilişkin kuralların varlığı, veri güvenliğine ilişkin olarak alınan tedbirler, veri işleme faaliyetine ilişkin riskler ve veri işleme sürecine katılma hakları konusunda bilgilendirilmeleri Veri Koruma Tüzüğü'nün genel gerekçesinde ifade edilmesi oldukça önemlidir. Veri Koruma Tüzüğü m. 5'te *"İlkeler"* başlığında kişisel verilerin, hukuk kurallarına uygun, adil ve şeffaflık ilkesine uygun bir biçimde işlenebileceği ifade edilmektedir (m. 5). Şeffaflık ilkesi Veri Koruma Tüzüğü m. 12'de düzenlenmiştir. Dolayısıyla veri sorumlusu olan kişi, verileri ilgili kişiden elde ettiği durumlarda Veri Koruma Tüzüğü m. 13 gereğince; kişisel verileri üçüncü kişilerden elde ettiği durumlarda m. 14 gereğince ilgili kişileri aydınlatmak zorundadır. Veri sorumlusu veya temsilcisi Veri Koruma Tüzüğü ile ilgili kişilere tanınan hakları açıkça söylemek zorundadır. Bu anlamda kişinin kendisine ait olan verileri düzelttirme, sildirme, gerektiğinde yargı yoluna başvurma gibi hakları olduğuna dair ilgili kişileri bilgilendirme yükümlülüğü bulunmaktadır.

Kişisel Verilerin Korunması Kanunu m. 16'da veri sorumlularının, Kişisel Verileri Koruma Kurul'unun gözetiminde kamuya açık olarak tutulan Veri Sorumluları Sicili'ne kayıt olma yükümlülüğü[342] kişisel verilerin işlenmesinde şeffaflık ilkesinin bir görünümü olarak ifade edilebilir. Çünkü Veri Sorumluları Sicili'nde yer alan veriler sayesinde ilgili kişiler,

[340] Guidelines on Transparency under Regulation 2016/679, s. 4.
[341] A. g. e., s. 7.
[342] Öngün, a. g. e., s. 218.

verilerini işleyen kişiler hakkındaki bilgileri elde ederek, kanun tarafından kendilerine tanınan haklarına ilişkin olarak veri sorumlularına başvurmak suretiyle kullanabilmeleri mümkün olacaktır. Bu sebeple Veri Sorumluları Sicili'ne kayıt olma zorunluluğu, ilgili kişilerin verilerinin kimler tarafından işlenebildiğini görmeleri açısından çok önemlidir. Bu durumların aksine Veri Sorumluları Sicili'ne kayıt olma zorunluluğu ile ilgili istisna getirildiğinde ve bunun sonucunda kişisel verilerin hukuka aykırı işlenmesi durumunda, ilgililerin kendilerine kanunla verilen haklarının yerine getirilmesi için muhatap aradıklarında bulamayacakları durumlar olabilecektir[343].

4.2.2. Aydınlatma Yükümlülüğü

Hukuk sistemimizde "aydınlatma yükümlülüğü" kavramı ile ilgili olarak genel bir hüküm ve buna bağlı olarak net bir tanımlamanın yapılmadığını ifade edebiliriz[344]. Bunun için KVKK bakımından aydınlatma yükümlülüğü kavramının tanımını yapabilmek için farklı hukuk dallarından yararlanmak gerekecektir.

Tıp hukukunda, tıbbi müdahalelerin hukuka uygunluğu açısından ön koşul olan hastanın tıbbi müdahaleye rıza göstermesi konusunda, hekimlerin ilgili hastayı aydınlatma yükümlülükleri bulunmaktadır. Bu sebeple aydınlatma yükümlülüğü kavramı ve söz konusu yükümlülüğün kapsamı tıp hukukunda uzun zamandır tartışılmaktadır[345]. Sağlık hukukunda aydınlatma yükümlülüğünün olması gerektiğini düşünenler için asıl amaç, ilgili kişinin vücut bütünlüğüne yönelik olan müdahalelerin hukuka uygun olmasını sağlamak için hastaya aydınlatma yükümlülüğünün yerine getirilerek rızasının alınması olarak ifade edilmektedir[346]. Burada dikkat edilmesi gereken, aydınlatma yükümlülüğünün asıl amacı hukuk kurallarına uygun bir rızanın alınması olduğudur. Dolayısıyla aydınlatma metninin içeriğinin de buna uygun olması gerekmektedir. Bunun için ilgili hastaya, uygulanması

[343] Mine, Kasapoğlu Turhan, Sağlık Hizmetlerinde İdarenin Kişisel Verileri Koruma Yükümlülüğü, IV. Sağlık Hukuku Kongresi, Ed.: İ. Hamit Hancı, Yener Ünver, Ankara, Seçkin, 2018, 118-159, s. 131.
[344] Özge, Erbek, Tüketici Satımlarında Satıcının Sözleşme Öncesi Aydınlatma Yükümlülüğü ve İhlalinin Sonuçları, Doktora Tezi, Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü, İzmir, 2010, s. 67.
[345] Hakan Hakeri, Tıp Hukuku, 16. Baskı, Ankara, Seçkin, 2019; Barış Erman, Ceza Hukukunda Tıbbi Müdahalelerin Hukuka Uygunluğu, Ankara, Seçkin, 2003; Sabah Altay, Tıbbi Müdahalenin Hukuka Uygunluğu Bakımından Hekimin Aydınlatma Yükümlülüğü ve Aydınlatılmış Rıza, IV. Sağlık Hukuku Kongresi, Ed.: İ. Hamit Hancı, Yener Ünver, Ankara, Seçkin, 2018, s. 407-419
[346] Hasan Seçkin Ozanoğlu, Hekimlerin Hastalarını Aydınlatma Yükümlülüğü, AÜHFD, C.52 S.3, 2003, s. 60.

planlanan tedavi metodu, alternatif metotlar, muhtemel riskler, faydaları ve diğer kararını vermesinin etkileyecek mühim meselelerde detaylı bilgi verilmesi gerekmektedir[347].

Bu anlamda Sağlık Bakanlığı tarafından hazırlanan "*Tıbbi Müdahalelerde Bilgilendirilmiş Rıza Alınması Yönetmeliği Taslağı"nda; "Bireyin; sağlık durumu, kendisine uygulanacak vücut bütünlüğüne müdahale gerektiren tanı ve tedavi yöntemleriyle, bunların da faydaları ve muhtemel riskleri, diğer tıbbi müdahale ve tedavi yöntemleri, tedavinin kabul edilmemesi halinde ortaya çıkabilecek muhtemel sonuçları ve hastalığın seyri, neticeleri ve öngörülemeyen acil durumlarda önerilen tedavinin dışına çıkma konularında ayrıntılı ve yazılı olarak bilgilendirilmesi*" biçiminde bir yönetmelik bulunmaktadır[348]. Aydınlatma yükümlülüğü, medeni hukuktaki tanımına baktığımızda "*sözleşmenin diğer tarafını, hukuki ilişki açısından önemli kabul edilen maddi ve hukuki hususlara işaret etmek"* biçiminde ifade edilmektedir[349].

Aydınlatma yükümlülüğü kavramının Kişisel Verileri Koruma Kanunu'na ilişkin düzenlemelerde tanımlanmadığını ifade etmiştik. Ancak aydınlatma yükümlülüğünü genel manada veri sorumlusunun, kendisinden talep edilmeden, ilgili kişinin kararını etkileyebilecek, fakat ilgili kişi tarafından bilinmesi mümkün olmayan durumlar ya da olgular hakkında bu kişiye bilgi verilmesi olarak ifade etmek yerinde olacaktır[350]. Sağlık hukuku veya medeni hukuk alanlarında yapılan tanımlamalara benzer biçimde KVKK hukukunda da aydınlatma yükümlülüğünde esas olan, ilgili kişilerin, kararlarını etkileyebilecek durumlar hakkında bilgilendirilmeleridir. Bu yaklaşımlar neticesinde kişisel verilerin korunması hususunda tesirli bir koruma sağlanabilmesi mümkün olacaktır[351]. Çünkü KVKK m. 3/1-a'da kişisel verilerin hukuk kurallarına uygun olarak işlenebilmesinin ön şartı ilgili kişilerin veri işlemeye, yapılan bilgilendirmeye dayalı olarak rıza göstermeleridir. KVKK bakımından ilgili kişileri aydınlatma yükümlülüğü, veri sorumluları

[347] Yusuf, Büyükay, İstenmeden Dünyaya Gelen Çocukların Bakım Eğitim ve Tedavi Giderlerinin Tazmin Edilmesi Sorunu, İstanbul, 2006, s. 62.
[348] Hakeri, a. g. e., s. 264.
[349] Hakeri, a. g. e., s. 264.
[350] Fahrettin, Aral, Türk Borçlar Hukukunda Kötü İfa, Ankara, Yetkin, 2011, s. 119-120.
[351] Nevzat Ali Anı, Kişisel Verilerin İşlenmesi ve Açık Rıza, Yüksek Lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2018, s. 134.

veya temsilcisi tarafından, verilerin hangi amaç için toplandığı, saklandığı ya da aktarıldığı hakkında ilgili kişiye lüzumlu bilgileri verme yükümlülüğü anlamına gelmektedir[352].

Bu tanımlamalar doğrultusunda kendisi hakkında verisinin işlendiğini öğrenen ilgili kişi, bu durum ile ilgili herhangi bir hak ihlali yapıldığını tespit etmesi durumunda mevzuatta düzenlenen hukuki koruma yollarına başvurabilecektir[353]. KVKK ile ilgili uluslararası belgelerde veri sorumlusunun aydınlatma yükümlülüğüne ilişkin hukuki düzenlemeler bulunmak birlikte ancak Türkiye'de olduğu gibi aydınlatma yükümlülüğü ile ilgili bir tanımlama yapılmamıştır. Örneğin, 108 sayılı Avrupa Konseyi Sözleşmesi m. 8'de, ilgili kişilerin hakları bakımından, kendileri hakkında otomatik yollar ile kişisel veri işlenip işlenmediği, kişisel veri işlenmesi söz konusu olduğunda bu faaliyeti gerçekleştiren yetkilinin kimliği, adresi gibi hususlarda bilgi alma haklarının bulunduğu ifade edilmektedir. Veri sorumlusunun aydınlatma yükümlülüğü ile ilgili Veri Koruma Tüzüğü'nde de aynı şekilde bahsedilmektedir. Veri koruma Tüzüğü m. 12'ye göre veri sorumlularının, veri işleme faaliyetine ilişkin olarak tüzükte bulunan her türlü bildirimi ilgili kişilere açık, öz, anlaşılır ve kolayca erişilebilir bir şekilde sade bir dil kullanarak yapması gerektiği ifade edilmektedir. Son olarak OECD Rehber İlkeleri'nde kişisel veri sahibinin, kendisi hakkındaki verilerin işlenme süreçlerine aktif olarak katılabileceği bu bakımdan veri sorumlusu veya temsilcisine başvurarak işlem süreçleri hakkında detaylı bilgi alma hakkının bulunduğu ifade edilerek veri sorumlusunun aydınlatma yükümlülüğüne işaret edildiğini söyleyebiliriz.

Kişisel Verilerin Korunması Kanunu m. 10'da aydınlatma yükümlülüğü düzenlenmektedir. KVKK m. 10 ve m. 11'de aydınlatma yükümlülüğünün bulundurması gereken asgari durumların düzenlendiğini ifade edebiliriz.

4.2.3. Aydınlatma Yükümlülüğünün Kapsamı

Kanun koyucu aydınlatma yükümlülüğünü, KVKK m. 10'da düzenlemiştir. Bu madde bakımından yapılan düzenlemeye göre veri sorumlusu ya da temsilcisi olan kişi, verilerin elde edilmesi esnasında ilgili kişilere, veri sorumlusunun ve varsa temsilcisinin kimlik

[352] Atak, a. g. e., s. 212.
[353] Şimşek, a. g. e., s. 13; Akgül, "a. g. e., s. 141; Öngün, a. g. e., s. 151.

bilgileri, kişisel veri toplamanın hukuki metodu ve nedeni, verilerin hangi maksatla işleneceği, işlenen verilerin kimlere, hangi maksatla aktarılabileceği ve verisi işlenen kişinin KVKK" m.11'de bahsedilen hakları hususlarında bilgi vermekle yükümlüdür. KVKK m. 11'de yapılan düzenlemeye göre; ilgili kişi, veri sorumlusuna başvurmak suretiyle, kendisine ait olan verilerin işlenmesine ilişkin olarak bilgi talep etme, verilerin işlenmesi söz konusu olmuş ise işlenen bu verilere ilişkin bilgi alma, verilerin işlenme maksadını ve bu maksada uygun olarak işlenip işlenmediğini öğrenme, yurt içi ve yurt dışına kişisel verilerin transferi söz konusuysa kimlere transfer edildiğini öğrenme, kişisel verilerin eksik veya yanlış işlenmiş olması durumunda bunların düzeltilmesini, kişisel verilerin hukuk kurallarına uygun olarak silinmesini ya da yok edilmesini, verilerin düzeltilmesi, silinmesi veya yok edilmesi hususundaki işlemlerin, verilerin aktarıldığı üçüncü kişilere bildirilmesini talep etme, işlenen verilerin otomatik yollarla analiz edilerek ilgilinin aleyhine bir sonuç ortaya çıkmasına itiraz etme, verilerin hukuka aykırı işlenmesinden doğan zararını talep etme haklarına sahip olduğunu ifade edebiliriz. KVKK'da yapılan düzenlemenin bir benzeri de Veri Koruma Tüzüğü'nde de yer bulmaktadır. Veri Koruma Tüzüğü m. 13'te yapılan düzenlemede kişisel verilerin veri sahibinden toplanması durumunda elde edilecek bilgilerin; m. 14'te de kişisel verilerin veri sahibinden toplanmadığı durumlarda elde edilecek bilgilerin düzenlendiği görülmektedir. Türk hukukunda düzenlenen KVKK'nın, Veri Koruma Tüzüğü'ne göre aydınlatma yükümlülüğü bakımından daha dar bir çerçevede hazırlandığını ifade edebiliriz. Bu anlamda örnek olması bakımından Veri Koruma Tüzüğü m.13'te, veri sorumlusunun ilgili kişilere, verilerin saklanacağı süre ile ilgili olarak, sürenin ilk başta tespit edilememesi durumunda sürenin tayin edilmesinde kullanılacak ölçütlerin, açık rıza verilmesi sonucu gerçekleştirilen işleme faaliyetlerinde ilgili kişinin rızasını geri alma hakkı, bir denetim makamına şikâyette bulunma hakkı ile ilgili konular da düzenlenmektedir. Aydınlatma yükümlülüğünde bulunması gereken asgari hususlar ile ilgili düzenlemeleri incelediğimizde, "KVKK" da ki düzenlemelerin "Veri Koruma Tüzüğü" ne göre daha yetersiz olduğunu görmekteyiz. "Veri Koruma Tüzüğü" m. 14'te kişisel verilerin, veri sahibinden elde edilmediği durumlarda yapılacak olan aydınlatmanın içeriğinin düzenlendiğini yukarıda bahsetmiştik. Bu durumda Veri Koruma Tüzüğü m. 13'te düzenlenen bilgiler dışında veri sorumlusu, kişisel verilerin hangi kaynaktan alındığına ilişkin ve uygun olduğu durumlarda verilerin kamu otoritesinin ulaşabileceği kaynaklardan gelip gelmediği hususlarında da ilgili kişilerin aydınlatılması gerekmektedir. Veri koruma

Tüzüğü m. 14/5-b'de ifade edilen düzenlemede de söz konusu bilgilerin ilgili kişilere imkânsız olması ya da ölçüsüz bir çaba gerektiriyorsa veya kişisel verilerin işlenmesi açıkça yasadan kaynaklanıyorsa bu hususlarda aydınlatma yükümlülüğünün yerine getirilmesi göz ardı edilebilecektir.

Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ'i[354] m. 6'da kişisel verilerin ilgili kişilerden elde edilmemesi durumunda, aydınlatma yükümlülüğünün yerine getirilmesine ilişkin düzenleme yer almaktadır. Ancak bu düzenlemede Veri Koruma Tüzüğü'nden farklı olarak, ilgili kişiye yapılacak olan aydınlatmanın içeriğine yer verilmemekte sadece aydınlatmanın yapılacağı zamana dikkat çekilmektedir. Saymış olduğumuz bu nedenlerden dolayı KVKK'nda yer alan düzenlemelerin Veri Koruma Tüzüğü'nde yer alan düzenlemeler ile uyumlaştırılması gerektiğini düşünmekteyiz. Nitekim Kişisel Verileri Koruma Kurumu'nun etkinliklerini takip ettiğimizde kurumun bu uyumlaştırmayı öncelikli hâle getirdiğini görmekteyiz.

4.2.4. Aydınlatma Yükümlülüğünde Amaç

Kişisel Verilerin Korunması Kanunu bakımından, ilgili kişilerin veri işleme faaliyetleri bakımından hukuk kurallarına uygun olarak bilgilendirilmeleri çok büyük öneme sahiptir[355]. Veri işleme faaliyetleri hakkında, veri sorumlusu toplanan kişisel verilerin hangi amaçla toplandığı ya da saklandığı hususunda ilgili kişileri bilgilendirmek zorundadır[356]. Bu durumda ilgili kişiler, herhangi bir baskı ve zorunluluk hissetmeden özgür iradeleriyle verilerinin işlenmesine karar verebilirler. Bu sebeple aydınlatma yükümlülüğü bakımından ilk amacın ilgili kişilerin verilerinin işlenmesine sağlıklı bir rıza göstermelerini sağlamak olduğu ifade edilebilir.

İlgili kişilerin verilerini işlemeye sıhhatli bir rıza göstermelerini sağlamak aydınlatma yükümlülüğü kapsamında değerlendirilmektedir. Aydınlatma Yükümlülüğü Tebliğ'inde, "*İlgili kişinin açık rızasına veya Kanundaki diğer işleme şartlarına bağlı olarak kişisel veri işlendiği her durumda aydınlatma yükümlülüğü yerine getirilmelidir*." biçiminde ilgili

[354] Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ, 10/03/2018 tarihli 30356 sayılı Resmî Gazete.
[355] Küzeci, a. g. e., s. 218;
[356] Öngün, a. g. e., s. 49.

mevzuatta düzenleme bulunmaktadır (m. 5/1-a). Bu düzenlemeden anlaşılacağı üzere aydınlatma yükümlülüğünün, sadece kişisel verilerin hukuk kurallarına uygun bir biçimde işlenebilmesi için ilgili kişinin açık rızasının alındığı vaziyette değil, ilgili kişinin açık rızası aranmadan da kişisel verilerin işlenebileceği diğer durumlarda da yerine getirilmek zorunda olduğunu ifade edebiliriz. Bahse konu Aydınlatma Tebliği'nde bu şekilde bir düzenlemenin bulunması elbette anlaşılırdır. Çünkü aydınlatma yükümlülüğü ile hedeflenen bir diğer konu, ilgili kişinin veri işleme süreçleri hakkında haberdar edilmesi ve kendisine hukuki olarak tanınan haklarını esas anlamda kullanabilmesinin sağlanmasını ifade etmektedir[357].

"Bilgilerin Geleceğini Belirleme Hakkı" başlığı içerisinde, aydınlatma yükümlülüğünün esas amacı olduğunu düşündüğümüz, ilgilinin kişisel verilerinin işlenmesi sürecinde aktif rol almasının sağlanması konusuna değinilecektir.

Aydınlatma yükümlülüğü bakımından bir diğer amaç, ilgilinin bilgilerinin geleceğini tayin etme hakkı kapsamında değerlendirilebilecek olan *"İlgilinin Açık Rızası"* konusunda aşağıdaki konu başlıklarımızda daha detaylı olarak açıklanacaktır.

4.2.4.1. İlgili kişinin rızası

4.2.4.1.1. Tanımı ve unsurları

Kişisel verilerin hukuk kurallarına uygun olarak işlenebilmesi için ilgili kişinin, verilerinin işlenmesi için açık rıza vermesi zorunluluğu bulunmaktadır[358].

Yapılacak olan bir işleme dair hukuki açıdan irade açıklaması[359] anlamına gelmekte olan rıza kavramı *"belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza"* biçiminde ifade edilmektedir (m. 3/1-a).

Konu ile ilgili yapılan diğer bir tanımlamaya baktığımızda, "*Rıza, rıza gösterme ehliyet ve yetkisine sahip olan kişinin; üzerindeki tasarruf yetkisi hukuk düzeni tarafından kendisine*

[357] Öngün, s. 217.
[358] Taştan, a. g. e., s. 57.
[359] Kılıçoğlu, a. g. e., s. 127.

*bırakılmış bir hukuksal değerine karşı gerçekleştirilen ve söz konusu hukuksal değeri tehlikeye düşüren veya zarara uğratan bir fiili kabul etmesi, onaylaması"*dır[360].

İlgili kişinin vermiş olduğu rıza, Veri Koruma Tüzüğü'nde bildirim yoluyla veya açık bir onay fiiliyle kendisine ait verilerin işlenmesine izin verdiğini gösteren özgür ve şeffaf bir şekilde verilmiş, spesifik, bilinçli ve açık gösterge olarak ifade edilmektedir (m. 4/11).

4.2.4.1.2. Rıza beyanının niteliği

Kişisel verilerin işlenmesine ilişkin verilen açık rızanın hukuk kuralları kapsamında değerlendirilebilmesi için çeşitli özelliklerin bir arada bulunması gerekmektedir[361]. Bunlardan bahsedecek olursak; verilen rızanın belirli bir konu ile ilgili olması, özgür iradeyle verilmesi, bilgilendirmeye dayanıyor olması, beyan yoluyla veya açık bir onay fiiliyle kişisel verilerin işlenmesine onay verildiğine ilişkin talebin açık bir göstergesi olması gerekmektedir[362].

Kişisel veri sahibinin vermiş olduğu açık rızanın hukuk kurallarına uygun ve belirli bir konuya has olması gerekmektedir. Veri sahibi tarafından verilen rızanın hukuk kurallarına uygun kabul etmemiz için belirli olan bir ya da daha fazla amaca özgülenmesi aslında ilgili kişinin, veri işleme faaliyetini denetleyebilmesini ve veri işlemenin şeffaflığı ilkesini güvence altına almaya yönelik olduğunu ifade edebiliriz[363].

Veri işlemi faaliyetinin hukuk kurallarına uygun olabilmesi için Veri Koruma Tüzüğü m.6'da yer alan düzenlemede "*veri sahibinin bir ya da daha fazla sayıda spesifik amaca yönelik olarak kişisel verilerinin işlenmesine onay vermesi"* gerektiği ifade edilmiştir. Veri Koruma Tüzüğü'ne paralel olarak 95/46/EC sayılı Yönerge'de de açık rızanın sadece söz konusu veri işleme faaliyeti kapsamında sınırlı olarak verilmesi gerektiği ifade

---

[360] Meral Ekici Şahin, Ceza Hukukunda Rıza, İstanbul, On İki Levha, 2012, s.7; Kayıhan İçel, Ceza Hukuku Genel Hükümler, Yenilenmiş Baskı, İstanbul, Beta, 2016, s.382; Hakeri, a. g. e., s. 355; M. Emin, Artuk, Ahmet, Gökcen, M. Emin, Alşahin, Kerim, Çakır, Ceza Hukuku Genel Hükümler, 13. Baskı, Ankara, Adalet, 2019, s. 549.

[361] Küzeci, a. g. e., s. 232;

[362] (Çevrimiçi), https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf , Guidelines on Consent under Regulation 2016/679, a. g. e., s. 5, (Erişim Tarihi: 02/03/2022),

[363] (Çevrimiçi), https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf , Guidelines on Consent under Regulation 2016/679, a. g. e., s. 11, (Erişim Tarihi: 02/03/2022),

edilmektedir[364]. Türk hukukunda düzenlenen KVKK'da açık rızanın belirli bir konu ile ilgili olması gerektiği şeklinde düzenleme yapılmıştır. Kişisel veri sahibi tarafından verilen rızaya örnek olması bakımından *"kişisel verilerimin işlenmesini kabul ediyorum"* biçiminde genel veya belirli bir konuya özgü olmayan beyanın tek başına açık rıza olarak kabul edilmesi mümkün değildir[365]. İlgili kişinin birden çok farklı verisinin işlenmesi söz konusu olması durumunda her bir yapılacak işlem bakımından ayrı ayrı rıza beyanında bulunması gerekmektedir[366]. Her bir farklı veri için ilgili kişiden rıza alınması veri işleme amacı bakımından, rızanın belirli bir konuya özgü olması ve özgürce verilmiş olması bakımından oldukça önemlidir[367].

Kişisel verisi işlenen ilgili kişinin verinin işlenme amacının değişmesi durumunda ilgili veri sahibinden yeniden açık rızasının alınması gerekmektedir[368].

İlgilinin açık rızasının hukuk kurallarına uygun kabul edilebilmesinin bir diğer koşulu, ilgili rızanın, serbest ve özgür bir zihni etkinliğin ürünü olması dolayısıyla ilgili kişinin kendi özgür iradesinin bir yansıması olmasını ifade etmektedir[369]. İlgili kişi verilerinin işlenmesine ilişkin olarak dışarıdan hiçbir baskı olmadan rıza vermesi gerekmektedir[370].

Serbest ve özgür bir rıza ilgili kişinin gerçekten seçim yapabildiği, rıza vermediği durumda herhangi bir olumsuzlukla karşılaşmayacağı konusunda emin olduğu durumlarda söz konusu olacaktır[371]. Verisi işlenen kişiye karşı cebir, tehdit, hata, hile gibi iradeyi sakatlayan bir durum söz konusu olduğunda kişi özgür iradesiyle rıza göstermiş olsa bile rızanın geçerliliğinden bahsedilemeyecektir[372]. Söz konusu kişinin yanıltılması veya kendi yaptığı hata nedeniyle yanıldığı durumlarda da kişinin esas iradesi ile açıkladığı iradesi arasında

[364] Kişisel Verilerin Korunması Kanunu"na İlişkin Uygulama Rehberi, s. 47.
[365] 100 Soruda Kişisel Verilerin Korunması Kanunu, s. 26.
[366] Kişisel Verilerin Korunması Kanunu"na İlişkin Uygulama Rehberi, s. 48.
[367] (Çevrimiçi), https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf , Guidelines on Consent under Regulation 2016/679, a. g. e., s. 12, (Erişim Tarihi: 02/03/2022).

[368] Kişisel Verilerin Korunması Kanunu"na İlişkin Uygulama Rehberi, s. 48.
[369] Küzeci, a. g. e., s. 233; Kılıçoğlu, a. g. e., s. 41.
[370] Küzeci, a. g. e., s. 233; 238; Atak, a. g. e., s. 135.
[371] Opinion 15/2011 on the Definition of Consent, s. 12.
[372] 100 Soruda Kişisel Verilerin Korunması Kanunu, s. 27; Şahin, a. g. e., s. 185.

uyumsuz olacağından verilen rızanın hukuken geçerliliği kabul edilmesi mümkün olamayacaktır[373].

İlgili tarafların eşit pozisyonlarda olmadığı durumlarda verilen rızaların özgür ve serbest iradeyle verilip verilmediği hususunda ayrıca değerlendirme yapılmalıdır[374]. Bu konuda özellikle zayıf tarafta olan işçi ve güçlü tarafta olan işveren ilişkilerinde, işçinin kişisel verilerinin işlenmesine rıza göstermediği durumda herhangi bir olumsuzlukla karşılaşması olası ise bu bakımdan özgür iradeyle verilmiş bir rızadan bahsetmek mümkün olmayacaktır[375]. Aynı durum doktor-hasta ilişkisinde de söz konusu olmaktadır. Burada hastanın vermiş olduğu rızayı özgür bir iradeyle verip vermediği konusunda tartışmalar bulunmaktadır[376]. Tartışmalı olan bu konularda ilgili kişilere alternatif güvenceler sağlanıp bu kişilerin özgür ve serbest iradeleriyle karar vermeleri sağlanmalıdır[377].

Kamu idarelerinin kişisel verileri işlediği hususlarda da rıza beyanının özgür iradeyle verilip verilmediğine özen gösterilmelidir. Örneğin üniversiteye kayıt yaptıran bir öğrencinin sisteme işlenen verileri ile ilgili olarak öğrencinin özgür ve serbest iradeyle rızasının alınması önemlidir. Verilerin hukuk kurallarına uygun işlenebilmesi için alternatif hukuki yollar mevcutsa öncelikle bunların kullanılması gerekmektedir[378]. İlgili kişinin açık rızasının alınması bir ön koşul anlamında dayatılmamalıdır. Bu durumda zaten özgür iradeyle bir rızadan bahsetmek mümkün olmayacaktır[379]. İlgili kişinin rızasının özgür iradeyle verilip verilmediği konusunda Veri Koruma Tüzüğü m. 7/4'te "*Rızanın özgür bir şekilde verilip verilmediği değerlendirilirken, her şeyden önce, bir hizmetin sağlanması da dahil olmak üzere bir sözleşmenin ifasının söz konusu sözleşmenin ifası için gerekmeyen kişisel verilerin işlenmesine yönelik bir rızaya bağlı olup olmadığına azami özen gösterilir*." Dile getirildiği üzere rıza göstermenin bir şarta bağlı olup olmadığı konusunda dikkat edilmesi gerektiği ifade edilmektedir. Kişisel Verileri Koruma Kurulu tarafından yayımlanan bir kararda, spor

[373] Şahin, a. g. e., s. 186, Eren, a. g. e., s. 377 vd, Haluk Nami Nomer, Borçlar Hukuku Genel Hükümler, 15. Baskı, İstanbul, Beta, 2017, s. 90 vd.
[374] Küzeci, a. g. e., s. 232; Kişisel Verilerin Korunması Kanunu"na İlişkin Uygulama Rehberi, s. 49.
[375] Kişisel Verilerin Korunması Kanunu"na İlişkin Uygulama Rehberi, s. 49.
[376] Küzeci, a. g. e., s. 234;
[377] Küzeci, a. g. e., s. 234.
[378] Çevrimiçi), https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf , Guidelines on Consent under Regulation 2016/679, a. g. e., s. 12, (Erişim Tarihi: 02/03/2022).
[379] Kişisel Verilerin Korunması Kanunu"na İlişkin Uygulama Rehberi, s. 50.

salonu üyelik sözleşmesi hususunda, avuç izinin alınmasına ilişkin onay verilmediği durumda spor salonu yetkilileri tarafından sözleşmenin kurulması için zorunlu unsur olarak öngörülmesi ve onay alınmadığı durumda da sözleşmenin feshedileceğine ilişkin hususlar birlikte değerlendirildiğinde ilgili kişi tarafından verilen rızanın geçerli bir rıza olmadığı ifade edilmektedir[380].

Burada önemle belirtmek gerekir ki geçerli bir rıza beyanının olabilmesi için, hiçbir şüpheye yer olmayacak derecede açık ve şeffaf olması gerekmektedir[381]. İlgili kişi tarafından verilen rıza beyanının içeriğinde kullanılan söz, yazı veya resim gibi araçların herhangi bir yoruma ve karışıklığa yer vermeyecek şekilde anlaşılması gerekmektedir[382]. İlgili kişi tarafından verilen rızanın ne şekilde verildiğinin hiçbir önemi bulunmamakla birlikte yazılı alınmasının ispat bakımından daha yararlı olacağını ifade edebiliriz[383]. Tüm bu ifade ettiklerimizin yanında şüpheye hiçbir biçimde yer bırakmayacak şekilde gerçekleştiren rıza örtülü de olsa hukuken geçerli olacaktır[384]. İlgili kişinin rıza beyanının alınması konusunda şekil bakımından herhangi bir sınırlama olmamakla birlikte, yazılı rızanın alınma durumunda ispat bakımından daha sağlıklı olacaktır[385]. İlgili kişinin göstereceği rıza bilgilendirmeye dayalı olmak zorundadır. Dolayısıyla kişisel verilerinin işlenmesine özgür iradesiyle rızasının söz konusu olabilmesi için neye rıza gösterdiğini açık ve net olarak bilmesi gerekir[386]. Kişinin vermiş olduğu rızanın hangi konuları kapsadığı bunun yanında verilen rızanın sonuçları hakkında bilgi sahibi olması gerekmektedir[387]. İlgili kişinin verilerini işleyen kişi tarafından aydınlatma yükümlülüğü rıza verilmeden önce yerine getirilmelidir[388].

