

**TÜRKİYE CUMHURİYETİ
ANKARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
ÖZEL HUKUK ANABİLİM DALI**

**İNTERNET ORTAMINDA KİŞİSEL VERİLERİN HUKUKA
AYKIRI İŞLENMESİNDEN DOĞAN HUKUKİ SORUMLULUK**

Yüksek Lisans Tezi

Ozan Berkan KARAMAN

Ankara, 2023

**TÜRKİYE CUMHURİYETİ
ANKARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
ÖZEL HUKUK ANABİLİM DALI**

**İNTERNET ORTAMINDA KİŞİSEL VERİLERİN HUKUKA
AYKIRI İŞLENMESİNDEN DOĞAN HUKUKİ SORUMLULUK**

Yüksek Lisans Tezi

Ozan Berkan KARAMAN

**Tez Danışmanı
Dr. Öğretim Üyesi Tuğçe ORAL MANAV**

Ankara, 2023

TÜRKİYE CUMHURİYETİ
ANKARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
ÖZEL HUKUK ANABİLİM DALI

İNTERNET ORTAMINDA KİŞİSEL VERİLERİN
HUKUKA AYKIRI İŞLENMESİNDEN DOĞAN HUKUKİ
SORUMLULUK

YÜKSEK LİSANS TEZİ

Tez Danışmanı
Dr. Öğretim Üyesi Tuğçe ORAL MANAV

TEZ JÜRİSİ ÜYELERİ

Adı ve Soyadı

İmzası

- 1- Prof. Dr. Hasan İŞGÜZAR
- 2- Prof. Dr. Süleyman YILMAZ
- 3- Dr. Öğr. Üyesi Tuğçe ORAL MANAV
- 4-
- 5-

Tez Savunması Tarihi

09.01.2024

T.C.
ANKARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜNE

Dr. Öğretim Üyesi Tuğçe ORAL MANAV danışmanlığında hazırladığım “İnternet Ortamında Kişisel Verilerin Hukuka Aykırı İşlenmesinden Doğan Hukuki Sorumluluk (Ankara.2023) ” adlı yüksek lisans tezimdeki bütün bilgilerin akademik kurallara ve etik davranış ilkelerine uygun olarak toplanıp sunulduğunu, başka kaynaklardan aldığım bilgileri metinde ve kaynakçada eksiksiz olarak gösterdiğimi, çalışma sürecinde bilimsel araştırma ve etik kurallarına uygun olarak davrandığımı ve aksinin ortaya çıkması durumunda her türlü yasal sonucu kabul edeceğimi beyan ederim.

Ozan Berkan KARAMAN

İÇİNDEKİLER

İÇİNDEKİLER	I
KISALTMALAR	VII
GİRİŞ	1

BİRİNCİ BÖLÜM

KİŞİSEL VERİ KAVRAMI VE MEVZUAT

I. KİŞİSEL VERİ KAVRAMI	3
A. Tanım	3
B. Hukuki Niteliğine İlişkin Görüşler	6
1. Hakların Genel Tasnifi	6
2. Mülkiyet Hakkı Görüşü	7
3. Fikri Hak Görüşü	9
4. Kişilik Hakkı Görüşü	10
C. Kişisel Verilerin Unsurları	12
1. Bilgi Unsuru	12
2. Gerçek Kişi ile İlintili Olma	13
3. İlişkili Şahsın Belirliliği veya Belirlenebilirliği	14
D. Kişisel Veri Türleri	15
1. Kişisel Veri – Anonim Veri Mukayesesi	15
2. Özel Nitelikli Kişisel Veri – Genel Nitelikli Kişisel Veri Ayrımı	17

II. KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN

DÜZENLEMELER	18
A. Kişisel Verilerin Korunması İhtiyacı	18
B. Uluslararası Düzenlemeler	21

1. Avrupa Birlięi D�zenlemeleri	21
a. 95/46/EC sayılı Direktifi	21
b. AB Temel Haklar Őartı	22
c. 2002/58 EC Sayılı Elektronik Gizlilik Direktifi	23
d. GDPR	24
2. Dięer D�zenlemeler	26
a. BirleŐmiŐ Milletler Rehber İlkeleri	26
b. OECD Rehber ilkeleri	28
c. Avrupa Konseyi D�zenlemeleri	30
C. Ulusal D�zenlemeler	31
1. Anayasa H�km�	31
2. KVKK	33
3. T�rk Ceza Kanunu	35
4. İnternet Ortamında Yapılan Yayınların D�zenlenmesi ve Bu Yayınlar Yoluyla İŐlenen Su�larla M�cadele Edilmesi Hakkında Kanun	36

İKİNCİ B L M

KİŐSEL VERİLERİN İNTERNET ORTAMINDA İŐLENMESİ

I. İNTERNET ORTAMI	41
A. Tanım	41
B. İnternet Akt�rleri	43
1. İnternet Servis Saęlayıcı	43
a. İnternet Servis Saęlayıcının Dięer Akt�rlerden Ayrılması	43
b. EriŐim Saęlayıcı (Access Provider)	45
c. Yer Saęlayıcı (Hosting Provider)	48
2. İ�erik Saęlayıcılar	51
3. Toplu Kullanım Saęlayıcı	53
4. İnternet Sitesi İŐletmecileri	55
a. İŐletmecilerin Dięer Akt�rlerden Ayrılması	55

b. Sosyal Ağ Sağlayıcı _____	56
II. İNTERNET ORTAMINDA KİŞİSEL VERİLERİN İŞLENMESİ SÜRECİ _____	59
A. Genel Çerçeve _____	59
B. Hâkim İlkeler _____	61
1. Hukuka ve Dürüstlük Kurallarına Uygunluk ve Şeffaflık _____	61
2. Doğruluk ve Güncellik _____	62
3. Belirli, Açık ve Meşru Amaç _____	63
4. İşlenme Amacıyla Bağlantılı, Sınırlılık ve Ölçülü Olma _____	64
5. Gerekli Süre Nispetinde Muhafaza Etme _____	65
III. KİŞİSEL VERİLERİN İŞLENMESİ SÜRECİNDE YER ALAN AKTÖRLER _____	67
A. Veri Sorumlusu _____	67
B. Veri İşleyen _____	69
C. Veri Sorumlusu ve Veri İşleyen Ayrımı Yükümlülüklerin Tespiti _____	70

ÜÇÜNCÜ BÖLÜM

KİŞİSEL VERİLERİN HUKUKA AYKIRI İŞLENMESİ VE BAŞVURU YOLLARI

I. İNTERNET ORTAMINDA KİŞİSEL VERİLERİN İŞLENMESİNDE HUKUKA UYGUNLUK SEBEPLERİ _____	72
A. Açık Rıza _____	72
1. Açık Rıza Kavramı _____	72
2. Açık Rızanın Unsurları _____	75
a. Belirli Bir Konuya İlişkin Olma _____	75
b. Bilgilendirmeye Dayanma _____	76
c. Özgür İrade _____	77
3. İnternet Ortamında Açık Rızanın Geçerlilik Şartları _____	78
a. Açık Rızanın Şekli : Opt-In Opt-Out _____	78

b. Ehliyet _____	79
B. KVKK Kapsamında Diğer Hukuka Uygunluk Sebepleri _____	81
1. Genel Olarak _____	81
2. Genel Nitelikli Kişisel Verilerin İşlenmesinde Diğer Hukuka Uygunluk Sebepleri _____	82
a. Kanunda Açıkça Öngörülmesi _____	82
b. Fiili İmkansızlık Hali _____	84
c. Sözleşme Taraflarının Verilerinin İşlenmesi _____	84
d. Veri Sorumlusunun Hukuki Yükümlülüğünü Yerine Getirmesi _____	87
e. Kişisel Verinin Alenileştirilmesi _____	88
f. Bir Hakkın Tesisi, Kullanılması veya Korunması İçin Zorunluluk _____	89
g. Veri Sorumlusunun Meşru Menfaati _____	90
3. Özel Nitelikli Kişisel Verilerin İşlenmesinin Şartları _____	94
II. KİŞİSEL VERİLERİN HUKUKA AYKIRI İŞLENMESİ _____	97
A. Yaygın Hukuka Aykırılık Halleri _____	97
1. Aktarım _____	97
2. Aydınlatma Yükümlülüğüne Aykırılık _____	98
3. Verilerin Muhafazası ve İmhası _____	100
B. Genel Hukuka Uygunluk Nedenleri _____	101
1. Üstün Kamusal Yarar _____	101
2. Üstün Özel Yarar _____	104
III. KİŞİSEL VERİLERİN HUKUKA AYKIRI İŞLENMESİ HALİNDE BAŞVURU YOLLARI _____	104
A. KVKK Kapsamında Başvuru Yolları _____	104
1. Veri Sorumlusuna Başvuru _____	104
2. Kurula Şikayet _____	106
B. Genel Hükümler Çerçevesinde Başvuru Yolları _____	107
1. Kişilik Hakkını Koruyucu Davalar _____	107

2. Tazminat Davası	108
a. Genel Olarak	108
b. Maddi Tazminat Talebi	110
c. Manevi Tazminat Talebi	112
SONUÇ	115
KAYNAKÇA	122
ÖZET	131
ABSTRACT	132



KISALTMALAR

A.Ş.	Anonim Şirket
AB	Avrupa Birliği
ABAD	Avrupa Birliği Adalet Divanı
ABD	Amerika Birleşik Devletleri
ABTHŞ	Avrupa Birliği Temel Haklar Şartı
ACM	<i>The Association for Computing Machinery</i> – Bilgisayar Derneği
AİHS	Avrupa İnsan Hakları Sözleşmesi
AÜHFD	Ankara Üniversitesi Hukuk Fakültesi Dergisi
AÜSBFD	Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi
AVM	Alışveriş merkezi
AYM	Anayasa Mahkemesi
bknz.	bakınız
BM	Birleşmiş Milletler
C.	cilt
CAN	<i>Campus Area Network</i> – Kampüs Alan Ağı
DEÜHFD	Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi
Direktif	Avrupa Komisyonu’nun 95/46/EC numaralı Direktifi
E.	Mahkeme Dosyası Esas Numarası
E.T.	erişim tarihi
E-Gizlilik	2002/58 EC Sayılı Elektronik Gizlilik Direktifi
EHK	5809 sayılı Elektronik Haberleşme Kanunu
GDPR	2016/679 sayılı GDPR (<i>General Data Protection Regulation</i> - Avrupa Birliği Genel Veri Koruma Tüzüğü)
hk.	Hakkında
HMK	6100 sayılı Hukuk Muhakemeleri Kanunu
İHEB	İnsan Hakları Evrensel Beyannamesi

İMÜHFD	İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi
İSS/ISP	İnternet Servis Sağlayıcı/Internet Service Provider
İÜHFM	İstanbul Üniversitesi Mecmuası
K.	Mahkeme Dosyası Karar Numarası
Kurul	Kişisel Verilerin Korunması Kurulu
Kurum	Kişisel Verilerin Korunması Kurumu
KVKK	6698 sayılı Kişisel Verilerin Korunması Hakkında Kanun
LAN	<i>Local Area Network</i> – Yerel Ağ Şebekesi
MAN	<i>Metropolitan Area Network</i> – Metropol Alan Ağı
m.	madde
MÜHFD	Marmara Üniversitesi Hukuk Fakültesi Dergisi
NetzDG	<i>Netzwerkdurchsetzungsgesetz</i> (Alman Ağ Yaptırım Yasası)
OECD	Ekonomik İşbirliği ve Gelişme Teşkilatı – <i>Organization for Economic Cooperation and Development</i>
s.	sayfa
S.	Sayı
SÜİİBFSEAD	Selçuk Üniversitesi İktisadi ve İdari Bilimler Fakültesi Eğitim ve Araştırma Dergisi
T.C.	Türkiye Cumhuriyeti
TBBD	Türkiye Barolar Birliği Dergisi
TBK	6098 sayılı Türk Borçlar Kanunu
TCK	5237 sayılı Türk Ceza Kanunu
TCKN	Türkiye Cumhuriyeti Kimlik Numarası
TCP/IP	<i>Transmission Control Protocol / Internet Protocol</i>
TMK	4271 sayılı Türk Medeni Kanunu
UMD	Uyuşmazlık Mahkemesi Dergisi
VUK	Vergi Usul Kanunu
WAN	<i>Wider Area Network</i> – Yerel Alan Ağı

GİRİŞ

İnsanlık tarihinde hiçbir zaman kişilere ait bilgileri toplamak, depolamak, analiz etmek, kullanmak, paylaşmak günümüzde olduğu kadar kolay olmamıştır. Dolayısıyla gelişen internet teknolojisinin etkisiyle tarihte bu denli insanlar üzerinde tahakküm kurabilen bir güce de rastlanmamıştır¹.

Başta internet olmak üzere gelişen iletişim teknolojileri, çok çeşitli ve dinamik olanakların günlük hayata girmesini sağlamıştır. İş hayatının da merkezine yerleşen bu olanaklar, iletişim teknolojilerinin temel süjesi olan gerçek kişilerin verilerinin internet ortamında korunmasını daha önemli hale getirmiştir². Bu kapsamda çalışmada kişisel verilerin internet ortamında hukuka aykırı işlenmesi sonucu doğacak hukuki sorumluluk üzerinde durulacak; internetin yapısına bağlı olarak ortaya çıkacak kompleks ve hukuki açıdan tanımlaması zor ilişkiler etüt edilecektir.

Kişisel verilerin işlenmesi son dönem itibarıyla birçok araştırmacı tarafından ele alınan bir konu olmasına karşın; literatürde kişisel verilerin en kolay ve yoğun bir şekilde işlendiği internet ortamı özelinde bir çalışma noksanlığı göze çarpmıştır. Bu kapsamda çalışmada genelden özele bir yaklaşımla kişisel verilerin işlenmesi müessesine ilişkin saptamalar yapılacaktır; bu saptamalardan hareketle internet ortamı özelinde değerlendirmelerde bulunmaya gayret edilecektir.

İnternet ortamında kişisel verilerin işlenmesine ilişkin mevzuat ve doktrin, internetin paylaşımına ve her kullanıcının katkısına açık yapısı nedeniyle çoğunlukla yeni gelişen trendleri karşılama noktasında yetersiz kalabilmektedirler. Bu kapsamda

¹ HARTZOG, Woodrow, “*What is Privacy? That's the Wrong Question*”, The University of Chicago Law Review, C. 88. S. 7, 2021, s. 1682.

² TURAN, Metin, Karşılaştırmalı Hukukta Kişisel Verilerin Korunması, 1. Baskı, Ankara, 2021, s. 41.

alışmada kazuistik bir metottan ziyade somut rnekler zerinden soyut saptamalar yapılarak yeni gelişmesi olası trendlere yönelik doktrine katkı sağlanması hedeflenmektedir.

alışma, internet ortamında gerekleşen kişisel verilerin hukuka aykırı işlenmesinden hukuki sorumluluk ile sınırlandırılmıştır. Bu kapsamda metodolojik olarak öncelikle kişisel veri kavramı üzerinde durulmuştur. İnternet ortamının lke sınırlarıyla baėlı olmayan yapısı göz önünde bulundurularak Türk mevzuatı ve uluslararası düzenlemeler incelenmiştir. AB düzenlemeleri gerek AB üyesi lkelerin iç düzenlemeleri mahiyetinde olması gerekse öngörlen yükmlölüklerin AB sınırları dışına çıkması nedeniyle özellikle üzerinde durulmuştur. alışmanın takip eden kısmında da Türk mevzuatı esas alınmasına karşı uluslararası düzenlemelerle mukayeseli bir alışma tarzı tercih edilmiştir.

alışmanın, kişisel verilerin internet ortamında işlenmesi ile sınırlı tutulması nedeniyle İkinci Bölümde internet ortamı, internet aktörleri üzerinde durularak kişisel verilerin internet ortamında işlenmesi süreçleri alışılmıştır. Hukuki sorumluluėun her iki disiplin bağlamında tayin edilebilmesi için; internet aktörleri ve kişisel verilerin işlenmesi sürecindeki aktörler mukayese edilmiştir.

Kişisel verilerin işlenmesi internet ortamında ele alınarak hukuki sorunlar tespit edildikten sonra son bölümde hukuki sorumluluk üzerinde durulmuştur. alışmamızda, hukuki sorun Medeni Hukuk bağlamında ele alındığından internet ortamında kişisel verilerin işlenmesinden doğan cezai sorumluluk kapsam dışında bırakılmıştır. Kişisel verilerin işlenmesinin hangi durumlarda hukuka aykırı olacağını tayin edebilmek adına kişisel verilerin işlenmesine temel oluşturabilecek başta “açık rıza” olmak üzere hukuki sebepler internet ortamı özelinde incelenmiştir. Son olarak hukuka aykırılık halinde başvurulabilecek yollar belirtilmiştir.

BİRİNCİ BÖLÜM

KİŞİSEL VERİ KAVRAMI ve MEVZUAT

I. KİŞİSEL VERİ KAVRAMI

A. Tanım

“Veri” kelimesi, sözlükte *“bir araştırmanın, bir tartışmanın, bir muhakemenin temeli olan ana öge, muta, done”* ve *“bilgi, data”*³ olarak tanımlanan bir terimdir. Çalışmamızın konusunun en önemli parçasını oluşturan “kişisel veri” sözcük öbeği ise; “kişisel” sıfatı ile kişiye ait bilgi anlamını kazanmaktadır. “Bilgi” kelimesinin *“insan aklının erebileceği olgu, gerçek ve ilkelerin bütünü”* anlamı⁴ göz önüne alındığında; kişisel verinin kişiye ait tüm malumat anlamını taşıdığı belirlenebilir. Nitekim; kişisel verilere ilişkin hukuk sistemimizdeki en temel mevzuat olan 6698 sayılı Kişisel Verilerin Korunması Kanunu (“KVKK”)⁵ m. 4/I-d’de “kişisel veri” kavramı, *“kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi”* şeklinde tanımlanmıştır.

Kişisel veri kavramı, Türk hukuk Sistemine benzer şekilde 2016/679 sayılı GDPR (*General Data Protection Regulation* - Avrupa Birliği Genel Veri Koruma Tüzüğü)’da *“belirli veya belirlenebilir gerçek kişilere ilişkin her türlü bilgi”* olarak tanımlanmıştır. Bunun yanında GDPR’da, *“her türlü bilgi”* ibaresi örnekleme yöntemiyle genişletilmiştir. Gerçek kişinin ismi, kimlik numarası, konum bilgisi ve kişinin fiziksel, psikolojik, genetik, mental, ekonomik, kültürel, sosyal kimliğini belirleyebilecek

³ Türk Dil Kurumu, Güncel Türkçe Sözlük, “Veri” (E.T. 17.08.2022).

⁴ Türk Dil Kurumu, Güncel Türkçe Sözlük, “Bilgi” (E.T. 17.08.2022).

⁵ 6698 sayılı Kişisel Verilerin Korunması Kanunu, R.G. Sayısı 29677, R.G. Tarihi 07.04.2016.

faktörler kişisel veri olarak sayılmıştır⁶. Bu kapsamda kişinin kimliğini belirlemeye yarayacak her türlü biyometrik veri de kişisel veri kapsamındadır⁷.

KVKK m. 2/I'de⁸ kişisel verilerin korunmasının kapsamı belirlenmiştir. Mezkûr hükme göre; tüzel kişilere ait veriler, kişisel veri niteliğini haiz değildir. Buna karşın tüzel kişiler, hukuki işlemlere yönelik iradelerini gerçek kişilerden müteşekkil organlarıyla gerçekleştirebilir⁹. Dolayısıyla verileri kişisel veri kapsamına alınmayan tüzel kişilerin bünyesinde gerçek kişiler bulunabilir. Tüzel kişilere ait veriler doğrudan kişisel veri olarak kabul edilmese de tüzel kişilerin organlarında görev alan gerçek kişilerin, bu görevleri nedeniyle işlenebilecek verileri kişisel veri sayılmalıdır¹⁰.

Kişisel verileri korunan gerçek kişilerin, “gerçek kişilik” halleri ölümle sona ermektedir¹¹. KVKK m. 2/I'de kişisel verilerin kapsamına gerçek kişiler dahil edildiğinden, kural olarak ölüm ile gerçek kişiliği sona ermiş kişilerin verilerinin kişisel veri kabul edilmeyeceği belirtilebilir. GDPR Gerekçesi m. 27'de sarahaten ölü kişilerin verilerinin düzenleme kapsamına girmeyeceği belirtilmiştir¹². Buna karşın; AB üyesi

⁶ Kişisel veri sahibi kavramları GDPR m. 4'te tanımlanmıştır: “*Kişisel veri*” tanımlanmış veya tanımlanabilir bir gerçek kişiye ilişkin her türlü bilgidir (‘veri sahibi’); tanımlanmış bir gerçek kişi özellikle bir isim, kimlik numarası, konum verileri, çevrim içi tanımlayıcı ya da söz konusu gerçek kişinin fiziksel, fizyolojik, genetik, ruhsal, ekonomik, kültürel veya toplumsal kimliğine özgü bir ya da daha fazla sayıda faktöre atıfta bulunularak doğrudan veya dolaylı olarak tanımlanabilen bir kişidir.

⁷ GUERRA, Ana Isabel/MACHADO, Maria Joao/FERNANDES, Maria Malta/AZEVEDO, Patricia Anjos/ TOMAS, Sergio Tenreiro/MACHADO, Susana Sousa, “*General Data Protection Regulation (GDPR): Legal, Ethic and Other Issues, Especially in COVID-19 Time*”, The Law, State and Telecommunications Review, S. 13, 2021, s. 32.

⁸ KVKK m. 2/I: “*Bu Kanun hükümleri, kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında uygulanır.*”

⁹ KAYIHAN, Şaban, Kişiler Hukuku, 1. Baskı, 2022, s. 50-51.

¹⁰ KORKMAZ, İbrahim; Kişisel verilerin Korunması Kanunu Hakkında Bir Değerlendirme, TBBD, S. 124, 2016, s. 91.

¹¹ KAYIHAN, s. 22.

¹² GDPR Gerekçe m. 27: “*Bu düzenleme ölmüş kişilerin verilerine uygulanmaz. Üye Devletler, ölmüş kişilerin kişisel verilerinin işlenmesine ilişkin düzenleme yapabilirler.*”

ülkelerde dahi GDPR'dan farklı düzenlemeler yer almaktadır. Fransa'nın 06/01/1978 tarihli, 78-17 sayılı "*Bilgi Teknolojileri, Veri Dosyaları ve Medeni Haklar Yasası*" m. 84-86'da¹³ ölmüş kişilerin verileri koruma kapsamına alırken; İspanya'nın 05/12/2018 tarihli ve 3/2018 sayılı "*Kişisel Verilerin Korunması ve Dijital Hakların Güvence Altına Alınması Temel Yasası*" m. 3¹⁴'te de ölen kişinin yakınları için veri sorumlusuna başvuru hakkı öngörülmüştür.

Hukukumuzda "kişinin hatırasına hakaret" başlıklı bir suç düzenlenerek¹⁵ cezai anlamda ölen kişinin korunması göz önüne alındığında, ölen bir kişinin verilerinin hukuki açıdan da korunmayı hak ettiğini belirtmek mümkündür. Öte yandan ölen kişinin verilerin hukuka aykırı işlenmesinin yakınları açısından üzüntü oluşturma söz konusu olabilir. Bu kapsamda tarafımızca Türk Medeni Kanunu ("TMK") m. 24¹⁶ ve Türk Borçlar Kanunu

GDPR Gereççeleri İngilizce metni için bkz: <https://gdpr-info.eu/recitals/no-27/>, E.T. 10/01/2023.

¹³ Fransız Veri Koruma Yasasının resmi olmayan İngilizce çevirisi için bkz: https://www.dataguidance.com/sites/default/files/france_data_protection_act.pdf E.T. 10/01/2023.

¹⁴ İspanyol Veri Koruma Yasası'nın İspanyolca metni için bkz: <https://www.boe.es/boe/dias/2018/12/06/pdfs/BOE-A-2018-16673.pdf>, E.T. 02/12/2023, Ölen kişilerin verisine ilişkin m. 3/I hükmünün resmi olmayan çevirisi : "*Ölen kişiyle ailevi veya fiili nedenlerle bağlantısı olan kişiler ve ayrıca bakmakla yükümlü olan kişiler şu amaçlarla veri sorumlusu ile iletişime geçebilir: Ölen kişinin kişisel verilerine erişim talep etmek, gerekli hallerde bunların düzeltilmesini veya silinmesini talep etmek.*"

¹⁵ 5237 sayılı TCK m. 130: "*Bir kimsenin öldükten sonra hatırasına en az üç kişiyle ihtilat ederek hakaret eden kişi, üç aydan iki yıla kadar hapis veya adli para cezası ile cezalandırılır. Ceza, hakaretin alenen işlenmesi halinde, altıda biri oranında artırılır.*"

¹⁶ TMK m. 24: "*Hukuka aykırı olarak kişilik hakkına saldırılan kimse, hâkimden, saldırıda bulunanlara karşı korunmasını isteyebilir. Kişilik hakkı zedelenen kimsenin rızası, daha üstün nitelikte özel veya kamusal yarar ya da kanunun verdiği yetkinin kullanılması sebeplerinden biriyle haklı kılınmadıkça, kişilik haklarına yapılan her saldırı hukuka aykırıdır.*"

(“TBK”) m. 58¹⁷ kapsamında ölen kişinin verilerin hukuka aykırı işlenmesinden hukuki sorumluluk doğacağı değerlendirilmektedir¹⁸.

B. Hukuki Niteliğine İlişkin Görüşler

1. Hakların Genel Tasnifi

Kişisel verilerin işlenmesine ilişkin hukuki sorumluluğun isabetli tayin edilebilmesi için öncelikle kişisel veri kavramının hukuki niteliğinin tartışılması gerekmektedir. Kişi, hakları ve borçları haiz olabilen varlıklar olarak tanımlanmaktadır¹⁹. Bu açıdan; “kişisel” sıfatı ile kişiye ait niteliği ortaya konulan kişisel veri kavramının da genel bir ifadeyle hak olduğu kabul edilebilir. Nitekim doktrinde de kişisel verilere ilişkin görüşler kişilik hakkı olduğundan hareketle şekillendirilmiştir²⁰.

Haklar doktrinde farklı boyutlardan tasniflenerek birden çok ayrım altında incelenmektedir²¹. Dolayısıyla hak olarak kabul gören bir olguyu tek bir ayrım üzerinden

¹⁷ TBK m. 58: “Kişilik hakkının zedelenmesinden zarar gören, uğradığı manevi zarara karşılık manevi tazminat adı altında bir miktar para ödenmesini isteyebilir. Hâkim, bu tazminatın ödenmesi yerine, diğer bir giderim biçimi kararlaştırabilir veya bu tazminata ekleyebilir; özellikle saldırıyı kınayan bir karar verebilir ve bu kararın yayımlanmasına hükmedebilir.”

¹⁸ OĞUZ, Sefer, “Kişisel Verilerin Korunması Hukukunun Genel İlkeleri”, Bilgi Ekonomisi ve Yönetimi Dergisi, C. 13, S. 2, s. 125.

¹⁹ YILMAZ, Süleyman/YILDIRIM, Abdülkerim, Medeni Hukuk – I, Ankara, 2021, s. 105; KAYIHAN, s. 19; AYAN Mehmet/AYAN Nurşen Kişiler Hukuku, 8. Baskı, Ankara, 2016, s. 29, KAYIHAN, Şaban/ÜNLÜTEPE, Mustafa, Medeni Hukuk Bilgisi, 4. Baskı, Ankara, 2017, s. 155, ANTALYA, Osman Gökhan/TOPUZ, Murat, Medeni Hukuk Cilt: I, 4. Baskı, Ankara, 2021, s. 157-158.

²⁰ ÖZDEMİR, Hayrünnisa, Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması, 1. Baskı, Ankara, 2009, s. 111, TURAN, s. 46, BASKIN, Onur, Türk Hukuku Bakımından Kişilik Hakkı Kapsamında Kişisel Verilerin Korunması, 1. Baskı, Ankara, 2021, s. 53, AKSOY, Hüseyin Can, Kişisel Verilerin Korunması, Yüksek Lisans Tezi, Ankara, 2008 s. 48; KÜZECİ, Elif, Kişisel Verilerin Korunması, Doktora Tezi, Ankara, 2010, s. 67.

²¹ ANTALYA/TOPUZ, s. 126, Bir görüşe göre haklar ilk olarak “düzenlendikleri hukuk alanı” bağlamında kamu hakları-özel haklar ayrımına tabi tutulur. “Özel haklar” ise “parasal değer taşıyıp taşıyamaması”, “el değiştirip değiştirememeleri”, “herkese karşı ileri sürülüp sürülememeleri”, “şahsen kullanılmalarının zorunlu olup olmaması”, bağımsız olup olmamaları”, kullanılmalarının etkisi” olmak üzere altı ayrım altında tasniflenebilir.

incelemek, hakkı nitelendirme noktasında eksiklik oluşturur. Buna karşın kişisel verilerin ekonomik bir değeri haiz mi olduğu yoksa kişinin tam ve sağ doğumuyla elde ettiği doğal bir hak mı olduğu, kişisel verilerin niteliğine ilişkin doktrinde tartışılan temel sorundur²². Buradan hareketle; kişisel verilerin hukuki niteliğinin tayininde önemli olan nokta malvarlığı değeri taşıyıp taşıyamaması olarak görülmektedir.

Kişisel veriler üzerinden başta İnternet ortamı olmak üzere çeşitli sektörlerdeki büyük aktörler; işleme, profil oluşturma hatta bazen üçüncü şahıslara verilere ivaz karşılığı satma gibi yöntemler ile gelir etmektedir. Amerikan hukuk sisteminde kişisel verilerden ekonomik kazanç elde edilmesi nedeniyle kişisel verilere ekonomik değer biçme cihetine gidilmiştir²³.

Kişisel verilere yönelik görüşler doktrinde mülkiyet hakkı, fikri hak, şahsi hak²⁴ olmak üzere üç başlık altında toplanmıştır. Mülkiyet hakkı ve fikri hak konusu bakımından ekonomik hak grubuna girerken; şahsi hak ekonomik olmayan hak grubundadır. Dolayısıyla, kişisel verilerin mülkiyet hakkı veya fikri hak oluşturduğuna ilişkin görüşleri temelde aynı kategoriye dahil etmek mümkündür.

2. Mülkiyet Hakkı Görüşü

Hakların konularına malvarlığı-şahıs varlığı olarak tasnif edildiği başlık altında mülkiyet hakkı malvarlığı hakkı kabul edilmektedir. Bu kategori altında; malvarlığı hakları “alacak hakları”, “ayni haklar”, “maddi değeri olan yenilik doğurucu haklar”,

Detaylı bilgi için bkz: AYAN, Mehmet/AYAN, Nurşen, Medeni Hukuka Giriş, 12. Baskı, Ankara, 2016, s. 105.

²² KÜZECİ, s. 67.

²³ SAMUELSON, Pamela, “*Privacy As Intellectual Property*”, Stanford Law Review, C. 52, S. 5, 2000, s. 1127.

²⁴ ÖZKAN, Oğulcan, Kişisel Verilerin Korunması, Yüksek Lisans Tezi, Ankara, 2020, s. 24.

“maddi değeri olan fikri haklar” olarak dörtlü bir ayrıma tabi tutulmaktadır²⁵. Çeşitlerinden biri mülkiyet hakkı olan ayni haklar, sahibine eşya üzerinde herkese karşı öne sürülebilen, herhangi bir aracı olmaksızın hakimiyet kurma yetkisi veren haklardır²⁶.

Kişisel verilerin mülkiyet hakkına göre korunacağı görüşü ekseriyetle Amerikan Hukuk sisteminde destek görmektedir. Mülkiyet hakkı görüşüne göre kişisel veri sahibinin, verilerinin ne ölçüde gizli kaldığı ekonomik bir değerle ölçülmüştür. *Pay-for-privacy* (gizlilik için ödeme) tabiri ile kişisel veri sahibi, kişisel verisinin gizlenmesini, işlenmemesini isteyerek, kişisel verisini işleyemeyen kişiyi ekonomik bir değerden mahrum bırakmaktadır²⁷. Nitekim ABD Federal Haberleşme Komisyonu kurallarına²⁸ karşı internet sağlayıcılar kişisel verilerinin işlenmesini kabul eden kullanıcılara daha hızlı bir internet deneyimi sunulması veya kişisel verilerinin işlenmesini kabul etmeyen kullanıcıların daha fazla ücret ödemesi gibi usullerin uygulanabilirliğini denemiştir²⁹. Kişisel verileri, mülkiyet hakkı temelinde ele alan benzer uygulamalar ile “kişisel veri ekonomisi” kavramı oluşmuştur³⁰. Nitekim bu kavram ile kişisel veriler, piyasa değeri olan bir ürün gibi ele alınmakta kişisel veri sahibi kullanıcılar ise verilerinin ne ölçüde paylaşılacağına ilişkin izin vermek suretiyle bir ekonomide süje niteliğini kazanmaktadır.

Mülkiyet hakkı, sahibine belirli bir şey üzerinde kullanma, yararlanma ve tasarrufta bulunma hakkı verdiğinden, kişisel verilerin üzerinde tasarrufta bulunulması

²⁵ YILMAZ/YILDIRIM, s. 128; OĞUZMAN, M. Kemal/BARLAS, Nami, Medeni Hukuk - Giriş – Kaynaklar - Temel Kavramlar, 22. Baskı, İstanbul, 2016, s. 125; BİLGE, Necip, Hukuk Başlangıcı, 35. Baskı, Ankara, 2017, s. 215.

²⁶ ÜNAL, Mehmet/BAŞPINAR, Veysel, Şekli Eşya Hukuku, 10. Baskı, Ankara, 2021 ,s. 59 vd.

²⁷ ELVY, Stacy-Ann, “*Paying For Privacy and The Personal Data Economy*”, Columbia Law Review, C. 117, S. 6, 2017, s. 1385.

²⁸ ABD Federal Düzenlemeler Yasası’nın 47/I başlığı altında düzenlenen Federal Haberleşme Komisyonu, 02/11/2016 tarihinde “*Genişbant Kullanıcılarının Gizliliğinin Korunması*” başlığı altında kararlar yayımlamıştır.

²⁹ ELVY, s. 1373.

³⁰ BAŞALP, Nilgün, Avrupa Birliği Veri Koruması Genel Regülasyonu’nun Temel Yenilikleri, MÜHFD, C. 21, S. 1, 2015, s. 78.

hususun incelenmesi gerekir. Tasarruf yetkisi, bir hakkı doğrudan etkileyerek sınırlayabilecek, değiştirebilecek, ortadan kaldıracabilecek işlem yapabilmeyi ifade etmektedir³¹. Kişisel veri sahibi, KVKK m. 5/I uyarınca kişisel verilerinin işlenmesine izin verme yetkisini haiz olmasına karşın; kişisel verilerini devretme veya yok etmesi fiilen mümkün değildir. Bu durumda kişisel veriler üzerinde tasarruf etme yetkisinin varlığından söz edilemeyeceğinden, mülkiyet hakkı görüşü isabetli görünmemektedir.

3. Fikri Hak Görüşü

Fikri haklar; hakların konularına göre ayrımında malvarlığı kategorisi altında yer almaktadır. Fikri hak kavramı, fikri ürünler üzerinde kurulan mutlak hakları tanımlamaktadır³². Fikri ürünler maddi niteliği haiz olmayıp düşünme marifetiyle yaratılır. Fikri ürünlerin maddi niteliği haiz olmaması hususu; fikri ürünün somut dünyada var olmamasını değil, ürünün somut dünyadaki varlığından ibaret olmamasını açıklamaktadır. Örneğin; bir ressamın çizdiği yağlı boya tablosunda fikri ürün icra edilen sanat faaliyeti neticesinde ortaya çıkan özgün çalışmadır. Resmin üzerine çizildiği tuvalin somut dünyada var olması, çizilen resmin maddi niteliği olmayan fikri bir ürün olma vasfını etkilemeyecektir. Kişisel verilen fikri hak oluşturduğu görüşünün savunulabilmesi için öncelikle kişisel verilerin fikri ürün niteliğini haiz olması gerekmektedir.

Hukukumuzda fikri ürünler 5846 sayılı Fikir ve Sanat Eserleri Kanunu (FSEK)'nin m. 2 ile m. 7 arasında tahdidi olarak sayılmıştır³³. Dolayısıyla Türk Hukuk

³¹ KILIÇOĞLU, Ahmet M., Borçlar Hukuku Genel Hükümler, 26. Baskı, Ankara, 2022, s. 74; AYAN/AYAN, Medeni, s. 112; ANTALYA/TOPUZ, s. 183.

³² DURAL, Mustafa/SARI, Suat, Türk Özel Hukuku Cilt 1 Temel Kavramlar ve Başlangıç Hükümleri, 15. Baskı, İstanbul, 2020, s. 160; KAVAK, Yalçın, Medeni Hukukun Temel Kavram ve Kurumları, 1. Baskı, İstanbul, 2019, s. 168.

³³ FSEK m. 2 ile m. 7 arasında düzenlenen “Fikir ve Edebiyat Eserleri” aşağıdaki gibidir:

1. İlim ve Edebiyat Eserleri
2. Musiki Eserleri

sistemine göre fikri ürün kapsamına girmeyen kişisel veriler hukuken fikri hak oluşturmaz. Diğer yandan fikri hakların konusunu insan yapımı ürünler oluştururken; kişisel veriler herhangi bir uğraş vermeksizin kendiliğinden oluşmaktadır³⁴. Kişisel verilerin korunmasında FSEK’te düzenlenen usullerin uygulanamayacağı açıktır.

4. Kişilik Hakkı Görüşü

Kişilik hakkı, hakların konularına göre ayrımında malvarlığı haklarının tersini oluşturmaktadır. Daha önce açıklanan “mülkiyet hakkı” ve “fikri hak” kavramları konuları bakımından kişilik hakkından farklı grupta yer almaktadır. Kişilik hakkı herhangi bir maddi değer taşımayan kişinin manevi dünyasına ilişkin haktır³⁵.

TMK m. 8’e göre hak ehliyeti insan olmakla kazanılır ve insanlar hak ehliyetine sahip olmakla eşit bir şekilde “kişi” sıfatını kazanırlar³⁶. Buradan da anlaşılabileceği üzere kişilik hakkına sahip olmak için insan olmak yeterlidir. Kişisel verilerin oluşması ve üzerinde aidiyet kurulması için de herhangi bir ek unsura ihtiyaç duyulmamaktadır.

Kişisel verilerin korunması hakkının, kişilik hakkının bir parçası olduğunu savunanlar gizlilik temelli bir teori ortaya atmaktadır. Gizlenmeyi temel bir insan hakkı gören Avrupa Birliği Temel Haklar Bildirgesi m. 8/I³⁷ ile de her insanın kişisel verilerinin

3. 3.Güzel Sanat Eserleri

4. Sinema Eserleri

5. İşlenmeler ve Derlemeler

6. Alenileşmiş ve Yayımlanmış Eserler”

Detaylı bilgi için bakınız: KARASU, Rauf/SULUK, Cahit/NAL, Temel, Fikri Mülkiyet Hukuku, 2022, s. 55 vd.

³⁴ PRINS, Corien, “When personal data, behavior and virtual identities become a commodity: Would a property rights approach matter?”, SCRIPTed, C.3, S. 4, 2006, s. 296.

³⁵ OĞUZMAN, M. Kemal/SELİÇİ, Özer/OKTAY ÖZDEMİR, Saibe, Kişiler Hukuku, 21. Baskı, İstanbul, 2022, s. 179; DURAL/SARI s. 170; ANTALYA/TOPUZ, s. 156.

³⁶ ÖZTAN, Bilge, Medeni Hukukun Temel Kavramları, 38. Baskı, 2013, s. 236.

³⁷ AB Temel Haklar Bildirgesi m. 8:

“1) Herkes, kendisine ilişkin kişisel bilgilerinin korunmasını isteme hakkına sahiptir.

korunmasını isteme hakkı olduğu hüküm altına alınmıştır. AB müktesebatına göre; kişisel verilerin gizli kalması hususu, bireyler için menfaatin ötesinde “temel hak” mahiyetinde görülmektedir³⁸.

Fikri hak ve mülkiyet hakkı görüşlerinin her ikisinin de kabulü halinde kişisel verilere maddi bir değer biçilmesi gerekmektedir. Kişisel verileri işleyen taraf dolaylı yoldan maddi bir gelir elde etmesine karşın; kişisel veri sahibi için gizli kalmak maddi değer ile ölçülebilecek bir durum değildir. Diğer yandan üzerinde mülkiyet hakkı ve fikri hak kurulabilecek şeyler devredilebilirken gizli kalma devir işlemine konu edilemez³⁹.

Kişisel verilerin korunmasının yansıması olan gizlilik hakkının devredilemez, maddi değerden yoksun ve herhangi bir müdahale olmaksızın oluşması niteliği nedeniyle kanaatimizce kişisel verilerin korunması, kişilik hakkının parçasıdır. Çalışmanın ilerleyen bölümlerinde de kişisel verilerin işlenmesinden doğan sorumluluk kişilik hakkı ihlali bağlamında incelenmiştir⁴⁰.

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

3) Bu kurallara uyulması, bağımsız bir makam tarafından denetlenecektir.”

³⁸ BERGKAMP, Lucas, “EU Data Protection Policy: The Privacy Fallacy: Adverse Effects of Europe’s Data Protection Policy in an Information-Driven Economy”, Computer Law & Security Review, C. 18, S. 1, s. 33; REMPELL, Scott, “Privacy, Personal Data and Subject Access Rights in the European Data Directive and Implementing UK Statute: Durant v. Financial Services Authority as a Paradigm of Data Protection Nuances and Emerging Dilemmas”, Florida Journal of International Law, C. 18, S. 3, 2006, s. 813.

