

**T.C.
ANKARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
ÖZEL HUKUK ANABİLİM DALI**

KİŞİSEL VERİLERİN KORUNMASI

Yüksek Lisans Tezi

Oğulcan ÖZKAN

Ankara - 2020

**T.C.
ANKARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
ÖZEL HUKUK ANABİLİM DALI**

KİŞİSEL VERİLERİN KORUNMASI

Yüksek Lisans Tezi

Oğulcan ÖZKAN

**Tez Danışmanı
Prof. Dr. Hasan İŞGÜZAR**

Ankara - 2020

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

Oğulcan ÖZKAN

KİŞİSEL VERİLERİN KORUNMASI

YÜKSEK LİSANS TEZİ

Tez Danışmanı

Prof. Dr. Hasan İŞGÜZAR

TEZ JÜRİSİ ÜYELERİ

Adı ve Soyadı

- 1- Prof. Dr. Hasan İŞGÜZAR
- 2- Prof. Dr. Erkan KÜÇÜKGÜNGÖR
- 3- Doç. Dr. Yildiz Abik
- 4-
- 5-

İmzası



Tez Savunması Tarihi

28.05.2020

T.C.
ANKARA ÜNİVERSİTESİ
Sosyal Bilimler Enstitüsü Müdürlüğü'ne,

Prof. Dr. Hasan İŞGÜZAR danışmanlığında hazırladığım “ Kişisel Verilerin Korunması (Ankara.2020) ” adlı yüksek lisans ☒ - doktora/bütünleşik doktora ☐ 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.

Tarih: 29. 05. 2020
Adı-Soyadı ve İmza

Oğulcan ÖZKAN


İÇİNDEKİLER

İÇİNDEKİLER.....	i
KISALTMALAR.....	vi
GİRİŞ.....	1

BİRİNCİ BÖLÜM

KİŞİSEL VERİ KAVRAMI, KİŞİSEL VERİLERİN HUKUKİ NİTELİĞİ VE KİŞİSEL VERİLERİN KORUNMASININ TARİHSEL GELİŞİM SERÜVENİ

§1. Kişisel Veri Kavramı	5
I. Tanımı	5
II. Unsurları	10
A. Her Türlü Bilgi (Any Information).....	10
B. Kimliği Belirli veya Belirlenebilir Kişi (Identified or Identifiable)	13
C. Bilginin Kişiye İlişkin Olması (Relating to).....	19
III. Özel Nitelikli (Hassas) Kişisel Veriler	22
§2. Kişisel Verilerin Hukuki Niteliği	24
I. Genel Olarak	24
II. Mülkiyet Hakkı Görüşü	25
III. Fikri Hak Görüşü	29
IV. Kişilik Hakkı Görüşü	31
§3. Kişisel Verilerin Korunmasının Tarihsel Gelişim Serüveni ve Kişisel Verilerin Korunmasının Hak Olarak Ortaya Çıkışı	40
I. Genel Olarak	40
II. Uluslararası Düzenlemeler.....	43
A. İnsan Hakları ve Özgürlüklerinin Korunmasına İlişkin Avrupa Sözleşmesi (Avrupa İnsan Hakları Sözleşmesi).....	43
B. OECD Rehber İlkeleri	45
C. Avrupa Konseyi 108 No.lu Sözleşme	47
D. Birleşmiş Milletler Rehber İlkeleri.....	51
E. 95/46/EC Sayılı AB Direktifi.....	52
F. 181 No.lu Protokol	56
G. AB Temel Haklar Şartı	57
H. 2016/679 AB Genel Veri Koruma Tüzüğü (GDPR)	58

1. Genel Olarak.....	58
2. GDPR’ın Kapsamı.....	62
3. Rıza Koşulları ve Çocuğun Rızası.....	64
4. Unutulma Hakkı	65
5. Kısıtlama Hakkı.....	73
6. Veri Taşınabilirliği Hakkı.....	74
7. Veri Koruma Etki Değerlendirmesi ve Ön Danışma.....	74
8. Veri Koruma Görevlisi	76
9. Avrupa Veri Koruma Kurulu.....	77
10. İdari Para Cezası.....	78
III. Ulusal Düzenlemeler	79
A. 5237 Sayılı TCK.....	79
B. T.C. Anayasa Hükmü.....	80
C. 6698 Sayılı Kişisel Verilerin Korunması Kanunu	82

İKİNCİ BÖLÜM

6698 SAYILI KİŞİSEL VERİLERİN KORUNMASI KANUNU KAPSAMINDA KİŞİSEL VERİLERİN KORUNMASI

§4. Kanunun Amacı, Kapsamı ve Terimler	85
I. Kanunun Amacı	85
II. Kanunun Kapsamı.....	86
A. Kanun Kapsamına Giren Haller.....	87
1. Kişi Bakımından	87
2. Konu Bakımından.....	88
B. Kanun Kapsamına Girmeyen Haller	91
1. Tamamen Kanun Kapsamına Girmeyen Haller.....	91
2. Kısmen Kanun Kapsamına Girmeyen Haller	93
III. Terimler	95
A. Genel Olarak	95
B. Veri Sorumlusu ve Veri İşleyen.....	95
§5. Kişisel Verilerin İşlenmesi	101
I. Genel Olarak	101
II. Kişisel Verilerin İşlenmesine İlişkin Genel İlkeler.....	101
A. Hukuka ve Dürüstlük Kuralına Uygun Olma İlkesi	104
B. Doğru ve Gerekliğinde Güncel Olma İlkesi	107

C. Belirli, Açık ve Meşru Amaçlar İçin İşlenme İlkesi	108
D. Amaçla Bağlantılı, Sınırlı ve Ölçülü Olma İlkesi.....	109
E. Belirli ve Sınırlı Süre Muhafaza Edilmesi İlkesi	113
III. Kişisel Verileri İşleme Şartları	116
A. Açık Rıza	118
1. Genel Olarak.....	118
2. Sessiz Kalınması.....	120
3. Açık Rızayı Açıklama Ehliyeti.....	123
4. Açık Rızanın Şekli.....	125
5. Açık Rızanın Açıklanacağı Zaman.....	126
6. Açık Rızanın Geri Alınması	126
7. Açık Rızanın Unsurları.....	127
a. Belirli Bir Konuya İlişkin Olma	127
b. Bilgilendirmeye Dayanma	128
c. Özgür İradeyle Açıklanma.....	129
B. Açık Rıza Gerekmeyen Haller	130
1. Kanunlarda Açıkça Öngörülmesi	131
2. Fiili İmkansızlık.....	132
3. Sözleşmenin Kurulması veya İfası İçin Gerekli Olması	134
4. Veri Sorumlusunun Hukuki Yükümlülüğünü Yerine Getirebilmesi İçin Zorunlu Olması	136
5. Kişisel Verilerin İlgili Kişinin Kendisi Tarafından Alenileştirilmesi	138
6. Veri İşlemenin Bir Hakkın Tesisi, Kullanılması veya Korunması İçin Zorunlu Olması	140
7. Veri İşlemenin Veri Sorumlusunun Meşru Menfaatleri İçin Zorunlu Olması.....	141
C. Özel Nitelikteki (Hassas) Kişisel Verilerin İşlenme Şartları	145
IV. Kişisel Verilerin Silinmesi, Yok Edilmesi ve Anonim Hale Getirilmesi.....	150
V. Kişisel Verilerin Aktarılması.....	158
A. Yurt İçinde Aktarılması	158
B. Yurt Dışına Aktarılması.....	161
1. Genel Olarak.....	161
2. Yeterli Korumanın Bulunması	162
3. Yeterli Korumanın Bulunmaması.....	163
§6. Tarafların Hak ve Yükümlülükleri	166

I. Veri Sorumlusunun Yükümlülükleri.....	166
A. Aydınlatma Yükümlülüğü	166
B. Veri Güvenliğine İlişkin Yükümlülükler	171
1. Teknik ve İdari Tedbirleri Alma Yükümlülüğü	171
2. Denetim Yükümlülüğü	176
3. Sır Saklama Yükümlülüğü	177
4. Kurul’a Bildirim Yükümlülüğü	177
C. Veri Sorumluları Sicili’ne Kayıt Yükümlülüğü.....	179
1. VERBİS	179
2. VERBİS’e Kayıt Yükümlülüğü ve İstisnaları	182
3. VERBİS’e Kayıt Bildirimi	184
4. Kişisel Veri İşleme Envanteri Hazırlama Yükümlülüğü	186
II. İlgili Kişinin Hakları	189
A. Öğrenme ve Bilgi Talep Etme Hakkı	189
B. Kişisel Verilerin Düzeltmesini, Silinmesini veya Yok Edilmesini İsteme Hakkı	191
C. İtiraz Etme Hakkı	193
D. Zararın Giderilmesini Talep etme Hakkı	194
E. Veri Sorumlusuna Başvuru Hakkı	194
F. Kurul’a Şikayet Hakkı.....	198
1. Kurul’a Şikayet.....	198
2. Kurul Tarafından Yapılan İncelemenin Usul ve Esasları.....	202
§7. Kişisel Verileri Koruma Kurumu	206
I. Kişisel Verileri Koruma Kurumu	206
II. Kişisel Verileri Koruma Kurulu.....	207

ÜÇÜNCÜ BÖLÜM

6698 SAYILI KİŞİSEL VERİLERİN KORUNMASI KANUNU DIŞINDA KİŞİSEL VERİLERİN KORUNMASI YOLLARI

§8. Kişisel Verilerin Korunması.....	209
§9. İş İlişkisinde Kişisel Verilerin Korunması	210
§10. 4721 Sayılı Türk Medeni Kanunu Kapsamında Kişisel Verilerin Korunması.....	216
I. Genel Olarak	216

II. Kişisel Verilerin Hukuki İşleme Gerçekleştirilen Saldırlara Karşı Korunması.....	217
III. Kişisel Verilerin Hukuka Aykırı Fiille Gerçekleştirilen Saldırlara Karşı Korunması.....	219
A. Genel Olarak.....	219
B. Kişisel Verilerin Hukuka Aykırı Olarak İşlenmesi Halinde Açılabilir Davalar	222
1. Korumaya Davalar	222
a. Saldırı Tehlikesinin Önlenmesi Davası	224
b. Saldırıya Son Verilmesi Davası.....	225
c. Saldırının Hukuka Aykırılığının Tespiti Davası.....	227
2. Tazminat Davaları	228
a. Maddi Tazminat Davası.....	229
b. Manevi Tazminat Davası.....	232
c. Kazancın Geri Verilmesi Davası	236
3. Davacı ve Davalı Taraf.....	237
a. Davacı Taraf	237
b. Davalı Taraf.....	239
4. Yetkili Mahkeme	239
§11. 5237 Sayılı Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması	241
I. Genel Olarak	241
II. Kişisel Verilerin Kaydedilmesi Suçu.....	243
III. Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme Suçu	249
IV. Verileri Yok Etmeme Suçu	254
SONUÇ	257
KAYNAKÇA.....	263
ÖZET	281
ABSTRACT	282

KISALTMALAR

5651 sayılı Kanun	: İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun
AAD	: Avrupa Adalet Divanı
AB	: Avrupa Birliği
ABİHA	: Avrupa Birliği'nin İşleyişi Hakkındaki Antlaşma
ABTHŞ	: Avrupa Birliği Temel Haklar Şartı
AB Direktifi	: “95/46/EC Sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi” (“Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data”)
AİHM	: Avrupa İnsan Hakları Mahkemesi
AİHS	: Avrupa İnsan Hakları Sözleşmesi
AK	: Avrupa Konseyi
AK 108 No.lu Sözleşme	: “Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi” (“Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data”)
AİHM	: Avrupa İnsan Hakları Mahkemesi
AİHS	: Avrupa İnsan Hakları Sözleşmesi
ASK	: 5352 sayılı Adli Sicil Kanunu
AÜHFD	: Ankara Üniversitesi Hukuk Fakültesi Dergisi

AÜSBFD	: Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi
AYM	: Anayasa Mahkemesi
AYT	: Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ
BDSG	: Bundesdatenschutzgesetz (Alman Federal Veri Koruma Kanunu)
BGBI.	: Bundesgesetzblatt (Alman Federal Resmi Gazetesi)
BGE	: Entscheidungen des Schweizerischen Bundesgerichts (İsviçre Federal Mahkemesi Kararları)
BM	: Birleşmiş Milletler
BVerfGE	: Entscheidungen des Bundesverfassungsgerichts (Alman Federal Anayasa Mahkemesi Kararları)
C.	: Cilt
c.	: Information and notices ('communications' in French) (Bilgi ve tebliğler)
CD.	: Ceza Dairesi
CGK.	: Ceza Genel Kurulu
CMK	: 5271 sayılı Ceza Muhakemesi Kanunu
DEÜHFD	: Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi
DLP	: Data Loss Prevention (Veri Sızıntısı Önleme)
DPO	: Data Protection Officer (Veri Koruma Görevlisi)
E.	: Esas
E.T.	: Erişim Tarihi
EDPB	: European Data Protection Board (Avrupa Veri Koruma Kurulu)
Envanter	: Kişisel Veri İşleme Envanteri

EU	: European Union (Avrupa Birliđi)
EUROJUST	: European Union Agency for Criminal Justice Cooperation (Avrupa Birliđi Ceza Adaleti İş Birliđi Ajansı)
EUROPOL	: European Union Agency for Law Enforcement Cooperation (Avrupa Birliđi Kolluk İş Birliđi Ajansı)
EÜHFD	: Erzincan Üniversitesi Hukuk Fakültesi Dergisi
GDPR	: General Data Protection Regulation (Genel Veri Koruma Tüzüğü)
GÜHFD	: Gazi Üniversitesi Hukuk Fakültesi Dergisi
HD.	: Hukuk Dairesi
HGK.	: Hukuk Genel Kurulu
HMK	: 6100 sayılı Hukuk Muhakemeleri Kanunu
IBAN	: International Bank Account Number (Uluslararası Banka Hesap Numarası)
İDDK.	: İdari Dava Daireleri Kurulu
İK	: 4857 sayılı İş Kanunu
İMÜHFD	: İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi
İSGHD	: İş Hukuku ve Sosyal Güvenlik Hukuku Dergisi
İÜHFD	: İnönü Üniversitesi Hukuk Fakültesi Dergisi
İÜHFM	: İstanbul Üniversitesi Hukuk Fakültesi Mecmuası
K.	: Karar
Kazancı	: www.kazancı.com (Kazancı İçtihat Bilgi Bankası)
KEP	: Kayıtlı Elektronik Posta
KTK	: 2918 sayılı Karayolları Trafik Kanunu
Kurul	: Kişisel Verileri Koruma Kurulu
Kurum	: Kişisel Verileri Koruma Kurumu

KVKK	: 6698 sayılı Kişisel Verilerin Korunması Kanunu
KVSYAY	: Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik
L.	: Legislation (Mevzuat)
m.	: Madde
MİT	: Milli İstihbarat Teşkilatı
MÜHF-HAD	: Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi
No	: Numara
OECD	: Organisation For Economic Cooperation And Development (Ekonomik Kalkınma ve İşbirliği Örgütü)
OECD Rehber İlkeleri	: “Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeler” (“Guidelines on the Protection of Privacy and Transborder Flows of Personal Data”)
OJ.	: Official Journal of the European Union (Avrupa Birliği Resmi Gazetesi)
p.	: page (sayfa)
PVSK	: 2559 sayılı Polis Vazife ve Salahiyet Kanunu
RFID	: Radio Frequency Identification (Radyo Frekansı ile Tanımlama)
RG.	: Resmi Gazete
s.	: Sayfa
S.	: Sayı
Se.	: Seite (Sayfa)
Sicil	: Veri Sorumluları Sicili

SSL	: Secure Sockets Layer (Güvenli Yuva Katmanı)
T.	: Tarih
T. C.	: Türkiye Cumhuriyeti
TBB	: Türkiye Barolar Birliği
TBK	: 6098 sayılı Türk Borçlar Kanunu
TCK	: 5237 sayılı Türk Ceza Kanunu
TMK	: 4721 sayılı Türk Medeni Kanunu
TTK	: 6102 sayılı Türk Ticaret Kanunu
TÜİK	: Türkiye İstatistik Kurumu
V.	: Volume (Cilt)
VERBİS	: Veri Sorumluları Sicil Bilgi Sistemi
VKED	: Veri Koruma Etki Değerlendirmesi
VKS	: Veri kayıt sistemi
VSBT	: Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ
VSSY	: Veri Sorumluları Sicili Hakkında Yönetmelik
vd.	: ve devamı
WP	: Working Party (Çalışma Grubu)
Y.	: Yıl

GİRİŞ

Her ne kadar kişisel verilerin korunması söylem ve istemi çok yeni olsa da çok eski zamanlardan beri özellikle kamu tarafından kişisel veriler toplanmakta ve işlenmektedir. Kişisel verilerin işlenmesine karşın bireylerin kişisel verilerinin korunması hakkının tanınması ve ülkeler tarafından kabul görmesi ise kişisel verilerin ekonomik değerinin ve kişisel verilerin işlenmesinden doğabilecek risklerin fark edildiği yakın bir döneme rastlamaktadır.

Değişen ve dönüşen toplum ile bağlantılı olarak dünya da çok hızlı bir şekilde değişmektedir. Dünya tarihi incelendiğinde yeni düşünce, fikir veya buluşların dünya düzenini değiştirdiği gözlemlenmektedir. Kişisel veriler konusu da yeni dünya düzeni ile birlikte önem kazanan konular arasındadır. Zira bilişim teknolojilerindeki ilerleme ile adeta dünyada kartlar yeniden dağıtılmaya başlanmıştır. Yeni dünya düzeninin getirilerinden olan küreselleşme ile birlikte bilgiler sabit olarak toplandığı yerde kalmamakta, aktarılmakta, adeta herhangi bir bilgiye dünyanın her noktasından kolayca ulaşılabilir.