[380] Kişisel Verileri Koruma Kurulu'nun 25/03/2019 tarihli ve 2019/81 sayılı Karar ve 31/05/2019 Tarihli ve 2019/165 sayılı Karar Özeti, (Çevrimiçi), https://kvkk.gov.tr/Icerik/5496/2019-81-165, (Erişim Tarihi: 02/03/2022).
[381] Küzeci, a. g. e., s. 232.
[382] Haluk Nami Nomer, Borçlar Hukuku Genel Hükümler, 15. Baskı, İstanbul, Beta, 2017, s. 42.
[383] Öngün, a. g. e., s. 137.
[384] Küzeci, a. g. e., s. 233; Nomer, a. g. e., s. 42.
[385] Öngün, a. g. e., s. 137.
[386] Kişisel Verilerin Korunması Kanunu"na İlişkin Uygulama Rehberi, s. 49; Şahin, a. g. e., s. 189.
[387] Kişisel Verilerin Korunması Kanunu"na İlişkin Uygulama Rehberi, s. 49.
[388] Meral Ekici Şahin, Ceza Hukukunda Rıza, İstanbul, On İki Levha, 2012, s. 190;

4.2.4.1.3. Rıza göstermede ehliyet kavramı

Kişisel Verilerin Korunması Kanunu'nda, kişisel verilerin işlenmesine rıza gösterme ehliyetine, verileri işlenen sadece gerçek kişiler sahiplerdir[389]. Bu durumda rıza gösterme, sadece rıza ehliyetine sahip kişiler tarafından verilebilecektir. Bahse konu ilgili kişilerin tam ehliyetli olmaları, rıza verebilmeleri açısından yeterli olacaktır[390].

Kişisel Verilerin Korunması Kanunu'nda, çocukların veri işlemeye rıza göstermeleri açısından hususi düzenlemeler bulunmaktadır. Çünkü çocuklar, çoğunlukla kişisel verilerinin işlenmesi neticesinde doğabilecek risklerin farkında olamayabilirler[391]. Bu sebeple verilerin güvenliği açısından, özel olarak daha hassas korunmaları gerekmektedir.

Veri Koruma Tüzüğü m. 8'e göre; "*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*." Dolayısıyla on altı yaşından büyük çocukların rızasına istinaden kişisel verilerinin işlenmesi hukuk kurallarına uygun olacaktır. Fakat on altı yaşından küçük çocuklar için verilerin hukuk kurallarına uygun olarak işlenebilmesi için çocuk üstünde velayet hakkı olan kişinin rıza vermesi ya da verilerinin işlenmesine onay vermesi gerekir. Bu durumda veri işleme faaliyeti sadece mevzuatta düzenlenen rıza veya onayın sınırları içerisinde hukuk kurallarına uygun olacaktır. Üye bulunan ülkelerin, on üç yaşından küçük olmamak şartıyla, ilgili maddede düzenlenen yaştan daha küçük bir yaşı yasal düzenlemeyle belirleyebilecekleri düzenlenmektedir.

Türk hukukuna baktığımızda KVKK açısından çocukların rıza ehliyeti ile ilgili özel bir düzenleme bulunmamaktadır. KVKK içerisinde düzenlenen haklar kişiye bağlı bulunan haklardandır. "*Ayırt etme gücüne sahip küçükler ve kısıtlılar, yasal temsilcilerinin rızası olmadıkça, kendi işlemleriyle borç altına giremezler. Karşılıksız kazanmada ve kişiye sıkı*

[389] Küzeci, a. g. e., s. 237.
[390] Nevzat Ali Anı, Kişisel Verilerin İşlenmesi ve Açık Rıza, Yüksek Lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2018, s. 61.
[391] Çevrimiçi), https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf , Guidelines on Consent under Regulation 2016/679, a. g. e., s. 23, (Erişim Tarihi: 02/03/2022).

sıkıya bağlı hakları kullanmada bu rıza gerekli değildir. Ayırt etme gücüne sahip küçükler ve kısıtlılar haksız fiillerinden sorumludurlar" (TMK, m. 16). Bu yasal düzenlemeden dolayı doğrudan çocuğa bağlıdır[392]. Tüm bu düzenlemeler dışında çocukların hususi olarak korunması ve üstün yararlarının gözetilmesi gereksiniminden dolayı çocukların kişisel verilerinin hukuk kurallarına uygun olarak işlenebilmesi için kendileri üzerinde vesayet hakkı sahibi bulunanların rıza ya da onay vermeleri gerekir[393].

KVKK çocuk olan kişiye bağlı bir hak olmasından dolayı çocuğun tek başına karar verebileceği durumlarda, çocuğun rızasına başvurulması gerekmektedir. Ancak çocuk olan kişinin verilerinin hukuk ve dürüstlük kurallarına uygun işlenebilmesi ve çocuğun üstün yararının gerektirdiği ve bu sebeple çocuğun kendi başına karar vermesinin beklenemeyeceği durumlarda vesayet hakkı sahibinin onayı ya da rızası aranmaktadır[394].

İlgili çocuğun yaşının rıza göstermeye yeterli olduğu durumlarda veri sorumluları aydınlatma yükümlülüklerini çocuğa karşı yerine getirmek zorundadırlar. Ancak burada dikkate edilmesi gereken veri sorumlularının yapmış olduğu aydınlatmanın çocuk bakımından anlaşılır olup olmadığına dikkat edilmelidir[395]. Yaşı küçük olan çocuğa ilişkin olarak kişisel verilerin işlenmesine vesayet hakkı sahibinin rıza gösterdiği veya onaylandığı durumlarda aydınlatma yükümlülüğü, vesayet hakkı sahibine karşı yerine getirilmelidir[396].

[392] Küzeci, a. g. e., s. 238.
[393] International Working Group on Data Protection in Telecommunications, Working Paper: Childrens' Privacy On Line: The Role of Parental Consent, Adopted at 31st Meeting, Auckland (New Zealand), 26/27 March 2002, s. 1.
[394] Working Paper: Childrens' Privacy On Line: The Role of Parental Consent, s. 1.
[395] Guidelines on Consent under Regulation 2016/679, s. 24.
[396] A. g. e., s. 24.

5. DÖRDÜNCÜ BÖLÜM

AYDINLATMA YÜKÜMLÜLÜĞÜ KAPSAMINDA KABAHAT VE YAPTIRIMLARI

5.1. AYDINLATMA YÜKÜMLÜLÜĞÜ KAPSAMINDA KORUNACAK OLAN HUKUKİ DEĞERLER

Veri sorumluları ve yetkilendirdikleri kişiler hakkında, kişisel verilerin toplanması esnasında aydınlatma yükümlülüğü ile ilgili düzenlemeler Kişisel Verilerin Korunması Kanunu m. 10'da düzenlenmiştir. Yapılan bu düzenleme gereğince sorumluluk yerine getirilmediğinde veri sorumlusu ve yetkilendirdiği kişi veya kişilere Kişisel Verilerin Korunması Kanunu m. 18 uyarınca "5.000 Türk Lirası ile 100.000 Türk Lirası arasında idari para cezası uygulanacağı" ifade edilmektedir.

Korunan hukuki değer bağlamında söz konusu kabahat ile hedeflenen, bireylerin kişisel verilerini modern hukuk düzeninde hukuk kaidelerine uygun olarak işlenmesini ve söz konusu haklarını etkili bir biçimde kullanabilmelerini temin etmek olarak ifade edilebilir. Dolayısıyla kabahat kavramı ile bireylerin kişisel verilerin korunması hakkının güvence altını alındığını net olarak ifade edebiliriz.

5.2. KABAHAT EYMENİN MADDİ UNSURLARI

Kabahatler Kanunu düzenlemesinde kabahat, "*kanunun, karşılığında idari yaptırım uygulanmasını öngördüğü haksızlık"* olarak tanımlandığını görmekteyiz (KK m. 2). Yapılan bu düzenlemede kabahatin bir haksızlık teşkil ettiği kabul edilmiştir. Fakat kabahat işleyen faile idari yaptırım uygulanabilmesi için sadece haksızlığın gerçekleşmesi yeterli olmayıp başka koşullar aranmaktadır. Dolayısıyla, failin kusurlu olması ve kanuni düzenlemede başka şartlar aramışsa, bu şartların da sağlanmış olması gerekmektedir.

Kabahatler bakımından bir fiile idari yaptırımın uygulanabilmesi için fiilin tipe uygunluğunun ve hukuka aykırılığının belirlenmesinden sonra, failinin kusurlu olmasının da belirlenmesi gerekmektedir. Dolayısıyla bir harekete idari yaptırım uygulanabilmesi için bazı özel şartların da yerine getirilmesi aranabilir. Bir harekete idari yaptırım

uygulanabilmesi için hukuka aykırılık, tipe uygunluk ve failin kusuru biçiminde üç ortak şartın bulunması gerekmektedir. Böylece kusur, kabahatin yapısal bir unsuru olarak kabul edilmemektedir. Çünkü kusur haksızlık teşkil ettiği fiili işlemesi dolayısıyla kişi hakkında bir kınama yargısı olduğu için, bir fiil, failinin kusuru olmadan işlense dahi, haksızlık ve dolayısıyla kabahat niteliğini korumaktadır. Böylece işlediği fiil dolayısıyla failin kusurlu sayılıp sayılmaması, bu fiilin kabahat niteliğine sahip bir haksızlık olması üzerinde etki doğurmamaktadır[397].

5.2.1. Kabahatin Konusu

Kabahat eylemine muhatap olan kişi veya eşya, kabahat kavramının konusunu oluşturur[398]. Kabahat kavramının konusunu kişinin şerefi, müşterinin sırrı gibi maddi olmayan değerler de kabahat kavramının konusu olabilir[399]. Dolayısıyla kabahatin konusunun her durumda fiziki varlığa sahip olması gerekli değildir[400]. Kişisel Verilerin Korunması Kanunu'nda kişisel verinin tanımı "K*imliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi*" biçiminde düzenlemiştir.

Kabahatin konusu, Kişisel Verilerin Korunması Kanunu m. 10'da düzenlenen ve kişisel verileri elde edilen veya elde edilmek istenilen ilgili kişilere verilmeyen bilgilerdir. Aydınlatma yükümlülüğünün yerine getirilmemesi kabahatin konusunu oluşturmaktadır. Konu bakımından aydınlatma yükümlülüğünün yerine getirilmemesi kabahati, soyut tehlike kabahati olarak ifade edilir[401]. Soyut tehlike kabahatlerinde, ilgili eylemin gerçekleşmesi durumunda idari yaptırımda bulunulması yeterli olacaktır[402].

Somut tehlikede soyut tehlikeden farklı olarak kabahat konusu bakımından gerçekten bir tehlike yaratılıp yaratılmadığı araştırılıp ona göre değerlendirmede bulunulur[ii]. Kişisel

[397] Zeynel, Kangal, Kabahatler Hukuku, İstanbul, onikilevha, 2019, s. 133.
[398] Artuk, Gökcen, Alşahin, Çakır, a. g. e., s. 377; Berrin Akbulut, Türk Ceza Kanunu ile Kabahatler Kanununun Genel Hükümlerinin Yaptırım Hükümleri Dışında Karşılaştırmalı Olarak İncelenmesi, 2. Baskı, Ankara, Adalet, 2014, s. 395-397; Soyaslan, a. g. e., s.15; Kayıhan, İçel, Füsun, Sokullu Akıncı, İzzet Özgenç, Adem Sözüer, Fatih S. Mahmutoğlu, Yener Ünver, Suç Teorisi: 2. Kitap, 3. Baskı, İstanbul, Beta, 2004, s. 88; Hakeri, a. g. e., s. 143;
[399] Artuk, Gökcen, Alşahin, Çakır, a. g. e., s. 413.
[400] Akbulut, a. g. e., s. 397;
[401] Artuk, Gökcen, Alşahin, Çakır, a. g. e., s. 397;
[402] Zeynel, Kangal, Kabahatler Hukuku, İstanbul, onikilevha, 2019, s. 105.

Verilerin Korunması Kanunu'nda ifade edilen aydınlatma yükümlülüğünün ifa edilmemesi kabahatinde eylemin gerçekleştirilmesiyle, söz konusu kişinin verilerinin ihlal edilip edilmemesinin bir önemi yoktur. Veri sorumlusu tarafından ilgili kişinin aydınlatılmaması durumunda kabahat fiilinin oluşması bakımından yeterli olacaktır.

5.2.2. Fiil Unsuru

KVKK m. 18/1-a'da yapılan düzenlemede "*Bu Kanun'un 10 uncu maddesinde öngörülen aydınlatma yükümlülüğünü yerine getirmeyenler hakkında 5.000 Türk lirasından 100.000 Türk lirasına kadar*" idari para cezaları uygulanacaktır. Bahse konu bu idari para cezaları sadece özel hukuk tüzel kişileri ve gerçek kişiler hakkında uygulanacaktır.

Aydınlatma yükümlülüğünün düzenlendiği Kişisel Verilerin Korunması Kanunu m. 10'a göre, veri sorumlusu, ilgili kişinin verilerinin elde edilmesi esnasında söz konusu kişiye, Kişisel Verilerin Korunması Kanunu m. 10 ve m. 11'de düzenlenen başlıklara ilişkin bilgi vermek zorundadır. Bu düzenlemeye göre veri sorumlusu ve yetkilendirdiği kişinin açık kimlik bilgisi, kişisel verilerin hangi yöntemle toplanacağı, kişisel verilerin hangi maksatla işleneceği, hukuki maksadı, hangi nedenlerle aktarılabileceği ve bunların yanında Kişisel Verilerin Korunması Kanunu m. 11'de belirtilen kişinin hakları konusunda ilgili kişiye bilgilendirme yapılmalıdır. Kişisel Verilerin Korunması Kanunu m. 11'de söz konusu kişinin kendi kişisel verileri ile ilgili olarak veri sorumlusu ya da yetkilendirdiği kişiye başvurarak haklarını kullanabileceği, veri işleme faaliyeti ile ilgili düzenlemelerden bahsedilmektedir. Bu bağlamda söz konusu kişi, kendine ait olan kişisel verinin işlenip işlenmediğini, işlendi ise bilgi talep etme, kişisel verilerin işlenme amacını öğrenme ve bu amaç doğrultusunda işlenme faaliyetinin gerçekleşip gerçekleşmediğini öğrenme, kişisel verilerin aktarılıp aktarılmadığını ve aktarılan kişileri öğrenme, kişisel verilerin noksan veya hatalı işlenmesi durumunda tashih talep etme, işlenen verilerin silinmesini talep edebilme, kişisel verilerin mevzuata aykırı bir biçimde işlenmesi nedeniyle zarara uğraması söz konusu olduğunda bu zararın giderilmesini isteme hakkına sahip olduğunu söyleyebiliriz.

Kabahatler, kural olarak icrai ya da ihmali hareketle işlenebilir[403]. İcrai bir eylem sonucu kabahatin işlenmesi durumunda, failin dış dünyada değişiklik meydana getiren bir eylemle, kabahat olarak ifade edilen bir ihlale sebep olması gerekmektedir. İcrai hareket ile anlatılmak istenen, mevzuatta düzenlenen kabahatin aktif bir hareket ile gerçekleştirilmesidir[404]. İhmali hareket ile işlenen kabahatlerde eylem normatif olarak belirlenir[405]. Dolayısıyla kişinin kendisinden beklenen iradi davranışı sergilememesi beklenmektedir[406]. İhmali hareketler ile işlenen kabahatlerde, harekete geçmeme, yapmama durumları söz konusu olmaktadır[407]. Bunun yanında icrai hareket ile işlenen kabahatler de fiil, doğal olarak belirlenmektedir[408].

Kabahatin ihmali davranış sonucu işlendiğinin kabul edilmesi için, kişi açısından icrai bir davranışının hukuken bulunması gerekmektedir[409] (KK m. 7).

Kişisel verileri işlenen bireylerin verilerine ilişkin aydınlatma yükümlülüğünün yerine getirilmemesi kabahati, gerçek ihmali kabahat kavramına karşılık gelmektedir. Çünkü hukuki düzenlemede tanımlandığı üzere, kabahatin çekimser kalınarak yerine getirilmesi gereken yükümlülüğün yerine getirilmemesi durumunda gerçek ihmali kabahat söz konusu olacaktır[410]. Dolayısıyla veri sorumlusu tarafından, verisi işlenen kişiye karşı aydınlatma yükümlülüğü yerine getirilmediğinde yasal olarak yükümlü bulunduğu icrai tutumu sergilenmemesi nedeniyle gerçek ihmali hareketle kabahat fiili işlenmesi söz konusu olacaktır.

[403] Elif Bekar, Kabahatler Kanunu'nun Genel Hükümlerinin Değerlendirilmesi, İÜHFM, C. LXIX, S. l-2, 1033-1050, 2011, s. 1041.
[404] İçel, Akıncı, Özgenç, Sözüer, Mahmutoğlu, Ünver, a. g. e., s. 164; Artuk, Gökcen, Alşahin, Çakır, a. g. e., s. 379; Hakeri, a. g. e., s. 320.
[405] İçel, Akıncı, Özgenç, Sözüer, Mahmutoğlu, Ünver, a. g. e., s. 164; Artuk, Gökcen, Alşahin, Çakır, a. g. e., s. 60.
[406] Hakeri, a. g. e., s. 165.
[407] Rahime, Erbaş, Türk Ceza Kanunu'nda Görünüşte İhmali Suçlarda Garantörlük, Doktora Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2019, s. 8.
[408] Özgenç, a. g. e., s. 173.
[409] Bekar, a. g. m., s. 1041.
[410] Akbulut, a. g. e., s. 274; Hakeri, Ceza Hukuku Genel Hükümler, s. 170; İçel, a. g. e., s. 269; Erbaş, a. g. e., s. 70.

Kişisel Verilerin Korunması Kanunu'nda düzenlendiği üzere aydınlatma yükümlülüğü, konunun bütünlüğü açısından çok önemli yer teşkil etmektedir. Kişilerin verileri üzerinden tasarruf haklarını tam manasıyla kullanabilmeleri için ve sağlıklı bir rıza göstermeleri bakımından aydınlatılmış olmaları oldukça önemlidir. Zira, kanun kapsamında aydınlatma yükümlülüğünün yerine getirilmesinde kullanılan yöntem ve aydınlatmanın muhteviyatı önemlidir. Bu bağlamda ilgili başlığımızın devamında hangi durumlarda kabahatin oluşup oluşmayacağı incelenecektir.

5.2.2.1. Kişiye karşı aydınlatma yükümlülüğünün yerine getirme zamanı

Kişisel Verilerin Korunması Kanunu'nda yapılan düzenleme gereği verilerin elde edilmesi ile birlikte aydınlatma yükümlülüğü gerçekleştirilmiş olmalıdır (KVKK m. 10). Bu noktada kişisel veriler ile ilgili olarak önemli olan sürecin başındayken bireyin aydınlatılmış olması gerekmektedir[411].

Aydınlatma yükümlülüğü ile ilgili düzenlemelere baktığımızda gerek 95/46/AT sayılı Yönerge (m. 10 ve m. 11) gerekse de Veri Koruma Tüzüğü'nde, verilerin ilgili kişilerden veya bir başka biçimde elde edilme durumlarına göre, veri sorumlusunun aydınlatma sorumluluğu düzenlenmektedir[412]. Veri Koruma Tüzüğü'ne göre veriler, ilgili kişiden toplandığı esnada aydınlatma yükümlülüğü sağlanmış olmalıdır (m. 13/1). Kişisel veriler, ilgili kişiden elde edilebileceği gibi farklı kaynaktan da elde edilmesi mümkün olabilir. Bu tür durumlarda aydınlatma yükümlülüğünün ne zaman yerine getirileceği bahse konu düzenlemeler açısından oldukça önemlidir. İlgili düzenlemelerden biri olan Veri Koruma Tüzüğü'ne göre, ilgili kişiden doğrudan alınan kişisel verilerin üçüncü kişilerle paylaşılması söz konusu olan durumlarda veya ilgili kişiden alınmayıp başka kaynaklardan elde edilmesi durumlarında kişinin aydınlatılması gerekmektedir[413]. Kişisel verileri, Veri Koruma Tüzüğü'ne göre kişinin kendisinden elde edilmeyen veriler ile ilgili makul süre içerisinde bilgilendirmenin yerine getirilmiş olması gerekmektedir. Ancak bu aydınlatma yükümlülüğünün en geç bir ay içerisinde sağlanmış olması gerekir.

---

[411] Guidelines on Transparency under Regulation 2016/679, s. 14-15.

[412] Hüseyin Murat, Develioğlu, 6698 sayılı Kişisel Verilerin Korunması Kanunun ile Karşılaştırmalı Olarak: Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku, İstanbul, On İki Levha, 2017, s. 83.

[413] Bergkamp, Dhont, a.g.e., s. 84.

İletişim kurmak maksadıyla kişisel verileri elde edilen kişi ile ilgili olarak aydınlatmanın en geç iletişimin gerçekleştiği anda olması gerekir. Kişisel verileri başka alıcılara açıklanmasının söz konusu olduğu durumlarda en geç bu verilerin açıklanmasının gerçekleşeceği ilk anda aydınlatma yükümlülüğünün sağlanmış olması gerekmektedir.

Yapılan düzenlemeler değerlendirildiğinde kişisel veri işleme faaliyetinin kişilerin temel hak ve özgürlüklerini kullanmaları bakımından nedenli önemli olduğu düşünüldüğünde, kanunla düzenlenen haklarını kullanabilmeleri ve verilerin işleme faaliyetine katılabilmeleri için aydınlatma yükümlülüğünün makul süre içerisinde yerine getirilmesi oldukça önemlidir. Çok uzun zaman sonra yapılan aydınlatmanın kişisel verilerin korunması açısından bir anlamı olmayacaktır[414]. Bu konuda istisna diyebileceğimiz durumlar söz konusu olabilir. Verisi işlenen ilgili kişinin bilgilendirilmesi imkânsız olabilir, orantısız çaba gerektiriyor olabilir veya kanundan kaynaklanan bir durum söz konusu olabilir bu tür durumlarda aydınlatma yükümlülüğünün yerine getirilmesi gerekmez[415].

Bir diğer düzenleme olan Aydınlatma Tebliği'nin içeriğinde kişisel verilerin ilgili veri sahibi kişiden sağlanmaması durumunda aydınlatma yükümlülüğünün hangi aşamada yerine getirileceği ile ilgili olarak düzenlemeler yapıldığını görmekteyiz. Yapılan bu düzenlemeye göre kişisel verisi elde edilen kişinin makul bir zaman diliminde aydınlatılması gerektiği ifade edilmiştir. Bunun yanında söz konusu kişi ile iletişim kurmak maksadıyla kişisel verisi elde edilen kişinin, ilk iletişim kurulduğu anda veya ilgili kişinin verilerinin aktarılması söz konusu olacaksa, en geç kişisel verilerin aktarılacağı anda aydınlatma yükümlülüğünün yerine getirilmesi gerekmektedir. Aydınlatma yükümlülüğünün bir ihlale sebep olmaması için belirlenen süreler içerisinde kişinin verileri hakkında aydınlatılmış olması gerekmektedir. Bu durumun sağlanamaması durumunda aydınlatma yükümlülüğünün yerine getirilmemesi kabahati oluşacaktır.

İlgili düzenlemelerden olan Aydınlatma Tebliği'nde yer alan makul süre ibaresinin birçok soruna neden olacağı kanaatindeyiz. Zira makul süreden ne anlaşılacağı belirsizlik ifade

[414] Guidelines on Transparency under Regulation 2016/679, s. 16.
[415] Bergkamp, Dhont, a. g. e., s. 84.

etmektedir. Düzenlemede kullanılan makul süre ifadesinin, kabahat eyleminin ne zaman işleneceği ile ilgili olarak net bir durumun olmaması hasebiyle, ilgili düzenlemenin kanunilik prensibine uymadığını ifade edebiliriz. Veri koruma Tüzüğü'nde yapılan düzenlemeler ile benzer olarak Aydınlatma Tebliği'nde de makul süre ifadesinin, sürenin net olarak belirtilerek aydınlatma yükümlülüğünün yerine getirilmesinin, kabahat fiilinin oluşmasını engelleyeceğini düşünmekteyiz. Bireyin toplanan kişisel verilerine ilişkin olarak daha önce zamanında aydınlatılma yükümlülüğü yerine getirilmiş olsa bile veri işleme faaliyetlerinde esaslı değişikliklerin olması durumunda, değişen faaliyetler etkisini göstermeden kişinin bilgilendirilmesi gerekmektedir[416]. Dolayısıyla kişisel verilerin toplanma amacından farklı olarak işlendiği durumda kişinin esaslı haklarının korunması adına makul bir süre içerisinde aydınlatılması gerekmektedir[417]. Aydınlatılma faaliyetinin özellikle kişinin verilerine ilişkin olarak vereceği rızadan önce yerine getirilmiş olması gerekmektedir.

Çeşitli araçlar ile ürünlerin, malların, işlerin, fikrin, hizmetlerin tanıtımının ve sürümünün arttırılmasını hedefleyen[418] kitle iletişim araçları kullanılarak belirli bir tüketici kitlesini istenilen doğrultuda davranışa yönelten[419] faaliyetler reklam olarak tanımlanabilir[420]. Tüketicilerin satın alma tercihleri konusunda nihai kararlarını etkileyebilecek biçimde yanlış, yanıltıcı ya da eksik bilgi içermek suretiyle[421] ya da vermiş olduğu bilgi doğru olsa bile bilginin aktarılma biçimi nedeniyle makul olan tüketiciyi aldatan ya da aldatma ihtimali olan tanıtımlar aldatıcı reklam olarak ifade edilmektedir[422]. Reklam içerisindeki iddiaların her koşulda mutlak ve bilimsel olarak ispatı aranmasa bile güvenilir, tutarlı ve makul bir biçimde ispat edilmesi yeterli görülmektedir. Açık ya da örtülü olarak bilimsellik iddiası bulunan bir reklamda makul bir tüketici bilimsel gerçeklik iddiasını algılamakta haklı görülüyorsa bu durumda reklamın bilimsel veriler ile ispatı gerekmektedir[423]. İnternet reklamcılığının, çeşitli sorunlara neden olduğunu düşünmekteyiz. Zira, internet ortamında

[416] Guidelines on Transparency under Regulation 2016/679, s. 17.
[417] Guidelines on Transparency under Regulation 2016/679, s. 24.
[418] Emrehan İnal/ Başak Baysal, Reklam Hukuku ve Uygulaması, İstanbul 2008, s. 7
[419] İnal/ Baysal, a. g. e., s. 7
[420] Zeynep Derya Tarman, Haksız Rekabetten ve Aldatıcı Reklamlardan Doğan Uyuşmazlıklarda Uygulanacak Hukuk, İstanbul 2011, s.153; Neval OKAN, Ağ Reklamları ve Haksız Rekabet, Ankara 2011, s. 39.
[421] İnal/ Baysal, a. g. e., s. 26
[422] İnal/ Baysal, a. g. e., s. 29-35.
[423] İnal/ Baysal, a. g. e., s. 36.

yapılan pazarlama ve reklam uygulamalarında kişisel verilerin ihlal edilmesine sıklıkla rastlanılmaktadır[424]. Kullanıcıların cihazlarına yerleştirilen çerezler[425] yardımıyla, teknolojik araçlarındaki datalara erişilmekte ve bu sayede kullanıcıya ait veriler toplanmaktadır[426]. Ulaşılan bu veriler yardımıyla kullanıcıların profilleri oluşturulmakta ve bu profillere uygun olan reklamlar kullanıcılara sunulmaktadır[427]. Zira bu reklamlar sayesinde verisi işlenen birey kolaylıkla yönlendirilebilmektedir. Reklam hukukunda esas olan tüketicilerin aldatılmasının önüne geçilerek serbest piyasanın, rakiplerin ve rekabetin korunması olması nedeniyle reklam serbestliğinin esas olmasının gözardı edilmeden reklamların kontrol edilmesi, tüketicilerin ekonomik davranış iradelerinin yanlış veya yanıltıcı bilgilerden korunması reklam hukuku açısından son derece önemlidir[428].

Kişilerin rızalarının alınmadan verilerinin işlendiği bir diğer önemli mecra, internet sitelerinin içerisine gömülü bulunan çevrimiçi davranışsal reklam uygulamalarıdır. Bu alanlarda aydınlatılma yükümlülüğü göz ardı edilerek, hatta kişinin rızası alınmadan kişisel verilerin işlendiği görülmektedir[429]. Oysa her ortamda olduğu gibi internet ortamında da kişilerin verilerine ilişkin olarak aydınlatılmaları ve buna uygun olarak rızalarının alınmaları gerekmektedir. Zira kişilerin verileri üzerinde denetim yetkilerini kullanmaları ancak bu şekilde sağlanabilecektir[430].

5.2.2.2. Aydınlatma yükümlülüğünün yerine getirilmesinde şekil unsurları

24/03/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu m. 10 uyarınca veri sorumluları veya yetkilendirdiği kişilerce yerine getirilmesi gereken aydınlatma yükümlülüğü; sözlü, yazılı veya ses kaydı yapılarak, fiziksel veya elektronik ortamlar kullanılarak yerine getirilebilir (m. 5/1). Bahse konu bu yükümlülük kişilerin yüzlerine karşı

[424]Mine Kaya, Elektronik Ortamda (Elektronik Haberleşme-İnternet-Sosyal Medya) Kişilik Hakkının Korunması, Ankara, Seçkin, 2015, s. 139; Funda Başaran, 'Ağ Ekonomisi ve İnternet, İletişim Ağlarının Ekonomisi, Ed.: Funda Başaran, Haluk Geray, Ankara, 2005, s. 251; Kaya, a. g. e., s. 139.
[425] Şimşek, a. g. e., s. 178.
[426] Başaran, a. g. e., s. 139.
[427] Başaran, a. g. e., s. 249; Kaya, a. g. e., s. 139.
[428] Emrehan İnal/ Başak Baysal, Reklam Hukuku ve Uygulaması, İstanbul 2008, s. 1.
[429] Öngün, a. g. e., s. 137.
[430] Başaran, a. g. m., s. 252.

sözlü yapılabileceği gibi, mobil uygulamalar vasıtasıyla ya da internet sayfalarında yer alan sayfaların giriş ekranları vasıtasıyla yerine getirilmesi mümkündür[431].

Görüldüğü üzere aydınlatma yükümlülüğü birçok yoldan yerine getirilebilmektedir. Zira aydınlatma yükümlülüğü yerine getirilirken somut olayın özelliği dikkate alınarak veri sorumlusu veya yetkilendirdiği kişi tarafından karar verilir[432]. Aydınlatma yükümlülüğünün sağlıklı bir şekilde yapılabilmesi için seçilen yöntemin somut olaya uygun olması oldukça önemlidir. Üniversitelere kayıtlı bulunan öğrencilerin öğrenci bilgi giriş ekranlarında, kişisel verileri işlenen öğrenci sayısı düşünüldüğünde aydınlatma yükümlülüğü kapsamında hazırlanan aydınlatma metninin üniversitenin internet sitesine, ilgili tüm öğrencilerin ulaşabileceği bir biçimde koyulması daha uygun olacaktır. Bunun dışında bir başka örnek verecek olursak ekran vasıtasıyla bir aydınlatmanın söz konusu olduğu durumlarda şayet ekran seçeneğimiz bulunmuyorsa, aydınlatma yükümlülüğünü yerine getirebilmek için ses dosyaları kullanılabilir[433]. Kişilerin engelli olması, çocuk olması düşünüldüğünde bu gruptaki kişilerin faaliyetlerinde aydınlatma metinleri somut durum düşünülerek hazırlanmalıdır[434]. Kişisel verisi işlenen kişi şayet çocuk ise aydınlatma yükümlülüğü, animasyonlar, çizgi karakterler ve buna benzer araçlar kullanılarak yerine getirilebilir[435]. Dolayısıyla verisi işlenen kişilerin somut durumları göz önünde bulundurularak aydınlatma metinleri hazırlanmalıdır.

Aydınlatma yükümlülüğünün, söz konusu kişilerin anlayacağı biçimde yalın, açık ve anlaşılır olması oldukça önemlidir[436]. Genel Veri Koruma Tüzüğü'ne göre; veri sorumlusu ve yetkilendirdiği kişi tüzükte düzenlenen her türlü bildirimi, şeffaf, anlaşılır, öz, kolay erişilebilir bir şekilde, açık ve sade bir dil kullanımını benimseyerek veri sahibi olan kişiye bunları sağlamak için gerekli tedbirleri almak zorundadır. İlgili kişilere yapılacak bildirimler somut olayın şartlarına uygun olarak yazılı olabileceği gibi elektronik yollar kullanılarak da yapılabilir. Bunun yanında Genel Veri Koruma Tüzüğü'ne göre, veri sorumlusunun talep

431 Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi, s. 14.
432 A. g. e., s. 14.
433 Guidelines on Transparency under Regulation 2016/679, s. 12.
434 Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi, s. 14.
435 Guidelines on Transparency under Regulation 2016/679, s. 12.
436 Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi, s. 14.

etmesi ve ilgili kişinin açık kimlik bilgisinin başka şekilde teyit edilmesi koşuluyla bilgiler sözlü olarak da sağlanabilmektedir (m. 12).

Kişisel verilerin korunması bakımından aydınlatma yükümlülüğü gereği yerine getirilirken çoğunlukla aydınlatma metinleri düzenlenerek veri sahiplerine sunulmaktadır.