³⁹ BERGKAMP, s. 33; ANTALYA/TOPUZ, s. 185; AYAN/AYAN, Medeni, s. 108-109.

⁴⁰ bkz: Üçüncü Bölüm.

C. Kişisel Verilerin Unsurları

1. Bilgi Unsuru

KVKK m. 3/I-a’da kişisel veriler “*kimliği belli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi*” şeklinde tanımlanmıştır. Görüldüğü üzere mezkûr hükümde veri kavramının tanımında bilgi ifadesine yer verilmiştir. Bu tanımda yer alan bilgi unsuru incelenmeden evvel veri ve bilgi kavramlarının kapsamını göz önüne alınması gerekmektedir.

“Her türlü bilgi” ifadesi KVKK’de bulunduğu gibi hem Kişisel Verilerin Korunması Direktifi⁴¹ (“Direktif”)’nde hem de GDPR⁴²’da yer almıştır. Her türlü bilgi ifadesi ile her iki düzenlemede de yasa koyucunun kişisel veriyi çok geniş bir kapsamda ele almayı amaçladığını belirtmek mümkündür⁴³. Tanımlardan da anlaşılacağı üzere bilgi ve veri kavramları iç içe geçmiş olup uygun düştüğü ölçüde birbirlerinin yerine kullanılabilir. Öte yandan bilgiyi, verinin işlenmiş hali olarak da tanımlamak mümkündür. Somutlaştırmak gerekirse; veri dünyaya ilişkin salt gözlemler iken, bilgi bu gözlemlerin anlamlı bir bütün oluşturacak şekilde bir araya getirilmesidir⁴⁴. Örneğin; bir şahsın 1 Ocak 2004’te doğmuş olması bir bilgidir. Aynı zamanda belirtilen şahsın 1 Ocak

⁴¹ 24/10/1995 tarihli Avrupa Komisyonu’nun 95/46/EC numaralı Direktifi m. 2’de kişisel veri; “*fiziksel, fizyolojik, zihinsel, ekonomik, kültürel veya sosyal kimliğine özel bir veya daha fazla faktöre veya bir kimlik numarasına atıf başta olmak üzere doğrudan veya dolaylı olarak tespit edilebilen bir tespit edilebilir veya tespit edilmiş gerçek kişiye ilişkin herhangi bir bilgi*” şeklinde tanımlanmıştır.

⁴² Detaylı bilgi için bkz.: Birinci Bölüm, II, B, 1, d.

⁴³ Article 29 Data Protection Working Party, Opinion 4/2007 on the Concept of Personal Data, 2007, s. 6 (Working Party).

⁴⁴ GELLERT, Raphael, “*Comparing Definitions of Data and Information in Data Protection Law and Machine Learning: A Useful Way Forward to Meaningfully Regulate Algorithms?*”, Regulation&Governance, C. 16, S. 1, 2020, s. 159, Detaylı bilgi için bkz.: ZINS, Chaim, “*Conceptual Approaches for Defining Data, Information, and Knowledge*”, Journal of the American Society for Information Science and Technology, C. 58, S. 4, 2007, Eserde, “*Knowledge Map of Information Science*” isimli çalışma altında 45 araştırmacının katılımıyla veri (data), bilgi (information), ilim (knowledge) kavramlarının 130 farklı tanımına yer verilmiştir.

2022 itibarıyla 18 yaşında olduğu bilgisine ulaşılmasını sağlayan bir veridir. Dolayısıyla veri ve bilgi kavramları geçişkenlik arz etmekte olup bu geçişkenlik karşımıza Direktif, GDPR'da ve KVKK'de iki kavramın birbirini tanımlamak için kullanılması olarak çıkar.

Korunma kapsamına giren kişisel veriler tayin edilirken; gizlilik mefhumu önem arz etmemektedir. Nitekim kişisel veriyi oluşturan bilgi gizli olmasa dahi, işlenmesi korumaya tabidir⁴⁵. Bu noktada KVKK'de, GDPR'da veya Direktif'te herhangi bir ayrıma gidilmemiştir. Bir gerçek kişi hakkında işlenecek aleni bilgilerin bir araya gelmesiyle ortaya çıkabilecek bilgi, o kişinin gizli kalmasını isteyebileceği bir bilgi olabilir. Bunun yanında bir kimse, gizli kalma lüzumu hissetmediği bir bilginin zaman içerisinde gizli kalmasını isteyebilir.

Bilginin objektif olması hususu da kişisel veri kapsamına girmesi için önem arz etmez. Söz gelimi; bir kişinin boyu objektif bir bilgi iken, borçlarına sadık olduğu yönünde bir bilgi sübjektiftir. Her iki bilgi de kişisel veri kapsamına girer. Hatta sübjektif bilginin yanında kanıtlanmamış veya yanlış bilgi dahi kişisel veri sayılmaktadır⁴⁶. Kişisel veri sahibi hakkında işlenecek hatalı bilgi, veri sahibine zarar vereceğinden yanlış bilgilerin de kişisel veri kapsamına alınması isabetli görünmektedir.

2. Gerçek Kişi ile İlintili Olma

KVKK'ye göre bir bilginin kişisel veri olarak kabul edilmesi için gerekli şartlardan birisi de “gerçek kişiye ilişkin” olmasıdır. Çoğu zaman bir bilginin gerçek kişiye ait olup olmadığı kolaylıkla ayırt edilebilse de uygulamada ayrık durumlarla da karşılaşılabilir. Bir bilgi, gerçek kişinin kimliği, karakteristik özellikleri veya

⁴⁵ AKSOY, s. 18; TAŞTAN, Furkan Güven, Türk Sözleşme Hukukunda Kişisel Verilerin Korunması, 2. Baskı, İstanbul, 2017, s. 40; ÖZKAN, s. 12.

⁴⁶ Working Party, s. 6.

davranışlarına işaret ediyor veya bu kişinin nasıl değerlendirileceği, muamele göreceğine ilişkin kanıya varılmasına yardımcı oluyorsa gerçek kişi ile ilintili kabul edilmektedir⁴⁷.

Gerçek kişi ile ilintili olma hususunda temelde iki farklı yorum bulunmaktadır. Bunlardan birincisine göre, bilginin gerçek kişinin menfaatini etkilemesiyle; ikincisine göre gerçek kişinin bir bu bilgi ile tanımlanmasıyla bilgi kişiyle ilişkili olma vasfını kazanır⁴⁸. İlk yorum ilişkili olmayı halihazırda oldukça geniş kapsamda tutarken; ikinci yorumda ise kişiyi dolaylı yoldan tanımlayabilecek bilgiler de göz önüne alındığında geniş bir kapsam karşımıza çıkacaktır. Nitekim illiyet bağı yoğun olmayan bir bilgi, başka bilgilerle birleşerek de kişiyi tanımlayabilir. Örneğin; X kişinin düzenli olarak Y adresine gitmesi, X kişiye ait kişisel veridir. Y adresinde hamilelik kursu verilmesi dolaylı yoldan X kişinin hamile olduğu bilgisine ulaşmayı sağlayacaktır. Buna karşın “Y adresinde hamilelik kursu verilmesi” hususunun X kişinin kişisel verisi olarak kabul etmek kişi ile ilişki olma unsurunu çok geniş tanımlamaya sebep olacaktır. Kişiyi doğrudan veya illiyet bağı kurulmak koşuluyla dolaylı yoldan tanımlayan bilgileri ilişkili olarak kabul etmek daha uygulanabilir görünmektedir.

3. İlişkili Şahsın Belirliliği veya Belirlenebilirliği

Kişisel verilerin, belirli veya belirlenebilir gerçek kişiler ile ilişkili bilgiler şeklinde tanımından hareketle; kişisel veriler bağlamında öncelikle kişi kavramının, ardından kişinin belirliliği veya belirlenebilirliğinin üzerinde durmak gerekmektedir.

⁴⁷ Working Party, s. 10.

⁴⁸BOOTH, Sharon/JENKINS, Richard/MOXON, David/SEMMENS, Natasha/SPENCER, Christopher/TAYLOR, Mark/TOWNEND, David, “*What are Personal Data?, A Study Conducted for the UK Information Commissioner*”, The University of Sheffield, 2004, s. 7.

Kişi en genel şekilde haklara ve borçlara sahip olan varlıklar olarak tanımlanabilir. Buna göre kişiler hukuk sistemlerinde öngörülen yetkilerden istifade edip yükümlülükleri yerine getirmektedirler⁴⁹. Kişisel veriler, gerçek kişilerle ilgili bir kavram olup gerçek kişilik, TMK m. 28 uyarınca tam ve sağ doğum ile başlar⁵⁰. Dolayısıyla mal ve kişi topluluklarından ibaret olan tüzel kişiler, belirli veya belirlenebilir kişi kapsamında değildir.

Belirlilik, bir grup içerisinde herhangi bir insanın diğer grup üyelerin ayırt edilebilmesi olarak açıklanmaktadır. Bundan hareketle de belirlenebilirlik; henüz belirlenmemiş fakat eldeki verilerle belirlenmesi mümkün kişiler için kullanılır⁵¹. Dolayısıyla bir bilgiden hareketle herhangi bir kişinin belirlenmesi mümkün değilse, kişisel veriden bahsedilemez. Herhangi bir bilgi, kişiyi doğrudan belirleyebildiği gibi dolaylı yoldan da belirleyebilir. Örneğin; bir kişinin ismi kişiyi doğrudan belirlemeye yararken; telefon numarası, araç plakası dolaylı olarak belirler⁵².

D. Kişisel Veri Türleri

1. Kişisel Veri – Anonim Veri Mukayesesi

Bir bilginin kişisel veri kabul edilebilmesi için belli veya belirlenebilir bir kişi ile ilişkilendirilebilmesi gerekmektedir. Belli veya belirlenebilir bir kişi ile ilişkilendirilemeyen veriler anonim veridir.

⁴⁹ ATAY, Ender Ethem, Hukuk Başlangıcı, 8. Baskı, Ankara, 2020, s. 379.

⁵⁰ TMK m. 28: “*Kişilik, çocuğun sağ olarak tamamıyla doğduğu anda başlar ve ölümle sona erer. Çocuk hak ehliyetini, sağ doğmak koşuluyla, ana rahmine düştüğü andan başlayarak elde eder.*”

⁵¹ Working Party, s. 12.

⁵² Working Party s. 13.

KVKK m. 7/I⁵³'de, kişisel verilerin anonim hale getirilmesi; silinme veya yok edilmeye benzer şekilde kişisel verilerin hukuka aykırı işlenmesinin neticelerini tanzim etme yöntemi olarak öngörülmüştür. Buna karşın; belli bir gerçek kişi ile ilişkisi kesilerek anonimleştirilen bilginin, ilgili kişiyle tekrar ilişkilendirilmesi çoğu zaman mümkün olmaktadır⁵⁴.

Alışlageldik geleneksel yöntemlerle işlenemeyecek hacimdeki veri setleri “*big data*” olarak adlandırılır⁵⁵. Gerçek kişi ile ilişkisi kesilen bilgi çoğu zaman “*big data*”ya özgü yöntemlerle anonim bir şekilde işlenmeye devam etmektedir. KVKK verilerin anonimleştirilerek “*big data*” olarak işlenmesine cevaz verse de anonimleştirilen verilerin ait olduğu gerçek kişilerin kimliğinin, veri uzmanlarınca tespit edildiği somut örnekler mevcuttur⁵⁶. Bu kapsamda; bilgilerin anonimleştirilerek kişisel veri kapsamından çıkarılması süreci dikkatle takip edilmelidir. KVKK m. 5/II-f’de⁵⁷ anonimleştirilen verinin işlenmesine cevaz verilmekle beraber kanun koyucunun anonimleşen verinin tekrar veri analizi ile kişiselleştirilebileceği ihtimalini göz ardı ettiği değerlendirilmektedir. Buna karşın; “*big data*” kapsamına giren anonimleştirilmiş her

⁵³ KVKK m. 7/I “*Bu Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir.*”

⁵⁴ BAROCAS Solon/NISSENBAUM, Helen, “*Computing Ethics Big Data’s End Run Around Procedural Privacy Protetions*”, Communications of the ACM, C. 57, S. 11, 2004, s. 32.

⁵⁵ FERGUSON, Andrew Guthrie, “*Big Data and Predictive Reasonable Suspicion*”, University of Pennsylvania Law Review, C. 163, S. 2, 2015, s. 352.

⁵⁶ ÇEKİN, Mesut Serdar, “*6698 Sayılı Kişisel Verilerin Korunması Hakkında Kanun’un Big Data (Büyük Veri) ve İrade Serbestisi Açısından Değerlendirilmesi*”, İÜHFİM, C. 124, S. 2, 2016, s. 635.

⁵⁷ KVKK m. 5/I “*Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez.*” m. 5/II “*Aşağıdaki şartlardan birinin varlığı halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilen işlenmesi mümkündür:*

...
f) *İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.*”

türlü bilgiyi, kişisel veri kapsamında ele alma; uygulanabilir bir usul olarak görünmemektedir. Örneğin; halka arz edilmiş şirketler, periyodik olarak yatırımcılarına raporlar sunmakta, birçoğu da müşterilere ilişkin anonimleştirilmiş istatistiki veriler olarak karşımıza çıkmaktadır. Bu durum yasal zorunluluk olmasa bile, şeffaflığın, günümüz serbest ekonomilerde güven ortamı oluşması açısından önemi büyüktür. Bu durumda; anonimleştirilerek “big data” kapsamında istatikselsel olarak işlenen verinin, veri uzmanlarınca tekrar kişiselleştirilmesi durumunda sorumluluk oluşmaması hayatın akışına daha uygun düşmektedir.

2. Özel Nitelikli Kişisel Veri – Genel Nitelikli Kişisel Veri Ayrımı

KVKK m. 6’da özel nitelikli kişisel verilere tahdidi olarak yer verilerek bu tür verilerin işlenmesinin ancak “açık rıza” ile mümkün olacağı belirtilmiştir. Hükme göre kişinin “ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri” özel nitelikli kişisel veri olarak sayılmış olup hükmün mefhum-u muhalifinden, sayılanlar dışında kalan bilgilerin genel nitelikli kişisel verileri oluşturacağı anlaşılmaktadır. Dolayısıyla özel nitelikli veriler Kanun’da tahdidi olarak sayıldığından kişisel verilerin işlenmesinde açık rıza, sadece sayılan kişisel veri türlerinde aranır.

Herhangi bir kişisel veriyi oluşturan bilginin özel niteliği haiz olup olmaması, o bilginin kişisel veri sahibi açısından önemini belirlememektedir. Nitekim niteliği itibarıyla genel nitelikli görünen bir veri de işlendikten sonra özel nitelikli verilere ulaşılmasını sağlayabilir⁵⁸. Buna karşın KVKK yürürlüğe girmeden önce yargısal

⁵⁸ KÜZECİ, s. 252.

kararlarda kişisel veriler niteliğine göre “hassas – hassas olmayan” ayrımına tabi tutulmuş, hassas nitelikte kişisel verilere yönelik suçların daha ağır cezalandırılması gerektiği hüküm altına alınmıştır⁵⁹. Mezkûr içtihat ceza hukuku alanına ilişkin olup KVKK m. 6’da özel nitelikli verilerin işlenmesi sürecine ilişkin yalnızca açık rıza zorunluluğu getirilmiş, hukuki müeyyide bağlamında ayrıma gidilmemiştir. Kanaatimizce özel nitelikli verilerin hukuka aykırı işlenmesi; konumuz olan hukuki sorumluluk çerçevesinde genel nitelikli verilere göre farklılık arz etmemelidir.

KVKK’de özel nitelikli kişisel veriler tahdidi olarak sayılmasına karşın, söz konusu kavramın tanımına yer verilmemiştir.

II. KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN DÜZENLEMELER

A. Kişisel Verilerin Korunması İhtiyacı

Hukukun, yalnızca fiziksel dünyada algılanabilen kavramları kapsamına aldığı 19. yüzyıl hukuk sistemlerinde duygu, düşünce ve hislerin de yasal tanınmaya ihtiyaç

⁵⁹ Yargıtay CGK, E. 2014/607, K. 2014/16665, T.07/07/2014 kararında “... Kişisel verilerin ceza hukuku anlamında suç konusu olabilmeleri, hassas kişisel bilgiler (veriler) hariç, şu şekilde bir sınırlamaya tabi tutarak suçta ve cezada kanunilik ve belirlilik ilkesine uymayan hükmü kısmen adaletli bir uygulamaya sokabiliriz. O da suç düzenlemelerinin yer aldığı bölüm başlığından hareketle özel hayata ve hayatın gizli alanına ait olup, kişinin başkaları ile paylaşmadığı ve alenileştirmedığı kişisel bilgiler olarak anlamak gerekir.

Buna göre kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, dernek, vakıf ya da sendika üyeliği, sağlığı veya cinsel hayatı ile ilgili verilerinin kaydı, bir başkasına verilmesi veya ele geçirilmesi bunlar hassas veriler oldukları için mutlak olarak cezai yaptırımlarla korunmaları gereken kişisel verilerdir. Bu kapsamda kişilerle ilgili bilginin; ilgili kişi tarafından alenileştirilmemiş, üçüncü kişilerle paylaşılmamış, bilinmesinin kişinin yaşam şekline, ekonomik ve finansal ve bilişim alanına zarar verme ihtimali bulunan bilgiler olması halinde kişisel verilerle ilgili suçların konusunu oluşturmali. Bunun dışında kalan kişilerle ilgili diğer bilgiler ise ancak kullanılış amacına göre hakaret, dolandırıcılık gibi suçların konusu olmalı ve hukuki ve idari yollarla korunmalıdır. ...”

duyduğuna ilişkin görüşler ortaya atılmıştır. Bu kapsamda gelişen yeni gelişmelere karşı bireyin korunması gerektiği ve bu korumanın “*yalnız kalma hakkı*” çerçevesinde şekillenmesi gerektiği savunulmuştur. Kişisel verilerin korunmasına ilişkin erken dönem görüşüne göre; gazetelerde insanların fotoğraflarının izinsiz yayılması ve gizliliğin ihlal edilmesine hukuki çare gereksinimi duyulmuştur⁶⁰. İrtibat teknolojilerinde gelişmelere bağlı olarak kişisel verilerin korunması hususunun her geçen gün önemi artsa doktrinde kişisel verilerin hukuki zemine oturması ihtiyacına değinilmeye başlanması kitlesel iletişim araçlarının yaygınlaşmasından önceki döneme dayanmaktadır.

Kişisel verilerin korunması ilk olarak 04/11/1950 tarihinde yürürlüğe giren Avrupa İnsan Hakları Sözleşmesi (AİHS) m. 8 hükmü⁶¹ ile yasal açıdan düzenlenmiştir. Nazi döneminde devlet yetkilileri özel hayata ilişkin bilgilere yönelik geniş yetkilerle donatılmıştı. İkinci Dünya Savaşı sona erdikten sonra özel hayata benzer müdahalelerin önüne geçilebilmesi adına AİHS m. 8 hükmü düzenlenmiştir⁶².

Bilgisayar sistemlerinin gelişmesi ve dijitalleşmenin ivmelendiği 20. yüzyılın ikinci yarısından itibaren kişisel verilerin depolanması, aktarılması, kullanılması gibi işlemler oldukça kolaylaşmıştır. Bu durum kişisel veri sahiplerinin korunması için hukuki açıdan yeni düzenlemeler ihtiyacını da beraberinde getirmiştir⁶³.

⁶⁰ WARREN, Samuel D./BRANDEIS, Louis D., “*The Right to Privacy*”, Harvard Law Review, C.4, S. 5, 1890, s. 195.

⁶¹ AİHS m. 8: “*Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.*”

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

⁶² REMPELL, s. 814.

⁶³ GRAHAM, Jonathan P., “*Privacy, Computers and the Commercial Dissemination of Personal Information*”, Texas Law Review, C. 65, S. 7, 1987, s. 1395.

Bilgisayar sistemlerin yaygınlaşması ile kişisel verilerin ortaya çıkış hızı da artmıştır. Her iki yılda bir tüm dünya genelindeki dijital veriler ikiye katlanarak çarpan etkisiyle büyümektedir. 2025 yılına gelindiğinde dijital ortamdaki toplam verinin 163 zetabayt⁶⁴ boyutuna ulaşacağı tahmin edilmektedir⁶⁵. Dolayısıyla kişisel verilerin işleneceği sistemler bu çapta veriyle başa çıkabilmek için daha komplike bir hal alırken verilerin korunmasına ilişkin hukuki düzenlemeler de daha özel bir hal almıştır. Bu kapsamda 1960'lı yıllarda kişisel verileri otomatik işleme sistemleri ortaya çıkmış, bu sistemlerin yaygınlaşmasıyla 1970'li yıllarda kişisel verilerin korunması özelinde hukuki düzenlemeler kabul edilmeye başlamıştır. Nitekim verilerin otomatik bir şekilde işlenmesinin bireyleri, devlet ve diğer tüzel kişiler karşısında güçsüz duruma düşüreceğinden hareketle yasa koyucu veri işleme sistemlerinin denetlenebilir olmasını öngörmüştür⁶⁶. Bu kapsamda ilk düzenleme Almanya Federal Cumhuriyeti'nin Hesse Eyaleti'nde 1970 yılında yürürlüğe girmiş ve bu düzenlemeyi İsveç, Avusturya, Danimarka, Fransa takip ederek 1970'li yıllarda bu ülkelerde kişisel verilerin korunmasına yönelik yasalar yürürlüğe girmiştir⁶⁷.

Bilgisayar sistemlerinin ve internet ortamının yaygınlaşmasıyla kişisel verilerin ülke sınırlarına bağlı kalmaksızın işlenmesinin kolaylaşması durumu ortaya çıkmıştır. Bu durum ise pratikte kişisel verilerin korunmasına yönelik ülke mevzuatlarının yeknesaklaşması ihtiyacını doğurmuştur. Öyle ki; OECD, BM, Avrupa Konseyi, AB gibi

⁶⁴ Zetabayt, bir milyar terabayta tekabül eden bir dijital veri depolama birimidir.

⁶⁵ AKINCI, Ayşe Nur, Büyük Veri Uygulamalarında Kişisel Veri Mahremiyeti, T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı, Yayın No:001, Uzmanlık Tezi, Ankara, 2019, s. 4.

⁶⁶ KÜZECİ, s. 116; GIURGIU, Andra/GERARD Lommel, "A New Approach to EU Data Protection: - More Control over Personal Data and Increased Responsibility", Critical Quarterly for Legislation and Law, C. 97, S. 1, 2014, s. 12.

⁶⁷ GÜRSEL, İlke, "Protection of Personal Data in International Law and the General Aspects of the Turkish Data Protection Law", DEÜHFD, C. 18, S. 1, 2016, s. 38.

çok taraflı uluslararası organizasyonlar çeşitli düzenlemeler ile bu kişisel verilerin korunması ihtiyacını ele almıştır⁶⁸.

B. Uluslararası Düzenlemeler

1. Avrupa Birliği Düzenlemeleri

a. 95/46/EC sayılı Direktifi

Kişisel verilerin korunmasına yönelik düzenlemeler hayata geçirme akımına AB de 1995 yılında yürürlüğe giren 95/46/EC sayılı “*Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Direktifi*” ile dahil olmuştur. Her ne kadar 95/46/EC sayılı Direktif, 2016 yılında GDPR’ın kabul edilmesiyle yürürlükten kalksa GDPR’ın yanı sıra KVKK dahil olmak üzere birçok ülkenin yerel mevzuatını etkilemiştir⁶⁹. “Tüzük” mahiyetinde olan ve üye devletler için tamamen bağlayıcı olan GDPR’ın aksine, AB müktesebatında direktifler; üye devletler için yalnızca ulaşılması istenen sonuç açısından bağlayıcıdır⁷⁰. Direktif ile ulaşılması gereken sonuç düzenlenirken buna hangi usul ve uygulamalarla ulaşılacağı üye devletlerin inisiyatifinde bırakılır.

1980’li yıllarda bilgisayar teknolojilerinin yaygınlaşması kişisel verilerin Avrupa genelinde ticari amaçlarla kullanımını da artırmıştır. 95/46/EC sayılı Direktif ile AB üyesi

⁶⁸ KÜZECİ, s. 118.

⁶⁹ ÖZKAN, s. 53.

⁷⁰ Avrupa Birliği’nin İşleyisi Hakkında Anlaşma m. 288: “*Kurumlar, Birliğin yetkilerinin kullanılması için tüzük, direktif, karar, tavsiye ve görüşler kabul eder. Tüzükler genel uygulama alanına sahiptir. Bütünüyle bağlayıcıdır ve tüm üye devletlerde doğrudan uygulanır.*

Direktifler, muhatap alınan her üye devleti, ulaşılması gerekli sonuçları itibarıyla bağlar, şekil ve yöntem seçimini ise ulusal otoritelere bırakır.

Kararlar bütünüyle bağlayıcıdır. Muhatabı belirtilen bir karar, yalnızca muhatabı için bağlayıcıdır.

Tavsiye ve görüşler bağlayıcı değildir.”

ülkelerde kişisel verilere yönelik “tek pazar” bağlamında farklı uygulamaların önüne geçilmesini sağlamak amaçlanmıştır⁷¹. Ayrıca Direktif’te kişisel verilerin düzenlenmesi iki farklı boyutuyla ele alınmıştır. Üye devletler kişisel verilerin işlenmesi sürecinde başta gizlilik hakkı olmak üzere temel hak ve özgürlükleri muhafaza etmekle mükellef olmanın yanı sıra üye devletler arası veri akışını da engelleyecek tedbirler alamayacaktır⁷². Burada yasa koyucunun, AB’nin temelini oluşturan ekonomik çıkarlar ile kişilik hakları arasında denge kurmaya çalıştığı değerlendirilmektedir. Yürürlükten kaldırılmış olsa da Direktif, AB’nin kişisel verilerin korunması hususuna yaklaşımı açısından önemli bir örnek olarak görülmektedir.

b. AB Temel Haklar Şartı

AB’nin yargı organı olan Avrupa Birliği Adalet Divanı (“ABAD”)’nın 1990’lı yıllara değin kararlarında başvurabileceği, AB üyesi ülkelerin vatandaşlarının temel haklarını düzenleyen bir mevzuat mevcut değildi. Bu nedenle ABAD, temel haklara ilişkin yargılamalarda AB açısından bağlayıcılığı olmayan AİHS’ye veya hukuk yaratma yoluna başvuruyordu⁷³. Bu ihtiyaca binaen Avrupa Birliği Temel Haklar Şartı (“ABTHŞ”) 07/12/2000’de imza altına alınarak AB üyesi ülkelerin vatandaşlarının temel haklarına ilişkin tek bir metin oluşturulmuştur⁷⁴.

⁷¹ AKINCI, s. 72; ÖZKAN, s. 54.

⁷² 95/46/EC sayılı Direktif m. 1: “Bu Direktife uygun olarak, Üye Devletler, kişisel verilerin işlenmesine dair başta kişisel mahremiyet hakkı olmak üzere gerçek kişilerin temel haklarını ve özgürlüklerini koruyacaktır;

Üye Devletler 1. paragraf kapsamında sağlanan korumayla bağlantılı nedenler için Üye Devletler arasında kişisel verilerin akışını yasaklamayacak ya da engellemeyeceklerdir.”

⁷³ METİN, Yüksel, “Avrupa Birliği Temel Haklar Şartı”, AÜSBFD, C. 57, S. 4, 2002, s. 41.

⁷⁴ AB Temel Haklar Bildirgesi resmi Türkçe çevirisi için bkz: <https://www.avrupa.info.tr/tr/avrupa-birligi-temel-haklar-bildirgesi-708> E.T. 15/12/2022.

ABTHŞ'nin çalışmamızın açısından önemi, kişisel verilerin korunmasının müstakil bir madde olarak düzenlenmesinden ileri gelmektedir⁷⁵. Kişisel verilerin temel insan hakkı vasfının onaylanması, bu görüşün desteklenmesi amacıyla düzenlemeye dahil edilmiştir⁷⁶.

Düzenleyici, madde hükmünde kişisel verilerin korunmasını isteme hakkının sahiplerini “herkes (*everyone*)” olarak tanımlamıştır. İlk bakışta tüzel kişilerin de kapsama girdiği akla gelse de; tarafımızca da itibar edilen bir görüşe göre düzenleyicinin bu maddede ilk olarak gerçek kişileri kastettiği değerlendirilmesi, kişisel verilerin korunması hukukunun temeline ve öncül düzenleme olan 95/46/EC sayılı Direktif'e daha uygun düşmektedir⁷⁷.

c. 2002/58 EC Sayılı Elektronik Gizlilik Direktifi

Çalışmamızın doğrudan konusunu oluşturan elektronik haberleşme ortamında kişisel verilerin nasıl işleneceğine ilişkin Avrupa Konseyi'nin 2002/58 EC sayılı “Gizlilik ve Elektronik Haberleşme Direktifi” (“E-Gizlilik Direktifi”) 31/07/2002 tarihinde yürürlüğe girmiştir. E-Gizlilik Direktifi'nde elektronik haberleşme ortamında gerçekleşen kişisel verilerin işlenmesi faaliyetlerine ilişkin hükümler yer alması

⁷⁵ ABTHŞ m. 8: “1) Herkes, kendisine ilişkin kişisel bilgilerinin korunmasını isteme hakkına sahiptir.

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

3) Bu kurallara uyulması, bağımsız bir makam tarafından denetlenecektir.”

⁷⁶ BERGKAMP, s. 33.

⁷⁷ KÜZECİ, s. 175.

nedeniyle aşağıda detaylı incelenen Avrupa Birliği Genel Veri Koruma Tüzüğü'nün tamamlayıcısı niteliğindedir⁷⁸.

d. GDPR

Avrupa Birliği Genel Veri Koruma Tüzüğü ("GDPR")'nü, 1995 yılında yürürlüğe giren 95/46/EC sayılı Direktif'in doğrudan halefi olarak tanımlamak mümkündür. Nitekim; GDPR m. 94⁷⁹'te, düzenlemenin yürürlüğe girdiği tarihte 95/46/EC sayılı Direktif'in ilga olacağının hükmedilmesi, yasa koyucunun da GDPR'ın ardıl düzenleme olacağı yönünde iradesini göstermektedir.

95/46/EC sayılı Direktif, kişisel verilere ilişkin temel ilkeleri ortaya koymuş olup Avrupa dışında ülkelerin düzenlemelerinde de bu temel ilkeler yol gösterici olmuştur. Buna karşın; Direktif, AB üyesi ülkelerin mevzuatlarının yeknesaklaşması noktasında yetersiz kalmıştır⁸⁰. Öte yandan; 1995 yılından bu yana hızlı bir şekilde bilişim teknolojilerinin hızlı gelişimine bağlı olarak kişisel verilerin korunması bağlamında 1995 tarihli mevzuatın çağı yakalayamadığını belirtmek mümkündür.

AB bünyesindeki ülkelerde kişisel verilere ilişkin farklı hukuki düzenlemelerin olması veri akışında ortak usul geliştirilmesini engellemiştir⁸¹. GDPR'ın "tüzük" seviyesinde bir düzenleme olması nedeniyle AB üyesi devletler için doğrudan yasa hükmünü kazanmasını sağlamıştır. Bu durum AB üyesi ülkelerin kişisel verilere ilişkin

⁷⁸ UZUNAL, Seda, Elektronik Haberleşme Sektöründe Kişisel Verilerin Korunması, Yüksek Lisans Tezi, İstanbul, 2023, s. 19.

⁷⁹ GDPR m. 94: "1) 95/46/EC sayılı Direktif 25 Mayıs 2018 tarihinden itibaren geçerli olmak üzere yürürlükten kaldırılmıştır.

2) Yürürlükten kaldırılan Direktif'e yapılan atıflar bu Tüzük'e yapılmış sayılır. 95/46/EC sayılı Direktif'in 29. maddesi ile kurulan Kişisel Verilerin İşlenmesiyle ilgili olarak Bireylerin Korunması hakkında Çalışma Grubuna yapılan atıflar bu Tüzük'le kurulan Avrupa Veri Koruma Kurulu'na yapılmış sayılır."

⁸⁰ BAŞALP, s. 85.

⁸¹ ÖZKAN, s. 59.

mevzuatlarını yeknesaklaştırarak, düzenlemenin gerekçelerinden biri olan "tek kıta, tek kanun (*one continent, one law*)" ilkesinin hayata geçmesini sağlamıştır⁸².

GDPR'ı önemli kılan bir başka husus, kapsamının yalnızca AB ile sınırlı olmamasından ileri gelmektedir. GDPR m. 3'e⁸³ göre veri işleyen veya veri sahibinden birinin AB bünyesindeki bir ülkede bulunması, somut olayda GDPR hükümlerinin uygulanması açısından yeterli görülmüştür. Bu hususun çalışmamız açısından önemli olduğu değerlendirilmektedir. Nitekim; büyük ölçekte faaliyet yürüten internet servis sağlayıcıların veri merkezlerini farklı coğrafyalara kurabildikleri bilinmektedir. Söz konusu madde hükmü ile çalışmamızın konusunu oluşturan servis sağlayıcıların, ilgili veriler Avrupa'da tutulmasa dahi GDPR kapsamında sorumlu olacağı akla gelmektedir.

GDPR m. 3'te AB'de mukim olmayan veri işleyenin kapsama girmesi için; AB vatandaşı şahıslara bir ürün veya hizmetin sunulması yeterli görülmüştür. Doktrinde "ürün veya hizmetin sunulması" muğlak bulunmuştur. Bir görüşe göre⁸⁴; veri işleyenin AB vatandaşlarına hizmet verme arzusunda olması yeterlidir. Bu arzunun tespiti için de internet sayfasında AB üyesi bir ülkenin dilinin veya para biriminin kullanılıp

⁸² BAŞALP, s. 86.

⁸³ GDPR m.3: "1) Bu Tüzük, işleme faaliyeti Birlik içerisinde gerçekleşip gerçekleşmediğine bakılmaksızın, Birlik içerisindeki bir kontrolör veya işleyicinin işletmesinin faaliyetleri bağlamında kişisel verilerin işlenmesine uygulanır.

2) Bu Tüzük, işleme faaliyetlerinin aşağıdaki hususlarla alakalı olması durumunda, Birlik içerisinde bulunan veri sahiplerinin kişisel verilerinin Birlik içerisinde kurulu olmayan bir kontrolör veya işleyici tarafından işlenmesine uygulanır:

(a) Veri sahibine bir ödeme yapılmasına gerek olup olmadığına bakılmaksızın, Birlik içerisindeki söz konusu veri sahiplerine mal ya da hizmetlerin sunulması veya

(b) Davranışları birlik içerisinde gerçekleştiği ölçüde, davranışlarının izlenmesi.

3) Bu Tüzük, Birlik içerisinde değil, ancak bir üye devletin hukukunun uluslararası kamu hukuku vasıtasıyla uygulandığı bir yerde kurulu bulunan bir kontrolör tarafından kişisel verilerin işlenmesine uygulanır."

⁸⁴ BURRI, Mira/SCHÄR, Rahel, "The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy", Journal of Information Policy, C. 6, 2016, s. 496.

kullanılmadığı gibi ölçütlere başvurulabileceği savunulmuştur. Bir diğer görüşe göre⁸⁵ AB üyesi bir ülkenin vatandaşı ile sözleşme ilişkisine girilmese veya bu yönde bir arzu da bulunulmasa dahi üçüncü kişiler aracılığıyla AB üyesi bir ülkenin vatandaşlarına hizmet sağlanması yeterlidir. Örneğin; AB sınırları içerisinde dahi olmayan yer sağlayıcıya ait sunucularda, AB üyesi bir ülkenin vatandaşına ait kişisel verilerin üçüncü kişi tarafından muhafaza edilmesi, sunucuları işleten yer sağlayıcıyı GDPR kapsamında sorumlu kılmaktadır. Tarafımızca birinci görüşe görüşe iştirak edilmekte olup, AB vatandaşlarına hizmet sunma güdüsünde olmayan üçüncü bir ülkede mukim veri işleyenin GDPR kapsamın girmeyeceği değerlendirilmektedir.

2. Diğer Düzenlemeler

a. Birleşmiş Milletler Rehber İlkeleri

İkinci Dünya Savaşı'nın ardından tesis edilen barış ortamının muhafazası amacıyla kurulan Birleşmiş Milletler tarafından 10 Aralık 1948 günü 48 üye devletin katılımıyla “İnsan Hakları Evrensel Beyannamesi” (“İHEB”) kabul edilmiştir. Üye devletler açısından bağlayıcı etkisi olmayan İHEB'in, 360 kadar dile çevrilmesi tavsiye niteliğinin üye devletler açısından etkin olduğunu göstermiştir.⁸⁶ İHEB içerisinde doğrudan kişisel verilerin korunmasına yönelik bir hüküm yer almasa da İHEB m. 12 hükmü⁸⁷ özel yaşamın gizliliğini düzenlemektedir. İlk bakışta kişisel verilerin korunması hakkı korunan hukuki değer bakımından özel yaşamın gizliliği hakkının içerisinde kabul

⁸⁵ VOSS, W. Gregory, “European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting”, The Business Lawyer, C. 72, S. 1, 2016, s. 223.

⁸⁶ AYBAY, Rona, Açıklamalı İnsan Hakları Evrensel Beyannamesi, Türkiye Barolar Birliği Yayınları, 2006, s. 6.

⁸⁷ İHEB m. 12 “Hiç kimsenin özel yaşamına, ailesine, konutuna ve haberleşmesine keyfi olarak karışılmaz, onur ve üzüne saldırlamaz. Herkesin bu tür karışma ve saldırılara karşı yasal korunma hakkı vardır.”

edilebilir. Nitekim her iki hakkın amacının insan onurunu ve bireysel özerkliği muhafaza etmek olması⁸⁸ bağlamında İHEB m. 12'nin kişisel verilerin korunmasına ilişkin düzenlemeleri etkilediği belirtilebilecektir.

Kişisel verilerin korunması hakkında spesifik bir hüküm içermeyen İHEB'in ardından 1990 yılında BM Genel Kurulu'nun 45/95 sayılı kararıyla, üye ülkeler açısından herhangi bir bağlayıcılığı olmayan, “*Bilgisayarlarla İşlenen Kişisel Veri Dosyalarına İlişkin Rehber İlkeler*” kabul edilmiştir⁸⁹. Birleşmiş Milletlerin “kişisel veri” kavramını kullandığı mezkur düzenlemede kişisel verilerin işlenmesine ilişkin tavsiye niteliğinde dokuz ilke yer almıştır⁹⁰. “Kişisel veri” kavramının ilk kez kullanıldığı bu düzenlemenin

⁸⁸ KÜZECİ, s. 84.

⁸⁹ OĞUZ, Sefer, s. 123.

⁹⁰ KILINÇ, Doğan, *Anayasal Bir Hak Olarak Verilerin Korunması*, AÜHFD, C. 61, S. 3, 2012, s. 1111-1112:

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

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

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

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

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

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

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

ardından BM tarafından 2013 yılına değin kişisel verilere ilişkin herhangi bir düzenleme kabul edilmemiştir. İnternet, mobil telefonlar, kablosuz bağlantı sunan tüm cihazların günlük hayatımızın birer parçası olduğu 2010’lu yılların başlamasıyla BM’nin kişisel veri gizliliği konusunda düzenlemeleri ivmelenmiştir. BM Genel Kurulu’nun 2013 tarihli, “*Dijitalda Çağda Gizlilik Hakkı*” başlıklı 68/167 sayılı kararının ardından kişisel veri gizliliğini konu alan çok sayıda karar ve rapor yayımlanmıştır⁹¹.

b. OECD Rehber ilkeleri

OECD tarafından, 1978 yılında üye ülkelerin veri koruma mevzuatları arasında ihtilafları giderebilmek adına Viyana’da “*Sınır Ötesi Veri Muhafazası ve Gizliliğin Korunması Uzmanlar Grubu*” tertip edilerek uluslararası veri korumaya ilişkin “Rehber İlkeler”i 1980 yılında yayımlanmıştır⁹². OECD Rehber İlkelerinde gizliliğin korunmasından daha çok üye ülkeler arasında ticaretin sekteye uğramaması amaçlanmıştır. Nitekim kişisel veriler, herhangi bir ticari ürün gibi gelişen teknolojilere paralel şekilde uluslararası ticaret için önemli bir öge haline gelmiştir⁹³.

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

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

⁹¹ Swiss Agency for Development and Cooperation, Compendium of Data Protection and Privacy Policies and Other Related Guidance Within The United Nations Organization and Other Selected Bodies of The International Community, 2021, s. 10 vd., https://unstats.un.org/legal-identity-agenda/documents/Paper/data_protecton_%20and_privacy.pdf, E.T. 19.01.2023

⁹² FLEISCHMANN, Amy, “*Personal Data Security: Divergent Standards in the European Union and the United States*”, Fordham International Law Journal, C. 19, S. 1, 1995, s. 154.

⁹³ AKSOY, s. 6.