Bilişim teknolojilerindeki gelişmeler bilgiye ulaşımı, bilginin toplanmasını, sunulmasını ve dağıtımını akıl almayacak şekilde kolay bir hale getirmiştir. Söz konusu gelişmelerin bilgiye ulaşımı kolaylaştırma sonucu yaratmasının, insan hayatına getirdiği faydanın büyüklüğü tartışılmaz bir gerçektir. Günümüzde nerdeyse herkesin birçok sosyal medya platformunda kişisel hesapları bulunmakta, alışverişler online olarak yapılmakta, online ortamdaki ticari hacimden söz etmeye gerek dahi bulunmamaktadır.

Tüm bu gelişmelerle birlikte değeri anlaşılan bilgi, hem kamu hem de özel sektör için vazgeçilmez hale gelmiştir. Kamu kurumları, kamu hizmetlerinin daha etkin bir şekilde yürütülebilmesi için kişisel verileri işlemektedir. Benzer şekilde şirketler de kişisel bilgileri işlemekte, bu bilgileri kullanmakta, paylaşmakta ve kişilere ait bilgiler

analiz edilerek ciddi manada gelir elde etmektedir. Kişilere ait bilgilerin işlenmesi birçok açıdan fayda sağlasa da işleme faaliyeti sonucunda kişinin temel hak ve özgürlükleri ihlal edilebilmektedir. Başka bir ifadeyle, kişisel verilerin işlenmesinden doğan menfaat karşısında “*bireyin kişisel verilerinin geleceğini belirleme hakkı*” bulunmaktadır.

Kişilerin attıkları her adımda kişisel verilerin işlenmesi, kişilerin hem fiziki hem de online ortamda takip edilmesi, şirketlerin ya da devletin kişilere ait bilgilere kişilerin yakınlarından daha çok vakıf olması distopik bir toplum düzenini çağrıştırmaktadır. Böyle bir düzende ise korku toplumunun oluşması kaçınılmaz olacaktır. Bu nedenle kişisel verilerin işlenmesinin kişisel verilerin korunması hakkını ihlal etmeyecek şekilde hukuka uygun olarak gerçekleştirilmesi önem arz etmektedir.

Kişisel Verilerin Korunması Hukuku’nun amacı, kişisel verilerin işlenmesini tamamen yasaklamak değildir. Açıkçası günümüz dünya düzeninde böyle bir amaç mümkün de değildir. Zira kişisel verilerin işlenmesi tek bir nedene dayanmamakta, işleme faaliyeti artık hayatın olağan bir parçası haline gelmiştir. Kişisel verilerin korunması düzenlemelerindeki asıl amaç ise veri işleme faaliyetinin belirli sınırlar çerçevesinde, hukuka ve dürüstlük kuralına riayet edilerek, insan haklarına ihlale sebebiyet vermeyecek şekilde belirli bir düzen çerçevesinde gerçekleştirilmesidir. Ancak her nasıl ki Ceza Hukukuna özgü düzenlemelerle suç işlenmesinin önüne geçilemiyorsa salt kişisel verileri koruyan düzenlemeler getirilerek de kişisel verilerin hukuka aykırı olarak işlenmesi engellenemez. Kişisel verilerin korunması mantalitesinin gerçek yaşamda tam olarak karşılık bulabilmesi için veri koruma bilincinin yediden yetmişe toplum tarafından içselleştirilmesi gerekmektedir. Aksi halde kişisel verilerin korunması için getirilen düzenlemeler ütopyik bir gayretten öteye gidemez.

Kişisel verilerin korunmasına özgü ulusal ve uluslararası düzenlemeler 1970’li yıllardan itibaren ortaya konulmaya başlanmıştır. Kişisel verilerin korunması hakkının ve bu hakkı koruyucu düzenlemelerin, tarihte kişisel verilerin hukuka aykırı işlenmesinin yol açabileceği sonuçları acıyla tecrübe eden Avrupa’da ortaya çıkmasına şaşkırmamak gerekir. Tarih olarak geç de kalınmış olsa Avrupa’daki gelişmelere paralel olarak Anayasamızda 2010 yılında yapılan değişiklikle kişisel verilerin korunması hakkı anayasal güvence altına alınmıştır. Anayasa tarafından çerçevesi çizilen söz konusu hakkın detayları ve etkin bir şekilde korunabilmesi için bu konuya özgü bir kanun yapılma gerekliliği doğmuştur. Bu kapsamda 6698 sayılı Kişisel Verilerin Korunması Kanunu (“**KVKK**”) 07.04.2016 tarihinde yürürlüğe girmiştir.

Kişisel verilerin korunması çok geniş bir alan olup, salt hukukun bir alanıyla ilişkilendirilmesi düşünülemez. Bu kapsamda, kişisel verilerin korunması, Medeni Hukuk, Borçlar Hukuku, Ceza Hukuku, İş Hukuku, Anayasa Hukuku, İdare Hukuku, Ticaret Hukuku gibi alanlarla bağlantılıdır. Tüm hukuk alanlarındaki korumanın ayrıntılarıyla incelenmesi çalışma konumuzun boyutlarını ciddi anlamda genişletecektir. Bu nedenle söz konusu çalışmamızda özellikle ülkemiz için çok yeni olan KVKK hükümleri detaylı olarak incelenmiş, bu alandaki bilinmezliklere ışık tutan Kişisel Verileri Koruma Kurulu kararlarına yer verilmiş, Medeni Hukuk, Ceza Hukuku ve İş Hukukuna özgü düzenlemeler açıklanmış, yeri geldikçe de konunun Anayasa Hukuku ve İdare Hukuku boyutu ile bağlantılar kurulmuştur.

Çalışmamız üç bölümden oluşmaktadır. İlk bölüme kişisel veri tanımı, kişisel verinin unsurları ve özel nitelikli kişisel veri ayrımı anlatılarak başlanmıştır. Uygulanacak hukuk kurallarının ve birçok sorunun tespiti amacıyla kişisel verilerin hukuki niteliği ile ilgili görüşler tartışılmıştır. Daha sonra kişisel verilerin korunması hakkının hak olarak ortaya çıkışı ve kişisel verilerin korunmasının tarihsel gelişim serüvenine yer verilmiştir. Bu kapsamda, Kişisel Verilerin Korunması Hukuku’nun oluşumunu sağlayan uluslararası

düzenlemeler inceleme konusu yapılmıştır. Kişisel verilerin korunması hakkına ve mevzuatına özel olarak ilgi gösteren Avrupa Birliği'nin bu konudaki güncel düzenlemelerine de yer vermeye çalışılmıştır. Bu bölümde, son olarak, kişisel verilerin korunması düzenlemelerinin ülkemizdeki gelişimi kronolojik olarak anlatılmıştır.

Çalışmanın ikinci bölümünde 7 Nisan 2016 tarihinde ülkemizde yürürlüğe giren ve bu alana özgü bir kanun olan KVKK kapsamında kişisel verilerin korunması detaylarıyla irdelenmiştir. Bu bölümde kanunun sistematığına sadık kalınmaya çalışılmıştır. Bu bağlamda, öncelikle kanunun amacı, kapsamı ve kanundaki önemli terimler anlatılmıştır. Daha sonra kişisel verilerin işlenmesi başlığı altında kişisel verilerin işlenmesinde genel ilkeler, kişisel verileri işleme şartları ve kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesi inceleme konusu yapılmıştır. Kişisel verilerin işlenmesi ilişkisinin tarafları olan veri sorumlusunun ve ilgili kişinin kanundan kaynaklanan haklarına ve yükümlülüklerine yer verilerek, KVKK'da yer alan, ilgili kişinin kişisel verilerinin korunması yolu detaylarıyla incelenmiştir.

Çalışmamızın son bölümü olan üçüncü bölümde ise Kişisel Verilerin Korunması Hukuku dışındaki hukuk dallarında kişisel verilerin korunması ele alınmıştır. Bu kapsamda, öncelikle hassas yapısı gereği iş ilişkisinde kişisel verilerin korunmasına ayrı bir parantez açılmıştır. Sonrasında kişisel verilerin hukuka aykırı işlenmesi halinde başvurulabilecek 4721 sayılı Türk Medeni Kanunu ("**TMK**") hükümlerine yer verilmiştir. Kişisel verilere ilişkin suçlar için KVKK'nın yaptığı atıf gereği 5237 sayılı Türk Ceza Kanunu ("**TCK**") ilgili hükümleri açıklanmıştır.

Bu çalışmada salt teorik bilgi vermekten kaçınılmış, teorik açıklamalar özellikle Kişisel Verileri Koruma Kurulu kararları ve yüksek mahkeme kararları ile somutlaştırılmaya çalışılmıştır.

BİRİNCİ BÖLÜM

KİŞİSEL VERİ KAVRAMI, KİŞİSEL VERİLERİN HUKUKİ NİTELİĞİ VE KİŞİSEL VERİLERİN KORUNMASININ TARİHSEL GELİŞİM SERÜVENİ

§1. Kişisel Veri Kavramı

I. Tanımı

Kişisel verilerin korunması için öncelikle kişisel veri kavramının net bir şekilde ortaya koyulması önem arz etmektedir. Kişisel veri kavramını tanımlayabilmek için öncelikle “*kişisel*” ve “*veri*” kavramlarını ayrı ayrı irdelenmek gerekmektedir. “*Kişisel*” kavramı “*kişi ile ilişkili, kişiye ilişkin olan, şahsi*”¹, “*bir gruptan ziyade tek veya belirli bir kişiye ait olan*”² anlamına gelmektedir. Kişisel kavramından daha komplike olan veri kavramı ise “*bilgi, data*”³ olarak ifade edilmektedir. Her ne kadar TDK veri ve bilgi kavramlarını eş tutsa da bu iki kavram tam olarak birbirini karşılamamaktadır⁴. Ancak

¹ **Türk Dil Kurumu (“TDK”)**, Güncel Türkçe Sözlük, <https://sozluk.gov.tr> (E.T.: 25.02.2020).

² **Cambridge Dictionary**, <https://dictionary.cambridge.org/dictionary/english/personal> (E.T.: 25.02.2020).

³ **TDK**, <https://sozluk.gov.tr> (E.T.: 25.02.2020).

⁴ Veri ve bilgi kavramları arasındaki nüanslar hakkında detaylı bilgi için bkz. **Küzeci, Elif**, Yenilenmiş ve Gözden Geçirilmiş 3. Baskı, Ankara 2019, s. 9-12; **Henkoğlu, Türkay**, Bilgi Güvenliği ve Kişisel Verilerin Korunması, Ankara 2015, s. 25-26.

hukuki düzenlemelerde, kişisel veri doktrinde ve uygulamada her iki kavram da aynı anlamda kullanılmaktadır. Bu çalışmada da anlamsal karmaşaya yol açmamak amacıyla veri ve bilgi kavramları eş anlamda kullanılmıştır. Kişisel veri kavramının İngilizcedeki karşılığı *“personal data”*dır. Almandaki karşılığı ise *“personenbezogene Daten”*dır. Kişisel veri kavramının yabancı dillerdeki karşılığına bakıldığında “data” kavramının ön plana çıktığı görülmektedir.

Uluslararası ve ulusal belgelerde kişisel verilerin tanımı yapılmıştır. 1980 tarihli Ekonomik Kalkınma ve İş Birliği Örgütü (*“OECD”*) Rehber İlkeleri⁵ uyarınca kişisel veriler, *“Kimliği belirli ya da belirlenebilir bir gerçek kişi (ilgili kişi) hakkındaki tüm bilgileri ifade eder.”* Avrupa Konseyi (*“AK”*) tarafından hazırlanan 108 No.lu sözleşmenin⁶ tanımlar maddesinde (m. 2/a) de kişisel veri tamamen aynı şekilde tanımlanmıştır⁷. Ülkemizde 2016 yılında yürürlüğe giren 6698 sayılı Kişisel Verilerin

⁵ **Organisation for Economic Cooperation and Development (*“OECD”*)**, *“Guidelines on the Protection of Privacy and Transborder Flows of Personal Data”* (*“Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeler”*) (Bundan böyle OECD Rehber İlkeleri olarak anılacaktır.), 23.09.1980, <https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprivacyandtransborderflowsofpersonaldata.htm> (E.T.: 25.02.2020).

⁶ **Council of Europe (Avrupa Konseyi)**, *“Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data”* (*“Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi”*) (Bundan böyle AK 108 No.lu sözleşme olarak anılacaktır.), European Treaty Series No. 108, 28.01.1981, <https://rm.coe.int/1680078b37> (E.T.: 26.02.2020).

⁷ *“Personal data means any information relating to an identified or identifiable individual (data subject).”*

Korunması Kanunu (“**KVKK**”) da uluslararası sözleşmelerdeki tanımlara uymuş, kişisel veriyi “*kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi*” olarak tanımlamıştır.

Avrupa Birliği (“**AB**”) düzenlemelerinden olan ve KVKK’ya esas oluşturan AB 95/46/EC sayılı Direktifi⁸ ve bir diğer AB düzenlemelerinden olan 2016/779 Genel Veri Koruma Tüzüğü⁹ (“**GDPR**”) kişisel veri tanımını yaparken farklı bir yöntem kullanmışlar, nelerin kişisel veri sayılacağı hususunda örneklerle yer vermişlerdir. Söz konusu düzenlemelerde kişisel verinin tanımı “*Kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiyle ilgili her türlü bilgidir. Bu gerçek kişi, özellikle bir isim, kimlik numarası, konum verileri ya da bu gerçek kişinin fiziksel, fizyolojik, genetik, ruhsal, ekonomik, kültürel veya toplumsal kimliğine özgü bir ya da daha fazla sayıda*

⁸ **European Union (“EU”)**, “*Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*” (“95/46/EC Sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi”) (Bundan böyle AB Direktifi olarak anılacaktır.), <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046> (E.T.: 02.03.2020).

⁹ **European Union**, “*Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR)*” (“2016/679 Avrupa Birliği Genel Veri Koruma Tüzüğü”) (Bundan böyle GDPR olarak anılacaktır.), <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679> (E.T.: 02.03.2020).

faktöre atıfta bulunularak doğrudan veya dolaylı olarak kimliği belirlenebilen kişidir.”¹⁰ şeklinde yapılmıştır. Alman Federal Veri Koruma Kanunu (**“Bundesdatenschutzgesetz”**) (**“BDSG”**)¹¹ da kişisel veriyi benzer şekilde tanımlamıştır¹². Netice itibariyle ulusal ve uluslararası düzenlemelerde kişisel veri tanımının örtüştüğü gözlemlenmektedir. Ancak kişisel verinin kapsamı burada örnek mahiyetinde sayılan verilerle sınırlı değildir. Burada sayılanlar genişletilebilir ancak daraltılamaz. Başka bir ifadeyle tanımda sayılan verilerin kişisel veri olduğu aşıkardır ancak bunlar dışında da kişisel veri kapsamına girecek birçok veri türü elbette mevcuttur. Örnekleme yoluyla saymadaki amaç kişisel verinin kapsamı sorununa misal oluşturmaktır.

¹⁰ *“Personal data means any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.”*

¹¹ BGBl. I, 27.06.2017, Se. 2097. BDSG son hali için bkz. https://www.gesetze-im-internet.de/bdsg_2018/BJNR209710017.html (E.T.: 09.04.2020).

¹² *“personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (betroffene Person) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser Person sind, identifiziert werden kann.”* BDSG m. 46/1.

Kişisel veri, “*bizi biz yapan*” her türlü bilgi olarak ifade edilebilir¹³. İnsanın adı, işi, adresi, sağlık durumu, medeni hali, cinsel yaşamına ait bilgiler gibi insanın insan oluşundan kaynaklanan bilgiler kişisel veri kategorisine dahil olduğu gibi teknolojiye ilerleme neticesinde zamanla banka hesap numarası, T.C. kimlik numarası, e-posta adresi gibi bilgiler de kişisel veri haline gelmiştir¹⁴. Özellikle bilişim alanındaki ilerleme devam ettiği sürece de kişisel veri kategori sayısı artmaya devam edecek, içinde bulunduğumuz şu zamanda adını bilmediğimiz, belki de anlamlandıramadığımız bilgi türleri de ilerleyen yıllarda kişisel veri kapsamına dahil olacaktır.

Kişisel veri tanımları incelendiğinde tanımlar çok geniş tutulmuş, hangi tür bilgilerin kişisel veri kapsamına dahil edilip edilmeyeceği sınırlandırılmamıştır. İşte bu sebeple kişisel veri tanımına dahil edilebilecek bilgilerin doktrin ve uygulama tarafından tespit edilmesi icap etmektedir. Doktrin ve uygulama tarafından yapılacak yorum, kapsamı genişletebileceği gibi daraltabilecektir¹⁵. Bu nedenle ne tür bilgilerin kişisel veri olup olmadığının sınırlarının iyi çizilmesi gerekmektedir. AB Direktifi m. 29 uyarınca kurulan Çalışma Grubu (“*Working Party*”) (“*WP*”) da kişisel veri kavramının anlamı ve unsurları hakkında ayrıca Direktif’in nasıl anlaşılması gerektiği ve somut durumlarda

¹³ **Kurum**, Kişisel Verilerin Korunması Kanunu ve Getirdikleri, Yayın No: 26, s. 2.

¹⁴ **Dülger, Murat Volkan**, Kişisel Verilerin Korunması Hukuku, 2. Baskı, İstanbul 2019, s. 1.

¹⁵ **Aksoy, Hüseyin Can**, Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması, Ankara 2010, s. 12.

nasıl uygulanması gerektiği hakkında tavsiye niteliğinde bir rapor¹⁶ hazırlamıştır¹⁷.

II. Unsurları

Kişisel veri kavramının genel olarak kabul görmüş, ulusal ve uluslararası düzenlemelere göre üç unsurunun olduğu görülür. Bunlar “bilgi”, “kimliği belirli veya belirlenebilir kişi” ve “bilginin kişiye ilişkin olması”dır. Doktrinde tartışmalı olmakla birlikte dördüncü unsur olarak “gerçek kişi (natural person)” de sayılabilmektedir¹⁸. Burada sayılan tüm unsurların bir arada olması koşuluyla bir bilgi kişisel veri sayılabilir ve ileride değineceğimiz korumalardan yararlanabilir.