Hazırlanan aydınlatma metinlerinin muhteviyatını incelediğimizde; bu metinlerde kullanılan dilin çok önemli olduğunu görmekteyiz. Aydınlatma yükümlülüğünün yerine getirilmesinde uyulacak usul ve esaslar hakkındaki tebliğ'e göre ilgili kişiye yapılacak aydınlatmanın açık, şeffaf, anlaşılır ve sade bir dil kullanılarak yapılması, muğlak ve genel nitelikli ifadelerin bulunmamasına dikkat edilmelidir (m. 5/1-g). Zira, Veri koruma Tüzüğü'nde yapılan düzenlemede de veri sorumlusu ve yetkilendirdiği kişinin, kişisel verilerin işlenmesine ilişkin olarak yapacağı tüm işlemleri açık ve sade bir dil kullanarak, şeffaf, anlaşır bir şekilde söz konusu kişilere sunması gerektiği söylenmektedir (m. 12). Toplanan kişisel verilerin olası farklı amaçlar için kullanılmaması için aydınlatma metinlerinde muğlak ifadelerin bulunmamasına azami dikkat edilmelidir (m. 5/1-g). Ancak tüm bu yapılan düzenlemelere rağmen uygulamada hazırlanan aydınlatma metinlerinde karmaşık ve muğlak ifadelerin kullanıldığını görmekteyiz[437].

Kişisel Verileri Koruma Kurumu tarafından, uygulayıcılara rehberlik etmesi için düzenlenip yayımlanan Kişisel Verilerin Korunması Kanununun Uygulanmasına Yönelik Soru ve Cevaplar isimli kaynakta veri sorumlusu olan kişi aydınlatma yükümlülüğünü yerine getirirken kişilere katmanlı bir biçimde bilgilendirme yapabileceği noktasında tavsiyede bulunmaktadır[438]. Söz konusu bu tavsiye doğrultusunda öncelikli olarak aydınlatma yükümlülüğünün yerine getirilmesi kapsamında kolayca ulaşılabilecek bir metnin hazırlanması ve hazırlanan bu metnin kısa, muğlak ifadelerden arındırılmış, açık ve anlaşılır olması gerekmektedir. Kişisel verilerin işleme faaliyeti hakkında detaylı bilgi sahibi olmak isteyen kişiler daha detaylı bilgi sahibi olabilecekleri kaynaklara yönlendirilirler[439]. Söz konusu katmanlı bu uygulamanın hukuka uygun olduğu Kişisel Verilerin Korunması

[437] Mesut Serdar, Çekin, 6698 sayılı Kişisel Verilerin Korunması Hakkında Kanun'un Big Data (Büyük Veri) ve İrade Serbestisi Açısından Değerlendirilmesi, İÜHFM, C. LXXIV, S.2, 2016, s. 637.
[438] 6698 sayılı Kişisel Verilerin Korunması Kanununun Uygulanmasına Yönelik Soru ve Cevaplar, s. 68.
[439] A. g. e., s. 68

Kanunu kapsamında yapılan düzenlemeler incelendiğinde görülmektedir. Ayrıca kişisel verilerin işlenmesine ilişkin aydınlatma yükümlülüğünün yerine getirilebilmesi için, veri işleme faaliyetinin açık rıza şartına bağlı olarak gerçekleştirilmesi durumunda, aydınlatma yükümlülüğü ve açık rıza işlemlerinin ayrı olarak düzenlenip ilgili kişilere bildirilmesi gerektiği kararına varılmıştır[440]. Açık rıza metni ve aydınlatma metinlerinin herhangi bir metin içerisinde kişiye sunulması hukuka uygun değildir. Bu konuda Kişisel Verileri Koruma Kurumu vermiş olduğu örnek bir kararında, aydınlatma yükümlülüğünün bağımsız bir faaliyet olduğu, açık rızanın arandığı durumlarda aydınlatma metninin, açık rıza aranan metinden farklı olarak kişilere sunulması gerektiği kararına varılmıştır[441]. Genel Veri Koruma Tüzüğü'nde yapılan düzenlemeye göre, veri işleme faaliyetine ilişkin olarak, veri sahibinin yeterli bilgi sahibi olduğu durumlarda, veri sorumlusunun aydınlatma yükümlülüğünü yerine getirmiş olduğu kabul edilir[442]. Veri sorumlusunun buradaki sorumluluğu veri sahibinin verilerinde herhangi bir değişikliğin olmadığı, kişinin verilerinin veri işleme faaliyetine uygun olup olmadığı ile ilgili sorumluluklar veri sorumlusundadır[443].

5.2.2.3. Aydınlatma yükümlülüğü kapsamında yapılan bilgilendirmede bulunması gereken unsurlar

Kişisel Verilerin Korunması Kanunu bakımından aydınlatma yükümlülüğünün yerine getirilmiş olabilmesi için kişilerin hangi hususlarda bilgilendirilmesi gerektiği gerek Kişisel Verilerin Korunması Kanunu'nda gerekse de Aydınlatma Tebliği'nde düzenlenmiştir.

Veri sorumlusu ve yetkilendirdiği kişinin kimlik bilgisi, veri toplamanın usulü ve hukuki gerekçesi, kişisel verilerin hangi amaçla işleneceği, işlenen verilerin kimlerle hangi saikle aktarılabileceği KVKK m. 10'da düzenlenmiştir. Bunun yanında verisi işlenen söz konusu kişinin, veri sorumlusuna ve varsa temsilcisine başvurmak suretiyle kullanabileceği, veri işleme faaliyeti bakımından var olan hakları da KVKK m. 11'de düzenlenmektedir. Yapılan bu düzenlemeler doğrultusunda verisi işlenen kişi, düzenlemeler kapsamında kişisel

[440] Küzeci, a. g. e., s. 242.
[441] Kişisel Verileri Koruma Kurulunun 26/07/2018 tarihli ve 2018/90 sayılı Kararı, (Çevrimiçi), https://kvkk.gov.tr/Icerik/5420/-Veri-sorumlusu-tarafindan-aydinlatma-yukumlulugu-ve-acik-riza-onayi-alinmasi-sureclerinin-ayri-ayri-yerine-getirilmesi-gerektigi-ile-ilgili-Kisisel-Verileri-Koruma-Kurulunun-26-07-2018-tarihli-ve-2018-90-sayili-Karar-Ozeti, (Erişim Tarihi: 03/05/2022).
[442] Guidelines on Transparency under Regulation 2016/679, s. 27.
[443] A. g. e., s. 27.

verisinin işlenip işlenmediği, şayet işlendiyse buna ilişkin bilgileri talep etme, aktarılan diğer kişileri bilme, verilerinin hatalı veya eksik işlenmesi durumunda düzeltilmesini isteme, başta belirlenen amaca uygun hareket edilip edilmediğini öğrenme, kayıt altına alınmış verilerinin silinmesini veya yok edilmesini isteme, talep edilen düzeltme, sildirme ve yok etme taleplerinin verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme, verilerin otomatik sistemler vasıtasıyla analiz edilmesi sonucunda verisi işlenen kişi aleyhine sonuçlar çıkarılmasına itiraz edebilme ve verilerin yapılan kanuni düzenlemelere aykırı biçimde işlenmesi nedeniyle zararın doğması durumunda, doğan bu zararın karşılanmasını talep etme haklarına sahiptir.

Veri sorumlusu ve yetkilendirdiği kişi, kişisel verileri ister veri sahibi kişiden, isterse de kişi haricinde başka bir kaynaktan elde etmiş olsun yukarıda sıralanan tüm konular hakkında ilgili kişiye karşı aydınlatma yükümlülüğünü yerine getirmelidir.

Kişisel Verilerin Korunması Kanunu kapsamında yukarıda açıkladığımız biçimde düzenleme yapılmış olmasına rağmen Veri Koruma Tüzüğü m. 13 ve m. 14'te verilerin elde edildiği kaynağa göre aydınlatma yükümlülüğünün içeriğinin düzenlenmesi gerektiği söylenmektedir. Veri Koruma Tüzüğü'nde kişisel verilerin ilgili kişiden elde edilmesi durumunda aydınlatma yükümlülüğünün yerine getirilme biçimi ile ilgili olarak m. 13 düzenlemesinin genel anlamda KVKK ile uyumlu olduğu görülmektedir. KVKK'dan farklı olarak Veri Koruma Tüzüğü'nde aydınlatma yükümlülüğü bağlamında gerekli asgari bilgilendirmenin yapılmasının yanı sıra, elde edilen verilerin hukuk kaidelerine uygun olarak ve şeffaf biçimde işlenmesinin sağlanması için gereken ek bilgiler de düzenlenmektedir.

Kişisel Verilerin Korunması Kanunu'nda yer alan düzenlemeler incelendiğinde, veri sahibine yapılacak olan aydınlatma yükümlülüğü hakkında gerekli asgari hususlar olduğundan veri sorumlusunun, hukuka uygun ve şeffaf bir veri işleme faaliyetini gerçekleştirmek adına çeşitli ek bilgiler vermesinin önünde herhangi bir engel bulunmamaktadır.

Veri Koruma Tüzüğü'nde yapılan düzenlemeye baktığımızda KVKK'dan farklı olarak, kişisel verilerin farklı bir kaynaktan elde edilmesi durumunda aydınlatma metninin içeriği

de ayrıca düzenlenmektedir. Yapılan düzenleme gereğince söz konusu verilerin hangi kaynaktan alındığının tespit edilmesi ve şayet kamunun ulaşabileceği kaynaklardan elde edilmiş ise bu konuda açıkça bilgilendirilmenin yapılması gerektiği ifade edilmiştir (m. 14/2-f). Kişisel Verilerin Korunması Kanunu açısından böyle bir düzenlemeden bahsedilmeyecek olsa bile, veri sorumlusu ve yetkilendirdiği kişi vasıtasıyla, kişisel verilerin toplanma yöntemi ve hukuki gerekçesi hakkında ilgili kişiyi bilgilendirdiği aşamada, kişisel verileri elde ettiği kaynağa ilişkin bilgiler de verebilir[444].

Veri Koruma Tüzüğü'ndeki bir diğer farklı düzenlemeye baktığımızda, veri sorumlusunun ve temsilcisinin kimlik bilgilerinin yanı sıra iletişim bilgilerinin de aydınlatma yükümlülüğü faaliyeti kapsamında açıklanması gerektiği ifade edilmiştir. Veri sorumlusu ve temsilcisinin iletişim bilgilerinin ilgili kişi tarafından bilinmesinin veri sahibinin KVKK kapsamında haklarını aktif bir biçimde kullanılması bakımından önemli olduğu düşünülmektedir[445]. Dolayısıyla her ne kadar KVKK'da veri sorumlusunun iletişim bilgilerinin aydınlatma yükümlülüğü bakımından düzenlenmemiş olsa bile ilgili kişinin haklarını aktif kullanabilmesi için bilgilendirmenin yapılması gerektiğini düşünmekteyiz.

Kişisel verilerin korunması bakımından, kişisel verilerin işlendiği bütün süreçlerde ve işlenme amacının değişiklik gösterdiği her durumda verisi işlenen bireyin aydınlatılması gerekmektedir (Aydınlatma Tebliği m. 5). Kişisel veri işleme amacının değişiklik gösterdiği durum söz konusu olduğunda daha önce ilgili kişiye yapılan aydınlatmanın geçerliliği kalmayacak olup, yeni amaç doğrultusunda aydınlatma yükümlülüğünün yerine getirilmesi gerekmektedir[446].

KVKK kapsamında verileri toplanan kişilerin, ilgili konu bağlamında karşılaşabilecekleri veri sızıntısı ya da diğer sorunlar bakımında ayrıntılı bilgilendirilmeleri ve bu sorunlara ilişkin çözümler açısından aydınlatılmış olmaları kişisel verileri hakkında verecekleri karar bakımından oldukça önemli olacaktır[447].

---

[444] Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi, s. 16.
[445] Develioğlu, a. g. e., s. 83.
[446] Kişisel Verilerin Korunması Kanununun Uygulanmasına Yönelik Soru ve Cevaplar, s. 66.
[447] Working Party on Information Security and Privacy, The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines, 2011, s. 25.

Günümüz uygulamalarında, kişisel verilerin internet ortamında ya da başka yollarla elde edilmesi durumunda aydınlatma metinlerinin kullanıldığını görmekteyiz[448]. Hazırlanan bu aydınlatma metinlerinin genel anlamda KVKK ile uyumlu olduğunu ifade edebiliriz. Ancak bu aydınlatma metinlerinin yukarıda bahsetmiş olduğumuz diğer düzenlemeler bakımından değerlendirdiğimizde kişisel verilerin işlenmesi bakımından özellikle olması gereken asgari hususlara değinmemesi açısından tam manasıyla aydınlatma yükümlülüğünün yerine getirildiğini söyleyemeyiz.

Kişisel Verileri Koruma Kurulu tarafından verilen kararlar konu bağlamında incelendiğinde, örnek olayımızda bir bankanın internet sayfasında ilgili kişilere sunulan yayımlanan aydınlatma metninde, kişisel verilerin hangi hukuki gerekçeye dayanılarak işlendiğinin açıkça ifade edilmediği, verilerin işleme koşullarının sıralamasından sonra "g*ibi amaçlar kapsamında işlenecektir."* biçiminde bir ifade kullanıldığı, ilgili ifadenin muğlak olduğu, dolayısıyla kişisel verilerin bilgilendirme kapsamı dışındaki amaçlar için işlenebileceği izlenimini uyandırdığı ve bu sebeple bankanın internet sayfasında sunduğu aydınlatma metninin ilgili düzenlemelere aykırı olduğu ifade edilmektedir[449].

KVKK kapsamında aydınlatma yükümlülüğünün muhteviyatı verilerin işlendiği alanlara göre değişiklik göstermektedir. Örneğin üniversite öğrencileri ile ilgili düzenlenecek özlük dosyaları içerisinde, kimlik bilgileri, iletişim bilgileri, ÖSYM puan bilgileri, bazı bölümler için sağlık raporu bilgilerinin saklamak zorunda olduğu bilinmektedir. İlgili üniversitenin veri sorumlusu veya yetkilendirdiği kişi ilgili kişinin özlük dosyası hakkında bilgilendirmek zorundadır. Söz konusu kişiye ait dosyanın hangi amaçla tutulduğu, toplanan bilgilerin nerede ve nasıl kullanılacağı ve kimlere aktarılabileceği noktasında ayrıntılı bir biçimde aydınlatılması gerekmektedir.

[448] Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi, s. 18.
[449] Kişisel Verileri Koruma Kurulunun 02/05/2019 tarihli ve 2019/122 sayılı Karar, (Çevrimiçi), https://kvkk.gov.tr/Icerik/5461/2019/122 , (Erişim Tarihi: 03/05/2022).

5.2.3. Fail

Kanun koyucu tarafından yapılan yasal düzenlemelerde kabahat olarak ifade edilen eylemi gerçekleştiren kişi, fail olarak ifade edilmektedir[450]. Fail olarak ifade edilen kişi, tipe uygun eylem üzerinde egemenliği bulunan kişidir[451]. Özgü kabahatler açısından baktığımızda, yasada düzenlenen eylemi yalnız yine yasada düzenlenen özelliklere sahip olan kişiler gerçekleştirebilir ve yalnızca bu kişiler fail olarak sorumlu tutulurlar[452]. Zira, özgü kabahatler kaide olarak, ancak özel bir sorumluluk altında bulunan kişilerce işlenebilir[453].

Aydınlatma yükümlülüğü bakımından kabahat fiilinin gerçekleşebilmesi için veri sorumlusu ve temsilcisinin bilgilendirme yapmamış olması gerekmektedir (KVKK m. 10). Zira KVKK bakımından aydınlatma yükümlülüğü, yalnızca veri sorumlusu veya temsilcisi açısından sorumluluk doğurmaktadır. Bu sebeple aydınlatma yükümlülüğünün sağlanamaması durumunda işlenen kabahat özgü kabahati ifade etmektedir.

Kişisel Verilerin Korunması Kanunu kapsamında ifade edilen veri sorumluları, gerçek veya tüzel kişi olabilir[454]. Veri sorumlusu ya da yetkilendirdiği kişi, verilerin işlenme politikalarını ve amaçlarını belirleyen kişilerdir (KVKK m. 3/1-ı). Kişisel veriler veri sorumlusu veya temsilcisi dışındaki kişilerce de işlenebilir. Veri sorumlusunun verdiği yetkiye dayanarak veri sorumlusu adına kişisel verilerin işlenmesini sağlayan gerçek veya tüzel kişiler olabilir. KVKK kapsamında veri sorumlusu tarafından yetkilendirilen veri işleyenlerin de aydınlatma yükümlülüğü bulunduğundan kabahatler bakımından fail olarak ifade edilebilirler.

Özel hukuk bakımından hak süjesi olan toplulukların tüzel kişiliklerinin kabul edilmesi durumunda, yapmış olduğu işlemlerden doğan sorumluluklarının kaide olarak kendi içerisinde barındırdığı gerçek kişilere ait olmaması, bu türden toplulukların yaygın hale

[450] Kangal, a. g. e., s. 134.
[451] Mahmut Koca, İlhan, Üzülmez, Türk Ceza Hukuku Genel Hükümler, 11. Baskı, Ankara, Seçkin, 2018, s. 114.
[452] Akbulut, a.g.e., s. 333; İçel, a.g.e., s. 140.
[453] İçel, a. g. e., s. 90.

gelmesinde katkı sağlamıştır[455]. Bunun dışında tüzel kişiye ait bir malvarlığının bulunması idari sorumluluk bakımından da tüzel kişiliği muhatap haline getirmiştir[456]. Cezai sorumluluk bakımından incelendiğinde ise gerçek kişilerin suç işlemesi esasına dayalı olarak inşa edilen, uygulanmakta olan klasik hukuk anlayışının bu türden toplulukların haksızlık oluşturup oluşturamayacakları sorusuna cevap bulunması kolay olmamış ve bu sorunun cevabı tartışılmaya devam etmektedir. Doktrinde tüzel kişiliğin hukuki niteliğine ilişkin çokça tartışılmış ve bu kapsamda birçok teori ileri sürülmüştür. İleri sürülen bu teorilerden Gerçeklik teorisine göre[457], tüzel kişilerin de gerçek kişiler gibi sosyal hayatın bir gerçekliği olduğunu ileri sürer. İleri sürülen bu teoriye göre tüzel kişilerin var olabilmesi için hukuka ihtiyacı bulunmamaktadır. Hukukun, zaten var olan tüzel kişileri tanıdığını ileri sürmektedir. Farazilik teorisine göre ise[458], doğal yaşamda sadece gerçek kişilerin bir kişiliği bulunduğunu iddia eder. Tüzel kişilerin ise sadece bir varsayımdan ibaret olduğunu ileri sürer. Bir diğer teori ise amaç birliği teorisi[459], varsayım ve farazilik teorilerinin olumlu taraflarını dikkate alarak, tüzel kişilerin belirli amaçlarla oluşturulmuş insan ve mal toplulukları olduğu görüşünü ileri sürmektedir. Soyutlama teorisinin ileri sürdüğü düşünceye göre ise[460], tüzel kişiler ne varsayım ne de soyutlamadır. Soyutlama teorisine göre tüzel kişilerin insan fikrinin bir ürünü olduğunu ileri sürmektedir.

Türk ceza hukukunun yaklaşımı diğer teoriler ile mukayese edildiğinde varsayım teorisine daha yakın durduğunu söyleyebiliriz. Zira ceza hukuku düzenlemesinde tüzel kişilerin cezai sorumlulukları bulunmamaktadır. Tüzel kişiler yalnızca iznin iptali ve müsadere gibi güvenlik tedbirlerinin muhatabı olabilirler (TCK m. 20/2; m. 60). Hareket kabiliyetleri ve

---

[455] Dural, Mustafa / Öğüz, Tufan, Türk Özel Hukuku C.II, Kişiler Hukuku, İstanbul 2012, s. 105; Oğuzman, Kemal / Seliçi, Özer / Oktay Özdemir, Saibe: Kişiler Hukuku (Gerçek ve Tüzel Kişiler), İstanbul 2012, s. 250; İkizler, Metin, Tüzel Kişilerin İlkeli Kişiliği Bu Uğurda Ana Statüsünün Anlamı ve İşlevi, Ankara 2012, s. 42; Kangal, Zeynel, Tüzel Kişilerin Cezai Sorumluluğu, Ankara 2003, s. 145

[456] Laue, Christian, Die Strafrechtliche Verantwortlichkeit von Verbanden, JURA 5/2010, s. 342.

[457] Tiedemann, Klaus, Tüzel Kişiler Hakkında Uygulanan Yaptırımlar, Editör, Prof. Dr. Ayşe Nuhoğlu, İstanbul 2013, s. 22.

[458] Oğuzman / Seliçi / Oktay Özdemir, s. 242; Ayan / Ayan, s. 196; Dönmezer, Sulhi / Erman, Sahir, Nazari ve Tatbiki Ceza Hukuku, C.II, İstanbul 1994, s. 403; Artuk, Mehmet Emin / Gökcen, Ahmet / Yenidünya, Caner: Ceza Hukuku Genel Hükümler, İstanbul 2009, s. 293; Kangal, Tüzel Kişilerin Ceza Sorumluluğu, s. 31; Demirbaş, Timur, Ceza Hukuku Genel Hükümler, Ankara 2014, s. 230.

[459] Oğuzman /Seliçi / Oktay Özdemir, s. 244

[460] (Çevrimiçi), https://link.springer.com/content/pdf/10.1007/978-94-007-0674-3.pdf , (Erişim Tarihi:07/05/2022), Pieth, Mark / Ivory, Radha, Corporate Criminal Liability; Emergence, Convergence, and Risk; Editor, Mark Pieth, Radha Ivory, 2011, s. 6

kusur yeteneklerinin olmamasından dolayı suç işleyemeyecekleri, yalnızca gerçek kişilerin suçun faili olabileceği kabul edilir[461]. Benzer biçimde Türk kabahatler hukukunda yapılan düzenlemelerde de tüzel kişilerin kabahat faili olamayacakları, gerçek kişilerin eylemlerinden doğan bir kabahat sorumlulukları olduğu kabul edilmektedir[462]. Bu söylediklerimizi Kabahatler Kanunu m. 8'le birlikte değerlendirdiğimizde yalnızca gerçek kişilerin fail olabileceği kabul edilmelidir[463]. Zira Kabahatler Kanunu'ndaki yükümlülükleri tüzel kişilik veya topluluk yerine getirmemiş gibi gözükse de esasen yükümlülüğü ihmal eden ilgili gerçek kişi veya kişiler olduğunu ifade edebiliriz.

Tüzel kişinin veri sorumlusu olması durumunda, aydınlatma yükümlülüğünün tüzel kişi tarafından ifa edilmediği durumda kabahat eyleminin gerçekleşip gerçekleşemediği tartışılmaktadır. Ceza hukukunda olduğu gibi kabahatler hukukunda da hareket, irade ve irade yeteneklerini taşımadığı düşünülen tüzel kişiler[464] fail olarak kabul edilmezler[465].

Kabahatler Kanunu m. 8 de, temsilcilik görevi yapan veya tüzel kişinin faaliyeti kapsamında vazifelendirilen kişinin bu vazife kapsamında işlemiş olduğu kabahatten ötürü tüzel kişiliğe ilişkin idari yaptırım uygulanacağı belirtilmektedir. Ceza hukukunda düzenlenen ceza sorumluluğunun şahsiliği ilkesi kabahatler bakımından kabul edilmediği bu bağlamda ifade edilebilir[466]. Dolayısıyla söz konusu düzenleme bakımından, tüzel kişiler kabahat işleyemezler[467]. Ancak şartların sağlanması durumunda, tüzel kişilik bünyesinde bulunan gerçek kişilerin işlemiş olduğu fiillerden dolayı kabahatlerden sorumlu tutulurlar. Ancak burada özellikle dikkat edilmesi gereken tüzel kişilik bünyesinde bulunan kişilerin işlemiş oldukları kabahatleri vazifeleri kapsamında işlemiş olmaları gerekmektedir[468].

---

[461] Centel, Nur / Zafer, Hamide / Çakmut, Özlem Yenerer, Türk Ceza Hukukuna Giriş, İstanbul 2011, s. 243; Özgenç, İzzet, Türk Ceza Hukuku Genel Hükümler, Ankara 2015, s. 194 ve s. 839; Hakeri, s. 140; Artuk / Gökcen / Yenidünya, s. 302.

[462] Kangal, Zeynel, Kabahatler Hukuku, İstanbul 2011, s. 216; Akbulut, s. 351; Pehlivan, Ali, Kabahatler Hukukunun Genel Esasları, İstanbul 2011, Doktora Tezi, s. 246.

[463] Öztürk, Gizem Sarıbay, İş Sağlığı ve Güvenliği Yükümlülüklerinin Yerine Getirilmesinin Hukuki, İdari ve Cezai Sonuçları, İstanbul 2015, s. 328.

[464] İçel, a. g. e., s. 265.

[465] Kangal, a. g. e., s.105; Hakeri, a. g. e., s. 148.

[466] Murat Ekinci, ''Ceza Hukuku İlkeleri Açısından İdari Yaptırımlar'', YBHD, S.3, 2017, s. 38.

[467] Akbulut, a. g. e., s.333; İçel, a. g. e., s. 352.

[468] Akbulut, a. g. e., s. 333; İçel, a. g. e., s. 379.

Örneğin, merkezi yurt dışında bulunan özel hukuk tüzel kişilerinin, organ ya da temsilcilik görevi yapmamakla birlikte tüzel kişinin faaliyeti bakımından görev yapan kişinin, Türkiye'de kabahat işlemesi durumunda, fiil Türkiye'de gerçekleştiğinden ve failin adresi Türkiye'de bulunduğundan söz konusu yabancı tüzel kişi hakkında idari para cezası uygulanması mümkün olacaktır[469].

Düzenlenen yasanın lafzı incelendiğinde tüzel kişilere idari müeyyide uygulanması takdire bırakıldığı görülmektedir. Ancak kabahatin düzenlendiği ilgili mevzuatta tüzel kişilere de idari müeyyide uygulanabileceği biçiminde düzenlemeler görülmektedir[470].

Veri sorumlusunu veya temsilcisinin tüzel kişi olması durumunda, aydınlatma yükümlülüğü yerine getirilmediğinde işlenen bu kabahatten dolayı idari para cezası tüzel kişiliğe uygulanabilecektir. Bu bağlamda KVKK m. 18/2 düzenlemesine göre, veri sorumlusu olan gerçek ve tüzel kişiler hakkında da idari para cezasının uygulanacağı ifade edilmektedir. Ancak burada özellikle ifade edilmesi gereken nokta, idari para cezalarının sadece özel hukuk tüzel kişileri için uygulanabileceğinin ifade edilmesi gerekir. KVKK m. 8'de bu konuyla ilgili açık düzenleme bulunmaktadır. Bu düzenlemeye göre özel hukuk veya kamu hukuku tüzel kişisi ayrımı yapılmadığı görülmektedir. Dolayısıyla kamu hukuku tüzel kişileri de veri sorumlusu olabileceği net olarak ifade edilebilir.

Kişisel Verilerin Korunması Kanunu m. 18'de yapılan düzenlemede görüleceği üzere idari para cezalarının gerçek veya özel hukuk tüzel kişilerine yönelik uygulanabilmesinden bahsedilmektedir. Ancak KVKK m. 18/3'te de bulunan düzenlemede kamu hukuku tüzel kişiliklerine idari para cezalarının uygulanmayacağı anlaşılmaktadır. Dolayısıyla söz konusu KVKK bakımından işlenen kabahatlerin kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarında işlenmesi durumunda buralarda görev yapanlar hakkında disiplin hükümlerine göre işlem tesis edilip sonucun kurula bildirilmesi gerekmektedir.

[469] Akbulut, a. g. e., s. 354.
[470] Kangal, a. g. e., s. 105; Hakeri, a. g. e., s. 153.

5.2.4. Mağdur

Kabahat konusunun ilişkin olduğu kişiler mağdur olarak ifade edilirler[471]. Kabahat teşkil eden eylemlerin devletler tarafından yasaklanmasının sebebi toplumun düzeninin veya belirli bir alandaki sistemin korunması amaçlandığı için, söz konusu kabahatlerin mağduru yoktur. Ancak bu anlamda işlenen bazı kabahatlerin mağduru söz konusu olabilir[472]. Bu bakımdan yalnızca gerçek kişi mağdur olarak ifade edilebilir[473]. Dolayısıyla tüzel kişiler mağdur olamazlar[474].

Kişisel Verilerin Korunması Kanunu kapsamında aydınlatma yükümlülüğü yerine getirilmediği durumda, kabahatin mağduru, verileri işlenen söz konusu kişilerdir. Bu bağlamda kimlerin veri sahibi olabileceği açıkça ifade edilmelidir. KVKK m. 10'da yapılan düzenlemede veri sorumlusu olan kişinin, veri sahiplerine karşı aydınlatma yükümlülüğünün yerine getirilmesi gerekmektedir. Aynı düzenlemede ilgili kişinin verisi işlenen gerçek kişi olarak ifade edildiğini görmekteyiz (KVKK m. 3/1-ç). Düzenlemelerde görüleceği üzere kaide olarak gerçek kişiler yalnızca veri sahibi olabilir. Zira KVKK'da kişisel verinin tanımı, "*kimliği belirli veya belirlenebilir kişiye ait her türlü bilgi"* olarak düzenlenmiştir. KVKK m. 2'de düzenlemenin yalnızca kişisel verileri işlenen gerçek kişiler bakımından uygulanacağı açıkça belirtilmiştir. Bir diğer önemli düzenleme Avrupa Birliği Genel Veri Koruma Tüzüğü'nde kişisel verinin tanımı, tanımlanabilir veya tanımlanmış gerçek kişiye ilişkin her türlü bilgi olarak tanımlandığını görmekteyiz (KVKK m. 4/1).

Yapılan düzenlemelerin tamamında, kişisel verilerin korunması hakkının, kaynağını esas olarak temel hak ve özgürlüklerden aldığını net olarak ifade edebiliriz. Bu temel hakların belki de en önemlisi özel hayatın gizliliği hakkı olarak ifade edilebilir. Özel hayatın gizliliği ile ilgili olarak, muhteviyat düşünüldüğünde, gerçek kişilere ait temel hak ve özgürlüklerin görüldüğü dolayısıyla verileri korunan kişilerin gerçek kişiler olduğu söylenebilir[475]. Uluslararası yasal düzenlemelerde gerçek kişilerin verilerinin korunmasına dair tedbirlerin alındığını görmekteyiz. Ancak gerek ulusal gerekse de uluslararası düzenlemelerde tüzel

[471] Akbulut, a. g. e., s. 333; İçel, a. g. e., s. 395; Artuk, Gökcen, Alşahin, Çakır, a. g. e., s. 374.
[472] Akbulut, a. g. e., s. 333; Kayıhan, a. g. e., s. 396.
[473] Artuk, Gökcen, Alşahin, Çakır, a. g. e., s. 374.
[474] Akbulut, a. g. e., s. 333; İçel, a. g. e., s. 396; Artuk, Gökcen, Alşahin, Çakır, a. g. e., s. 374.
[475] Handbook on European Data Protection Law, 2018, s. 84-85.

kişilere ait verilerin korunmaması gerektiği ile ilgili bir ifadenin bulunmadığı söylenebilir[476]. Zira, tüzel kişilere ait verilerin korunması ile ilgili görüş birliğinin bulunmadığı açıkça ifade edilebilir[477]. Bu bağlamda görüş birliği her ne kadar bulunmasa da yapılan bazı düzenlemelerde tüzel kişilerin de verilerine ilişkin menfaatlerin korunması gerektiği ifade edilmiştir[478].

5.2.5. Manevi Unsurlar

Kural olarak kabahat taksirle ve kasten işlenebilir[479]. Ancak yasal düzenlemelerde sadece kasten işlenebileceği ifade edilen kabahatler, söz konusu kişinin taksirle işlemesi durumunda sorumluluğu bulunmayacaktır[480].

Hem taksir hem de kast TCK'de tanımlanmaktadır. Bu tanımlamaya göre taksir "*dikkat ve özen yükümlülüğüne aykırılık dolayısıyla, bir davranışın suçun kanuni tanımında belirtilen neticesi öngörülmeyerek gerçekleştirilmesi*" şeklinde tanımlanmaktadır. Kast ise "*suçun kanuni tanımındaki unsurların bilerek ve isteyerek gerçekleştirilmesi"* olarak tanımlanmaktadır.

Aydınlatma yükümlülüğünün yerine getirilmemesi kabahati kasten ve taksirle işlenebilmektedir. Çünkü KVKK incelendiğinde aydınlatma yükümlülüğünün kasten işlenmesi gerektiği ile ilgili bir ibarenin bulunmadığı görülecektir. Veri sorumlusu veya yetkilendirilen kişinin dikkat ve özen yükümlülüğüne aykırı davranması halinde taksirli sorumluluğu söz konusu olacaktır.

Kabahatler Kanunu'na göre, TCK içerisinde düzenlenen hataya ilişkin hükümler, sadece kasten işlenebilen kabahatler bakımından uygulanabilmektedir[481]**.** TCK'da yapılan düzenlemeye göre ''*Fiilin icrası sırasında suçun kanuni tanımındaki maddi unsurları bilmeyen bir kimse, kasten hareket etmiş olmaz. Bu hata dolayısıyla taksirli sorumluluk hali saklıdır.*'' (m. 30/1). Zira anlaşılacağı üzere failin taksirli sorumluluğu devam etmektedir.