OECD yapısı itibarıyla kıtalararası bir ticaret örgütü olup kurucu üyeleri arasında ABD'nin yanı sıra Avrupa ülkeleri de bulunmaktadır. OECD'nin kişisel verilere yönelik düzenlemesi, mezkur konuya farklı perspektiflerden bakan ABD'li ve Avrupalı temsilcileri ilk kez bir araya getirmesi bakımından önemli husustur. Nitekim 1980'li yıllarda ABD'de kişisel verilerin korunması yalnızca hukuki ihtilaf halinde işletilen ve önem açısından ekonomik çıkarların arkasında yer alan kurallar bütünü olarak görülmekteydi. Avrupalılarca kişisel verilerin korunmasına ilişkin yeterli güvence sağlanmayan ve veri işleme sistemlerinin oldukça gelişmiş olduğu ABD'ye veri transferi sakıncalı bir durum olarak kabul edilmekteydi⁹⁴. Uzmanlar Grubu kapsamında kişisel verilere farklı yaklaşım sergileyen iki partiyi bir araya getirilerek kişisel verilerin gizliliği ve veri akışı arasında denge oluşturulmaya gayret edilmiştir⁹⁵.

Üye ülkeler için bağlayıcılığı olmayan OECD Rehber İlkeleri ihtiva ettiği kişisel verilerin korunmasına ilişkin sekiz temel ilke⁹⁶ başta olmak üzere Avrupa Birliği düzenlemeleri ve Türk hukukunu etkilemiştir⁹⁷.

⁹⁴ GÜR, İkbâl, Kişisel Verilerin Korunması Hususunda AB ile ABD Arasında Çıkan Uyuşmazlıklar ve Çözüm Yolları, Yüksek Lisans Tezi, Ankara, 2009, s. 109-110.

⁹⁵ GÜR, s. 110.

⁹⁶ 1. Verinin toplanmasının sınırlanması

2. Verinin doğruluğu ve güncelliği

3. Spesifik amaca uygunluk

4. Veri kullanımının sınırlanması

5. Güvenlik önlemlerinin alınması

6. Şeffaflık

7. İlgili kişinin katılımı

8. Hesap verilebilirlik

⁹⁷ BASKIN, s. 33; TURAN, s. 318; GÖÇMEN UYARER, s. 250.

c. Avrupa Konseyi Düzenlemeleri

Kişisel verilerin korunması ilk olarak 04/11/1950 tarihinde yürürlüğe giren Avrupa İnsan Hakları Sözleşmesi (AİHS) m. 8⁹⁸ ile yasal açıdan düzenlenmiştir. Nazi döneminde devlet yetkilileri, özel hayata ilişkin bilgilere yönelik geniş yetkilerle donatılmıştı. İkinci Dünya Savaşı sona erdikten sonra özel hayata benzer müdahalelerin önüne geçilebilmesi adına AİHS m. 8 düzenlenmiştir⁹⁹. Belirtilen hüküm doğrudan kişisel verilerin korunmasını konu almamasına karşın, “özel ve aile hayatı” ile “yazışma”ya saygı gösterilmesine ilişkin düzenleme ile kişisel verilerin de koruma altına alındığını belirtmek mümkündür. Nitekim, bir ülkede spesifik olarak kişisel verilerin korunmasına ilişkin düzenleme olmasa da bu ülkenin AİHS’ye taraf olması halinde bir birey, AİHS m. 8’e dayanarak kişisel verilerinin korunmasını talep edebilir¹⁰⁰.

Bilgisayar sistemlerinin yaygınlaştığı 1970’li yıllardan itibaren Avrupa Konseyi kişisel veriler alanında çalışmalarını yoğunlaştırmış ve bu çalışmalardan hareketle 28/01/1981 tarihinde imzaya açılan “108 No.lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi” 01/10/1985 tarihinde yürürlüğe

⁹⁸ AİHS m. 8: “Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.

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

⁹⁹ REMPELL, s. 814.

¹⁰⁰ BYGRAVE, Lee A., “Data Protection Pursuant to the Right to Privacy in Human Rights Treaties”, International Journal of Law and Information Technology, C. 6, S. 3, 1998, s. 247-248.

girmiştir. Sözleşmeyi ilk imzalayan devletlerden olan Türkiye Cumhuriyeti, 2016 yılında¹⁰¹ sözleşmeyi iç hukuka dahil etmiştir¹⁰².

108 No.lu Sözleşme yalnızca otomatik işleme süreçlerini kapsamına alarak OECD Rehber İlkeleri ve diğer uluslararası düzenlemelerden ayrılmıştır. 108 No.lu Sözleşmede “otomatik işlem” kavramının tanımına da yer verilmiştir¹⁰³. Otomatik işleme özelinde kişisel verilerin ele alınması gibi çağın gelişimlerini yakalayan bir düzenleme olmasına rağmen 108 No.lu Sözleşme OECD Rehber İlkelerine benzer şekilde üye devletlerin kişisel verilerin korunmasına ilişkin mevzuatlarının yeknesaklaştırılmasına hizmet edememiştir¹⁰⁴.

C. Ulusal Düzenlemeler

1. Anayasa Hükmü

Anayasamızın¹⁰⁵ “Temel Haklar ve Ödevler” başlıklı ikinci kısmında yer alan m. 20’de “Özel Hayatın Gizliliği” ayrı bir madde olarak düzenlenmiştir. Bahsi geçen maddeye 2010 yılında 5982 sayılı Kanun ile kişisel verilerin korunmasına ilişkin bir fıkra daha eklenerek madde hükmü bugünkü şeklini almıştır¹⁰⁶. Avrupa Birliği mevzuatının

¹⁰¹ 30/01/2016 tarihli ve 6669 sayılı 6669 Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun.

¹⁰² Kişisel Verilerin Korunması Kurumu, Kişisel Verilerin Korunması Alanında Uluslararası ve Ulusal Düzenlemeler, s. 3 (<https://www.kvkk.gov.tr/Icerik/4183/Kisisel-Verilerin-Korunmasi-Alaninda-Uluslararası-ve-Ulusal-Düzenlemeler>), E.T. 29/11/2022.

¹⁰³ Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireyin Korunması Sözleşmesi m. 2/I-c bendi: “*Otomatik işlem, tamamen veya kısmen otomatik yöntemlerle gerçekleştirilen; verilerin kaydı, bu verilere mantıksal ve/veya aritmetik işlemlerin uygulanması, verilerin değiştirilmesi, silinmesi, geri elde edilmesi veya dağıtılması anlaşılar.*” (<https://www.resmigazete.gov.tr/eskiler/2016/03/20160317-2.pdf>), E.T. 30/11/2022.

¹⁰⁴ FLEISCHMANN, s. 154.

¹⁰⁵ 2709 sayılı T.C. Anayasası, R.G. Sayısı 17863(Mükerrer), R.G. Tarihi 09/11/1982.

¹⁰⁶ T.C. Anayasası m. 20: “*1) Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz.*”

gelişim sürecine benzer şekilde Anayasa m. 20'ye 2010 yılında eklenen düzenlemeden önce de, başta özel hayatın gizliliğine ilişkin hüküm olmak üzere ilgili düzenlemelerle kişisel verilerin korunmasına Anayasal dayanaklar mevcut bulunmaktadır¹⁰⁷. Söz konusu düzenleme ile kişisel verilerin korunması doğrudan anayasal dayanak kazanmış, bilahare yayımlanan KVKK, Anayasa'ya dayandırılmıştır.

Kişisel verilerin korunmasının Anayasal dayanak kazanarak temel hak ve özgürlük vasfını kazanması, diğer temel hak ve özgürlüklere benzer şekilde sınırsız olmasını sağlamamıştır¹⁰⁸. Anayasa m. 13'te¹⁰⁹ temel hak ve hürriyetlerin özlerine dokunulmaksızın kanunla sınırlandırılabilceği düzenlenmiştir. Anayasa m. 20'de kişisel verilerin işlenmesi için açık rıza şartı aranmıştır. Normlar hiyerarşisi gereğince kanun veya hiyerarşik açıdan daha aşağıda bir düzenleme ile bu şartın mevzuattan kaldırılması hukuki açıdan mümkün değildir. Bununla birlikte Anayasa m. 13'de belirtilen şartların varlığı halinde, diğer temel hak ve hürriyetler gibi kişisel verilerin korunması hakkı da özüne dokunulmaksızın kanun ile ve Anayasa m. 20'de sayılan sebeplerle kısıtlanabilir.

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

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

¹⁰⁷ KILINÇ, s. 1131.

¹⁰⁸ ÇEKİN, s. 640.

¹⁰⁹ Anayasa m. 13: “Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz.”

Söz konusu maddede, “*kanunda öngörülen hallerde veya kişinin açık rızasıyla*” ifadesine yer verildiğinden; kanunda öngörülmesi şartıyla milli güvenlik gibi gerekçelerle açık rıza aranmaksızın kişisel verilerin işlenebileceği değerlendirilmektedir.

2. KVKK

Anayasa m. 20’de 2010 yılında gerçekleştirilen düzenleme ile kişisel verilerin korunması hususu dahil edilirken usul ve esasların da bilahare yayımlanacak kanun ile düzenleneceği hüküm altına alınmıştır. Nitekim 2016 yılında yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu¹¹⁰ (“KVKK”)’nın 1. maddesinin gerekçesinde¹¹¹ de kanunun kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasların da düzenlenmesi Kanunun amaçları arasında yer almaktadır.

Türk hukukunda kişisel verilere ilişkin ilk bütüncül yasa olan KVKK’dan önceki süreçte de Türkiye’de kişisel verilere ilişkin yasal düzenlemeler bulunmaktadır. Nitekim, Türkiye Cumhuriyeti, Avrupa Konseyi “*108 No.lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi*”ni ilk imzalayan devletlerden biri olmuştur¹¹². Uzun bir kişisel verilere ilişkin yasal düzenleme sürecinden sonra yürürlüğe giren KVKK muhtevasında genel anlamda AB’nin kişisel verilere ilişkin mevzuatı esas alınmıştır¹¹³.

“Amaç” başlıklı KVKK m. 1’de Kanunun amacı “*başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak*” olarak tanımlanmıştır¹¹⁴.

¹¹⁰ 6698 sayılı Kişisel Verilerin Korunması Kanunu R.G. Tarihi: 07/04/2016, R.G. Sayı 29677

¹¹¹ Gerekçe için bkz: <https://www5.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf>, E. T. 20/08/2023

¹¹² Detaylı bilgi için bkz: Birinci Bölüm, II, B, 2, c.

¹¹³ KORKMAZ, s. 88.

¹¹⁴ KVKK m. 1: “*Bu Kanunun amacı, kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri*

Bizim de katıldığımız görüşe göre, KVKK'nin lafzında yer almasa da amaç salt özel hayatın gizliliğini muhafaza etmek değildir. Özel hayatın gizliliğinin yanı sıra ticari ve ekonomik hususlar da tarihi kanun koyucunun amaçları arasında yer almaktadır¹¹⁵. OECD Rehber İlkeleri ve diğer ilgili uluslararası düzenlemelere benzer şekilde bireyin kişisel verileri koruma altına alınırken kişisel verilerden istifade eden piyasa aktörlerinin ticari faaliyetlerinin sürdürülebilirliği arasında bir denge kurulmaya gayret edilmiştir. Nitekim KVKK m. 9/II'de¹¹⁶ belli şartların varlığı halinde yurt dışına kişisel veri aktarımında açık rıza aranmayacağı belirtilmiştir. İnternet ortamında uluslararası ticaretin sürdürülebilirliği için yurt dışı veri aktarımı son derece önem arz etmektedir. Bu durumu somutlaştırmak gerekirse; “*Big Tech*” olarak anılan *Alphabet, Amazon, Apple, Meta* ve *Microsoft* firmalarının her biri 1 trilyon ABD Dolarının üstünde piyasa değerine sahip olup¹¹⁷ bu firmalar neredeyse tüm dünya genelinde faaliyet yürütmektedir. Söz konusu firmaların yurt dışı merkezli faaliyet yürüttüğü göz önüne alındığında; salt özel hayatın gizliliğinin korunmasından hareketle uluslararası veri akışını tamamen engellemek, bilgi toplumunun gereklerine aykırı düşecektir. Bu noktada; KVKK m. 9/II hükmü ile internet ortamında yaşayan uluslar üstü ekonomi ile kişisel mahremiyet arasında bir denge kurma amacının gözetildiği değerlendirilmektedir. Söz konusu firmaların aynı zamanda veri

işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektir.”

¹¹⁵ ÖZKAN, s. 83; TAŞTAN, s. 25.

¹¹⁶ KVKK m. 9/II: “*Kişisel veriler, 5 inci maddenin ikinci fıkrası ile 6 ncı maddenin üçüncü fıkrasında belirtilen şartlardan birinin varlığı ve kişisel verinin aktarılacağı yabancı ülkede;*

a) Yeterli korumanın bulunması,

b) Yeterli korumanın bulunmaması durumunda Türkiye’deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurulun izninin bulunması,

kaydıyla ilgili kişinin açık rızası aranmaksızın yurt dışına aktarılabilir.”

¹¹⁷ Ocak 2022 ayı itibarıyla Apple, market değeri 3 trilyon ABD Dolarını geçen ilk şirket olmuştur. Apple’ı 2.5 trilyon ABD Doları ile Microsoft takip etmiştir. Alphabet ve Amazon ise birer trilyon ABD Doları değere sahip olmuştur. İlgili haber için bkz: <https://www.reuters.com/markets/europe/apple-gets-closer-3-trillion-market-value-2022-01-03> (E.T. 29/12/2022).

merkezlerini kendi bünyelerinde tutmaları sebebiyle yer sağlayıcı sıfatları da bulunmakta olup bu konu çalışmanın ilerleyen bölümlerinde incelenecektir.

3. Türk Ceza Kanunu

5237 sayılı Türk Ceza Kanunu (“TCK”)¹¹⁸’nin yürürlüğe girdiği tarihte KVKK gibi kişisel verilerin korunmasına ilişkin genel bir mevzuat düzenlemesi mevcut değildir. Buna karşın TCK’nin ikinci kitap ikinci kısım “*özel hayata ve hayatın gizli alanına karşı suçlar*” başlıklı dokuzuncu bölümü oluşturan 135-140 maddeleri arasında kişisel verilerle alakalı suçlara yer verilmiştir.

TCK m. 135’te “*kişisel verilerin kaydedilmesi*”, TCK m. 136’de “*kişisel verileri hukuka aykırı olarak verme veya ele geçirme*” TCK m. 138’de “*verileri yok etmeme*” suçları düzenlenmiştir. m. 137,139,140 hükümlerinde ise tamamlayıcı hükümler yer almıştır. Mezkur maddeler “doğrudan ilişkili maddeler” olarak tasniflenmektedir¹¹⁹. Nitekim 2016 yılında yürürlüğe giren KVKK m. 17/I’de¹²⁰ bahsi geçen altı maddenin kişisel verilere ilişkin suçlarda uygulanacağı düzenlenmiştir. KVKK’de, daha eski tarihli TCK’de yer alan suç tiplerine açıkça atıfta bulunulması; bu suç tiplerini doğrudan kişisel verilerle alakalı kılmaktadır. TCK m. 132, 133, 134, 239, 243, 244, 258 ve 279 hükümleri kişisel verilerle dolaylı olarak alakalıdır¹²¹.

TCK’nin kişisel veriler ile doğrudan alakalı hükümleri KVKK’dan daha eski tarihli olduğu için, yürürlük tarihinde henüz “kişisel veri” kavramı tanımlanmamıştır. Bu

¹¹⁸ 5237 sayılı Türk Ceza Kanunu, R.G. Tarihi: 12/10/2014, R.G. Sayısı: 25611.

¹¹⁹ DÜLGER, Murat, Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması, İMÜHFD, C.3, S. 2, 2016, s. 120.

¹²⁰ KVKK m. 17/I: “*Kişisel verilere ilişkin suçlar bakımından 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununun 135 ila 140 ıncı madde hükümleri uygulanır.*”

¹²¹ BATU, Betül, 6698 Sayılı Kişisel Verilerin Korunması Kanunu Kapsamında Kişisel Verilerin İşlenmesi ve Açık Rıza, Yüksek Lisans Tezi, 2022, s. 43.

durumun; TCK’de düzenlenen suça ilişkin hükümlerinin cezanın belirlenebilirliği bağlamında kanunilik ilkesine aykırılık oluşturduğu yönünde görüşler mevcuttur¹²². Bir görüşe göre; TCK m. 135-140 arasında düzenlenen ve ihlali hapis cezası öngörölmüş suçlarda hukuki açıdan korunan değerin tanımlanmamış olması kanunilik ilkesine aykırıdır¹²³. Buna karşın; TCK m. 135’in gerekçesinde¹²⁴ kişisel veriler, Avrupa Konseyi 108. No’lu “*Kişisel Nitelikteki Verilerin Otomatik İşleme Tâbi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme*”ye atıfta bulunularak “gerçek kişiyle ilgili her türlü bilgi” olarak tanımlanmıştır. Mezûr sözleşmeye Türkiye’nin taraf olması, usulüne uygun onaylanmış uluslararası sözleşmelerin de kanun hükmünde olmasından hareketle kanaatimizce kişisel verilerin TCK’de tanımlanmaması, kanunilik ilkesine aykırılık oluşturmamaktadır.

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

5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun¹²⁵ (“5651 sayılı Kanun”) muhtevasında kişisel verilerin işlenmesine ilişkin doğrudan bir hüküm yer almamaktadır.

¹²² KÜZECİ, s. 308; ÖZKAN, s. 80.

¹²³ OĞUZ, Sefer, s. 125.

¹²⁴ “ Suçun konusu, kişisel verilerdir. Gerçek kişiyle ilgili her türlü bilgi, kişisel veri olarak kabul edilmelidir. Söz konusu suç tanımında kişisel verilerin bilgisayar ortamında veya kağıt üzerinde kayda alınması arasında bir ayırım gözetilmemiştir. Bu bakımdan, söz konusu suç tanımı ile, Avrupa Konseyi bünyesinde hazırlanan Türkiye'nin de 28 Ocak 1981 tarihinde imzalamakla taraf olduğu “*Kişisel Nitelikteki Verilerin Otomatik İşleme Tâbi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme*”nin ilgili hükümlerine geçerlilik tanınmıştır.” TCK gerekçesi için bkz. <https://www.lexpera.com.tr/mevzuat/gerekceler/turk-ceza-kanunu-madde-gerekceleri/1> E.T. 02/01/2022.

¹²⁵ 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun R.G. Tarihi: 23/05/2007, R.G. Sayısı: 26530.

Buna karřın 5651 sayılı Kanun’da internet aktörleri tanımlanarak, yükümlölükleri düzenlenmiştir¹²⁶. Bu çalışma kapsamında, belirtilen tanımlar çerçevesinde internet aktörleri ele alınıp kişisel verilerin işlenmesi sürecinde yükümlölükleri ve sorumlulukları tartışılmaya çalışılacaktır. 5651 sayılı Kanun, internet aktörlerinin belirlenmesi ve sorumluluk tayini açısından önem arz etse de internet ortamındaki kişilik hakkı ihlallerine

¹²⁶ ÖZBAKIR, Ali Fuat, İnternet Servis Sağlayıcılarının Hukuki Sorumluluđu, Yüksek Lisans Tezi, 2016, s. 30.

ilişkin m. 9¹²⁷ ve m. 9/A¹²⁸ düzenlemelerini de içermektedir. Söz konusu düzenlemeler ile internet ortamının çarpan etkisi göz önünde bulundurularak kişilik hakları ihlalinin en

¹²⁷ 5651 sayılı Kanun m. 9: “I) İnternet ortamında yapılan yayın içeriği nedeniyle kişilik haklarının ihlal edildiğini iddia eden gerçek ve tüzel kişiler ile kurum ve kuruluşlar, içerik sağlayıcısına, buna ulaşamaması hâlinde yer sağlayıcısına başvurarak uyarı yöntemi ile içeriğin yayından çıkarılmasını isteyebileceği gibi doğrudan sulh ceza hâkimine başvurarak içeriğin çıkarılmasını ve/veya erişimin engellenmesini de isteyebilir.

II) İnternet ortamında yapılan yayın içeriği nedeniyle kişilik haklarının ihlal edildiğini iddia eden kişilerin talepleri, içerik ve/veya yer sağlayıcısı tarafından en geç yirmi dört saat içinde cevaplandırılır.

III) İnternet ortamında yapılan yayın içeriği nedeniyle kişilik hakları ihlal edilenlerin talepleri doğrultusunda hâkim bu maddede belirtilen kapsamda içeriğin çıkarılmasına ve/veya erişimin engellenmesine karar verebilir.

IV) Hâkim, bu madde kapsamında vereceği erişimin engellenmesi kararlarını esas olarak, yalnızca kişilik hakkının ihlalinin gerçekleştiği yayın, kısım, bölüm ile ilgili olarak (URL, vb. şeklinde) içeriğe erişimin engellenmesi yöntemiyle verir. Zorunlu olmadıkça internet sitesinde yapılan yayının tümüne yönelik erişimin engellenmesine karar verilemez. Ancak, hâkim URL adresi belirtilerek içeriğe erişimin engellenmesi yöntemiyle ihlalin engellenemeyeceğine kanaat getirmesi hâlinde, gerekçesini de belirtmek kaydıyla, internet sitesindeki tüm yayına yönelik olarak erişimin engellenmesine de karar verebilir.

V) Hâkimin bu madde kapsamında verdiği içeriğin çıkarılması ve/veya erişimin engellenmesi kararları doğrudan Birliğe gönderilir.

VI) Hâkim bu madde kapsamında yapılan başvuruyu en geç yirmi dört saat içinde duruşma yapmaksızın karara bağlar. Bu karara karşı 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanunu hükümlerine göre itiraz yoluna gidilebilir.

VII) Erişimin engellenmesine konu içeriğin yayından çıkarılmış olması durumunda hâkim kararı kendiliğinden hükümsüz kalır.

VIII) Birlik tarafından ilgili içerik ve yer sağlayıcılar ile erişim sağlayıcıya gönderilen içeriğin çıkarılması ve/veya erişimin engellenmesi kararının gereği derhâl, en geç dört saat içinde ilgili içerik ve yer sağlayıcılar ile erişim sağlayıcı tarafından yerine getirilir.

IX) Bu madde kapsamında hâkimin verdiği içeriğin çıkarılması ve/veya erişimin engellenmesi kararına konu kişilik hakkının ihlaline ilişkin yayının başka internet adreslerinde de yayınlanması durumunda ilgili kişi tarafından Birliğe müracaat edilmesi hâlinde mevcut karar bu adresler için de uygulanır. Müracaatın Birlik tarafından kabulüne karşı itiraz, kararı veren hâkimliğe yapılır. İnternet sitesindeki yayının tümüne yönelik erişimin engellenmesi kararlarında bu fıkra hükmü uygulanmaz.

X) İnternet ortamında yapılan yayın içeriği nedeniyle kişilik hakları ihlal edilenlerin talep etmesi durumunda hâkim tarafından, başvuranın adının bu madde kapsamındaki karara konu internet adresleri ile ilişkilendirilmemesine karar verilebilir. Kararda, Birlik tarafından hangi arama motorlarına bildirim yapılacağı gösterilir.

XI) Sulh ceza hâkiminin kararını bu maddede belirtilen şartlara uygun olarak ve süresinde yerine getirmeyen içerik, yer ve erişim sağlayıcıların sorumluları, beş yüz günden üç bin güne kadar adli para cezası ile cezalandırılır.”

¹²⁸ 5651 sayılı Kanun m. 9/A: “I) İnternet ortamında yapılan yayın içeriği nedeniyle özel hayatının gizliliğinin ihlal edildiğini iddia eden kişiler, Kuruma doğrudan başvurarak içeriğe erişimin engellenmesi tedbirinin uygulanmasını isteyebilir.

hızlı şekilde bertaraf edilmesinin amaçlandığı değerlendirilmektedir. Zira TMK ve TBK kapsamında halihazırda kişilik haklarına saldırı halinde başvurulabilecek genel yollar düzenlenmiştir.

İnternet ortamında hukuka aykırı içeriğin hızlı yayımlanmasını önlemeye yönelik ivedi tedbirlerin, eş zamanlı olarak internet ortamındaki ifade özgürlüğüne halel getirmemesi başka bir hukuki problem olarak karşımıza çıkmaktadır. AYM bir kararında¹²⁹ 5651 sayılı Kanun m. 9'da yer alan tedbirlerin, kişilik haklarına saldırıdan

II) Yapılan bu istekte; hakkın ihlaline neden olan yayının tam adresi (URL), hangi açılardan hakkın ihlal edildiğine ilişkin açıklama ve kimlik bilgilerini ispatlayacak bilgilere yer verilir. Bu bilgilerde eksiklik olması hâlinde talep işleme konulmaz.

III) Başkan, kendisine gelen bu talebi uygulanmak üzere derhâl Birliğe bildirir, erişim sağlayıcılar bu tedbir talebini derhâl, en geç dört saat içinde yerine getirir.

IV) Erişimin engellenmesi, özel hayatın gizliliğini ihlal eden yayın, kısım, bölüm, resim, video ile ilgili olarak (URL şeklinde) içeriğe erişimin engellenmesi yoluyla uygulanır.

V) Erişimin engellenmesini talep eden kişiler, internet ortamında yapılan yayın içeriği nedeniyle özel hayatın gizliliğinin ihlal edildiğinden bahisle erişimin engellenmesi talebini talepte bulunduğu saatten itibaren yirmi dört saat içinde sulh ceza hâkiminin kararına sunar. Hâkim, internet ortamında yapılan yayın içeriği nedeniyle özel hayatın gizliliğinin ihlal edilip edilmediğini değerlendirerek vereceği kararını en geç kırk sekiz saat içinde açıklar ve doğrudan Kuruma gönderir; aksi hâlde, erişimin engellenmesi tedbiri kendiliğinden kalkar.

VI) Hâkim tarafından verilen bu karara karşı Başkan tarafından 5271 sayılı Kanun hükümlerine göre itiraz yoluna gidilebilir.

VII) Erişimin engellenmesine konu içeriğin yayından çıkarılmış olması durumunda hâkim kararı kendiliğinden hükümsüz kalır.

VIII) Özel hayatın gizliliğinin ihlaline bağlı olarak gecikmesinde sakınca bulunan hâllerde doğrudan Başkanın emri üzerine erişimin engellenmesi Kurum tarafından yapılır.

IX) Bu maddenin sekizinci fıkrası kapsamında Başkan tarafından verilen erişimin engellenmesi kararı, yirmi dört saat içinde sulh ceza hâkiminin onayına sunulur. Hâkim, kararını kırk sekiz saat içinde açıklar.”

¹²⁹ AYM Keskin Kalem Yayıncılık ve Ticaret A.Ş. Ve Diğerleri Başvurusu, Başvuru Numarası: 2018/14884 Karar Tarihi: 27/10/2021 R.G. Tarihi 07/01/2022, R.G. Sayısı: 31712 “... Başvuruya konu olan ve Kanun'un 9. maddesinde yer alan erişimin engellenmesi yolu kanun koyucu tarafından hukuk sistemindeki mevcut yargılama usullerinden farklı bir yol olarak tasarlanmıştır. Erişimin engellenmesi yolunun kendine özgü karakterinin de etkisiyle uygulamada, erişimin engellenmesi kararlarına karşı gidilen itiraz başvurusunun reddedilmesi ile karar kesinleşmekte; Kanun gerekçesinde erişimin engellenmesi yolu tedbir olarak tanımlanmış olmasına rağmen şikâyet konusu internet içeriklerine erişim belirsiz süreyle engellenmiş olmaktadır. Bu şekilde süresiz kısıtlamaların ifade ve basın özgürlükleri için büyük tehlikeler arz ettiği açıktır. Demokratik bir hukuk devletinde -güdülen amaç ne olursa olsun- sınırlamalar

bahisle internet ortamındaki bir içeriğin sınırsız olarak erişime engellenmesi nedeniyle yapısal açıdan sorunlu olduğuna hükmetmiştir.



özgürlüğün kullanılmasını ölçüsüz biçimde ortadan kaldıracak düzeyde olamaz. Dolayısıyla şekli yönden kesin hükmün bütün sonuçlarını doğuran ve süresiz etki gösteren bir kuralın keyfî ve orantısız müdahalelere karşı mutlaka koruyucu birtakım güvenceler içermesi gerekir...”

İKİNCİ BÖLÜM

KİŞİSEL VERİLERİN İNTERNET ORTAMINDA İŞLENMESİ

I. İNTERNET ORTAMI

A. Tanım

Kişisel verilerin işlenmesi denilince akla ilk olarak internet ortamında gerçekleşen fiiller gelse de internet kişisel verilerin işlenebileceği ortamlardan yalnızca biridir. Çalışmamızda kişisel verilerin işlenmesi müessesesi, internet ortamı bağlamında sınırlandırıldığından; internet ortamının tanımının yapılması, yeni gelişen bir teknoloji olarak çalışma prensiplerinin hukuki açıdan incelenmesi, internet ortamında kişisel verilerin işlenmesinden doğan hukuki sorumluluğun tayini noktasında önem arz etmektedir.

TDK Güncel Türkçe Sözlük'te, internet kavramı genel ağ ile eş anlamlı kabul edilmiş, genel ağ ise; “*Bilgisayar ağlarının birbirine bağlanması sonucu ortaya çıkan, herhangi bir sınırlaması ve yöneticisi olmayan uluslararası bilgi iletişim ağı*” olarak tanımlanmıştır¹³⁰. Teknik açıdan internet, TCP/IP¹³¹ iletişim protokolünden istifadeyle

¹³⁰ Bknz: <https://sozluk.gov.tr>, E.T. 21/01/2023, TDK sözlükte “İnternet” kelimesinin Uluslararası (International) ve Ağ (Network) kelimelerinin birleşiminde oluştuğu hususu yer almaktadır.

¹³¹ Ağların birbirine bağlanarak “*Inter-networking*” kurma fikrinden hareketle 1974 yılında *Transmission Control Protocol* (TCP) isimli veri paketi değişim protokolü geliştirilmiştir. Bilahare -İnternet kavramının da kuramsallaşmasıyla- veri paketi değişim protokolünün adı “*Internet Protocol*”ün kısaltması olan “IP”nin eklenmesiyle “TCP/IP” olarak anılmıştır. TCP/IP o günden bu yana İnternet ortamı için *lingua franca* mahiyetindedir. Detaylı bilgi için bknz: ROSENZWEIG, Roy, *Wizards, Bureaucrats, Warriors, and Hackers: Writing the History of the Internet*, The American Historical Review, C. 103, S. 5, 1998, s. 1536.

dünya çapında bilgi işleyen tüm cihazların birbiriyle iletişim kurmasını sağlayan genel bir ağıdır¹³².

İnternet, herhangi bir sınırlamaya bağlı kalmaksızın tüm bilişim cihazlarının bir protokol üzerinden birbirine bağlı kalmasını sağlar. Bunun yanında; bilişim cihazlarını birbirlerine bağlayan ağ tipleri internetten ibaret değildir. Ağ bağlantıları; “LAN (*Local Area Network* – Yerel Alan Ağı)”, “CAN (*Campus Area Network* – Kampüs Alan Ağı)”, “MAN (*Metropolitan Area Network* – Metropol Alan Ağı)” ve “WAN (*Wide Area Network* – Geniş Alan Ağı)” olmak üzere dört gruba ayrılmaktadır. Özellikle WAN’lar birbirleriyle bağlantı kurarak sınır tanımaksızın internet ortamını oluştururlar¹³³.

LAN tamamen içe dönük dışarıya kapalı bağlantı sağlayan bir ağıdır. Buna karşın; LAN, çoğu zaman internet ortamına erişmek için yerel bir omurga görevini üstlenebilir¹³⁴. Örneğin; bireylerin evlerinde *router/modem* cihazlarına kablo marifetiyle kurulan bağlantı LAN olarak isimlendirilir. Bu bağlantı iki taraflı olup herhangi bir dış müdahale mümkün değildir. Bunun yanında *router/modem* WAN oluşturarak bilgisayarları internete bağlamaktadır. Dolayısıyla somut örnekte; internet erişimi sağlayabilmek adına LAN, WAN’a ulaşmak için omurga görevi görmüştür. LAN bağlantıların yerel niteliği, kişisel veri işlenmesini olanaksız kıldığından çalışma kapsamına girmemektedir.

Belirli bir işletme veya kampüs içerisinde kurulan bağlantıyı ifade eden CAN ve belirli bir şehir veya bölge içerisinde kurulan bağlantıyı ifade eden MAN bağlantıları, WAN’ın aksine sınırlandırılmış bağlantılardır¹³⁵. Sınırlandırılmış yapıları nedeniyle bu

¹³² ÖZBAKIR, s. 5.

¹³³ ÖZTEKİN, Alp, Teori ve Uygulamada İnternet Hukuku, 2. Baskı, Ankara, 2023, s. 107.

¹³⁴ ÖZTEKİN, s. 41.

¹³⁵ ÖZTEKİN, s. 107.

bağlantıların kurulduğu ortam, İnternet yerine “intranet” ve “extranet” olarak isimlendirilmiştir¹³⁶. İtranet; internet prosedürlerinden istifadeyle bir kuruluşun iç bağlantısını sağlayan ortamlar olup tüm dünyayı birbirine bağlayan internetin aksine sınırlı ve belli bilişim cihazları dışında erişime kapalıdır¹³⁷. İtranet yalnızca kuruluşlarla sınırlı olmayıp bütün bir ülkeyi kapsayan bir ortam da arz edebilir¹³⁸. Extranet ise internet ve intranet arasında gri bir alan oluşturmaktadır¹³⁹. İtranet insanları özel ve kapalı bir ağ üzerinden birbiriyle bağlarken; extranet sınırlandırılmış bir topluluğu birbirine bağlamaktadır¹⁴⁰. Bu açıdan LAN bağlantılarının aksine; intranet ve extranet ortamlarının internet gibi sınırsız olmasa dahi, fiziken veya kullanıcı bazlı sınırlı bir ortamda veri paylaşımını mümkün kıldığı görülmektedir¹⁴¹. Bu açıdan; veri paylaşımının mümkün olması sebebiyle intranet ve extranet ortamlarında da kişisel verilerin korunmaya muhtaç olduğu değerlendirilmektedir.

B. İnternet Aktörleri

1. İnternet Servis Sağlayıcı

a. İnternet Servis Sağlayıcının Diğer Aktörlerden Ayrılması

İnternet ortamında kişisel verilerin işlenmesinden kaynaklanan hukuki sorumluluğun tayin edilebilmesi adına öncelikle internet aktörlerinin irdelenmesi

¹³⁶ ÖZTEKİN, s. 107-108.

¹³⁷ MALIK, Sohail Jehangir/NAZLI, Hina/ABRAR, Kashif, “*Solving Organisational Problems with Intranet Technology.*” The Pakistan Development Review C.38, S. 4, 1999, s. 1022; KAYA, Turgut, İnternet Servis Sağlayıcılarının Hukuki ve Cezai Sorumluluğu, 1. Baskı, Ankara, 2019, s. 27.

¹³⁸ İtranetin ülke çapında kullanımına Kuzey Kore’de uygulanan *Kwangmyong* isimli kapalı devre İtranet ortamı verilebilir. Detaylı bilgi için bkz: ÖZTEKİN, s. 107.

¹³⁹ GALBREATH, Jeremy, “*The Internet: Past, Present, and Future.*” Educational Technology, C. 37, S. 6, 1997, s. 44; ÖZTEKİN, s. 107.

¹⁴⁰ LEHR, William/CLARK, David/BAUER, Steve/BERGER, Arthur/RICHTER, Philipp, “*Whither the Public Internet?*”, Journal of Information Policy, C. 9, 2019, s. 12.

¹⁴¹ GALBREATH, s. 42; ÖZTEKİN, s. 126.

gerekmektedir. Zira internetin karmaşık yapısı içerisinde çoğu zaman internet aktörlerinin arasındaki ayırım net olmamakta; aynı gerçek veya tüzel kişi aynı anda birden çok internet aktörü vasfını haiz olabilmektedir.

Mevzuatımızda internet aktörlerinin en genel tanımı 5651 sayılı Kanun'da yapılmıştır. "Tanımlar" başlıklı m. 4'te¹⁴² "erişim sağlayıcı", "içerik sağlayıcı", "yer sağlayıcı", "sosyal ağ sağlayıcı", "toplu kullanım sağlayıcı" kavramları tanımlanmıştır. Teknik açıdan yaygın bir ifade olan "internet servis sağlayıcı" ("İSS") (*Internet service providers* – ISP) kavramı 5651 sayılı Kanunda yer almamasına karşın; doktrinde kullanıcıların internetten yararlanmasını sağlayan çatı bir aktör olarak tanımlanmıştır¹⁴³. Buna karşın karşılaştırmalı hukuk bağlamında; yabancı literatürde İSS'nin eş anlamlısı olan ISP'nin internet erişimi sağlayan aktörlere indirgendiği görünmüştür¹⁴⁴.

Türk mevzuatında "internet servis sağlayıcı" kavramı tanımlanmamıştır¹⁴⁵. Literatürde ise bu kavram "*İnternetin kullanıcılara ulaştırılmasına ve kullanıcıların*

¹⁴² 5651 sayılı Kanun m. 4: "1) Bu Kanunun uygulamasında;

...
e) Erişim sağlayıcı: Kullanıcılarına internet ortamına erişim olanağı sağlayan her türlü gerçek veya tüzel kişileri,
f) İçerik sağlayıcı: İnternet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişileri,
i) Toplu kullanım sağlayıcı: Kişilere belli bir yerde ve belli bir süre internet ortamı kullanım olanağı sağlayan,
m) Yer sağlayıcı: Hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişileri,
s) Sosyal ağ sağlayıcı: Sosyal etkileşim amacıyla kullanıcıların internet ortamında metin, görüntü, ses, konum gibi içerikleri oluşturmalarına, görüntülemelerine veya paylaşımlarına imkân sağlayan gerçek veya tüzel kişileri ifade eder."

¹⁴³ ÖZTEKİN s. 201.

¹⁴⁴ RAMAN, Mittal, "Online Copyright Infringement Liability of Internet Service Providers", C.46, S. 2, Intellectual Property Rights Special Issue, 2004, s. 288.

¹⁴⁵ İnternet Servis Sağlayıcı kavramı tanımlanmamış olmasına karşın Elektronik Haberleşme Sektörüne İlişkin Yetkilendirme Yönetmeliği (R.G. Tarihi 28/05/2009, R.G. Sayısı 27241) Geçici m. 1 hükmünde herhangi bir tanımlama yapılmaksızın bu kavrama yer verilmiştir.

Elektronik Haberleşme Sektörüne İlişkin Yetkilendirme Yönetmeliği Geçici m. 1/III:

kullanımına sunulmasına aracılık eden unsurlar”¹⁴⁶ olarak tanımlanmıştır. Söz konusu tanımdan hareketle internet servis sağlayıcı kavramı, internet ortamının oluşmasını teknik açıdan mümkün kılan süjeler olarak açıklanabilir. Dolayısıyla çalışmamızda erişim sağlayıcılar ve yer sağlayıcılar; internet servis sağlayıcılar çatı başlığı altında incelenecektir.

Literatürde internet servis sağlayıcıların erişim sağlayıcılar ile eş anlamda kullanıldığı örneklerin yanı sıra; internet servis sağlayıcı kavramının, 5651 sayılı Kanun’da yer alan erişim sağlayıcı, içerik sağlayıcı, yer sağlayıcı kavramlarının hepsini karşıladığı; yerine getirdiği hizmete göre bu aktörlerden biri olacağı¹⁴⁷ yönünde görüşe tarafımızca iştirak edilmemektedir. Nitekim kanaatimizce, internet servis sağlayıcı internet ortamının teknik altyapısını oluşturulması faaliyetinde rol alan aktörleri işaret etmekte olup içerik sağlayıcılar teknik altyapıdan istifade ederek internet ortamına her türlü veriyi sağlayan aktörlerdir.

b. Erişim Sağlayıcı (Access Provider)

5651 sayılı Kanun md. 2/I-a bendinde “*kullanıcılarına internet ortamına erişim olanağı sağlayan her türlü gerçek veya tüzel kişiler*” olarak tanımlanan erişim sağlayıcılar, internet ortamında yalnızca içerikleri aktarılması ve bu içeriklerin başkaları

“Kablo Platform Hizmetine ilişkin olarak Kurumdan 2. Tip Telekomünikasyon Ruhsatı almış olan işletmeciler, Altyapı İşletmeciliği Hizmeti, **İnternet Servis Sağlayıcılığı** ve Kablolulu Yayın hizmeti için Kuruma bildirimde bulunmuş sayılırlar. Telefon hizmeti sunmak isteyen Kablo Platform Hizmeti işletmecilerinin ise, Sabit Telefon Hizmetine yönelik olarak Kuruma bildirimde bulunmaları ya da Kullanım Hakkı için ayrıca başvuruda bulunmaları gerekir.”

¹⁴⁶ YILDIZ, Sevil, *İnternet Servis Sağlayıcılar ve Cezai Sorumlulukları*, SÜİİBFSEAD, S. 3, 2002, s. 168.

¹⁴⁷ PEKER DEMİR, Esra, *İnternet Aracılığı ile Kişilik Haklarına Saldırı*, Yüksek Lisans Tezi, 2014, s. 129.

tarafından kullanılmasının sağlanması noktasında faaliyet yürütürler¹⁴⁸. 5651 sayılı Kanun m. 2/I-a’da erişim sağlayıcılar için “gerçek veya tüzel kişiler” ibaresi kullanılmış olmasına karşın “Telekomünikasyon Kurumu Tarafından Erişim Sağlayıcılara ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik”¹⁴⁹ m. 4¹⁵⁰ ve devamında; erişim sağlayıcıların, faaliyet belgesi almakla mükellef olduğu, bu faaliyet belgesinin de yalnızca sermaye şirketlerine verilebileceği hüküm altına alınmıştır. Bu açıdan yönetmelik ile kanun hükmünün daraltıldığını, gerçek kişilerin erişim sağlayıcı olamayacağını belirtmek mümkündür.