A. Her Türlü Bilgi (Any Information)

AB Direktifi’nde yer alan “her türlü bilgi (any information)” terimi direktifteki amacın kişisel veri kavramını oldukça geniş olarak belirleme isteğini gösterir. KVKK’da da benzer şekilde kişisel veri tanımında “her türlü bilgi” terimine yer verilmiştir. Bilginin niteliği, içeriği ve yer aldığı teknik format ne olursa olsun kişisel veri olarak kabul etmek için geniş yorumlamak gerekir¹⁹. “Her türlü bilgi” ifadesi yalnızca bireyin direkt olarak adı, soyadı veya doğum tarihi gibi kişiyi tanıma imkanı sağlayan verileri değil, bununla birlikte kişiyi tanınabilir kılan ailevi, sosyal, fiziksel ve ekonomik bilgilerini de

¹⁶ Söz konusu rapor için bkz. **Data Protection WP**, Opinion 4/2007 on the Concept of Personal Data, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf (E.T.: 03.03.2020).

¹⁷ **Aksoy**, Kişisel Veri, s. 13.

¹⁸ **Data Protection WP**, Concept, s. 21.

¹⁹ **Data Protection WP**, Concept, s. 1.

kapsamaktadır²⁰.

Kişisel verilerle ilgili tanım Anayasa Mahkemesi ("**AYM**") kararlarında da yer almış, söz konusu kararda ayrıca hangi tür bilgilerin kişisel veri kapsamına dahil olacağı ifade edilmiştir²¹. Buna göre, "*Kişisel veri kavramı, belirli veya kimliği belirlenebilir olmak şartıyla, bir kişiye ilişkin bütün bilgileri ifade etmektedir. Bu bağlamda adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil; telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler, IP adresi, e-posta adresi, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler kişisel veri kapsamındadır.*" Yine AYM tarafından verilen bir kararda güvenlik soruşturması ve arşiv araştırması sonucunda elde edilen bilgilerin kişisel veri olduğu belirtilmiştir²².

Kimliği belirli veya belirlenebilir olan kişiye ait mesleki alışkanlıklar ve uygulamalar, telefon bankacılığında kişinin kayıt altına alınan ses kaydı, bireylerin tanınabilir olduğu ölçüde video kaydı görüntüsü yine kişisel veriye gösterilecek başka örneklerdir²³.

Kişisel veri kapsamına kişiyle ilgili nesnel bilgiler gireceği gibi görüş ve değerlendirmeler gibi öznel değerlendirmeler de girecektir. Örneğin kişide Corona virüsünün bulunduğu dair bilgi kişinin nesnel sağlık bilgisiyken, kişinin iş yerinde işvereni ya da iş arkadaşları tarafından kişi hakkında yapılan görüş ve değerlendirmeler öznel bilgilerdir. Her iki örnekteki bilgilerin de kişisel veri sayılacağı aşıkardır. Kişisel

²⁰ **Kurum**, Örneklerle Kişisel Verilerin Korunması, Yayın No: 29, Ankara 2019, s. 50.

²¹ AYM, 09.04.2014 T., 2013/122 E., 2014/74 K., RG. 26.04.2014, S. 29072.

²² AYM, 19.02.2020 T., 2018/163 E., 2020/13 K., RG. 28.04.2020, S. 31112.

²³ **Data Protection WP**, Concept, s. 8.

veri kavramı, kişinin sadece özel²⁴ ve aile yaşamına ilişkin bilgileri değil, ayrıca kişinin sosyal, ekonomik ve çalışma yaşamına ilişkin bilgileri²⁵ de içerir. Özel hayat, Avrupa Birliği Temel Haklar Şartı²⁶ m. 7’de düzenlenirken kişisel verilerin korunması bu maddeden ayrı olarak m. 8’de düzenlenmiştir²⁷.

Gizli bilgiler kişisel veri sayıldığı gibi gizli olmayan, aleni bilgiler de kişisel veri sayılmaktadır²⁸. Örneğin kişinin gizli olan cinsel yaşam bilgileri de desteklediği futbol takımına ait kamuya açık alanda giydiği formadan tespit edilebilecek desteklediği futbol takımı bilgisi de kişisel veridir. Elbette bilgilerin gizli olması veya kişi tarafından

²⁴ “Özel hayat” kavramının geniş olarak yorumlanması gerektiğine ilişkin Avrupa İnsan Hakları Mahkemesi (“*AİHM*”) (European Court of Human Rights) kararı için bkz. [https://hudoc.echr.coe.int/tur#{"fulltext":\["Amann%20v%20Switzerland"\],"documentcollectionid2":\["GRANDCHAMBER","CHAMBER"\],"itemid":\["001-58497"\]}](https://hudoc.echr.coe.int/tur#{) (E.T.: 03.03.2020).

²⁵ “Kişisel veri” kavramının telefon koordinatları, çalışma koşulları ve hobileri de kapsayacağı ile ilgili Avrupa Adalet Divanı (“*AAD*”) (European Court of Justice) kararı için bkz. <http://curia.europa.eu/juris/document/document.jsf?text=&docid=48382&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=125691> (E.T.: 03.03.2020).

²⁶ **European Union**, “*Charter of Fundamental Rights of the European Union*”, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012P%2FTXT> (E.T.: 09.03.2020).

²⁷ **Data Protection WP**, Concept, s. 6.

²⁸ **Aksoy**, Kişisel Veri, s. 14.

alenileştirilmesi kişisel verilerin işleme şartları bakımından önem kazanacaktır²⁹.

Bilginin kişisel veri olarak sayılabilmesi için kanıtlanmış olması gerekmediği gibi doğru olması da gerekli değildir, tamamen yalan yanlış bilgiler de kişisel veri olarak kabul edilecektir. Zaten bilginin yanlış olması durumunda işlenen veri ile ilgili bilgilendirilme hakkı ve verinin düzeltilmesini talep etme hakkını³⁰ kullanabilmek için yanlış bilginin de kişisel veri olarak kabul edilmesi gerekmektedir³¹.

B. Kimliği Belirli veya Belirlenebilir Kişi (Identified or Identifiable)

İkinci unsur kişinin kimliği belirli veya belirlenebilir bir kişi olmasıdır. Bu sebeple öncelikle kişi kavramının hangi kişileri kastettiği tartışması üzerinde durulacak, sonrasında ise belirli veya belirlenebilir olma hali işlenecektir.

Kişiler hukukunda kişi, hak ehliyeti olan varlık şeklinde tanımlanır. Hak ehliyeti ise hak sahibi olabilme ve borç altına girebilme ehliyetidir. Yani kişi ile hak ehliyeti anlam olarak birbirlerine denktir³². Hak ehliyeti sahibi kişileri belirleyecek olan makam kanun koyucudur³³. Türk Medeni Kanunu ("**TMK**"), kişileri gerçek kişiler ve tüzel kişiler

²⁹ Bu hususa "*Kişisel Verilerin İşleme Şartları*" bölümünde ayrıntılı olarak değinilecektir.

³⁰ Bu hususa "*İlgili Kişinin Hakları*" bölümünde ayrıca değinilecektir.

³¹ **Data Protection WP**, Concept, s. 6.

³² **Akıntürk, Turgut/Ateş, Derya**, Medeni Hukuk, 25. Baskı, İstanbul 2019, s. 107.

³³ **Arpacı, Abdülkadir**, Kişiler Hukuku (Gerçek Kişiler), Gözden Geçirilmiş ve Genişletilmiş 2. Bası, İstanbul 2000, s. 1; **Hatemi, Hüseyin**, Kişiler Hukuku, Güncellenmiş 7. Bası, İstanbul 2018, s.1; **Helvacı, Serap**, Gerçek Kişiler, 7. Bası, İstanbul 2016, s. 21; **Helvacı, Serap/Erlüle Fulya**, Medeni Hukuk, 5. Bası, İstanbul 2018, s. 55.

olmak üzere ikiye ayırmıştır. Gerçek kişiler insanlardır. TMK m. 8'e göre "*Her insanın hak ehliyeti vardır*". Bütün insanlar kişidir ve haklara ehil olma konusunda eşittirler³⁴. Tüzel kişiler ise kendilerine ayrı bir kişilik tanınmış olan kişi ya da mal topluluklarıdır³⁵.

Hangi kişilerin kişisel verilerinin korunacağı hususu doktrinde tartışmalıdır. Bazı düzenlemeler ve yazarlar kişisel verilerin korunması kapsamında kişi kavramına sadece gerçek kişileri dahil ederken diğer görüş ise tüzel kişilerin de kişisel verilerin korunması kapsamına alınmasını iddia etmektedir. Gerçek kişilere ait bilgilerin kişisel verilerin korunması kapsamında olduğu hususunda tartışma bulunmamaktadır. Ancak tüzel kişilere ait bilgilerin kişisel verilerin korunması kapsamında sayılıp sayılmayacağı hususu net değildir.

KVKK m. 3/1/d uyarınca kişisel veri tanımında yalnızca gerçek kişilerden bahsedildiği görülür. KVKK'ya esas oluşturan OECD Rehber İlkeleri, AK 108 No.lu Sözleşme, AB Direktifi ve GDPR gibi uluslararası belgelerde de veri koruması kapsamına sadece gerçek kişilerin alınması göze çarpmaktadır. Çalışma Grubu da kişisel verinin unsurlarını sayarken gerçek kişiyi ("*natural person*") dördüncü unsur olarak kabul etmiştir. AB Direktifi'nde öngörülen korumanın gerçek kişiler için olduğu ifade edilmiştir. Buna göre kişisel verilerin korunması hakkı dünyadaki ülkelerden herhangi birindeki vatandaşlara indirgenemeyecek evrensel bir haktır³⁶. Tanımda salt gerçek kişilere değinildiği için tüzel kişiler kapsam dışında kalmaktadır. Ancak bazı durumlarda tüzel kişiler doğrudan koruma altında olmasa da dolaylı olarak koruma kapsamına

³⁴ **Helvacı**, Gerçek, s.23; **Helvacı/Erlüle**, s.55; **Kılıçoğlu, Ahmet M.**, Medeni Hukuk, Gözden Geçirilmiş-Güncellenmiş 3. Bası, Ankara 2019, s. 195.

³⁵ **Dural, Mustafa/Öğüz, Tufan**, Türk Özel Hukuku, Kişiler Hukuku, C.II, 20. Baskı, İstanbul 2019, s. 215.

³⁶ **Data Protection WP**, Concept, s. 21.

sokulabilir³⁷. Yine kişisel verilerin korunması kapsamına yalnızca gerçek kişilerin dahil olduğu, tüzel kişilerin dahil olmadığı GDPR 14. paragrafta da vurgulanmıştır.

AB 2002/58/EC sayılı Direktifi'nde³⁸ ise gerçek kişilerin yanında tüzel kişilerin de kişisel verilerin korunmasından yararlanacağı hükme bağlanmıştır³⁹. Söz konusu Direktif m. 1 uyarınca Direktif gerçek kişiler dışında tüzel kişilerin de meşru menfaatlerini korumaktadır. Ülkemizde hazırlanan “*Kişisel Verilerin Korunması Kanunu Tasarısı*”nda da ilgili kişi, “*hakkında kişisel veri işlenen gerçek ve tüzel kişi olarak*” tanımlanmıştır. Ayrıca kişisel veri “*belirli veya kimliği belirlenebilir bir kişiye ilişkin bütün bilgiler*” olarak tanımlanarak, kişisel veri tanımında gerçek kişi vurgusu yer almamıştır. Yani Tasarıya göre kişisel verilerin korunmasının kapsamına tüzel kişiler de dahildi⁴⁰. Ancak 2016 yılında yürürlüğe giren KVKK'da açıkça sadece gerçek kişilere ait bilgilerin kişisel verilerin korunmasına dahil olduğu belirtilmiştir. Bu nedenle ülkemiz hukuku bakımından tüzel kişilerin bilgilerinin koruma altına alınması söz konusu olmayacaktır.

³⁷ **Data Protection WP**, Concept, s. 23.

³⁸ **European Union**, “*Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector-Directive on Privacy and Electronic Communication*” (“*Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Özel Yaşamın Gizliliğinin Korunmasına İlişkin Direktif*”), <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN> (E.T.: 05.03.2020).

³⁹ **Başalp, Nilgün**, Kişisel Verilerin Korunması ve Saklanması, Ankara 2004, s.27.

⁴⁰ **Başalp**, s. 109.

Bir diğerk tartışmalı husus ceninin⁴¹ kişisel veri korumasından yararlanıp yararlanamayacağıdır. TMK m. 28 uyarınca “*Kişilik, çocuğun sağ olarak tamamıyla doğduğu anda başlar.*” Görüldüğü üzere kişiliğin başlangıcı için çocuk tam ve sağ doğmalıdır. Çocuk, tam ve sağ doğduktan sonra zaten veri süjesi haline gelecek ve koruma kapsamına kendiliğinden dahil olacaktır. Burada tartışmalı olan husus çocuğun ana rahmine düşmesiyle doğum anı arasındaki süreçte korumadan yararlanıp yararlanamayacağıdır. TMK m. 28/2’ye göre “*Çocuk hak ehliyetini, sağ doğmak koşuluyla, ana rahmine düştüğü andan başlayarak elde eder.*” Bu sebeple ceninin hak ehliyeti geciktirici şarta bağlıdır⁴². Söz konusu şart gerçekleşirse cenin geçmişe yönelik olarak hak ehliyetini elde edecektir. Hükmün amacı cenini korumak, gelecekte menfaat kaybına uğramasını önlemektir⁴³. Kanaatimce ceninin korunması amacı ön planla tutularak, geçmişe yönelik olarak da hak ehliyetini kazanacağını göz önüne alınarak cenine ait bilgiler kişisel veri koruma hukuku nazarında korunmalıdır. Çalışma Grubu’nun görüşüne göre⁴⁴ ise doğumdan önceki dönemde bu korumadan yararlanma hususunun tespiti için her bir devletin kendi ulusal düzenlemelerine bakmak gerekir. T.C. Anayasası 41. maddede çocuk haklarına ve korunmasına ayrı bir madde ayrılması ve yukarıda zikredilen ilgili TMK hükümleri ülkemiz hukuk sisteminin çocuğu koruma yaklaşımını göstermektedir. Bu nedenle kişisel veriyle ilgili tartışmanın da zayıf nitelikte olan çocuk lehine çözümlenmesi gerekir. Her nasıl ki çocuk tam ve sağ doğmak kaydıyla geçmişe yönelik miras hakkını elde ediyorsa veri korumasından da yararlandırılması

⁴¹ Bu konuda ayrıntılı bilgi için bkz. **Aydın Ünver, Tülay**, Ceninin Hukuki Konumu, İstanbul 2011.

⁴² **Kurt, Leyla Müjde**, “*Cenin Malvarlığı Hakları*”, İÜHFD, 2011, C. 2, S. 1, s. 183.

⁴³ **Helvacı**, Gerçek, s.30; **Helvacı/Erlüle**, s. 60; **Kılıçoğlu**, Medeni, s. 199.

⁴⁴ **Data Protection WP**, Concept, s. 23.

gerekir.

Ölülere ilişkin bilgilerin kişisel verilerin korunması kapsamında korunup korunmayacağına da değerlendirilmesi gerekmektedir. TMK m. 28'e göre "*Kişilik ölümle sona erer.*" Ölüm anından itibaren kişilik biteceği için ölü artık hak sahibi olamayacak ve borç altına giremeyecektir. Bu nedenle ölülerin bilgilerinin kişisel verilerin korunması kapsamında sayılmaması gerektiği savunulmaktadır. Medeni Hukuk'a göre ölüler artık gerçek kişi olarak sayılamayacağından bilgileri kişisel veri sayılamaz ve kişisel veri korumalarından da yararlanamazlar. GDPR 27. paragrafta da ölülerin GDPR kapsamına girmeyeceğinden bahsedilmiştir. Kural bu olmakla birlikte istisnalar mevcuttur. Ölülerin bilgileri, birtakım durumlarda, doğrudan olmasa da dolaylı yoldan korunabilir. Ölülere ilişkin bilgiler, yaşayan kişilere ilişkin bilgileri de etkileyebilir. Bu duruma bir babanın kalıtsal bir hastalık olan hemofili sebebiyle hayatını kaybettiği durum örnek olarak verilebilir. Babanın hastalık bilgisi, yaşayan çocuğunda da hemofili hastalığı olduğuna dair bir bilgi olduğundan yaşayan kişiyi etkileyebilir. İşte bu durumda, kişi ölmüş de olsa bu hastalık bilgisi kişisel veri sayılıp veri koruma kurallarından yararlanmalıdır. Yine doktorun sır saklama yükümlülüğü, hasta hayatını kaybetse dahi devam eder. Ölünün tamamen veri koruma kapsamı dışında tutulması -bu görüşe katılmamakla birlikte- kabul edilse bile kişinin onurunu koruyan ulusal mevzuat hükümleri de ölülerin anısına saygı amacıyla düzenlenmişse buna riayet edilmesi gerekir⁴⁵.

Ayrıca belirtmek gerekir ki, ölü beden üzerinde ahlaka ve kamu düzenine aykırı eylemlerde bulunulamaz⁴⁶. Ayrıca ölenin yakınlarının ve mirasçılarının ölü üzerinde kendilerine özgü kişisel hakka sahip olduğu ve bu hakkın korunması gerektiği de öne

⁴⁵ **Data Protection WP**, Concept, s. 22.

⁴⁶ **Arpacı**, s.187.

sürülmektedir. Kişilik ölümle son da bulsa ölenin insanlık değeri gereği en azından saygı görme hakkı olmalıdır⁴⁷.

Kişinin birçok kişi içinde diğer kişilerden ayırt edilebilmesi kişinin kimliğinin belirli olması olarak ifade edilebilir. Kişi henüz tam olarak ayırt edilemese de daha sonrasında ayırt edilebilmesi mümkünse bu durumda kimliği belirlenebilir kişi olarak adlandırılır. TDK kimliği “*toplumsal bir varlık olarak insanın nasıl bir kimse olduğunu gösteren belirti, nitelik ve özelliklerin bütünü*” olarak tanımlamıştır⁴⁸. Buna kişinin boyu, kilosu, dış görünüş özellikleri, giyimi kuşamı, mesleği, ünvanı, adı gibi bir hayli şey örnek olarak verilebilir⁴⁹.