[476] Ayözger, a. g. e., s. 18.
[477] Kuşkonmaz, a. g. e., s. 9.
[478] Handbook on European Data Protection Law, 2018, s. 84-85;
[479] Bekar, a. g. e., s. 1044.
[480] Kangal, a. g. e., s.105; Hakeri, a. g. e., s. 168.
[481] Bekar, a. g. e., s. 1046.

5.2.6. Hukuka Aykırılık Unsuru

Kabahatler Kanunu'nda yapılan düzenlemeye göre, "*Kanunda aksine hüküm bulunmayan hallerde, Türk Ceza Kanunu'nun hukuka uygunluk nedenleri ile kusurluluğu ortadan kaldıran nedenlere ilişkin hükümleri kabahatler bakımından da uygulanır.***"** (m. 12) denilmektedir.

Türk Ceza Kanunu'nda yapılan düzenlemede hukuka uygunluk nedenlerine baktığımızda; yasa gereğinin ve amirin hukuk kaidelerine uygun talebinin yerine getirilmesi (m. 24), meşru savunma (m. 25), ilgilinin rızası ve hakkın kullanılmasıdır (m. 26). Bu bağlamda hukuka uygunluk nedenleri niteliklerine uygun olduğu oranda kabahatler açısından da uygulanabilmektedir. Hukuka aykırılık kavramı için yapacağımız tanım, tipik bir eylemin hukuk düzeniyle çelişmesi olarak ifade edilebilir[482]. Dolayısıyla ortaya konulan bir fiilde yasal anlamda uygunluk sebebinin bulunması halinde, tipe uygun olan fiil hukuka aykırılık oluşturmayacaktır[483].

Yukarıda saymış olduğumuz hukuka uygunluk nedenlerinden birinin varlığı durumunda, veri sorumlularının veya temsilcilerinin aydınlatma yükümlülüklerini yerine getirmemeleri biçimindeki eylemleri, kanundaki tipikliğe uygun olsa da hukuk kaidelerine uygun olduğu kabul edilerek bahse konu eylemlerinden dolayı veri sorumlusu veya temsilcisine idari para cezası uygulanamayacaktır. Dolayısıyla aydınlatma yükümlülüğünün yerine getirilmediği durumlarda öncelikli olarak bakılması gereken hukuka uygunluk nedenlerinin bulunup bulunmadığı mutlaka tespit edilmelidir. Zira bu yönde bir tespit yapılmaması hak kayıplarının yaşanmasına yol açacaktır.

Kişisel Verilerin Korunması Kanunu kapsamında, hukuka uygunluk nedenlerinin düzenlenmediği görülmektedir. Zira, aydınlatma yükümlülüğünün düzenlendiği KVKK m.

[482] Hakeri, a. g. e., s. 301; Artuk, Gökcen, Alşahin, Çakır, a. g. e., s. 377.
[483] İçel, Akıncı, Özgenç, Sözüer, Mahmutoğlu, Ünver, a. g. e., s. 268; Hakeri, a. g. e., s. 297; Artuk, Gökcen, Alşahin, Çakır, a. g. e., s. 483.

10'da ve aydınlatma yükümlülüğünün yerine getirilmemesi kabahatinin düzenlendiği KVKK m. 18'de bulunmadığını net olarak ifade edebiliriz.

Veri sorumluları veya yetkilendirdiği kişi bakımından aydınlatma yükümlülüğünün yerine getirilmesi açısından istenilen, ilgili kişilerin veri işleme faaliyetleri hakkında bilgilendirmesi ve kişinin verilerinin işlenmesine yönelik olarak sağlıklı bir şekilde rızalarının alınmasıdır. Zira yapılan bu açıklamalardan anlaşılacağı üzere, aydınlatma yükümlülüğünün, hukuk kaidelerine uygun veri işleme faaliyetinin açıkça rıza şartının arandığı durumlarda zorunlu olarak ifa edilmesi gerektiği, buna mukabil ilgili kişilerin verilerine dair rıza alınmadan da hukuk kaidelerine uygun olarak işlenebileceği diğer durumlarda, ilgili yükümlülüğün yerine getirilmesinin gerekmediği sonucu çıkarılabilir. Ancak, Aydınlatma Tebliğ'inde yapılan düzenleme gereğince "*İlgili kişinin açık rızasına veya Kanundaki diğer işleme şartlarına bağlı olarak kişisel veri işlendiği her durumda aydınlatma yükümlülüğü yerine getirilmelidir*." (Aydınlatma Tebliği m. 5/1-a). "Kişisel Verileri Koruma Kurumu" tarafından hazırlanıp toplumun istifadesine sunulan Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi'nde[484] de aydınlatma yükümlülüğünün ister açık rıza ister mevzuata uygun işleme şartlarından bağımsız olarak yerine getirilmesi gereken yükümlülük olduğu ifade edilmektedir. Dolayısıyla yapılan düzenlemeler bakımından bir değerlendirme yaptığımızda, aydınlatma yükümlülüğünün her koşulda yerine getirilmesi gerektiği söylenebilir. Aydınlatma yükümlülüğünün kural olarak bütün durumlarda yerine getirilmesinin söz konusu olması, ilgili yükümlülüğün öngörülme sebebi ile örtüşmektedir. İlgili kişilerin veri işleme faaliyetleri bakımından aydınlatılmaları, yaşanan süreçte sahip olduğu hakları kullanabilmeleri ve verileri üzerinde denetim yapabilmeleri yönünden oldukça önemlidir.

Bahse konu düzenlemeler bakımından değerlendirme yapılacak olursa, aydınlatma yükümlülüğünün prensip olarak her koşulda ifa edilmesi gerektiği biçiminde özel hükümler bulunduğundan TCK'da düzenlenen hukuka uygunluk sebepleri ilgili kabahat bakımından uygulanması mümkün olmayacaktır.

[484] Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi, s.12.

İlgili konu bakımından, ‘‘*İstisnalar*’’ başlıklı KVKK m. 28’in irdelenmesi gerekmektedir. KVKK m. 28/1’de, KVKK hükümlerinin uygulanmayacağı durumların düzenlendiğini görmekteyiz. KVKK m.28/1 kapsamında veri işleme faaliyeti esnasında kişinin verilerinin korunmasına ilişkin hüküm uygulanmayacaktır. KVKK m. 28/2 kişisel veriler ile ilgili aydınlatma yükümlülüğünün ifa edilmesi ile ilgili KVKK m. 10, veri sahibinin haklarını düzenleyen KVKK m. 11 ve Veri Sorumluları Sicili’ne kayıt yükümlülüğüne ilişkin olarak m. 16’nın uygulanmaması gereken durumlar düzenlenmektedir. Dolayısıyla “*kişisel veri işlemenin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması’’*[485] (m. 28/2-a), “*ilgili kişinin kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi*”[486] (m. 28/2-b), “*kişisel veri işlemenin kanunun 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*” (m. 28/2-c), “*kişisel veri işlemenin bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olması*” (m. 28/2-d) durumunda yapılan veri işleme faaliyeti açısından veri sorumlusu veya temsilcisinin, ilgili kişiyi aydınlatma yükümlülüğü, en baştan itibaren bulunmadığından, bu bağlamda açıkladığımız düzenlemenin kabahat bakımından, hukuka uygunluk nedeni olmadığı ifade edilebilir.

5.2.7. Suçun Unsurları Bakımından Kusurluluk

Kusur, failin fiili sonucu işlenen ve haksızlık oluşturan failin fiili nedeniyle kınanabilmesini, mesul tutulabilmesini ifade etmektedir[487]. Kabahatler Kanunu m. 12’deki düzenlemeye göre aksine hüküm bulunmayan durumlarda TCK’nin kusurluluğu ortadan kaldıran sebepler ve hukuka uygunluk sebeplerine ilişkin hükümleri kabahatler açısından da uygulanmaktadır.

Akıl sağlığı bakımından gerçekleştirdiği eylemin hukuki anlam ve sonucunu kavrayamayan veya söz konusu eylem ile ilgili davranışlarını yönlendirme kabiliyeti önemli ölçüde azalmış kişiler hakkında idari para cezası uygulanmayacağı ilgili düzenlemede ifade edilmektedir (KK m. 11/2) Bununla birlikte yine Kabahatler Kanunu m. 11’de fiilin işlendiği esnada on

[485] Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi, s. 13.
[486] KVKK, m. 5 gerekçesi.
[487] Artuk, Gökcen, Alşahin, Çakır, a. g. e., s. 569.

beş yaşını doldurmamış olması çocuk hakkında idari para cezası uygulanamayacağı ifade edilmiştir.

Kabahatin oluşabilmesi için failin kusurlu olması aranmamaktadır. Zira, kusur haksızlığın bir unsuru değildir[488]. Ancak idari para cezalarının uygulanabilmesi için kusur zorunlu olarak aranmaktadır. Bunun haricinde idari tedbirler açısından kusurun herhangi bir etkisi bulunmamaktadır[489]. Tüzel kişiler için idari yaptırımların uygulanabilmesi için mutlak surette failin kusurlu olması aranmaktadır[490]. Bahse konu bu yaklaşımlar ilgili konu bağlamında aydınlatma yükümlülüğünün yerine getirilmemesi kabahati açısından uygulanması mümkün olacaktır.

5.2.8. Suçun Özel Görünüş Biçimleri

5.2.8.1. Teşebbüs

Kabahatler Kanunu m. 13'te yapılan düzenleme gereği kabahatlere ilişkin teşebbüsün varlığı kural olarak cezalandırılamaz. Ancak ilgili kanuni düzenlemelerde kabahate teşebbüsün cezalandırılması ile ilgili düzenlemeler yapılabilir. Dolayısıyla TCK' nın suça teşebbüse ve gönüllü vazgeçmeye ilişkin hükümleri uygulanabilecektir.

Teşebbüs ile ilgili TCK m. 35'deki düzenlemeye göre kişinin işlemeyi kastettiği suçu doğrudan veya uygun hareketlerle işlemeye başlayıp, elinde olmayan nedenlerle tamamlayamazsa bile teşebbüs yüzünden cezalandırılması gerekmektedir.

Yasal düzenlemelerde ifade edilen teşebbüs hükümlerinden kaynaklı olarak, tipiklikte öngörülen netice gerçekleşmemiş olsa bile failin, gerçekleştirdiği eylem sonucunda hukuki yararları ihlal etmesi nedeniyle yaptırım söz konusu olacaktır[491].

Kural olarak, kabahatlere ilişkin teşebbüs kabul edilmemektedir. Zira KVKK aydınlatma yükümlülüğünün yerine getirilmemesi ile ilgili düzenlemelerde de özel bir hüküm bulunmadığından dolayı kabahate teşebbüs cezalandırılması söz konusu olmayacaktır.

---

[488] Hakeri, a. g. e., s. 378. Artuk, Gökcen, Alşahin, Çakır, a. g. e., s. 483.
[489] Akbulut, a. g. e., s. 384.
[490] A. g. e., s. 385.
[491] Adem Sözüer, Suça Teşebbüs, İstanbul, Kazancı, 1994, s. 45;

5.2.8.2. İştirak

Kabahatler hukuku açısından tek tip fail yaklaşımının kabul edildiği bilinmektedir[492]. Çünkü, kabahatler hukukunda yapılan düzenlemelerde ceza hukukundaki gibi iştirak statülerinin yer almadığı görülmektedir. Dolayısıyla kabahate iştirak eden her bir kişi fail olarak sorumlu tutulmaktadır[493].

Kabahate iştirak eden ve fakat özel fail olmanın niteliklerinin arandığı şartları bulundurmayan kişiler hakkında da fail olarak idari para cezası uygulanabilir[494]. Dolayısıyla özel faillik niteliklerini kimlerin taşıdığı, failin tespit edilmesi ve idari yaptırımın uygulanabilmesi açısından önemli olmadığı söylenebilir[495].

Özel fail olma niteliklerini bulunduran kişi bakımından suç olarak ifade edilen eylem, özel fail olma niteliklerini bulundurmayan diğer kişiler açısından kabahat olarak ifade edilmiş ve söz konusu bu eylem her iki kişi tarafından birlikte işlenmiş ise bu bağlamda, suça ilişkin iştirak hükümlerinin uygulanması gerekmektedir (KK m. 14/4). Kanun koyucu yaptığı yasal düzenlemelerde, suça ilişkin düzenlemelerin kabahate göre asli norm olması nedeniyle, asli normların uygulanması önceliklendirilmiştir[496].

Kabahat işleyen bir kişide özel faillik niteliklerinin arandığı durumda, kabahat eylemini gerçekleştiren özel niteliklere sahip failin, bu özel niteliklere sahip olmayan kişinin araç olarak kullanılması sonucu işlendiğinde, dolaylı fail olarak Kabahatler Kanunu m. 14/2 kapsamında ceza uygulanması gerektiği ifade edilmektedir[497].

Kabahate ilişkin iştirakin söz konusu olabilmesi için iştirakin kasten işlenmesi gerekmektedir. Çünkü Kabahatler Kanunu m. 14 gereğince kabahate iştirak söz konusu olabilmesi için gerçekleştirilen fiilin kasten ve hukuka aykırı olarak gerçekleştirilmiş olması

[492]Bekar, a. g. e., s. 1047;
[493] Devrim Aydın, Türk Ceza Hukukunda Suça İştirak, Ankara, Yetkin, 2009, s. 287.
[494] Bekar, a. g. e., s. 1048; Aydın, a. g. e., s. 287.
[495] Otacı, Keskin, a. g. e., s. 56.
[496] Akbulut, a. g. e., s.633.
[497] Kangal, a. g. e., s.105; Hakeri, a. g. e., s.228.

yeterli olacaktır[498]. Burada özellikle vurgulanması gereken hem iştirakin hem de iştirak edilen eylemin kasten işlenmesi kural olarak zorunludur[499]. Kabahat olarak ifade edilen fiilin bir haksızlığa sebep olmuş olması gerekmektedir. Kabahate iştirak edenlerden bazılarının kusurunun bulunmaması diğer iştirak eden kişilere yaptırım uygulanmayacağı anlamı taşımamaktadır[500]. Ancak burada kabahate iştirak eden kişilerin tamamının cezalandırılabilmesi için objektif cezalandırılma koşullarının sağlanmış olması gerekmektedir[501]. Dolayısıyla cezayı ortadan kaldıran şahsi nedenin kendisinde bulunduğu şerik, bu fiillerden dolayı sorumlu tutulacak ancak diğer şeriklerin sorumluluğu elbette bu durumdan etkilenmeyecektir[502].KVKK'da düzenlenen aydınlatma yükümlülüğünün yerine getirilmemesi kabahati, veri sorumlusu tarafından işlenebilir. Dolayısıyla bu haliyle özgü bir kabahat olduğu tartışmasızdır. Kabahate iştirak eden faillerin idari para cezası açısından sorumluluğu, diğer sorumlulardan bağımsız olarak değerlendirilmektedir (KK m. 14/3).

5.2.8.3. İçtima

Kişisel verisi işlenen kişi açısından aydınlatma yükümlülüğünün yerine getirilmemesi kabahati, kesintisiz bir eylem ile gerçekleştirilebilecek bir kabahattir. Kesintisiz kabahatin sürekli olduğu durumda eylem kesintisiz sürdürülmekte, herhangi bir kesinti söz konusu olmadığından kabahat kesinti olmadan işlenmeye devam edecektir[503].

Verisi işlenen kişinin bilgilendirmesinin amaçlandığı, aydınlatma yükümlülüğü ile ilgili olarak veri sorumlusu ya da yetkilendirdiği kişiler açısından belirli bir icrai tutumda bulunması gerekmektedir. Söz konusu yükümlülüğün ifa edilmemesi biçimindeki ihmali davranışın devam ettiği süre boyunca, kabahat işlenmeye devam etmektedir[504].

Veri sorumlusu tarafından aydınlatma yükümlülüğünün yerine getirilmemesi sebebiyle idari para cezasına hükmedilen ve uygulanan bu ceza sonrasından aydınlatma yükümlülüğü aynı şekilde ifa edilmezse idari para cezasının tatbik edilmesinden sonra ayrıca bir kabahatin

[498] Otacı, Keskin, a. g. e., s.56.
[499] Akbulut, a. g. e., s.627.
[500] Kangal, a. g. e., s.105; Hakeri, a. g. e., s.226.
[501] Akbulut, a. g. e., s.631.
[502] A. g. e., 632.
[503] Otacı, Keskin, a. g. e., s. 58.
[504] Kangal, a. g. e., s. 105; Hakeri, a. g. e., s. 238.

işlendiği kabul edilip, işlenen bu kabahat için farklı bir idari para cezası söz konusu olacaktır[505]. Çünkü Kabahatler Kanunu m. 15/2'de yapılan düzenlemeye göre kesintisiz bir eylemle gerçekleştirilebilen kabahatlerde, idari para cezası uygulanmasına ilişkin ceza kesinleşinceye kadar geçen süre içerisinde gerçekleştirilen fiiller tek bir kabahat olarak ifade edilir. Bu nedenle idari para cezasının söz konusu olduğu andan itibaren aydınlatma yükümlülüğünün yerine getirilmemesi kabahatinin yasal olarak kesintiye uğradığı varsayılmaktadır[506]. Kabahat niteliğini taşıyan bir eylem, sadece kanuni yükümlülüğün yerine getirilmemesinden kaynaklanıyorsa ve bunun sonucunda idari yaptırım uygulanacak ise, bu kabahatin işlenmesinden etkilenen herkes açısından idari yaptırım uygulanması söz konusu olmamakta, yalnızca bir yaptırım uygulanmaktadır[507]. Yasal zorunluluk yerine getirilmeden bir işlemin tesis edilmesi ve bunun neticesinde bir idari yaptırımın söz konusu olması durumunda, fiilden etkilenen kişiler adedince kabahatin oluştuğunu ve her biri açısından ayrı ayrı idari yaptırımın uygulanması gerektiğini ifade edebiliriz[508]. Çünkü burada bahsedilen durumda kesintisiz bir kabahat olmadığından işlenen her bir eylem ayrı kabahat olarak dikkate alınacaktır[509].

Aydınlatma yükümlülüğü kişisel verilerin korunması bağlamında verisi işlenen kişiye karşı ifa edilir. Aydınlatma yükümlülüğünün ifa edilmemesi durumunda, yükümlülüğün yerine getirilmeden verilerinin işlenmesi sonucunda başka işlemlerin yapılması söz konusu olacaktır. Konuyu somutlaştırmak adına yukarıda bahsetmiş olduğumuz örneği farklı bir biçimde ele alacak olursak; Üniversite sınavını kazanan öğrencinin kazandığı üniversiteye kaydını gerçekleştirmesi ve bunun sonucunda üniversiteye giriş kartı talep etmesi durumunu inceleyelim. Öğrenci tarafından talep edilen üniversite giriş kartlarının başka bir kurum tarafından üretildiğini ve dolayısıyla öğrencilerin kişisel verilerinin paylaşıldığını bilmekteyiz. Üniversite giriş kartına ilişkin olarak verileri paylaşılacak olan kişilerin aydınlatılmadan ve kişisel verilerin işlenmesi anlamından açık rızası alınmadan ilgili öğrencilerin verilerinin aktarılması ve bu esnada verilerinin işlenmesi durumunda, aydınlatma yükümlülüğünün yerine getirilmeden işlemler yapıldığı görülmektedir. Vermiş olduğumuz örnekte, aydınlatma yükümlülüğünün ifa edilmemesi kabahatinin her bir öğrenci

[505] Özgenç, a. g. e., s. 654.
[506] Otacı, Keskin, a. g. e., s. 58.
[507] Özgenç, a. g. e., s. 655; Kangal, a. g. e., s. 105; Hakeri, a. g. e., s. 238.
[508] Özgenç, a. g. e., s. 656; Kangal, a. g. e., s. 105; Hakeri, a. g. e., s. 238.
[509] Özgenç, a. g. e., s. 656.

bakımından oluştuğu ve dolayısıyla bahse konu fiillerin sayısı adedince idari para cezasının mı yoksa bahse konu fiiller bakımından tek bir kabahatin oluştuğu kabul edilerek idari para cezasının mı uygulanması gerektiğinin tespit edilmesi konumuz açısından önemli olduğunu ifade edebiliriz. Bu kapsamda bir diğer örneğimiz, ünlü bir alışveriş sitesinde ilgili kişilerin verilerinin toplanıp akabinde işlendiği ancak buna ilişkin aydınlatma yükümlülüğünün yerine getirilmediği örnek olayımızda da ilgili siteyi kullanan ve verileri işlenen kişilerin yapmış oldukları işlemler bakımından, aydınlatma yükümlülüğünün yerine getirilmemesi kabahatinin birden fazla defa işlendiği mi yoksa tek bir kabahatin mi işlendiği konusunun tespiti önemlidir.

Zira verdiğimiz her iki örnekte de her bir işlem bakımından söz konusu kabahatin işlendiği ve bunun sonucunda idari para cezasının ayrı ayrı uygulanması gerektiğini kabul ettiğimizde, söz konusu fiil sayısını tespit etmek oldukça zor olabilmekte veya tespit edilen toplam idari para cezaları çok yüksek olabilmektedir. Dolayısıyla veri sorumlusu veya temsilcileri bakımından yerine getirilmesi gereken aydınlatma yükümlülüğü, yalnızca kanuni sorumluluğunun yerine getirilmesi olarak kabul edilebilir. Bu durumda söz konusu yükümlülüğün sağlanmamış olması açısından tek bir kabahatin işlendiği ve buna göre bir cezanın uygulanması gerektiği ifade edilebilir. Söz konusu fiil hem suç hem de kabahat olarak tanımlanmışsa yalnızca suçtan dolayı yaptırım uygulanabileceğini söyleyebiliriz. Fakat suç nedeniyle yaptırım uygulanamayan durumlarda kabahat için öngörülen yaptırım uygulanacaktır (KK m. 15/3). Yasal düzenlemelerde görüleceği üzere, kabahatlerin suçlardan niteliksel değil niceliksel yönden ayrıldığı kabul edildiğinden yalnızca bir fiille hem kabahat hem de suç işlendiğinde, bu durumda ayrı ayrı yaptırım uygulanmasının kabul edilmediği ifade edilmiştir[510].

Veri sorumlusu tarafından aydınlatma yükümlülüğünün ifa edilmemesi durumunda yalnızca kabahatin işlenmesi durumunda aynı fiil sonucu oluşan başka bir suç bulunmamaktadır. Zira yukarıda açıkladığımız hüküm aydınlatma yükümlülüğünün ifa edilmemesi bakımından uygulanamayacaktır.

[510] Akbulut, a. g. e., s. 651.

Kişisel Verilerin Korunması Kanunu'nda yapılan düzenleme gereği aydınlatma yükümlülüğü ifa edilmeden kişilerin verilerinin işlenmesi durumunda bu veri işleme faaliyetinin mevzuata aykırı olduğu kabul edilmektedir. Aydınlatma yükümlülüğü ifa edilmeden veri işlemenin yapılması durumunda, kişisel verilerin mevzuata aykırı olarak kaydedilmesi söz konusu ise bu durumda TCK'da düzenlenen "*kişisel verilerin kaydedilmesi*'' (m. 135) suçu karşımıza çıkacaktır. Bunun dışında kişisel verileri kişinin kendisinden değil de başkası üzerinden elde edilmesi durumunda veri sahibine karşı aydınlatma yükümlülüğünün yerine getirilmediği durumda *"verileri hukuka aykırı olarak verme veya ele geçirme"* (m. 136) suçu karşımıza çıkmaktadır. Zira burada, veri sorumlusu bakımından *"verileri hukuka aykırı olarak ele geçirme suçu''* işlenmiş olması söz konusu olacaktır. Veri sorumlusunun, veri sahibini aydınlatmadan kişisel verileri kaydetmesi durumunda bu veri işleme faaliyeti açıkça mevzuata aykırı olacaktır. Aynı zamanda veri sorumlusu açısından Türk Ceza Kanunu m. 135'te düzenlenen verilerin hukuka aykırı olarak kaydedilmesi suçunun işlemesi söz konusu olacaktır. Ancak burada dikkat edilmesi gereken önemli bir durumu belirtmekte fayda olacağını düşünmekteyiz. Veri sorumlusunun, aydınlatma yükümlülüğünü yerine getirmemesi iki durumda söz konusu olabilir. Birinci fiil ihmali hareketle ikinci fiil icrai hareketle söz konusu olabilmektedir. Bu durumda tek bir fiille hem suçun işlenmesini hem de kabahatin işlenmesi kabul edilmesi mümkün olmadığından, Kabahatler Kanunu m. 15/3'te yapılan düzenlemenin uygulanması söz konusu olmayacaktır. Bu durumda veri sorumlusu, aydınlatma yükümlülüğünü yerine getirmediğinden kaynaklı olarak kabahatten, aynı zamanda kişisel verileri hukuka aykırı olarak kaydetmesi nedeniyle de cezalandırılacaktır. İlgili kişiden elde edilmeyen kişisel veriler hakkında da veri sahibinin aydınlatılması gerekmektedir (Aydınlatma Tebliği m. 6). Veri sorumlusu, başkasından elde ettiği kişisel veriler bakımından aydınlatma yükümlülüğünü düzenlemede belirtilen süreler içerisinde ilgili kişiyi mutlaka bilgilendirmek zorundadır. Aksi durumda kişisel verilerin mevzuata aykırı olarak ele geçirilip işlendiği kabul edilecektir. Bu durumun sonucunda da TCK m. 136'da düzenlenen "*verileri hukuka aykırı olarak verme veya ele geçirme suçu"* işlenmiş olacaktır. Sonuç olarak veri sorumlusu, aydınlatma yükümlülüğünün yerine getirmediğinden dolayı kabahatten, söz konusu yükümlülüğü sağlamayarak kişinin verilerini elde etmesinden dolayı da "*verileri hukuka aykırı olarak verme veya ele geçirme*" suçlarından ayrı ayrı yaptırım uygulanması söz konusu olacaktır. Görüldüğü üzere veri sorumlusunun iki ayrı fiili bulunmaktadır.

5.2.9. Kişisel Verilerin Korunmasında Denetim Ve Yaptırım Yöntemleri

5.2.9.1. Veri sorumlusuna başvuru yoluyla koruma

Kişisel verileri ihlal edilen kişilerin veri sorumlusuna başvuru ile ilgili yapılan düzenlemeler incelendiğinde; Veri Koruma Tüzüğü nün ilgili maddelerinde bulunan düzenlemelerde, bunun dışında 10/03/2018 tarih ve 30356 sayılı Resmî Gazete'de yayımlanan Veri Sorumlusuna Başvuru Usul ve Esaslar Hakkında Tebliğ'inde düzenlendiği görülmektedir. Bu düzenlemelere göre, kişisel verileri ile ilgili taleplerini yazılı bir biçimde ya da KVKK'da belirtilen yöntemlerle veri sorumlusuna iletmesi gerekmektedir. Veri sorumlusu bu talebe ilişkin olarak en geç otuz gün içerisinde yapacağı inceleme ile iki sonuca varmak zorundadır. İlk olarak talebi kabul edip kararın gereğini yerine getirebilir veya talebi reddedebilir. Veri sorumlusunun inceleme sonucunda vermiş olduğu kararını, talepte bulunan kişiye yazılı veya elektronik ortamda ulaştırabilir. Bahsetmiş olduğumuz düzenlemelerin Veri Koruma Tüzüğü'yle de uyumlu olduğunu ifade edebiliriz. Veri Koruma Tüzüğü m. 12'de veri sorumlusunun, kişisel veri sahibinin haklarını kullanabilmek için veri sorumlusundan talepte bulunması durumunda, talebe ilişkin cevabın en geç bir ay içerisinde veri sorumlusu tarafından talepte bulunan kişiye iletilmesi gerektiği ifade edilmektedir[511]. İlgili kişinin talebinin kompleks olması durumunda bir aylık sürenin iki ay daha uzatılabileceği de bilinmektedir. Kişilerin veri sorumlusuna başvururken izleyecekleri yöntem, Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'i m. 5'te düzenlenmiştir. Bu düzenlemeye gereğince; veri sahibi olan kişi KVKK kapsamında ki taleplerini, yazılı olarak, güvenli elektronik imza, mobil imza veya veri sorumlusunun veri tabanında kayıtlı bulunan elektronik posta adresine yollamak suretiyle veri sorumluna iletebilmektedir. İlgili kişinin taleplerine ilişkin olarak yapmış olduğu işlemler Veri Koruma Tüzüğü'ne göre ücretsiz yapılmaktadır. Ancak ilgili kişi tarafından yapılan başvuruların asılsız, ölçüsüz veya tekrarlanan talepler olması durumunda uygun bir ücretin talep edilmesi mümkün olabilecektir[512]. Veri sorumlusuna başvuru ile ilgili olarak bir düğer düzenleme de ise Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'i m. 7'de, başvuran kişiye yazılı cevap verilmesi durumunda, on sayfaya kadar ücret alınmaması, on sayfadan fazla olan durumlarda ise sayfa başına bir Türk Lirası işlem bedeli alınacağı biçiminde düzenleme

[511] Develioğlu, a. g. e., s. 119.
[512] Develioğlu, a. g. e., s. 119.

bulunmaktadır. Ayrıca aynı düzenlemede talepte bulunan kişiye verilen cevabın, harici bellek veya benzeri araçlarla verilmesi halinde alınacak ücretin kayıt maliyetini geçmemesi gerektiği ifade edilmiştir.

Veri sahibi olan birey, kendisine ait olan verilerin hangi koşullarda işlenebileceği veya aktarılabileceği konularında, veri sorumlusunun ya da temsilcisinin kendisini aydınlatmasını isteyebilir. Zira, aydınlatma veri sorumlusu veya temsilcisinin doğal yükümlülüğü olup söz konusu kişinin ayrıca talepte bulunulmasına gerek yoktur (Aydınlatma Tebliği m. 5/1-d). Ancak aydınlatma yükümlülüğünün yerine getirilmediği durumlarda veya aydınlatmanın ilgili kişi bakımından yetersiz ve anlaşılmadığında ilgili kişi, veri sorumlusundan başvuruda bulunmak suretiyle aydınlatma yükümlülüğünün gerektiği şekilde yerine getirilmesini talep edebilecektir. Bu talebin reddedilmesi, süresi içinde cevap verilmemesi veya eksik cevap verilmesi durumlarında ilgili kişi, cevabı öğrendiği tarih itibari ile otuz gün her halükârda başvuru tarihinden itibaren altmış gün içerisinde Kurul'a şikâyette bulunma hakkını kullanabilecektir.

5.2.9.2. İdari yaptırım yoluyla koruma

5.2.9.2.1. İdari yaptırım

Yasaların açıkça vermiş olduğu yetki gereğince idareler, bir yargısal karar olmaksızın doğrudan yaptığı işlemler ve idare hukukuna özgü yöntemlerle uygulamış olduğu yaptırımlara idari yaptırım denilmektedir[513]. Kabahatler Kanunu m. 2'de kabahatin tanımı; "*kanunun, karşılığında idarî yaptırım uygulanmasını öngördüğü haksızlık anlaşılır.*" biçiminde tanımlanmıştır. Dolayısıyla yapılan bu tanımlamaya baktığımızda kabahatin yaptırımı idari yaptırımlardır[514]. Yapılan tanımlamada kullanılan idari yaptırım kavramından anlamamız gereken ise, Kabahatler Kanunu m. 16'da düzenlendiğini görüyoruz. KK m. 16'da yapılan düzenleme gereğince, kabahat karşılığında uygulanacak olan idari yaptırımlar, idari para cezası ve idari tedbirlerden oluşmaktadır[515]. İdari yaptırımlar ile ceza yaptırımları arasında çeşitli farklılıklar bulunmaktadır. Bu farklılıkların başında yaptırımı uygulayan kurum, yaptırımın türü, kullanılan yöntem, miktarı ve sonuçları açısından farklılıkların

[513] İlhan Özay, İdari Yaptırımlar: Kuramsal Bir Deneme, İstanbul, İstanbul Üniversitesi, 1985, s. 35.
[514] Zeynel, Kangal, Kabahatler Hukuku, İstanbul, onikilevha, 2019, s. 259
[515] Ulusoy, Ali, İdari Yaptırımlar, İstanbul, 2013, s. 11,141

olduğunu ifade edebiliriz[516]. İdari yaptırımlar bahsettiğimiz üzere birbirinden farklıdır. Zira, idari yaptırımlar, ceza yaptırımlarından organik anlamda farklı olduğunu ifade edebiliriz. Ceza yaptırımları yalnızca kesinleşmiş yargı kararının sonucunda uygulanabiliyor iken[517] İdari yaptırımların uygulanması, yasalarla yetkili kılınmış idari kurumlarca yerine getirilen idari işlemlerdir[518]. İdari yaptırımlar hürriyeti bağlayıcı nitelikte olamazlar, zira idari yaptırımlar herhangi bir mahkeme kararı olmaksızın idari işlemler sonucu verilen cezalardır. Anayasa m.19'da görüleceği üzere kişi hürriyetin yalnızca mahkeme kararıyla kısıtlanabileceği açıkça ifade edilmiştir[519]. İdari yaptırımlar ile ceza yaptırımları arasında her ne kadar nicelik açısından farklılıklar olsa da niteliksel olarak benzer yönleri de bulunmaktadır. Bu benzerliğin en bariz durumu her ikisinin de caydırıcı özelliklere sahip olmasıdır[520]. Ancak idari yaptırımlarda cezalara oranlara kusur ve haksızlık içeriğinin suçlara oranla daha hafif olmasından dolayı idari yaptırımlar cezalar ile kıyaslandığında daha hafif olacağını söyleyebiliriz[521].