Uygulamada sıklıkla erişim sağlayıcılar, İSS/ISP ile aynı anlamda kullanılmaktadır. ISS/ISP’ler -yukarıda tafsilatlı şekilde açıklandığı üzere- internet ortamının teşekkülünü sağlayan unsurların genel ismi iken; erişim sağlayıcılar yalnızca internet erişimini sağlama noktasında faaliyet yürüten internet servis sağlayıcılarıdır¹⁵¹.

5809 sayılı Kanun¹⁵² ve “Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunmasına İlişkin Yönetmelik”¹⁵³,te “*elektronik haberleşme hizmeti sunan ve/veya elektronik haberleşme şebekesi sağlayan ve altyapısını işleten şirket*”ler işletmeci olarak tanımlanmıştır. Belirtilen mevzuattaki işletmeci kavramı, 5651 sayılı Kanun’daki “erişim sağlayıcı” ile aynıdır¹⁵⁴. Çünkü; Elektronik haberleşme

¹⁴⁸ KAYA, s. 33.

¹⁴⁹ R.G. Tarihi 24/10/2007, R.G. Sayısı 26680.

¹⁵⁰ Telekomünikasyon Kurumu Tarafından Erişim Sağlayıcılara ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik m.4/I: “Türkiye Cumhuriyeti sınırları içerisinde erişim sağlayıcı olmak isteyen sermaye şirketleri ile yer sağlayıcı olarak faaliyet göstermek isteyen gerçek veya tüzel kişiler, hizmet vermeye başlamadan önce Kurum tarafından düzenlenecek faaliyet belgesini almakla yükümlüdür.”

¹⁵¹ SOSYAL, Tamer, İnternet Servis Sağlayıcılarının Hukuki Sorumlulukları, TBBD, S. 61, 2005, s. 309

¹⁵² 5809 sayılı Elektronik Haberleşme Kanunu, R.G. Tarihi 10/11/2008, R.G. Sayısı 27050 Mükerrer

¹⁵³ R.G. Tarihi 04/12/2020, R.G. Sayısı 31324.

¹⁵⁴ ÖZTEKİN, s. 203.

bağlamında altyapı ve şebeke sağlanması internete erişim sağlama olanağıyla doğrudan bağlantılıdır. Öte yandan “Telekomünikasyon Kurumu Tarafından Erişim Sağlayıcılara ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik”te erişim sağlayıcıların yalnızca tüzel kişilerle sınırlandırılmıştır.

Erişim sağlayıcılar; kendi kurdukları veya başka bir erişim sağlayıcının kurduğu uydular, baz istasyonları, radyolink sistemleri, telefon hatları veya televizyon hatları üzerinden geçen internet ağ altyapısı üzerinden internet ortamı süjelerinin birbirleriyle bağlantı kurmasını sağlayan internet servis sağlayıcılarıdır. Turkcell İletişim Hizmetleri A.Ş. ve TTNNet A.Ş. gibi yaygın erişim sağlayıcıların yanı sıra ticari amaçlı olmayan TÜBİTAK/ULAKBİM de işlettiği ULAKNET¹⁵⁵ ağı bakımından teknik açıdan erişim sağlayıcıdır¹⁵⁶. “Telekomünikasyon Kurumu Tarafından Erişim Sağlayıcılara ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik”te erişim sağlayıcı olmak isteyen sermaye şirketlerinin faaliyet belgesi alması gerektiğinin hüküm altına alınması ve ULAKBİM’in sermaye şirketi olmaması nedeniyle ULAKBİM’in erişim sağlayıcı sayılmayacağı, erişim sağlayıcıların yalnızca özel hukuk tüzel kişileri arasından belirlenebileceğine ilişkin görüşe¹⁵⁷ tarafımızca iştirak edilmemektedir. Nitekim kanaatimizce “Telekomünikasyon Kurumu Tarafından Erişim Sağlayıcılara ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik”te hüküm altına alınan faaliyet belgesi müessesesi erişim sağlayıcılık için kurucu şart değil özel şahıslara yönelik bir yükümlülük olarak öngörülmüştür. Dolayısıyla kamu tüzel kişiliklerinin, sermaye şirketi olmaması erişim

¹⁵⁵ ULAKNET Kullanım Politikası m.3: *ULAKNET; 17/07/1963 tarih ve 278 sayılı “TÜBİTAK Kurulması Hakkında Kanun”daki görevlendirme çerçevesinde, Türkiye Cumhuriyeti yasalarına ve TÜBİTAK mevzuatına uygun olarak, eğitim ve araştırma kuruluşlarının elektronik haberleşme hizmeti ve/veya elektronik haberleşme altyapısı gereksinimlerinin karşılandığı Ulusal Akademik Ağ’dır.*

¹⁵⁶ ÖZTEKİN, s. 205-206.

¹⁵⁷ ÖZTEKİN, s. 206.

sağlayıcı olma vasıflarını etkilememekte; yalnızca faaliyet belgesi edinme noktasında kanuni bir muafiyet getirmektedir. Dolayısıyla binlerce akademik personel ve öğrencinin kişisel verilerinin iletildiği ULAKNET sisteminin işletmecisi olan ULAKBİM'in de kişisel verilerin internet ortamında işlenmesi noktasında erişim sağlayıcı vasfı ile sorumlu olacağı mütalaa edilmektedir.

c. Yer Sağlayıcı (*Hosting Provider*)

Yer sağlayıcılık kavramı mevzuatımızda en temel olarak 5651 sayılı Kanun'da¹⁵⁸ “*hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişiler*” şeklinde tanımlanmıştır. Erişim sağlayıcılar hususunda ortaya çıkan tenakuz yer sağlayıcı tanımında görülmemiş olup “Telekomünikasyon Kurumu Tarafından Erişim Sağlayıcılara ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik”¹⁵⁹ ve “İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik”¹⁶⁰ hükümlerinde de aynı tanıma yer verilerek mevzuat içerisinde yeknesaklık sağlanmıştır.

İnternet yer sağlayıcısı, internet ortamındaki her türlü içeriği barındıran dijital bir depo işletmecisi niteliğindedir¹⁶¹. Bahsi geçen her türlü içeriği belli bir kapasite

¹⁵⁸ 5651 sayılı Kanun m. 2/I-m: “*Yer sağlayıcı: Hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişileri, ifade eder.*”

¹⁵⁹ Telekomünikasyon Kurumu Tarafından Erişim Sağlayıcılara ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik m.3/1/ş: “*Yer sağlayıcı: İnternet ortamında hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişileri,*”

¹⁶⁰ İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik m.3/I-s: “*Yer sağlayıcı: İnternet ortamında hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişileri*”

¹⁶¹ ÖZEL, Sibel, Uluslararası Alanda Medya ve İnternette Kişilik Hakkının Korunması, 1. Baskı, Ankara, 2004, s. 287.

kapsamında barındıran bu depolar ise sunucu (*server*) olarak isimlendirilir¹⁶². Dolayısıyla bir bakıma sunucular, başka kullanıcılara ait verileri tutan bilgisayar sistemleridirler. Bu noktada dikkat edilmesi gereken husus; sunucuların, gerçek veya tüzel kişi statüsünde bir internet aktörü olmadığıdır. Sunucuları işletmek suretiyle internet ortamındaki hizmet ve içeriklerin, işlettikleri sunucularda barındırılmasını sağlayan gerçek veya tüzel kişiler ise yer sağlayıcı sıfatıyla internet aktörüdür. Bu durum, kişisel verilerin işlenmesinden doğan hukuki sorumluluğun tayini noktasında basit ama önemli bir ayrımıdır.

Yukarıdaki açıklamalardan hareketle; erişim sağlayıcının sunduğu bağlantı aracılığıyla iletilen içeriklerin ve hizmetlerin barındırıldığı sunucuyu işleten gerçek veya tüzel kişi yer sağlayıcıdır¹⁶³. Burada önemle altı çizilmesi gereken nokta ise aynı kişinin hem erişim sağlayıcı hem yer sağlayıcı sıfatını haiz olabileceğidir. Söz gelimi; Turkcell’e ait sunucularda barındırılan bir internet sayfasına Turkcell tarafından sunulan bir altyapı aracılığıyla bağlantı sağlanarak veri işlenirse, bu noktada Turkcell’in hem erişim sağlayıcı hem yer sağlayıcı olarak sorumlu olacağını belirtmek mümkündür.

Yer sağlayıcının hizmet ve içeriklerin barındırıldığı sunucuların mülkiyet hakkını haiz olmaması, yer sağlayıcılık vasfına hâlel getirmemektedir¹⁶⁴. Nitekim kanun koyucu, 5651 sayılı Kanun’da yer sağlayıcılık tanımını “*sağlayan veya işleten*” ibaresi çerçevesinde şekillendirmiştir. Dolayısıyla, mülkiyeti başkasına ait bilgisayar sistemlerini, kendisine veya başkasına ait içerik ve hizmetleri barındırmak adına işleten kişi “işleten” ibaresi gereğince yer sağlayıcı olurken; mezkur sistemlerin zilyedi olmayan malik “sağlayan” ibaresi gereğince yer sağlayıcı sayılacaktır.

¹⁶² AVŞAR, Zakir/ÖNGÖREN Gürsel, Bilişim Hukuku, İstanbul, 2010, s. 120; SOSYAL, s. 309.

¹⁶³ ÖZBAKIR, s. 52.

¹⁶⁴ ÖZTEKİN, s. 252-253.

Yer sağlayıcıların işlettikleri veya sağladıkları sistemlerdeki verinin büyüklüğü ve karmaşıklığı nedeniyle kanun koyucu 5651 sayılı Kanun m. 5/I'de¹⁶⁵, yer sağlayıcılara barındırdıkları hukuka aykırı verilerden kural olarak sorumsuzluk öngörmüştür. Burada sorumsuzluğun sınırı yer sağlayıcının hukuka aykırı içeriğin varlığını bilmediği durumlar ile sınırlı tutulmuştur. Dolayısıyla yer sağlayıcı, hukuka aykırı içerikten haberdar edildiği anda sorumsuzluk ortadan kalkmaktadır¹⁶⁶. Yer sağlayıcıların işlettikleri sunucular vasıtasıyla depoladıkları üçüncü kişilere ait verileri teknik açıdan tasnifleyerek hukuka aykırı bir kişisel veri işleme faaliyeti olup olmadığını tespit etmesi mümkün değildir. Bu nedenle çalışmanın konusu bağlamında kişisel verilerin bir sunucuda hukuka aykırı olarak kaydedilmesi, depolanması, muhafaza edilmesinden mezkûr sunucuyu sağlayan veya işleten yer sağlayıcının haberdar edilene kadar sorumlu olmadığı değerlendirilmektedir.

Yer sağlayıcılar, işlettikleri veya sağladıkları sunucular vasıtasıyla salt başka internet kullanıcılarına ait verileri barındıran kişiler olarak sınırlandırılmamalıdır. Nitekim 5651 sayılı Kanun'da yer alan ve yukarıda açıklanan tanımda yer verildiği üzere; yer sağlayıcılar internet ortamındaki yalnızca içerikleri değil hizmetleri de barındıran sistemleri işletmekte veya sağlamaktadırlar. Dolayısıyla; kullanıcıların içerik paylaşımı yapılmasına olanak tanıyan forum sitelerini, satış ilanları verebildiği e-ticaret sitelerini ve buna benzer üçüncü kişilerin içerik sunmasına imkân sağlayan internet sitelerini işleten gerçek veya tüzel kişiler de yer sağlayıcı sıfatını haizdir¹⁶⁷. Bunun yanında; bu tarz internet sitelerin işletmecileri yer sağlayıcılık sıfatını taşımanın yanı sıra mezkûr sitelere

¹⁶⁵ 5651 sayılı Kanun m. 5/I: “Yer sağlayıcı, yer sağladığı içeriği kontrol etmek veya hukuka aykırı bir faaliyetin söz konusu olup olmadığını araştırmakla yükümlü değildir.”

¹⁶⁶ KAYA, s. 35.

¹⁶⁷ ÖZBAKIR, s. 52-53.

kendilerince üretilen veya paylaşılan içeriklerden ötürü aynı zamanda içerik sağlayıcı sıfatına sahiptirler.

2. İçerik Sağlayıcılar (*Content Providers*)

İçerik sağlayıcılar, 5651 sayılı Kanun'un m. 2/1-f'de tanımlanmış olup bu tanıma göre içerik sağlayıcılar “*internet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişiler*”dir¹⁶⁸. Aynı tanıma; “Telekomünikasyon Kurumu Tarafından Erişim Sağlayıcılara ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik” m. 3/I-1 ve “İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik” m. 3/I-1’da da yer verilmiştir. Tanımdan da anlaşılacağı üzere, içerik sağlayıcı internet ortamının teşekkülü noktasında teknik açıdan herhangi bir hizmet sağlamamaktadır.

Tanımda yer alan “üretme, değiştirme ve sağlama” ifadesi muğlaklık oluşturmaktadır¹⁶⁹. Öncelikle “sağlayıcılık” kavramının tanımında “sağlama” kelimesine yer verilmesi, tekerrüre sebep olmuştur. Bu nedenle içerik sağlayıcı olmanın şartını içeriği üretme ve değiştirme olarak ele almak daha isabetli olacaktır. Tanımda belirtildiği üzere içerik sağlayıcılar gerçek ve tüzel kişilerden oluşabilmektedir. Dolayısıyla bir kişinin internet ortamında yer alan herhangi bir içeriği üretmiş veya değiştirmiş olması başka bir koşula bağlı olmaksızın o kişiye “içerik sağlayıcı” sıfatını kazandıracaktır. Bu kapsamda; içerik sağlayıcılar grubuna kamu kurumları, özel işletmeler, çok uluslu şirketler vb. çok geniş bir yelpazedeki şahıslar girmektedir¹⁷⁰.

¹⁶⁸ 5651 sayılı Kanun m. 2/I-f.

¹⁶⁹ ÖZTEKİN, s. 373.

¹⁷⁰ AVŞAR/ÖZGÖREN, s. 120.

Günümüzde internet ortamı, yalnızca internet sitelerinin işletmecilerinin veri yüklediği statik depolar değildir. ABD’li yazar Tim O’REILLY tarafından 2004 yılında bir konferansta ortaya atılan “*Web 2.0*” kavramı ile internetin artık yalnızca kullanıcılara içerik sunulan bir ortam değil, kullanıcıların da içerik oluşturabildiği interaktif bir ortam olduğu öne sürülmüştür¹⁷¹. Buradan hareketle artık içerik sağlayıcı tanımını yalnızca internet sitesi işletmecilerine indirgemenin mümkün olmadığını belirtmek mümkündür. Nitekim; *Web 2.0* ile birlikte internette veri akışı tek taraflı olmaktan çıkmıştır. Bu durum da içerik sağlayıcı tanımının kapsamını geniş ele alınması sonucunu doğurmaktadır. 5651 sayılı Kanun’da yer alan tanımdan hareketle internet ortamında herhangi bir içeriği üretmiş veya değiştirmiş olan basit bir kullanıcı da içerik sağlayıcı olabilecektir.

İçerik sağlayıcılık kavramı, yukarıda açıklandığı üzere dinamik olup durumun şartlarına göre internet ortamına erişim sağlayan her süjenin kazanabileceği bir sıfattır. Buna göre kendisi veya başkası tarafından üretilmiş bir içeriği kendisine veya başkasına ait bir internet sayfasına yükleyen kişi, internette yer alan gazeteleri hazırlayanlar, gazete haberine yorum yazısı girenler¹⁷², yalnızca bu durumlarla sınırlı olmamakla beraber somut olay kapsamında içerik sağlayıcı sıfatını haiz olurlar.

Herhangi bir internet süjesinin içerik sağlayıcı olabilmesi için evleviyetle gerçek veya tüzel kişi olmalıdır. Sunucular, daha önceki bölümlerde açıklandığı üzere yer sağlayıcılar tarafından internette yer alan içeriklerin depolanması amacıyla kullanılan fiziki ortamlardır. Gerçek veya tüzel kişi olmayan sunuculara ne içerik sağlayıcı ne de yer sağlayıcı sıfatıyla sorumluluk atfetmek mümkün değildir. Çalışmamız öznesinde

¹⁷¹ LEE, Bryan/ZOLOTOVA, Margarita, “*Web 2.0, Social Media, and the ‘New’ Media.*” *New Media Solutions in Nonproliferation and Arms Control: Opportunities and Challenges*, James Martin Center for Nonproliferation Studies, 2013, s. 10-11.

¹⁷² DÜLGER, Murat Volkan, Bilişim Suçları ve İnternet İletişim Hukuku, 9. Baskı, 2022, s. 693.

değerlendirildiğinde sunucuların bu durumunun tespit edilmesi, kişisel verilerin işlenmesi sürecinde sunucular aparat olarak kullanıldığından önem arz etmektedir.

3. Toplu Kullanım Sağlayıcı

Toplu kullanım sağlayıcılar 5651 sayılı Kanun'da¹⁷³ “*belli bir yerde ve belli sürede internet kullanım olanağı sağlayan kişiler*” olarak tanımlanmıştır. Tanım itibarıyla erişim sağlayıcılara benzese de toplu kullanım sağlayıcılar erişim sağlayıcılar ile karıştırılmamalıdır. Esasında toplu kullanım sağlayıcı da internete erişimi erişim sağlayıcılar gibi teknik açıdan mümkün kılmaktadır. Buna karşın erişim sağlayıcılık söz konusu olduğunda kullanıcılar kendilerine ait bilgisayarlar vasıtasıyla kendilerine özel şifre ile erişim sağlayıcının bilgisayarlarına erişmek suretiyle internete bağlanırken; toplu sağlayıcılık söz konusu olduğunda kullanıcı toplu sağlayıcıya ait bilgisayarlardan erişim sağlamaktadır.

Toplu kullanım sağlayıcılar belirli bir yerde ve belirli sürede internet kullanım olanağı sağladıkları için erişim sağlayıcılara nazaran kullanıcılara daha kısıtlı bir hizmet sağlamaktadırlar. Somutlaştırmak icap ederse; şirketler, oteller, kafeler, üniversiteler, AVM'ler, internet kafeler toplu kullanım sağlayıcı kategorisine girmektedir¹⁷⁴. Erişim sağlayıcılar ise, mekan mefhumundan ari bir şekilde kullanıcılara kendi cihazlarından internete erişme imkanı sağlamaktadır.

¹⁷³ 5651 sayılı Kanun m. 2/I-i: “*Toplu kullanım sağlayıcı: Kişilere belli bir yerde ve belli bir süre internet ortamı kullanım olanağı sağlayan ... ifade eder.*”

¹⁷⁴ ÖZTEKİN, s. 364.

Toplu kullanım sağlayıcıların yükümlülükleri “İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik”¹⁷⁵ m. 4¹⁷⁶ ve m. 5¹⁷⁷ hükümlerinde düzenlenmiştir. Yönetmelik ticari amaçla toplu kullanım sağlama ile adi toplu kullanım sağlayıcılık arasında yükümlük açısından farklılıklar öngörmüştür. Bu farklardan en dikkat çeken ticari amaçla toplu kullanım sağlayıcılık için bir izin müessesesi düzenlenmiş olmamasıdır¹⁷⁸.

Toplu kullanım sağlayıcının ticari amaç güdüp gütmemesinden bağımsız olarak “İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik”te düzenlenen “cihaz verilerini kayıt” ve “kullanıcıları tanımlayacak sistemleri kurma” yükümlülükleri¹⁷⁹

¹⁷⁵ R.G. Tarihi: 11/04/2017, R.G. Sayısı: 30035.

¹⁷⁶ “1) İnternet toplu kullanım sağlayıcılarının yükümlülükleri şunlardır:

a) Konusu suç oluşturan içeriklere erişimi önleyici tedbirleri almak amacıyla içerik filtreleme sistemini kullanmak.

b) Erişim kayıtlarını elektronik ortamda kendi sistemlerine kaydetmek ve iki yıl süre ile saklamak.

c) Kamuya açık alanlarda internet erişimi sağlayan toplu kullanım sağlayıcılar, kısa mesaj servisi (sms) ve benzeri yöntemlerle kullanıcıları tanımlayacak sistemleri kurmak.

2) İnternet toplu kullanım sağlayıcılar, konusu suç oluşturan içeriklere erişimi önleyici tedbirleri almak amacıyla içerik filtreleme sisteminin yanı sıra, ilave tedbir olarak güvenli internet hizmeti de alabilirler.”

¹⁷⁷ “1) Ticarî amaçla internet toplu kullanım sağlayıcılarının yükümlülükleri şunlardır:

a) Mülki idare amirinden izin belgesi almak,

b) Ailenin ve çocukların korunması ile konusu suç oluşturan içeriklere erişimi önleyici tedbirleri almak amacıyla içerik filtreleme sistemini ve güvenli internet hizmetini kullanmak,

c) Kullanılan içerik filtreleme sistemini aktif ve güncel halde bulundurarak, herhangi bir müdahale ile devre dışı kalmasını önlemek,

ç) Erişim sağlayıcılardan sabit IP almak, sabit IP kullanmak ve sabit IP değişikliklerini on beş gün içerisinde mülki idare amirliklerine bildirmek,

d) Erişim kayıtlarını elektronik ortamda kendi sistemlerine kaydetmek ve iki yıl süre ile saklamak,

e) (d) bendi gereğince kaydedilen bilgileri ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini teyit eden değeri kendi sistemlerine günlük olarak kaydetmek ve bu verileri iki yıl süre ile saklamak,

f) 14/7/2005 tarihli ve 2005/9207 sayılı Bakanlar Kurulu Kararıyla yürürlüğe konulan İşyeri Açma ve Çalışma Ruhsatlarına İlişkin Yönetmeliğe göre işyerinin kapatılmasının veya devrinin on beş gün içinde yetkili mülki idare amirliğine bildirmek ve izin belgesini teslim etmek.”

¹⁷⁸ AVŞAR/ÖNGÖREN, s. 96-97.

¹⁷⁹ ÖZTEKİN, s. 368.

kişisel verilerin işlenmesi süreciyle ilintili görünmektedir. Toplu kullanım sağlayıcılar Yönetmelik'in m.4/I-b hükmü uyarınca erişim kayıtlarını iki yıl süreyle saklamakla mükelleftir. Kullanıcıların eriştiği internet içeriklerine ilişkin erişim kayıtlar kişisel veri oluşturmakla beraber toplu kullanım sağlayıcılar için kanuni bir hukuka uygunluk sebebinin oluştuğunu belirtmek mümkündür. Yönetmelik'in m.4/I-c'de düzenlenen kullanıcıların "kullanıcıları tanımlayacak sistemleri kurma yükümlülüğü" ise kısa mesaj gibi doğrulama sistemlerinden istifade ederek tekil kullanıcının kimliğini tespitini amaçlamaktadır. Gerek telefon numarası, gerek tekil kullanıcının diğer kimlik bilgileri ve trafik bilgisi gibi verilerin kişisel veri oluşturacağı göz önüne alındığında bu verilerin KVKK uyarınca işlenme amacına uygun şekilde muhafaza edilmesi gerekmektedir.

Toplu kullanım sağlayıcılık en az iki kişiye belirli bir mekanda belirli bir vakitte internete erişim sağlamak olarak tanımlanmış olup¹⁸⁰ kanaatimizce kullanıcı ile toplu kullanım sağlayıcı arasındaki ilişki internet ortamına erişmeye kadar olan safhada vukuu bulmaktadır. Dolayısıyla kullanıcının kişisel verilerinin internet ortamına eriştikten sonraki safhada hukuka aykırı işlenmesinden toplu kullanım sağlayıcının sorumluluğu doğmamaktadır.

4. İnternet Sitesi İşletmecileri

a. İşletmecilerin Diğer Aktörlerden Ayrılması

İnternet sitesi işletmecileri 5651 sayılı Kanun'da tanımlanan internet aktörlerine göre değişiklik arz etmektedir. Yukarıda kişisel verilerin işlenmesi bağlamında tafsilatlı şekilde açıklanan içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı gibi internet aktörleri, internet ortamında yer alan süjelere somut olaya göre verilen sıfat mahiyetindedir.

¹⁸⁰ SAĞLAM, Kadir, İnternet Aktörlerinin 5651 Sayılı Kanun Kapsamındaki İdari Sorumluluğu, Yüksek Lisans Tezi, Ankara, 2022, s. 34.

İnternet siteleri ise her türlü işaret, yazı, ses, görüntü gibi ögeyi içinde barındıran bir bütündür¹⁸¹. Bu bütünü yöneten veya bu bütünün maliki olan şahıslar ise internet sitesi işletmecileridir.

İnternet sitesi işletmecilerini, 5651 sayılı Kanun’da yer alan internet aktörlerinden yalnızca biri olarak kabul etmek mümkün olmamakla beraber; bir internet sitesi işletmecisi somut olayın mahiyetine göre bu sıfatlardan bir veya birkaçını kazanabilir. Örneğin; internet sitesine ait olan verileri başka bir sunucuda depolayan işletmeci kişisel verilerin hukuka aykırı işlenmesinden yer sağlayıcı sıfatıyla sorumlu olmayacaktır¹⁸².

b. Sosyal Ağ Sağlayıcı

Sosyal medya, insanların küresel ölçekte birbirleriyle çok çeşitli şekilde etkileşim kurmasına imkân sağlayan platformları ifade etmektedir¹⁸³. Tanımdan da anlaşılacağı üzere sosyal medya platformlarının yapısı gereği kişisel verilerin işlenmesi hususunda ana odak olduğunu belirtmek mümkündür. Bu itibarla; çalışmamızın konusu olan internet ortamında kişisel verilerin işlenmesinden doğan hukuki sorumluluk bağlamında, sosyal medyanın önemi göz önüne alındığında sosyal medyayı sağlayan kişinin tayini önem arz etmektedir. Sosyal ağ sağlayıcılığı, 5651 sayılı Kanunda yürürlük tarihinden sonra

¹⁸¹ BAŞPINAR, Veysel/KOCABEY, Doğan, İnternette Fikri Hakların Korunması, 1. Baskı, Ankara, 2007, s. 73; ZORLUUEL, Mustafa, Fikrî Haklar Bağlamında İnternet Sitelerinin ve Web Sayfalarının Eser Niteliği – Fikri Mülkiyet Hukuku Monografileri, 1. Baskı, Ankara, 2022, s. 31.

¹⁸² ÖZTEKİN, s. 294.

¹⁸³ OYMAK, Hasan, 7253 Sayılı “İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun”’un Getirdikleri, Yeni Medya Dergisi, Ankara Hacı Bayram Veli Üniversitesi İletişim Fakültesi, S. 9, 2020, s. 129, AKKURT, Sami Sinan, Sosyal Medyada Gerçekleşen İhlaller Karşısında Kişilik Hakkının Korunması, 1. Baskı, Ankara, 2020 s. 134-135; ÖZTEKİN, s. 297-298; KULULAR İBRAHİM, Merve Ayşegül, Sosyal Medyaya Yönelik Yeni Düzenlemelerin Hukukî Değerlendirilmesi, Bilişim Hukuku Dergisi, C. 4, S. 1, 2022, , s. 14.

gerçekleştirilen düzenleme¹⁸⁴ ile mevzuatımızda yer bulan bir tanımlamadır. Belirtilen tanıma göre sosyal ağ sağlayıcı; “sosyal etkileşim amacıyla kullanıcıların internet ortamında metin, görüntü, ses ve konum gibi içerikleri oluşturmalarına, görüntülemelerine veya paylaşımlarına imkân sağlayan gerçek veya tüzel kişileri” ifade etmektedir.

Sosyal ağ sağlayıcı kavramı mevzuatımızda münferiden tanımlanmadan önce, sosyal medya platformlarını işleten gerçek veya tüzel kişilerin sorumlulukları 5651 sayılı Kanunda yer alan “yer sağlayıcı” ve “içerik sağlayıcı” kavramları üzerinden belirlenmekte idi. Sosyal ağ sağlayıcıların kural olarak kendi yükledikleri içerikten içerik sağlayıcı olarak; kullanıcıların paylaşımlarından ise paylaşımları yapacak ortamı sundukları için yer sağlayıcı olarak sorumlu olduğu kabul edilmekteydi¹⁸⁵. Bu durumu örnek ile somutlaştırmak gerekirse; bir mikroblog sitesi olan *X* (eski adıyla *Twitter*)’de herhangi bir kullanıcının paylaştığı yazıdan *X*’in işletmecisi yer sağlayıcı olarak sorumlu iken, sitesinde yayımladığı topluluk kurallarından içerik sağlayıcı olarak sorumlu olmaktaydı.

7253 sayılı Kanun ile sosyal ağ sağlayıcı kavramının mevzuatta tanımlanması, sosyal medya sitesi işletmecilerinin içerik sağlayıcılık ve yer sağlayıcılıktan kaynaklanan sorumluluklarını ilga etmemiş olup yeni sorumluluklar getirmiştir¹⁸⁶. Mezkûr düzenleme,

¹⁸⁴ 7253 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun, R.G. Tarihi 31.07. 2020, R.G. Sayısı 31202, m. 1: “4/5/2007 tarihli ve 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunun 2 nci maddesinin birinci fıkrasının (j) bendine “IP adresi,” ibaresinden sonra gelmek üzere “port bilgisi,” ibaresi ve fıkraya aşağıdaki bent eklenmiştir.

“s) Sosyal ağ sağlayıcı: Sosyal etkileşim amacıyla kullanıcıların internet ortamında metin, görüntü, ses, konum gibi içerikleri oluşturmalarına, görüntülemelerine veya paylaşımlarına imkân sağlayan gerçek veya tüzel kişileri,”

¹⁸⁵ AKKURT, s. 135.

¹⁸⁶ AKKURT, s. 176.

doğrudan iktibas edilmemesine karşın büyük oranda Alman Ağ Yasası olarak bilinen NetzDG¹⁸⁷’den esinlenilmiştir. NetzDG Almanya’da temelde internet ortamındaki zararlı içeriklerle mücadele için çıkarılmış ve idare lehine sosyal ağ sağlayıcılara birtakım yükümlülükler getirmiştir¹⁸⁸. NetzDG’de çalışmamızın konusunu oluşturan kişisel verilere ilişkin olarak; sosyal ağ sağlayıcılara konusu tahdidi olarak sayılmış olan suçları oluşturan içeriklerin paylaşan kullanıcılara ilişkin bilgileri adli makamlarla paylaşma yükümlülüğü getirilmiştir¹⁸⁹.

Sosyal medya sitelerinin, kullanıcıların birbirleriyle etkileşim halinde fotoğraf, video, metin vb. şekillerde paylaşım olanağı veren yapısının; kişisel veriler bağlamında bu platformları oldukça önemli kıldığı hususu izahtan varestedir.

Birinci bölümde tafsilatlı şekilde açıklandığı üzere gerçek bir kişi ile ilişkilendirilebilecek her türlü bilgi kişisel veri sayılmaktadır. Sosyal medyada kullanıcı gerçek şahısla ilişkilendirilebilecek ve kimliğini tespiti yarayabilecek verilerin yüklendiği göz önüne alındığında sosyal ağ sağlayıcıların sorumlu olduğu kişisel veri miktarı da artmaktadır. Bu kapsamda; kullanıcıların sosyal medya sitelerine kayıt olmasının tek başına kişisel verilerinin işlenmesine zımni bir onay niteliği taşıdığı kabulü mümkün değildir¹⁹⁰. Bununla beraber; kişinin umuma açık şekilde paylaştığı verilerin işlenmesi noktasında sosyal ağ sağlayıcıya da zımni rıza verdiği akla gelmektedir. Kişi, umuma açık şekilde paylaşım yaptığında, paylaşımında yer alan kişisel verilerin herhangi bir şahsın tarafından depolanabileceği veya üçüncü kişilerle paylaşılabilirliğini göze aldığını kabul etmek gerekir. Herhangi bir şahıs tarafından

¹⁸⁷ Sosyal Ağlarda Hukuk Uygulamasının İyileştirilmesi Hakkında Kanun -*Das deutsche Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken*) Alman Federal Meclisi tarafından 01/09/2017 tarihinde yayımlanan yasa.

¹⁸⁸ YURDAKUL, Afşin, *The Impact of Polarization On Turkey's Information Environment*, Ekonomi ve Dış Politika Araştırmalar Merkezi (EDAM), 2020, s. 16.

¹⁸⁹ NetzDG, §2/1/(1).

¹⁹⁰ AKKURT, s. 206.

kolaylıkla depolanmak veya aktarılmak suretiyle işlenebilecek kişisel veriler için sosyal ağ sağlayıcıya kısıtlama getirmek fiilen mümkün değildir.

II. İNTERNET ORTAMINDA KİŞİSEL VERİLERİN İŞLENMESİ SÜRECİ

A. Genel Çerçeve

Kişisel verilerin internet ortamında işlenmesinden doğan sorumluluğun tayini için kişisel verilerin işlenmesi sürecini incelemek gerekmektedir. KVKK’de kişisel verilerin işlenmesi m.3/I-e’de¹⁹¹ tanımlanmıştır. Sözü geçen tanıma göre; elde etmek, kaydetmek, depolamak, muhafaza etmek, değiştirmek, yeniden düzenlemek, açıklamak, aktarmak, devralmak, elde edilebilir hale getirmek, sınıflandırmak, kullanılmasını engellemek eylemlerinin her biri münferiden veya müştereken kişisel verilerin işlenmesi durumunu oluşturmaktadır. Öte yandan; kanun koyucu, kişisel verilerin işlenmesi durumunu oluşturan eylemlerin ardından “gibi” bağlacına yer vererek kişisel verilerin işlenmesi teşkil eden eylemlerin tahdidi olarak belirlenmediğini, farklı eylemlerle de kişisel verilerin işlenebileceğini ortaya koymuştur.

Kişisel verilerin işlenmesine ilişkin KVKK’de yer alan tanıma göre kişisel verilerin işlenmesi sürecinin hukuken vukuu bulması için “*tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik*

¹⁹¹ KVKK m.3/I-e: “Bu Kanunun uygulanmasında;

...

e) Kişisel verilerin işlenmesi: Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi,

...

ifade eder.”

olmayan yollarla” işlenmesi şartı aranmıştır. Buna karşın KVKK’de otomatik yollarla veri işlemenin tanımına yer verilmemiştir. GDPR m. 4/II’e¹⁹² bakıldığında kişisel veri işlenmesine yönelik eylemlerin otomatik veya otomatik olmayan sistemlere gerçekleştirilmesinin önem arz etmediği görülmektedir. Bu noktada KVKK, GDPR’ye göre farklılık göstermektedir. KVKK’de, otomatik olmayan yollarla gerçekleştirilen eylemlerin, kişisel verilerin işlenmesi olarak görülmesi için “veri kayıt sisteminin parçası” olması gerektiği hükmedilmiştir. Veri kayıt sistemleri ise KVKK m.3/I-h’de “*kışisel verilerin belirli kriterlere göre yapılandırılarak işlendiğı sistemler*” olarak tanımlanmıştır. Otomatik yolla veri işlenmesi tanımlanmamış olmakla birlikte; bilgisayar gibi teknik destek ile işleme süreçlerinin otomatik veri işleme süreci olduğı değerlendirilmektedir¹⁹³. Dolayısıyla çalışmamızın konusu bağlamında; kişisel verilere yönelik internet ortamında gerçekleştirilen eylemler, her hâl ve kârda KVKK kapsamında kişisel verilerin işlenmesi olarak kabul edilmektedir.

Kişisel verilerin korunması meselesi; kişisel veri sahibi ile veri işleyen kişi arasında dengenin oluşturulması sürecidir. Bu nedenle kişisel verilerin korunması, üç aşamalı olarak ele alınmaktadır. Kavramsal çerçeve ve temel ilkelerin yanı sıra işleme gerekçeleri, kişisel verilerin korunması sürecinde göz önünde bulundurulmaktadır¹⁹⁴.

¹⁹² GDPR m.4/II: “*işleme faaliyeti, otomatik yöntemlerle olsun veya olmasın, kişisel veri veya kişisel veri setleri üzerinde gerçekleştirilen toplama, kaydetme, düzenleme, yapılandırma, saklama, uyarılma veya değıştirme, elde etme, danışma, kullanma, iletim yoluyla açıklama, yayma veya kullanıma sunma, uyumlaştırma ya da birleştirme, kısıtlama, silme veya imha gibi herhangi bir işlem veya işlem dizisidir*”

¹⁹³ BASKIN, Onur, Türk Hukuku Bakımından Kişilik Hakkı Kapsamında Kişisel Verilerin Korunması, 1. Baskı, Ankara, 2021, s. 56-57.

¹⁹⁴ TURAN, s. 70.

B. Hâkim İlkeler

1. Hukuka ve Dürüstlük Kurallarına Uygunluk ve Şeffaflık

Dürüstlük kurallarına uygun davranma yükümlülüğü TMK m. 2/I¹⁹⁵'de düzenlenmiştir. Buna göre; salt kişisel verilerin işlenmesinde değil; her türlü hukuki ilişkide dürüstlük kurallarına uygun davranmak Türk hukukunda genel bir ilkedir. Kişisel verilerin işlenmesi sürecinde de ortalama zekalı, makul, objektif mantıklı bir insanın hareket tarzı, dürüstlük kuralına uygunluk ölçütü olarak ele alınmaktadır¹⁹⁶.

Hukuka ve dürüstlük kurallarına uygunluk ilkesi, diğer ilkeleri de kapsayan çatı bir ilke olarak görülmektedir¹⁹⁷. KVKK'de doğrudan düzenlenen hukuka ve dürüstlük kurallarına uygunluk ilkesi kişisel verilerin işlenmesi sürecinin her aşamasında aranmaktadır¹⁹⁸.

KVKK'de belirtilmeyen fakat GDPR'de yer alan bir diğer ilke ise “şeffaflık” ilkesidir. Avrupa Komisyonu’nun 95/46/EC sayılı “Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Direktifi”¹⁹⁹nde de şeffaflık ilkesi açık bir şekilde belirtilmemiş olup GDPR’ın yürürlüğe girmesiyle açık bir şekilde düzenlenmiştir. Şeffaflık unsuru; kişisel verilerin işlenmesi sürecinde veri sahibinin gerektiğinde bilgilendirilmesini veya kendi verilerine erişmesini kapsamaktadır²⁰⁰.

¹⁹⁵ TMK m. 2/I: “Herkes, haklarını kullanırken ve borçlarını yerine getirirken dürüstlük kurallarına uymak zorundadır.”

¹⁹⁶ OĞUZ, Habip, s. 23; ÖZDEMİR, s. 98.; YILMAZ, Tüze, Avrupa Birliğinde, Kişisel Verilerin Korunması Hukuku, 1. Baskı, Ankara, 2022, s. 60.

¹⁹⁷ BASKIN, s. 59; ÖZDEMİR, s. 138; GÜNAY, s. 98; YILMAZ, Tüze, s. 60.

¹⁹⁸ TAŞTAN, s. 48; BASKIN, s. 59; ÖZDEMİR, s. 138.

¹⁹⁹ 95/46/EC sayılı Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Direktifi hakkında detaylı bilgi için bkz: Birinci Bölüm, II, B, 1, a.

²⁰⁰ KAYA İslam Safa/TOLUN, Yüksel, Türkiye’de, Avrupa’da ve California’da Kişisel Verilerin İşlenmesi, 2022, s. 79; YILMAZ, Tüze, s. 59

Bir veri sahibinin herhangi bir internet sitesine giriş yaptığında ortaya çıkan “kişisel verilerin işlenmesine onay verme” kutucuğunda detaylı bilgi okuma seçeneği de bulunmakta olup bu bilgilendirme de şeffaflık ilkesinden ileri gelmektedir.

2. Doğruluk ve Güncellik

KVKK m. 4/II-b’de düzenlenen “doğru ve gerektiğinde güncel olma” ilkesi ile hem veri sorumlusunun çıkarları korunurken veri sahibinin de temel hak ve özgürlüklerine halel gelmemesi amaçlanmaktadır²⁰¹. Zira kişisel verilerin doğru ve gerektiğinde güncel olması veri sahibinin zarar görmesini engellediği gibi; veri işleyen yanlış sonuçlar elde etmesini önler²⁰².

Kişisel verilerin doğruluğu ve güncelliğini sağlayabilmek adına veri sahibinin kendilerine ait bilgilerin doğruluğunu ve güncelliğini rutin olarak kontrol etme haklarının olduğunu kabul etmek gerekir²⁰³. Nitekim, işlenen kişisel veriler, yanlış olabileceği gibi; bu verilerin zaman içerisinde güncelliğini yitirme ihtimali mevcuttur. Çalışmanın konusu bağlamında; kanaatimizce internette kişisel verilerin daha hızlı işlendiği göz önünde bulundurulduğunda internet sitesi işletmecilerinin, kullanıcılara ait verileri güncel tutmaya matuf yazılımlar geliştirmesinin bahse konu ilkeye uygunluk açısından gereklidir. Bunu sağlayabilmek adına kişisel veri işleyen internet sitesi işletmecisinin, kişisel verisi işlenen kullanıcılara kendilerine ait verileri güncelleyebileceği bir sistem sağlayabileceği akla gelmektedir²⁰⁴. Sosyal medya işletmecilerinin, kullanıcılara

²⁰¹ Kişisel Verilerin Korunması Kurumu, Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi, <https://www.kvkk.gov.tr/Icerik/4197/Kisisel-Verilerin-Korunmasi-Kanununa-Iliskin-Uygulama-Rehberi>, E.T. 18.07. 2023; BASKIN, s. 60; GÜNEY, s. 102-103; GÖÇMEN UYARER, Sinem, Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması, 2. Baskı, Ankara, 2020, s. 125.

²⁰²BASKIN, s. 60.

²⁰³ ÖZDEMİR, s. 138.