Bir kişi doğrudan doğruya adı ve soyadı ile belirlenebileceği gibi dolaylı olarak T.C. kimlik numarasıyla, mailiyle, arabasının plakasıyla, telefon numarasıyla veya kişinin ait olduğu özellikler (medeni durumu, yaşı, cinsiyeti) daraltılarak belirlenebilir. Eldeki bilgilerin kişiyi belirli kılıp kılmaması somut duruma göre değerlendirilmelidir. Örneğin yaygın bir soyadı ülkede genelinde birini belirlemek için yeterli olmazken küçük bir arkadaş grubunda yeterli olacaktır. Kişinin direkt olarak belirlenmesi genelde isim bilgisiyle mümkün olmaktadır. Dolaylı olarak tanımada ise bilgilerin her biri tek başına kişiyi belirlemede yeterli olmasa da hepsi bir araya gelerek kişi belirlenebilir. Yukarıda kişisel veri tanımında belirtilen “*fiziksel, fizyolojik, genetik, ruhsal, ekonomik, kültürel veya toplumsal kimliğine özgü bir ya da daha fazla sayıda faktör*” işte tam olarak da bunu kastetmektedir. Burada yazılan faktörler tek başına bir kişiyi belirlemede yeterli olmasa

⁴⁷ **Arpacı**, s.187; **Hatemi**, s. 86; **Helvacı**, Gerçek, s. 137; Bu konu hakkında detaylı bilgi için bkz. **Petek, Hasan**, Kişilik Değerlerinin Ölümden Sonra Korunması, Ankara 2015.

⁴⁸ **TDK**, <https://sozluk.gov.tr> (E.T.: 04.03.2020).

⁴⁹ **Data Protection WP**, Concept, s. 12.

da hepsi ya da birkaçı birleşerek kişi tespit edilebilir⁵⁰.

Genel olarak kişi isim bilgisiyle belirlenebilse de kişinin tespiti için her zaman isim bilgisine ihtiyaç duyulmamaktır. Bir kişiyi diğerlerinden ayırmak için başka belirleyiciler de vardır⁵¹. Örneğin bir hapisanede gerçek isimlerini gizleyen mahkumlardan her birine sayılardan oluşan bir kod numarası tahsis edilmiştir. Her bir mahkumun fotoğrafları ve fiziksel özellikleri de bu kod numarasıyla ilişkilendirilmiştir. Normal şartlarda hiçbir öneme ve belirleyici bir özelliğe sahip olmayan sayılar, söz konusu durumda her bir mahkumu diğer mahkumlardan ayırt etmeye ve onun kimliğini belirli kılmaya yol açtığı için kişisel veri olarak kabul edilmelidir.

Kişinin mahlası (takma ad) ya da lakabının da kişisel veri sayılıp sayılmayacağı hususunu incelemek gerekir. Mahlas ya da lakap direkt olarak ya da başka verilerle birleşerek kişi tanımlanabiliyorsa söz konusu mahlas ve lakap kişisel veri kabul edilir⁵². Burada yeri gelmişken takma ad ile anonim veri arasındaki farka değinmek gerekir. İleride de detaylı bir şekilde inceleyeceğimiz anonim veriler, kişisel veri olarak kabul edilmezken, takma adlar veri koruma yasasına tabi olacaktır. Çünkü takma ad ile kişi arasında bağlantı kurulabilme ihtimali vardır⁵³.

C. Bilginin Kişiyi İlişkin Olması (Relating to)

Genel itibarıyla bilginin bir kişiyle ilgili olduğu zaman o kişiyle “*ilişkili (relate)*” olduğu akla gelebilir. Bilgiler bir kişinin kimliğine, karakterine, hislerine veya

⁵⁰ **Data Protection WP**, Concept, s. 13.

⁵¹ **Data Protection WP**, Concept, s. 14.

⁵² **Kurum**, Örnekler, s. 4.

⁵³ **Kuner, Christopher**, European Data Protection Law (Corporate Compliance and Regulation), Second Edition, Oxford 2007, s. 66.

davranışlarına atıfta bulunuyorsa o kişiyle ilgilidir⁵⁴. Birçok halde söz konusu ilişki kolayca kurulabilir. Örneğin bir kişinin çalıştığı yerde onun hakkında kaydedilen bilgiler ve kayıtlar kişinin çalışma durumu ile açıkça ilgilidir. Yine hastanede hastaya yapılan testler sonucunda teşhis edilen hastalık bilgisinde de kişiye ilişkin olma unsuru belirgindir. Bunun yanında bilgilerin kişiyle bağlantısının açıkça anlaşılmadığı durumlar da söz konusu olabilir. Kimi durumlarda bilgiler doğrudan kişilerle değil, ilk etapta nesnelerle ilgilidir ve bu durumlarda kişinin bilgiyle ilişkisi dolaylı olarak kurulur. Örneğin bir arabanın bedeli nesneyle ilgili bir bilgidir. Söz konusu bilgi ülkedeki araba piyasa fiyat tespiti için kullanılıyorsa veri koruma kuralları açıkça uygulanmaz. Ancak kişiyle dolaylı da olsa ilgi kurulabildiği ölçüde arabanın bedeli bilgisi kişisel veri kapsamına dahil olacaktır. Bu duruma, arabanın bedeli bilgisinin araba sahibi kişinin arabadan kaynaklanan vergi yükümlüğünün tespiti için kullanılması durumu örnek olarak gösterilebilir⁵⁵.

Bir bilginin kişiyle ilişkili olup olmadığı; içerik, amaç veya sonuç olarak üç unsurun varlığına bağlı olarak tespit edilebilir. Bu unsurlar seçimlik unsurlar olup üçünden birinin olması yeterlidir. Başka bir ifadeyle, kişi ile bilgi arasında ilişki kurulabilmesi için her üç unsurunda bir arada olması gerekmez⁵⁶.

İçerik unsurunun tespiti kolaydır. Zira içerik açısından bilgi ile kişi arasında ilişki kurulabilmesi için söz konusu bilginin kişi “*hakkında (about)*” olması gerekir. Misalen bir giyim mağazasının müşterisiyle ilgili dosyasında müşteriyle ilgili yer alan bilgiler

⁵⁴ **Data Protection WP**, Working Document on Data Protection Issues Related to RFID technology, s.8. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp105_en.pdf (E.T.: 04.03.2020).

⁵⁵ **Data Protection WP**, Concept, s. 9.

⁵⁶ **Data Protection WP**, Concept, s. 10.

müşteri hakkında olduğu için içerik unsuru açısından bağlantı kurulup bu bilgiler kişisel veri sayılacaktır⁵⁷. Yine internet üzerinden satın alınan opera konser bileti için girilen bilgiler açıkça izleyiciye ait bilgiler içerdiği ve bilgilerin izleyici hakkında olduğu kolayca tespit edilebildiği için içerik unsuru bakımından bilgi ile kişi arasında ilişki kurulur. Yani bir bilgi içerik olarak kolayca kişi ile ilişkilendirilebiliyorsa bu unsurun varlığından söz edilir.

Bilgi ile kişi arasındaki ilişki amaç unsurundan da kaynaklanabilir. Burada bilginin hangi “*amaçla (purpose)*” tutulduğu önemlidir⁵⁸. Örneğin üniversitenin güvenliğini sağlamak için çıkış kapılarına konulan kartlı giriş-çıkış sistemi, çalışanların çalışma saatlerinin tespiti amacıyla kullanılırsa çalışanlar açısından kişisel veri olarak kabul edilecektir.

Bilgi ile kişi arasındaki bağlantıyı belirlemede kullandığımız ve tespiti diğerlerine göre daha zor olan unsur, sonuç unsurudur. İçerik ve amaç unsuru olmamasına rağmen, somut olayın tüm şartları dikkate alındığında netice itibarıyla söz konusu bilgi kişinin haklarına “*etki (impact)*” yapıyorsa bu unsurun varlığından söz edilir. Sonucun çok büyük olması önem teşkil etmez. Önemli olan bu bilgilerin işlenmesi durumunda kişinin aynı şartlardaki diğer kişilerden farklı bir muameleye tabi tutulabilme ihtimalidir⁵⁹. Yukarıdaki örnekte çalışanların üniversiteye giriş yapabilmeleri için kartlı geçiş sisteminden geçmeleri gerçekten de üniversitenin güvenliğini sağlamak amacıyla kullanılsa bile sonuç itibarıyla elde edilen bilgiyle işe giriş-çıkış saatleri de tespit edilebildiğinden bu bilgilerin de kişi ile ilişkilendirilerek kişisel veri olduğu belirlenebilir.

⁵⁷ **Data Protection WP**, Concept, s. 10.

⁵⁸ **Data Protection WP**, Concept, s. 10.

⁵⁹ **Data Protection WP**, Concept, s. 10.

III. Özel Nitelikli (Hassas) Kişisel Veriler

Çeşitli düzenlemelerde “*hassas veri (sensitive data)*”, “*özel nitelikli veri*” veya “*özel koruma gerektiren veri*” olarak adlandırılan bu veriler, yapısı gereği kişilerin temel hak ve özgürlüklerini ihlal edebilecek düzeydedir. Bu nedenle özel olarak korunmaları gerekmektedir. Hukuki düzenlemelerde özel nitelikli kişisel verilerin tanımı yapılmamış, hangi tür verilerin bu kategoriye gireceği sayma yoluyla tespit edilmiştir⁶⁰.

Özel nitelikli kişisel veriler KVKK m. 6/1’de “*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*” olarak sayılmıştır. İlgili hüküm incelendiğinde hassas verilerin sınırlı sayma yoluyla⁶¹ belirlendiği görülmektedir. Bu sebeple KVKK m. 6’da yazmayan bir kişisel veri, özel nitelikli kişisel veri kategorisine dahil edilemez. Burada sayılmayan her türlü veri özel nitelikli olmayan (genel nitelikli) kişisel veri sayılacaktır.

Kanuna göre özel nitelikli sayılan veriler incelendiğinde bu verilerin yapısı gereği hassas olduğu görülecektir. Bu verilerin hassaslığı veri sahibi dışındaki kişilerin bilgi sahibi olması durumunda ilgili kişinin zarar görme, dışlanma ya da ayrımcılığa maruz kalma ihtimalinden kaynaklanmaktadır. Bu husus KVKK m. 6 gerekçesinde “*Bu verilerin, başkaları tarafından öğrenildiği takdirde ilgili kişinin mağdur olabilmesine veya ayrımcılığa maruz kalabilmesine neden olabilecek nitelikte veriler olmaları dikkate alınmakta, bu sebeple bu tür veriler özel nitelikli (hassas) veri olarak kabul*

⁶⁰ Aksoy, Kişisel Veri, s. 30.

⁶¹ Günümüz teknolojik ilerleme hızı karşısında yeni hassas veri türleri çıkabileceği ve bu nedenle hassas verilerin sınırlı sayma yoluyla tespitinin eleştirisi için bkz. Aksoy, Kişisel Veri, s. 32.

edilmektedir.” şeklinde ifade edilmiştir. Tüm bu nedenlerle de kanun koyucu KVKK m. 6’da özel nitelikteki kişisel verilerin işleme şartlarını diğer kişisel veri işleme şartlarından (KVKK m. 5) ayrı olarak düzenlenmiştir. Bu husus kişisel verilerin işleme şartları başlığında ayrıntılı olarak incelenecektir.

Kişinin uçak bileti alırken belirttiği, dini inancını gösteren yemek seçimi bilgisi hassas veriye örnek olarak verilebilir⁶². Kişiyle ilgili din veya mezhep bilgileri doğası gereği hassastır. Misalen ceza mahkumiyetine ilişkin veriler, kişinin işe giriş aşamasında sonucu etkileyebilecektir. Zira bu veri, narin bir veridir. Bu veriye müdahale edilmesi, işlenmesi kişinin haksızlığa uğramasına sebep olabilir. Bu nedenle ceza mahkumiyetine ve güvenlik tedbirlerine ilişkin veriler, hassas kişisel veri sayılmıştır.

Keza kişinin sağlığı⁶³ ve cinsel hayatı ile ilgili bilgiler çok narindir. Bu bilgilerin 3. kişiler tarafından bilinmesi kişi açısından olumsuz sonuçlar doğurabilir. Bu verilerin genel nitelikteki verilerle aynı koruma değerine tabi tutulması mantık kurallarıyla bağdaşmamaktadır.

Hassas veriler KVKK’da sayılmakla birlikte, sayılan verilerin tanımına yer verilmemiştir. Bu nedenle özellikle sağlık verileri, genetik ve biyometrik veriler gibi teknik anlamı olan verilerin tanımlarının yapılması gerekmektedir. Zira bir verinin hassas veri kategorisinde olup olmadığını belirleyebilmek için hassas veri türlerinin tam olarak açıklığa kavuşturulması gereklidir.

⁶² **Kaya, Cemil**, “*Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi*”, İÜHFİM, 2011, C. 69, S. 1-2, s. 322.

⁶³ Kişisel sağlık verileri, kişinin fiziksel veya ruhsal sağlığıyla ilgili her türlü bilgidir. GDPR, 35. paragraf.

GDPR’a göre kişisel sağlık verisi (*data concerning health*), kişinin fiziksel veya ruhsal sağlığıyla ilgili her türlü bilgidir⁶⁴. “*Kişisel Sağlık Verileri Hakkında Yönetmelik*”⁶⁵ kişisel sağlık verisini tanımlamıştır. Buna göre, “*Kişisel sağlık verisi, kimliği belirli veya belirlenebilir gerçek kişinin fiziksel ve ruhsal sağlığına ilişkin her türlü bilgi ile kişiye sunulan sağlık hizmetleriyle ilgili bilgileri ifade eder.*”

Genetik veri (*genetic data*), “*Gerçek kişinin fizyolojisi ya da sağlığı hakkında benzersiz bilgi veren ve özellikle söz konusu kişiden alınan bir biyolojik numunenin analizinden kaynaklanan ve söz konusu kişinin kalıtsal özellikleri ile ilgili kişisel verilerdir.*”⁶⁶ Biyometrik veri (*biometric data*) ise “*Gerçek kişinin fiziksel, fizyolojik veya davranışsal özelliklerine ilişkin olan, yüz görüntüleri gibi gerçek kişinin benzersiz olarak tanınmasını sağlayan, özel teknik işlemeden kaynaklanan kişisel verilerdir.*”⁶⁷

§2. Kişisel Verilerin Hukuki Niteliği

I. Genel Olarak

Kişisel verilerin nasıl korunacağını belirlemek için öncelikle hukuki niteliğinin tespit edilmesi önem arz etmektedir. Bu tespit kişisel verilerin korunmasının özünü oluşturan hakkın belirlenmesinden ibarettir. Söz konusu görüşler; “*mülkiyet hakkı görüşü*”, “*fikri hak görüşü*” ve “*kişilik hakkı görüşü*” olarak sayılabilir. Çalışmanın sınırlarını aşmamak için burada hukuki nitelik ile ilgili görüşlere genel olarak yer verilecek

⁶⁴ GDPR, m. 4/15.

⁶⁵ RG. 21.06.2019, S. 30808.

⁶⁶ GDPR, m. 4/13.

⁶⁷ GDPR, m. 4/14.

ve genel kabul gören görüş saptanacaktır⁶⁸.

II. Mülkiyet Hakkı Görüşü

“Mülkiyet hakkı görüşü”⁶⁹ genel olarak Amerikan Hukuku’nda kabul edilmektedir⁷⁰. Bu görüşü destekleyenler, kişisel verinin temelinde mülkiyet hakkının yer aldığını öne sürmektedir.

Mülkiyet hakkı, kişiye en geniş yetkileri sağlayan bir ayni haktır⁷¹. Ayni haklar, tam ve sınırlı olmak üzere ikiye ayrılmaktadır. Tam ayni hak, mülkiyet hakkıdır. Zira

⁶⁸ Hukuki niteliğin saptanması ile ilgili görüşler hakkında detaylı bilgi için bkz. **Aksoy**, Kişisel Veri, s. 37-72; **Küzeci**, s. 58 vd.; **Taştan, Furkan Güven**, Türk Sözleşme Hukukunda Kişisel Verilerin Korunması, İstanbul 2017, s. 51-66.

⁶⁹ **Bartow, Ann**, “*Our Data, Ourselves: Privacy, Propertization and Gender*”, University of San Francisco Law Review, 2000, C. 34, s. 633; **Janger, Edward J.**, “*Privacy Property, Information Costs and the Anticommons*”, Hastings Law Journal, 2003, C. 54, S. 4, s. 899; **Kang, Jerry**, “*Information Privacy in Cyberspace Transactions*”, Stanford Law Review, 1998, C. 50, s. 1246; **Litman, Jessica**, “*Information Privacy/Information Property*”, Stanford Law Review, 2000, C. 52, s. 1283; **Prins, Corien**, “*When personal data, behavior and virtual identities become a commodity: Would a property rights approach matter?*”, SCRIPT-ed, 2006, C. 3, S. 4, s. 270; **Prins, J.E.J.**, “*The Propertization of Personal Data and Identities*”, Electronic Journal of Comparative Law, 2004, C. 8, S. 3, s. 1.

⁷⁰ **Aksoy**, Kişisel Veri, s. 57.