İdari yaptırımlar, kanunların yetkilendirdikleri idarelerin araya yargısal bir karar girmeden, doğrudan herhangi bir işlem ile ve idare hukukuna özgü usullerle vermiş olduğu yaptırımlardır[522]. Aydınlatma yükümlülüğünün yerine getirilmemesi fiili işlendiğinde kabahat söz konusu olacaktır ve bunun karşılığında uygulanacak temel yaptırım idari para cezası olacaktır[523]. İdari tedbirler tarafında ise, (KK m. 16) mevzuatta düzenlendiği üzere ilk akla gelen mülkiyetin kamuya geçirilmesi, bir meslek veya sanatın yerine getirilmemesi, işyerinin kapatılması, verilen ruhsat ve ehliyetin geri alınması, kara, deniz veya hava nakil araçlarının trafikten ya da seyrüseferden men edilmesi gibi yaptırımları sıralayabiliriz.

Kabahat karşılığı olan idari yaptırımların türü, süresi ve miktarı, genel düzenleyici işlemlerle belirlenmesi mümkün olmayıp kanun tarafından düzenlenmesi zorunludur (KK m. 4/2).

---

[516] Yücel Oğurlu, İdari Yaptırımlara Genel Bir Bakış ve İdari Yaptırım-Ceza Yaptırımı Ayrımı, AÜ Erzincan Hukuk Fakültesi Dergisi, C. III, S.1, s. 159.
[517] Burcu Erdinç, İdari Yaptırımların Kavramsal Çerçevesi ve Cezai Yaptırımlarla Karşılaştırılması, Ankara Barosu Dergisi, Y.2012, S.2, s. 249.
[518] Erdinç, a. g. e., s. 249.
[519] Yücel Oğurlu, İdari Yaptırımlar Karşısında Yargısal Korunma, Ankara, Seçkin, 2000, s. 162.
[520] Erdinç, a. g. e., s. 251.
[521] Zeynel, Kangal, Kabahatler Hukuku, İstanbul, onikilevha, 2019, s. 105; Hakeri, a. g. e., s. 261.
[522] Ulusoy, Ali, İdari Yaptırımlar, İstanbul, 2013, s. 9-10.
[523] Zeynel, Kangal, Kabahatler Hukuku, İstanbul, onikilevha, 2019, s. 261

5.2.9.2.2. İdari para cezası yaptırımı

Yasal düzenlemeler gereğince, kabahatler için öngörülen temel yaptırım türü idari para cezaları olduğunu bilmekteyiz. İdari para cezaları, kanunda açıkça öngörülen kabahatler gereğince açıkça yetki verilen idari mercilerin, bir yargı kararı olmadan, kanunun doğrudan idari merciler tarafından karar vermesine müsaade ettiği ve belirli bir miktar paranın alınmasına sebep olan idari yaptırım türü olduğunu söyleyebiliriz[524]. İdari para cezaları yargı makamları tarafından karara bağlanmış olsa da (KK m. 24, 43/A) adli para cezalarından farklı olduğunu ifade edebiliriz[525]. İdari para cezaları kabahat karşılığında idari merciiler tarafından yargısal bir usule bağlı kalınmadan karar verilirken, adli para cezaları suç karşılığında ceza mahkemelerince muhakeme usulü işletilerek karar verilmektedir[526]. Dolayısıyla adli para cezalarında sosyal etik açıdan bir kınama söz konusu iken, idari para cezalarında ise kişiye sorumluluklarını hatırlatması söz konusu olmaktadır[527]. Kabahatler Kanunu düzenlenmesinde idari para cezalarının üçe ayrıldığını görmekteyiz. Bu düzenlemeye göre, İdari para cezaları nispi ya da maktu olabileceği gibi, düzenlemede alt ve üst sınırlar gösterilmek şartıyla da belirlenmesi mümkündür[528] (KK m. 17/1-2). Nispi idari para cezaları, işlenen fiilin vermiş olduğu zarar veya fiil sonucu elde edilen yarara oranla belirlenen para cezalarıdır[529]. Maktu idari para cezaları ise, yasa koyucu tarafından düzenlemede açıkça miktarı belirtilen para cezalarıdır[530]. Nispi idari para cezası mevzuat düzenlemelerinde yer alan her suçun mahiyetine göre belirlenen sabit olmayan, miktarı belli bir oranda azalıp çoğalan para cezalarıdır[531]. 1984 tarihli Yargıtay İçtihadı Birleştirme Kararı'nda nispi para cezalarına ilişkin şu ölçütleri belirlemiştir: "*Nispi para cezaları ise, Mer'iyet Kanununun 20. maddesinde tarif edildiği gibi, miktarı muayyen bir nispet dairesinde ve hadiseye göre azalıp çoğalabilir mahiyette bulunan para cezalarıdır. Kanun, bazı hallerde, para cezasının miktarının önceden maktu bir biçimde tayini yoluna gitmemekte; bu miktarı, ya suç nedeniyle verilen zararla veya failin suçtan elde ettiği*

[524] Yücel Oğurlu, İdari Yaptırımlar Karşısında Yargısal Korunma, Ankara, Seçkin, 2000, s. 88.
[525] Zeynel, Kangal, Kabahatler Hukuku, İstanbul, onikilevha, 2019, s. 263.
[526] Can, Sibel, İdari Para cezası, TAAD 2017, yıl:7, sy:29, s. 417.
[527] Zeynel, Kangal, Kabahatler Hukuku, İstanbul, onikilevha, 2019, s. 263.
[528] Zeynel, Kangal, Kabahatler Hukuku, İstanbul, onikilevha, 2019, s. 266.
[529] Kangal, a. g. e., s. 267.
[530] Kangal, a. g. e., s.279.
[531] Ekinci, Mustafa, Anlatımlı-Gerekçeli Kabahatler Kanunu ile İdari Suç ve Cezaları, Ankara 2005. s. 75.

kazançla orantılı olarak tespit etmektedir. Kanun koyucu, bu tür para cezasını düzenlerken, bazı amaçları gözönünde tutmaktadır. Birincisi, TCK. nun 278. madde gerekçesinde de belirtildiği gibi, sadece asgari ve azami hadlerin tespiti halinde para cezasının yeterli şekilde yüksek olmama eksikliğini göstermesidir. 2. ise, paranın değerini kaybetmesi halinde etkili bir müeyyide olmamasıdır. Nispi para cezaları konusunda belirtilmelidir ki, asgari ve azami hadleri kanunda gösterilen cezalar için uygulanabilecek olan ferdileştirme kuralı, yani temel cezanın tayini, nispi para cezaları için uygulanamaz"[532].

Uygulanacak olan cezanın sabit olarak veya nispi olarak belirlendiği durumlarda idari para cezasına karar verecek makam kanunda düzenlenmiş olanı uygulamak zorundadır. Bu bakımdan cezanın bireyselleştirmesi mümkün değildir. Ancak kanuni düzenlemede cezanın alt ve üst sınırlarının belirli olması halinde; Kabahatler Kanunu m. 17/2 fıkrasında belirtilen kabahatin haksızlık içeriği, failin kusuru ve ekonomik durumuna ilişkin hususlar dikkate alınarak cezayı verecek olan makam tarafından cezanın bireyselleştirilmesi gerekmektedir[533]. Kabahatin haksızlık içeriğinden anlaşılması gereken, fiilin ihlal ettiği toplumsal yarar, fiilin işlenme biçimi, yeri, zamanı, tehlikenin boyutu gibi konuların anlaşılması gerekmektedir[534]. Hukuk kaidelerinin her ihlali hukuka aykırı ve haksız bir fiil niteliğindedir. Bu durumda gerek fiilin işleniş şekli ve gerekse fiilin yol açtığı neticeler ve olaya münhasır diğer şartlar sebebiyle toplum nezdinde algılanış şekli aynı ağırlık derecesinde değildir. Bu sebeple fiilin haksızlık seviyesinin az ya da çok olması yani haksızlık içeriği idari para cezası tespit edilirken dikkate alınması gerekmektedir[535]. İdari para cezasının alt ve üst sınırı üzerinde belirlenmesinde dikkate alınacak bir diğer unsur failin ekonomik durumudur. Faile verilecek idari para cezaları, ilgili kişinin ekonomik olarak çökmesine sebep olmamalıdır. Fail olan kişinin yaşam koşullarını ağır seviyede zorlaştıracak nitelikteki orantısız para cezaları amacını aşacaktır. Bu sebeple idari para cezasının tespitinde failin ekonomik durumunun mutlak surette dikkate alınması zorunluluğu getirilmiştir[536].

[532] Yargıtay İçtihadı Birleştirme Kararı, 25.06.1984, E.1984/41, K.1984/5, (Kazancı Hukuk Otomasyonu)
[533] Erdoğan, O, s. 482, Anayasa Mahkemesi Kararı, 08/12/2015, E. 2014/87, K. 2015/112, RG. 28/01/2016, sy:29607
[534] Çağlayan, İdari Yaptırımlar, s. 159; Otacı, s. 68
[535] Gökcan, "İdari Para Cezalarının Uygulanması", s. 18.
[536] Danıştay 10.D, 13.06.1995, E.1994/665, K.1995/3085, AKDP

Böyle bir yaklaşım idari para cezaları açısından sübjektif bir nitelik taşıdığı söylenebilir[537]. Zira kanun koyucu tarafından yetkilendirilen idari merci tarafından verilen idari yaptırımların miktarı belirlenirken her somut olayın özellikleri dikkate alınarak yaptırım uygulanır[538]. Belirlenen bu kural "fiille orantılı ceza" ilkesinin uygulanması gayesiyle düzenlenmiş olup[539], idari para cezasına karar verecek makamın takdir yetkisini keyfi olarak kullanmasının önüne geçilmiş olacaktır[540] .

Maktu idari para cezalarına ilişkin kanuni düzenlemede belirlenen oranlar enflasyonist ortamda zamanla tesirini yitirme riski ile karşı karşıyadır. Böyle bir durumun oluşmaması için Kabahatler Kanunu m. 17/7'de düzenleme yapılmıştır. Bu düzenlemeye göre, idari para cezaları her takvim yılı başından geçerli olmak üzere o yıl için 213 sayılı Vergi Usul Kanunu mükerrer m. 298 hükümlerince tespit ve ilan edilen yeniden değerleme oranında artış yapılarak uygulanır. Yapılan bu hesaplamaya göre, idari para cezasının bir Türk Lirası'nın küsuratı dikkate alınmaz. KK m. 17/7 nispi nitelikteki idari para cezaları bakımından uygulanmaz. Maktu ve alt üst sınırları kanunda gösterilmiş olan idari para cezalarının 5252 sayılı Türk Ceza Kanunu'nun Yürürlük ve Uygulama Şekli Hakkında Kanun'u m. 4 dikkate alınarak aşağıda belirtildiği şekilde her yıl hesaplanması gerekmektedir[541],

i. İdari para cezası içeren kanunun ya da maddenin yürürlüğe girdiği tarihin tespiti gerekmektedir.
ii. İlgili düzenlemede yer alan idari para cezasının miktarı 5252 sayılı Kanun m. 4'te kanunların yürürlük tarihleri dikkate alınarak tespit edilen katsayı ile çarpılır.
iii. Yapılan hesaplama sonucu bulunan ya da 31/12/2002 tarihinden sonra yürürlüğe giren düzenlemede belirtilen miktar 2005 yılından sonra 213 Sayılı Vergi Usul Kanun'u mükerrer m. 298 gereğince her yıl için tespit ve ilan edilen yeniden değerleme oranına göre arttırılmış miktarı üzerinden hesaplama yapılır.

[537] Sakine Arık, 'dari Yaptırımlarda Ölçülülük İlkesi, Yüksek Lisans Tezi, Gazi Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, Ankara, 2010, s. 14.
[538] Sakine Arık, 'dari Yaptırımlarda Ölçülülük İlkesi, Yüksek Lisans Tezi, Gazi Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, Ankara, 2010, s. 14.
[539] Gökcan, Hasan Tahsin, Kabahatler Kanununa Göre İdari Para Cezalarının Uygulanması, Türk Hukuk Dergisi, S.104, Kasım 2005, s. 18
[540] Yalçın, s. 88.
[541] Otacı, Cengiz/ Keskin, İbrahim Türk Kabahatler Hukuku, s. 18; Güçlü, Yaşar, İdari Para Cezaları ve Diğer İdari Yaptırımlar, 2. Baskı, s. 94-101.

Kabahatler Kanunu'nda idari para cezalarının ayrıca kanunda alt ve üst sınırları gösterilmek suretiyle belirlenebileceği ifade edilmiştir. Bu açıdan ölçülülük ilkesini tanımlayacak olursak, bir hedefe ulaşmak için tercih edilen yolun ve aracın hedeflenen amaca uygunluğunu ifade etmektedir[542]. İdari yaptırımlar açısından ölçülülük ilkesi, idarenin işlem ve eylemlerinde kullandığı yolların, araçların idarenin hedeflediği amaca uygun olmasını ifade etmektedir[543]. Zira, amaç ile araç arasında makul bir orantının bulunması gerekmektedir[544]. Danıştay vermiş olduğu bir kararında[545], "*Özgürlükler alanında getirilen sınırlamanın onu belirleyen durumla orantılı olmasını, hak ve özgürlüğün varlığını zedelemesini ifade eden orantılık ilkesinin gereği olarak; o suçun toplum hayatında sakınca dikkate alınarak idarece verilecek cezanın takdiri gerekir*." diyerek ölçülülük ilkesine vurgu yaptığını görüyoruz. Ancak buna rağmen, ilgili mevzuatımızda idari para cezalarına ilişkin düzenlemeler ekseriyetle maktu olarak belirlenmiştir. Bu durumun ölçülülük ilkesi ile çeliştiğini söyleyebiliriz[546].

İdari para cezalarında alt ve üst sınırlar belirlenirken kanun koyucu takdir hakkını kullanır. Ancak kanun koyucu bu takdir hakkını sınırsız kullanamayıp işlenen kabahatin niteliği ve ağırlığıyla orantılı olarak alt ve üst sınırları belirlemesi gerekmektedir. Bu bağlamda Anayasa Mahkemesi'nin 2004 tarihli kararında şu şekilde bir denetim gerçekleştirmiştir: *"... tahsil edilen kamu alacağının süresinde ilgili yerlere aktarılmasındaki gecikmeden dolayı, kamu alacağının yüzde onu oranında idârî para cezası öngörülmesi bu cezaların çok yüksek miktarlara ulaşması sonucunu doğurabilecektir. Böylece yasa hükmü, sorumluları ödeme güçlerini aşan, adaletli ve eylemle orantılı olmayan ölçüsüz bir yükümlülükle karşı karşıya bırakmaktadır. Bu ölçütlerden yoksun olarak konulan Yasa kurallarının Anayasa'nın 2. maddesinde sözü edilen hukuk devleti ilkesine uygun olduğundan söz edilemez"*[547] denilmiştir. Yine 2014 yılında vermiş olduğu bir diğer kararında *"... Sertifikasız faaliyette*

[542] Özbudun, Ergun, Türk Anayasa Hukuku, 6. Baskı, Ankara 2000, s. 105; Oğurlu, Yücel, Karşılaştırmalı İdare Hukukunda Ölçülülük İlkesi, Ankara 2002, s. 21.
[543] Yücel Oğurlu, İdari Yaptırımlar Karşısında Yargısal Korunma, Ankara, Seçkin, 2000, s. 21.
[544] Tanör, Bülent – Yüzbaşıoğlu, Necmi, 1982 Anayasasına Göre Türk Anayasa Hukuku, 2. Baskı, İstanbul 2001, s.151; Özbudun, Ergun, Türk Anayasa Hukuku, 6. Baskı, Ankara 2000, s. 105; Oğurlu, Yücel, Karşılaştırmalı İdare Hukukunda Ölçülülük İlkesi, Ankara 2002, s. 21.
[545] Danıştay 10.D, 13.06.1995, E.1994/665, K.1995/3085, AKDP
[546] Yıldırım, Resul, İdari Para Cezaları Karşısında Yargısal Korunma, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, Konya 2005, s. 58.
[547] Anayasa Mahkemesi Kararı, 23/03/2004, E. 2001/119, K.2004/37, RG: 21.07.2004, S:25529

bulunma eylemi ile bu eylem için itiraz konusu kuralda öngörülen para cezasının orantısız olduğu, kuralın bu haliyle uygulanması durumunda küçük çaplı işletmelerin ekonomik varlıklarının sona ermesine sebebiyet verebileceği…, cezanın alt sınırı hususunda kademelendirme yapılmayarak tüm işletmeler için onbin Türk lirasından başlayan para cezasının öngörülmesinin eşitsizliğe neden olduğu belirtilerek kuralın…Anayasanın 90. maddesine aykırı olduğu ileri sürülmüştür…Sertifika almaksızın fikir ve sanat eserlerinin tespit edilmesi ve çoğaltılmasına ilişkin materyalleri üreten ve bu materyalleri dolum, çoğaltım ve satışını yapan ve herhangi bir şekilde yayan ve umuma arz eden işletmelerin ekonomik büyüklüklüğü ve sınıfına göre adil bir denge gözetilmeden, itiraz konusu kuralla ölçülü ve makul olmayan idari para cezaları ile cezalandırılmaları, hukuk devletinin gereği olan "adalet" ve "hakkaniyet" ilkeleriyle bağdaşmamaktadır[548]" denilmiştir. Dolayısıyla verilmiş olan kararları incelediğimizde bazı kararlarında işlenen kabahate oranla ceza alt sınır miktarının yüksek belirlenmesini ölçülülük ilkesine aykırı görmüştür. Uygulanacak yaptırım, ihlalin ağırlığıyla orantılı olmalıdır. İdari para cezalarında cezanın alt ve üst sınırları arasındaki miktarın tespitinde ya da ihlalin tekrarı gibi durumlarda verilecek olan cezanın ağırlaştırılması sırasında ölçülülük ilkesinin dikkate alınması gerekir[549].

Kabahatler Kanunu'nda kusuru etkileyen sebepler, teşebbüs, kaçınabilir hata gibi hususlarda idari para cezasında indirim yapılıp yapılmayacağını, şayet yapılacaksa hangi oranda yapılacağına ilişkin olarak ilgili düzenlemede değinilmemiştir. Ancak, idari para cezasını vermeye yetkili kişi veya makamlar, bu türden hususları, Kabahatler Kanunu m. 17/2, c. 2 çerçevesinde değerlendirebilecek nitelikte iseler, dikkate alarak idari para cezasının miktarını belirleyebileceklerdir. Bu miktarların tespiti yapılırken kanunda gösterilen alt sınırın altına inilemez, üst sınır ise aşılamaz[550].

Her ne kadar yıllık yeniden değerleme yapılsa da bu idari para cezaları hiçbir şekilde caydırıcı nitelik taşıyor gibi görünmemektedir. En son bunu yemek sepeti firmasının veri ihlalinde gördük[551]. Bahse konu ihlal bildiriminde, 18/03/2021 tarihinde kimliği tespit

[548] Anayasa Mahkemesi Kararı, 03/07/2014, E. 2014/62, K. 2014/125, RG. 2/12/2014, sy:29203
[549] Erdoğan, Oktay, Para Cezaları ve İnfazı, 2. Baskı, İstanbul 2007, s. 495.
[550] Zeynel, Kangal, Kabahatler Hukuku, İstanbul, onikilevha, 2019, s. 286
[551] Kişisel Verileri Koruma Kurulunun 23/12/2021 Tarihli ve 2021/1324 Sayılı Karar, (Çevrimiçi), https://www.kvkk.gov.tr/Icerik/7168/2021-1324 , (Erişim Tarihi: 05/05/2022).

edilemeyen şahıs/şahıslar tarafından veri sorumlusuna ait bir web uygulama sunucusuna erişildiği ve bu İhlalden 21.504.083 Yemeksepeti kullanıcısının etkilendiği tespit edilmiştir. Bunun yanısıra büyük miktarda kişisel veri işleyen veri sorumlusunun bu boyutta bir ihlal yaşamasının ve müdahalede geç kalmasının mevcut risk ve tehditleri iyi belirlemediğinin göstergesi olduğu anlaşılmıştır. Dolayısıyla tespit edilen hususlar gözönünde bulundurularak Kişisel Verileri Koruma Kurumu tarafından *"6698 sayılı Kişisel Verilerin Korunması Kanununun 12 nci maddesinin (1) numaralı fıkrası hükmü çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca ihla*lin boyutu, *kabahatin haksızlık içeriği, veri sorumlusunun kusuru ve ekonomik durumu da göz önünde bulundurularak 1.900.000 TL idari para cezası uygulanmasına karar verilmiştir.*" Yemek sepeti firmasının yapmış olduğu ihlalde milyonlarca kişinin verisinin sızdırıldığı buna karşılık bu kadar büyük bütçeye sahip olan firmaya kesilen idari para cezasının yeterli olmadığı kanaatindeyiz. Zira öbür tarafta daha küçük bütçeli bir firmada böyle bir veri ihlali olduğunda da ona da benzer rakamlarda idari para cezasının kesildiğini görmekteyiz. Dolayasıyla biz bunun mutlaka o şirketin ekonomik durumuna göre yeniden organize edilmesi, böyle bir alt üst belirlenmiş idari para cezasının caydırıcılıktan ve kabahatin bireyselleştirilmesinden fevkalade uzak olduğunu düşünüyoruz.

5.2.9.2.3. Mülkiyetin kamuya geçirilmesi yaptırımı

İşlenen kabahat karşılığında öngörülen idari para cezası dışında bir diğer önemli yaptırım türü mülkiyetin kamuya geçişidir. İdari yaptırımların birden çok türü bulunmakla beraber bunlardan en dikkat çekenlerin başında ve özellikle kabahatler kanununda ayrıntılı düzenlenen mülkiyetin kamuya geçirilmesi tedbiri olduğunu ifade edebiliriz. Kabahatler Kanunu m.18 yer alan düzenlemede yasada açık hüküm bulunan durumlarda, işlenen kabahatin konusunu oluşturan ya da işlenmesi yoluyla ele geçirilen eşyanın mülkiyetinin kamuya geçirilmesi hükmü verilebilmektedir. Mülkiyetin kamuya geçirilmesi ile ilgili anlam karmaşasına neden olmamak için Kabahatler Kanunu m. 16 düzenlemesinin gerekçesinde, Türk Ceza Kanunu'nda suçun karşılığında öngörülen güvenlik tedbiri mahiyetinde ki eşya müsaderesi kavramı bir karışıklığa neden olmamak için; fiilin işlenmesiyle elde edilen eşyanın sadece Devlet'e değil başka kamu kurum veya kuruluşlarına da geçirilmesi söz

konusu olabileceğinden, kabahatlerle ilintili olarak mülkiyetin kamuya geçirilmesi kavramının kullanıldığı görülmektedir[552].

5.2.9.2.4. Diğer idari önlemler

İncelediğimiz kabahatte bulunmamakla birlikte diğer idari tedbirler başlığının altında özellikle Kabahatler Kanunu m. 19'da ve diğer yasal düzenlemelerde yer bulan kabahat fiillerine karşılık belirli bir süreliğine uygulanması öngörülen çeşitli idari tedbirlere yer verildiğini görmekteyiz. Bu idari tedbirler, iş yerinin kapatılması tedbiri, ruhsat veya ehliyetin geri alınması tedbiri, bir meslek veya sanatın yerine getirilmemesi tedbiri, kara, deniz veya hava nakil aracının trafikten alıkonulması şeklinde sıralanabileceğini ifade edebiliriz.

5.2.9.3. İhlal durumunda kişisel verileri koruma kuruluna şikâyet

5.2.9.3.1. Kişisel verileri koruma kurulu

Kişisel verilerin işlenmesi ile ilgili denetim yapılabilmesi oldukça önemlidir. Bu anlamda bağımsız bir denetim organının kurulması gerektiği Veri koruma Tüzüğü'nde düzenlendiğini görmekteyiz. KVKK genel gerekçesi incelendiğinde, kişisel verilerin işlenmesi ile ilgili bir denetim organının bulunmadığı bu nedenle böyle bir düzenlemeye gereksinim duyulduğu ifade edilmiştir. Denetim organı görevini yerine getirecek bu kurumun bağımsızlığı en az böyle bir organının kurulması kadar önemli olup, kurumun bağımsızlığı bir kural olarak kalmamalı, yapılan uygulamalarda da bağımsızlık önceliklenmelidir[553]. Denetim organı, özellikle temel hak ve özgürlüklerin korunması adına hareket etmesi gerekmektedir[554]. Zira, KVKK m. 21'de Kişisel Verileri Koruma Kurumu yetkilerini kullanırken bağımsız olması gerektiği ile ilgili olarak; görev alanına giren tüm hususlarda hiçbir makam merci ya da kişiden emir talimat ya da tavsiye almayacağını açıkça söyleyebiliriz. Aksi durumda kişi hak ve hürriyetinin korunması söz konusu olmayacaktır. Kurul'un görevleri ayrıca m. 22'de düzenlenmiştir. Bu görevlerin başında, kişisel verileri mevzuata uygun biçimde işlenmesini sağlamak, Kişisel Verileri Koruma Kurumu'na gelen şikayetleri süresi içerisinde incelemek, özel nitelikli verilerin işlenmesi adına sağlanması

[552] Kabahatler Kanunu m. 16 gerekçesi.
[553] Küzeci, a. g. e., s. 363.
[554] Küzeci, a. g. e., s. 364.

gereken asgari önlemleri belirlemek ve bu alanda gerekli düzenleyici işlemlerin yapılmasını sağlamak Kurul'un başlıca görevleri olarak sayılabilir.

5.2.9.3.2. Şikâyet

Kişisel Verilerin Korunması Kanunu m.13'de yapılan düzenlemede şikâyet usulü hakkında bilgi verilmektedir. İlgili kişinin veri sorumlusuna yapmış olduğu talebin reddedilmesi, talep sonucunda verilmiş olan cevabın yetersiz bulunması veya talebin süresi içerisinde cevaplandırılmaması durumunda, Kurul'a şikâyette bulunma hakkı bulunmaktadır. İlgili kişi bu talebi ile ilgili verilen cevabın verilmesinden itibaren otuz gün veya her halükârda başvuru tarihinden itibaren altmış gün içerisinde şikâyet hakkını kullanabilmesi gerekmektedir. İlgili kişinin veri sorumlusuna yapmış olduğu başvuru ile ilgili olarak, veri sorumlusuna ilgiliye kişiye cevap verilmediği durumda kişinin bekleyeceği maksimum süre altmış günü geçmemiş olması gerekmektedir. İlgili kişinin altmış günden daha fazla cevabı beklememesi gerektiği dolayısıyla Kurul'a şikâyet hakkını kullanabilmesi açısından önemlidir. İlgili kişinin talepleri ile ilgili olarak Kurul'a şikâyette bulunabilmesi için mutlaka veri sorumlusuna başvuru yolunu tüketmiş olması gerekmektedir (KVKK m. 14/2). Kurul'a yapılan şikayetler gerekli incelemeler yapılarak söz konusu kişilere bilgi verilmektedir. Zira altmış gün içerisinde cevaplandırılmayan şikayetler reddedilmiş sayılmaktadır (KVKK m. 15/4). Kurul yaptığı incelemede herhangi bir ihlalin varlığını tespit ederse, giderilmesi için veri sorumlusuna bildirimde bulunmaktadır. Veri sorumlusu bu bildirim kendisine tebliğ edildiği tarihten itibaren söz konusu ihlali otuz gün içerisinde giderilmesi gerekmektedir. Kurul ayrıca KVKK m. 22'de düzenlenen yetkisine dayanarak veri sahibi tarafından gelen şikâyet üzerine tespit edeceği ihlalin sonucunda idari yaptırım tatbik edilmesi yetkisine haizdir. Kurul'a gelen şikâyet veya Kurul'un re'sen yaptığı inceleme neticesinde veri sorumlusunun aydınlatma yükümlülüğünü yerine getirmediği kabahati ile ilgili olarak, Kurul'un idari para cezası uygulama yetkisi bulunmaktadır.

5.2.9.3.3. İdari para cezasının tatbik edilmesi

Yasa koyucu tarafından Kabahatler Kanunu m. 22'de yapılan düzenlemeye göre işlenen kabahat nedeniyle idari yaptırım uygulama yetkisinin yasada açıkça düzenlenen kurul, makam ya da kamu görevlilerinde olduğu ifade edilmektedir. İdari yaptırım uygulama

salahiyeti bulunan kurul, makam ya da kamu görevlileri yalnızca görev alanına giren yerlerde işlenen kabahatler için idari para cezası uygulayabilmektedirler (KK m. 22/3).

5252 sayılı Kanun'u m. 7 son fıkraya göre "*Bu madde hükmüne göre idari para cezasına karar vermeye Cumhuriyet savcısı yetkili" ise de bu düzenleme Kabahatler Kanunu'nun 23. maddesindeki "Cumhuriyet savcısı, kanunda açıkça hüküm bulunan hallerde bir kabahat dolayısıyla idarî yaptırım kararı vermeye yetkilidir"* hükmüne paralel olarak Cumhuriyet savcısı, ilgili mevzuat düzenlemelerinde açıkça hüküm bulunan hallerde, bir kabahat nedeniyle idari yaptırım kararı vermeye yetkilidir. Bunun yanında bir suç nedeniyle başlatılan soruşturma kapsamında herhangi bir kabahatin işlendiğini öğrenmesi durumunda Cumhuriyet savcısı durumu ilgili kamu kurum ve kuruluşuna bildirebileceği gibi, kendisi de idari yaptırım kararı verebilir. Bir soruşturma kapsamında, fiilin kabahat oluşturduğunun anlaşılması durumunda ilgili kamu kurum ve kuruluşu tarafından idari yaptırım kararı verilmemiş olması şartıyla, Cumhuriyet savcısı idari yaptırım kararı verebilir. Ancak, Cumhuriyet savcısının bu yetkisi henüz dava konusu edilmemiş kabahat fiillerine ilişkindir. Zira davaya konu olmuş kabahat fiilleri için de geçerli mutlak bir görev hükmü değildir[555]. Aksinin düşünülmesi durumunda, yargıya taşınmış bulunan davalarda görevsizlik kararı verilmesi gerekir[556]. İdari yaptırım kararı verebilecek bir diğer makam olan mahkeme ise, kovuşturma konusu fiilin kabahat oluşturduğunun anlaşılması durumunda idari yaptırım kararını mahkemenin bizatihi kendisi verecektir. Bu düzenleme Kabahatler Kanunu m. 24'ün amir hükmü olup, fiilin idari ceza gerektirdiği nedeniyle görevsizlik kararı verilemeyecektir[557]. Ancak, mahkemelerin idari yaptırım kararı verebilmesi istisnai bir durum olup, suç vasfının değişmesi, yanlış nitelendirme ile dava açılmasına rağmen iddianamenin kabul edilmesi ya da sonradan yapılan değişiklikle eylemin kabahat olması[558] gibi durumlarda söz konusu olacaktır.

---

[555] Gökcan, Hasan Tahsin, Cumhuriyet Savcısının Ceza Vermeye Yetkili Olduğu Kabahatler, Türk Hukuk, Aralık 2005, sayı 105, s. 16

[556] . Ceza Dairesi, 29/01/2009, 2006/4448 E., 2009/1129 K; 11. Ceza Dairesi, 25/12/2008, 2008/460 E., 2008/13853 K.

[557]. Ceza Dairesi, 01/04/2009, 2006/10419 E., 2009/3817 K., Ceza Genel Kurulu, 12/02/2008, 2008/YYB-12 E., 2008/19 K.

[558] 7. Ceza Dairesi, 29/9/2005 2003/14059 E., 2005/16238 K.

Kişisel Verilerin Korunması Kanunu m. 22'de yer alan düzenleme gereğince Kanun'da ifade edilen idari yaptırımlara karar verilmesine ilişkin ilgili Kurul'un yetkili olduğu ifade edilmektedir (m. 22/1-ğ). Kişisel verileri işlenen kişilere karşı aydınlatma yükümlülüğünü yerine getirmeyen veri sorumluları hakkında Kurul tarafından "5.000 Türk Lirası ile 100.000 Türk Lirası arasında idari para cezası" uygulanmaktadır. Bahse konu idari para cezaları yalnızca gerçek veya özel hukuk tüzel kişileri hakkında uygulanmaktadır (KVKK m. 18/2).

İdari Para cezalarının uygulanması ile ilgili KVKK m. 18'in gerekçesinde, idari para cezalarının uygulanması ilişkin olarak belirlenen aralığın bilinçli olarak geniş tutulduğu, idari para cezalarının belirlenmesinde işlenmiş olan kabahatin haksızlık içeriği, failin kusur derecesi ve failin ekonomik durumu dikkate alınacağı, dolayısıyla farklı ekonomik bütçeye sahip gerçek ve tüzel kişiler arasında uygulanacak olan yaptırımın hakkaniyetli bir şekilde uygulanması amaçlanmaktadır[559]. Ancak daha somut kriterler dikkate alınarak idari para cezasının miktarının belirlenmesi yerinde olacağı kanaatindeyiz[560]. KVKK idari para cezaları için öngörülen idari para ceza miktarlarının minimum ve maksimum aralıklarının geniş tutulması ve idari para cezalarının tespit edilmesinde dikkate alınacak somut kriterlerin bulunmaması, uygulamada tutarsız kararların ortaya çıkmasına sebep olduğu görülmektedir.