²⁰⁴ TAŞTAN, s. 50.

kendilerine ait profilleri düzenlemeye imkân sağlamasının da doğruluk ve gerektiğinde güncel olma ilkesiyle ilintili olduğu değerlendirilmektedir.

Doğruluk ve gerektiğinde güncel olmak ilkesi GDPR m. 5/I-d²⁰⁵'de de düzenlenmiş olup bu ilke KVKK'ye nazaran daha geniş ele alınmıştır. İlgili hükme göre doğruluk ve gerektiğinde güncel olma ilkesi, verinin doğru olmadığı takdirde ivedilikle silinmesini de kapsamaktadır. GDPR'nin uygulanmasında ise; güncel tutma ilkesi istisnasız kabul edilmektedir. Kural olarak veri sahibine düzeltme hakkı tanınmış olsa da bazı durumlarda veri sahibinin ilgili verinin silinmesini veya düzeltilmesini isteme hakkı öngörülmemiştir. Hastalık geçmişi gibi kaydının muhafaza edilmesi icap eden geçmişteki belirli durumlar güncelleme isteme hakkına istisna oluşturmaktadır²⁰⁶.

3. Belirli, Açık ve Meşru Amaç

KVKK m. 4/I-c'de yer alan kişisel verilerin işlenmesinin belirli, açık ve meşru bir amaç kapsamında gerçekleştirilmesi ilkesi, faaliyet amacının ilgili kişi tarafından dayandığı hukuki işlem şartının açık ve belirli olmasını ifade etmektedir²⁰⁷. Bu ilkeye göre veri işleyen, kişisel veri sahibine belirtilen amaç dışında verinin işlenmesinden sorumlu olmaktadır.

Kişisel verilerin işlenmesinin amacının belirliliği, açıklığı ve meşruluğu; veri sahibinin kendisine ait verilerin işlenmesine rıza gösterdiği anda mevcut olması

²⁰⁵ GDPR m. 5/I-d: “doğrudur ve gerektiğinde güncel tutulur; işlenme amaçları göz önünde tutularak, doğru olmayan kişisel verilerin gecikmeksizin kalıcı olarak silinmesi veya düzeltilmesinin sağlanmasıyla ilgili makul tüm adımlar atılmalıdır (“doğruluk”)”

²⁰⁶ KAYA/TOLUN, s. 81.

²⁰⁷ KVKK Kişisel Verilerin İşlenmesi Rehberi, s. 67.

gerekmektedir. Kişisel veri işleyen, bu ilke uyarınca henüz gelecekte ortaya çıkması muhtemel bir amaca dayanarak kişisel veri işleyemeyecektir²⁰⁸.

Kişisel verilerin işlenmesine ilişkin veri sahibinden alınan rızanın olası amaç değişikliklerinde geçersiz olmaktadır. Nitekim bu durum, spesifik bir amaç için verilen rızanın veri sahibi aleyhine geniş yorumlanması sonucunu doğurmaktadır. Bu açıdan bu ilke, sınırlılık ilkesi ile de ilgili olmaktadır²⁰⁹.

Kanımızca, kişisel verilerin işlenme amacı çalışmamızın konusunu oluşturan internet ortamında işlenen kişisel veriler bağlamında önem arz etmektedir. İnternet ortamının dinamik yapısı göz önüne alındığında, veri işleme amaçlarının da hızlı bir şekilde değişebileceği akla gelmektedir. Söz gelimi; kullanıcıya daha isabetli içerikler sunmak amacıyla göz atma geçmişini işleyen ve bu hususta kullanıcının rızasını alan bir internet sitesi işletmecisinin, yeni bir rıza almaksızın göz atma geçmişini kullanıcıya kişiselleştirilmiş reklam sunma amacıyla kullanması “belirli, açık ve meşru amaçlar için işlenme ilkesi”ne aykırılık oluşturur.

4. İşlenme Amacıyla Bağlantılı, Sınırlılık ve Ölçülü Olma

KVKK m. 4/I-ç’de düzenlenen kişisel verilerin işlenmesi faaliyetinin işlenme amacıyla bağlantılı, sınırlı ve ölçülü olması ilkesi; işlenecek kişisel verinin belirlenmiş amaç ile bağlantılı olmasını, amacın hasıl olması için gerekli olandan daha fazla verinin işlenmemesini, işleme faaliyetiyle amaç arasında makul bir denge kurulmasını ifade eder²¹⁰. İşleme faaliyetinin belirlenmiş amaç ile bağlantılı olması gerekliliği, kişisel veri

²⁰⁸ TAŞTAN, s. 50-51.

²⁰⁹ ÖZDEMİR, s. 142; GÖÇMEN UYARER, s. 128; BUDAK/MALKOÇ, s. 75 DOĞAN, Bayram, Karşılaştırmalı Hukukta Anayasal Bir Hak Olarak Kişisel Verilerin Korunması Hakkı, 1. Baskı, Ankara, 2022, s. 205.

²¹⁰ KVKK Kişisel Verilerin İşlenmesi Rehberi, s. 68-69.

sahibine, kendisine ait verinin ne amaçla işlendiğini öğrenme hakkı doğurmaktadır²¹¹. İnternet sitelerine “KVKK Bilgilendirme Metni” gibi metinlerin konulmasındaki temel hedef, söz konusu ilke kapsamında verileri işlenen kimselerin, verilerinin hangi amaçla işlendiği ve işlemenin sınırları hususunda bilgi sahibi olmalarının sağlanmasıdır.

Kişisel verilerin daha önceden belirlenmiş amacı gerçekleştirmeye yetecek nispette işlenmesi gerekmektedir²¹². Bu kapsamda, kural olarak kişisel veri sahibinin rızası alınırken belirtilen amacın değişmesi halinde yeniden rıza alınmaksızın yeni amaç uyarınca ilave kişisel veri işlenmesi belirtilen ilkeye aykırılık oluşturacaktır²¹³. KVKK’de “amaç ile sınırlılık” olarak düzenlenen bu ilkeye ek olarak GDPR m. 5/I-b’de “*purpose limitation*” başlığıyla “amacın sınırlandırılması” ilkesi yer almaktadır. Bu ilkeden kişisel verilerin işlenmesi sürecinde yeni bir amacın ortaya çıkmasının, tamamen yeni bir işleme faaliyeti oluşturacağı ve yeni bir hukuki işleme dayanması gerektiği anlaşılmaktadır²¹⁴.

5. Gerekli Süre Nispetinde Muhafaza Etme

KVKK m. 4/I-d’de kişisel verilerin “ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme” ilkesi düzenlenmiştir. Bu ilkeye göre kişisel verileri işleyen kişi, belirli bir süre sonunda kişisel verinin silinmesi veya anonim hale getirilmesi için gerekli idari ve hukuki tedbirleri almakla mükelleftir²¹⁵.

Gerekli süre nispetinde muhafaza edilebilme ilkesi işlenme amacıyla sınırlılık ilkesiyle bağlantılıdır. Dolayısıyla kişisel verileri işleyen kişi, her aşamada işlenme amacını

²¹¹ BASKIN, s. 62.

²¹² BASKIN, s. 62; GÜNAY, s. 91.

²¹³ ÖZDEMİR, s. 741; GÖÇMEN UYARER, s. 127.

²¹⁴ KAYA/TOLUN, s. 79-80; GÖÇMEN UYARER, s. 127.

²¹⁵ KVKK Uygulama Rehberi, s. 70.

göz önünde bulundurulmalıdır²¹⁶. Zira amaca ulaşıldığında veya amaç ortadan kalktığında ilgili mevzuatta öngörülen azami sürenin dolmamış olması halinde dahi kişisel verilerin silinmesi veya anonim hale getirilmesi gerekmektedir²¹⁷. Bu durum internet ortamının dinamik yapısı göz önüne alındığında daha önemli bir hal almaktadır. Nitekim; internet ortamında çoğu zaman arzulanan amaç daha hızlı gerçekleşebilmektedir. Örneğin; bir alışveriş internet sitesinde gezinirken satın alınması düşünülen ürüne ilişkin arama geçmişinin, ilgili ürün satın alındıktan sonra muhafaza edilemeyeceği değerlendirilmektedir. Uygulamada internet sitelerinde üyeliksiz satış seçeneği sunulması zaruri hale getirilerek üye olmaksızın alışveriş yapan kullanıcıların sipariş öncesi yaptığı arama ve göz atma geçmişinin iletişim bilgileriyle ilişkilendirilmesinin önüne geçilmesi mümkün görünmektedir.

Kişisel verilerin gerekli nispette muhafaza edilebileceğine ilişkin ilkeye GDPR’de de yer verilmiştir. GDPR m. 5/I-a²¹⁸’da KVKK’dan farklı olarak kişisel verilerin kamu yararı, bilimsel ve tarihi araştırmalar söz konusu olduğunda daha uzun süre muhafaza edilebileceği öngörülmüştür. Bunun yanında bilimsel ve tarihi araştırmalara yönelik öngörülen süreden daha fazla muhafaza edilecek bilginin anonimleştirilerek istatistiksel olarak tutulması gerekmektedir²¹⁹.

²¹⁶ BASKIN, s. 63.

²¹⁷ GÖÇMEN UYARER, s. 129; ÖZDEMİR, s. 144.

²¹⁸ GDPR m. 5/I-e: “*veri öznelerinin, yalnızca kişisel verilerin işleme amaçlarının gerektirdiği sürece kimliğinin belirlenmesini sağlayan bir şekilde tutulur; kişisel veriler, veri öznesinin hakları ve özgürlüklerinin güvence altına alınması için bu Tüzük’ün gerektirdiği uygun teknik ve düzenlemeye ilişkin tedbirlerin uygulanmasına tabi olmak kaydıyla, 89/1 maddesi uyarınca yalnızca kamu yararına arşivleme amaçlarıyla, bilimsel veya tarihi araştırma amaçlarıyla ya da istatistikî amaçlarla işlendikleri sürece, daha uzun sürelerle depolanabilir (“depolamanın sınırlandırılması”)*”

²¹⁹ KAYA/TOLUN, s. 81-82.

III. KİŞİSEL VERİLERİN İŞLENMESİ SÜRECİNDE YER ALAN AKTÖRLER

A. Veri Sorumlusu

Veri sorumlusu kavramı, “Tanımlar” başlıklı KVKK m. 3/I-ı²²⁰’da “*kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından, yönetilmesinden sorumlu olan gerçek veya tüzel kişi*” olarak tanımlanmıştır. GDPR m. 4²²¹’de yer alan veri sorumlusu tanımı da KVKK’ye benzer olmakla beraber; GDPR’da kamu tüzel kişilerinin veri sorumlusu olabileceği sarıh bir şekilde belirtilmiştir. KVKK’de kamu tüzel kişilerinin veri sorumlusu olabileceği açıkça belirtilmemiş olmasına karşın KVKK hükümleri kamu tüzel kişileri için de bağlayıcı olduğundan; veri sorumlusu kavramının tanımında yer alan “tüzel kişi” ifadesi geniş yorumlanarak kamu tüzel kişileri de dahil edilmektedir²²².

Veri sorumlusu, kişisel verilerin işlenmesi sürecinin başından sonuna kadar var olan karar verme mekanizmasını haiz olan kişidir. Bu kapsamda KVKK’de veri sorumlusu “veri kayıt sistemi”ni kurmak ve yönetmekten sorumlu tutulmuştur. Veri kayıt sistemi, KVKK m. 3/I-h’de²²³ kişisel verilerin “belirli kriterlere göre yapılandırılarak”

²²⁰ KVKK m.3/I-ı: “*Veri sorumlusu: Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi, ifade eder.*”

²²¹ GDPR m. 4/7: “*“veri sorumlusu” yalnız başına veya başkalarıyla birlikte kişisel verilerin işlenmesinin amaçlarını ve yollarını belirleyen gerçek veya tüzel kişi, kamu makamı, kamu kurumu veya diğer organlardır; söz konusu işlemin amaçları ve yollarının Birlik ya da Üye Devlet hukukuna göre belirlenmesi halinde, veri sorumlusu veya veri sorumlusunun tayinine özgü kriterler Birlik ya da Üye Devlet hukukuna göre öngörülebilir*”

²²² BAKIREL, Nur Buğçe, Veri Sorumlusu ve Veri İşleyen Arasındaki Sorumluluk Paylaşımı Avrupa Birliği Genel Veri Koruma Tüzüğü ve Kişisel Verilerin Korunması Kanunu Çerçevesinde Değerlendirilmesi, 1. Baskı, Ankara, 2021, s. 51; ÇELİKEL, Serdar, Kişisel Verilerin Korunması Hukuku Kapsamında Veri Sorumlusu ve Veri Sorumlusunun Yükümlülükleri, 1. Baskı, Ankara, 2022, s. 80.

²²³ KVKK m.3/I-h: “*Veri kayıt sistemi: Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini ... ifade eder.*”

işlendiği sistemler olarak tanımlanmıştır. Dolayısıyla, veri sorumlusu, kişisel verilerin nasıl işleneceği, nerede depolanacağı, nasıl tasnif edileceği vb. birçok duruma karar veren gerçek veya tüzel kişidir²²⁴. Veri sorumlusu, tüm kişisel veri işlenmesi sürecinin “patron”u olarak tanımlanmaktadır²²⁵. Nitekim veri sorumlusunun kim olduğu, kişisel verilerin işlenmesi sürecinden doğan sorumluluğun tayini ve yükümlülüklerin muhatabını belirleme noktasında önem arz etmektedir.

Tüzel kişiler, haklara ve borçlara ehil olurken ve hukuki işlem gerçekleştirmek üzere iradelerini açıklarken organlarından istifade ederler²²⁶. Veri sorumlusu sıfatı tüzel kişiliğin kendisinde olmakla beraber; maddi dünyada kişisel veri işleme faaliyetlerini yetkili organlar yürütmektedir. Dolayısıyla tüzel kişiyi temsile yetkili kişilerin veri sorumlusu olarak kabul edilmesi mümkün olmayıp kişisel verilerin hukuka aykırı işlenmesinden sözü geçen şahısların hukuki sorumluluğu doğmayacaktır²²⁷. Veri sorumlusu gerçek veya tüzel kişiyi temsile yetkili kişi vasıtasıyla yürütülen kişisel veri işlenmesi sürecinden hukuki açıdan veri sorumlusu gerçek veya tüzel kişi sorumlu olacaktır²²⁸. Bunun yanında şirketler topluluğu gibi yapılar söz konusu olduğunda; münferit tüzel kişiliğe sahip her kişi ayrı ayrı veri sorumlusu sıfatını haiz olmaktadır²²⁹.

KVKK ve GDPR gibi düzenlemelerin öncesinde, alelade bir kişi gibi mevzuata uygun şekilde kişisel verileri işlemesi yeterli olan veri sorumlusuna; veri sorumlusu kavramının hukuki olarak tanımlanmasıyla beraber özel bir organize etme sorumluluğunu

²²⁴ BASKIN, s. 64.

²²⁵ ÇELİKEL, s. 81.

²²⁶ KUŞ, Ulaş Baran, Tüzel Kişilik Perdesinin Kaldırılması (Sermaye Şirketlerinde Sınırlı Sorumluluk İlkesinin İstisnası), 2. Baskı, Ankara, 2023, s. 30.

²²⁷ ÇELİKEL, s. 82.

²²⁸ Kişisel Verilerin Korunması Kurumu, Veri Sorumlu ve Veri İşleyen, s. 1, <https://www.kvkk.gov.tr/Icerik/4195/Veri-Sorumlusu-ve-Veri-Isleyen>, E.T.: 31.07.2023, GÖÇMEN UYARER, s. 118.

²²⁹ BASKIN, s. 59-60.

da yükletilmiştir²³⁰. Buna göre veri sorumlusu kişisel verilerin hukuka uygun işlenmesi için birtakım idari, hukuki ve teknik tedbirleri almakla mükelleftir.

KVKK ve GDPR’de veri sorumluları için öngörülen en önemli yükümlülüklerden biri aydınlatma yükümlülüğüdür. Şeffaflık ilkesiyle yakından irtibatlı olan bu yükümlülük kişisel verilerin internet ortamında işlenmesi sürecinde daha da önemli bir hal almaktadır. Nitekim; internet ortamında hâkim olan yapay zeka uygulamaları ve akıllı cihazlar vasıtasıyla yürütülen otomatik veri işleme yöntemlerinin dinamik yapısı nedeniyle kullanıcıların her aşamada, hangi verilerinin ne amaçla işlendiğine dair bilgilendirilmesi önem arz etmektedir²³¹.

B. Veri İşleyen

KVKK m. 3/I-ğ’de veri işleyen kavramı; *“veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi”* olarak tanımlanmıştır. Tanımdan anlaşılabacağı üzere veri işleyen gerçek kişi olabileceği gibi, tüzel kişi de olabilmektedir. KVKK’ye çok benzer şekilde veri işleyen kavramı, GDPR m. 4²³²’de; veri sorumlusu adına kişisel verileri işleyen gerçek veya tüzel kişiler olarak tanımlanmıştır. Bunun yanında; GDPR’da açık bir şekilde veri işleyen olabilecek tüzel kişiler geniş tutularak kamu kurum, kuruluş veya herhangi bir yapının veri işleyen sıfatını haiz olabileceği belirtilmiştir²³³.

Veri sorumlusu; kişisel verilerin saklanma yöntemi, alınacak güvenlik önlemleri, aktarım yöntemleri, sürelerin kontrolü metotları, kişisel verilerin nasıl silineceği veya

²³⁰ ÇEKİN, s. 642.

²³¹ AŞIKOĞLU, Şehriban İpek, Veri Sorumlularının Aydınlatma Yükümlülüğü – Avrupa Birliği ve Türk Hukukunda-, Kişisel Verileri Koruma Dergisi, C. 1. S. 2, 2019, s. 43.

²³² GDPR m.4/8: *“veri işleyen, veri sorumlusu adına kişisel verileri işleyen bir gerçek ya da tüzel kişi, kamu makamı, kamu kurumu veya diğer organlardır.”*

²³³ ÇELİKEL, s. 84.

anonim hale getirileceği, kişisel verilerin hangi sistemler vasıtasıyla toplanacağı gibi hususlarda veri işleyeni yetkili kılabilir²³⁴. Veri sorumlusu adına işleme faaliyeti yürüten veri işleyenin statüsüne ilişkin farklı görüşler bulunmaktadır. Bir görüşe göre²³⁵ veri işleyen ile veri sorumlusu arasında hizmet alımı veya iş akdi olabileceği öne sürülürken; bir başka görüşe göre²³⁶ veri işleyen ile veri sorumlusu arasında iş sözleşmesi bulunması hukuken mümkün değildir. Tarafımızca ikinci görüşe iştirak edilmektedir. Zira, günümüzde ağırlıkla büyük şirketlerin veri sorumluları olduğu ve bu şirketlerin bünyesinde kalabalık insan gruplarının çalıştığı göz önünde bulundurulduğunda; “veri işleyen” kavramının kapsamı çok genişlemektedir. Söz konusu büyük şirketlerin, çalışmanın konusu olan internet ortamından da azami derece istifade etmesi, sıradan bir çalışanı dahi kişisel veriyi fiilen işleme eylemlerinden birini yapmaya itebilmektedir. Dolayısıyla arada bir iş sözleşmesi mevcut ise bu durumda veri işleyen kişi “veri işleyen” değil, “veri sorumlusunun çalışanı” sıfatıyla veri işleme faaliyetini yürütür²³⁷.

C. Veri Sorumlusu ve Veri İşleyen Ayrımı Yükümlülüklerin Tespiti

İnternet ortamında kişisel verilerin hukuka aykırı işlenmesinden doğacak sorumluluğun tayini için veri sorumlusu ile veri işleyen kavramlarının ayırt edilmesi ve bu kavramların internet aktörleri ile kıyaslanması önem arz etmektedir. Bazı durumlar veri sorumlusu ve veri işleyeni ayırt etmek ilk bakışta mümkün olmamasına karşın, sorumluluk, yükümlülük, karar alma yetkisi belirleyicidir²³⁸. Veri sorumlusu, kişisel verilerin işlendiği sistemleri kurma, işletme ve karar alma noktasında doğrudan yetkili ve

²³⁴ KVKK Uygulama Rehberi, s. 57-58; ÇELİKEL, s. 85-86; BAKIREL, s. 56; UNCULAR, Selen, İş İlişkisinde İşçinin Kişisel Verilerinin Korunması, 2. Baskı, Ankara, 2018, s. 112.

²³⁵ BAKIREL, s. 56.

²³⁶ ÇELİKEL, s. 85; UNCULAR, s. 112.

²³⁷ ÇELİKEL, s. 85.

²³⁸ TURAN, s. 64.

sorumlu iken; veri işleyen yetki ve sorumluluğu veri sorumlusu ile arasındaki hukuki ilişkiye bağlıdır²³⁹. Veri işleyen; kişisel veri işleme sürecini, veri sorumlusunun nam ve hesabına yürüten ayrı bir tüzel ya da gerçek kişiliği haiz kişisel veri süreci aktörüdür²⁴⁰.

KVKK m. 12/II'de²⁴¹ veri sorumlusunun veri işleyen belirlese dahi mevzuatta öngörülen veri güvenliğine ilişkin yükümlülüklerle bağlı olmaya devam ettiği düzenlenmiştir. Dolayısıyla veri güvenliği ihlal edildiği takdirde veri sorumlusu, veri işleyen belirlediğini öne sürerek hukuki sorumluluktan kurtulamamakta hem veri sorumlusu hem veri işleyen gerekli tüm teknik ve organizasyonel veri güvenliği önlemlerini aldıklarını ispat etmeleri gerekmektedir²⁴².

İnternet ortamının aktörleri ile kişisel veri sürecinin süjeleri mukayeseli olarak incelendiğinde; kavramların birbirlerinin doğrudan karşılamadığı görülmektedir. Örneğin; kullanıcıların ürün satışı yapabildiği bir elektronik ticaret internet sitesinin işletmecisi, internet hukuku açısından yer sağlayıcı ve içerik sağlayıcı olarak sorumlu iken²⁴³; kişisel veri koruma hukuku açısından veri sorumlusu olmaktadır. Zira site kullanıcılarının verilerini kendi nam ve hesabına işlemektedir. Buna karşın; aynı internet sitesi işletmecisi, pazarlama stratejileri geliştirmek adına başka bir gerçek veya tüzel kişiden internet sitesinin kullanıcıların verilerini analiz etmesine yönelik bir sözleşme akdettiği takdirde, sözleşmenin karşı tarafı olan veri analiz edecek firma veri işleyen olarak sorumlu olacaktır²⁴⁴.

²³⁹ ÇELİKEL, s. 84.

²⁴⁰ BAKIREL, s. 56.

²⁴¹ KVKK m. 12/II: “Veri sorumlusu, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, birinci fıkrafta belirtilen tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumludur.”

²⁴² MEMİŞ, Tekin, Veri Sorumlusu ve Veri İşleyen Arasındaki İlişkiler ve Sorumluluk Düzeni, *Beykent Üniversitesi Hukuk Fakültesi Dergisi*, C. 3, S. 6, 2017, s. 17; ÇELİKEL, s. 86.

²⁴³ İnternet ortamı aktörleri hakkında detaylı bilgi için bkz: İkinci Bölüm, I, B.

²⁴⁴ KVKK Uygulama Rehberi, s. 59; BAKIREL, s. 57-58.

ÜÇÜNCÜ BÖLÜM

KİŞİSEL VERİLERİN HUKUKA AYKIRI İŞLENMESİ VE BAŞVURU YOLLARI

I. İNTERNET ORTAMINDA KİŞİSEL VERİLERİN İŞLENMESİNDE HUKUKA UYGUNLUK SEBEPLERİ

A. Açık Rıza

1. Açık Rıza Kavramı

KVKK m. 5/I'de²⁴⁵ kişisel verilerin, ilgili kişinin açık rızası olmadan işlenemeyeceği düzenlenmiştir. Benzer düzenleme KVKK m. 6/II'de²⁴⁶ tekrarlanarak; özel nitelikli kişisel veriler bağlamında da açık rıza olmadan işleme faaliyetleri yasaklanmıştır. KVKK m. 3/I-a'da²⁴⁷ “açık rıza” kavramı tanımlanmış olup özgür iradeyle açıklanması, bilgilendirmeye dayanması ve belirli bir konuya ilişkin olması, mezkur kavramın unsurları olarak sayılmıştır. Kanun hükümlerinden de anlaşılacağı üzere; açık rıza, kişisel verilerin işlenmesi için temel şartını oluşturmaktadır²⁴⁸. Açık rızanın varlığı kişisel verilerin işlenmesi için tek başına yeterli olmayıp işleme faaliyetinin KVKK'de belirlenen genel ilkelere de uygun olması gerekmektedir. Öte yandan; istisnai hallerde açık rıza olmasa dahi kişisel verilerin işlenebileceği düzenlenmiştir.

²⁴⁵ KVKK m. 5/I: “Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez.”

²⁴⁶ KVKK m. 6/II : “Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır.”

²⁴⁷ KVKK m. 3/I-a: “Açık rıza: Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı, ... ifade eder.”

²⁴⁸ BATU, s. 99; ERDOĞMUŞ, Elif, 6698 Sayılı Kişisel Verilerin Korunması Kanunu Kapsamında Açık Rıza, 1. Baskı, Ankara, 2022, s. 72.

GDPR m. 4/11’de “rıza” kavramı, KVKK’ye benzer şekilde; ilgili kişinin belirli bir hususta, özgürce, belirli ve tereddüde yer bırakmayacak şekilde açık irade beyanı olarak tanımlanmıştır.

Açık rıza kavramı KVKK ile Türk mevzuatına dahil olmasına karşın TMK m. 23’de düzenlenen genel rıza ile benzerlik göstermektedir²⁴⁹. Öte yandan; KVKK’de açık rızanın hukuki niteliğine ilişkin herhangi bir düzenlemeye yer verilmemiş olup bunun için de genel hükümlere başvurulması gerekmektedir. Kişilik haklarına saldırıya ilişkin TMK m. 24/II’de²⁵⁰ kişilik hakkı zedelenen kimsenin rızasının, saldırıyı hukuka uygun kılacağı düzenlenmiştir. TBK m. 63/II’de²⁵¹ ise “rıza” haksız fiiller için genel bir hukuka uygunluk sebebi olarak sayılmıştır. Dolayısıyla hukuki niteliği bakımından rıza, açık veya örtülü olarak hukuki bir sonuca yönelik açıklanan tek taraflı irade beyanıdır²⁵².

KVKK ile mevzuatımıza dahil olan açık rızanın, genel hükümlerde düzenlenen rızadan hukuki nitelik bağlamında farkı olmamasına karşın geçerliliği bakımından en önemli farkı, hukuki sonuca yönelik irade beyanının zımni bir şekilde verilememesidir²⁵³. Kanun koyucu açık rızanın gerekli olduğu durumlarda, rızası aranan kişinin menfi fiiline

²⁴⁹ BASKIN, s. 115; ERDOĞMUŞ, s. 71.

²⁵⁰ TMK m. 24: “Hukuka aykırı olarak kişilik hakkına saldırılan kimse, hâkimden, saldırıda bulunanlara karşı korunmasını isteyebilir.

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

²⁵¹ TBK m. 63: “Kanunun verdiği yetkiye dayanan ve bu yetkinin sınırları içinde kalan bir fiil, zarara yol açsa bile, hukuka aykırı sayılmaz.

Zarar görenin rızası, daha üstün nitelikte özel veya kamusal yarar, zarar verenin davranışının haklı savunma niteliği taşıması, yetkili kamu makamlarının müdahalesinin zamanında sağlanamayacak olması durumunda kişinin hakkını kendi gücüyle koruması veya zorunluluk hâllerinde de fiil, hukuka aykırı sayılmaz.”

²⁵² OĞUZMAN/SELİÇİ/OKTAY ÖZDEMİR, s. 235; EREN, Fikret, Borçlar Hukuku Genel Hükümler, 28. Baskı, Ankara, 2023, s. 688-689; KAYIHAN, Şaban/ÜNLÜTEPE, Mustafa, Borçlar Hukuku Genel Hükümler, 6. Baskı, Ankara, 2018, s. 242; ÜNLÜTEPE, s. 149; AYAN, 2016, s. 259; YILMAZ/YILDIRIM, s. 217; ERDOĞMUŞ, s. 72.

²⁵³ ÇELİKEL, Serdar, Kişisel Verilerin İşlenmesinde, Açık Rıza Hukuka Uygunluk Nedeninin, 95/46 Sayılı Direktif ve GDPR’la Karşılaştırmalı Olarak İncelenmesi, UMD, S. 17, 2021, s. 163; ERDOĞMUŞ, s. 72.

herhangi bir hukuki sonuç bağlamamıştır. Dolayısıyla internet ortamında; kullanıcıların kişisel verilerin işlenmesine ilişkin herhangi bir onam formunu reddetmemesi, açık rıza kapsamına girmediğinden kişisel verilerin işlenmesi noktasında hukuki sebep oluşturmamaktadır.

GDPR’da KVKK’nin aksine yalnızca özel nitelikli kişisel verilerin işlenmesi için açık rıza (*explicit consent*) aranmıştır. GDPR m. 6/I-a’da²⁵⁴ kişisel verilerin işlenebilmesi için yalnızca rıza aranırken; GDPR m. 9’de²⁵⁵ ise etnik köken, politik ideoloji, sendika üyeliği, dini inanç, cinsel yaşam, sağlık durumu gibi özel nitelikli verilerin işlenmesinde açık rıza aranmıştır. Tarafımızca da iştirak edilen görüşe göre²⁵⁶; her ne kadar gramatiksel açıdan farklılıklar bulunsa da KVKK ile GDPR’da rıza müessesesini işleyişinde farklılık bulunmamaktadır. Nitekim GDPR’da “rıza” kavramı veri sahibinin açık, net, bilgilendirilmiş ve özgürce verdiği beyan olarak tanımlanmıştır. Kanun koyucunun burada özel nitelikli verilerin işlenmesindeki hassasiyetini vurgulamak amacıyla “açık” (*explicit*) kelimesine yer verdiği değerlendirilmektedir.

²⁵⁴ GDPR m. 6/I-a: “İşleme, ancak aşağıdaki hususlardan en az biri geçerli olduğunda ve geçerli olduğu ölçüde hukuka uygundur

...
veri öznesinin, kişisel verilerinin bir ya da daha fazla spesifik amaca yönelik olarak işlenmesine rıza vermesi”

²⁵⁵ GDPR m. 9: “1) Irk veya etnik köken, siyasi görüşler, dini veya felsefi inançlar ya da sendika üyeliğini açığa çıkaran kişisel verilerin işlenmesi ve bir gerçek kişinin kimliğini benzersiz bir şekilde belirleyen genetik veriler ile biyometrik verilerinin işlenmesi, sağlık verilerinin veya bir gerçek kişinin cinsel yaşamı veya cinsel eğilimine ilişkin verilerin işlenmesi yasaktır.

2) 1. paragraf aşağıdakilerden birinin geçerli olması hâlinde uygulanmaz:
Birlik veya Üye Devlet hukukunun 1. paragrafta belirtilen yasağın veri öznesi tarafından kaldırılmayacağını öngörmesi haricinde, veri öznesinin, belirtilen bir veya daha fazla amaca yönelik olarak söz konusu kişisel verilerin işlenmesine açık rıza vermesi”

²⁵⁶ ÇELİKEL, Açık Rıza, s. 169.

2. Açık Rızanın Unsurları

a. Belirli Bir Konuya İlişkin Olma

Açık rızanın belirli bir konuya yönelik verilmesi gerekliliği gerek KVKK'de gerekse GDPR'da düzenlenmiştir. Bu kapsamda; ilgili kişinin kapsamı, sınırları belli olmayan bir veri işleme faaliyetine yönelik vereceği rızanın, kişisel verilerin korunması hukuku kapsamında geçerli olmadığı kabul edilmektedir. Bu açıdan belirli bir konuya ilişkin olma unsurunun, KVKK'nin genel ilkeler başlığı altında düzenlenen “amaca bağlılık” ilkesiyle doğrudan bağlantılı olduğu değerlendirilmektedir²⁵⁷.

İlgili kişinin, kişisel verilerinin işlenmesine ilişkin verdiği rıza, rıza verdiği konu ve amaçla sınırlıdır. Kişisel verilerin işlenmesine yönelik verilen rızanın, ilgili kişinin tüm verilerinin herhangi bir amaçla işlenmesine “torba rıza” gibi hukuki sebep oluşturamayacağı yönünde görüşe²⁵⁸ tarafımızca da iştirak edilmektedir. Özellikle internet ortamının dinamik ve sürekli yeni ihtiyaçlar oluşturan yapısı, burada işlenen kişisel verilerin, veri sorumlusu tarafından açık rıza alınırken belirtilen amaçların dışında kullanılmasını sonucunu doğurabilmektedir. İşlenen kişisel verilerin farklı amaçlarla kullanılması halinde ilgili kişiden yeniden açık rıza alınması gerekmektedir²⁵⁹. Örneğin; kişisel veriler bağlamında veri sorumlusu konumunda olan bir internet yer sağlayıcısının veri merkezinin farklı bir ülkeye taşınması sebebiyle, kişisel verilerin yurt dışına aktarımı ihtiyacı ortaya çıkabilir. Böyle bir durumda veri sorumlusu olan yer sağlayıcının, kişisel verileri yurt dışına aktarmak suretiyle işlenmesi yönünde ilgili kişilerin tekrardan açık rızasını alması gerekmektedir²⁶⁰. Öte yandan; internet ortamının sürekli yinelenen yapısı göz önüne alındığında; konvansiyonel yöntemlerin aksine, kolaylıkla ilgili kişilerin

²⁵⁷ ERDOĞMUŞ, s. 98; BATU, s. 116.

²⁵⁸ TAŞTAN, s. 158; ERDOĞMUŞ, s. 198; BATU, s. 115; UZUNAL, s. 59.

²⁵⁹ BASKIN, s. 115; ERDOĞMUŞ, s. 99; GÖÇMEN UYARER, s. 115.

²⁶⁰ ERDOĞMUŞ, s. 99.

rızalarının alınabileceği değerlendirilmektedir. İnternetin kendine has yapısı; açık rızanın yinelenmesi ihtiyacını artırdığı gibi, açık rıza verilmesine yönelik beyanın kolayca tekrardan verilmesine olanak sağlamaktadır.

b. Bilgilendirmeye Dayanma

KVKK ve GDPR’da yer alan bir başka açık rıza unsuru “bilgilendirilmeye dayalı” olmasıdır. Açık rızanın bilgilendirilmeye dayalı olması; ilgili kişinin açık rıza beyanında bulunmadan önce, işlenecek olan veriler, işleme faaliyetinin konusu ve amacı, ne süreyle işleneceği, veri sorumlusuna karşı hakları, rızayı geri alma imkânı, yurt dışına transfer durumu, verilerine nasıl bir koruma sağlanacağı, korumaya önlemlerin alınmaması halinde gibi oluşabilecek komplikasyonlar gibi hususlarda bilgilendirilmesidir²⁶¹. Bilgilendirmenin, ilgili kişinin anlayabileceği şekilde yapılmalıdır. Bu kapsamda bilgilendirmenin; sıradan bir kişinin anlayamayacağı teknik terimlerin arınmış olması, yazılı ise okunabilecek büyüklükte puntolardan oluşması, hususi olarak ilgili kişinin gözünden kaçırılacak şekilde yapılmaması gerekmektedir²⁶².

Açık rızanın bilgilendirmeye dayalı olması, KVKK m. 10’da²⁶³ düzenlenen “aydınlatma yükümlülüğü” doğrudan bağlantılıdır²⁶⁴.

²⁶¹ GÖÇMEN UYARER, s. 112; ERDOĞMUŞ, 100.

²⁶² ÖZDEMİR, s. 170; ERDOĞMUŞ, s. 111; BASKIN, s. 115.

²⁶³ KVKK m. 10: “I) Kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişi, ilgili kişilere;

a) Veri sorumlusunun ve varsa temsilcisinin kimliği,

b) Kişisel verilerin hangi amaçla işleneceği,

c) İşlenen kişisel verilerin kimlere ve hangi amaçla aktarılabilmesi,

ç) Kişisel veri toplamanın yöntemi ve hukuki sebebi,

d) 11 inci maddede sayılan diğer hakları,

konusunda bilgi vermekle yükümlüdür.”

²⁶⁴ ERDOĞMUŞ, s. 101; TAŞTAN, s. 159.

c. Özgür İrade

Açık rızanın, ilgili kişinin özgür iradesine dayalı olarak verilmesi hem KVKK'de hem GDPR'da düzenlenen bir başka açık rıza unsurudur. Bu kapsamda ilgili kişi, kişisel verilerinin işlenmesine ilişkin rızasını hiçbir baskı, cebir, tehdit, hile vb. iradesini sakatlayacak durumdan uzak bir şekilde vermelidir²⁶⁵.

Sıradan bir internet kullanıcısının açık rıza beyanında bulunduğu esnada iradesini fesata uğratacak bir durum olup olmadığını tespit etmek oldukça güç olması nedeniyle ilgili kişinin kişisel verilerinin işlenmesine özgür iradesiyle rıza gösterip göstermediğini objektif bir şekilde tayin etmek uygulamada mümkün olmamaktadır. Kanaatimizce, internet ortamında verilen bir açık rızanın özgür iradeye dayanıp dayanmadığını saptayabilmek için; kişisel veri işleme faaliyetinin ilgili kişi aleyhine nispeten bir durum ortaya çıkarıp çıkarmadığına bakılmalıdır. Diğer yandan; somut olayın şartlarından kişinin verilerinin işlenmesine rıza göstermek zorunda kaldığı anlaşılıyorsa da özgür iradenin varlığından bahsedilemeyecektir. Bir örneğe göre; bir şirkette çalışan işçi, şirkete ait intranet sistemine fotoğrafının yüklenmesine rıza göstermiş olsa dahi, şirket ile arasındaki hizmet akdi göz önüne alındığında, işçinin mezkûr rızayı özgür iradesiyle vermemesi söz konusu olabilir. Bu örnekte özgür iradenin söz konusu olabilmesi için şirketin işçileri detaylı bir şekilde bilgilendirerek rızalarını alması ve işçilerin rıza vermedikleri takdirde dahi işveren tarafından herhangi bir ayrımcılığa tabi tutulmamalı gerekmektedir²⁶⁶.

²⁶⁵ BASKIN, s. 115; UZUNAL, s. 61.

²⁶⁶ Article 29 Data Protection Working Party, Opinion 15/2011 On The Definition Of Consent, s. 14, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf, E. T. 10/09/2023.

3. İnternet Ortamında Açık Rızanın Geçerlilik Şartları

a. Açık Rızanın Şekli: *Opt-In/Opt-Out*

KVKK’de kişisel verilerin işlenmesine ilişkin açık rıza beyanının ne şekilde verileceğine ilişkin şekil şartı öngörülmemiştir. Bu kapsamda genel hüküm olan TBK m. 12 hükmü²⁶⁷ çerçevesinde açık rıza beyanında şekil şartı aranmamaktadır. Açık rıza beyanı yazılı, sözlü veya elektronik ortamda e-posta vb. uygulamalar üzerinden verilebilir²⁶⁸. Bunun yanında her ne kadar açık rızanın nasıl alınacağına ilişkin doğrudan bir düzenleme bulunmasa da “Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ²⁶⁹” m. 5/I-f’de²⁷⁰ aydınlatma yükümlülüğünün yerine getirilmesi ile açık rıza alınmasının farklı işlemler vasıtasıyla gerçekleştirilmesi gerektiği düzenlenmiştir²⁷¹. Bu hükümden hareketle internet ortamında kişisel verilerin işlenmesine verilecek açık rıza söz konusu olduğunda, aydınlatma metninin okunduğuna dair onay ve kişisel verilerin işlenmesine ilişkin onayın ayrı ayrı beyanlar ile verilmesi gerekmektedir. Dolayısıyla internet sitelerinde yaygın bir şekilde yer alan, “*üye olarak aydınlatma metninin ve kişisel verilerin işlenmesinin kabul edileceği*” yönünde ibarelerin usulüne uygun alınmış bir açık rıza olmadığı değerlendirilmektedir.

İnternet ortamında en yaygın karşılaşılan açık rıza beyanı usulü, kutucuk işaretleme ya da işaret kaldırma şeklindedir. Kişisel veri literatüründe bu durum “*opt-in*”

²⁶⁷ TBK m. 12: “I) Sözleşmelerin geçerliliği, kanunda aksi öngörülmedikçe, hiçbir şekle bağlı değildir.

II) Kanunda sözleşmeler için öngörülen şekil, kural olarak geçerlilik şeklidir. Öngörülen şekle uyulmaksızın kurulan sözleşmeler hüküm doğurmaz.”

²⁶⁸ BASKIN, s. 114; TAŞTAN, s. 164; ÇELİKEL, Açık Rıza, s. 173.

²⁶⁹ R.G. Tarih: 10/03/2018, R.G. Sayı: 30356.

²⁷⁰ Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ m. 5/I-f: “Kişisel veri işleme faaliyetinin açık rıza şartına dayalı olarak gerçekleştirilmesi halinde, aydınlatma yükümlülüğü ve açık rızanın alınması işlemlerinin ayrı ayrı yerine getirilmesi gerekmektedir.”