⁷¹ **Keskin, A. Dilşad/Demircioğlu, H. Reyhan**, Medeni Hukuk-II (Eşya Hukuku – Miras Hukuku), Ankara 2018, s. 83; **Sirmen, A. Lale**, Eşya Hukuku, 6. Baskı, Ankara 2018, s. 29.

mülkiyet hakkı, aynı hakkın bütün özelliklerini barındırma bakımından tektir. Mülkiyet hakkından başka tam aynı hak bulunmamaktadır⁷². Bu nedenle mülkiyet hakkı, “*aynı hakların en mükemmeli*” olarak ifade edilmektedir⁷³. Mülkiyet hakkı mutlak bir haktır⁷⁴. Mülkiyet hakkı, sahibine eşya üstünde tam bir hakimiyet hakkı sağlamaktadır. Mülkiyetin sağladığı yetkiler; “*kullanma yetkisi*”, “*yararlanma yetkisi*” ve “*tasarruf yetkisi*” olarak sayılabilir⁷⁵. Bu görüşü savunanlara göre kişinin, verileri üzerinde mülkiyet hakkı bulunmaktadır⁷⁶. Buna göre kişiler, kişisel verileri üzerinde tasarrufta bulunma, kullanma ve yararlanma haklarına sahip olacaklardır⁷⁷. “*Verilerin mülkleştirilmesini*”⁷⁸ destekleyen söz konusu görüşe göre, kişiler, kişisel verilerini “*adil bir bedel*”⁷⁹ karşılığında satabilmelidir⁸⁰. Yeni dönemde kişisel verilerin parasal değeri son derece yükselmiştir ve yükselmeye de devam etmektedir. Şirketler kişisel verileri kendi şirket faaliyetlerinde kullanarak yarar sağladıkları gibi bu verileri başkalarına satarak da ciddi

⁷² **Ünal, Mehmet/Başpınar, Veysel**, Şekli Eşya Hukuku, Güncellenmiş ve Genişletilmiş 8. Baskı, Ankara 2016, s. 61.

⁷³ **Akipek, Jale/Akıntürk Turgut/Ateş, Derya**, Eşya Hukuku, 2. Baskı, İstanbul 2018, s. 19.

⁷⁴ **Serozan, Rona**, Eşya Hukuku I, Genişletilmiş 3. Bası, İstanbul 2014, s. 202.

⁷⁵ **Akipek/Akıntürk/Ateş**, s. 380; **Antalya, O. Gökhan/Topuz, Murat**, Eşya Hukuku, C. IV/1, Genişletilmiş 3. Baskı, Ankara 2019, s. 110; **Sirmen**, s. 29.

⁷⁶ **Prins, Corien**, s. 278.

⁷⁷ **Taştan**, s. 52.

⁷⁸ **Küzeci**, s. 60.

⁷⁹ **Prins, J.E.J.**, s. 1.

⁸⁰ **Kang**, s. 1256.

anlamda gelir elde edebilmektedir⁸¹. Son teknolojilerle birlikte kişisel verilerin toplanması çok masrafsız hatta bedelsiz hale gelmiştir. Nitekim veri toplayanlar bu verilerden bir kazanç elde etmekte ancak karşılığında bir bedel vermemekte ya da çok az bir bedel vermektedir. Bu görüşe göre kişisel verileri işleyen şirketler kişisel veri için veri sahibine uygun bir bedel ödemek zorunda olursa daha az veri işlemeyi tercih edebilirler. Başka bir ifadeyle söz konusu görüş savunucuları, veri işleyen şirketlerin bedel ödememek için daha az veri işleyeceklerini ve bunun sonucunda kişisel verilerin korunmuş olacağını iddia etmektedir⁸². Ayrıca mülkiyet hakkının kabulüyle kişisel verilerin, verileri toplayanlara değil ilgili kişilere ait olduğunun netlik kazanacağı öne sürülmüştür⁸³.

Bu görüşe göre, kişisel verileri işlemek için veri sahibine “*adil bir bedel*” verilmesi gerektiğinden yukarıda bahsettik. Söz konusu görüşe yönelik ilk eleştiri bu konuyla ilgilidir. Zira veri sahibi ile veri sorumluları arasında “*verinin satışıyla ilgili pazarlıkta*” adaletsiz durumlar ortaya çıkabilir. Her iki tarafın pazarlık gücünün eşit olduğundan söz edilemez⁸⁴. Gerçekten de çoğu zaman veri işlenmesi faaliyetinin her iki tarafı eşit şartlara haiz değildir⁸⁵. Çoğu zaman veri sahibi daha güçsüz ve tecrübesizdir.

⁸¹ **Schwartz, Paul M.**, “*Property, Privacy and Personal Data*”, Harvard Law Review, 2004, C. 117, S. 7, s. 2056-2057; **Aksoy**, Kişisel Veri, s. 57-58. Söz konusu görüş kişisel verilerin son dönemde “*ticari değer*” haline gelmesini temel almaktadır. **Aksoy**, Kişisel Veri, s. 64.

⁸² **Aksoy**, Kişisel Veri, s. 59.

⁸³ **Prins, Corien**, s. 279.

⁸⁴ **Bibas, Steven A.**, “*A Contractual Approach to Data Privacy*”, Harvard Journal of Law & Public Policy, 1994, C. 17, S. 2, s. 605-606.

⁸⁵ **Küzeci**, s. 61.

Özellikle karşı tarafta güçlü şirketler, kamu kuruluşları veya işveren olduğunda pazarlık şansı olmayacak ve göstermelik bir bedel ödenebilecektir. Bu da veri sahibi kişinin menfaatine aykırı bir durum teşkil edecektir.

Söz konusu görüşe getirilen temel eleştiri ise mülkiyet hakkının muhtevasının kişisel verilerle bağdaşmayacağı eleştirisidir. Mülkiyet hakkının sahibine tanıdığı yetkiler ikiye ayrılabilir. Bunlardan ilki mülkiyet hakkının sahibine, direkt eşya üstünde bazı yetkiler tanınmasıdır. Bir diğeri ise mülkiyet hakkının malike, 3. kişilere karşı ileri sürebileceği bazı yetkilere⁸⁶. Hakikaten mülkiyet hakkı malikin *“olumlu yetki”* ve *“koruyucu yetki”* olarak iki tane yetkisi vardır. Olumlu yetki, TMK m. 683/1’de yer bulmuştur. Buna göre, *“Bir şeye malik olan kimse, hukuk düzeninin sınırları içinde, o şey üzerinde dilediği gibi kullanma, yararlanma ve tasarrufta bulunma yetkisine sahiptir.”* Koruyucu yetki ise TMK m. 683/2’de hüküm altına alınmıştır. Buna göre, *“Malik, malını haksız olarak elinde bulunduran kimseye karşı istihkak davası açabileceği gibi, her türlü haksız elatmanın önlenmesini de dava edebilir.”* Koruyucu yetki, 3. kişilere karşı eşyanın korunması imkanını verir. Olumlu yetki ise; malikin mülkiyete konu olan şey üzerindeki kullanma, yararlanma ve tasarrufta bulunma yetkisine sahip olması anlamına gelir⁸⁷. Tasarruf yetkisi olan malik mülkiyet hakkını diğer bir kişiye temlik edebilir⁸⁸. Özellikle tasarruf yetkisinin kişisel verilerle uyuşmadığı görülmektedir. Nitekim söz konusu görüşün kabul edilmesi halinde, kişinin kişisel verileri üzerinde tasarruf yetkisi olacaktır.

⁸⁶ **Ayan, Mehmet**, Eşya Hukuku-II-Mülkiyet, Güncelleştirilmiş 9.Baskı, Ankara, 2016, s. 29.

⁸⁷ **Nomer, Haluk Nami/Ergüne, Mehmet Serkan**, Eşya Hukuku, Gözden Geçirilmiş 7. Bası, İstanbul 2019, s. 188; **Sirmen**, s. 245.

⁸⁸ **Ertas, Şeref**, Eşya Hukuku, Gözden Geçirilmiş ve Genişletilmiş 14. Baskı, İzmir 2018, s. 215.

Buna göre, kişiden kişisel verileri satın alındıktan sonra söz konusu veriler 3. bir kişiye devredilebilecektir. Bu da veri sahibi kişinin, kişisel verilerinin istemediği kişilere kolaylıkla geçebilmesi sonucunu doğurur. Sonuç olarak bu görüşün “*kişi*” ve “*veri*” arasındaki bağı koparacağı tespiti yapılabilir⁸⁹.

Kanaatimce kişisel verilerin mülkiyet hakkı kapsamında değerlendirilmesi bir başka açıdan da sıkıntılı görünmektedir. Zira mülkiyet hakkı, bir ayni haktır. Kural olarak ayni hak eşya üzerinde kurulabilir. Eşya, duyu organlarıyla kavranabilen cismani bir varlıktır⁹⁰. Bu nedenle kural olarak ayni hakkın konusunu maddi şeyler oluşturmaktadır. İstisna olarak kanunda bazen maddi olmayan şeyler de bu konuya dahil olabilmektedir⁹¹. Yani mülkiyet hakkının konusunu eşya oluşturmaktadır⁹². Kişisel veriler, cismani olmadığından eşya kapsamında değerlendirilemez. Ayrıca kişisel verilerle ilgili olarak kanunda yukarıda belirttiğimiz gibi bir istisna da tanınmamıştır.

III. Fikri Hak Görüşü

Fikri hak, “*insan aklının ve zekasının ürünü olan maddi olmayan değerler üzerindeki mutlak nitelikte bir hak*”⁹³ şeklinde tanımlanabilir⁹⁴. Kişisel verilerin hukuki niteliği tartışmasında ortaya atılan bir başka görüş, “*fikri hak*” görüşüdür⁹⁵. Bu görüşe

⁸⁹ Aksoy, Kişisel Veri, s. 64-65.

⁹⁰ Ünal/Başpınar, s. 15.

⁹¹ Ünal/Başpınar, s. 30.

⁹² Nomer/Ergüne, s. 187.

⁹³ Arbek, Ömer, Fikir ve Sanat Eserlerine İlişkin Lisans Sözleşmesi, Ankara 2005, s. 45.

⁹⁴ Bu görüşün temelini oluşturan fikri mülkiyet ile ilgili detaylı bilgi için bkz. Tekinalp, Ünal, Fikri Mülkiyet Hukuku, Güncelleştirilmiş ve Genişletilmiş 5. Bası, İstanbul 2012.

⁹⁵ Bartow, s. 684.

göre, fikri hak ile kişisel verilerin korunması arasında amaç yönünden benzerlik vardır. Buna göre, her iki hakkın da korunma maksadı asıl olarak bilginin dağıtımını ve kullanımını korumaktır⁹⁶. İki hak arasında kimi benzerlikler bulunsa da söz konusu haklar genel anlamda ayrılmaktadır. Yani kişisel verilerin korunması ile fikri mülkiyet arasında bir ilişki vardır. Ancak kişisel verilerin korunması doğrudan fikri mülkiyetin kapsamında değerlendirilmemektedir⁹⁷. Söz konusu farklılık özellikle “*irade*” hususunda ortaya çıkmaktadır. Fikri ürünler insan iradesi sonucu üretilmektedir⁹⁸. Yani insanların fikri çabası sonucunda fikri ürün ortaya çıkmaktadır. Ancak kişisel verilerin çabalarımızın ürünü olduğu öne sürülemez. Zira kişisel veriler iradi olarak oluşmaktan ziyade belirli davranışlar veya tercihler sonucunda kişinin doğal mevcudiyetinden ortaya çıkmaktadır⁹⁹. Bu nedenlerle fikri hak görüşünün de kişisel verilerin hukuki niteliği tam olarak ifade ettiği söylenemez¹⁰⁰.

Ayrıca belirtmek gerekir ki, mülkiyet hakkı görüşü de fikri hak görüşü de kişisel verilerin metalaştırılmasına yol açacağı sebebiyle eleştirilmektedir. Nitekim her iki görüş de veri sahibinden çok veri işleyenlerin çıkarlarına hizmet etmektedir¹⁰¹.

Anglo-Amerikan hukuk sisteminde kişisel veri, mülkiyet hakkı ve fikri hak ile bağlantılı görülürken Kıta Avrupası, kişisel verileri kişilik hakkı ile

⁹⁶ **Prins, Corien**, s. 279.

⁹⁷ **Tekinalp**, s. 3.

⁹⁸ **Arbek**, s. 44.

⁹⁹ **Prins, Corien**, s. 296.

¹⁰⁰ Fikri hak görüşüne ilişkin diğer eleştiriler için bkz. **Aksoy**, Kişisel Veri, s. 66-67.

¹⁰¹ **Aksoy**, Kişisel Veri, s. 69.

ilişkilendirmektedir¹⁰². Bu nedenle kişilik hakkı görüşü de detaylı bir şekilde incelenmelidir.

IV. Kişilik Hakkı Görüşü

Kişisel verilerin hukuki niteliğine ilişkin en çok tartışılan ve üzerinde durulan görüş, “*kişilik hakkı görüşü*”dür. Bu görüşün varyasyonları ileride incelenecektir. Ancak konunun daha net anlaşılması için öncelikle “*kişilik hakkı*” kavramının irdelenmesi elzemdir.

Yargıtay’ın da belirttiği gibi¹⁰³ “*Kanunda kişilik hakkının tanımı yapılmadığı gibi, nelerin kişilik haklarına dahil olduğunu da belirtmemiştir.*” Yargıtay’ın başka bir kararına göre¹⁰⁴, “*Şüphesiz, yapılan tanımlamaların hepsi kişilik hakkını değişik yönden anlatmaktadır. Ancak, çok genel bir ifadeyle, kişilik hakkı, kişinin, kişisel değerleri üzerinde sahip olduğu mutlak ve tekelci haktır, şeklinde kısa ve öz bir tanımlama da yapılabilir.*” Doktrinde çeşitli tanımlar yapılmıştır. Kişilik hakkı, kişiliği oluşturan değerlerin tamamının üstündeki hak olarak tanımlanabilir¹⁰⁵. Söz konusu değerler, gerçek kişiler için sağ ve tam doğumla kazanılır. Tüzel kişilerde ise hak ehliyetine sahip olmakla

¹⁰² **Aksoy, Hüseyin Can**, “*The Right to Personality and Its Different Manifestations as the Core of Personal Data*”, Ankara Law Review, 2008, C. 5, S. 2, s. 236.

¹⁰³ Yargıtay 13. HD., 26.05.2016 T., 2015/4104 E., 2016/13597 K. (Kazancı, E.T.: 17.04.2020).

¹⁰⁴ Yargıtay HGK., 27.06.2012 T., 2012/4-179 E., 2012/412 K. (Kazancı, E.T.: 17.04.2020).

¹⁰⁵ **Helvacı, Serap**, Türk ve İsviçre Hukuklarında Kişilik Hakkını Koruyucu Davalar, İstanbul 2001, s. 41; **Zevkliler, Aydın/Acabey, M. Beşir/Gökyayla, K. Emre**, Medeni Hukuk, Gözden Geçirilmiş ve Genişletilmiş 6. Baskı, Ankara 2000, s. 395.

kazanılır¹⁰⁶. Yine kişilik hakkı, “*kişinin toplum içindeki saygınlığını ve kişiliğini serbestçe geliştirmesini sağlayan varlıkların tümü üzerindeki hak*” olarak da tanımlanabilir¹⁰⁷.

Kişilik hakkına dahil olan değerlerin tespit edilmesi gerekmektedir. TMK m. 24 incelendiğinde bu değerlerin sınırlı sayma yoluyla belirlenmediği gözlemlenmektedir. Bu hüküm çerçeve bir hükümdür. Söz konusu değerlerin tek tek sayılması mümkün değildir¹⁰⁸. TMK’da tek tek belirlenmediğinden kişilik hakkına konu olan değerlerin tespitini yapacak olan hakimdir¹⁰⁹. Kişisel değerlerin içeriği zamana ve yere göre dönüşmektedir¹¹⁰. Zira güncel gereksinimler yeni değerleri şekillendirmektedir. Hızla gelişen ve dönüşen, toplum ve teknoloji karşısında bu değerlerin sınırlandırılmamış olması yerindedir¹¹¹. Aksi halde kanun yeni ihtiyaçlara cevap veremeyeceğinden sürekli olarak değiştirilmesi gerekecektir. Zira dün kişilik hakkı kapsamında değerlendirmedığımız yahut adını bile bilmediğimiz bir değer, yarın kişilik hakkına konu oluşturabilecektir.

¹⁰⁶ **Helvacı**, Gerçek, s. 101-102.

¹⁰⁷ **Dural/Öğüz**, s. 100.

¹⁰⁸ **Yavuz, Nihat**, Borçlar Hukuku El Kitabı, Ankara 2018, s. 257.

¹⁰⁹ **Dural/Öğüz**, s. 101; **Helvacı**, Gerçek, s. 103; **Kılıçoğlu, Ahmet M.**, Şeref, Haysiyet ve Özel Yaşama Basın Yoluyla Saldırlardan Hukuksal Sorumluluk, Yeniden Gözden Geçirilmiş, Güncelleştirilmiş 4. Bası, Ankara 2013, s. 5.

¹¹⁰ **Erlüle, Fulya**, Türk Borçlar Kanunu’na Göre Bedensel Bütünlüğün İhlalinde Manevi Tazminat, Gözden Geçirilmiş 2. Baskı, Ankara 2015, s. 90.

¹¹¹ **Helvacı**, Koruyucu Davalar, s. 44.

Kişilik hakkı, herkese karşı ileri sürülebilen mutlak bir haktır¹¹². Kişilik hakkı gereğince her kişinin başkalarının kişiliğine saygı göstermesi gerekmektedir¹¹³. Yani bu hak, kişilik hakkı sahibine hakkın korunması yetkisi verir. Aynı zamanda diğer kişilere de kişinin bu hakkına saygı duyma zorunluluğu yüklemektedir¹¹⁴.

Kişilik hakkı, malvarlığı haklarına değil, şahıs varlığı haklarına dahildir. Zira kişilik hakkına konu değerler para ile ölçülemez¹¹⁵. Ancak bu husus bu hakka yapılan saldırıların asla malvarlığını etkilemeyeceği olarak anlaşılmamalıdır. Nitekim kişilik hakkına karşı yapılan saldırılar malvarlığını ekonomik yönden zarara uğratabilmektedir¹¹⁶. Kişilik hakkı, kişiye sıkı sıkıya bağlı bir haktır¹¹⁷. Bu nedenle söz konusu hakkı yalnızca hakkın sahibi kullanabilir¹¹⁸. Bu haktan vazgeçilemeyeceği gibi

¹¹² **Tekinay, Selahattin Sulhi**, Medeni Hukukun Genel Esasları ve Gerçek Kişiler Hukuku, Gözden Geçirilmiş İlaveli 6. Bası, İstanbul 1992, s. 249; Yargıtay 11. HD., 31.03.2005 T., 2004/4866 E., 2005/3085 K. (Kazancı, E.T.: 17.04.2020).

¹¹³ **Zevkliler/Acabey/Gökyayla**, s. 398.