Veri sorumlusu tarafından işlenen kabahatin, kamu kurumu veya kamu kurumu niteliğindeki meslek kuruluşunda işlenmesi durumunda bahse konu kurumlarda çalışan kişiler hakkında disiplin soruşturmaları yapılıp, ilgili Kurul'a soruşturmanın sonucu bildirilir (KVKK m. 18/3). Kamu Kurumu niteliğinde olan Mimar Sinan Üniversitesi'nde gerçekleşen öğrenci verilerinin ihlaline yönelik olarak, Kurul tarafından ihlale sebebiyet veren personeller hakkında disiplin soruşturmasının açılması gerektiği ifade edilmiştir[561].

Fail tarafından işlenen fiillere karşı kurul tarafından verilen idari para cezalarına karşı yargı yoluna her zaman başvurulabilir[562]. Yasa koyucu tarafından düzenlenen Kabahatler Kanunu gereğince kurul tarafından verilen idari para ceza kararının, tebliği ya da tefhiminden itibaren

[559] KVKK, m.18 gerekçesi.
[560] Küzeci, a. g. e., s. 376.
[561] Kişisel Verileri Koruma Kurulunun 01/07/2019 Tarihli ve 2019/188 Sayılı Karar, (Çevrimiçi), https://kvkk.gov.tr/Icerik/5506/2019-188 , (Erişim Tarihi: 03/03/2022).
[562] KVKK, m.18 gerekçesi.

on beş gün içinde sulh ceza hakimliğine başvurabilmektedir (KK m. 27/1). KVKK'da yer alan çeşitli düzenlemelerin ihlali durumunda herhangi bir idari yaptırım uygulanmayabilir. Söz konusu düzenlemeler açısından vereceğimiz örnek; kişisel verilerin meşru amaçlar dışından işlenmesi halinde fiili işleyene yönelik bir yaptırım söz konusu olmayabilir[563].

5.2.10. Kişisel Verilerin Korunmasında Zamanaşımı

Kanunda yapılan düzenlemeye göre iki ayrı zamanaşımı türü bulunmaktadır. Birincisi Kabahatler Kanunu m. 20'de düzenlenen soruşturma zamanaşımı ikincisi de Kabahatler Kanunu m. 21'de düzenlenen yerine getirme zamanaşımı olarak ifade edebiliriz.

5.2.10.1. Soruşturma zamanaşımı

Kanun koyucu tarafından yapılan düzenlemeye göre,

"Soruşturma zamanaşımı süresi;

a) *Yüzbin Türk Lirası veya daha fazla idarî para cezasını gerektiren kabahatlerde beş,*
b) *Ellibin Türk Lirası veya daha fazla idarî para cezasını gerektiren kabahatlerde dört,*
c) *Ellibin Türk Lirasından az idarî para cezasını gerektiren kabahatlerde üç yıldır."* (KK m. 20)

Nispi para cezalarının öngörüldüğü kabahatler açısından soruşturma zamanaşımı süresi sekiz yıl olarak Kabahateler Kanunu m. 20/3'de düzenlenmiştir.

Maktu ve nispi para ceza kavramlarını açıklayacak olursak; işlenen kabahat karşılığında düzenlenen para cezasının sabit olması durumunda maktu para cezasından bahsedilir[564]. Ancak miktar yasa koyucu tarafından önceden belirlenmeyen ve fakat fiili işleyen failin kabahati işleyerek elde etmiş olduğu yarar veya sebep olduğu zarara oranla belirlenen para cezası söz konusu olduğunda da nispi para cezalarından bahsedilmektedir[565]. İfade edilen bu para cezaları dışında kanun koyucu tarafından alt ve üst limitleri belirlenmek suretiyle düzenlenebilir[566]. Konumuz bağlamında aydınlatma yükümlülüğünün yerine getirilmemesi durumunda verbis sorumlusu bakımından kabahat söz konusu olacaktır. Failin işlediği bu

[563] Küzeci, a. g. e., s. 375.
[564] Cüneyd Altıparmak, Kabahatler Hukukunda Soruşturma Zamanaşımı, İstanbul Barosu Dergisi, C.82, S.1, Y.2008, 49-57, s. 54.
[565] Kangal, a. g. e., s. 279.
[566] Kangal, a. g. e., s. 282.

fiil nedeniyle Kişisel Verilerin Korunması Kanunu m. 18 de ki düzenlemeye göre "5000 Türk Lirasından 100.000 Türk Lirasına kadar idari para cezası uygulanabileceği" ifade edilmiştir. Kanun koyucunun ilgili yasal düzenlemeyi yaparken yaklaşımı, idari para cezaları belirlenirken alt ve üst limitler gösterilerek belirlendiği görülmektedir.

İdari para cezasının, mevzuatta alt ve üst sınırları belirtilmek suretiyle soruşturma zamanaşımı, Kabahatler Kanunu m. 20/2'de yer alan düzenlemeye göre belirlenir[567]. Yasal düzenlemede alt ve üst sınırların farklı zamanaşımı dilimlerine dahil olduğu bir durumda soruşturma zamanaşımı, uygulanacak olan idari para cezası yasada belirlenen üst sınır dikkate alınarak belirlenmektedir[568]. Dolayısıyla veri sorumlusunun aydınlatma yükümlülüğünün yerine getirilmemesi kabahati bakımından soruşturma zamanaşımı beş yıl olduğunu söyleyebiliriz.

Veri sorumlusu veya temsilcisi tarafından işlenen kabahat fiilinin işlendiği tarihten itibaren düzenlemede belirlenen süreler içerisinde yetkili kişi veya kurullarca işlenen kabahat hakkında uygulanması gereken idari yaptırımın uygulanmaması durumunda belirlenen süreler geçtikten sonra soruşturma, zamanaşımına uğrayacak olup bu aşamadan sonra herhangi bir idari yaptırım söz konusu olmayacaktır[569]. İlgili konu bağlamında soruşturma kavramı ceza muhakemesinde ki soruşturma kavramından farklı anlam taşımaktadır[570].

Burada soruşturma zamanaşımından anlamamız gereken, idari yaptırımın uygulanabileceği zaman ifade edilmektedir. Zira soruşturma zamanaşımı fail tarafından kabahat fiilinin işlenmesi veya sonucun gerçekleşmesinden itibaren süre işlemeye başlamaktadır[571].

Konumuz açısından aydınlatma yükümlülüğünün yerine getirilmemesi kabahatinin işlenmesi durumunda soruşturma zamanaşımı veri sahibinden kişisel verisinin alınması esnasında yükümlülüğün ifa edilmemesi halinde işlemeye başlayacağını ifade edebiliriz.

---

[567] Kangal, a. g. e., s. 424.
[568] Kangal, a. g. e., s. 424.
[569] Altıparmak, a. g. e., s. 53; Murat Kayançiçek, Ceza Hukuku ve Kabahatler Hukukunda Zamanaşımı, Ankara, Adalet, 2014, s. 310.
[570] Kayançiçek, a. g. e., s. 310.
[571] Altıparmak, a. g. e., s. 53; Kayançiçek, a. g. e., s. 53.

Kişisel verilerin kişinin kendisinden elde edilememesi durumunda soruşturma zamanaşımı süresi, Aydınlatma Tebliği'nde düzenlenen süreler baz alınarak işlemeye başlayacağını söyleyebiliriz. Düzenlenen sürelerde aydınlatma yükümlülüğünün ifa edilmemesi durumunda söz konusu kabahat işlenmiş olacaktır. Soruşturma zamanaşımı ile ilgili olarak örnek verecek olursak, kişisel verileri iletişim kurmak amacıyla elde edilen kişinin aydınlatma yükümlülüğü iletişim kurulduğu anda yerine getirilmesi gerekmektedir (Aydınlatma Tebliği m. 6/1-b). Şayet ilgili kişi ile iletişim kurulduğu anda aydınlatma yükümlülüğü yerine getirilmemesi söz konusu ise bu durumda kabahat işlenmiş olacaktır. Soruşturma zamanaşımı kabahatin söz konusu olduğu andan itibaren işlemeye başlayacaktır. Fakat bir diğer düzenleme olan Aydınlatma Tebliği m. 6/1-a'da yer alan düzenlemeye göre kişisel verilerin ilgili kişiden elde edilmemesi durumunda bahse konu kural kişinin verilerinin elde edilmesinden itibaren makul bir süre içerisinde aydınlatma yükümlülüğünün yerine getirilmesi gerektiği ifade edilmektedir. Ancak yukarıda da belirtildiği üzere makul süre ifadesi, kabahatin ne zaman işlenmiş sayılacağı konusunda ciddi belirsizliklere yol açmaktadır. Dolayısıyla makul sürenin ne zaman son bulacağı akabinde aydınlatma yükümlülüğünün ifa edilmemesi durumunda kabahatin ne zaman işlenmiş sayılacağı ve soruşturma zamanaşımın ne zaman başlayacağı ile ilgili tespitte bulunmak oldukça zor olacaktır.

Yasal düzenlemelerde belirlenen sürelere ilişkin olarak, soruşturma zamanaşımı süresinin tamamlanması neticesinde, idari para cezasını tatbik etmeye yetkili makam tarafından *"soruşturma zamanaşımının dolması nedeniyle idari para cezasının uygulanmasına yer olmadığına"* ile ilgili karar verilecektir[572]. Fail tarafından gerçekleştirilen fiil neticesinde hem kabahat hem de suç oluşması durumunda, suça ilişkin dava zamanaşımı ayrıca uygulanacaktır (KK m. 20/5). Soruşturma zamanaşımının durması veya kesilmesi söz konusu olmayacaktır[573].

5.2.10.2. Yerine getirme zamanaşımı süresi

Yasa koyucu tarafından düzenlenen Kabahatler Kanunu m. 21'deki düzenleme gereğince,

[572] Kayançiçek, a. g. e., s. 312; Altıparmak, a. g. e., s. 55;
[573] Otacı, Keskin, a. g. e., s. 60.

"*Yerine getirme zamanaşımı süresi;*

a) *Ellibin Türk Lirası veya daha fazla idarî para cezasına karar verilmesi halinde yedi,*
b) *Yirmibin Türk Lirası veya daha fazla idarî para cezasına karar verilmesi halinde beş,*
c) *Onbin Türk Lirası veya daha fazla idarî para cezasına karar verilmesi halinde dört,*
d) *Onbin Türk Lirasından az idarî para cezasına karar verilmesi halinde üç yıldır.*"

"*Zamanaşımı süresi, kararın kesinleşmesinin rastladığı takvim yılını takip eden takvim yılı başından itibaren işlemeye başlar."* şeklinde ifade edilmektedir. Yerine getirme zamanaşımı süresi, fail tarafından işlenen fiil için verilen idari para cezasının kesinleşmesi ile başlamaktadır. Kararın kesinleşmesinin söz konusu olabilmesi için işlenen fiil hakkında verilen karar ile ilgili olarak iç hukuk yollarının tüketilmiş olması veya iç hukuk yollarının tüketilmeden verilen kararın uygulanabilmesi için şartların oluşması gerekmektedir[574].

İşlenen fiil neticesinde Kişisel Verileri Koruma Kurumu tarafından verilen idari para cezalarına karşı yargı yolu açık olup Kabahatler Kanunu m. 27 gereğince verilen karara karşı, kararların tefhim ve tebliğinden itibaren on beş gün içinde sulh ceza hâkimliğine başvuruda bulunulması gerekmektedir. Verilen idari para cezasına karşı yargı yolunu kullanmak isteyen kişi belirtilen süreyi, sulh ceza hâkimliğine başvurmadan geçirmesi durumunda karar kesinleşecektir. Kararın kesinleşmesinden itibaren yerine getirme zamanaşımı süresi işlemeye başlayacaktır. Failin işlediği fiil bakımından verilen idari para cezasına itiraz etmek için, sulh ceza hâkimliğine başvurması durumunda, mahkeme tarafından verilen kararın kendisine tebliğ edildiği tarihten itibaren yedi gün içerisinde CMK'da yapılan düzenlemeler gereğince itiraz edebilecektir (KK m. 29). Dolayısıyla verilen idari para cezasının kesinleşebilmesi için idari para cezasına yapılmış olan itirazın reddedilmesi gerekmektedir. İtirazın kesinleşmesinden sonra yerine getirme zamanaşımı süresini başlatacaktır.

Hem KVKK hem de Kabahatler Kanunu'nda idari para cezalarının tahsiline ilişkin olarak, yerine getirme zamanaşımın durması veya kesilmesi ile ilgili özel hükümler

[574] Otacı, Keskin, a. g. e., s. 63.

bulunmamaktadır. Yalnızca konumuz açısında ilişkilendirebileceğimiz 6183 sayılı Amme Alacaklarının Tahsili Usulü Hakkında Kanun m. 103'te yapılan düzenleme gereğince yerine getirme zamanaşımını kesen durum, m. 104'te yapılan düzenleme gereğince de yerine getirme zamanaşımını durduran durum ifade edilmektedir[575]. Söz konusu ilgili kanunun m. 103'e gereğince, ödeme emri tebliği, haciz gerçekleştirmesi, ödeme gibi durumlarda yerine getirme zamanaşımı süresi kesilmektedir. Dolayısıyla zamanaşımının kesilmesi halinde *"Kesilmenin rastladığı takvim yılını takip eden takvim yılı başından itibaren zamanaşımı yeniden işlemeye başlar.*" (6183 sayılı Kanun m. 103/2). İlgili kanunun m. 104 gereğince "*borçlunun yabancı memlekette bulunması, hileli iflas etmesi veya terekesinin tasfiyesi dolayısıyla hakkında takibat yapılmasına imkân yoksa bu hallerin devamı müddetince zamanaşımı işlemez*." Zamanaşımını durduran nedenlerinin kalkması durumunda yerine getirme zamanaşımı süresi, kaldığı yerden devam edecektir (6183 sayılı Kanun m. 104/2).

[575] Otacı, Keskin, a. g. e., s. 64.

6. SONUÇ

Bireylerin kişisel verilerin korunması, genel anlamda bakıldığında yeni gelişen ve genel koruma yöntemleri ile korunması gereken bir alan olarak görülebilir, ancak bu alana bu şekilde yaklaşmak kişilerin bugünü ve geleceği adına risklerin oluşmasına sebebiyet verebilir. Ulusal ve ulusal uluslararası düzenlemeler incelendiğinde kişisel verilerin korunmasının çözüm bulunması gereken ve genel koruma yöntemlerinden çok daha öte dikkatli ve özenli düzenlemelerin yapılması gerektiğini ifade edebiliriz.

Bahse konu bu alan, esas olarak kişiliğinin korunmasına, bireyin kendisine ait olan verilerin geleceğine karar verme süreçlerine ilham olmaktadır. Bireyin kişiliğinin ön plana alınması, bu alanın rakamlardan oluşmadığının ispatıdır. Toplum tarafından sanki teknoloji olduğu için kişisel verilerimiz var olmakta oysa kişisel verilerin korunması alanı esasen doğrudan teknoloji ile bağlantılı değildir. Burada karıştırılan ya da gözden kaçırılan teknolojinin bireylerin kişisel verilerine yönelik tehditleri çok ciddi boyutlara taşıdığını ifade edebiliriz.

Bilişim alanında yaşanan gelişmeler hayatımızda veri kavramının dillendirilmesine sebebiyet vermiştir. Veri bakımından yaşanan teknolojik gelişmeler verinin korunması gerektiği ve bunun da kişisel verilerin korunması konusu olduğunu görmekteyiz. Modern dünyada teknolojide yaşanan hızlı değişim ve günümüzdeki niteliğe evrilmesi, bireylerin verilerine ilişkin güvenlik kaygılarının artmasına sebep olmuştur. Kişisel verilerin korunmasına ilişkin kaygıların artması bu alanda hukuki manada usul ve esasların hazırlanması gerektiği bilincinin oluşmasında etkili olan konulardan biri olduğunu ifade edebiliriz.

Sanayi devrimi ile birlikte teknolojik ürünlerin sayısının artması ve bu ürünleri kullanan kullanıcıların sayısının artmasına neden olmuştur. Kullanıcı sayısından yaşanan bu artış kişisel verilerin her an daha fazla üretilmesine, toplanmasına, kullanılmasına ve en önemli bu teknolojiler sayesinde verilerin birbirileri ile ilişkilendirilip transfer edilmesine neden olduğunu açıkça ifade edebiliriz. Teknolojide yaşanan bu gelişmeler elbette olumlu ve önemli adımlar olmak birlikte ciddi manada olumsuz etkileri de bulunmaktadır. Üretilen teknolojik ürünlerin güvenlik kaygılarına yönelik gelişimi bunun açık göstergesidir.

Bireyin kişiliğinin, devletlerin ve işletmelerin kurduğu düzen içerisinde kaybolmadan, kişiliğini koruyabilmesi ve geliştirebilmesi için, verilerinin geleceğini belirleme hakkına sahip olması gerekir. Bu bakımdan kişisel verileri, kimin ve nasıl kullanacağı sorusu elbette önem kazanmakta olup, kişilerin, kurumların ve devletlerin gücü ile ilgili önemli tespitlerde bulunmamıza imkân sunmaktadır.

Temel bir hak olarak ifade edilen kişisel verilerin korunması konusu sadece teknolojik gelişmelere bağlı olarak ulusal ve uluslararası hukukta bulunan düzenlemelere eklemlenmiş bir alan değildir. Anayasa faaliyetlerinin başlamasına müteakip bireylerin verilerinin koruması konusu günümüz anlamında dile getirilmemiş olsa bile bireylere ait olan verilerin işlenmesi faaliyetini gerçekleştiren ve bu verileri işleyen ister kişileri ister kamu gücü isterse de özel şirketlerin nasıl sınırlandırılması gerektiği ve kişisel verilerin korunması bakımından doğmuş ya da doğacak haklara hangi ölçüde müdahale edilebileceği bütün zamanlarda anayasa metinlerinin gündeminde yer bulmuştur. Bu bakımdan kişisel verilerin korunması konusu yeni gelişmekte olan bir alan olarak düşünülse bile kişisel veri alanının ilişki içerisinde olduğu birçok disiplin ile iç içe geçmiş olan yapısı dikkate alındığında, verilerin korunması hakkı denildiğinde dile getirilen ifadelerin bir hakkın çok daha ötesinde, ulusal ve uluslararası kuruluşların gücünü etkilen bir hukuki alanın dile getirildiği görülmektedir.

Kişisel verilerin korunması dair geçmişi incelediğimizde bu alana yönelik ilk yasal düzenlemelerin, merkezi veri bankalarının kullanımı ile ilgili projelerin geliştirildiği 1970'li yıllara dayandığını görmekteyiz. 1970'li yıllarda çalışılan bu projelerde temel hedef bireyi devlete karşı korunaklı hale getirmektir. Zaman içerisinde devletlerin politikalarını değiştirmesi ve şirketlerin bulundukları ülkede yaşam alanının her noktasını etkileyebilmeleri düşünüldüğünde bireyin sadece devlete karşı değil, özel kuruluşlara karşıda korunması gerektiği ortaya çıkmıştır. Zira bahse konu özel kuruluşlar günümüzde bireylerin verilerini çok daha fazla ihtiyaç duymakta ve hatta bu şirketlerin ayakta kalabilmesinin yegâne şartı haline geldiğini söyleyebiliriz.

Günümüz modern dünyasında, kişilere ait olan sağlık verileri, fotoğrafları, yargılama süreçleri ve sonuçları, alışveriş alışkanlıkları, sendikal bilgileri, nüfus kayıt bilgileri, çalışma bilgileri, eğitim bilgileri gibi kişisel veriler çok kolay bir biçimde depo edilmekte ve ihtiyaç

duyulduğunda teknoloji dünyasının sağlamış olduğu imkanlardan faydalanmak suretiyle analiz edilip çeşitli anlamlı çıktılar elde edildiğini ifade edebiliriz. Son zamanlarda yapay zekanın her alana sirayet etmesinin bir sonucu olarak kişisel veriler bakımından yapılan analizlerde insan müdahalesine dahi gerek duyulmadan birey hakkında çok ciddi anlamlı sonuçlara ulaşılabilmektedir. Yapay zekâ sayesinde bireylerin görüntüleri, sesleri ve bulundukları yerler analiz edilip kayıt altına alınabilmektedir. Sağlık verileri bakımından, DNA profilleri vasıtasıyla bireylere ve akrabalarına ait olan daha önce kendilerinin bile bilmediği bilgilere bu analizler sonucunda ulaşmak mümkün hale gelmiştir. Bütün bu teknolojik gelişmelerin getirdiği sonuç irdelendiğinde varılan sonuç özel yaşama yönelen tehdidin ne denli bir boyuta geldiğini görmemek mümkün değildir.

Kişisel verilerin, sosyal medya şirketlerinin yegâne kaynakları olduğu durumlardan bahsetmiştik. Kişilerin sanal dünyada, internet arama motorları üzerinde bırakmış olduğu izleri takip edildiğinde yapay zekâ marifetiyle, sanal kimlikleri üzerinden kişiliğinin tespit edilmesi yapılabilmektedir. Özel ve kamusal alanda yapılan kişilik çalışmalarına ilişkin "profilleme" bahse konu kişinin davranışları, alışkanlıkları ve tanınmasına ilişkin bir kanı elde edilmesi noktasında çalışmalar yapılabildiğini biliyoruz. Bu durumda veri sahibi bulunan kişi hakkında günlük davranışları, alışveriş alışkanlıkları, siyasi düşüncesi, sağlık bilgileri ve hatta cinsel hayatı hakkında kamu ve özel şirketler tarafından yapılacak bir tespitte rahatlıkla kullanılabilmesi mümkün olacaktır. İfade ettiğimiz üzere teknolojinin ve yapay zekanın bu denli hızlı bir gelişme içerisinde olması kişisel verilerin ne denli kolay elde edilip kullanılabileceğini bizleri kaygı duymaya sevk edecek derecede göstermektedir. Dolayısıyla yapay zekanın bu şekilde gelişmesinin bir sonucu olarak bireyin kişiliğine yönelik olarak artmış ve bu artışın bir sonucu olarak bireyleri bu tehditlere karşı korumanın yolları devletler tarafından hukuk zemininde aranmaktadır.

Yapay zekâ marifetiyle yukarıda bahsetmiş olduğumuz veriler basit bir biçimde ilişkilendirilebilmekte ve kişiliğe ilişkin anlamlı sonuçlar üretilebilmektedir. Belki de korkutucu olan tüm bu işlemler yapılırken insan müdahalesi olmadan çok kolay bir şekilde yapılabilmesidir. Dolayısıyla gelinen noktada kişinin özerkliğine ve birey olmasından kaynaklı olarak sahip olduğu haklarına karşı ciddi tehditlerin oluşabileceğini ifade edebiliriz.

Zira bireyin yaşamına yönelik çıkarsamaların sayısal verileri değerlendiren teknolojik ürünlere bırakılması insanın özneden objeye dönüşmesi söz konusu olabilecektir.

Yaşanan bu teknolojik gelişmelere paralel olarak artış gösteren, veri işleme faaliyetlerine bağlı olarak, bireylerin verilerinin basit bir şekilde elde edilebilmesi, hiçbir sınırlama olmadan toplanabilmesi ve kişi veya kurumlara transfer edilebilmesi ihtimallerine karşın kişinin korunması kamu kurum ve kuruluşları ve özel sektör tarafından amaçlanmaktadır. Çünkü teknolojik gelişimin bireylere sunmuş olduğu imkanlar olmakla birlikte belirli riskleri de beraberinde getirdiğini söyleyebiliriz. Tahmin dahi edilemeyen bu hızlı gelişimden kaynaklı olarak oluşan kaos ortamı kişiyi tehlikelere karşı adeta açık hava sahası haline getirdiğini ifade edebiliriz.

Yaşanan teknolojik gelişmeler, özellikle devletlerin ve özel şirketlerin yapay zekâ teknolojisinden faydalanarak kişilere yönelik verilere kolayca ulaşılabilmesi mümkün hale gelmiştir. Dolayısıyla gelinen noktada bir tarafta kişisel verileri her türlü işleme tabi tutulan birey ve bunun karşısında devlet ve özel şirketlerin gücü düşünüldüğünde bireyin aleyhine terazinin dengesinin bozulduğunu ifade edebiliriz. Kişiler lehine terazi dengesinin kurulabilmesi ve kişinin ön plana alınarak yeniden hak temelli gücün sahibi olması gerekmektedir. Zira kişisel verilerin korunması hukukunun, yaşanan bu gelişmelerin eseri olduğunu rahatlıkla söyleyebiliriz.

Teknolojinin bireyleri getirdiği noktaya baktığımızda, yaşadığı hayatın teknolojik ürünlerle her an gözetlendiği ve tabiri caizse maddeye dönüşen kişilere dönüşmemek için teknolojinin bize sunduğu imkanları görmezden gelmeden kişinin özel alanının korunması gerekir. Dolayısıyla amaç teknolojinin bize sunduğu bilgi akışını engellemek olmamalıdır. Verinin üretilmesi, kullanılması ve transfer içinde bulunduğumuz yüzyılın en önemli unsuru olduğunu ifade edebiliriz. Bilgi çağı olarak ifade edebileceğimiz bu dönemde kişisel veriler bakımından birey kesinlikle özerkliğini korumalı ve kendisine ait olan veriler üzerinde karar verme yetkisine sahip olmalıdır. Bahse konu bu hakların korunabilmesi için kişisel veriler bakımından çatışan çıkarların mutlak surette dengelenmesine bağlı olduğunu söyleyebiliriz.

Teknolojikler ürünler sayesinden birbirileri ile ilişkilendirilip çeşitli anlamlı sonuçlar çıkarılan verilerin kullanımı ve kişisel verilerin korunması hukuku arasında hassas ve birey lehine dengenin kurulması gerekmektedir. Zira bilginin modern dünyada en önemli bileşen olduğu günümüzde bireylere ait verilerin korunması elbette çok boyutlu olmak zorundadır. Bu anlamda, öncelikle ekonomik, siyasal ve sosyal yansımalarının bulunduğunu, bunun yanında hukuksal bakımdan ise ceza hukukundan, idare hukukuna, medeni hukuktan ticaret hukukuna kişisel verilerin korunmasına ilişkin ilkelerin temas etmediği alanın neredeyse bulunmadığını söyleyebiliriz.

Kişisel veriler bakımından bireylerin istedikleri özgür bir hareket alanına sahip olması yanında, kişisel tercihleri doğrultusunda demokratik modern toplum hayatının gereklerini yerine getirebilmeleri oldukça önemlidir. Dolayısıyla kişisel verilerin korunması sadece kanun bazında değil daha da ileri gidilerek anayasa bazında korunma sağlanması gereken alan olmuştur. Bu noktadan hareketle, anayasa ve insan hakları bakımından "insan onuru", "bireyin özerkliği", "kişisel verileri üzerinde tasarruf ve verilerinin geleceğini belirleme" gibi çok önemli sayılacak haklar ve kurumlar bakımından kişisel verilerin ele alınarak yasal zemine dayandırılması gerektiği düşüncesi artan bir biçimde dile getirilmiştir. Bu bağlamda yaşanan gelişmelere bakıldığında 1970'li yıllardan itibaren kişisel verilerin korunmasına dair tartışmaların uluslararası platformlarda yapıldığı görülmektedir. Bu tarihten itibaren yaşanan tartışmalar kişisel verilerin korunması bakımından farkındalık oluşturup bu anlamda yasal düzenlemelerin oluşmasına zemin hazırlamıştır. Yaşanan bu tartışmalarda devletlerin öncelikle anayasal seviyede sınırlandırılması planlanmış iken, gelinen noktada kişisel verilere yönelik olarak yapılan yasal düzenlemelerin özel hukuk bireylerini kapsayacak biçimde everildiğini görüyoruz.

Kişisel verilerin korunması ile ilgili tüm süreçleri değerlendirdiğimizde yasal anlamda ilk düzenlemenin, 1980 yılında İktisadi İş birliği ve Kalkınma Teşkilatı tarafından yapıldığını görmekteyiz. Ardından, Kişisel verilerin korunması bakımından temel esasların düzenlendiği "OECD Rehber İlkeler" yayınlandığını bilmekteyiz. Yapılan bu önemli düzenlemenin ardından üye devletler arasında uyum sağlanabilmesi için kurulmuş olan Avrupa Konseyi'nin "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması" na dair 108 sayılı Avrupa Konseyi Sözleşmesi düzenlenmiştir.

Sözleşmede temel amaç üye devletler arasında verilerin korunması anlamında uygulama birliği sağlanması hedeflenmiştir. Bunun dışında kişisel verilerin transferi konusunda standartlar belirlenmiştir. 108 Sayılı Sözleşmenin akabinde üye devletler arasında bulunan mevzuat farklılıklarının giderilmesi, kişisel verileri koruma noktasında ortak standartların oluşturulması ve üye devletler arasında kişisel verilerin sorunsuz bir şekilde dolaşımının gerçekleştirilmesi amacıyla "95/46/AT sayılı Kişisel Verilerin Korunması Yönergesi" kabul edilerek yürürlüğe konulmuştur. En son GDPR yürürlüğe konularak verilerin korunması daha kurumsal bir yapıya kavuşturulması amaçlanmıştır.

Saymış olduğumuz tüm bu düzenlemelerin ortak noktasına baktığımızda, kişisel verilerin toplanması ve kayıt altına alınması süreçlerini zorlaştırıcı yasal tedbirler düzenlendiğini, bu düzenlemeler ile kişisel veriler bakımından herhangi bir zarar oluşmadan önce kişinin verilerinin korunmasının amaçlandığını açıkça ifade edebiliriz. Dolayısıyla kişisel verilerin hangi amaçla işleneceğinin belirli olması gerektiği, ilgili kişinin rıza bildiriminin önemi, özel nitelikli kişisel verilerinin kural olarak yasaklanmasının bu temel düşünceden kaynaklandığını ifade edebiliriz. Temel olarak benimsenen düşünce zorunlu değil ise hiçbir verinin depolanmaması görüşü öne çıkarıldığını görmekteyiz.

Kişisel verilerin korunması anlamında Türk hukuku açısından her ne kadar uyumlaştırma süreci devam ediyor olsa da ne yazık ki bu konuda önemli eksikliklerin olduğunu belirtmek isteriz. Türkiye yukarıda bahsetmiş olduğumuz teknolojik gelişmelerin içinde olmasına rağmen kişisel verilerin korunması açısından yeterli hukuksal korumaların alınmadığını söyleyebiliriz. Zira Türkiye'de kişisel verilerin korunması düzenlemelerinin daha ziyade zarar oluştuktan sonra bu zararların giderilmesi adına neler yapılacağına dair düzenlemelerin yapıldığını görmekteyiz. İfade edildiği üzere, kişisel verilerin korunmasında hedeflenen, en sade hali ile "kişinin verisini kaydetme ve işleme tabi tutma şayet aksini yapacaksan rızasını almak için ara ve haber ver" anlayışı üzerine kurulmuştur.

Çalışmamızın temel konusunu oluşturan, "kişisel veri" Avrupa Birliği'ne üye devletler tarafından düzenlenen 95/46/AT sayılı Yönergesinde "Bireylerin Kişisel Verilerinin İşlenmesi ve Serbestçe Dolaşımı Karşısında Korunmasına İlişkin Yönergenin 2/a maddesinde kişisel veri: "*Bir gerçek kişinin belirli veya belirlenebilir olması, şifre*

numarasına göre ya da psişik, psikolojik, fiziksel, ekonomik, kültürel veya sosyal benliği ifade eden bir veya birden fazla unsura, aidiyeti aracılığıyla doğrudan veya dolaylı olarak teşhis edilebilmesi" anlamında kullanıldığını görmekteyiz. OECD Rehber ilkelerin 1/b maddesinde ise kişisel verinin tanımı "belirli veya kimliği belirlenebilir gerçek ve tüzel kişilere ilişkin bütün bilgiler" şeklinde ifade edilmiştir.

Türk hukuk sisteminde yapılan düzenlemede de KVKK m.3'de kişisel verilerin tanımı yapılmıştır. Yapılan bu tanım GDPR ve Yönergeye paralel olarak uluslararası mevzuattaki kişisel veri tanımının tekrar edildiği görülmektedir. Kişisel veri *"kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilg*i" olarak tanımlandığını görüyoruz. Yapılan tüm tanımlamalara bakıldığında, kişisel verilerin tanımlanması bakımından üç temel unsurun vurgulandığı görülmektedir.

Kişisel verilerin korunması bakımında zamanla bazı verilerin daha fazla korunması gerektiği ihtiyacı hasıl olmuştur. Özleri bakımından kişisel veri niteliğinde olması ile birlikte, daha fazla korunması gereken veri grubuna "*hassas kişisel veri*" olarak ifade edilmiştir. Bu kişisel veriler ayrı bir koruma rejimine tabi tutulduklarını söyleyebiliriz.