²⁷¹ ÇELİKEL, Açık Rıza, s. 174.

ve “*opt-out*” olarak ifade edilmektedir. Buna göre *opt-in* yönteminde, kullanıcı müspet bir irade beyanı ile onay verirken; *opt-out* yönteminde halihazırda önceden onaya yönelik yapılmış işaretleme kaldırılmaktadır²⁷². Dolayısıyla, bir bakıma *opt-out* yönteminde kullanıcının menfi fiiline hukuki sonuç bağlanması nedeniyle zımni rıza oluşmaktadır. Kanaatimizce; internet ortamında *opt-out* yöntemiyle alınacak rıza beyanı, açık rıza kabul edilmemelidir. İnternet ortamında kişisel verilerin işlenmesine ilişkin açık rıza paylaşılmış olan aydınlatma metninin öncelikle okunduğuna; ardından metinden hareketle işleme faaliyetine onay verildiğine ilişkin ayrı ayrı *opt-in* yöntemiyle onay verilmesi suretiyle gerçekleşmelidir.

b. Ehliyet

Kişisel verilerin işlenmesine ilişkin rızayı verme ehliyetini incelemek için öncelikle kişisel verilerin hukuki niteliğine bakılması gerekmektedir. Kişisel verilerin, kişilik haklarının bir türünü oluşturduğuna ilişkin görüş çerçevesinde²⁷³ TMK m. 9 hükmü²⁷⁴ uyarınca fiil ehliyetini haiz kimseler kişisel verilerin işlenmesi için rıza verebilmektedir.

Kişisel verilerin şahsa sıkı sıkıya bağlı hak olduğu bu nedenle yalnızca kişisel veri sahibi tarafından işlenebileceğine ilişkin yaygın görüşe²⁷⁵ tarafımızca iştirak edilmemektedir. Nitekim kişiye sıkı sıkıya bağlı haklar; nişanlanma, evlenme, zina yapan eşi affetme, boşanma davası açma gibi ilgili kişinin, kişiliği ile yakın ilişki içerisinde olan haklardır²⁷⁶. Kişisel verilerin işlenmesine rıza verilmesi, öteden beri kişiye sıkı sıkıya

²⁷² ERDOĞMUŞ, s. 114-115; ÖZDEMİR, s. 156-157.

²⁷³ bkz: Birinci Bölüm, I, B, 4.

²⁷⁴ TMK m. 9: “*Fiil ehliyetine sahip olan kimse, kendi fiilleriyle hak edinebilir ve borç altına girebilir.*”

²⁷⁵ ÖZDEMİR, s. 168; ERDOĞMUŞ, s. 106; ÇELİKEL, Açık Rıza, s. 165.

²⁷⁶ ANTALYA/TOPUZ, s. 181.

bağlı kabul edilen haklara nazaran kişinin maddi ve hukuki durumunu daha seyrek bir şekilde etkilemektedir. Bunun yanında; hassas nitelikli kişisel verilerin işlendiği takdirde ilgili kişinin maddi ve hukuki durumunu daha yoğun bir şekilde etkileyebileceği değerlendirildiğinden yalnızca hassas nitelikli kişisel verilerin işlenmesine ilişkin açık rıza verme yetkisinin kişiye sıkı sıkıya bağlı hak oluşturduğu değerlendirilmektedir. Öte yandan; konumuz bağlamında internet ortamında verilecek bir açık rızanın gerçek sahibinin tespiti de ispat hukuku bakımından farklı bir sorun oluşturmaktadır.

İnternet ortamında fiil ehliyeti bakımından tam ehliyetli olmayan çocukların da erişimine açıktır. Bu açıdan çocukların verilerin işlenmesi noktasında kimin açık rıza göstereceği bir başka sorunu oluşturmaktadır. KVKK’de çocukların kişisel verilerinin işlenmesinde açık rıza vermeye kimin yetkili olduğu hususunda net bir hüküm bulunmamaktadır. Kurul tarafından, bir özel öğrenim kurumunda öğrenci velilerinin aydınlatılarak açık rızalarının alınmadığı bir somut vakıada²⁷⁷ *“ilgili kişinin/velinin açık rızasının alınmadığı, açık rızanın aranmadığı diğer durumların da bulunmadığı gerekçesiyle veri işleme faaliyetinin hukuka aykırı olduğu sonucuna varıldığı”* yönünde karar alınmıştır. Buna göre çocukların kişisel verilerinin işleneceği durumlarda velisinin açık rızasının alınması gerekmektedir²⁷⁸. Aynı durum GDPR uygulamasında da geçerli olup GDPR’a göre bir çocuğun 16 yaşının altında olması halinde veli/vasisinin açık rızası olmaksızın kişisel verileri işlenememektedir. AB üyesi ülkeler yasal mevzuatları ile velinin izni gerekliliğini “13 yaş”a kadar indirebilmektedir²⁷⁹. Görüldüğü üzere hem GDPR, hem KVKK uygulamasında açık rızanın yasal temsilci tarafından verilebileceğinin öngörülmüştür.

²⁷⁷ Kurul’un 02/04/2020 tarihli ve 2020/255 sayılı Kararı.

²⁷⁸ DENİZ, İlknur, Çocuklara Ait Kişisel Verilerin Türk Medeni Kanunu ve Kişisel Verilerin Korunması Kanunu Kapsamında Korunması, 1. Baskı, Ankara, 2021, s. 170.

²⁷⁹ VOSS, s. 225.

B. KVKK Kapsamında Diğer Hukuka Uygunluk Sebepleri

1. Genel Olarak

Kişisel verilerin işleme şartları KVKK m. 5²⁸⁰'de düzenlenmiştir. Kanun koyucu mezkur madde hükmünde ikili bir ayrıma gitmiş olup kişisel verilerin işlenmesi için “açık rıza” şartını düzenlemiştir. Açık rızanın olmadığı durumlarda ise KVKK m. 5/II’de yer alan şartlardan en az birinin sağlanması gerekliliği öngörülmüştür. Buna göre; kişisel veri sahibinin açık rızasının alınmadığı veya açık rızanın olmadığı durumlarda KVKK m. 5/II’de tahdidi olarak sayılan şartlardan birinin sağlanmadığı internet ortamında kişisel verilerin işlenmesi faaliyeti hukuka aykırı olmaktadır²⁸¹.

²⁸⁰ KVKK m. 5: “I) Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez.

II) Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür:

a) Kanunlarda açıkça öngörülmesi.

b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.

c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.

ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.

d) İlgili kişinin kendisi tarafından alenileştirilmiş olması.

e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.

f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.”

²⁸¹ Kurum, Kişisel Verilerin İşlenme Şartları, s. 2-3, <https://www.kvkk.gov.tr/Icerik/4190/Kisisel-Verilerin-Islenme-Sartlari>, E.T. 15/08/2023.

2. Genel Nitelikli Kişisel Verilerin İşlenmesinde Diğer Hukuka Uygunluk Sebepleri

a. Kanunda Açıkça Öngörülmesi

KVKK m. 5/II-a hükmü uyarınca kişisel verilerin işlenmesine ilişkin açık rıza verilmemiş olsa dahi kanunda açıkça öngörülen durumlarda kişisel verilerin işlenmesi hukuka uygun olacaktır. Bu düzenlemenin Anayasa m. 20/III'te yer alan "...kişisel verilerin işlenmesine ilişkin usul ve esaslar kanunla düzenlenir." ibaresini bir uzantısı olduğu değerlendirilmektedir²⁸².

İnternet ortamında gerçekleşen kişisel verilerin işlenmesi faaliyetlerine yönelik olarak 5809 sayılı Elektronik Haberleşme Kanunu ("EHK")²⁸³ m. 51²⁸⁴'de internet servis

²⁸² BASKIN, s. 118; AŞIKOĞLU, Şehriban İpek, Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri, Yüksek Lisans Tezi, İstanbul, 2018, s. 115.

²⁸³ 5809 Sayılı Elektronik Haberleşme Kanunu, R.G. Tarihi: 10. 11. 2008, R.G. Sayısı: 27050 Mükerrer

²⁸⁴ EHK m. 51: "I) Kişisel verilerin işlenmesinde; hukuka ve dürüstlük kurallarına uygun olması, doğru ve gerektiğinde güncel olması, belirli, açık ve meşru amaçlar için işlenmesi, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması ile işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi ilkelerine uyulur.

II) Elektronik haberleşmenin ve ilgili trafik verisinin gizliliği esas olup, ilgili mevzuatın ve yargı kararlarının öngördüğü durumlar haricinde, haberleşmeye taraf olanların tamamının rızası olmaksızın haberleşmenin dinlenmesi, kaydedilmesi, saklanması, kesilmesi ve takip edilmesi yasaktır.

III) Elektronik haberleşme şebekeleri, haberleşmenin sağlanması dışında abonelerin/kullanıcıların terminal cihazlarında bilgi saklamak veya saklanan bilgilere erişim sağlamak amacıyla işletmeciler tarafından ancak ilgili abonelerin/kullanıcıların verilerin işlenmesi hakkında açık ve kapsamlı olarak bilgilendirilmeleri ve açık rızalarının alınması kaydıyla kullanılabilir.

IV) İşletmeciler şebekelerinin, abonelerine/kullanıcılarına ait kişisel verilerin ve sundukları hizmetlerin güvenliğini sağlamak amacıyla uygun teknik ve idari tedbirleri alır.

V) Bu Kanunun 49 uncu maddesi kapsamında veya kamu yararının sağlanması amacıyla Kurum tarafından işletmecilere getirilen yükümlülüklerin yerine getirilebilmesi için kişisel veriler işlenebilir.

VI) Kişisel verilerin yurt dışına aktarılmasına ilişkin ilgili mevzuat hükümleri saklı kalmak kaydıyla, trafik ve konum verileri ancak ilgili kişilerin açık rızaları alınmak koşuluyla yurt dışına aktarılabilir.

VII) Trafik verileri; trafiğin yönetimi, arabağlantı, faturalama, usulsüzlük/dolandırıcılık tespitleri ve benzeri işlemleri gerçekleştirmek veya tüketici şikâyetleri ile arabağlantı ve faturalama anlaşmazlıkları başta olmak üzere, uzlaşmazlıkların çözümü amacıyla sadece işletmeci tarafından yetkilendirilen kişilerle sınırlı kalmak kaydıyla işlenir ve bu

sağlayıcılarının hakları ve yükümlülükleri düzenlenmiştir. EHK m. 51/VII'de, internet servis sağlayıcılarının faturalama, usulsüzlük tespiti, tüketici şikayeti, trafiğin yönetimi, ara bağlantı gibi sebeplerle kullanıcılara ait trafik verilerinin işlenebileceği belirtilmiştir. Bu hükümde açık rıza aranmamış olmakla beraber, yalnızca internet servis sağlayıcı tarafından yetkilendirmiş kişi tarafından ve ihtiyaç duyulan süre kadar işlenebileceği de belirtilmiştir. Bu açıdan mevzuatta açıkça öngörülen durumlarda dahi kişisel verilerin

uzlaşmazlıkların çözüm süreci tamamlanıncaya kadar gizliliği ve bütünlüğü sağlanarak saklanır. Katma değerli elektronik haberleşme hizmetlerinin sunulması ya da elektronik haberleşme hizmetlerinin pazarlanması amacıyla ihtiyaç duyulan trafik verileri ile konum verileri anonim hâle getirilerek veya ilgili abonelerin/kullanıcıların açık rızalarının alınması ve sadece işletmeci tarafından yetkilendirilen kişilerle sınırlı kalmak kaydıyla, belirtilen faaliyetlerin gerektirdiği ölçü ve sürede işlenebilir.

VIII) İşletmeciler konum verilerinin işlenmesinde abonelere/kullanıcılara bu verilerin işlenmesini reddetme imkânı sağlar. İlgili mevzuatın ve yargı kararlarının öngördüğü durumlar haricinde ancak acil yardım çağrıları ile 29/5/2009 tarihli ve 5902 sayılı Afet ve Acil Durum Yönetimi Başkanlığının Teşkilat ve Görevleri Hakkında Kanunda tanımlanan afet ve acil durum hâllerinde abonelerin/kullanıcıların açık rızası aranmaksızın konum verileri ve ilgili kişilerin kimlik bilgileri işletmeci tarafından yetkilendirilen kişilerle sınırlı olmak kaydıyla işlenebilir.

IX) Abone/kullanıcı şikâyetlerinin incelenmesi ve denetim faaliyetleri kapsamında trafik ve konum verileri ile kişisel veriler, belirtilen faaliyetlerle sınırlı olmak kaydıyla işlenebilir.

X) Bu Kanun kapsamında sunulan hizmetlere ilişkin olarak;

a) Soruşturma, inceleme, denetleme veya uzlaşmazlığa konu olan kişisel veriler ilgili süreç tamamlanıncaya kadar,

b) Kişisel verilere ve ilişkili diğer sistemlere yapılan erişimlere ilişkin işlem kayıtları iki yıl,

c) Kişisel verilerin işlenmesine yönelik abonelerin/kullanıcıların rızalarını gösteren kayıtlar asgari olarak abonelik süresince,

saklanır. Veri kategorileri ile haberleşmenin yapıldığı tarihten itibaren bir yıldan az ve iki yıldan fazla olmamak üzere verilerin saklanma süreleri yönetmelikle belirlenir.

XI) (Değişik:17/7/2019-7186/22 m.) Tahsilata ilişkin riskin yönetilmesi ve kötü niyetli kullanımların önlenmesi amacıyla abonelerin elektronik haberleşme hizmetlerine ve elektronik kimlik bilgisini haiz cihazlara yönelik tarafların kendi sistemlerinde oluşan fatura tutarı ve ödeme bilgileri ile sahtecilik, dolandırıcılık riski içeren şüpheli veya zarar doğurucu vakalara ve işlem hareketlerine ilişkin kayıtlar, işletmeciler ve Kurumun MCKS'si arasında paylaşılabilir veya işlenebilir.

XII) Bu Kanun kapsamında kişisel verilerin gizliliğinin, güvenliğinin ve amacı doğrultusunda kullanılmasının temininden işletmeciler sorumludur.

XIII) Bu maddenin uygulanmasına ilişkin usul ve esaslar Kurum tarafından belirlenir."

işlenmesine ilişkin ilkeler geçerliliğini korumakta olup belirlenen amaç dışına çıkan veya süreyi aşan işleme faaliyetleri hukuka aykırı olmaktadır²⁸⁵.

b. Fiili İmkansızlık Hali

KVKK m. 5/II-b’de, kişisel verilerin işlenmesinin “*fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması*” halinde işlenebileceği düzenlenmiştir. Dolayısıyla kişisel veri sahibinin açıkça verdiği bir rıza olmasa dahi can kaybı veya yaralanma ihtimallerinde kişisel veriler işlenebilir²⁸⁶. Sözelimi; kaybolmuş bir kişinin cep telefonunun konum bilgisinin internet ortamında işlenerek, ilgili kişilerin erişimine açılmasının, fiili imkansızlık halinde gerçekleştirilen şartları sağlanmış bir işleme faaliyeti olduğu belirtilebilir²⁸⁷.

c. Sözleşme Taraflarının Verilerinin İşlenmesi

KVKK m. 5/II-c’de kişisel verilerin “*bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması*” halinde işlenebileceği hüküm altına alınmıştır. Hükümden de anlaşılacağı üzere iki taraf arasında sözleşme akdedilmiş olması tek başına tarafların kişisel verilerin işlenmesi için gerekli hukuki şartı sağlamamaktadır. Sözleşmenin karşılıklı olarak ifa edilebilmesi amacıyla sınırlı olarak veri işleme faaliyeti bu kapsama girmektedir²⁸⁸. Sözelimi; kredi için bankaya başvurulduğunda bankanın başvuru

²⁸⁵ AŞIKOĞLU, s. 116.

²⁸⁶ AŞIKOĞLU, s. 118; GÖÇMEN UYARER, s. 132.

²⁸⁷ Kurum, Kişisel Verilerin İşlenmesinin Şartları, s. 7.

²⁸⁸ GÖÇMEN UYARER, s. 132; BASKIN, s. 120.

sahibine ait tapu kaydı, maaş bordrosu gibi verileri edinmesi bu hüküm kapsamında değerlendirilmektedir²⁸⁹.

Kişisel verilerin, bir sözleşmenin kurulması veya ifası ile doğrudan ilgili olmak kaydıyla işlenmesi incelenirken sözleşmenin kurulması ve ifası aşamalarını ayrı ayrı ele almak gerekmektedir²⁹⁰. Sözleşmenin kurulması aşamasında, sözleşme ile ilgili verilerin toplanmasının TMK m. 2’de yer alan dürüstlük kurallarına uygun işlenmesi gerekir²⁹¹. Örneğin; internet ortamında gerçekleşecek olan bir satış işleminde satıcının, vergi mükellefi olmayan gerçek kişi bir alıcıya ait TCKN bilgisini talep etmesi veya bir şekilde elde ederek faturada yer vermek suretiyle işlemesi bu madde kapsamında değerlendirilmemektedir. 213 sayılı Vergi Usul Kanunu²⁹² m. 230/I²⁹³,’de faturada yer alması gereken hususlar düzenlenmiş olup TCKN, faturada yer alması gereken zorunlu bir unsur olarak belirtilmemiştir. Vergi mükellefi olmayan gerçek kişinin taraf olduğu

²⁸⁹ Kurum, Kişisel Verilerin İşlenmesinin Şartları, s. 8.

²⁹⁰ DEVELİOĞLU, Hüseyin Murat, 6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku, 1. Baskı, İstanbul, On İki Levha Yayıncılık, 2017, s. 61.

²⁹¹ TAŞTAN, s. 134.

²⁹² 213 sayılı Vergi Usul Kanunu, R.G. Sayısı 10705, R.G. Tarihi 12/01/1961.

²⁹³ 230 sayılı VUK m. 230/I: “Faturada en az aşağıdaki bilgiler bulunur:

1. Faturanın düzenlenme tarihi seri ve sıra numarası;
2. Faturayı düzenleyeninin adı, varsa ticaret unvanı, iş adresi, bağlı olduğu vergi dairesi ve hesap numarası;
3. Müşterinin adı, ticaret unvanı, adresi, varsa vergi dairesi ve hesap numarası;
4. Malın veya işin nev'i, miktarı, fiyatı ve tutarı;
5. Satılan malların teslim tarihi ve irsaliye numarası, (Malın alıcıya teslim edilmek üzere satıcı tarafından taşındığı veya taşıttırıldığı hallerde satıcının, teslim edilen malın alıcı tarafından taşınması veya taşıttırılması halinde alıcının taşınan veya taşıttırılan mallar için sevk irsaliyesi düzenlemesi ve taşıtta bulundurulması şarttır. Malın, bir mükellefin birden çok iş yerleri ile şubeleri arasında taşındığı veya satılmak üzere bir komisyoncu veya diğer bir aracıya gönderildiği hallerde de, malın gönderen tarafından sevk irsaliyesine bağlanması gereklidir. Bu bentte yazılı irsaliyeler hakkında fiyat ve bedel ile ilgili bilgiler hariç olmak üzere, bu madde hükmü ile 231 inci madde hükmü uygulanır. İrsaliyelerde malın nereye ve kime gönderildiği ayrıca belirtilir. Şu kadar ki nihai tüketicilerin tüketim amacıyla perakende olarak satın aldıkları malları kendilerinin taşıması veya taşıttırması halinde bu mallara ait fatura veya perakende satış fişinin bulunması şartıyla sevk irsaliyesi aranmaz.)”

internet ortamında kurulan sözleşmelerde TCKN yerine “1111111111” gibi jenerik ifadeler yazılması doğru bir uygulamadır.

Sözleşmenin kurulması aşamasında işlenecek kişisel veriler için GDPR ile KVKK’nin ilgili hükümleri farklılık arz etmektedir. GDPR m. 6/I-b’de²⁹⁴ sözleşmenin ifası aşamasında ayırım gözetilmezken; sözleşmenin kurulması aşamasında kişisel veri işlenebilmesi için akdedilmesini veri sahibinin talep ettiği bir sözleşme olması şartı aranmıştır²⁹⁵. KVKK m. 5/II-c’de böyle bir ibare yer verilmemesine karşın; hükümde yer alan işlenecek kişisel verilerin sözleşmenin kurulmasıyla “doğrudan doğruya ilgili olma” ibaresinin, talebin veri sahibinden gelme şartına işaret ettiği yönünde görüşler mevcuttur²⁹⁶. Kanaatimizce; KVKK’nin uygulanmasında da sözleşmenin kurulması aşamasında talebin veri sahibinden sadır olması, çalışmamızın konusunu oluşturan internet ortamında işlenen kişisel veriler açısından daha isabetlidir. Nitekim internet ortamında çoğu zaman herhangi bir siteye girildiği anda yalnızca bir form doldurmak suretiyle sözleşme kurulabilmektedir. Sözleşme kurulması talebinin veri sahibinden gelmesinin gerektiği görüşünün kabul edilmemesi durumunda; veri sorumlusunun, internet sitesinde yer verdiği teklif içeren bir formun, sözleşmenin kurulması talebi olması sebebiyle kullanıcıya ait veriyi işlemek için hukuka uygunluk sebebi sayılması durumu ortaya çıkacaktır.

²⁹⁴ GDPR m. 6/I-b: “İşleme, ancak aşağıdaki hususlardan en az biri geçerli olduğunda ve geçerli olduğu ölçüde hukuka uygundur:

...

veri öznesinin taraf olduğu bir sözleşmenin uygulanması veya bir sözleşme yapılmadan önce veri öznesinin talebiyle adımlar atılması için işlemenin gerekli olması.”

²⁹⁵ UZUNAL, s. 68.

²⁹⁶ YÜCEDAĞ, Nafiye, *Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu’nun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri*, İÜHFİM, C. 75, S. 2, 2018, s. 778.

d. Veri Sorumlusunun Hukuki Yükümlülüğünü Yerine Getirmesi

KVKK m. 5/II-ç’de, kişisel verilerin “veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması” halinde işlenebileceği düzenlenmiştir. Aynı düzenleme GDPR m. 6/1/c’de²⁹⁷ de yer almıştır.

Kanun koyucu KVKK m. 5/II-ç’de veri sorumlusu için kamu veya özel hukuk tüzel kişisi olmasına ilişkin bir ayrım gözetmediği için hem özel hukuk hem de kamu hukukundan kaynaklanan yükümlülüklerin yerine getirilmesinin kişisel verilerin işlenmesi şartını oluşturduğu kabul edilmektedir²⁹⁸.

5651 sayılı Kanun m. 5/III’te²⁹⁹ yer sağlayıcılar kullanıcılara ait internet trafik bilgisini³⁰⁰ bir yıldan kısa, iki yıldan uzun olmamak kaydıyla saklamakla yükümlendirilmiştir. IP adresi, internet ortamında gerçekleştirilen işlemler, gönderilen ve indirilen veriler gibi çeşitli bilgiler ve bu bilgilerden hareketle farklı bilgilere ulaşmayı sağlayan trafik bilgisinin kişisel veri oluşturduğu izahtan varestedir³⁰¹. Dolayısıyla internet ortamının 5651 sayılı Kanun’da tanımlanmış aktörlerinden olan yer sağlayıcılarının, veri sorumlusu sıfatını haiz oldukları durumlarda kullanıcılarına ait trafik verilerini belirlenen süre nispetinde saklaması, açık rıza olmasa dahi hukuki bir

²⁹⁷ GDPR m. 6/1-c: “İşleme, ancak aşağıdaki hususlardan en az biri geçerli olduğunda ve geçerli olduğu ölçüde hukuka uygundur:

...
veri sorumlusunun tabi olduğu bir yasal yükümlülüğe uyulması amacıyla işlemenin gerekli olması.”

²⁹⁸ TAŞTAN, s. 136.

²⁹⁹ 5651 sayılı Kanun m. 5/III: “Yer sağlayıcı, yer sağladığı hizmetlere ilişkin trafik bilgilerini bir yıldan az ve iki yıldan fazla olmamak üzere yönetmelikte belirlenecek süre kadar saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakta yükümlüdür..”

³⁰⁰ Yer sağlayıcı trafik bilgisi İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik m.3/I-ş’de; “İnternet ortamındaki her türlü yer sağlamaya ilişkin olarak; kaynak IP adresi, hedef IP adresi, bağlantı tarih ve saat bilgisi, istenen sayfa adresi, işlem bilgisi (GET, POST komut detayları) ve sonuç bilgileri” şeklinde tanımlanmıştır.

³⁰¹ KÜZECİ, s. 330.

yükümlülük yerine getirildiğinden hukuka uygun bir kişisel verilerin işlenmesi durumunu oluşturmaktadır.

e. Kişisel Verinin Alenileştirilmesi

KVKK m. 5/II-d’de ilgili kişinin (kişisel veri sahibi) kendisince alenileştirilen kişisel verilerin işlenmesinin hukuka uygun olacağı düzenlenmiştir³⁰². Burada dikkat edilmesi gereken temel husus; kişisel verilerin bizzat veri sahibi tarafından aleni hale getirilmiş olması gerekliliğidir. Örneğin; bir kişinin ticari bir amaçla internet ortamına umuma açık bir şekilde paylaştığı telefon numarasının alenileştirildiği belirtmek mümkündür³⁰³.

Herhangi bir kişisel verinin alenileştirilmiş olmasının, ilgili kişisel verinin alenileştirilme amacı dışında işlenmesini hukuka uygun kılmadığı değerlendirilmektedir³⁰⁴. Örneğin bir kişinin herhangi bir hizmet ilanı amacıyla internet ortamında paylaştığı cep telefonu numarasının, ticari reklam gönderme amacıyla üçüncü kişilerle paylaşılacak suretiyle işlenmesi durumunda, alenileştirilme işleme faaliyeti için hukuki sebep oluşturmayacaktır. Uyuşmazlık konusu olan benzer bir somut olayda da Kurul; iletişim bilgilerini finansal güvence danışmanlığı hizmeti almak üzere ilgili sitelerde aleni şekilde paylaşan kişiyi sigorta şirketinin aramasının, alenileştirme amacına hizmet etmediği gerekçesiyle hukuka aykırı olduğuna karar vermiştir³⁰⁵.

³⁰² Kurum, Kişisel Verilerin İşlenmesinin Şartları, s. 10.

³⁰³ Kurum, Kişisel Verilerin İşlenmesinin Şartları, s. 10.

³⁰⁴ BASKIN, s. 121, BUDAK, Muhammed Alparşlan/MALKOÇ, Seda, Kişisel Verilerin Korunması Kanunu'na Aykırı Davranılmasında Hukuki Sorumluluk, 1. Baskı, Ankara, 2021, s. 78, GÖÇMEN UYARER, s. 134.

³⁰⁵ Kişisel Verileri Koruma Kurulu T. 07. 11. 2019, S. 2019/331: “...Şikâyetçinin kişisel verilerine kendisi tarafından daha önce alenileştirilen internet sitesinden ulaşılması halinde dahi Şirket tarafından Şikâyetçinin bu bilgilerinin internet sitesinde bulunma ve alenileştirilme amacıyla kullanılmadığı, diğer bir deyişle Şikâyetçinin mesleki yetkinliğinden faydalanmak için kendisine ulaşılmaya çalışılmadığı, aksine Şirket

f. Bir Hakkın Tesisi, Kullanılması veya Korunması İçin Zorunluluk

KVKK m. 5/II-e’de kişisel verilerin “bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması” halinde işlenebileceği düzenlenmiştir. Kanun koyucu “zorunluluk” ibaresine yer vererek; bir hakkın başkaca bir yöntemle tesis edilmesi, kullanılması veya korunmasının mümkün olduğu durumlarda kişisel veri işlemenin hukuka uygun olmayacağına işaret etmiştir. Bir kısıtlının haklarını korumak üzere vasisinin, kısıtlıya ait mali bilgileri saklaması; sona eren bir sözleşmenin ardından yasal takiplere karşı zamanaşımı dolana kadar faturanın, dolayısıyla faturada yer alan kişisel verilerin muhafaza edilmesi gibi durumlar KVKK m. 5/II-e’ye örnek gösterilmektedir³⁰⁶.

KVKK’de bir hakkın tesisi, kullanılması veya korunması için zorunlu olan işleme faaliyetine esas oluşturan hakkın, kanundan veya sözleşmeden doğması veya hak sahibinin veri sorumlusu mu yoksa kişisel verileri işlenen kişi mi olacağı yönünde ayrımlar yapılmamıştır. İştirak ettiğimiz görüşe göre; hem veri sorumlusunun hem de kişisel veri sahibinin hakkının kullanılması, tesisi veya korunması için zorunluluk hasıl olduğunda kişisel veriler işlenebilecektir³⁰⁷. Kurul’un bir kararına konu olan somut olayda internet aboneliği sözleşmesi akdetmek üzere kimlik fotokopisi istenen bir şahıs, bu nedenle abonelik sözleşmesi akdetmeyerek kişisel verilerinin silinmesini talep etmiştir. Kurul, daha sonra ortaya çıkan bir uyuşmazlıkta işletmecinin savunma hakkını

faaliyetlerine ilişkin randevu talebi ile Şikâyetçinin arandığı anlaşıldığından, Şirket tarafından gerçekleştirilen veri işleme faaliyetinin 6698 sayılı Kişisel Verilerin Korunması Kanununun 5 inci maddesinin (2) numaralı fıkrasının (d) bendi çerçevesinde değerlendirilemeyeceği kanaatine varılmış olup, ... Şirket hakkında ... idari para cezası uygulanmasına karar verilmiştir.”, <https://www.kvkk.gov.tr/Icerik/6623/2019-331>, E. T. 22/10/2023.

³⁰⁶ Kurum, Kişisel Verilerin İşlenme Şartları, s. 11; AŞIKOĞLU, s. 125; BASKIN, s. 123.

³⁰⁷ AŞIKOĞLU, s. 125-126.

kullanmasını teminen veri sahibinin verilerinin silinmemesini hukuka uygun bulmuştur³⁰⁸.

GDPR’da bir hakkın kullanılması, tesisi veya korunması için zorunlu olma hali kişisel verilerin işlenmesi sebeplerinden biri olarak sayılmamıştır³⁰⁹. Bunun yanında; kişisel verilerin silinmesine ilişkin GDPR m. 17/III-e’de³¹⁰; yasal bir hakkın tesisi, kullanılması ve savunulması için gerekli olduğu durumlarda kişisel verilerin silinmeyebileceği düzenlenmiştir. Buradan da anlaşılabileceği üzere GDPR’da, KVKK’dan farklı olarak bir hakkın kullanılması, tesisi veya korunmasını kişisel verilerin işlenmesi için değil silinmemesi için bir sebep olarak görülmüştür. Dolayısıyla GDPR’a göre kişisel verilerin işlenmesi için mezkur gerekçe yeterli değildir.

İnternet ortamının çoklu aktörlü yapısı göz önüne alındığında mezkûr kanun hükmünün üçüncü şahıslara da genişletilebileceği değerlendirilmektedir. Zira, internet ortamının eş zamanlı milyonlarca kişiye açık yapısı, konvansiyonel hukuki ilişkilerin ötesinde yeni hak ve menfaatler ortaya çıkarmaktadır.

g. Veri Sorumlusunun Meşru Menfaati

KVKK m. 5/II-f’de; “ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması”

³⁰⁸ Kişisel Verileri Koruma Kurulu T. 26.08. 2021, S. 2021/859, <https://www.kvkk.gov.tr/Icerik/7135/2021-859>, E. T. 20/11/2023; UZUNAL, s. 72.

³⁰⁹ BASKIN, s. 123; AŞIKOĞLU, s. 126

³¹⁰ GDPR m. 17: “1) Veri öznesinin kendisi ile ilgili kişisel verilerin fazla gecikmeksizin kalıcı olarak silinmesini veri sorumlusundan temin etme hakkı bulunur ve aşağıdaki hâllerden birinin geçerli olması durumunda, veri sorumlusu kişisel verileri fazla gecikmeksizin kalıcı olarak silmekle yükümlüdür:

...

3) İşleme aşağıdaki amaçlar doğrultusunda gerekli olduğu ölçüde 1 ve 2. paragraflar uygulanmaz:

...

e) hak taleplerinin oluşturulması, hakkın yerine getirilmesi veya savunulması açısından.”

halinde kişisel verilerin işlenebileceği düzenlenmiştir. Hükümden de anlaşılacağı üzere bu düzenleme kapsamında kişisel verilerin işlenebilmesi için veri sorumlusunun menfaatinin meşru olması ve kişisel verileri işlenecek kişinin temel hak ve özgürlüklerine hâlel getirilmemesi gerekmektedir. Dolayısıyla kişisel veri sahibinin temel hak ve özgürlükleriyle, veri sorumlusunun meşru menfaati arasında bir denge kurulmalıdır³¹¹. Bu denge kapsamında meşru menfaat, temel hak ve özgürlükle yarışabilecek yoğunlukta olmalıdır.

KVKK gerekçesinde³¹² mezkur hükmün uygulama alanına örnek olarak bir işverenin liyakatli işçilerini terfi ettirmesinin kendi menfaatine hizmet ettiği, dolayısıyla terfiler için kişisel verilerin meşru menfaat kapsamında işlenebileceği ifade edilmiştir. Bunun yanında meşru menfaatin tanımına KVKK’de yer verilmemiş olup KVKK m. 5/II-f hükmü kişisel verilerin korunması isteme hakkını objektif olmayan kriterlere göre kısıtlandığından eleştirilmektedir³¹³.

GDPR m. 6/I-f’de³¹⁴ meşru menfaat kavramı yalnızca veri sorumlusu ile sınırlı tutulmamış; üçüncü kişilerin de meşru menfaatinin gerektiği durumlarda kişisel verilerin işlenebileceği düzenlenmiştir³¹⁵. Ayrıca KVKK’den farklı olarak veri sorumlusunun menfaatine bağlı olarak işleme faaliyetinin, kişisel verileri işlenen kişinin temel hak ve hürriyetine hâlel getirmemesinin yanı sıra bu kişinin menfaatlerine aykırı olmaması şartı

³¹¹ Kurum, Kişisel Verilerin İşlenme Şartları, s. 13; AŞIKOĞLU, s. 126; BASKIN, s. 124; BUDAK/MALKOÇ, s. 80.

³¹² Gerekçe için bknz: <https://www5.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf> E.T. 28/10/2023.

³¹³ GÖÇMEN UYARER, s. 134; AŞIKOĞLU, s. 126; UZUNAL, s. 73.

³¹⁴ GDPR m. 6/I-f: “İşleme, ancak aşağıdaki hususlardan en az biri geçerli olduğunda ve geçerli olduğu ölçüde hukuka uygundur:

...
Özellikle veri öznesinin çocuk olması hâlinde, kişisel verilerin korunmasını gerektiren, veri öznesinin menfaatleri veya temel hak ve özgürlüklerinin bir veri sorumlusu veya üçüncü kişi tarafından gözetilen meşru menfaatlere ağır basması haricinde, söz konusu meşru menfaatler doğrultusunda işlemenin gerekli olması.”

³¹⁵ UZUNAL, s. 73.

aranmıştır. Doktrinde yer alan mezkûr kanun hükmüne göre kişisel verilerin işlenmesi halinde; veri sorumlusu ve kişisel veri sahibinin menfaatleri arasında bir denge kurulması gerektiği yönündeki görüşe³¹⁶ tarafımızca iştirak edilmemektedir. Veri sorumlusunun menfaatine dayanarak veri işleyebilmesi için ilgili kişinin menfaatinin zedelenmemesi gerekmektedir. Zira lafzi yorum yapıldığında; kanun koyucu iki durum arasında herhangi bir ayırım gözetmediğinden veri işleme sürecinin ilgili kişinin temel hak ve hürriyetlerini ihlal ettiği durumda da denge kurulması cihetine gidilmesi gerekmektedir. Amaçsal yorum yapıldığında ise; veri sorumlusu ve veri sahibinin menfaatlerinin çakışması durumunda rıza alınmamasının kanunun özüne aykırı olduğu değerlendirilmektedir.

GDPR gerekçelerinin dördüncü kısmında³¹⁷ kişisel verilerin işlenmesi süreçlerinin insanlığın ortak yararına olacak şekilde kurgulanması gerektiği ve kişisel verilerin korunmasını isteme hakkının mutlak bir hak olmadığı hususları yer almaktadır. Bundan da hareketle her ne kadar yukarıda veri sahibinin menfaatinin olduğu durumlarda veri sorumlusunun menfaatine bakılmayacağı yönünde bir görüş ortaya konmuş olsa da; tıbbi araştırma gibi tüm insanlığın menfaatine olacak durumlarda ilgili kişinin menfaati olsa dahi menfaat dengesine gidilebileceği mütalaa edilmektedir. Zira GDPR’da zaten üçüncü kişinin menfaati ilgili hükümde düzenlenmiştir.

Veri sorumlusunun menfaatine bağlı olarak kişisel verilerin işlenmesi çalışmamızın konusu bağlamında da önem arz etmektedir. Zira internet ortamının girift

³¹⁶ ÇEKİN, s. 636; UZUNAL, s. 73-74.

³¹⁷ GDPR Recital 4: “Kişisel verilerin işlenmesi insanlığa hizmet edecek şekilde tasarlanmalıdır. Kişisel verilerin korunması hakkı mutlak bir hak değildir; toplum içindeki işleviyle ilişkili olarak ele alınmalı ve orantılılık ilkesine uygun olarak diğer temel haklarla denge içinde olmalıdır. Bu Tüzük tüm temel haklara saygı gösterir ve özel hayata ve aile hayatına, konuta ve iletişime saygı, kişisel verilerin korunması, düşünce, vicdan ve din özgürlüğü, ifade ve bilgi edinme özgürlüğü, iş yapma özgürlüğü, etkili bir hukuk yolu ve adil yargılanma hakkı ile kültür, din ve dil çeşitliliği başta olmak üzere, Antlaşmalarda güvence altına alındığı gibi Şart’ta tanınmış olan özgürlük ve ilkeleri gözetir..”

ve dinamik yapısı sayısız ilişki ağı, karşılık menfaat dengesi oluşturmaktadır. Özellikle internet sitesi işletmecileri, internet sitesini ziyaret eden kullanıcıların kişisel verilerini, reklam geliri elde etmek suretiyle ticari menfaat amacıyla işleyebilmektedirler. Kurul tarafından incelenen bir uyumsuzlukta internet sitesine girişte rıza alınmaksızın zorunlu olmayan çerezlerin de kaydedildiği, Kurul'un uyumsuzluğu KVKK m. 5/II-f hükmü çerçevesinde de değerlendirdiği, netice itibarıyla veri sorumlusunun menfaatinin yeterli olmadığı yönünde karar verdiği görülmüştür³¹⁸. Bunun yanında Kurul tarafından karar kaleme alınırken; internet sitesinin faaliyet göstermesi için teknik açıdan gerekli verilerin işlenebileceğine işaret edilmiştir. İnternet sitesinin faal olması, veri sorumlusunun yanı sıra üçüncü kişilerin de menfaatine olacağı göz önüne alındığında, bu kararın GDPR'da kurgulanan menfaat dengesi modeline uygun olduğu değerlendirilmektedir.

³¹⁸ Kişisel Verileri Koruma Kurulu T. 23. 12. 2022, S. 2022/1358: "... bir oyun platformunun internet sayfasına giriş yapıldığında çerez işleme süreçleriyle ilgili kullanıcılara aydınlatma yapılmadığı ve zorunlu olmayan çerezler için açık rıza alınmadığı, siteye üye olan kullanıcılardan kimlik ve iletişim bilgilerinin talep edildiği ancak aydınlatma ve açık rıza metinlerinin sunulmadığı

... ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla veri sorumlusunun meşru menfaati için veri işlenmesinin zorunlu olması hallerinde ilgili kişinin açık rızası olmaksızın kişisel verilerin işlenmesinin mümkün olduğunun hükme bağlandığı,

... Öte yandan, bir internet sitesinin düzgün çalışması için zorunlu çerezler vasıtasıyla kişisel verilerin işlenmesinde kişilerin açık rızasına gerek duyulmayacak iken; reklam, pazarlama ve performans amacıyla çalışan çerezlerin kullanılmasının ilgili kişinin açık rızasına tabi olduğu, "kesinlikle gerekli çerezler" in internet sitesinin düzgün çalışması için gerekli çerezler olduğu, ilgili kişinin açık rızası olmaksızın Kanun'un 5'inci maddesinin (2) numaralı fıkrasında ve Kanun'un 6'ncı maddesinin (3) numaralı fıkrasında yer alan işleme şartlarından birine dayanılarak kişisel veri işleme faaliyeti gerçekleştirilebileceği, "kesinlikle gerekli çerezler" statüsünde olmayan çerezler ile kişisel veri işleme faaliyeti gerçekleştirilmesi ve Kanun'un 5'inci maddesinin (2) numaralı fıkrası ile 6'ncı maddesinin (3) numaralı fıkrasında yer alan işleme şartlarından birinin bulunmaması durumunda ilgili kişinin açık rızasına başvurulması gerektiği,

... Veri sorumlusu tarafından internet sayfasında herhangi bir işleme şartına dayanmadan reklam ve pazarlama amacı gibi zorunlu olmayan çerezler vasıtasıyla kişisel veri işlendiği, bu durumun ise Kanun'un 12'nci maddesinin (1) numaralı fıkrasında yer alan yükümlülüklerle aykırılık teşkil ettiği... " <https://www.kvkk.gov.tr/Icerik/7595/2022-1358>, E. T. 24/12/2023.

Kanaatimizce de; internet ortamında KVKK m. 5/II-f uyarınca gerçekleşen bir kişisel veri işleme faaliyetinde hem veri sorumlusunun hem veri sahibinin menfaati olması halinde; üçüncü kişilerin menfaati olup olmadığına bakılması gerekmektedir.

3. Özel Nitelikli Kişisel Verilerin İşlenmesinin Şartları

KVKK m. 6³¹⁹'da özel nitelikli kişisel verilerin³²⁰ işlenme şartları düzenlenmiştir. Kanun koyucu tarafından, mezkur madde hükmünde tahdidi olarak belirtilen özel nitelikli kişisel verilerin işlenebilmesi için ilgili kişinin açık rızasının ve Kurul tarafından belirlenen yeterli önlemlerin alınması şartı getirilmiştir.