¹¹⁴ **Ayan, Mehmet/Ayan Nurşen**, Kişiler Hukuku, Gözden Geçirilmiş 8. Baskı, Ankara 2016, s. 87.

¹¹⁵ **Dural/Öğüz**, s. 103; **Helvacı**, Gerçek, s. 105.

¹¹⁶ **Helvacı**, Koruyucu Davalar, s. 47.

¹¹⁷ “Medeni hukuk kapsamında kişilik hakları, kategorik anlamda mutlak haklar içinde yer alan, her zaman varolan, zamanla tükenmeyen, herkese karşı ileri sürülebilen, çoğu zaman kişiye sıkı sıkıya bağlı ve devredilemeyen haklardandır.” Yargıtay 19. CD., 11.11.2019 T., 2019/31517 E., 2019/14002 K. (Kazancı, E.T.: 17.04.2020).

¹¹⁸ **Helvacı**, Koruyucu Davalar, s. 47.

hakkın devredilmesi de söz konusu olmaz¹¹⁹. Kişilik hakkı devredilemese de hakka konu değerlerin devredilebilmesi mümkündür¹²⁰. Kişilik hakkı ölümle sona erer. Bu hakkın mirasçılara geçmesi de söz konusu olmayacaktır. Zira söz konusu hak kişiye sıkı sıkıya bağlı bir hak olduğu için ancak hak sahibince kullanılması mümkündür.

Kişilik hakkı zamanaşımına uğramaz. Bu hak, hak düşürücü süreye de tabi değildir¹²¹.

Daha önce de belirttiğimiz gibi, kişilik hakkının konusuna giren değerler¹²² saymakla bitmez. Zira her geçen gün yeni bir değer eklenebilir¹²³. Ancak sıklıkla karşılaşılan bazı değerler örnek oluşturması bakımından sayılabilir. “*Hayat ve sağlık*”, “*vücut bütünlüğü*”, “*hayat alanı*”, “*şeref ve haysiyet*”, “*resim ve ses*” ve “*ad*” gibi değerler kişilik hakkının kapsamında değerlendirilmektedir¹²⁴.

Kişisel verilerin temelinde kişilik hakkının olduğunu savunan görüş, kişisel veriler ile kişilik hakkına konu olan değerlerden olan özel hayat arasında bağlantı

¹¹⁹ **Dural/Öğüz**, s. 104; **Serozan, Rona**, Medeni Hukuk-Genel Bölüm/Kişiler Hukuku, 7. Bası, İstanbul 2017, s. 455.

¹²⁰ **Helvacı**, Gerçek, s. 106.

¹²¹ **Helvacı**, Gerçek, s. 107.

¹²² Yargıtay kararında da isabetli bir şekilde belirtildiği gibi “*Hukuk düzenince korunan kişisel değerlerin tamamı kişilik hakkının konusunu oluşturur. Kişisel değerler, insanın insan oluşu nedeniyle sahip olduğu vücut, sağlık, yaşam gibi bedensel bütünlüğe bağlı değerler ile ruhsal bütünlük, faaliyet özgürlüğü gibi ruhsal değerleri kapsar.*” Yargıtay HGK., 12.03.2019 T., 2015/21-2925 E., 2019/277 K. (Kazancı, E.T.: 17.03.2020).

¹²³ **Tekinay**, s. 250.

¹²⁴ Kişilik hakkının konusunu oluşturan değerlerle ilgili ayrıntılı bilgi için bkz. **Helvacı**, Gerçek, s. 107-137.

kurmaktadır¹²⁵. Anayasamızda kişisel verilerin korunması hakkının “*özel hayatın gizliliği ve korunması*” maddesinde düzenlenmesi de bu görüşün tezahürüdür. Bu vesileyle, özel hayat ve nihayetinde yukarıda bahsettiğimiz hayat alanı kavramlarının üzerinde durulması önem arz etmektedir.

Hayat alanı, kişilik hakkının kapsamına dahildir. Kişi, hayatındaki gelişmelerin başkaları tarafından bilinmesini istemeyebilir. Hayat alanı, “*gizli hayat*”, “*özel hayat*” ve “*kamuya açık hayat*”tan oluşmaktadır. Gizli hayat, kişinin sadece paylaştığı kişilerle sınırlı tuttuğu ve diğer kişilerin bu sınırı aşmaması gereken kısımdır. Özel hayat, gizli hayat kadar sır dolu olmasa da kişinin sadece ailesi ve arkadaşları gibi yakın çevresiyle paylaştığı alandır. Kamuya açık hayat ise adı üstünde herkes tarafından rahatlıkla bilinebilen hayat olaylarını kapsayan geniş alandır¹²⁶. Özel ve gizli hayat alanına yapılan müdahaleler kişilik hakkını ihlal eder¹²⁷. Kural olarak kişilik hakkına saldırıya karşı korumalar kişinin kamuya açık hayat alanını kapsamamaktadır. Bu korumalar özel ve gizli hayat alanına ilişkindir¹²⁸.

Kişisel verilerin kişilik hakkı olduğunu savunanlar, “*kişisel verilerin korunması*” ile “*mahremiyetin ve özel hayatın korunmasını*” eş gördükleri için eleştiriye maruz kalmışlardır. Zira kişisel verilerin korunmasını salt özel hayatın korunmasına bağlamak sıkıntılı ve yetersiz bir sonuca ulaşmaya yol açabilir. Yargıtay’ın bir kararında¹²⁹ isabetli olarak belirttiği gibi “*Kişisel verilerin korunması temel hak ve özgürlükler ile yakından*

¹²⁵ **Aksoy**, Kişisel Veri, s. 54.

¹²⁶ **Helvacı**, Gerçek, s. 121.

¹²⁷ **Dural/Öğüz**, s. 139.

¹²⁸ **Helvacı**, Gerçek, s. 122-125.

¹²⁹ Yargıtay HGK., 06.11.2018 T., 2017/4-1340 E., 2018/1622 K. (Kazancı, E.T.: 25.04.2020).

ilişkilidir. Çünkü kişisel verilerin açıklanması öncelikle özel hayatın gizliliğini ihlal edilebileceği gibi başka bir takım bağlantılı hakları da zarara uğratabilir.” Elbette kişisel verilerin korunması ile özel hayatın korunması ilişkilidir ve birçok noktada benzeşmektedir. Ancak kişisel verilerin korunmasını salt özel hayat perspektifinden değerlendirmek birtakım yanlış sonuçları beraberinde getirebilir. Yukarıda da ifade ettiğimiz gibi, kişinin hayat alanı 3 bölüme ayrılmaktadır. Kişilik hakkı korumaları, gizli ve özel hayat alanını kapsarken, kamuya açık alanı kapsamamaktadır. Kişisel verilerin salt özel hayatla bağdaştırılması durumunda kamuya açık alanda kişisel verilerin korunması mümkün olmayacaktır¹³⁰. Oysa kişisel veriler illaki gizli ve özel olmak zorunda değildir. Kişisel veriler kamuya açık alanda da korunmaya muhtaçtır. Aksi halde kamuya açık hayat alanına özgü bilgilerin işlenmesine karşı kişi korunamayacaktır¹³¹. Sonuç olarak klasik kişilik hakkı görüşü, kamuya açık alandaki bilgilerin kişisel veri olarak kabul edilmesine cevap verememektedir¹³². Söz konusu sebepler kişisel verilerin korunması ile özel hayatın gizliliğinin korunmasının birebir örtüşmediğini göstermektedir¹³³.

Bir diğer eleştiri ise kişisel verilerin korunmasının “*özel hayata ve aile hayatına saygı hakkı*”nın ötesine geçtiğidir. Daha önce de ifade ettiğimiz gibi, bilginin kişisel veri olarak kabul edilmesi için doğru veya kanıtlanmış olması gerekmemektedir. Gerçek kişi ile ilişkilendirilebilen bir veri, yanlış olsa dahi kişisel veridir ve korumalardan

¹³⁰ **Prins, Corien**, s. 281.

¹³¹ Benzer yönde Yargıtay kararı için bkz. “*Gizli olmayan ve herkes tarafından bilinen kişisel veriler de hukuka aykırı eylemlere karşı korunmalıdır.*” Yargıtay CGK., 17.06.2014 T., 2012/12-1510 E., 2014/331 K. (Kazancı, E.T.: 25.04.2020).

¹³² **Aksoy**, Personal Data, s. 241.

¹³³ **Aksoy**, Kişisel Veri, s. 62.

yararlanmalıdır¹³⁴. Doğru olmayan bir bilgi, gizlilik alanını ihlal etmese de bu bilgi kişisel veridir ve korunmalıdır. Bu nedenle veri ile ilgili korumaların salt özel hayata indirgenmesi mantıklı gözükmemektedir¹³⁵. Aksi halde doğru olmayan, yalan-yanlış bilgilere karşı kişinin korunamaması tehlikesi belirecektir.

Yukarıda bahsettiğimiz klasik kişilik hakkı görüşünün bazı sıkıntılarını olduğundan kişilik hakkı temelinden ayrılmayan ancak kişisel verileri sadece özel hayata bağlamayan bir görüş ortaya çıkmıştır. Bu görüş, Almanya’da bir mahkeme kararıyla ortaya atılmıştır. 1982 yılında Almanya’da “*Nüfus Sayımı Kanunu*” kabul edilmiştir. Bu kanun, verilerin korunması açısından oluşacak risklerle ilgili tartışma yaratmıştır. Zira kişilerin cevaplayacağı 160 soruluk bir anket öngörülmüştür. Ayrıca kişisel veriler içeren bu anket sonuçlarının önemli bir süre saklanması öngörülmüştür. Bu nedenlerle Alman Anayasa Mahkemesi’ne başvurulmuştur¹³⁶. Alman Anayasa Mahkemesi (“*Bundesverfassungsgericht*”), 1983 yılında verdiği Nüfus Sayımı (“*Volkszählung*”) kararıyla¹³⁷ yeni bir hak olan “*bireyin kişisel verilerinin geleceğini belirleme hakkını*” (“*Das Recht auf informationelle Selbstbestimmung, The Right to Informational Self-Determination*”) veri koruma hukukuna kazandırmıştır¹³⁸. Bu kararla birlikte Alman veri

¹³⁴ **Data Protection WP**, Concept, s. 6-7.

¹³⁵ **Aksoy**, Kişisel Veri, s. 62; **Aksoy**, Personal Data, s. 240.

¹³⁶ **Hornung, Gerrit/Schnabel, Christoph**, “*Data Protection in Germany I: The Population Census Decision and The Right To Informational Self-Determination*”, Computer Law & Security Report, 2009, C. 25, S. 1, s. 85.

¹³⁷ BVerfGE 65,1.

¹³⁸ **Franzius, Claudio**, “*Das Recht auf informationelle Selbstbestimmung*”, Zeitschrift für das Juristische Studium, 3/2015, s. 259.

koruma yasasının da temelleri atılmıştır¹³⁹. Bu kararda mahkeme, kişisel verilerin korunması hakkını, insan onuruyla ve kişinin varlığını geliştirme hakkıyla ilişkilendirerek kişilik hakkının bir biçimi olarak belirlemiştir. “*Bireyin kişisel verilerinin geleceğini belirleme hakkı*”, kişinin, kişisel verilerinin ne zaman, kim tarafından ve hangi düzeyde işlenebileceğine karar verme hakkı şeklinde ifade edilebilir¹⁴⁰. Yani kişisel verileri ile ilgili karar merci bireyin kendisidir¹⁴¹. Söz konusu hak bireyi, kişisel verilerinin sınırsız şekilde toplanması ve depolanmasından korumaktadır. Ancak mahkeme kişinin kendi kişisel verileri üzerinde sınırsız bir hakka sahip olmadığını da vurgulamıştır. Yine de devlet veri işleme ile ilgili düzenlemelerde bireysel özerkliğe saygı göstermelidir¹⁴².

Sonuç olarak, kişisel verinin hukuki niteliğinin sadece kişilik hakkının konusunu oluşturan değerlerden biri olan özel hayatla bağdaştırmak yerine, kişilik hakkının konusunu oluşturan ayrı bir değer olarak (“*bireyin kişisel verilerinin geleceğini belirleme hakkı*”) değerlendirilmesi kanaatimce de isabetlidir. Diğer ifadeyle, “*bireyin kişisel verilerinin geleceğini belirleme hakkı*” kişilik hakkının bir parçasıdır¹⁴³. Ancak salt özel hayatla örtüştürülmemelidir. Zira bireyin kişisel verilerinin geleceğini tayin hakkı, kişinin verilerinin hepsini koruma altına almaktadır. Nitekim yukarıda klasik kişilik hakkı görüşünde belirttiğimiz kamuya açık alandaki kişisel verilerin korunmaması tehlikesi de

¹³⁹ **Hornung/Schnabel**, s. 85.

¹⁴⁰ **Schwartz, Paul**, “*The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination*”, The American Journal of Comparative Law, 1989, C. 37, S. 4, s. 690.

¹⁴¹ **Şimşek, Oğuz**, Anayasa Hukukunda Kişisel Verilerin Korunması, İstanbul 2008, s. 115.

¹⁴² **Schwartz**, Self Determination, s. 690.

¹⁴³ **Hornung/Schnabel**, s. 86.

burada söz konusu olmayacaktır¹⁴⁴. Bu nedenle bütün kişisel verilerin korunması sağlanmış olacaktır. Aynı zamanda verilerin serbest dolaşımı da engellenmiş olmayacaktır¹⁴⁵. Saydığımız tüm nedenlerle, kişisel verilerin hukuki niteliğinin tespitinde kanımızca en isabetli görüş “*bireyin kişisel verilerinin geleceğini belirleme hakkı*”na dayanan görüştür.

Kişisel verilerin korunması hakkı, Anayasamızda da yer alan “*kişinin maddi ve manevi varlığını koruma ve geliştirme hakkı*”¹⁴⁶ ve “*insan onuru ilkesi*” ile bağlantılıdır. Kişisel verilerin korunması hakkı, söz konusu sayılan hakların özel bir biçimi olarak ifade edilmektedir¹⁴⁷. Kişisel veriler işlenirken söz konusu haklara da uyulması gerekmektedir¹⁴⁸. Yargıtay bir kararında¹⁴⁹ isabetli olarak “*Bilgi toplumunda giderek önemli bir konu hâline gelen kişisel verilerin korunması hakkı, bireyin demokratik bir hukuk devletinde özgür iradesiyle kendi yaşamını bizzat düzenleyebilmesinin bir gereği olarak karşımıza çıkmaktadır. Diğer taraftan bireyin kişiliğini serbestçe geliştirmesi, kişiliğinin korunması ve özgür bireylerden oluşan bir toplum düzeninin oluşturulması, ancak bireyin kişisel verilerine ilişkin hakkının korunmasıyla mümkündür.*” ifadelerine

¹⁴⁴ **Aksoy**, Kişisel Veri, s. 71-72.

¹⁴⁵ **Ayözger Öngün, Çiğdem**, Kişisel Verilerin Korunması Hukuku (Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil), Genişletilmiş 2. Baskı, İstanbul 2019, s. 19.

¹⁴⁶ Anayasa m. 17.

¹⁴⁷ **Bilir, Faruk**, “*Kişisel Verilerin Korunması Kanununa Genel Bir Bakış*”, İnşaat Sanayi Dergisi, 2018, S.165, s. 62.

¹⁴⁸ **Şimşek**, s. 114.

¹⁴⁹ Yargıtay HGK., 17.06.2015 T., 2014/4-56 E., 2015/1679 K. (Kazancı, E.T.: 22.04.2020).

yer vermiştir. Yine AYM'nin bir kararında¹⁵⁰ “*Kişisel verilerin korunması hakkı, kişinin insan onurunun ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak, bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır.*” ifadelerine yer verilmiştir. Söz konusu kararların Almanya'daki Nüfus Sayımı kararıyla benzer yönleri dikkat çekmektedir. Yukarıda nedenlerini detaylarıyla açıkladığım şekilde, fikrimce gerek Yargıtay'ın gerekse AYM'nin kararları yerindedir.

§3. Kişisel Verilerin Korunmasının Tarihsel Gelişim Serüveni ve Kişisel Verilerin Korunmasının Hak Olarak Ortaya Çıkışı

I. Genel Olarak

Kişisel verileri koruma bilincinin oluşması ve kişisel verilerin korunması bakımından düzenlemeler yapılması çok eskilere dayanmaz. Günümüzde bu kadar popüler olan ve veri koruması konusunda ülkelerin azami gayret gözetmeye çalıştığı alanın elli yıllık bir tarihi geçmişi olduğu söylenebilir.

“*Sanayi toplumu*”ndan “*bilgi toplumu*”na geçiş döneminde, kişilerin haklarının zarar görme kaygısı, ülkeleri ve uluslararası kuruluşları veri koruma alanında düzenlemeler yapmaya itmiştir¹⁵¹. 1970'lerde çeşitli AB ülkelerinde kişisel verilerin özellikle otomatik işlenmesini konu eden düzenlemeler yapılmaya başlanmıştır¹⁵². Söz

¹⁵⁰ AYM, 09.04.2014 T., 2013/122 E., 2014/74 K., RG. 26.07.2014, S. 29072; AYM, 19.02.2020 T., 2018/163 E., 2020/13 K., RG. 28.04.2020, S. 31112.

¹⁵¹ **Akıncı, Ayşe Nur**, Büyük Veri Uygulamalarında Kişisel Veri Mahremiyeti, Uzmanlık Tezi, T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı, Yayın No: 0001, Ankara 2019, s. 59.

¹⁵² **Henkoğlu**, s. 29.

konusu düzenlemeler, kişisel verilerin korunmasının bir hak olarak kabul edilmeye başlamasına vesile olmuştur. Bu düzenlemeler iki farklı şekilde yapılmıştır. AB ülkelerinde kişisel veri ile ilgili düzenlemeler ya özel, belirli bir konuya ilişkin yapılmış ya da anayasal düzeyde bazı hükümler getirmişlerdir. Başka bir ifadeyle, ya belirli bir konu ile ilgili kişisel veri düzenlemesi yapılmış ya da anayasaya hüküm ekleme yoluna gidilmiştir¹⁵³.