Yukarıda detaylı bir şekilde bahsetmiş olduğumuz düzenlemelerde kural olarak özel nitelikli kişisel verilerin işlenmesi yasaklanmış yalnızca istisnai durumlarda izin verildiği görünmektedir. Bahse konu istisnalar, hayati çıkarların korunması, kamuya yararlı ve özel hukuk kişisi tarafından işlenme, iş hukukundan doğan yükümlülüklere uyulması, ilgili kişisel verinin veri sahibi tarafından kamuya açıklanması, yargılama nedeniyle işlenmesi, sağlık nedeniyle işlenmesi, cezalara yönelik işleme ve ilgilinin rızası olarak sıralanabilir.

İlgili bölümde detaylı bir şekilde açıklamaya çalıştığımız kişisel verilerin hukuki niteliği de tartışılan konular arasında bulunmaktadır. Bu tartışmalarda öne sürülen çeşitli görüşler bulunmaktadır. Özel hayatın gizliliği görüşü, insan onuru, bireysel özerklik ve bilgilerin geleceğini belirleme hakkı görüşü, fikri mülkiyet hakkı görüşü ve mülkiyet hakkı görüşü başlıkları şeklinde ifade edilmektedir.

Uluslararası belgelerde ve iç hukukumuzda yapılan düzenlemeler dikkate alındığında kişisel verilerin işlenmesi esnasında dikkate alınması gereken temel esaslar; *"kişisel verilerin işlenmesinde esasa ilişkin ilkeler, kişisel verilerin hukuka ve dürüstlük kuralına uygun işlenmesi, ilgilinin rızasının alınması ilkesi, belli bir amacın bulunması ilkesi, amaca bağlılık ilkesi, orantılılık ve gereklilik ilkesi, verilerin doğruluğu ve güncelliği ilkesi*" olarak sıralanabilir. Bu bağlamda usule ilişkin ilkeler "*veri güvenliği ilkesi, ilgili kişilerin bilgilendirilmesi ilkesi, bilgi edinme, düzeltme, kaldırma, sildirme, engelleme ve itiraz hakkının garanti edilmesi ilkesi, işlem aleniyeti ilkesi, işlemin güvenliği ve gizliliği ilkesi, ön denetim ve zararın tazmin edilmesi ilkesi*" şeklinde sıralayabiliriz.

Kişisel verilerin korunmasına ilişkin sınırlamalar getirilirken dikkate alınması gereken ilkeler bulunmaktadır. Bu ilkelerin dışına çıkıldığında bu hakka ilişkin müdahaleler hakkın kullanılması imkânsız hale getirecek ve keyfilik söz konusu olacaktır. Kamu düzeni ilkesi, demokratik toplum düzeni ilkesi, ölçülülük ilkesi, yapılacak olan sınırlamanın yasa ile yapılması ilkesi ve son olarak hakkın özüne dokunulmaması ilkesi olarak ifade edebiliriz.

Tez çalışmamızda, aydınlatma yükümlülüğünün yerine getirilmemesi kabahati incelenmeye çalışılmaktadır. Bu bakımdan, KVKK "m.18/1-a'ya göre aydınlatma yükümlülüğünü yerine getirmeyenlere, 5.000 Türk Lirası'ndan 100.000 Türk Lirası'na kadar idari para cezası verilir." şeklinde düzenlenmiştir.

"KVKK" m.10'a göre veri sorumlusu veya yetkilendirdiği kişi, kişisel verilerin elde edilmesi sırasında ilgili kişileri, veri işleme faaliyeti hakkında bilgilendirmelidir. Dolayısıyla m.10 ve m.11'de veri sorumlusu veya temsilcisi tarafından veri işleme faaliyeti hakkında verisi işlenen kişilere sunması gereken asgari bilgiler düzenlenmiştir. Bu düzenlemede, veri sorumlusunun ya da temsilcisinin açık kimliği, verilerin hangi amaçla işleneceği, işlenen verilerin kimlere hangi amaçlarla transfer edileceği, kişisel veri toplamanın yöntemi ve hukuki nedenleri ile m.11'de bahsedilen hakları konusunda veri sahibinin bilgilendirilmesi gerekmektedir.

Aydınlatma yükümlülüğünün yerine getirilmemesi kabahati esas olarak "Kişisel Verilerin Korunması Kanunu", Kişisel Verileri Koruma Kurumu tarafından çıkarılan ''Aydınlatma

Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ'' (Aydınlatma Tebliği), "Kabahatler Kanunu" ve bunların yanında "Kişisel Verileri Korumu Kurumu" tarafından düzenlenen ikincil düzenlemeler, yayımlanan çeşitli rehberler ve verilen kararlar ile irdelenmeye çalışılmıştır.

Yapmış olduğumuz çalışmanın ilk bölümünde, kişisel verilerin korunması ihtiyacının ortaya çıkışı, tarihsel gelişimi, kişisel verilerin korunması kavramının hukuki niteliği, uluslararası hukukta kişisel verilerin korunmasına ilişkin temel metinlerden kısaca bahsedilmiştir. Zira bahse konu bilgilerin ayrıntılarına, çalışmamın sınırlarını aşacağı endişesiyle yer verilmediğini belirtmek isterim. Yapılan olduğumuz çalışmanın İkinci bölümünde, kişisel verilere ilişkin genel tanımlar ve kişisel verilerin korunmasında temel unsurlar hakkında bilgilere yer verilmiştir. Üçüncü bölümde ise, kişisel verilerin ceza ve kabahatler hukuku bakımından incelenmesi ve aydınlatma yükümlülüğünün ilkeleri hakkında açıklamalar yapılmıştır. Genel şartları bakımından öncelikle, aydınlatma yükümlülüğünün kaynağı olarak ifade edilen şeffaflık ilkesi hakkında açıklamalarda bulunduk. Kişisel verilerin işlenmesi açısından yapılan mevzuat düzenlemelerinin, uygulama ve politikaların ilgili kişiler tarafından bilinebilir olması şeffaflık ilkesinin karşılığı olarak ifade edilebilir.

Kişisel verilerin işlenme faaliyetinin verisi işlenen kişiler tarafından bilinebilir olması oldukça önemlidir. Zira, ilgili kişiler kendisine ait olan verilerin hukuk kaidelerine ve dürüstlük kaidelerine uygun olarak işlenip işlenmediği konusunda bilgi talep edebilir. Veri işleme faaliyetlerine ilişkin veri sahibine tanınan hak ve sorunluluklarını aktif bir biçimde yerine getirme fırsatı bulabilir. Veri sahibi veya temsilcisinin kişisel verilerin işlenmesi bakımından şeffaflık ilkesinin gereğinin yerine getirilmesi ilgili kişilerin aydınlatılması ile mümkün olacaktır.

Yukarıda açıklamaya çalıştığımız düzenlemelerde görüldüğü üzere aydınlatma yükümlülüğü kavramı düzenlenmemiştir. Dolayısıyla veri sorumlusu veya yetkilendiği kişi, kendisinden talep edilmeden, ilgili kişinin kararını etkileyebilecek ve kişi tarafından bilinmeyen olaylar hakkında kişinin aydınlatılması, aydınlatılma yükümlülüğü olarak ifade edilmektedir.

6698 sayılı Kişisel Korunması Kanunu düzenlemesini incelediğimizde büyük oranda uluslararası düzenlemeler ile paralellik göstermektedir. Zira Kişisel Verileri koruma Kurumu yaptığı çalışmalarda uluslararası alanda kabul görmüş yasal düzenlemelere uyumluluk süreçlerini devam ettirmektedir. Dile getirilen bu yasanın ülkemizde uygulanması ile birlikte tarafı olduğumuz uluslararası anlaşmaların uygulanma fırsatı doğduğu gibi, insan haklarından olan kişisel verilerin korunması kapsamının sınırları belirlenmiş ve bu temel insan hakkının korunması bakımından yasal düzenlemeler yapılmış ve uygulamada sorun çıkabilecek alanlar tespit edilmiştir. Çalışmamızın ilgili bölümlerinde sorun yaşanılan başlıklardan yeri geldikçe bahsedilmiştir. Bu sorunların başında TCK'da suç olarak düzenlenen fiillerin Kişisel Verileri Koruması Kanunu'nda idari para cezasını gerektiren kabahatler olarak ifade edildiğini görmekteyiz. Bu bakımdan Kişisel Verileri Korunması Kanunu m.17'de bireylerin verilerine ilişkin işlenen suçlar açısından TCK'nın m.135 ve m.140 düzenlemelerine göndermede bulunularak verilerin ceza hukuku düzenlemeleri bağlamında korumanın TCK hükümlerine bağlı kalınarak sağlanacağı ifade edilmiştir.

Bir diğer sorunlu konu başlığı, "Kişisel Verilerin Korunması Kanunu" m.22/1-ğ bendi uyarınca Kişisel Verileri Koruma Kurulu'nun Kişisel Verilerin Korunması Kanunu m.18 uyarınca kabahat fiillerine karşılık olarak uygulanacak idari yaptırımlara karar verme yetkisine haiz olduğunu bilmekteyiz. Zira Kişisel Verileri Koruma Kurumu bu yetkisine dayanarak azımsanmayacak kadar idari yaptırım uygulamıştır. Bu bağlamda dikkat çekilmesi gereken nokta, Kabahatler Kanunu m.15/3'de düzenlenen içtima hükmü gereğince tek bir eylem ile aynı anda hem suça ve hem de kabahate karşılık gelmesi bu bakımdan suç ve kabahatler konusunda içtimaının irdelenmesi ihtiyacı hasıl olmuştur. Dolayısıyla burada olması gereken işlenen fiile karşılık hem suç soruşturması hem de idari soruşturma yapılabilmesinin kanun koyucu tarafından düzenlenmesi gerekmektedir. Ancak yapılacak bu düzenlemelerin diğer hukuki düzenlemelere uyumlu hale getirilmesi en az bu sorun kadar önemli olacaktır.

Kişisel verilerin Korunması Kanunu ile birlikte değerlendirildiğinde çelişkilerin bulunduğu Devlet İstihbarat Hizmetleri ve Millî İstihbarat Teşkilâtı Kanunu m.6/b ve 6563 sayılı Elektronik Ticaretin Düzenlenmesi Kanunun çeşitli hükümleri bulunmaktadır. 6563 sayılı

yasanın zımni rızayı kabul ettiği görülmektedir. Ancak hem Anayasa hem de Kişisel Verilerin Korunması Kanunu'nda açıkça ifade edildiği üzere verilerin işlenmesinde veri sahibinin açık rızasının alınması gerektiği hem ulusal hem de uluslararası düzenlemelerde ifade edilmektedir. Dolayısıyla ülkemizde bulunan düzenlemelerin incelenerek Kişisel Verilerin Korunması bakımından uyumlu hale getirilmesi gerektiği kanaatindeyiz. Zira, kişisel verilerin korunması dinamik bir süreç ve bu sürece uyum sağlayabilmek için uyumlaştırma bu sürecin belki de en önemli basamaklarından bir tanesidir.

İlgili bölümlerde anlattığımız üzere kişisel verilerin korunması düzenlemelerinde gerçek kişilerin tüzel kişiler karşısında dezavantajlı olabileceği düşüncesiyle yapılan düzenlemelerde gerçek kişilerin korunması ön plana çıkarılmaktadır. Gerçek kişiler için böyle bir eğilim varken Tüzel Kişiler bakımından ceza ve ticaret kanunları dikkate alınarak koruma sağlandığını ifade edebiliriz. Ancak günümüzde basit sıradan tüzel kişiliklerin yanında makro düzeyde tüzel kişiliklerin bulunduğunu ve bu şirketlerin yapmış olduğu faaliyetleri toplum tarafından takip edilen, itibar edilen hatta toplumu yönlendirebilen kurumsal şirketler haline gelmiştir. Bu tüzel kişilikler öyle bir konuma gelmiştir ki, sadece ticari sır kapsamında verileri ve bilgilerinin korunması mümkün görülmemektedir. Zira bu tüzel kişilikler toplum nezdinde takip edilen, açıklamalarına itibar edilen kurumsal yapılar haline gelmişlerdir. Dolayısıyla kurumsal yapıda olan bu şirketlerin ayakta kalabilmeleri ve faaliyetlerinin devamı için kurumsal itibarlarının korunması oldukça önemli olduğu kanaatindeyiz.

Bilgi ve teknoloji kullanımının zirve yaptığı modern dünyada tüzel kişilere ve özellikle uluslararası şirketlere ait olan verilerin hukuk düzenlemeleri çerçevesinde koruma altına alınması zorunlu bir gerekliliktir. Zira bu tür uluslararası firmaların yegâne sermayesi kişisel veriler olduğunu açıkça ifade edebiliriz.

"KVKK" m.10 ve m.11'de aydınlatma yükümlülüğünde bulunması gereken zorunlu hususlar düzenlenmiştir. 6698 Sayılı düzenleme, Veri Koruma Tüzüğü dikkate alınarak hazırlandığı için büyük oranda paralellik göstermektedir. GPDR m.13'te yapılan düzenlemede, ülkemizde bulunan düzenlemeye göre daha detaylı olarak düzenlendiğini açıkça ifade edebiliriz. Dolayısıyla Kişisel Verileri Koruma Kurumunun vermiş olduğu

kararlar incelendiğinde de Veri Koruma Tüzüğü'nün daha detaylı düzenlendiğini ve karşılaşılan sorunlar bakımından daha tatmin edici çözümler sunduğunu görmekteyiz.

Bireysel verilerin kişiden elde edilmediği durumda, verilerin hangi kaynaktan alındığı, şayet bu veriler kamu kaynaklarından elde edilmiş ise bu durumda kişinin ayrıca açıkça aydınlatılması gerekmektedir. Yapılacak bu aydınlatmanın AB Veri Koruma Tüzüğü'ne paralel bir içerikte olması gerektiği kanaatindeyiz.

6698 Sayılı yasa gereğince, veri sahibi tarafından verilecek rızanın öncelikle özgür iradeyle, belirli bir konuya ilişkin ve bilgilendirmeye dayalı olması gerekmektedir. Bu bakımdan kişisel verisi işlenen kişinin vermiş olduğu rızanın bilgilendirme esaslı olması gerekmektedir. Çünkü, kişinin sadece kendi kararıyla hareket edebilmesi ve açıkça neye rıza gösterdiğini bilmesine bağlı olacaktır. Dolayısıyla kişinin rıza verdiği konu ve sonuçları bakımından detaylı bilgi sahibi olması elzemdir. Tüm bu sebeplerden ötürü ilgili kişi verileri için rıza göstermeden önce, bu kişinin açıkça aydınlatılması gerekmektedir. Aydınlatma yükümlülüğünün hangi zaman aralığında yerine getirildiğinin tespiti bu anlamda önemlidir. Aydınlatma yükümlülüğü, verisi işlenen kişinin talebine bağlı olmaksızın hukuk kaidelerine uygun olarak yerine getirilmesi bir zorunluluktur. Aksi durumda aydınlatma yükümlülüğü bakımından sorumluluk doğacaktır. Bu sorumluluk Kişisel Verilerin Korunması Kanunu'nda kabahat olarak düzenlenmiştir. Veri sorumlusu ya da yetkilendirdiği kişi bakımından düzenlenen aydınlatma yükümlülüğün yerine getirilmemesi kabahati ihmali hareket sonucu işlenebilmektedir. Dolayısıyla burada veri sorumlusunun veya yetkilendirdiği kişinin pasif kalarak, yükümlülüklerini yerine getirmeyerek kabahat söz konusu olup, bu durumda da gerçek ihmali kabahat ifade edebilecektir. Dolayısıyla aydınlatma yükümlülüğünün yerine getirilmemesi kabahati gerçek ihmali kabahat olarak ifade edilecektir. Ayrıca bu kabahat yalnızca veri sorumlusu veya yetkilendirdiği kişi tarafından işlenebildiğinden özgü kabahat olduğunu belirtmek gerekir.

6698 Sayılı yasa bakımından veri sorumluları, gerçek kişiler ya da tüzel kişiler olabilirler. Ancak, elbette tüzel kişilerin kendilerinin kabahat işlemeleri mümkün değildir. Tüzel kişilerin bünyesinde görev yapan gerçek kişilerin, görevleri bakımından işledikleri kabahatlerden dolayı sorumlu tutulabilmeleri söz konusu olacaktır.

Kişisel Verilerin Korunması Kanunu m.18/2'ye göre, veri ihlali kapsamından düzenlenen idari para cezalarının, veri sorumlusu olan gerçek ya da tüzel kişiler bakımından uygulanması gerektiği ifade edilmiştir. Ulusal mevzuatımızda Kişisel Verilerin Korunması Kanunu m.18 ile Kabahatler Kanunu m.8 arasında sorunlu bir alan bulunmaktadır. Kabahatler Kanunu m.8'e göre organ, temsilci veya görevlinin "görevi kapsamında işlemiş olduğu kabahat" kriteri uygulandığında, Kişisel Verileri Koruma Kurulu'nun tüzel kişiler için bir yaptırımın söz konusu olabilmesi için öncelikle gerçek kişi tarafından işlenen kabahatin tespit edilmesi ve söz konusu bu kabahatin gerçek kişinin görev kapsamında işlendiğinin ortaya konulması gerekmektedir. Dolayısıyla bu bakımdan Kişisel Verileri Koruma Kurulu'nun kendisine gelen şikayetlerde titiz ve kapsamlı araştırmalar yapması ve en önemlisi yapmış olduğu araştırmaları kararlarında belirtmesi beklenecektir. Kurulun böyle bir araştırma yapması ve bunu kararlarında belirtmesi ilgili yasal düzenlemenin ruhuna uygun olacak mı veya idari yaptırım olması nedeniyle Kabahatler Kanunu'ndan bağımsız bir yaklaşımda mı bulunmak lazım bunların tartışılması gerekmektedir.

Yapmış olduğumuz çalışma kapsamında, 6 Aralık 2021 tarihinde Berlin Eyalet Mahkemesi önüne gelen bir dava kapsamında, Avrupa Birliği Adalet Divanı'na kişisel veri koruma düzenlemesi konusunda önemli soruları gündeme getirmiştir. İlk olarak GDPR açısından öngörülen bir yaptırım doğrudan şirkete karşı uygulanabilecek mi, gerçek ve kimliği tespit edilebilir bir kişi tarafından işlenmiş kabahatin tespit edilmesi zorunlu mu, şirkete doğrudan yaptırım uygulanabilecekse bu yaptırımın niteliği ne olacak, çalışan tarafından gerçekleştirilen kabahatin tüzel kişiliğe isnat edilmesi kapsamında kusur aranacak mı, ya da kusursuz sorumluluk mu söz konusu olacak bu hayati soruların cevaplarının arandığını görmekteyiz. Berlin Eyalet Mahkemesi önüne gelen bu davada, kişisel veri ihlalinin hangi organ veya çalışan tarafından gerçekleştirildiğinin tespit edilmediği gerekçesiyle verilmiş olan kararı iptal etmiştir. Kararın iptali üzerine Berlin Eyalet Mahkemesi, söz konusu kararı Adalet Divanı'na taşımıştır. Burada özellikle karar açısından aranan, GPDR kapsamında düzenlenen yaptırımlar için kabahatler hukukunda kabul gören kaideler mi öncelikle uygulanmalı yoksa GDPR'ın özerk bir biçimde mi uygulanması gerektiği cevapları aranmaktadır. Berlin Eyalet Mahkemesi özellikle sorumluluğun hukuki niteliğinin açıklığa kavuşturulmasını istemektedir.

Uluslararası düzenlemelerde bu tür soruların cevaplarını aranıyor iken, konu ile ilgili Ülkemizde bulunan ilgili düzenleme m.18/3'e göre, veri sorumlusu kamu tüzel kişiliklerine idari para cezasının uygulanması söz konusu değildir. Bahse konu kabahatlerin, kamu kurum ve kuruluşları ile kamu kurumu niteliğinde ki meslek kuruluşlarında işlenmesi durumunda, bu kuruluşlarda görev yapanlar hakkından para cezası dışındaki disiplin cezası uygulanıp bu disiplin cezalarının sonucunu kurula bildirilmek zorundadır. Disiplin cezasına konu olan aydınlatma yükümlülüğünün yerine getirilmemesi kabahati, kasten ya da taksirle işlenebilir. Aydınlatma yükümlülüğü yerine getirilirken dikkat ve özenli olunmaması durumunda veri sorumlusunun taksirli sorumluluğuna gidilecektir.

Kişisel Verilerin Korunması Kanunu gereğince yalnızca gerçek kişiler kabahat işleyebilirler. Tüzel kişiler bakımından sadece organlarının ya da temsile yetkili kişilerin eylemlerinin bu kişilere yüklenmesi ile kabahat işlemeleri ve bunun neticesinde kabahat kanununa dayalı cezai yaptırımların uygulanması söz konusu olacaktır.

Gerçek kişiler fiil ehliyetini haiz oldukları için kabahat işleyebilirler. Tüzel kişililerde ise ancak organlarının veya temsile yetkili gerçek kişilerin davranışlarının bunlara isnat edilmesi ile kabahat işlemeleri ve dolayısıyla kabahatler kanununa dayalı cezai yaptırıma muhatap olmaları söz konusu olabilir. Ancak yukarıda bahsetmiş olduğumuz Berlin Eyalet Mahkemesi önüne gelen davada, hakkında verilen yaptırım kararında hangi organın eylemlerinin hukuka aykırılığı nedeniyle verildiğine dair bir gerekçe bulunmadığından karar tamamıyla iptal edilmiştir. Bu kararın temelinde yatan tartışma, tüzel kişilerin veri koruma hukukuna aykırı davranışlarından dolayı kabahatler kanunu kaideleri mi esas alınacak veya GDPR kaidelerine uygun mu hareket edilecek soruları tartışılmaktadır. Bu konuda gerek Türk hukukunda gerekse de Uluslararası hukukta net bir durum söz konusu değildir. Kanaatimizce bu kararların tartışılmaya başlanması ile bu konular daha net hale gelecektir. Türk hukuku açısından yapılması gereken bir an önce bütün uyum süreçlerinin tamamlanması ve bu tartışmalar doğrultusunda hazırlıkların yapılması gerekmektedir.

Kabahatler Kanunu m.12' gereğince, ilgili yasal düzenlemede aksine hüküm bulunmaya durumlarda "TCK" nın hukuka uygunluk sebepleri ile kusurluluğu kaldıran sebeplere ilişkin

hükümleri kabahatler açısından da uygulanabilecektir. Bu noktada, "Aydınlatma Tebliği" m.5/1-a ile Kişisel Verilerin Korunması Kanunu'nun aydınlatma yükümlülüğüne ilişkin düzenlemeleri birlikte değerlendirildiğinde aydınlatma yükümlülüğünün verilerin işlendiği her durumda yerine getirilmesinin zorunlu olduğu, bu nedenle kural olarak, aydınlatma yükümlülüğünün yerine getirilmemesi kabahati açısından hukuka uygunluk nedenlerinin uygulanmayacağını bilmekteyiz. Hukuka uygunluk nedenlerinin uygulanmayacağını belirtmemize rağmen KVKK m.28/2'de istisnai düzenleme yapılmıştır. İlgili bölümlerde detaylı olarak bahsetmiş olduğumuz istisnai düzenlemeler gereğince, çeşitli konularda aydınlatma yükümlülüğünün yerine getirilmemesi söz konusu olabilecektir. Ancak KVKK m.28/2 düzenlenen bahse konu istisna durumları GPDR ile birlikte değerlendirildiğinde, hukuka uygun nitelikte olduğunu söylemek mümkün olmayacaktır.

Veri sorumlusunun verisi işlenen kişiye karşı aydınlatılma yükümlülüğüne yerine getirmeyerek iki tür sorumluluğu bulunmaktadır. İhmali hareketten dolayı kabahatten, verileri elde etmesinden kaynaklı olarak da ''verileri hukuka aykırı olarak verme veya ele geçirme'' suçundan ayrı ayrı yaptırıma tabi tutulması söz konusu olacaktır. Dolayısıyla görüldüğü üzere veri sorumlusunun iki farklı fiilinden bahsetmekteyiz.

Son konu başlığımız olan soruşturma zamanaşımı, verilerin elde edilmesi esnasında aydınlatma yükümlülüğünü ifa etmeyen veri sorumlularının ihmali hareketlerinin gerçekleştirilmesiyle birlikte işlemeye başlar. Ancak, kişisel verilerin ilgili kişiden elde edilmediği durumlarda bu veri sahibine karşı aydınlatma yükümlülüğünün makul süre içerisinde yerine getirilmesi gerektiğine ilişkin yasal düzenleme kabahat eyleminin hangi zaman aralığında işlenmiş olduğu belli olmadığından soruşturma zamanaşımın ne zaman başlayacağı bakımından bir belirsizlik olduğu kanaatindeyiz.

Son olarak günümüz teknoloji çağında attığımız her adımda verilerimiz toplanmakta, kullanılmakta ve aktarılmakta bu nedenle karşı karşıya olduğumuz tehlikenin farkında olduğumuzu bilerek bilinçlenmemiz ve bu doğrultuda yaşam alanımızın her alanında verilerimize ilişkin güvenlik tedbiri alınması konusunda talepte bulunmamız en az yasal düzenlemeler kadar önemli olduğunu söyleyebiliriz. Dolayısıyla geldiğimiz noktada, kişinin

mahremiyetinin korunması, değişen dünyanın değişmeyen bir gerçeği olduğunu söyleyerek çalışmamızı tamamlayalım.

REFERANSLAR

(1960, 12 14). Retrieved from oecd: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188

(1968). Retrieved from https://www.parliament.uk/about/living-heritage/transformingsociety/private-lives/relationships/collections1/1968-race-relations/1968-race-relations-act/#:~:text=On%2025th%20October%201968%2C%20the,promoting%20racial%20hatred%20a%20crime

(1968). Retrieved from www.parliament.uk/about/living-heritage/transformingsociety/private-lives/relationships/collections1/1968-race-relations/1968-race-relations-act/#:~:text=On%2025th%20October%201968%2C%20the,promoting%20racial%20hatred%20a%20crime.

(1971). Retrieved from https://law.justia.com/cases/california/supreme-court/3d/4/529.html

(1973). Retrieved from opinioiuris.de: https://opinioiuris.de/entscheidung/3331

(1973). Retrieved from https://opinioiuris.de/entscheidung/3331

(1974). Retrieved from https://www.justice.gov/opcl/privacy-act-1974

(1974). Retrieved from www.justice.gov/opcl/privacy-act-1974

(1975). Retrieved from https://www.legislation.gov.uk/ukpga/1975/65/pdfs/ukpga_19750065_en.pdf

(1975). Retrieved from www.legislation.gov.uk/ukpga/1975/65/pdfs/ukpga_19750065_en.pdf

(1978). Retrieved from https://www.cnil.fr/

(1978). Retrieved from https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000441676

(1985). Retrieved from www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108

(1987). Retrieved from legislationonline.org: https://www.legislationline.org/download/id/3521/file/Case_of_Leander_v_Sweden_1987_en.pdf

(1989). Retrieved from https://ips.ligazakon.net/document/ES015218

(1990, 12 14). Retrieved from refworld.org: https://www.refworld.org/docid/3ddcafaac.html

(1992). Retrieved from http://hudoc.echr.coe.int/eng?i=001-57887

(1996). Retrieved from https://www.garanteprivacy.it/web/garante-privacy-en/home_en

(1997). Retrieved from https://www.dataguidance.com/notes/italy-data-protection-overview

(1997). Retrieved from www.hudoc.echr.coe.int/tur#{%22fulltext%22:[%22\%2222009/93\%22%22],%22

documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-58033%22]}
(1997). Retrieved from www.hudoc.echr.coe.int/tur#{%22fulltext%22:[%2252019/07%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-142673%22]}
(1997). Retrieved from www.dataguidance.com/notes/italy-data-protection-overview
(1998). Retrieved from http://www.gesetze-im-internet.de/englisch_stgb/
(2000). Retrieved from https://hudoc.echr.coe.int/fre#{%22fulltext%22:[%22Amann%20v.%20Switzerland%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-58497%22]}
(2001). Retrieved from www.rm.coe.int/1680080626
(2001). Retrieved from https://www.kisiselverilerinkorunmasi.org/wp-content/uploads/2017/09/GDPR-T%C3%BCrk%C3%A7e-%C3%87eviri-AB-Bakanl%C4%B1%C4%9F%C4%B1.pdf
(2004). Retrieved from www.idare.gen.tr/akillioglu-idariusul.htm
(2005). Retrieved from https://www.legislationline.org/download/id/3316/file/France_Criminal%20Code%20updated%20on%2012-10-2005.pdf
(2008). Retrieved from http//www.tbd.org.trusrimgcdkamubib14raporlarPDFRP2-2008.pdf
(2009). Retrieved from https://www.sciencedirect.com/science/article/pii/S0267364908001696
(2009). Retrieved from www.sciencedirect.com/science/article/pii/S0267364908001696
(2011). Retrieved from https://link.springer.com/content/pdf/10.1007/978-94-007-0674-3.pdf
(2012, 07 10). Retrieved from sol.org.tr: https://haber.sol.org.tr/dunyadan/google-225-milyon-dolar-ceza-odeyecek-haberi-56851
(2012). Retrieved from https://www.legislationline.org/download/id/3316/file/France_Criminal Code updated on 12-10-2005.pdf
(2013). Retrieved from oecd: https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf
(2013). Retrieved from www.coe.int/en/web/portal/28-january-data-protection-day-factsheet
(2014, 05 13). Retrieved from rm.coe.int: https://rm.coe.int/ozelyasam-aile-ceza/16808e940d
(2014). Retrieved from https://curia.europa.eu/juris/liste.jsf?td=ALL&language=en&jur=C,T&num=c-131/12

(2015, 02 17). Retrieved from forbes: https://www.forbes.com/sites/matthewherper/2015/02/17/how-pfizer-is-using-big-data-to-power-patient-care/?sh=573a8d96ceb4
(2015). Retrieved from www.forbes.com/sites/matthewherper/2015/02/17/how-pfizer-is-using-big-data-to-power-patient-care/#60a23635ceb4
(2016). Retrieved from https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf
(2017). Retrieved from finland.fi: https://finland.fi/business-innovation/medicine-world-needs-great-data-finlands-got/
(2017). Retrieved from www.finland.fi/business-innovation/medicine-world-needs-great-data-finlands-got/
(2018). Retrieved from europa.eu:), https://curia.europa.eu/jcms/jcms/j_6/en/
(2018, 04 04). Retrieved from dw.com: https://www.dw.com/tr/facebook-87-milyon-kullan%C4%B1c%C4%B1-etkilendi/a-43258048
(2018, 05 02). Retrieved from ntv.com.tr: https://www.ntv.com.tr/galeri/teknoloji/facebook-skandalinin-merkezinde-yer-alan-cambridge-analytica-sirketi-kapanacagini,gHYfdIZ7rkmn2NcnJW9q7A
(2018, 04 11). Retrieved from aa.com.tr: https://www.aa.com.tr/tr/dunya/facebookun-ust-yoneticisi-zuckerberg-abd-senatosunda-ifade-verdi/1114367
(2018, 03 11). Retrieved from newyorker.com: https://www.newyorker.com/books/double-take/sunday-reading-the-world-of-adrian-chen
(2018). Retrieved from un.org: https://www.un.org/en/about-us
(2018, 05 18). Retrieved from https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f
(2018, 09 28). Retrieved from https://hudoc.echr.coe.int/tur#{%22fulltext%22:[%2265599/10%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-183947%22]}
(2018). Retrieved from https://kvkk.gov.tr/Icerik/5424/-Ilgili-mevzuatta-ongorulen-veya-islendikleri-amac-icin-gerekli-olan-sure-kadar-muhafaza-edilme-ilkesi-gereginces-kisisel-verilerin-silinmemesi-hakkinda-Kisisel-Verileri-Koruma-Kurulunun
(2018). Retrieved from https://www.kvkk.gov.tr/Icerik/5483/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-Pizza-Restaurantlari-A-S-Domino-s-Pizza-
(2018). Retrieved from https://datenschutz-hamburg.de/assets/pdf/wp260rev01_en.pdf
(2018). Retrieved from www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election
(2018). Retrieved from www.tandfonline.com/doi/abs/10.1080/07481756.1987.12022837
(2018). Retrieved from www.researchgate.net/profile/Ahmet-Oezker/publication/330703883_Financial_Performance_Objective_of_Public_Exp

enditures_in_Last_Period_and_Its_in_Connected_with_Economic_Budget_in_Turkey/links/5c503e9192851c22a3989c81/Financial-Performance-Objectiv
(2018). Retrieved from www.ntv.com.tr/galeri/teknoloji/facebook-skandalinin-merkezinde-yer-alan-cambridge-analytica-sirketi-kapanacagini,gHYfdIZ7rkmn2NcnJW9q7A
(2018). Retrieved from www.aa.com.tr/tr/dunya/facebookun-ust-yoneticisi-zuckerberg-abd-senatosunda-ifade-verdi/1114367
(2018). Retrieved from haber.sol.org.tr/dunyadan/google-225-milyon-dolar-ceza-odeyecek-haberi-56851
(2018). Retrieved from www.newyorker.com/books/double-take/sunday-reading-the-world-of-adrian-chen
(2018). Retrieved from www.rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1
(2018). Retrieved from www.medium.com/@elfkzc/avrupa-konseyinin-108-say%C4%B1l%C4%B1-ki%C5%9Fisel-verilerin-korunmas%C4%B1-s%C3%B6zle%C5%9Fmesi-yenilendi-bc8daad9decc
(2018). Retrieved from www.rm.coe.int/ozelyasam-aile-ceza/16808e940d
(2019). Retrieved from https://kvkk.gov.tr/Icerik/5496/2019-81-165
(2019). Retrieved from www.gesetze-im-internet.de/englisch_stgb/
(2019). Retrieved from www.kvkk.gov.tr/Icerik/5483/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-Pizza-Restaurantlari-A-S-Domino-s-Pizza-
(2021). Retrieved from finland.fi: https://finland.fi/business-innovation/medicine-world-needs-great-data-finlands-got/
(2021). Retrieved from refworld.org: http://www.refworld.org/docid/3ddcafaac.html
(2021). Retrieved from ssrn: https://poseidon01.ssrn.com/delivery.php?ID
(2021, 03 19). Retrieved from coe.int: https://www.coe.int/en/web/conventions/full-list/conventions/treaty/108/signatures?p_auth=gXtFjq5a
(2021, 03 18). Retrieved from coe.int: https://www.coe.int/t/e/legal_affairs/legal_cooperation/data_protection/Default_DP_Day_en.asp#TopOfPa.g.e
(2021). Retrieved from sozluk.gov.tr: http://sozluk.gov.tr
(2021). Retrieved from mevzuat.gov.tr: https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6698&MevzuatTur=1&MevzuatTertip=5
(2021). Retrieved from turkcebilgi.com: https://www.turkcebilgi.com/kamu_hukuku
(2021). Retrieved from https://www.kvkk.gov.tr/Icerik/7168/2021-1324
(2022). Retrieved from oecd: https://www.oecd.org/
(2022). Retrieved from Council of Europe: https://www.coe.int/t/e/legal_affairs/legal_cooperation/data_protection/Default_DP_Day_en.asp#TopOfPa.g.e
(2022). Retrieved from coe.int: https://www.coe.int/en/web/conventions/full-list/
(2022). Retrieved from kvkk: https://kvkk.gov.tr/

(2022). Retrieved from ADALET BAKANLIĞI İNSAN HAKLARI DAİRESİ BAŞKANLIĞI: https://inhak.adalet.gov.tr/
(2022). Retrieved from rm.coe.int: https://rm.coe.int/1680080626
(2022). Retrieved from https://search.coe.int/cm/pages/result_details.aspx?ObjectId=090000016807c65bf
(2022). Retrieved from https://hudoc.echr.coe.int/fre#{%22fulltext%22:[%22Amann%20v.%20Switzerland%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-58497%22]}
(2022). Retrieved from https://hudoc.echr.coe.int/tur#{%22fulltext%22:[%22\%2222009/93\%22%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-58033%22]}
(2022). Retrieved from apple: https://support.apple.com/tr-tr/guide/security/welcome/web
(2022). Retrieved from https://www.kvkk.gov.tr/Icerik/2032/Veri-Sorumlusu-Kimdir
(2022). Retrieved from cnil.fr: https://www.cnil.fr/
(2022). Retrieved from legifrance.gouv.fr: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000441676/
(2022). Retrieved from gesetze-im-internet.de: https://www.gesetze-im-internet.de/englisch_gg/
(2022). Retrieved from germanlawarchive.iuscomp.org: https://germanlawarchive.iuscomp.org/
(2022). Retrieved from https://www.garanteprivacy.it/web/garante-privacy-en/home_en
(2022). Retrieved from http://sozluk.gov.tr/
(2022). Retrieved from https://ec.europa.eu/info/policies/justice-and-fundamental-rights_en
(2022). Retrieved from https://ico.org.uk/media/fororganisations/documents/1554/determining-what-is-personaldata
(2022). Retrieved from https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6698&MevzuatTur=1&MevzuatTertip=5
(2022). Retrieved from https://edpb.europa.eu/about-edpb/more-about-edpb/article-29-working-party_en
(2022). Retrieved from ico.org.uk: https://ico.org.uk/media/about-the-ico/policies-and procedures/1873/section_10_guidance_for_staff.pdf
(2022). Retrieved from https://www.kvkk.gov.tr/Icerik/5388/Madde-ve-Gerekcesi-ile-Kisisel-Verilerin-Korunmasi-Kanunu-Bilgi-Notu-ve-Kisisel-Verilerin-Korunmasina-Iliskin-Terimler-Sozlugu

ABAD. (2014). *C-11/12 sayılı T.13/05/2014 kararı, (çevrimiçi)*. Retrieved from https://rm.coe.int/ozelyasam-aile-ceza/16808e940d

Akgül, A. (2013). Kişisel Verilerin Korunması Açısından İdarenin Hukuki Sorumluluğu ve Yargısal Denetimi. Kocaeli.