KVKK m. 6/II'de, özel nitelikli kişisel verilerin ilgili kişinin açık rızası alınmaksızın işlenemeyeceği belirtildikten sonra takip eden KVKK m. 6/III'de "sağlık" ve "cinsel hayat" dışında kalan kişisel verilerin kanunda öngörülen hallerde işlenebileceği düzenlenmiştir³²¹. Aynı fıkranın devamında sağlık ve cinsel hayata ilişkin kişisel verilerin açık rıza dışında işlenebileceği hallerin de düzenlenmesi adeta istisnanın istisnası olarak karşımıza çıkmaktadır. Bu durum kanaatimizce Kanun'un sistematığına aykırılık oluşturmaktadır. Nitekim üçüncü fıkra da her çeşit özel nitelikli olmayan kişisel veriler

³¹⁹ KVKK m. 6: "I) Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir.

II) Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır.

III) Birinci fıkra da sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir.

IV) Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır."

³²⁰ Özel nitelikli kişisel veriler için bkz: Birinci Bölüm, I, D, 2.

³²¹ TAŞTAN, s. 138; GÖÇMEN UYARER, s. 136; BASKIN, s. 125.

için açık rıza aranmaksızın kişisel verileri işlenebileceği istisnalar sayıldığından ikinci fıkra hükmü madde içerisinde çelişki yaratmaktadır.

KVKK m. 6/III’de yer alan sağlık ve cinsel yaşama ilişkin verilerin “*kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla*” işlenebileceğine ilişkin hükümde “kanunda öngörülme” şartı aranmamasının eleştirildiği görüşe³²² tarafımızca iştirak edilmektedir. Nitekim oldukça hassas olan sağlık ve cinsel hayata dair kişisel verilerin işleme amaçları, “kanunda öngörülme” gibi bir objektif koşul aranmaksızın muğlak ve geniş tutulmuştur.

Dinamik yapısı, bilgi işleme sistemlerinin çok seri ve takip edilemez olduğu internet ortamında yapılacak basit paylaşımların dahi kullanıcıya ait bir profil oluşturarak özel nitelikli kişisel verilerine ulaşmaya imkân kılması, internet ortamındaki verilerin ne ölçüde özel nitelikli sayılacağı tartışmalarına sebep olmaktadır³²³. Kanaatimizce de, özel nitelikli kişisel verilere ulaşmayı sağlayacak özel nitelikli olmayan verilerin de özel nitelikli sayılabileceği değerlendirilmektedir.

KVKK m. 6/IV’te özel nitelikli kişisel verilerin işlenebilmesi için Kurul tarafından belirlenmiş “yeterli” önlemlerin alınması gerekliliği düzenlenmiştir. Kurul’un 2018 yılında verdiği bir kararda³²⁴ Kanun’un atıf yaptığı kurallar belirlenmiştir. Çalışmamızın konusu bağlamında mezkur kararda elektronik ortamda işlenecek veriler için kriptoyöntemler kullanılması, *loglama*, kullanıcı yetkilendirmeleri, iki aşamalı doğrulama gibi ilave tedbirler öngörülmüştür³²⁵.

³²² GÖÇMEN UYARER, s. 136-137.

³²³ KÜZECİ, s. 250.

³²⁴ Kişisel Verileri Koruma Kurulu T. 31.01. 2018, S. 2018/10.

³²⁵ GÖÇMEN UYARER, s. 139.

GDPR m. 9/I'de³²⁶; kişinin ırkı, etnik kökeni, politik fikirleri, dini ve felsefi inançları, sendika üyeliğini gösteren verileri, genetik, biyometrik verileri, sağlık ve cinsel yaşama ilişkin verilerinin özel nitelikli olduğu düzenlenmiş olup bunların işlenmesi yasaklanmıştır. Bunun yanında özel nitelikli verilerin işlenmesine ilişkin mezkûr yasağa GDPR m. 9/II'de detaylı bir şekilde istisnalar getirilmiştir³²⁷. KVKKda özel nitelikli kişisel verilerin ancak açık rıza ile işlenebileceği ana kural olarak öngörülmüşken; GDPR'da açık rıza da istisna hali olarak düzenlenmiştir.

³²⁶ GDPR m. 9/I: “İrk veya etnik köken, siyasi görüşler, dini veya felsefi inançlar ya da sendika üyeliğini açığa çıkaran kişisel verilerin işlenmesi ve bir gerçek kişinin kimliğini benzersiz bir şekilde belirleyen genetik veriler ile biyometrik verilerinin işlenmesi, sağlık verilerinin veya bir gerçek kişinin cinsel yaşamı veya cinsel eğilimine ilişkin verilerin işlenmesi yasaktır.”

³²⁷ GDPR m. 9/II'de özel nitelikli verilerin işlenmesi yasağına getirilen istisnalar kısaca;
Veri sahibinin açık rızasının bulunması
Veri sahibinin temel haklarının korunması
Veri sorumlusunun hayati çıkarları
Politik, dini, sendikal amaçlı sivil toplum kuruluşların dışarı açıklanmamak koşuluyla üyelerinin verileri
Veri sahibinin alenileştirmesi
Yargıya konu olması
Kamu menfaati
Sağlık çalışanları ile sözleşme yapılması
Sağlık risklerine karşı korunma
Arşivleme, araştırma
olarak maddelenmiştir. Detaylı bilgi için bkz: YILMAZ, Tüze, Avrupa Birliğinde, Kişisel Verilerin Korunması Hukuku, 1. Baskı, Ankara, 2022, s. 94-95.

II. KİŞİSEL VERİLERİN HUKUKA AYKIRI İŞLENMESİ

A. Yaygın Hukuka Aykırılık Halleri

1. Aktarım

KVKK m. 8³²⁸ ve m. 9³²⁹ hükümlerinde kişisel verilerin yurt içinde veya yurt dışına aktarımı şartları düzenlenmiştir. Esasında kişisel verilerin yurt içinde veya yurt dışına aktarımı, KVKK m. 3/I-e uyarınca kişisel verilerin işlenmesi alt yöntemlerinden birisidir. Dolayısıyla kişisel verilere işlenmesine ilişkin öngörülen şartların, kişisel verilerin aktarımı içinde aranması gerekmektedir. Kişisel verilerin yurt içinde aktarımının

³²⁸ KVKK m. 8 : “I) Kişisel veriler, ilgili kişinin açık rızası olmaksızın aktarılamaz.

II) Kişisel veriler;

a) 5 inci maddenin ikinci fıkrasında,

b) Yeterli önlemler alınmak kaydıyla, 6 ncı maddenin üçüncü fıkrasında, belirtilen şartlardan birinin bulunması hâlinde, ilgili kişinin açık rızası aranmaksızın aktarılabilir.

III) Kişisel verilerin aktarılmasına ilişkin diğer kanunlarda yer alan hükümler saklıdır.”

³²⁹ KVKK m. 9: “I) Kişisel veriler, ilgili kişinin açık rızası olmaksızın yurt dışına aktarılamaz.

II) Kişisel veriler, 5 inci maddenin ikinci fıkrası ile 6 ncı maddenin üçüncü fıkrasında belirtilen şartlardan birinin varlığı ve kişisel verinin aktarılacağı yabancı ülkede;

a) Yeterli korumanın bulunması,

b) Yeterli korumanın bulunmaması durumunda Türkiye’deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurulun izninin bulunması,

kaydıyla ilgili kişinin açık rızası aranmaksızın yurt dışına aktarılabilir.

III) Yeterli korumanın bulunduğu ülkeler Kurulca belirlenerek ilan edilir.

IV) Kurul yabancı ülkede yeterli koruma bulunup bulunmadığına ve ikinci fıkranın (b) bendi uyarınca izin verilip verilmeyeceğine;

a) Türkiye’nin taraf olduğu uluslararası sözleşmeleri,

b) Kişisel veri talep eden ülke ile Türkiye arasında veri aktarımına ilişkin karşılıklılık durumunu,

c) Her somut kişisel veri aktarımına ilişkin olarak, kişisel verinin niteliği ile işlenme amaç ve süresini,

ç) Kişisel verinin aktarılacağı ülkenin konuyla ilgili mevzuatı ve uygulamasını,

d) Kişisel verinin aktarılacağı ülkede bulunan veri sorumlusu tarafından taahhüt edilen önlemleri, değerlendirmek ve ihtiyaç duyması hâlinde, ilgili kurum ve kuruluşların görüşünü de almak suretiyle karar verir.

V) Kişisel veriler, uluslararası sözleşme hükümleri saklı kalmak üzere, Türkiye’nin veya ilgili kişinin menfaatinin ciddi bir şekilde zarar göreceği durumlarda, ancak ilgili kamu kurum veya kuruluşunun görüşü alınarak Kurulun izniyle yurt dışına aktarılabilir.

VI) Kişisel verilerin yurt dışına aktarılmasına ilişkin diğer kanunlarda yer alan hükümler saklıdır.”

düzenlendiği KVKK m. 8’de, kişisel verilerin işlenmesi şartlarına ilave bir husus öngörülmemiştir.

İnternet ortamında işlenen kişisel verilerin veri sorumlusunun kendi “*server*”ları (sunucu) arasında veya veri işleyen ile arasında aktarımının KVKK m. 8 ve m. 9 hükmü kapsamında değerlendirilip değerlendirilmeyeceğinin tayini gerekmektedir. Nitekim GDPR m. 44-50 arasındaki bölümlerde kişisel verilerin “*üçüncü ülkelere veya uluslararası organizasyonlara aktarımı*” düzenlenmiştir. GDPR m. 4/10’da ise üçüncü kişiler “*veri sorumlusunun veya veri işleyenin doğrudan tahakkümü altında olmayan kişiler*” olarak tanımlanmıştır³³⁰. KVKK’de üçüncü kişi tanımına yer verilmemesinin yanı sıra aktarımın düzenlendiği KVKK m. 8 ve m. 9 hükümlerinin tasarısından “*üçüncü kişiye aktarım*” ibaresi çıkarılmıştır³³¹. Dolayısıyla uygulamada sıklıkla karşımıza çıkan internet ortamındaki kişisel verilerin veri sorumlusu veya veri işleyene ait farklı bir veri merkezine aktarılmasının, KVKK m. 8 ve m. 9 hükümlerine uygun yapılması gerekmektedir. Her ne kadar GDPR’da aktarım faaliyeti için “*üçüncü kişi*” şartı aranmış olsa da; tarihi kanun koyucunun KVKK tasarısından “*üçüncü kişi*” ibaresini çıkarması nedeniyle daraltıcı yorum yapılarak kişisel verilerin aktarımına ilişkin KVKK hükümlerinin yalnızca üçüncü kişileri kapsayacağını yorumlamak, tarihi kanun koyucunun iradesiyle ters düşecektir.

2. Aydınlatma Yükümlülüğüne Aykırılık

Kişisel verilerin işlenmesi sürecinde veri sorumlusu aydınlatma yükümlülüğü ile mükelleftir. KVKK m. 10³³²’da düzenlenen aydınlatma yükümlülüğünü ihlal etmek

³³⁰ UZUNAL, s. 80.

³³¹ GÖÇMEN UYARER, s. 140.

³³² KVKK m. 10: “*1) Kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişi, ilgili kişilere;*

suretiyle ilgili kişilerin; veri sorumlusunun veya temsilcisinin kimliği, kişisel verilerin işlenme amacı, kişisel verilerin kime, ne amaçla aktarılacağı, kişisel verilerin toplama yöntemleri ve hukuki sebebi, ilgili kişinin hakları konusunda veri sorumlusu veya temsilcisi tarafından bilgilendirilmemesi kişisel verilerin işlenmesi faaliyetini hukuka aykırı kılmaktadır³³³.

İnternet ortamının interaktif ve sürekli yenilenen yapısı, veri sorumlusu açısından aydınlatma yükümlülüğünün yerine getirilmesi açısından kolaylık sağlamaktadır. Nitekim uygulamada internet sitelerinin birçoğunda “aydınlatma metni” için ayrı bir bölüm düzenlenmiştir. Anayasa’nın m. 20’de de yer alan aydınlatma yükümlülüğünün önemine binaen “*Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ*”³³⁴ yürürlüğe girmiştir.³³⁵ Mezkûr düzenlemede aydınlatma yükümlülüğünün ne şekilde yerine getirileceğine ilişkin usul ve esaslar ortaya konulmuştur. Usul ve esaslardan internet ortamında gerçekleştirilecek bilgilendirme faaliyeti özelinde mezkûr düzenlemenin m. 5/I-d³³⁶’de düzenlenen talepten mücerretlik ve m. 5/I-f³³⁷’de yer alan açık rıza ve bilgilendirmenin ayrı ayrı yapılması hususları önem arz etmektedir. İnternet ortamında çoğu zaman kullanıcılar verilerinin işlenmesine ilişkin bilgilendirmeyi okumadan onay vermektedir. Talep olmaksızın bilgilendirmenin yapılması yükümlülüğü, internet deneyimini hızlandırmak adına bilgilendirilmekten

-
- a) Veri sorumlusunun ve varsa temsilcisinin kimliği,
 - b) Kişisel verilerin hangi amaçla işleneceği,
 - c) İşlenen kişisel verilerin kimlere ve hangi amaçla aktarılabilceği,
 - ç) Kişisel veri toplamanın yöntemi ve hukuki sebebi,
 - d) 11 inci maddede sayılan diğer hakları,
- konusunda bilgi vermekle yükümlüdür.”

³³³ TAŞTAN, s. 142; GÖÇMEN UYARER, s. 93; UZUNAL, s. 75.

³³⁴ R.G. Sayısı: 30356, R.G. Tarihi: 10.03. 2018.

³³⁵ TURAN, s. 80; AŞIKOĞLU, s. 115.

³³⁶ “Aydınlatma yükümlülüğünün yerine getirilmesi, ilgili kişinin talebine bağlı değildir.”

³³⁷ “Kişisel veri işleme faaliyetinin açık rıza şartına dayalı olarak gerçekleştirilmesi halinde, aydınlatma yükümlülüğü ve açık rızanın alınması işlemlerinin ayrı ayrı yerine getirilmesi gerekmektedir.”

imtina edilmesinin önüne geçmektedir. Bilgilendirme yapılması ve rızanın alınması işlemlerinin eş zamanlı gerçekleştirilmemesini teminen; veri sorumlusu olan internet sitesi işletmecilerinin, aydınlatma metninin sonuna kadar okunmadan rıza verme seçeneğinin aktif olmaması gibi çözümlerle, aydınlatma yükümlülüğünü hukuka uygun bir şekilde yerine getirebileceği değerlendirilmektedir.

3. Verilerin Muhafazası ve İmhası

KVKK m. 4/I-d'de³³⁸ kişisel verilerin yalnızca mevzuatta öngörülen veya amaç ile sınırlı olmak kaydıyla muhafaza edilebileceği düzenlenmiştir. Mezkûr hükümle bağlantılı olarak KVKK m. 7/I'de³³⁹ kişisel verilerin işlenmesini gerektiren hukuki sebebin ortadan kalktığı durumlarda re'sen veya talep üzerine verilerin silinmesi, yok edilmesi veya anonimleştirilmesi gerektiği belirtilmiştir. Görüldüğü üzere; kişisel verilerin imhası için KVKK'de üç farklı yöntem öngörülmüştür.

Üç farklı yöntemle gerçekleştirilebilen kişisel verilerin imhası; "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik"³⁴⁰'te tüm yöntemleri kapsayan genel bir ibare olarak ele alınmıştır. Kişisel verilerin silinmesi, kullanıcılar tarafından erişilemez hale getirilmesi; kişisel verilerin yok edilmesi, kimse tarafından geri dönüşü olmayacak şekilde erişilemez hale getirilmesi; kişisel verilerin anonimleştirilmesi, verilerin belirli veya belirlenebilir bir kişi ile ilişkilendirilmesinin

³³⁸ KVKK m. 4/I-d: "İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme."

³³⁹ KVKK m. 7/I: "Bu Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir."

³⁴⁰ R.G. Tarihi: 28. 10. 2017, R.G. Sayısı: 30224.

imkânsız hale getirilmesi olarak tanımlanmıştır.³⁴¹ Konumuz bağlamında silme ve yok etme arasındaki farklılık önem arz etmektedir. Nitekim internet ortamında silme yöntemi kapsamında yalnızca kullanıcıların veriye erişimi engellendiğinden yer sağlayıcı sıfatını haiz veri sorumlusunun kişisel veriye erişimi devam etmektedir. Buna karşın; internet ortamının saldırıya açık yapısı nedeniyle kullanıcıların erişimine kapatılan bir veriye, çeşitli yöntemlerle erişilmesi mümkündür. Bu kapsamda internet ortamında işlenen kişisel veriler söz konusu olduğunda; mevzuatta imha öngörülen durumlarda, “silme” yöntemi yerine “yok etme” yönteminin kullanılmasının gerektiği değerlendirilmektedir.

Kişisel verilerin imhası, “silme hakkı (unutulma hakkı)” başlıklı GDPR m. 17’de düzenlenmiştir. Mezkur hükümde kişisel verilerin silinmesi hakkı detaylı bir şekilde ele alınmış olup *Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik* hükümlerinin aksine silme, yok etme, anonimleştirme gibi bir ayrıma gidilmemiştir³⁴².

B. Genel Hukuka Uygunluk Nedenleri

1. Üstün Kamusal Yarar

Kişisel verilerin kişilik hakkı olması nedeniyle hukuka aykırı bir şekilde işlenmesi kişilik haklarına saldırı durumunu oluşturmaktadır³⁴³. TMK m. 24/II hükmünün³⁴⁴ mefhum-u muhalifinden kamu yararının gerektirdiği durumlarda kişilik haklarına yönelik saldırılar hukuka uygun kabul edildiği anlaşılmaktadır. Öte yandan, kamu yararı

³⁴¹ UZUNAL, s. 85; Detaylı bilgi için bkz: SAKA, Rıza/ÇAĞLAYAN, Ramazan/KOCA, Mahmut, Avrupa Birliği Hukuku, İdare Hukuku ve Ceza Hukuku Açısından Kişisel Verilerin imhası, 2. Baskı, Ankara, 2022, s. 46-60.

³⁴² SAKA/ÇAĞLAYAN/KOCA, s. 50; UZUNAL, s. 84.

³⁴³ Detaylı bilgi için bkz: Birinci Bölüm, I, B.

³⁴⁴ TMK m. 24/II: “*Kişilik hakkı zedelenen kimsenin rızası, daha üstün nitelikte özel veya kamusal yarar ya da kanunun verdiği yetkinin kullanılması sebeplerinden biriyle haklı kılınmadıkça, kişilik haklarına yapılan her saldırı hukuka aykırıdır.*”

Anayasa’da muhtelif kısımlarda hak ve özgürlüklerin kısıtlanması noktasında hukuka uygunluk sebebi olarak belirtilmiştir.

Üstün kamu yararı halihazırda kişisel verilerin işlenmesi için genel bir hukuka uygunluk olmasına karşın KVKK’de kamu yararını da kapsayıcı şekilde Kanunun uygulama alanlarına istisnalar getirilmiştir. KVKK m. 28/I’de³⁴⁵ düzenlenen istisnalar kapsamında milli savunma, milli güvenlik, kamu güvenliği, kamu düzeni, ekonomik güvenlik gibi durumlarda yetkili kamu kurumlarınca işlenen kişisel verilerde KVKK hükümleri uygulanmamaktadır. Bu noktada, hukuka uygunluk sebeplerinin yarıştığı değerlendirilmektedir. Kanaatimizce; KVKK’nin özel nitelikte hükümler getirmesi ve daha yeni bir düzenleme olması nedeniyle hukuka uygunluk nedeni olarak “kamu yararı”nın KVKK m. 28/I hükmü bağlamında uygulaması gerekmektedir.

Her devlet için, ülkeye veya vatandaşlara yönelecek tehdidi engellemek varoluşsal bir görevdir. KVKK m. 28/I’de buna uygun bir düzenleme yapılarak kamu düzeni, milli güvenlik gibi durumlarda yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında herhangi bir şart aranmaksızın işlenebileceği öngörülmüştür. Kanaatimizce de; güvenlik ve istihbarat kurumlarının milli güvenliğe yönelik yürüttükleri faaliyetlerde

³⁴⁵ KVKK m. 28/I: “(1) Bu Kanun hükümleri aşağıdaki hâllerde uygulanmaz:

a) Kişisel verilerin, üçüncü kişilere verilmemek ve veri güvenliğine ilişkin yükümlülüklerle uyulmak kaydıyla gerçek kişiler tarafından tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında işlenmesi.

b) Kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi.

c) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi.

ç) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi.

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

yalnızca rıza değil herhangi bir şart aranmaksızın kişisel verilerin işlenmesi hukuka uygun olmaktadır. Bu hukuka uygunluk, çalışmamızın konusu olan internet ortamını ve kamu kurumlarının intranet sistemlerini de kapsamaktadır. Kamu güvenliği gerektirdiği hallerde kişisel verilerin işlenmesi veya analiz edilmek üzere intranet sistemlerine aktarılması da hukuka uygun bir işleme faaliyetidir. Benzer değerlendirmeye İsviçre Federal Mahkemesince de varılmış olup kapalı devre kamera sistemiyle 24 saat kayıt alınmasının terör olaylarının önlenmesi gibi bir kamusal menfaat için gerekli olduğundan hukuka uygunluğuna hükmedilmiştir³⁴⁶.

Kamu yararının gerektirdiği durumlarda kişisel verilerin işlenebileceği GDPR m. 6/1-e’de³⁴⁷ de yer almıştır. Bununla beraber; mezkûr hüküm kamu yararı ibaresinin muğlak olması nedeniyle eleştirilmiştir³⁴⁸. Türk hukuku çerçevesinde mezkûr eleştiriye iştirak edilmemektedir. Nitekim kamu düzeni ve milli güvenliğe yönelik tehditler her geçen gün evrilmekte ve boyut değiştirmektedir. Böyle bir ortamda ne gibi durumların kamu düzeni ve milli güvenliğe tehdit oluşturacağını belirlemek güçtür. Dolayısıyla bu durumun uygulayıcıların takdirine bırakılması, ihtilaf söz konusu olduğunda yargı makamlarınca takdir edilmesi yerinde olacaktır.

NetzDG’de sosyal ağ sağlayıcılara konusu tahdidi olarak sayılmış olan suçları oluşturan içeriklerin paylaşan kullanıcılara ilişkin bilgileri adli makamlarla paylaşma yükümlülüğü getirilmiştir³⁴⁹. Bu durum kamu yararının gerektirdiği durumlarda kişisel verilerin işlenmesine bir başka örnek oluşturmaktadır.

³⁴⁶ ÖZDEMİR, s. 172; TAŞTAN, s. 169.

³⁴⁷ GDPR m. 6/1-e: “*kamu yararına gerçekleştirilen bir görevin yerine getirilmesi veya veri sorumlusuna verilen resmi bir yetkinin kullanılması için işlemenin gerekli olması*”

³⁴⁸ AŞIKOĞLU, s. 83.

³⁴⁹ NetzDG, §2/1/(1).

2. Üstün Özel Yarar

TMK m. 24/II’de kamusal yarara benzer şekilde üstün özel yarar olan durumlarda da kişilik haklarına saldırının hukuka aykırı olmayacağı düzenlenmiştir. Üstün özel yarara ilişkin olarak KVKK m. 5/II-b’de³⁵⁰ düzenlemeye gidilmiştir. Buna göre ilgili kişinin rızasının alınması mümkün değil ve kişisel verilerin işlenmesi hayat ve beden bütünlüğü bakımından zorunlu ise; işleme faaliyeti hukuka uygun olmaktadır³⁵¹. Kanaatimizce de KVKK’de özel ve yeni bir düzenleme olması nedeniyle kişisel verilerin işlenmesi noktasında üstün özel yarar KVKK m. 5/II-b hükmü ile sınırlı olarak ele alınmalıdır.

III.KİŞİSEL VERİLERİN HUKUKA AYKIRI İŞLENMESİ HALİNDE BAŞVURU YOLLARI

A. KVKK Kapsamında Başvuru Yolları

1. Veri Sorumlusuna Başvuru

Kişisel verilerin korunmasını isteme hakkı, Anayasa m. 20/III’te³⁵² düzenlenmesi nedeniyle anayasal bir hak olarak karşımıza çıkmaktadır. Anayasa’da yapılan atıftan

³⁵⁰ Detaylı bilgi için bkz: Üçüncü Bölüm, I, B, 2, b.

³⁵¹ TAŞTAN, s. 168.

³⁵² Anayasa m. 20/III: “Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.”

hareketle KVKK m. 11’de³⁵³ hangi hususlarda veri sorumlusuna başvurulabileceği ve m. 13’te³⁵⁴ başvuru usulü düzenlenmiştir.

Kişisel veri sahibi, veri sorumlusuna başvuru yapmak suretiyle; kişisel verilerin işlenip işlenmediği, işlenme amacı ve amaca uygun kullanılıp kullanılmadığı, verinin kimlere aktarıldığı hakkında bilgi talebinin yanı sıra verilerin düzeltilmesini, yok edilmesini isteyebilir. Talep başvurusunun yazılı veya Kurul’un belirleyeceği şekilde yapılacağına ilişkin düzenlemeye karşın; internet ortamında işlenen kişisel verilere “*usulde paralellik ilkesi*” de göz önünde bulundurularak elektronik ortamda iletilebileceği değerlendirilmektedir.

Veri sorumlusuna başvuru yolu, Kurul’a şikayet öncesi tüketilmesi gereken bir kanun yoludur. İlgili kişi, veri sorumlusuna başvurmadan Kurul’a şikayette

³⁵³ KVKK m. 11: “I) Herkes, veri sorumlusuna başvurarak kendisiyle ilgili;

- a) Kişisel veri işlenip işlenmediğini öğrenme,
 - b) Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,
 - c) Kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,
 - ç) Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,
 - d) Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme,
 - e) 7 nci maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme,
 - f) (d) ve (e) bentleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,
 - g) İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,
 - ğ) Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme,
- haklarına sahiptir.”

³⁵⁴ KVKK m. 13: “I) İlgili kişi, bu Kanunun uygulanmasıyla ilgili taleplerini yazılı olarak veya Kurulun belirleyeceği diğer yöntemlerle veri sorumlusuna iletir.

II) Veri sorumlusu başvuruda yer alan talepleri, talebin niteliğine göre en kısa sürede ve en geç otuz gün içinde ücretsiz olarak sonuçlandırır. Ancak, işlemin ayrıca bir maliyeti gerektirmesi hâlinde, Kurulca belirlenen tarifedeki ücret alınabilir.

III) Veri sorumlusu talebi kabul eder veya gerekçesini açıklayarak reddeder ve cevabını ilgili kişiye yazılı olarak veya elektronik ortamda bildirir. Başvuruda yer alan talebin kabul edilmesi hâlinde veri sorumlusunca gereği yerine getirilir. Başvurunun veri sorumlusunun hatasından kaynaklanması hâlinde alınan ücret ilgiliye iade edilir.”

bulunmamaktadır. Buna karşın; bu durum ilgili kişinin genel hükümlere göre dava açma hakkını engellememektedir³⁵⁵.

Veri sorumlusuna başvuru, GDPR m. 12 vd. hükümlerinde düzenlenmiştir. Buna göre veri sorumlusu ilgili kişinin başvurusuna bir ay içerisinde cevap vermekle mükellef kılınmıştır³⁵⁶.

2. Kurula Şikayet

KVKK m. 14'te³⁵⁷ kişisel veri sahibinin, veri sorumlusuna gerçekleştirdiği başvuru ile öngördüğü neticeyi alamaması halinde Kurul'a veri sorumlusunun cevabından itibaren 30 gün veya her hal ve karda başvuru tarihinden itibaren 60 gün içinde başvurabileceği düzenlenmiştir.

Veri sorumlusuna başvuru, Kurul'a şikayet öncesi tüketilmesi gereken bir yol iken; Kurul'a şikayet ihtiyari bir başvuru yoludur³⁵⁸. İlgili kişi, KVKK m. 14/III uyarınca genel mahkemelere başvurarak zararının tazmin edilmesini talep edebilmektedir. Öte yandan; tazminat taleplerinin mahkeme nezdinde gündeme getirilmesi gerekmekte olup Kurul'un veri sorumlusu aleyhine, ilgili kişi lehine tazminata hükmetme yetkisi bulunmamaktadır.

³⁵⁵ YILMAZ, Tüze, s. 117; ÖZKAN, s. 195.

³⁵⁶ Detaylı bilgi için bkz: DEVELİOĞLU, s. 119-120.

³⁵⁷ KVKK m. 14: “I) Başvurunun reddedilmesi, verilen cevabın yetersiz bulunması veya süresinde başvuruya cevap verilmemesi hâllerinde; ilgili kişi, veri sorumlusunun cevabını öğrendiği tarihten itibaren otuz ve her hâlde başvuru tarihinden itibaren altmış gün içinde Kurula şikâyetle bulunabilir.

II) 13 üncü madde uyarınca başvuru yolu tüketilmeden şikâyet yoluna başvurulamaz.

III) Kişilik hakları ihlal edilenlerin, genel hükümlere göre tazminat hakkı saklıdır.”

³⁵⁸ YILMAZ, Tüze, s. 119; ÖZKAN, s. 198.

B. Genel Hükümler Çerçevesinde Başvuru Yolları

1. Kişilik Hakkını Koruyucu Davalar

Kişisel verilerin hukuka aykırı işlendiği durumlarda genel hükümlere göre açılacak davaları temelde iki kategoriye ayırmak mümkündür. İlk kategoriye TMK m. 24³⁵⁹ ve m. 25³⁶⁰ hükümlerinde düzenlenen koruyucu davalar iken ikinci kategori TBK’de düzenlenen tazminata ilişkin hükümlerdir.

Kişisel veriler hukuka aykırı işlendiğinde, ilgili kişi veri sorumlusunun kusuru aranmaksızın mahkemeye başvurarak “önleme”, “son verme” veya “tespit” davalarından birini açabilir³⁶¹. İnternet ortamının dinamik yapısı üç dava arasındaki farklı noktaları zayıflatmaktadır. Örneğin; kullanıcıların açık rızasına başvurmaksızın kişisel verilerin işlendiği bir internet sitesine giriş yapmadan önce önleme davası açılacakken; yalnızca tek bir tıklama ile mezkûr internet sitesine giriş yapılması, davanın mahiyetinin “son verme” olarak değişmesine sebep olacaktır. TMK m. 25/V’e göre kişisel verisi hukuka aykırı işlenen kişi, önleme, son verme veya tespit davasını; veri sorumlusunun

³⁵⁹ TMK m. 24: “I)Hukuka aykırı olarak kişilik hakkına saldırılan kimse, hâkimden, saldırıda bulunanlara karşı korunmasını isteyebilir.

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

³⁶⁰ TMK m. 25: “I)Davacı, hâkimden saldırı tehlikesinin önlenmesini, sürmekte olan saldırıya son verilmesini, sona ermiş olsa bile etkileri devam eden saldırının hukuka aykırılığının tespitini isteyebilir.

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

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

IV)Manevî tazminat istemi, karşı tarafça kabul edilmiş olmadıkça devredilemez; miras bırakan tarafından ileri sürülmüş olmadıkça mirasçılara geçmez.

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

³⁶¹ OĞUZMAN/SELİÇİ/OKTAY ÖZDEMİR, s. 219; GÜNAY, Buket, Kişiliğin Korunması Kapsamında Kişisel Verilerin Hukuka Aykırı Kullanılması Nedeniyle Hukuki Sorumluluk, 1. Baskı, Ankara, 2023, s. 190; ÖZDEMİR, 187-198.

yerleşim yerinde açabileceği gibi kendi yerleşim yerinde de açabilir. Öte yandan; mezkûr hüküm kesin yetki kuralı oluşturmadığından³⁶² ilgili kişi HMK kapsamında genel yetki kurallarına göre de dava açabilmektedir.

2. Tazminat Davası

a. Genel Olarak

KVKK m. 14/III’te kişisel verilerin işlenmesi sürecinde kişilik hakkı ihlal edilenlerin genel hükümlere göre tazminat; KVKK m. 11/I-ğ’de ise zararın giderilmesini talep etme hakkı düzenlenmiştir. Kişisel verilerin, ilgili kişiler için kişilik hakkı oluşturduğuna ilişkin değerlendirmemiz³⁶³ ve mezkur kanun hükmü göz önüne alındığında genel hükümler ifadesinden, TMK ve TMK’den atıfla TBK’de yer alan kişilik haklarına karşı koruma yöntemlerinin kastedildiği anlaşılmaktadır.

Kişisel verilerin hukuka aykırı işlenmesinden ötürü genel hükümlere göre öne sürülecek maddi tazminat talepleri için TBK m. 49³⁶⁴; manevi tazminat talepleri için TBK m. 58³⁶⁵ çerçevesinde değerlendirme yapmak gerekmektedir. KVKK’de genel hükümlere göre tazminat talep edilebileceğine ilişkin hüküm yalnızca saptamada bulunmakta olup TBK’de yer alan düzenlemelere ek olarak yeni bir objektif sorumluluk

³⁶² ÖZKAN, s. 240.

³⁶³ bknz: Birinci Bölüm, I, B, 4.

³⁶⁴ TBK m. 49: “I) Kusurlu ve hukuka aykırı bir fiille başkasına zarar veren, bu zararı gidermekle yükümlüdür.

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

³⁶⁵ TBK m. 58: “Kişilik hakkının zedelenmesinden zarar gören, uğradığı manevi zarara karşılık manevi tazminat adı altında bir miktar para ödenmesini isteyebilir.

Hâkim, bu tazminatın ödenmesi yerine, diğer bir giderim biçimi kararlaştırabilir veya bu tazminata ekleyebilir; özellikle saldırıyı kınayan bir karar verebilir ve bu kararın yayımlanmasına hükmedebilir.”

hali oluşturmamaktadır³⁶⁶. Dolayısıyla kişisel verilerin hukuka aykırı işlenmesinden doğan sorumluluk da bir kusur sorumluluğudur.

Genel hükümlere göre maddi tazminat talep edilmesi için “zarar”, “kusur”, “hukuka aykırı fiil” ve “illiyet bağı” olmak üzere dört şartın sağlanması gerekmektedir³⁶⁷. Dolayısıyla internet ortamında kişisel verilerin hukuka aykırı işlenmesi nedeniyle maddi tazminat talebinde bulunabilmek için öncelikle hukuka aykırı işleme fiili mevcut olmalıdır. Bu işleme fiili nedeniyle ilgili kişi zarara uğramalı ve veri sorumlusu konumundaki internet aktörünün kusuru bulunmalıdır. Kişilik hakkını koruyucu davaların aksine tazminat davalarında zarar şartı aranması temel farklılığı oluşturmaktadır.

Kişisel verilerin hukuka aykırı işlenmesinde hangi durumlarda zarar doğduğunu tespit edebilmek adına evvelce zararın tanımı yapılmalıdır. Zarar geniş anlamda; bir kişinin iradesi dışında maddi veya manevi varlığında meydana gelen eksilme olarak tanımlanırken³⁶⁸ dar anlamda manevi zararı kapsamayacak şekilde kişinin malvarlığında zararı oluşturan olaydan önceki ve sonraki değerler arasındaki fark³⁶⁹ olarak açıklanmıştır. Türk hukukunda TBK m. 58 ile manevi zarar ifadesine yer verilmiş olduğundan; kanaatimizce kişisel verilerin hukuka aykırı işlenmesinde “zarar” kavramının geniş anlamda tanımını esas alarak malvarlığında eksilme olan durumlarda “maddi zarar”, malvarlığında eksilme oluşturmayan durumlarda “manevi zarar” çerçevesinde inceleme yapılması isabetli görülmektedir.

³⁶⁶ GÜNAY, s. 190; ÖZDEMİR, s. 208.

³⁶⁷ OĞUZMAN, M. Kemal/ÖZ, M. Turgut, Borçlar Hukuku Genel Hükümler Cilt 2, 17. Baskı, İstanbul, 2022, s. 13; AYAN, s. 250; KAYIHAN/ÜNLÜTEPE, s. 226; ERDOĞAN, İhsan, Borçlar Hukuku Genel Hükümler, 4. Baskı, Ankara, 2019, s. 120.

³⁶⁸ ORAL, Tuğçe, Tüzel Kişilerin Manevi Zararının Tazmini, 1. Baskı, Ankara, 2018, s. 28; TANDOĞAN, Haluk, Türk Mes’uliyet Hukuku, 1. Baskı, İstanbul, 2010, s. 63.

³⁶⁹ ERDOĞAN, s. 130; KAYIHAN/ÜNLÜTEPE, s. 260; ORAL, s. 29.

b. Maddi Tazminat Talebi

Kişisel verilerin hukuka aykırı işlenmesi neticesinde, ilgili kişinin uğradığı maddi zarara karşılık maddi tazminat davası açılabilir. Bu dava ile amaçlanan fark teorisi kapsamında ilgili kişinin malvarlığının hukuka aykırı işleme faaliyeti hiç olmasaydı olacağı duruma getirilmesidir³⁷⁰.

Maddi tazminatın talep edilebilmesi için maddi zararın malvarlığına yönelik saldırıdan ileri gelmesi gerekmemekte olup kişinin bedensel bütünlüğü, şerefi, haysiyeti gibi şahıs varlığına yönelik eylemler neticesinde de maddi zarar meydana gelebilir³⁷¹. Bu durum çalışmamız kapsamında önem arz etmektedir. Zira internet ortamının kendine özgü yapısı, kişisel verilerin hukuka aykırı işlenmesi suretiyle hem malvarlığı hem de şahıs varlığını etkileyebilir. Söz gelimi; banka tarafından bir kişinin kredi notunun hatalı bir şekilde kayıt altına alınması durumu tipik bir kişisel verilerin hukuka aykırı işlenmesi durumunu oluşturmaktadır³⁷². Bu durumda malvarlığına yönelik bir eylem olmamasına karşın ilgili şahıs kötü kredi notu nedeniyle kredi alamayarak maddi zararlarla karşılaşmaktadır. Başka bir durumda İnternet ortamında bir kişinin kredi kartı bilgilerinin üçüncü kişilerce hukuka aykırı şekilde ele geçirilmesi ve harcama yapılması ise doğrudan malvarlığına yönelmiş bir eylemden kaynaklanan maddi zararı oluşturur.

Maddi tazminat talebinde bulunabilmek için kusur şart olmakla beraber; kusur kast veya ihmal şeklinde vukuu bulabilir³⁷³. KVKK'de belirlenen kişisel verilerin işlenmesine ilişkin açık rıza veya diğer durumların olmadığı hukuka aykırı bir işleme

³⁷⁰ OĞUZMAN/ÖZ, s. 42-43; TAŞTAN, s. 181; ÖZDEMİR, s. 207-208; BASKIN, s. 135.

³⁷¹ OĞUZMAN/ÖZ, s. 44; DOĞAN, Murat/ATAMULU, İsmail/ŞAHAN, Gökhan, Borçlar Hukuku Genel Hükümler, 2. Baskı, Ankara, 2021, s. 136; ERDOĞAN, s. 131.

³⁷² TAŞTAN, s. 181.

³⁷³ OĞUZMAN/ÖZ, s. 59-60; EREN, s. 656; KILIÇOĞLU, s. 824; ERDOĞAN, s. 125; ÖZDEMİR, s. 123.

faaliyetinde kanaatimizce veri sorumlusu veya veri işleyen en azından ihmalinin olmadığı bir somut olayın vaki olması mümkün değildir.

Maddi tazminat talebinde kusur, kural olarak davacı tarafından ispat edilmelidir³⁷⁴. Bununla birlikte TBK. m. 112'ye göre³⁷⁵ zarar gören ve zarar veren arasında sözleşme ilişkisi bulunduğu takdirde ispat yükü tersine çevrilmektedir. Tarafların arasında sözleşme olan durumlarda kişisel verilerin işlenmesi hukuka aykırı işlenmesi durumunda, veri sorumlusu veya veri işleyen kusuru olmadığını veya işleme faaliyetinin hukuka aykırı olmadığını ispatla mükelleftir. Örneğin; internet ortamında akdedilen bir satış sözleşmesinde hukuka aykırı kişisel verilerin işlenmesi durumunda malvarlığı zararı olursa, veri sorumlusu kusursuzluğunu ispat etmelidir. Bunun yanında; ilgili kişi ile akdi bir ilişkide olmayan ve satışın yapıldığı siteye *hosting* hizmeti veren yer sağlayıcıya yöneltilecek bir davada, ilgili kişi, yer sağlayıcının kusurlu olduğunu ispatlamalıdır.

Maddi tazminat belirlenirken TBK m. 51³⁷⁶ uyarınca hâkime takdir yetkisi tanınmıştır. Hafif ihmal olan durumlarda tazminatın indirilebileceği hükmedilmiştir. Bununla beraber; internet ortamında kişisel verilerin hukuka aykırı işlendiği durumlarda, ilgili kişinin veri sorumlusu karşısında güçsüz pozisyonu göz önüne alındığında TBK m. 51'in uygulanmaması gerektiği değerlendirilmektedir³⁷⁷.

³⁷⁴ EREN, s. 831; KILIÇOĞLU, s. 824; DOĞAN/ATAMULU/ŞAHAN, s. 136; ERDOĞAN, s. 129.

³⁷⁵ TBK m. 112: “*Borç hiç veya gereği gibi ifa edilmezse borçlu, kendisine hiçbir kusurun yüklenemeyeceğini ispat etmedikçe, alacaklının bundan doğan zararını gidermekle yükümlüdür.*”

³⁷⁶ TBK m. 51: “*I) Hâkim, tazminatın kapsamını ve ödenme biçimini, durumun gereğini ve özellikle kusurun ağırlığını göz önüne alarak belirler.*

II) Tazminatın irat biçiminde ödenmesine hükmedilirse, borçlu güvence göstermekle yükümlüdür.”