Kişisel verilerin korunması ile ilgili öncü hukuki düzenlemeler sırasıyla; 1970’de Hessen eyaletinde (Almanya), 1973’te İsveç’te, 1977’de Almanya’da ve 1978’de Fransa’da yapılmıştır. 1970 yılında başlayan kişisel veri ile ilgili ulusal düzenlemeler yapma akımı 1981 yılında kabul edilen 108 No.lu Sözleşme’ye kadar devam etmiştir¹⁵⁴.

Dünya tarihinde kişisel verilerin korunması, ilk olarak Almanya’nın Hessen eyaletinde 1970 yılında kabul edilen Veri Koruma Kanunu (**“Hessisches Datenschutzgesetz”**) ile düzenlenmiştir¹⁵⁵. Veri koruma hukukunun ilk göz ağrısı olarak kabul edebileceğimiz bu kanun, eyalet tarafından kabul edilmesi sebebiyle ve kapsamı gereği sınırlı bir uygulamaya sahiptir. Zira sadece kamu tarafından yapılan otomatik işlemlere uygulanma kabiliyeti vardır¹⁵⁶. Ancak bu kanunun, sonraki yıllarda kişisel veriyle ilgili hem ulusal çapta hem de uluslararası alanda kabul edilecek birçok düzenlemenin fitilini ateşlediği kabul edilebilir.

¹⁵³ **Fuster, Gloria Gonzalez**, The Emergence of Personal Data Protection as a Fundamental Right of the EU, Springer, 2014, s. 55.

¹⁵⁴ **Fuster**, s. 56.

¹⁵⁵ **Kilian, Wolfgang**, “Germany”, James B. Rule and Graham Greenleaf, Global Privacy Protection, The First Generation, United Kingdom 2008, s. 83.

¹⁵⁶ **Fuster**, s. 56, s. 70.

Avrupa’da kişisel veriyi konu edinen ilk kanun, 1973 tarihli İsveç Veri Koruma Kanunu’dur¹⁵⁷. Almanya’ da veri koruma ile ilgili çıkan tartışmalar eyalet sınırlarını aşan bir kanun yapılmasına vesile olmuştur. Almanya’ da 1977 yılında Alman Federal Veri Koruma Kanunu) (*“BDSG”*)¹⁵⁸ kabul edilmiştir. BDSG, eksiklikler barındırmasına rağmen takdire şayan bir ilk adım olarak ifade edilmektedir¹⁵⁹. 70-80 dönemi arası veri koruma kanunu furyasına 1978 yılında Fransa da katılmıştır¹⁶⁰.

Yukarıda belirttiğimiz gibi bazı AB ülkeleri veri korumaya ilişkin kanunlar çıkarmaya başlarken, diğer ülkeler anayasalarına kişisel veri ile ilgili hükümler ekleme yolunu tercih etmiştir. Söz konusu ülkeler Portekiz, Avusturya ve İspanya olarak sayılabilir. Ancak burada Avusturya’ya dikkat çekmek gerekir. Zira Avusturya, veri koruma hakkını (*“right to data protection”*) anayasal anlamda ilk kez kullanan ülkedir. Ancak burada bu hakkın bağımsız bir şekilde düzenlenmediğine, özel ve aile hayatına saygı hakkı çerçevesinde koruma altına alındığına değinmek yerinde olacaktır¹⁶¹.

Veri koruma alanındaki ulusal çabalar uluslararası örgütleri de söz konusu konuyla ilgili düzenlemeler yapma noktasında tetiklemiştir. Zaten gün geçtikçe artan veri işleme karşısında insanların korkmaya başlaması durumu, bu alanda açık, net ve etkin bir şekilde koruma sağlayan düzenlemelerin yapılmasını mecbur kılmıştır. Bu nedenle

¹⁵⁷ **Cate, Fred H.**, *“The Changing Face of Privacy Protection in the European Union and The United States”*, Indiana Law Review, 1999, C. 33, s. 180; **Fuster**, s. 58-59.

¹⁵⁸ BGBl. I, 27.01.1977, Se. 201.

¹⁵⁹ BDSG ile ilgili ayrıntılı bilgi için bkz. **Riccardi, J. Lee**, *“The German Federal Data Protection Act of 1977: Protecting the Right to Privacy?”*, Boston College International and Comparative Law Review, 1983, C.6, S. 1, s. 243-271.

¹⁶⁰ **Fuster**, s. 61-65.

¹⁶¹ **Fuster**, s. 66-71.

OECD, AK, AB VE BM veri koruması konusunda çeşitli düzenlemeler yaparak hem bu konunun gelişimine hem de kişisel verilerin anayasal bir hak olarak tanınmasına katkıda bulunmuşlardır. Bu konudaki top point (en üst nokta) düzenleme 2016 yılında kabul edilen GDPR'dır. Uluslararası örgütlerin çabaları veri korumasına özgü bir doktrin ve içtihat sisteminin oluşmasını sağlamıştır. Ayrıca uluslararası anlaşmalara imza atan ve uluslararası örgütlere üye olan devletler kişisel verilerin etkin bir şekilde korunmasını ülkelerindeki mevzuatlara yansıtmak zorunda kalmışlardır. Zira uluslararası alanda kabul gören haklara ve ilkelere saygı göstermeyen ülkeler dışlanmaya mahkumdur. Şimdi sırasıyla veri koruma hukukunu şekillendiren uluslararası düzenlemeleri inceleyelim.

II. Uluslararası Düzenlemeler

A. İnsan Hakları ve Özgürlüklerinin Korunmasına İlişkin Avrupa Sözleşmesi (Avrupa İnsan Hakları Sözleşmesi)

4 Kasım 1950'de Roma'da imzalanan bu sözleşme 3 Eylül 1953'de yürürlüğe girmiştir. Türkiye sözleşmeyi ilk imzalayan devletlerden biri olmasına rağmen sözleşmenin onayı ve yürürlüğe girmesi 18 Mayıs 1954 tarihini bulmuştur¹⁶². AK tarafından yayımlanan Avrupa İnsan Hakları Sözleşmesi'nde ("*AİHS*") kişisel verilerin korunması açıkça düzenlenmese de AİHS 8.maddede yer alan "*özel ve aile hayatına*

¹⁶² RG. 19.03.1954, S. 8662. Sözleşmeyi imzalayan ülkeler ve hangi ülkelerin sözleşmeyi ne zaman yürürlüğe soktuğu ile ilgili detaylı bilgi için bkz. <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005/signatures> (E.T.: 07.03.2020). Sözleşmenin orijinal metni için bkz. **Council of Europe**, European Convention on Human Rights, https://www.echr.coe.int/Documents/Convention_ENG.pdf (E.T.: 07.03.2020).

saygı hakkı”nın kişisel verilerin korunmasını kapsamı altına aldığı görüşü hakimdir. AİHS m. 8/1 gereği “*Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.*” Söz konusu hakka karşı kamu tarafından yapılabilecek müdahaleler ise 2. bentte sayılmıştır¹⁶³. Buna göre “*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.*”

Kişisel verilerin korunmasının AİHS m. 8 kapsamında görülmesi özellikle veri koruma yasası olmayan ülkeler açısından önemlidir. Zira bu ülkelerde veri koruma yasası olmasa bile kişiler AİHS m. 8’e dayanabilecektir¹⁶⁴.

Özellikle AİHM, AİHS m. 8’i geniş yorumlayarak¹⁶⁵ kişisel verilerin korunmasını bu madde kapsamında değerlendirmektedir¹⁶⁶. Başka bir ifadeyle AİHM, kişisel verilerin

¹⁶³ Sözleşmenin Türkçe metni için bkz. **Council of Europe**, Avrupa İnsan Hakları Sözleşmesi, https://www.echr.coe.int/Documents/Convention_TUR.pdf (E.T.: 07.03.2020).

¹⁶⁴ **Bygrave, Lee A.**, “*Data Protection Pursuant to the Right to Privacy in Human Rights Treaties*”, International Journal of Law and Information Technology, 1998, C. 6, S. 3, s. 248.

¹⁶⁵ **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 Report, 2002, C. 18, S. 1, s. 33.

¹⁶⁶ AİHS m. 8 dışındaki diğer maddelere (m. 6-10-13) ilişkin içtihatlarda da kimi zaman veri koruma hususuna değinilmiştir. Ancak asıl önem teşkil eden hüküm 8. maddedir. **Bygrave**, s. 254.

korunması hakkını içtihatlarıyla kabul etmiştir¹⁶⁷. Örneğin 12 yaşındaki bir çocuğun yaşı, fiziksel özellikleri gibi kişisel verilerinin, çocuğun bilgisi dışında internette buluşma sitesinde yayımlanması olayında AİHM m. 8 özelinde değerlendirme yapmıştır¹⁶⁸.

B. OECD Rehber İlkeleri

Türkiye'nin kurucu üyeleri arasında olduğu OECD, 1961 yılında kurulmuştur. Doğrudan kişisel verilerin korunmasıyla ilgili ilk uluslararası belgelerden olan “*OECD Rehber İlkeleri (Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeleri)*” 1980 tarihinde düzenlenmiştir. OECD globalleşmenin yarattığı ekonomik, sosyal ve çevre ile ilgili sorunlara çözüm aramak üzere ülkeler arasında iş birliği amacı güden örgüttür¹⁶⁹. Avrupa kıtası dışındaki ABD, Japonya, Avustralya gibi birçok ülkeyi de bünyesinde barındıran OECD tarafından veri koruma alanında çalışma yapılması önemlidir¹⁷⁰. Zira Avrupa’da AB, AK ve ülkelerin belli bir veri koruma anlayışı oluşmaya başlamıştı. Ancak bu zihniyetin diğer ülkelere de sirayet etmesi önemliydi.

¹⁶⁷ **Başalp**, Kişisel Veri, s.26; **Küzeci**, s.134 vd.; **Fuster**, s. 104.

¹⁶⁸ AİHM, 02.12.2008 T., No: 2872/02; **Gür, İkbāl**, Kişisel Verilerin Korunması Hususunda AB ile ABD Arasında Çıkan Uyuşmazlıklar ve Çözüm Yolları, Ankara 2010, s. 13.

¹⁶⁹ **OECD**, OECD e-Government Studies Turkey, Orijinal metin için bkz. https://read.oecd-ilibrary.org/governance/oecd-e-government-studies-turkey-2007_9789264028456-en#page1 (E.T.: 07.03.2020), Metnin Türkçesi için bkz. https://read.oecd-ilibrary.org/governance/oecd-e-government-studies_9789264037700-tr#page1 (E.T.: 07.03.2020), s.3.

¹⁷⁰ **Gür**, s. 155.

OECD adı üstünde ekonomik alanda uluslararası dayanışmayı amaçlayan bir örgüttür. Bu örgütün kişisel verilerin korunmasıyla ilgili rehber ilkeler yayımlamasındaki amaç verilerin sınır ötesi akışındaki hızın ve büyüklüğün çok büyük miktarlara ulaşması karşısında veri korumayla ilgili önlemler almaktır. Rehber İlkeler'in kabul edildiği o dönemde, OECD üyesi bazı ülkeler, ulusal veri koruma düzenlemelerini yürürlüğe koymuşken diğer ülkeler herhangi bir girişimde bulunmamıştır. Veri korumasıyla ilgili ulusal mevzuatlardaki farklılıkların kişisel verilerin serbestçe sınır ötesi dolaşımını engelleme ihtimali ve bu ihtimalin ekonominin önemli sektörlerinde (bankacılık, sigorta gibi) olumsuz sonuçlara yol açacağı durum karşısında ekonomik bir örgüt olan OECD, söz konusu ilkeleri yayımlamıştır¹⁷¹. OECD ekonomik iş birliği amacı taşıyan bir örgüt olduğundan rekabet şartları çerçevesinde serbestçe yapılabilen serbest piyasa ekonomisini geliştirmeyi hedefler. Bu nedenle kişisel veri koruması ve verilerin ülkeler arası serbestçe dolaşımı arasında denge kurmaya çalışır¹⁷².

OECD Rehber İlkeler'i taraf ülkeler için bağlayıcı değildir. Ülkelere uyma konusunda ülkelerin takdir yetkisi bulunmaktadır¹⁷³. Ancak uluslararası ilk düzenleme olmasının getirdiği sonuç, tüm dünyada veri korumayla ilgili düzenlemelere önayak olması ve temel ilkeler konusunda uzlaşının sağlanmasıdır¹⁷⁴.

Söz konusu düzenlemenin giriş kısmında OECD, taraf ülkelere tavsiye kısmına yer vermiştir. OECD, üye ülkelere özel yaşamın korunmasıyla ilgili ulusal düzenlemelerde OECD Rehber İlkeleri'ni dikkate almalarını, kişisel verilerin sınır ötesi dolaşımında çıkabilecek engelleri bertaraf etmelerini ve bu konuda iş birliğinde

¹⁷¹ **OECD**, Rehber İlkeler, Preface (Önsöz).

¹⁷² **Aksoy**, Kişisel Veri, s.5.

¹⁷³ **Akıncı**, Veri Mahremiyeti, s. 65; **Cate**, s. 180.

¹⁷⁴ **Küzeci**, s. 115.

bulunulmasını önermiştir¹⁷⁵. Üye ülkeler ulusal düzenlemelerde kişisel veri koruma kuralları koyarken Rehber İlkeleri alt sınır olarak kabul etmelidir. Bunun ötesinde daha özgürlükçü ve kişisel verileri daha çok koruyan düzenlemeler elbette yapabileceklerdir¹⁷⁶.

Kişisel verilerin uluslararası alanda dolaşımını konu alan OECD Rehber İlkeleri 2. kısımda temel ilkeler başlığıyla sırasıyla sekiz ilke saymıştır. Bu ilkeler; “*veri toplamanın sınırlı olması ilkesi (m.7)*”, “*veri kalitesi ilkesi (m.8)*”, “*amacın belirli olması ilkesi (m.9)*”, “*kullanımın sınırlı olması ilkesi (m.10)*”, “*veri güvenliği ilkesi (m.11)*”, “*açıklık ilkesi (m. 12)*”, “*bireysel katılım ilkesi (m.13)*”, “*hesap verebilirlik ilkesi (m.14)*” olarak sayılabilir.

OECD Rehber İlkeleri, yayımlandıktan sonra 2013 yılına kadar değişikliğe uğramamıştır. Ancak aradan geçen 33 yıl sonucu değişen ve dönüşen dünya ve bunun akabinde gün geçtikçe önem kazanan veri koruma hukukunun değişen gereksinimleri dolayısıyla 1980 yılında uzlaşılan temel ilkeler aynı kalmak kaydıyla, eski metin 2013 yılında revize edilmiştir¹⁷⁷.

C. Avrupa Konseyi 108 No.lu Sözleşme

Kişisel verilerin korunması ile ilgili AK tarafından 1970’lerden başlayarak devam eden çalışmalar neticesinde 1981 yılında “*108 No.lu Sözleşme (Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi)*” imzaya

¹⁷⁵ **OECD**, Rehber İlkeler, Council Recommendation (Örgüt Tavsiye Kararı).

¹⁷⁶ **Küzeci**, s. 114.

¹⁷⁷ OECD Rehber İlkeleri revize edilen maddeler için bkz. **OECD**, revision 2013, https://www.oecd.org/internet/ieconomy/oecd_privacy_framework.pdf (E.T.: 07.03.2020).

açılmıştır¹⁷⁸. Sözleşme 28 Ocak 1981’de imzaya açılmış, 1 Ekim 1985 yılında yürürlüğe girmiştir. Sözleşmeyi imzalayan ilk ülkelerden biri olan Türkiye de olsa, sözleşmenin iç hukuka dahil edilmesi 17 Mart 2016 tarihinde olmuştur¹⁷⁹. Sözleşme iç hukukumuza dahil edildiğinden, ülkemizdeki veri koruma uygulamalarında sözleşmeye riayet edilmesi gerekmektedir. Bu vesileyle çalışmamızın sınırlarını aşmayacak şekilde 108 No.lu sözleşmenin incelenmesi kıymetlidir.

1985’de yürürlüğe giren AK Sözleşmesi, veri korumanın önemine daha çok odaklanmasına rağmen OECD Rehber İlkelerine benzemektedir¹⁸⁰. Ancak elbette kişisel verilerin korunması açısından bu sözleşme önemlidir. Sözleşmenin önemi, hem AK üyesi olmayan ülkelerin de bu sözleşmeyi imzalayabilmelerinden hem de kişisel veri hukukunda uluslararası alanda bağlayıcılığı olan yegane belge oluşundan kaynaklanmaktadır¹⁸¹. Sözleşme bağlayıcı da olsa etki gücü yüksek olmamış, taraf devletlerin kişisel veriyle ilgili ulusal düzenlemelerinde uyumu sağlayamadığı için sınır ötesi veri akışı istenen düzeyde olmamıştır. Yine de sözleşmenin ana hatları daha sonraki AB veri düzenlemelerine ilham kaynağı olmuştur¹⁸².

Sözleşmedeki temel veri koruma ilkeleri ve veri koruma amacıyla konulmuş diğer hükümler veri koruma açısından alt sınırı oluşturmaktadır. Başka bir ifadeyle, sözleşmeye taraf ülkeler ulusal düzenlemelerinde elbette verileri korumada daha hassas hükümler kabul edebilir ve daha özgürlükçü düzenlemeler yapabilirler. Ancak bu sözleşmedeki

¹⁷⁸ **Kuner**, s. 48; **Kurum**, Kişisel Verilerin Korunması Alanında Uluslararası ve Ulusal Düzenlemeler, s. 3.

¹⁷⁹ RG. 17.03.2016, S. 29656.

¹⁸⁰ **Cate**, s. 181.

¹⁸¹ **Küzeci**, s. 126; **Akıncı**, Veri Mahremiyeti, s. 62.

¹⁸² **Aksoy**, Kişisel Veri, s. 6.

asgari veri koruma sınırının altına inemezler¹⁸³.