Akıllıoğlu, P. D. (2004, 08). Retrieved from https://www.idare.gen.tr/akillioglu.htm

Aksoy, H. C. (2010). *Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması.* Ankara: Çakmak yayınları.

Aktaş, B. (2017). İnsan Hakları Avrupa Mahkemesi ve Yargıtay Kararları Açısından Özel Hayatın Gizliliğini İhlal Suçu. *İstanbul: Der Yayınları*.

Alina, K. (2009). *"European Union Law".* London and New York: Routledge.Cavendish, Taylor and Francis Group.

Angel, J. C. (2007). *"ComputerLaw, The Law and Regulation of Information Technology", Sixth Edition.* Oxford University Press.

Aral, F. (2011). *Türk Borçlar Hukukunda Kötü İfa.* Ankara: Yetkin.

Aşıkoğlu, Ş. İ. (2018). *Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri.* İstanbul: On İki Levha.

ATAK, S. (2010). AVRUPA KONSEYİ'NİN. *TBB dergisi*.

Atay, E. E. (2013). *Hukuk Başlangıcı.* Ankara: Gazi kitabevi.

AVCI, Y. (2019). Kişisel Verilerin Korunması. *Yayımlanmamış Yüksek Lisans Tezi*. Konya.

Avrupa Veri Koruma Hukuku El Kitabı. (2017). Retrieved from kpveri.com: https://kpveri.com/wpcontent/uploads/2017/07/avrupa Veri Koruma Hukuku El Kitabi.pdf

Aydın, S. E. (2015). *AİHM İçtihatları Bağlamında Kişisel Verilerin Kaydedilmesi Suçu.* İstanbul: On İki Levha.

Aysun, Melike Köse ''Kişisel Verilerin Kaydedilmesi Suçu'', (Yayımlanmamış Yüksek Lisans Tezi), Akdeniz Üniversitesi Sosyal Bilimler Enstitüsü, Antalya, 2018. (n.d.).

Bainbridge, D. (2007). *"Introduction to Informaion Technology Law", Six Edition.* Pearson Longman.

Başalp, N. (2004). *Kişisel Verilerin Korunması ve Saklanması.* Ankara: Yetkin yayınları.

Berrin Akbulut. (2014). *Türk Ceza Kanunu ile Kabahatler Kanununun Genel Hükümlerinin Yaptırım Hükümleri Dışında Karşılaştırmalı Olarak İncelenmesi, 2. Baskı.* Ankara: Adalet.

Börekçi, E. B. (2019). Kişisel Verileri Verme, Yayma veya Ele Geçirme Suçu Yükseklisans Tezi. *Yeditepe Üniversitesi, Sosyal Bilimler Enstitüsü, Kamu Hukuku Anabilimdalı, İstanbul*, s. 26.

Boz, A. (2014). "Kişisel Verilerin Korunması; Türkiye, ABD ve AB Örnekleri", Yayımlanmamış Yüksek Lisans Tezi. Ankara: Polis Akademisi, Güvenlik Bilimleri Enstitüsü.

Briscoe. (1971). Retrieved from https://law.justia.com/cases/california/supreme-court/3d/4/529.html

Bundesanzeiger. (1977, 02 01). *Komplette Ausgabe*. Retrieved from Bundesanzeiger Verlag:

http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl177007.pdf

Burcu Erdinç, ‘‘İdari Yaptırımların Kavramsal Çerçevesi ve Cezai Yaptırımlarla Karşılaştırılması’’. (2012). Ankara Barosu Dergisi.

Bussche, v. d., & Voigt, P. (2017). *Data Protection in Germany.* C.H.BECK.

Büyükay, Y. (2006). *İstenmeden Dünyaya Gelen Çocukların Bakım Eğitim ve Tedavi Giderlerinin Tazmin Edilmesi Sorunu.* İstanbul.

Can, S. (2017). *İdari Para cezası, , yıl:7, sy:29.* s. 417, TAAD .

Carey, P. (2018). *Data Proctection A Practical Guide to UK And EU Law, 5. Baskı,.* İngiltere: Oxford University Press.

CATE, F. H. (1997). Privacy in the Information Age. *Brookings Instution Press, ABD*, s. 32.

Çekin, M. S. (2019). *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku.* İstanbul: On İki Levha yayıncılık.

ÇELİK, S. (2017). Büyük Veri Teknolojilerinin İşletmeler İçin Önemi. *SOCIAL SCIENCES STUDIES JOURNAL (SSSJournal)*.

Cenk, D. (2017). Büyük Veri ve Mahremiyet. *TÜBİTAK 1.Ulusal Bulut Bilişim ve Büyük Veri Sempozyumu B3S17 Sempozyumu Bildiri Kitabı, 2017* (p. 1). TÜBİTAK.

Çetin, A. (2011). “Avrupa Birliği Hukukunda Kişisel Verilerin Üçüncü Ülkelere Aktarılması”. *Kazancı Hakemli Hukuk Dergisi*, 32-35.

Christoph Sobotta, J. K. (2013). "The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR". *International Data Privacy Law*, 222.

Çiğdem, A. Ö. (2019). *Kişisel Verilerin Korunması Hukuku: Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil.* İstanbul : Beta Yayıncılık.

Çokmutlu, M. (2014). "Türk Ceza Hukukunda Kişisel Verilerin Korunması", Yayımlanmamış Doktora Tezi. Kocaeli: Kocaeli Üniversitesi, Sosyal Bilimler Enstitüsü.

Colin, T. (1992). "New European Directions in Data Protection". *Journal of Law, Information and Science*.

Consept of Personal Data. (2018, 05 25). *(11)*. Retrieved 03 01, 2022, from https://edpb.europa.eu/about-edpb/more-about-edpb/article-29-working-party_en

Council of Europe. (1981, 1 28). *Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi*. Retrieved from inhak.adalet.gov.tr: https://inhak.adalet.gov.tr/Resimler/Dokuman/2712020140848108_tur.pdf

Council of Europe. (2014). *"Handbook on European Data Protection Law".* European Union Agency for Fundamental Rights.

Cüneyd Altıparmak, ‘‘Kabahatler Hukukunda Soruşturma Zamanaşımı’’, İstanbul Barosu Dergisi. (2008).

Cunningham, M. (2018). Complying with International Data Protection Law. *University of Cincinnati Law Review Vol.84*. Retrieved from https://scholarship.law.uc.edu/uclr/vol84/iss2/4

Dağ, G. (2011). Kişisel Verilerin Ceza Muhakamesi Hukukunda Delil Olarak Kullanılması, Doktora Tezi. *Marmara Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, İstanbul*, s. 13.

datenschutz.hessen.de. (2021, 1 8). *Geschichte des Datenschutzes*. Retrieved from Der Hessische Beauftragte für Datenschutz und Informationsfreiheit: https://datenschutz.hessen.de/ueber-uns/geschichte-des-datenschutzes

David Towned, S. B. (2004). *"The Data Protection Directive and Medical Research Across Europe".* Burlington: Ashgate Publishing Limited.

Devrim Aydın, Türk Ceza Hukukunda Suça İştirak, Ankara, Yetkin, 2009. (n.d.).

Doğan, S. (2010). *Ceza Hukuku Özel Hükümler, 8. Baskı.* Ankara: Yetkin.

Döner, A. (2006). Kişisel Verilerin Korunması Hakkında Federal Kanun. *Erzincan Binali Yıldırım Üniversitesi Hukuk Fakültesi Dergisi*, 1-13.

Dülger, M. V. (2015). *Bilişim Suçları ve İnternet İletişim Hukuku, 6.Baskı.* Ankara: Seçkin.

Edward J., B. (1964). *"Privacyas an Aspect of Human Dignity: An Answer to Dean Prosser".* 39 N.Y.U. L. Rev. 962.

Eker, B. K. (2007). "Kişilerin İzinsiz Görüntülerinin Alınmasının TCK m. 134 Çerçevesinde Değerlendirilmesi". *DEÜHFD*, 131.

Ekinci, M. (2005). *Anlatımlı-Gerekçeli Kabahatler Kanunu ile İdari Suç ve Cezaları.* Ankara : s. 75.

Erdoğan, O. (2007). *Para Cezaları ve İnfazı, 2. Baskı.* İstanbul : s. 495.

Ersan, Ş. (2009). "Kişisel Verilerin Korunması Kanunu Tasarısı'nın Anayasa ve Türk Ceza Kanunu Hükümleri Çerçevesinde Değerlendirilmesi". *İstanbul Barosu Dergisi*, 1206.

Ersoy, U. (2009). "Bir İnsan Hakları Kavramı Olarak Kişisel Verilerin Korunması", Yayımlanmamış Yüksek Lisans Tezi. Ankara : Gazi Üniversitesi Sosyal Bilimler Enstitüsü.

European Data Protection Board. (2018, 05 25). *Article 29 Working Party*. Retrieved from European Data Protection Board: https://edpb.europa.eu/about-edpb/more-about-edpb/article-29-working-party_en

European Union. (2012). *"Proposal For A Regulation Of The Europeanparliament And Of The Council On The Protection Of İndividuals With Regard To The Processing Of Personal Data And On The Free Movement Of Such Data (General Data Protection Regulation)".* European Commission.

European Union Agency for Fundamental Rights and Council of Europe. (2018, 04). Handbook on European data protection law.

Evans, A. (1981). "European Data Protection Law". *American Journal of Comparetive Law*, 572.

Finlandidya karar. (1997, 02 25). Retrieved from https://hudoc.echr.coe.int/tur#{%22fulltext%22:[%22\%2222009/93\%22%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-58033%22]}

FOIA. (2021). Retrieved from https://www.thoughtco.com/us-government-4133021

Forbes. (2015). Retrieved from forbes: https://www.forbes.com/sites/matthewherper/2015/02/17/how-pfizer-is-using-big-data-to-power-patient-care/#60a23635ceb4

Gaskin. (2018). Retrieved from https://ips.ligazakon.net/document/ES015218

GDPR. (2017). Retrieved from kisiselverilerinkorunmasi.org: https://www.kisiselverilerinkorunmasi.org/wp-content/uploads/2017/09/GDPRT%C3%BCrk%C3%A7e-%C3%87eviri-AB-Bakanl%C4%B1%C4%9F%C4%B1.pdf

Gerrit, H. (2012). "A general data protection regulation for Europe? Light and Shade in the Commission's Draft of 25th January 2012.". *Script-ed 9*, 75.

Gökcan, H. T. (2005). Kabahatler Kanununa Göre İdari Para Cezalarının Uygulanması. *Türk Hukuk Dergisi, S.104, Kasım*, s. 18.

Gözübüyük, A. Ş. (2013). *Hukuka Giriş ve Hukukun Temel Kavramları.* Ankara: Turhan.

Güçlü, Y. (2020). *İdari Para Cezaları ve Diğer İdari Yaptırımlar, 2. Baskı,.* Ankara: s. 94-101.

guidance for staff. (2021). Retrieved from ico.org.uk: https://ico.org.uk/media/about-the-ico/policies-and procedures/1873/section_10_guidance_for_staff.pdf

Gültekin, N. M. (2012). Kişisel Verilerin Ceza Hukuku Yönünden Korunması, Yüksek Lisans Tezi,. *Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, İstanbul* , s.39.

Gürsakal, N. (2017). *Büyük Veri 3. baskı.* Dora yayıncılık.

Gürsel, İ. (2016). "Protection of Personal Data in International Law and The General Aspects of TheTurkish Data Protection Law". *DEÜHF Dergisi*.

Gutwirth S., /. Y. (2008). "The Contribution of the Article 29 Working Party to the construction of a harmonised European data protection system: an illustration of reflexive governance?". *Brussels*, 570-580.

Güven, B. (2010). Hasta Bilgilerinin Gizliliği Prensibi, Yüksek Lisans Tezi. *İstanbul Bilgi Üniversitesi, Sosyal Bilimler Enstitüsü*, s. 48.

Hansen, J.-I. C. (2018, 07 13). Cross-Cultural Research on Vocational Interests. Retrieved 03 04, 2022, from https://www.tandfonline.com/doi/abs/10.1080/07481756.1987.12022837

Hasan Seçkin Ozanoğlu. (2003). ''Hekimlerin Hastalarını Aydınlatma Yükümlülüğü''. *AÜHFD*.

Hayrunisa, Ö. (2009). "Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması" Yayınlanmamış Doktora Tezi. Ankara: Ankara Üniversitesi Sosyal Bilimler Enstitüsü.

Henderson, H. (2006). *Privacy in the Information Age (Library in a Book).* Facts On File.

Hüseyin Murat, Develioğlu, 6698 sayılı Kişisel Verilerin Korunması Kanunun ile Karşılaştırmalı Olarak: Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku, İstanbul, On İki Levha, 2017. (n.d.).

Ian J., L. (2008). *"İnformation Tecnology Law", Fifth Edition.* Oxford: Oxford University Press.

İlhan Özay. (n.d.). İdari Yaptırımlar: Kuramsal Bir Deneme, İstanbul, İstanbul Üniversitesi, 1985.

İnal, E., & Baysal, B. (2008). *Reklam Hukuku ve Uygulaması.* İstanbul : s. 7.

Information Commissioner's Office. (2021). *Determining what is personal data*. Retrieved from https://ico.org.uk/media/fororganisations/documents/1554/determining-what-is-personaldata.pdf

International Working Group on Data Protection in Telecommunications, Working Paper: Childrens' Privacy On Line: The Role of Parental Consent, Adopted at 31st Meeting, Auckland (New Zealand). (2002).

IOS Security. (2021). Retrieved from apple.com: https://www.apple.com/business/docs/site/iOS_Security_Guide.pdf

Kamu Hukuku. (2021). Retrieved from turkcebilgi.com: https://www.turkcebilgi.com/kamu_hukuku

Kangal, Z. (2019). *Kabahatler Hukuku.* İstanbul: On İki Levha,.

Karahisar, T. (2014). Tuba, Karahisar, "Özel Hayatın Gizliliği ve İnternette İşlenen Suçlar". *II. Medya ve Etik Sempozyumu, Medya Kültür İlişkisinde Etik* (p. 599). Elazığ: Fırat Üniversitesi.

Karen, M. (2007). "Data Sensitivity: resolving the conundrum". *Journal of International Commercial Law and Technology*, 12.

KAYA, C. (2011). Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi. *İÜHFM*.

Keklik, R. (2012). *Özel Hayatın Gizliliğini İhlal Suçları.* Ankara: Adalet Yayınevi.

Kenneth, C. (2021, 01 02). *Big Data is Better Data, .* Retrieved from Youtube: https://www.youtube.com/watch?v=8pHzROP1D-w

Ketizmen, M. (2008). *"Kişisel Verilerin Korunması" Tebliğ, (Çevrimiçi), .* Retrieved from http//www.tbd.org.trusrimgcdkamubib14raporlarPDFRP2-2008.pdf

Kılınç, D. (2012). "Anayasal Bir Hak Olarak Kişisel Verilerin Korunması". *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, 1100.

Kişisel Verileri Koruma Kurumu. (2021). Retrieved from KVKK: https://kvkk.gov.tr/

kisiselveri.com. (2021). Retrieved from https://kisiselveri.com/9546ec-turkce

kisiselverilerinkorunmasi.org. (2017). Retrieved from https://www.kisiselverilerinkorunmasi.org/wp-content/uploads/2017/09/GDPR-T%C3%BCrk%C3%A7e-%C3%87eviri-AB-Bakanl%C4%B1%C4%9F%C4%B1.pdf

Korff, D. (2002). *"EC Study on Implementation of Data Protection Directive – Comparative Summary of National Laws".* Cambridge.

Korkmaz, İ. (2016). "Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme". *Türkiye Barolar Birliği Dergisi*, 89.

Kosinski, M. (2018, 06). Retrieved from https://www.researchgate.net/profile/Ahmet-Oezker/publication/330703883_Financial_Performance_Objective_of_Public_Expenditures_in_Last_Period_and_Its_in_Connected_with_Economic_Budget_in_Turkey/

Krause, R. (2011). “New Developmentsin Data Privacy for Employees in German Law”. *The Law in the Information and Risk Society, (Ed. GunnarDuttge/SangWon Lee), Universitäts verlag Göttingen*, 89.

Kuechler/ScottSweeney, F. H. (2002). “Dealing with Data Privacy Protection: An Issue for the 21st Century”. *Law Investigations and Ethics*.

Kuner, C. (2007). *"European Data Protection Law, Corporate Compliance and Regulation", Second Edition.* United Kingdom: Oxford University Press.

Kuner, C. (2021). Kuner, Cristopher. *European Data Privacy Law*, European Data Privacy Law, 13.

Kuşkonmaz, Elif Mendos, ‘‘Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması’’, (Yayımlanmamış Yüksek Lisans Tezi), İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2013. (n.d.).

Küzeci, E. (2010). "Kişisel Verilerin Korunması", Doktora Tezi,. Ankara: Ankara Üniversitesi.

Küzeci, E. (2018, 07 05). Retrieved from https://medium.com/@elfkzc/avrupa-konseyinin-108-say%C4%B1l%C4%B1-ki%C5%9Fisel-verilerin-korunmas%C4%B1-s%C3%B6zle%C5%9Fmesi-yenilendi-bc8daad9decc

Küzeci, E. (2019). *Kişisel Verilerin Korunması.* Ankara: Turhan Kitabevi.

KVKK. (2021). *Veri Sorumlusu Kimdir*. Retrieved from https://www.kvkk.gov.tr/Icerik/2032/Veri-Sorumlusu-Kimdir

Letonya. (2018, 04 29). Retrieved from https://hudoc.echr.coe.int/tur#{%22fulltext%22:[%2252019/07%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-142673%22]}

Levallois, C. A. (2007). *"Data Protection in the European Union".* Bruxelles.

Lucas, B. (2002). "EU Data Protection Policy, The Privacy Fallacy: Adverse Effects Of Europe's Data Protection Policy İn An Information-Dirven Economy". *Computer Law and Security Report*, 33.

Mahmut Koca, İlhan, Üzülmez, Türk Ceza Hukuku Genel Hükümler, 11. Baskı, Ankara, Seçkin, 2018. (n.d.).

Mehmet Semih, G. (2013). *“Ulusalüstü İnsan Hakları Hukukunun Genel Teorisine Giriş”.*

Mesut Serdar, Çekin, ‘‘6698 sayılı Kişisel Verilerin Korunması Hakkında Kanun’un Big Data (Büyük Veri) ve İrade Serbestisi Açısından Değerlendirilmesi’’, İÜHFM, C. LXXIV, S.2, 2016. (n.d.).

Mine Kaya, Elektronik Ortamda (Elektronik Haberleşme-İnternet-Sosyal Medya) Kişilik Hakkının Korunması, Ankara, Seçkin, 2015. (n.d.).

Mine, Kasapoğlu Turhan, ‘‘Sağlık Hizmetlerinde İdarenin Kişisel Verileri Koruma Yükümlülüğü’’, IV. Sağlık Hukuku Kongresi. (2018).

Murat Kayançiçek, Ceza Hukuku ve Kabahatler Hukukunda Zamanaşımı, Ankara. (2014). Adalet.

Nevzat Ali Anı, ‘‘Kişisel Verilerin İşlenmesi ve Açık Rıza’’, (Yayımlanmamış Yüksek Lisans Tezi), İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2018. (n.d.).

Niemietz, Almanya . (1992). *Başvuru No: 13710/88, Tarih: 16.12.1992, (Çevrimiçi),* . Retrieved from http://hudoc.echr.coe.int/eng?i=001-57887

Nilgün, B. (2015). "Avrupa Birliği Veri Koruması Genel Regülasyonu'nun Temel Yenilikleri". *MÜHF*, 92.

OECD. (2018). *Privacy Framework*. Retrieved from OECD: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

OECD. (2021). Retrieved from OECD: http://www.oecd.org

OECD. (2021). *ieconomy*. Retrieved from OECD: https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransbor derflowsofpersonaldata.html

Osman Yaşar, H. T. (2010). *Yorumlu-Uygulamalı Türk Ceza Kanunu, C.III.* Ankara: Adalet.

Otacı, C. K. (2010). *Türk Kabahatler Hukuku.* İstanbul: s. 18.

Özge, Erbek, ''Tüketici Satımlarında Satıcının Sözleşme Öncesi Aydınlatma Yükümlülüğü ve İhlalinin Sonuçları'', (Yayımlanmamış Doktora Tezi), Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü, İzmir, 2010. (n.d.).

Parlar, A. H. (2008). *Türk Ceza Kanunu Yorumu* (Vol. 2). Ankara: s. 2043.

Paul M., S. (1995). "European Data Protection Law and Restrictions on International Data Flows". *IOWA LawReview*, 80.

PEARCE, G., & PLATTEN, N. (1998). Achieving Personal Data Protection in the European Union. *Journal of Common Market Studies*, 529-547.

Peter, C. (2009). "Privacy and Data Protection". *Articles/Data Protection: Backto Basics*.

Raab, C. J. (2004). "The Governance of Privacy Policy Instruments in Global Perspective". *Ashgate Publishing Company, England*, 72.

Rahime, Erbaş, ''Türk Ceza Kanunu'nda Görünüşte İhmali Suçlarda Garantörlük'', (Yayımlanmamış Doktora Tezi), İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2019. (n.d.).

Reid, M. v. (1931, 02 28). Retrieved from https://casetext.com/case/melvin-v-reid

Rezzan İtişgen. (2015). ''Türk Ceza Hukukunda Kişisel Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme Suçu'. *Türkiye Adalet Akademisi*.

Rotaru, Romania, Başvuru No: 28341/95, Tarih: 04.05.2000, (Çevrimiçi), . (2000). Retrieved from http://hudoc.echr.coe.int/eng?i=001-58586

Ruiter, L. B. (2014). "Data and Law: Beyond the Sweat of the Brow: Who Owns Published Data? And What Is Data?". *Journal of Significance*, 29.

Sakine Arık, ''İdari Yaptırımlarda Ölçülülük İlkesi'', (Yayımlanmamış Yüksek Lisans Tezi), Gazi Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, Ankara, 2010. (n.d.).

Salihpaşaoğlu, Y. (2013). "Özel Hayatın Kapsamı: Avrupa İnsan Hakları Mahkemesi İçtihatları Işığında Bir Değerlendirme". *GÜHFD*.

Salihpaşaoğlu, Y. (2013). Özel Hayatın Kapsamı: Avrupa İnsan Hakları Mahkemesi İçtihatları Işığında Bir Değerlendirme. *Gazi Üniversitesi Hukuk Fakültesi Dergisi, Cilt- 17, Sayı 3, Ankara*, s. 228.

Sandra C. Henderson, C. A. (1999). “Personal Information Privacy: Implicationsfor MIS Managers”. *Information & Management*, 214.

Sanem Baykal, İ. G. (2013). *"Avrupa Birliği Hukukunun Kaynakları Bakımından Normlar Hiyerarşisi" Prof. Dr. Erdal Onar'a Armağan,.* Ankara .

Schwartz, D. J. (2006). *"Information Privacy Law".* New York: Apsen Publishers.

Şen, E. (2005). ‘‘5237 sayılı TCK’da Özel Hayata Karşı Suçlar’. *İstanbul Barosu Dergisi*, 717-718.

Sezen, K. I. (2019). Avrupa Veri Koruma Hukukuna Anayasal Bir Bakış, Doktora Tezi. *Marmara Üniversitesi, Sosyal Bilimler Enstitüsü, Kamu Hukuku Anabilimdalı İstanbul*, s. 75.

Şimşek, O. (2008). *Anayasa Hukukunda Kişisel Verilerin Korunması.* İstanbul, İstanbul: Beta Yayınları.

Sınar, H. (2020). Kişisel Verileri Hukuka Aykırı Olarak Verme, Yayma veya Ele Geçirme Suçu (TCK Md. 136). *Kişisel Verileri Koruma Dergisi C.2, S.1,*, 37.

Sprague, L. D. (2011). “Intrusive Monitoring: Employee Privacy Expectations are Reasonable in Europe, Destroyed in the United States”. *Berkeley Technology Law Journal*, 1025.

Steven, S. M.-S., & Anne, T. H. (2014). *"Research Guide to European Data Protection Law".* 42 Int'l J.Legal Info.

Sümeyye Hilal, Ü. (2018). “Medeni Yargılama Hukukunda Kişisel Verilerin ve Sırların Korunması”, Yayınlanmamış Doktora Tezi. Ankara .

T.C. Resmi Gazete. (1969, 04 07). Avukatlık Kanunu. *(sayı: 13168)*.

T.C. Resmi Gazete. (2005, 11 01). Bankacılık Kanunu. *(sayı: 25983)*.

T.C. Resmi Gazete. (2016, 4 7). KİŞİSEL VERİLERİN KORUNMASI KANUNU. *(sayı: 29677)*.

Taştan, F. G. (2017). *TÜRK SÖZLEŞME HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASI.* On İki Levha yayınları.

Tekin, A. (2021). *“İdari Usul ve Kişisel Verilerin Korunması”,.* Retrieved from idare.gen.tr: www.idare.gen.tr/akilliogluidariusul.htm

Tezcan, D. E. (2014). İnsan Hakları El Kitabı . *Seçkin Yayınevi* .

The Guardian. (2021, 05 05). Retrieved from https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Topaloğlu, M. (2005). Bilişim Hukuku. *Karahan Kitabevi, Adana*, s. 166.

Türk Ceza Kanunu, m.135 Gerekçesi, s.88. (n.d.).

Ulusoy, A. (2013). *İdari Yaptırımlar.* İstanbul: s. 9-10.

Uncular, S. (2014). *İş İlişkisinde İşçinin Kişisel Verilerinin Korunması.* Ankara: Seçkin Yayıncılık.

United Nations. (2021). Retrieved from United Nations: https://www.un.org/en/about-un

Ünver, Y. (2008). Kişisel Verilerin Korunması. *Galatasaray Üniversitesi Hukuk Fakültesi, S.1*, s. 175.

Üzeltürk, S. (2004). *1982 Anayasası ve İnsan Hakları Avrupa Sözleşmesine Göre Özel Hayatın Gizliliği Hakkı.* İstanbul: Beta Yayınevi.

Veli Özer Özbek, Koray Doğan, Pınar Bacaksız, İlker Tepe, Türk Ceza Hukuku Özel Hükümler, 11. Baskı. (2017). Ankara: Seçkin.

Vondem Bussche, A. F. (2017). *Data Protection in Germany, 2nd Edition s. 1.* Almanya .

working party. (2021). Retrieved from europa.eu: https://edpb.europa.eu/about-edpb/more-about-edpb/article-29-working-party_en

Working Party on Information Security and Privacy, The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines, 2011. (n.d.).

Yıldırım, R. (2005). İdari Para Cezaları Karşısında Yargısal Korunma. *Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, Konya* , s. 58.

Yıldız, E. T. (2003). İnternet Üzerinde Kişisel Verilerin Korunması. *Marmara Üniversitesi Hukuk Fakültesi, Beta Basım, İstanbul* , s. 817.

Yılmaz, S. S. (2021). Tıp Alanında Kişisel Verilerin Korunması. 133. Retrieved from Yılmaz, Sabire Sanem, Tıp Alanında Kişisel Verilerin Korunması, 2021, s. 133

Yücedağ, N. (2019). ‘‘Kişisel Verilerin Korunması Kanunu” Kapsamında Genel İlkeler’’. *Kişisel Verileri Koruma Dergisi*, 47-63.

Yücel Oğurlu, ‘‘İdari Yaptırımlara Genel Bir Bakış ve İdari Yaptırım-Ceza Yaptırımı Ayrımı’’, AÜ Erzincan Hukuk Fakültesi Dergisi, . (1999).

Z / Finlandiya Karar, 22009/93 (Avrupa İnsan Hakları Mahkemesi 02 25, 1997). Retrieved from https://hudoc.echr.coe.int/tur#{%22fulltext%22:[%22\%2222009/93\%22%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-58033%22]}

[i] Metin, Çokmutlu, Türk Ceza Hukukunda Kişisel Verilerin Korunması", Doktora Tezi, Kocaeli Üniversitesi, Sosyal Bilimler Enstitüsü, Kamu Hukuku Anabilimdalı, Kocaeli, 2014, s. 52.

[ii] Akbulut, a. g. e., s. 400; Artuk, Gökcen, Alşahin, Çakır, a. g. e., s. 378; Akbulut, a. g. e., s. 381.