³⁷⁷ UZUNAL, s. 165.

c. Manevi Tazminat Talebi

Hukukumuzda manevi tazminat, TBK'nin 56 ve 58. maddelerinde düzenlenmiştir. TBK m. 56'da ölüm ve vücut bütünlüğünün ihlalden doğan manevi tazminat, m. 58'de ise, kişilik hakkının ihlali neticesinde hak kazanılabilecek manevi tazminat hüküm altına alınmıştır. Ölüm ve vücut bütünlüğünün ihlali halinde manevi tazminatı düzenleyen TBK m. 56'nın konumuz bağlamında uygulama alanı bulmayacağı değerlendirilmektedir.

Manevi tazminata hükmedilebilmesinin ilk şartı, manevi zararın bulunmasıdır. Manevi zarar hususunda doktrinde üç farklı görüş bulunmaktadır. Bu görüşlerde subjektif görüşe göre, manevi zarar, kişilik hakkının ihlal edilmesi sonucu kişinin duyduğu elem, acı, keder, yaşama sevinci kaybı ve ıstıraptır³⁷⁸. Bizim de katıldığımız ikinci görüş olan objektif görüşe göre, manevi zarar kişinin kişilik değerlerinde meydana gelen objektif eksilmedir³⁷⁹. Son olarak, karma görüşe göre ise, manevi zararın doğması için kişilik değerlerinde objektif azalmanın yanında kişinin acı çekmesi gerekmektedir³⁸⁰.

İnternetin geniş kitlelere ulaşma vasfı nedeniyle kişisel verilerin hukuka aykırı işlenmesi sonucunda ilgili kişinin kişilik hakkını unsurları olan adı, resmi, fotoğrafı üzerindeki hakkı, gizli ve özel hayatı üzerindeki hakkı ya da şeref haysiyet ve saygınlığı ihlal edilerek manevi zararının doğabileceği açıktır.

Manevi tazminat talebinin, maddi tazminat talebinden temel farklarından biri kural olarak devredilememesi ve mirasçılara geçmemesidir³⁸¹. Bu durum internet ortamında işlenen kişisel veriler bağlamında önem arz etmektedir. Nitekim kişisel veri

³⁷⁸ OĞUZMAN/ÖZ, s. 279; EREN, s. 608; GENÇ ARIDEMİR, Arzu, Sözleşmeye Aykırılıktan Doğan Manevi Tazminat, 1. Baskı, İstanbul, 2008, s. 184; ORAL, s. 35.

³⁷⁹ EREN, s. 610; AYAN, s. 279-280; NARTER, Sami, Uygulamada Manevi Tazminat, 1. Baskı, Ankara, 2022, s. 7-9; ORAL, s. 36-37; DOĞAN/ATAMULU/ŞAHAN, s. 240.

³⁸⁰ EREN, s. 614; ORAL, s. 39.

³⁸¹ OĞUZMAN/ÖZ, s. 285; ERDOĞAN, s. 143; DOĞAN/ATAMULU/ŞAHAN, s. 241; BASKIN, s. 137.

sahibi kiři öldükten sonra dahi kendisine ait kiřisel veriler hukuka aykırı řekilde iřlenmeye devam edebilir. Hatta bu veriler hukuka aykırı řekilde herhangi bir internet sitesinde aleni bir řekilde yayımlanabilir. Bu durumlarda dahi TMK m. 25/IV³⁸² gereęi mirasçılar tarafından manevi tazminat davası açabilmesi için kiřisel veri sahibinin ölmeden önce talebini öne sürmesi gerekmektedir. Bununla birlikte; kanımızca manevi tazminat davası açma hakkının bulunmaması, mirasçıların kiřilik hakkını koruyucu davalara başvurmasını engellemeyecektir.

Manevi zarar ve tazminat miktarı konusunda kanunen ortaya konulmuş somut ölçütler bulunmadığından bu tür tazminatın para cinsinden belirlenmesi maddi zarara nazaran güçtür³⁸³. Manevi zararın bir rayiç değeri olmadığından, kiřilik değerlerinde, başka bir ifadeyle, para ile ölçülemeyen bir değerde eksilme bulunmasına karşın, bu eksilmenin para ile giderilecek olması düşüncesi, hâkimleri, manevi tazminatın sebepsiz zenginleřtirmeye vücut vereceęi düşüncesine sokmakta ve bu sebeple hükmedilen manevi tazminat miktarları çoęunlukla düşük olmaktadır. Manevi tazminat miktarının nasıl belirlenmesi gerektięi hususunda doktrinde farklı teoriler olmakla birlikte³⁸⁴ bizim de katıldığımız iki aşamalı yöntemle göre, manevi tazminat miktarının belirlenmesi için öncelikle objektif olarak en yüksek düzeyden ve herkes için eşit olmak üzere manevi zarar belirlenmeli, ardından somut olayın özelliklerine göre bu tazminattan indirim yapılmalıdır³⁸⁵. Bizim de katıldığımız görüşe göre, manevi tazminattan indirim yapılmasını gerektirecek sebepler, mağduru dünya üzerinde olumlu ya da olumsuz olarak

³⁸² TMK m. 25/IV: “Manevî tazminat istemi, karşı tarafça kabul edilmiş olmadıkça devredilemez; miras bırakan tarafından ileri sürülmüş olmadıkça mirasçılara geçmez.”

³⁸³ BASKIN, s. 139; ÖZDEMİR, s. 222.

³⁸⁴ Bu teoriler hk. ayrıntılı bilgi için bkzn. ORAL, s. 165 dn. 58.

³⁸⁵ ORAL, s. 169 vd.

tanıyan kiři sayısı, zarar verenin kusuru, zarar görenin kusuru ve zarar verenin iktisadi durumudur³⁸⁶.



³⁸⁶ ORAL, s. 172 vd.

SONUÇ

Ülke sınırlarının her geçen belirsizleştiği ve küreselleşmenin kendisini daha fazla hissettirdiği günümüz dünyasında internet başta olmak üzere iletişim teknolojilerinin beraberinde gelişmiş veri işleme yöntemleri hayatımıza girmiştir. Tüm dünyaya –belki gelecekte evrene- kolaylıkla erişebilmeyi mümkün kılan internet; insan ilişkilerini, iş hayatını, kamu-birey ilişkisini daha sarmallı ve kompleks hale getirmiştir. Çok da uzak olmayan geçmiş dönemde ülke içerisinde bir paylaşım dahi günler süren yolculuklar gerektirirken gelinen noktada dünyanın herhangi bir noktasıyla herhangi bir veri paylaşımı saniye dahi sürmemektedir. Hatta bu durum, yalnızca belirli iki kişi arasında cereyan etmemekte; internet ortamı milyonların veri paylaşabildiği dijital bir forum haline gelmektedir. Yapılan her işlemin, girilen her verinin, hatta basit bir tıklamanın dahi dijital iz bıraktığı internet ortamından istifade eden şahısların verileri, başta küresel çapta faaliyet gösteren şirketler olmak üzere birçok farklı aktör tarafından ticari amaçla işlenebilmektedir. Öte yandan kamu gücünü haiz otoriteler de kamu hizmetlerinin devamı veya milli güvenlik gibi kaygılarla bu yöntemlere başvurmaktadır. Bu kapsamda; kullanıcı ile veri işleyen şahıslar arasında güç ve imkân dengesizliğinin yoğun olduğu internet ortamında kişisel verilerin işlenmesine ilişkin temel hukuki sorunların ortaya çıkarılması ve değerlendirilmesi son derece önemlidir.

Zaman içerisinde şahıslar arasında iletişimin çok katmanlı bir hal alması veri üretiminin çarpan etkisiyle artış göstermesine sebep olmuştur. İnsanlara ait her neviden verinin işlenmeye açık hale gelmesi, küresel çapta hukuk dünyasını çare bulmaya sevk etmiştir. Kişisel verilerin korunması ihtiyacı 19. yüzyılda ortaya çıkmış ve günümüze kadar çeşitli düzenlemelere konu olmuştur. Dinamik, anonim ve erişime açık yapısı ile internet teknolojisi, kişisel verilerin işlenmesi ve korunması noktasında milat olmuştur. Öyle ki internet; kullanıcılar için kullanımı basit, veri sorumlusu sıfatını haiz internet

aktörleri için kompleks ve sorumluluklardan kaçınması kolay bir ortam olmuştur. Bu durum çalışmanın konusunun seçilmesi noktasında motivasyon oluşturmuştur.

Kişisel veriler kavramı, yalnızca gerçek kişileri kapsayıcı bir ifade olmasının yanında internet ortamında tüzel kişilerin maddi açıdan kullanıcı sıfatıyla bulunması zaten mümkün değildir. Kişisel verilerin, hukuki niteliği bakımından kişilik hakkı oluşturduğu kanaatine varılmış olup çalışmanın devamında hukuki sorumluluk bu çerçevede ele alınmıştır. Dolayısıyla kişilik hakkının gereği olarak, ilgili kişinin ölümünün gerçekleşmesinden sonraki dönemde dahi kişisel verilerin korunması gerektiği kanısına varılmıştır.

Veri toplama sistemlerinin sofistike bir hal alması, iki yönlü (*download* ve *upload*) veri işleme sistemlerinin hızının ve trafiğinin yoğunlaşması, kullanıcı sayısındaki artış internet ortamındaki veri miktarını dramatik bir şekilde çoğaltmıştır. Bu durum “*big data*” adı verilen çok büyük boyuttaki yapılandırılmamış ve anlamlandıramayan veri kümelerini oluşturmuştur. Geleneksel yöntemlerle analiz edilmesi mümkün olmayan bu veri kümelerinin içinde tanımlamayacak şekilde yer alan verilerden sorumluluk doğması hayatın olağan akışına uygun düşmeyecektir. Öte yandan; dağınık ve tanımlanamayan veri setlerinin, veri sorumlusunun bilgisi dışında veri analiz uzmanlarınca işlenerek belirli bir kişiyle ilişkilendirilmesi halinde de veri sorumlusunun sorumluluğu doğmayacaktır. Meğerki; veri sorumlusu dağınık haldeki verinin üçüncü kişilere geçmemesi için gerekli önlemleri almış olsun.

Çalışmamızın konusunu, bilişim cihazlarının sınırsız bir şekilde birbirine bağlayan en geniş ağ topluluğu internet ile sınırlı tutulsa da belirli bir kitleyi birbirine bağlayan intranet ve extranet ağlarında da kişisel verilerin korunması gerekmektedir. Özellikle intranet sisteminin kullanımının yaygın olduğu kamu kurumlarının çok çeşitli kişisel verilere erişebilmesi bu tarz sistemleri önemli kılmaktadır.

Başta 5651 sayılı Kanun olmak üzere mevzuatımızda düzenlenmiş olan “yer sağlayıcı”, “içerik sağlayıcı”, “erişim sağlayıcı”, “sosyal ağ sağlayıcı” gibi internet aktörlerinin tanımlamalarının ve rollerinin düzenlemeler bazında değişiklik arz ettiği görülmüştür. İnternetin dinamik yapısı nedeniyle anlaşılabilir olan bu duruma karşılık çalışmamızda bahsi geçen internet aktörleri durumdan duruma değişebilen, belirli durumda yetki ve sorumluluğu belirlemeye yarayan ölçütler olarak ele alınmıştır. Nitekim; internet ortamında aynı kişi, hem verileri kendi uhdesinde tutup hem de içerik ürettiği durumlarda hem içerik hem yer sağlayıcı sıfatını haiz olmaktadır. Bunun yanında, çalışmada tanımlanan “internet sitesi işletmecisi” kavramı, objektif bir boyut içermekte ve somut olayın şartlarına göre 5651 sayılı Kanunda yer alan aktörlerden biri olarak sorumlu tutulabilmektedir. Uygulamada sıklıkla erişim sağlayıcı ile eş anlamlı kabul edilen “internet servis sağlayıcısı” kavramının kullanıcıların internetten yararlanmasını sağlayan aktör olması nedeniyle, mezkûr ifade “yer sağlayıcı” ve “erişim sağlayıcı”lar için çatı kavram olarak kullanılmıştır.

Bir şahıs, kendi işlettiği internet sitesinin verilerini kendi uhdesinde barındırarak “yer sağlayıcı” sıfatını haiz olabileceği gibi üçüncü kişilere de barındırma (*hosting*) hizmeti verebilir. Üçüncü kişilere hosting hizmeti verildiği durumlarda yer sağlayıcı, veri sorumlusu sıfatını haiz değildir; dolayısıyla kendisine haber verilene kadar hukuka aykırı işlenen veriden sorumluluğu bulunmamaktadır.

Kişisel verilerin işlenmesine ilişkin mevzuatımızdaki temel düzenleme KVKK’nin kapsamına, otomatik yollarla veya veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan işleme faaliyetleri girmektedir. İnternet ortamında işlenen kişisel verilerin, bilişim teknolojilerinden istifade edilmesi nedeniyle otomatik işleme olduğu, bu nedenle her hâl ve kârda KVKK kapsamına girdiği değerlendirilmiştir.

Kişisel verilerin işlenmesine ilişkin temel ilkelerden olan “doğruluk ve gerektiğinde güncel olma” internet ortamının dinamik yapısı nedeniyle veri sorumluları

gerekli veriler işlenebilmektedir. Uygulamada sıklıkla karşılaşılan internet ortamında gerçekleşen tüketici satışlarında alıcıya ait TCKN'nin talep edilmesi hususu kişisel verilerin hukuka aykırı bir şekilde işlenmesine yaygın bir örnek oluşturmaktadır.

Veri sorumlusunun meşru menfaatine dayanarak yürüteceği kişisel verileri işleme faaliyetinde menfaat dengesinin gözetilmesi gerekmektedir. Nitekim internet ortamının eş zamanlı çok kullanıcı yapısı, veri sorumlusu ve ilgili kişi dışında üçüncü kişilerin menfaatinin de göz önünde bulundurulması durumunu ortaya çıkarmaktadır. İnternet sitesinin faaliyeti için zorunlu verilerin işlenmesinde üçüncü kişilerin de menfaati varken veri sorumlusunun reklam geliri için işleyeceği verinin ilgili kişi göz önüne alındığında meşru menfaat olmadığı değerlendirilmiştir.

Kişisel verilerin aktarımı için ilgili kişiden rıza alınması gerekmektedir. Bu noktada GDPR ve KVKK'de farklı düzenlemelere gidilmiştir. GDPR'da yalnızca üçüncü kişiye aktarım için rıza alınması gerektiği yer alırken KVKK'de bu yönde bir ayrım bulunmamaktadır. Kanun taslağında yer alan “üçüncü kişi” ibaresinin nihai metinden çıkarılmasıyla tarihi kanun koyucunun irade ortaya koyduğu değerlendirilmiş olup KVKK kapsamında veri sorumlusunun kendine ait veri merkezleri arasında gerçekleştireceği aktarımlarda rıza alması gerektiği değerlendirilmektedir.

Aydınlatma yükümlülüğü, irade fesadına uğramamış bir açık rızaya ulaşabilmek bağlamında önemlidir. Özellikle internet ortamının hızlı akan yapısı nedeniyle kullanıcıların, arzulanan içeriğe ulaşabilmek adına bilgi sahibi olmadan onay vermesi sıklıkla karşılaşılan bir durumdur. Mezkûr alışkanlığın veri sorumlularının aydınlatma yükümlülüğüne halel getirmemesini teminen internet ortamında rıza metninin sonuna kadar okunmasının ardından onay butonunun aktif edilmesi gibi düzenlemelerin isabetli olacağı mütalaa edilmektedir.

Rıza veya bir başka sebebe dayanarak işlenen kişisel verilerin, işlemeye temel oluşturan hukuki sebebin ortadan kalkması halinde; silinmesi, yok edilmesi veya anonim hale getirilmesi gerekmektedir. Silme ile yok etme gramatiksel olarak yakın anlamlı görünse de internet ortamında ciddi farklılık göstermektedir. Nitekim silme eylemi, verinin erişilemez hale getirilmesi iken; yok etme verinin tamamen imha edilmesidir. İnternet ortamının çok kullanıcı ve saldırıya açık yapısı; erişilmez hale getirilen verinin, çeşitli üçüncü kişi saldırılarıyla yeniden erişilebilir hale getirilme olasılığını beraberinde getirmektedir. Bu kapsamda internet ortamında, veri sorumlusunun yok etme metoduna başvurması gerektiği değerlendirilmektedir.

Üstün kamusal yarar, TMK gereğince kişilik haklarına yönelik saldırılar için genel bir hukuka uygunluk sebebidir. Bu durum KVKK’de da tekrarlanarak kamu düzeni, milli güvenlik gibi durumlarda KVKK’nin uygulanmayacağı hüküm altına alınmıştır. TMK’ye nazaran daha yeni ve daha özel bir düzenleme getiren KVKK’de isabetli bir düzenlemede bulunduğu değerlendirilmektedir. Zira küreselleşen dünya, her geçen gün evrilen yeni tehdit alanlarını beraberinde getirmektedir. Özellikle terör örgütlerinin geliştirdiği yeni teknikler, güvenlik bürokrasisini de proaktif bir yaklaşımla sorunu ele alma mecburiyetine itmektedir. Güvenlik bürokrasisinin idari kısıtlamalarla hareket alanını daraltmanın, olası bir terör saldırısında en temel insani değer olan yaşam hakkına saldırının önünü açabileceği göz önünde bulundurularak güvenlik ve istihbarata ilişkin faaliyetlerin kişisel verilerin korunması mevzuatından mücerret tutulması isabetlidir. Faaliyetlerin gizliliğini de esas alarak güvenlik ve istihbarat kurumlarının kendi içinde geliştirdikleri iç denetim mekanizmalarıyla kişisel verilerin yalnızca kamu yararı amacıyla işlenmesini gözetmeleri, birey ve kamu arasındaki menfaat dengesini sağlamak adına önemlidir.

İnsanlığın bilgiye ulaşımı açısından vazgeçilmez bir ortam olan internette varlığı bulunan büyük şirketlerin, kişisel verilerin işlenmesi ile ciddi ticari kazanç elde ettikleri

yadsınamaz bir gerçektir. Öte yandan son kullanıcıların, özellikle büyük piyasa aktörlerine karşı internet ortamında savunmasız kalması da önemli bir sorundur. Kişisel verilerin korunması kapsamında bireylerin kişilik haklarının korunması ve piyasa aktörlerinin ticari menfaatleri hassas bir denge kurulması önem arz etmektedir. Çalışmanın temelinde, hukuki enstrümanlar bu perspektifte yorumlanmış olup internetin dinamik yapısı göz önüne alınarak soyut değerlendirmelerin, gelişmesi muhtemel yeni somut hukuki sorunlara cevap verebilmesi amaçlanmıştır.



KAYNAKÇA

- AKINCI, Ayşe Nur**, Büyük Veri Uygulamalarında Kişisel Veri Mahremiyeti, T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı, Yayın No:001, Uzmanlık Tezi, Ankara, 2019.
- AKKURT, Sami Sinan**, Sosyal Medyada Gerçekleşen İhlaller Karşısında Kişilik Hakkının Korunması, 1. Baskı, Ankara, 2020.
- AKSOY, Hüseyin Can**, Kişisel Verilerin Korunması, Yüksek Lisans Tezi, Ankara, 2008.
- ANTALYA, Osman Gökhan/TOPUZ, Murat**, Medeni Hukuk Cilt:I, 4. Baskı, Ankara, 2021.
- AŞIKOĞLU, Şehriban İpek**, “*Veri Sorumlularının Aydınlatma Yükümlülüğü – Avrupa Birliği ve Türk Hukukunda-*“, Kişisel Verileri Koruma Dergisi, C. 1. S. 2, 2019, s. 41-65.
- AŞIKOĞLU, Şehriban İpek**, Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri, Yüksek Lisans Tezi, İstanbul, 2018.
- ATAY, Ender Ethem**, Hukuk Başlangıcı, 8. Baskı, Ankara, 2020.
- AVŞAR, Zakir/ÖNGÖREN Gürsel**, Bilişim Hukuku, Türkiye Bankalar Birliği, 1. Baskı, İstanbul, 2010.
- AYAN Mehmet/AYAN Nurşen** Kişiler Hukuku, 8. Baskı, Ankara, 2016.
- AYAN Mehmet/AYAN Nurşen** Medeni Hukuka Giriş, 12. Baskı, Ankara, 2016. (Medeni).
- AYAN, Mehmet**, Borçlar Hukuku Genel Hükümler, 11. Baskı, Ankara, 2016.
- AYBAY, Rona**, Açıklamalı İnsan Hakları Evrensel Beyannamesi, Türkiye Barolar Birliği Yayınları, 2006.
- BAKIREL, Nur Buğçe**, Veri Sorumlusu ve Veri İşleyen Arasındaki Sorumluluk Paylaşımı Avrupa Birliği Genel Veri Koruma Tüzüğü ve Kişisel Verilerin Korunması Kanunu Çerçevesinde Değerlendirilmesi, 1. Baskı, Ankara, 2021.
- BAROCAS, Solon/NISSENBAUM, Helen**, “*Computing Ethics Big Data’s End Run Around Procedural Privacy Protections*”, Communications of the ACM, C. 57, S. 11, 2014, s. 31-33

- BASKIN, Onur**, Türk Hukuku Bakımından Kişilik Hakkı Kapsamında Kişisel Verilerin Korunması, 1. Baskı, Ankara, 2021.
- BAŞALP, Nilgün**, Avrupa Birliği, Veri Koruması Genel Regülasyonunun Temel Yenilikleri, MÜHFD, C. 21, S. 1, 2015, s. 77-106.
- BAŞPINAR, Veysel/KOCABEY, Doğan**, İnternette Fikri Hakların Korunması, 1. Baskı, Ankara, 2007.
- BATU, Betül**, 6698 Sayılı Kişisel Verilerin Korunması Kanunu Kapsamında Kişisel Verilerin İşlenmesi ve Açık Rıza, Yüksek Lisans Tezi, Konya, 2022.
- BERGKAMP, Lucas**, “*EU Data Protection Policy: The Privacy Fallacy: Adverse Effects of Europe’s Data Protection Policy in an Information-Driven Economy*”, Computer Law & Security Review, C. 18, S. 1, 2002, s. 31-47.
- BİLGE, Necip**, Hukuk Başlangıcı, 35. Baskı, Ankara, 2017.
- BOOTH, Sharon/JENKINS, Richard/MOXON, David/SEMMENS, Natasha/SPENCER, Christopher/TAYLOR, Mark/TOWNEND, David**, “*What are Personal Data? – A Study Conducted for the UK Information Commissioner*”, The University of Sheffield, 2004.
- BUDAK, Muhammed Alparslan/MALKOÇ, Seda**, Kişisel Verilerin Korunması Kanunu'na Aykırı Davranılmasında Hukuki Sorumluluk, 1. Baskı, Ankara, 2021.
- BURRI, Mira/SCHÄR**, “*Rahel, The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for Data-Driven Economy*”, Journal of Information Policy, C. 6, 2016, s. 479-511.
- BYGRAVE, Lee A.**, “*Data Protection Pursuant to the Right to Privacy in Human Rights Treaties*”, International Journal of Law and Information Technology, C. 6, S. 3, 1998, s. 247-284.
- ÇEKİN, Mesut Serdar**, “*6698 Sayılı Kişisel Verilerin Korunması Hakkında Kanun’un Big Data (Büyük Veri) ve İrade Serbestisi Açısından Değerlendirilmesi*”, İÜHFM, C. 124, S. 2, 2016, s. 629-644.
- ÇELİKEL, Serdar**, Kişisel Verilerin Korunması Hukuku Kapsamında Veri Sorumlusu ve Veri Sorumlusunun Yükümlülükleri, 1. Baskı, Ankara, 2022.

- ÇELİKEL, Serdar**, *Kişisel Verilerin İşlenmesinde, Açık Rıza Hukuka Uygunluk Nedeninin, 95/46 Sayılı Direktif ve GDPR’la Karşılaştırmalı Olarak İncelenmesi*, UMD, S. 17, 2021, s. 161-190. (Açık Rıza)
- DENİZ, İlknur**, *Çocuklara Ait Kişisel Verilerin Türk Medeni Kanunu ve Kişisel Verilerin Korunması Kanunu Kapsamında Korunması*, 1. Baskı, Ankara, 2021.
- DEVELİOĞLU, Hüseyin Murat**, 6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku, 1. Baskı, İstanbul, 2017.
- DOĞAN, Bayram**, *Karşılaştırmalı Hukukta Anayasal Bir Hak Olarak Kişisel Verilerin Korunması Hakkı*, 1. Baskı, Ankara, 2022.
- DOĞAN, Murat/ATAMULU, İsmail/ŞAHAN, Gökhan**, *Borçlar Hukuku Genel Hükümler*, 2. Baskı, Ankara, 2021.
- DURAL, Mustafa/SARI, Suat**, *Türk Özel Hukuku Cilt 1 Temel Kavramlar ve Başlangıç Hükümleri*, 15. Baskı, İstanbul, 2020.
- DÜLGER, Murat Volkan**, “*Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması*”, İMÜHFD, C.3, S. 2, 2016, s. 101-167.
- DÜLGER, Murat Volkan**, *Bilişim Suçları ve İnternet İletişim Hukuku*, 9. Baskı, Ankara, 2022.
- ELVY, Stacy**, “*Paying for Privacy and the Personal Data Economy*”, Columbia Law Review, C. 117, S. 6, 2017), s. 1369-1459.
- ERDOĞAN, İhsan**, *Borçlar Hukuku Genel Hükümler*, 4. Baskı, Ankara, 2019.
- ERDOĞMUŞ, Elif**, 6698 Sayılı Kişisel Verilerin Korunması Kanunu Kapsamında Açık Rıza, 1. Baskı, Ankara, 2022.
- EREN, Fikret**, *Borçlar Hukuku Genel Hükümler*, 28. Baskı, Ankara, 2023.
- FERGUSON, Andrew Guthrie**, “*Big Data and Predictive Reasonable Suspicion*”, University of Pennsylvania Law Review, C. 163, S. 2, 2015, s. 327-410.
- FLEISCHMANN, Amy**, “*Personal Data Security: Divergent Standards in the European Union and the United States*”, Fordham International Law Journal C. 19, S. 1, 1995 s. 143-180.

- GALBREATH, Jeremy**, *“The Internet: Past, Present, and Future.”* Educational Technology, C. 37, S. 6, 1997, s. 39–45.
- GELLERT, Raphael**, *“Comparing definitions of data and information in data protection law and machine learning: A useful way forward to meaningfully regulate algorithms?”* Regulation & Governance Dergisi, C. 16, S. 1, 2020, s. 156-176.
- GENÇ ARIDEMİR, Arzu**, Sözleşmeye Aykırılıktan Doğan Manevi Tazminat, 1. Baskı, İstanbul, 2008.
- GIURGIU, Andra/GERARD Lommel**, *“A New Approach to EU Data Protection: - More Control over Personal Data and Increased Responsibility”*, Critical Quarterly for Legislation and Law, C. 97, S. 1, 2014, s. 10–27.
- GÖÇMEN UYARER, Sinem**, Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması, 2. Baskı, Ankara, 2020.
- GRAHAM, Jonathan P.** *“Privacy, Computers and the Commercial Dissemination of Personal Information”*, Texas Law Review, C. 65, S. 7, 1987, s. 1395-1440.
- GUERRA, A. I./MACHADO, M. J./FERNANDES, M. M./AZEVEDO, P. A./TOMAS, S. T./ MACHADO, S. S.**, *“General Data Protection Regulation (GDPR): Legal, Ethic and Other Issues, Especially in COVID-19 Time”*, The Law, State and Telecommunications Review, C. 13, S. 2, 2021, s. 28-41.
- GÜNAY, Buket**, Kişiliğin Korunması Kapsamında Kişisel Verilerin Hukuka Aykırı Kullanılması Nedeniyle Hukuki Sorumluluk, 1. Baskı, Ankara, 2023.
- GÜR, İkbāl**, Kişisel Verilerin Korunması Hususunda AB ile ABD Arasında Çıkan Uyuşmazlıklar ve Çözüm Yolları, Yüksek Lisans Tezi, Ankara, 2009.
- GÜRSEL, İlke**, *“Protection of Personal Data in International Law and the General Aspects of the Turkish Data Protection Law”*, DEÜHFD, C. 18, S. 1, 2016, s. 33-61.
- HARTZOG, Woodrow**, *“What is Privacy? That's the Wrong Question”*, The University of Chicago Law Review, C. 88. S. 7, 2021, s. 1677-1688.
- KARASU, Rauf/SULUK, Cahit/NAL, Temel**, Fikri Mülkiyet Hukuku, 6. Baskı, Ankara, 2022.

- KAVAK, Yalçın**, Medeni Hukukun Temel Kavram ve Kurumları, 1. Baskı, İstanbul, 2019.
- KAYA, İslam Safa/TOLUN, Yüksel**, Türkiye’de, Avrupa’da ve California’da Kişisel Verilerin İşlenmesi, 2. Baskı, Ankara, 2022.
- KAYA, Turgut**, İnternet Servis Sağlayıcılarının Hukuki ve Cezai Sorumluluğu, 1. Baskı, Ankara, 2019.
- KAYIHAN, Şaban**, Kişiler Hukuku, 1. Baskı, Ankara, 2022.
- KAYIHAN, Şaban/ÜNLÜTEPE, Mustafa**, Borçlar Hukuku Genel Hükümler, 6. Baskı, Ankara, 2018, (KAYIHAN/ÜNLÜTEPE, Borçlar).
- KAYIHAN, Şaban/ÜNLÜTEPE, Mustafa**, Medeni Hukuk Bilgisi, 4. Baskı, Ankara, 2017.
- KILIÇOĞLU, Ahmet M.**, Borçlar Hukuku Genel Hükümler, 26. Baskı, Ankara, 2022.
- KILINÇ, Doğan**, *Anayasal Bir Hak Olarak Verilerin Korunması*, AÜHFD, C. 61, S. 3, 2012, s. 1089-1169.
- KORKMAZ, İbrahim**, “*Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme*”, TBBD, S. 124, 2016, s. 81-152.
- KULULAR İBRAHİM, Merve Ayşegül**, *Sosyal Medyaya Yönelik Yeni Düzenlemelerin Hukukten Değerlendirilmesi*, Bilişim Hukuku Dergisi, C. 4, S. 1, 2022, s. 1-32.
- KUŞ, Ulaş Baran**, Tüzel Kişilik Perdesinin Kaldırılması (Sermaye Şirketlerinde Sınırlı Sorumluluk İlkesinin İstisnası), 2. Baskı, Ankara, 2023.
- KÜZECİ, Elif**, Kişisel Verilerin Korunması, Doktora Tezi, Ankara, 2010.
- LEE, Bryan/ZOLOTOVA, Margarita**, “*Web 2.0, Social Media, and the ‘New’ Media.*” *New Media Solutions in Nonproliferation and Arms Control: Opportunities and Challenges*, James Martin Center for Nonproliferation Studies, 2013, s. 10–12.
- LEHR, William/CLARK, David/BAUER, Steve/BERGER, Arthur/RICHTER, Philipp**, “*Whither the Public Internet?*”, Journal of Information Policy, C. 9, 2019, s. 1-42.

- MALIK, Sohail Jehangir/NAZLI, Hina/ABRAR, Kashif**, “*Solving Organisational Problems with Intranet Technology.*” The Pakistan Development Review C.38, S. 4, 1999, s. 1021–1036.
- MEMİŞ, Tekin**, “*Veri Sorumlusu ve Veri İşleyen Arasındaki İlişkiler ve Sorumluluk Düzeni*”, Beykent Üniversitesi Hukuk Fakültesi Dergisi, C. 3, S. 6, 2017, s. 9-23.
- METİN, Yüksel**, *Avrupa Birliği Temel Haklar Şartı*, AÜSBFD, C. 57, S. 4, 2002, s. 37-63.
- NARTER, Sami**, Uygulamada Manevi Tazminat, 1. Baskı, Ankara, 2022.
- OĞUZ, Habip**, Elektronik Ortamda Kişisel Verilerin Korunması, Bazı Ülke Uygulamaları ve Ülkemizdeki Durum, UMD, S. 3, 2013, s. 1-38.
- OĞUZ, Sefer**, “*Kişisel Verilerin Korunması Hukukunun Genel İlkeler*”, Bilgi Ekonomisi ve Yönetimi Dergisi, C. 13, S. 2, 2018, s. 121-138.
- OĞUZMAN, M. Kemal/BARLAS, Nami**, Medeni Hukuk – Giriş – Kaynaklar – Temel Kavramlar, 22. Baskı, İstanbul, 2016.
- OĞUZMAN, M. Kemal/SELİÇİ, Özer/OKTAY ÖZDEMİR, Saibe**, Kişiler Hukuku, 21. Baskı, İstanbul, 2022.
- OĞUZMAN, M. Kemal/ÖZ, M. Turgut**, Borçlar Hukuku Genel Hükümler Cilt 2, 17. Baskı, İstanbul, 2022.
- ORAL, Tuğçe**, Tüzel Kişilerin Manevi Zararının Tazmini, 1. Baskı, Ankara, 2018.
- OYMAK, Hasan**, “*7253 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun’un Getirdikleri*”, Yeni Medya Dergisi, Ankara Hacıbayram Veli Üniversitesi İletişim Fakültesi, S. 9, 2020.
- ÖZBAKIR, Ali Fuat**, İnternet Servis Sağlayıcılarının Hukuki Sorumluluğu, Yüksek Lisans Tezi, İstanbul, 2016.
- ÖZDEMİR, Hayrünnisa**, Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması, 1. Baskı, Ankara, 2009.
- ÖZEL, Sibel**, Uluslararası Alanda Medya ve İnternette Kişilik Hakkının Korunması, 1. Baskı, Ankara, 2004.

- ÖZKAN, Oğulcan**, Kişisel Verilerin Korunması, Yüksek Lisans Tezi, Ankara, 2020.
- ÖZTAN, Bilge**, Medeni Hukukun Temel Kavramları, 38. Baskı, Ankara, 2013.
- ÖZTEKİN, Alp**, Teori ve Uygulamada İnternet Hukuku, 2. Baskı, Ankara, 2023.
- PEKER DEMİR, Esra**, İnternet Aracılığı ile Kişilik Haklarına Saldırı, Yüksek Lisans Tezi, İstanbul, 2014.
- PRINS, Corien**, “*When personal data, behavior and virtual identities become a commodity: Would a property rights approach matter?*”, SCRIPTed, C.3, S. 4, 2006, s. 270—303.
- RAMAN, Mittal**, “*Online Copyright Infringement Liability of Internet Service Providers*”, C.46, S. 2, Intellectual Property Rights Special Issue, 2004, s. 288-321.
- REMPELL, Scott**, “*Privacy, Personal Data and Subject Access Rights in the European Data Directive and Implementing UK Statute: Durant v. Financial Services Authority as a Paradigm of Data Protection Nuances and Emerging Dilemmas*” Florida Journal of International Law, C. 18, S. 3, 2006, s. 808-840.
- ROSENZWEIG, Roy**, Wizards, Bureaucrats, Warriors and Hackers: Writing the History of the Internet, The American Historical Review, C. 103, S. 5, 1998, s. 1530-1552.
- SAĞLAM, Kadir**, İnternet Aktörlerinin 5651 Sayılı Kanun Kapsamındaki İdari Sorumluluğu, Yüksek Lisans Tezi, Ankara, 2022.
- SAKA, Rıza/ÇAĞLAYAN, Ramazan/KOCA, Mahmut**, Avrupa Birliği Hukuku, İdare Hukuku ve Ceza Hukuku Açısından Kişisel Verilerin İmhası, Seçkin Hukuk, 2. Baskı, Ankara, 2022.
- SAMUELSON, Pamela**, “*Privacy As Intellectual Property?*”, Stanford Law Review, “Cyberspace and Privacy: A New Legal Paradigm?” Sempozyumu, C. 52, S. 5, 2000) s. 1125-1173.
- SOSYAL, Tamer**, İnternet Servis Sağlayıcılarının Hukuki Sorumlulukları, TBBD, S. 61, 2005, s. 304-339.
- TANDOĞAN, Haluk**, Türk Mes’uliyet Hukuku, 1. Baskı, İstanbul, 2010, s. 63.
- TAŞTAN, Furkan Güven**, Türk Sözleşme Hukukunda Kişisel Verilerin Korunması, 2. Baskı, İstanbul, 2017.

- TURAN, Metin**, Karşılaştırmalı Hukukta Kişisel Verilerin Korunması, 1. Baskı, Ankara, 2021.
- UNCULAR, Selen**, İş İlişkisinde İşçinin Kişisel Verilerinin Korunması, 2. Baskı, Ankara, 2018.
- UZUNAL, Seda**, Elektronik Haberleşme Sektöründe Kişisel Verilerin Korunması, Yüksek Lisans Tezi, İstanbul, 2023.
- ÜNAL, Mehmet/BAŞPINAR, Veysel**, Şekli Eşya Hukuku, 10. Baskı, Ankara, 2021.
- ÜNLÜTEPE, Mustafa**, Borçlar Hukuku Genel Hükümler, 1. Baskı, Ankara, 2021.
- VOSS, W. Gregory**, “*European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting*”, The Business Lawyer, C. 72, S. 1, 2016, s. 221–234 .
- WALDEN, I.N./SAVAGE, R.N.**, “*Data Protection and Privacy Laws: Should Organisations Be Protected?*” The International and Comparative Law Quarterly C.37, S. 2, 1988 s. 337-347.
- WARREN, Samuel/BRANDEIS Louis**, “*The Right to Privacy*”, Harvard Law Review, C.4, S. 5, 1890, s. 194-221.
- YILDIZ, Sevil**, İnternet Servis Sağlayıcılar ve Cezai Sorumlulukları, SÜİİBFSEAD, S. 3, 2002, s. 167-184.
- YILMAZ, Süleyman/YILDIRIM Abdülkerim** Medeni Hukuk – I, 2. Baskı, Ankara, 2021.
- YILMAZ, Tüze**, Avrupa Birliğinde, Kişisel Verilerin Korunması Hukuku, 1. Baskı, Ankara, 2022.
- YURDAKUL, Afşin**, *The Impact of Polarization On Turkey’s Information Environment*, Cyber Governance and Digital Democracy, S. 5, Ekonomi ve Dış Politika Araştırmalar Merkezi, 2020.
- YÜCEDAĞ, Nafiye**, “*Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu’nun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri*”, İÜHFM, C.75, S. 2, 2018, s. 765-789.

ZINS, Chaim, “*Conceptual Approaches for Defining Data, Information, and Knowledge*”, Journal of the American Society for Information Science and Technology, C. 58, S. 4, 2007, s. 479-493.

ZORLUEL, Mustafa, Fikrî Haklar Bağlamında İnternet Sitelerinin ve Web Sayfalarının Eser Niteliği – Fikri Mülkiyet Hukuku Monografileri, 1. Baskı, Ankara, 2022.



ÖZET

Dünyanın küreselleşmesine ve insanların birbirleriyle mesafe tanımaksızın iletişim kurmasında başat rol oynayan kitlesel iletişim araçları, internetin hayatımıza girmesi ve her geçen gün yeni bir boyut kazanarak yeni teknolojiler ile birlikte geniş tabana yayılmasıyla yeni bir boyut kazanmıştır. İnternet, milyonlarca insanın herhangi bir zahmete girmeksizin birbiriyle iletişim kurması imkanı çerçevesinde boyutu rakamlarla ifade edilmesi güç boyutlarda veri üretimine sebep olmaktadır. İnternetin kendine has yapısı nedeniyle, bu ortamda kişisel verilerin korunması her geçen gün daha önemli bir hal almaktadır.

İnternetin bilgiye ulaşım noktasında sağladığı olanakların insanlığın ortak yararına olduğu sarıh olmakla beraber; başta büyük firmalar olmak üzere internette faaliyet yürüten aktörler ile gerçek kişi kullanıcılar arasında ciddi bir güç dengesizliği bulunmaktadır. Kişisel verilerin ticari kaygılarla işlenmesi, bir noktada internetin devamı için gereklilik iken; temel hakların da göz ardı edilmemesi gerekmektedir. Çalışmamızda yarışan iki menfaat arasında dengenin kurulmasına yönelik hukuki değerlendirmeler Türk hukuku ve uluslararası mevzuat ile karşılaştırmalı bir şekilde ele alınmaya gayret edilmiştir.

Anahtar Kelimeler: *İnternet, Kişisel Veri, Kişisel Verilerin İşlenmesi, İnternet Aktörleri, Hukuki Sorumluluk*

ABSTRACT

Playing the principal role in the globalization of the world and the enabling of communication among people regardless of distances, mass media has reached a whole new level with the introduction of the internet in our lives and the development of an ever-expanding user base with the help of new technologies as well as extra novelties delivered every single day. Internet triggers massive amounts of data generation in quantities beyond numerical definition with the means and services it offers to millions of people enabling them to communicate with each other without breaking a single drop of sweat. The protection of personal data in this environment becomes increasingly important because of the unique nature of the internet.

While it is true that the many services and facilities offered by the internet in accessing information contributes to the collective benefit of the humankind, a substantive power imbalance exists between the real person users and the actors operating on the internet, big corporations in particular. Processing personal data for business concerns is essential for the sustainability of the internet; it is, however, equally essential not to overlook the fundamental rights. This study tries to address the legal analyses concerning the balancing of the two competing interests from the comparative perspective of the Turkish laws and the international legislation.

Key words: *Internet, personal data, processing personal data, internet actors, legal liability*