Sözleşmenin amacı; sözleşmeye taraf ülkelerdeki gerçek kişilerin-tabiiyeti ve ikameti ne olursa olsun- kişisel verilerini otomatik işleme tabi tutulması karşısında korumaktır¹⁸⁴. Sözleşme, adından da belli olduğu gibi, kişisel verilerin otomatik olarak işlenmesine karşı koruma sağlamaktadır. Yani esasen sözleşme, verilerin otomatik olmayan yolla işlenmesinde (elle işlenmesinde) koruma sağlamamaktadır. Ancak sözleşmenin 2. maddesinde otomatik işlem tanımına “*kısmen otomatik işleme*” de dahil edilmiştir. Zaten taraf ülkelerin yapacakları ulusal düzenlemelerle, sözleşmeyi, verilerin otomatik olmayan yolla işlenmesinde de uygulamaları mümkündür¹⁸⁵.

Her taraf ülkenin sözleşmedeki temel veri ilkelerine ulusal düzenlemelerle işlerlik kazandırmaları zorunluluğu bulunmaktadır¹⁸⁶. Bu temel veri koruma ilkeleri; “*verilerin niteliğinin kaliteli olması (m.5)*”, “*hassas verilerin daha sıkı korunması (m.6)*”, “*verilerin güvenliği (m.7)*”, “*ilgili kişinin bilgilendirilme, verilere ulaşma, verilerin düzeltilmesini ve silinmesini talep etme hakkı (m.8)*” olarak sayılabilir. Ayrıca sözleşme ile taraf ülkelere, temel veri koruma ilkelerinin ihlali halinde müeyyide uygulama ve ihlal halinde başvuru yolu sağlama yükümlülüğü getirilmiştir¹⁸⁷.

“*Verilerin niteliğinin kaliteli olması ilkesi*”ne göre, otomatik yolla işlenen veriler; hukuki yolla elde edilmeli ve işlenmelidir. Veriler, belirli ve meşru amaçlar için işlenmelidir. Veriler, işlenme amaçlarına uygun olarak kullanılmalıdır. Ayrıca bilgiler doğru ve güncel olmalıdır. Veri, işlenme amacına uygun sınırlı süre muhafaza

¹⁸³ AK 108 No.lu sözleşme, m. 11.

¹⁸⁴ AK 108 No.lu sözleşme, m.1.

¹⁸⁵ AK 108 No.lu sözleşme, m.3/2/c.

¹⁸⁶ AK 108 No.lu sözleşme, m.4.

¹⁸⁷ AK 108 No.lu sözleşme, m.10.

edilmelidir.

“*Hassas verilerin daha sıkı korunması ilkesi*”ne göre, bazı veriler daha özeldir ve özel olarak korunmayı hak etmektedir. Kişinin “*ırkı, siyasi düşüncesi, dini veya her türlü başka inancı ile ilgili bilgileri, sağlık ve cinsel yaşamla ilgili bilgileri*” sözleşmeye taraf ülke tarafından yeterli önlemler alınmadıkça otomatik yolla işlenemez.

“*Verilerin güvenliği ilkesi*”ne göre, otomatik yolla işlenen verilerin yok olmasını, izinsiz olarak ele geçirilmesini, değiştirilmesini veya dolaşımını engellemek amacıyla gerekli veri güvenliğinin sağlanması gerekir.

“*İlgili kişinin bilgilendirilme, verilere ulaşma, verilerin düzeltilmesini ve silinmesini talep etme hakkı*” ise ilgili kişinin kendisi hakkında tutulan bilgileri, bilgilerin işlenme amaçlarını öğrenmesidir. Yine kişinin belirli aralıklarla işbu bilgilerin hala bulunup bulunmadığını öğrenme, kendisine açıklanmasını isteme hakkı bulunmaktadır. Ayrıca ilgili kişinin gerekiyorsa kendi hakkında tutulan bilgileri düzelttirme hakkı vardır. Yine veri işleme ilkelerine aykırı olarak işlenen bilgilerini sildirtme hakkı vardır. Eğer bu talepleri karşılanmazsa başvuruda bulunma hakkına da sahiptir.

AB, veri koruma alanına ilişkin sert yasaklar getirmek yerine üye ülkeler arasında kişisel verilerin güvenli olarak akışını sağlayacak entegrasyon kuralları getirmeyi tercih etmiştir¹⁸⁸. Kişisel verilerin ülkeler arası dolaşımı hususunda taraf ülkeler bu dolaşımı yasaklayamaz ve engelleyici düzenlemeler getiremez. Kural bu olmakla birlikte, sadece belli veri kategorilerinde geçerli olmak üzere, bir taraf ülkenin iç hukuk düzenlemelerindeki veri koruması ile diğer taraf ülkenin iç hukuk düzenlemelerindeki veri koruma düzeyinin eşit olmaması durumunda veri dolaşımı konusunda engellemeler söz konusu olabilir. Ayrıca kişisel veri aktarımı sözleşmeye taraf olmayan bir ülkede

¹⁸⁸ Henkoğlu, s. 54.

yapılacaksa bu aktarımın engellenmesi de ikinci istisna olarak belirtilmelidir¹⁸⁹.

Sözleşmenin uygulanmasını sağlamak, gerektiğinde sözleşme değişiklik önerisini sunmak ve taraf ülkelerin sözleşmenin uygulanmasıyla ilgili sorularında görüş bildirmesi amacıyla Danışma Komitesi kurulmuştur. Bu komitede her taraf devletin temsilcisi bulunmaktadır¹⁹⁰.

1981 yılından itibaren bilişim hukuku ve veri koruma hukukunda meydana gelen aşırı değişim sözleşmede revizyon yapma ihtiyacı doğurmuştur. Bu nedenle “*Kişisel Verilerin İşlenmesi Karşısında Bireylerin Korunması İçin Modernize Edilmiş Sözleşme (108+)*”¹⁹¹ Avrupa Konseyi tarafından 18 Mayıs 2018’de kabul edilmiştir.

D. Birleşmiş Milletler Rehber İlkeleri

II. Dünya Savaşı boyunca milyonlarca insan hayatını kaybetmiş, dünya tarihinde insan hakları ihlallerinin en fazla olduğu dönemlerden biri yaşanmıştır. İşte bu savaştan sonra uluslararası barışı sağlamak maksadıyla 1945’de 51 kurucu devlet tarafından Birleşmiş Milletler (“**BM**”) kurulmuştur. Türkiye, BM kurucu üyeleri arasındadır. Günümüzde BM üye sayısı 193’e ulaşmıştır.

¹⁸⁹ AK 108 No.lu sözleşme, m.12.

¹⁹⁰ AK 108 No.lu sözleşme, m. 18-19.

¹⁹¹ **Council of Europe**, “*Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data*” (“*Kişisel Verilerin İşlenmesi Karşısında Bireylerin Korunması İçin Modernize Edilmiş Sözleşme*”) <https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1> (E.T.: 08.03.2020).

1948 yılında BM tarafından kabul edilen “İnsan Hakları Evrensel Beyannamesi”¹⁹² m. 12 özel yaşamı koruma altına almaktadır. Buna göre, “Hiç kimse özel hayatı, ailesi, meskeni veya yazışması hususlarında keyfi karışmalara, şeref ve şöhretine karşı tecavüzlere maruz kalmaz. Herkesin bu karışma ve tecavüzlere karşı kanun ile korunmaya hakkı vardır.” Beynamede doğrudan kişisel veri ile ilgili bir madde bulunmamaktadır.

Ancak 1990 yılına gelindiğinde BM, doğrudan kişisel verilerin korunmasıyla ilgili olarak “Bilgisayarla İşlenen Kişisel Veri Dosyalarına İlişkin Rehber İlkeleri”¹⁹³ düzenlemiştir. BM Rehber İlkeleri, üye ülkeler açısından yönlendirici olması ve bu ülkelerin veri korumayla ilgili ulusal düzenlemelerinde göz önüne almaları amacıyla yayımlanmıştır. Yani bu ilkelerin herhangi bir bağlayıcılığı olmayıp, ilkeler tavsiye niteliğindedir. Sırasıyla bu ilkeler; “yasal ve meşru yollarla veri toplama ve işleme ilkesi”, “doğruluk ilkesi”, “amacın belirliliği ilkesi”, “ilgili kişinin erişimi ilkesi”, “ayrımcılık yapmama ilkesi”, “güvenlik ilkesi”, “denetim ve yaptırım ilkesi” ve “sınır ötesi veri akışı ilkesi” olarak sayılabilir.

E. 95/46/EC Sayılı AB Direktifi

Kişisel verilerin korunması alanında uluslararası düzeyde artan çalışmalara AB kayıtsız kalamamış, 1995 yılında “95/46/EC Sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa

¹⁹² BM, İnsan Hakları Evrensel Beyannamesi,

<https://www.tbmm.gov.tr/komisyon/insanhaklari/pdf01/203-208.pdf> (E.T.: 09.03.2020).

¹⁹³ **United Nations**, “Guidelines for the Regulation of Computerized Personal Data Files”, (Bundan böyle BM Rehber İlkeleri olarak anılacaktır.) <https://www.refworld.org/pdfid/3ddcafaac.pdf> (E.T.: 09.03.2020).

Konseyi Direktif”ini kabul etmiştir¹⁹⁴. Bu direktif, 2018 yılında yürürlüğe giren “*AB Genel Veri Koruma Tüzüğü (GDPR)*” ile yürürlükten kalkmış da olsa hem birçok ülkenin ulusal veri mevzuatına (KVKK dahil olmak üzere) esas oluşturması hem de GDPR’ın da aslında bu direktifin teknolojik ve bilimsel gelişmelere yani günümüze uyarlanmış hali olması, AB Direktifi’nin önemini ortaya koyduğundan inceleme konumuza dahil olmuştur.

Bilişim alanındaki hızlı değişimin kişisel veri işlenmesini ve iletimini çok kolay bir düzeye indirdiği, üye ülkelerin birbirleriyle veri paylaşımının gün geçtikçe arttığı ve bunun da gerekli olduğu ortadadır. Üye ülkelerdeki kişisel verilerin korunmasına ilişkin ulusal düzenlemelerin birbiriyle bağdaşmaması durumu, verilerin ülkeler arasında dolaşımını yavaşlatacağından ve hatta engelleyeceğinden ekonomik anlamda olumsuz sonuçlara yol açabilmektedir. AB Direktifi; AB özelinde, ortak pazar, ortak para birimi, siyasi birliğin sağlanması anlayışının uzantısıdır¹⁹⁵. AB Direktifi’nin asıl düzenleniş amacı ulusal mevzuatlardaki bu farklılıkların giderilmesi, veri yasalarındaki korumanın eşitlenmesidir. Ayrıca amaç, kişisel verilerin korunması hukuku kapsamında teklik¹⁹⁶, birlik, eşitlik sağlanması ve farklı ülkeler arasındaki veri akışındaki handikapların sona erdirilmesidir¹⁹⁷. Ülkeler arası veri dolaşımının sekteye uğramaması ekonomik sebeplerle o kadar önemlidir ki üye ülkelerin veri dolaşımını engelleyemeyecekleri ve

¹⁹⁴ OJ. 23.11.1995, L. 281, V. 38, p. 31-50.

¹⁹⁵ **Başalp**, Kişisel Veri, s. 25; **Gür**, s. 13.

¹⁹⁶ AB ekonomik ve sosyal sebeplerle sadece kişisel veri alanında değil, bir çok alanda mevzuatların uyumlaştırılmasını hedeflemektedir. “*Tek pazar*” yaklaşımı da buna örnek olarak verilebilir., **Küzeci**, s. 160.

¹⁹⁷ AB Direktifi, 1.-10. paragraf.

yasaklayamayacakları ayrıca vurgulanmıştır¹⁹⁸. Ancak elbette verilerin ülkeler arası serbest dolaşımında kişilerin, kişisel bilgilerinin korunması dikkate alınmalıdır. AB Direktifi'nde verilerin rahatça dolaşımı ile kişisel verilerin korunması arasında denge kurma gayreti vardır¹⁹⁹. Başka bir ifadeyle bu Direktif'te iki zıt amaç bir arada yer almaktadır. Bunlardan ilki kişisel verileri, özel hayata saygı hakkı çerçevesinde korumaktır. Bu amaca zıt gibi gözüken diğer amaç ise ülkelerin veri akışını engellememelerini sağlamaktır²⁰⁰. Saydığımız iki amacın bir arada gerçekleşmesi zordur. Ancak bu zor başarılırsa, kişilerin hakları korunmuş olacağı gibi ekonomik hayat da darbe yememiş olacaktır. Hep vurguladığımız gibi, veri koruma hukuku olarak oluşan yeni hukuk dalının da hedefi terazide dengeyi sağlamak olmalıdır.

AB Direktifi bahsi geçen uyumlaştırmayı sağlamak amacıyla kişisel verilerle ilgili ayrıntılı hükümlere yer vermiştir. Bu hükümler arasında önemli görülenlerden bir tanesi Direktif'in kapsamını düzenleyen 3. maddedir. Buna göre Direktif, 2. fıkrada belirtilen istisnalar dışında kişisel verilerle ilgili her türlü işlemi kapsayacak, özel bir alanla sınırlandırılmayacaktır²⁰¹.

Bilgilerin işlenmesinin yasal zemine oturtulabilmesi için gereken temel ilkeler (m.5-6), veri işleme şartları (m.7), hassas veri kategorileri (m.8), verilere erişim hakkı (m.9) gibi bir çok madde önemlidir ve hala temel başvuru maddeleridir.

¹⁹⁸ AB Direktifi, m. 1.

¹⁹⁹ **Akıncı, Ayşe Nur**, “Avrupa Birliği Genel Veri Koruma Tüzüğü’ nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi”, Çalışma Raporu 6, T.C. Kalkınma Bakanlığı Yayın No: 2968, 2017, s. 6.

²⁰⁰ **Gür**, s. 26.

²⁰¹ **Gür**, s. 27.

AB Direktifi'nin 6. maddesinde veri kalitesine ilişkin temel ilkeler düzenlenmiştir. Bunlar; “*adil ve yasal olarak işleme ilkesi*”, “*belirli, açık ve meşru amaçlar için işlenme ilkesi*”, “*toplandıkları amaçla bağlantılı ve sınırlı olma ilkesi*”, “*doğru ve güncel olarak tutulma ilkesi*” ve “*gerekli süreden fazla saklanmama ilkesi*” olarak sayılabilir. Kişisel veri işlenmesinin her aşamasında bu ilkelere riayet edilmesi önemlidir.

Direktif'in 28. maddesinde üye ülkelerdeki veri koruma hukukunun işleyişinin takibi ve veri korumasının güvence altına alınması için özerk bir denetleme makamı kurulması öngörülmüştür²⁰². Ülkemizde Kişisel Verilerin Korunması Kurulu, bu maddedeki makama tekabül etmektedir.

AB Direktifi'nin 29. maddesi gereğince “*Çalışma Grubu*” kurulmuştur. Bağımsız nitelikte olan bu makam danışma statüsündedir, kararları bağlayıcı değildir. Çalışma Grubu'nun bazı önemli görevleri; üye ülkelerdeki ve üçüncü ülkelerdeki veri koruma güvenlik düzeyini tespit etmek ve Komisyon'a bildirmektir. Ayrıca gerçek kişileri koruyucu ilave tedbirler alınması için öneride bulunmak ve kişisel verilerin korunması konusunda yıllık durum raporu hazırlamaktır²⁰³. Bu Çalışma Grubu formalite bir kuruluş olarak kalmamış, kişisel verilerin korunması hukukuna katkı sağlayacak pek çok görüş ve öneride bulunmuştur²⁰⁴.

AB, 95 yılındaki Direktifi yayımladıktan sonra “*2002/58/EC Sayılı Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Özel Hayatın Gizliliğinin*

²⁰² AB Direktifi, m. 28.

²⁰³ AB Direktifi, m. 29; **Gür**, s. 42.

²⁰⁴ Çalışma Grubu'nun görüş ve önerileri için bkz. **Data Protection WP**, Opinions and Recommendations, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm (E.T.: 09.03.2020).

Korunmasına İlişkin Direktif”i kabul etmiştir²⁰⁵. Bu direktif, gelişen teknoloji karşısında AB Direktifi’nin tamamlayıcısı olarak ifade edilmektedir Söz konusu Direktif’te “spamming”, “cookies” ve “profilleme” gibi spesifik sorunlar hakkında düzenleme yapılmıştır²⁰⁶.

F. 181 No.lu Protokol

AK 108 No.lu Sözleşme’de temel veri koruma ilkelerine yer vermiş, verilerin nasıl hukuka uygun işleneceğini düzenlemiştir. Ancak verilerin hukuka aykırı işlenmesini önleyici bir denetim makamı öngörmemiştir. İşte AK 108 No.lu Sözleşmedeki bazı noksanlıklar işbu Protokol²⁰⁷ ile tamamlanmaya çalışılmıştır²⁰⁸. Türkiye, AK 181 No.lu Protokol’ü 8 Kasım 2001 tarihinde imzalamıştır. Ancak Protokol’ün yürürlüğe girmesi 5 Mayıs 2016 tarihini bulmuştur²⁰⁹. Protokol’de ayrıca ülkeler arası veri akışına ilişkin düzenlemeler mevcuttur. Buna göre, 108 No.lu Sözleşme’ye taraf olmayan 3. ülkelere

²⁰⁵ Söz konusu Direktif ile ilgili detaylı bilgi için bkz. **Gür**, s. 78-82

²⁰⁶ Detaylı bilgi için bkz. **Başalp**, s. 92-97.

²⁰⁷ **Council of Europe**, “*Additional Protocol to the Convention for the Protection of Individuals with regard to Processing of Personal Data Regarding Supervisory Authorities and Transborder Data Flows*” (“*Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi’ne Ek Denetleyici Makamlar ve Sınır Ötesi Veri Akışına İlişkin Protokol*”) (Bundan böyle AK 181 No.lu Protokol olarak anılacaktır.), European Treaty Series No. 181, 08.11.2001, <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680080626> (E.T.: 09.04.2020).

²⁰⁸ **Dülger**, *Kişisel Veri*, s.30.

²⁰⁹ RG. 05.05.2016, S. 29703.

veri aktarılırken dikkat edilmesi gereklidir. Ayrıca yeterli korumanın o ülkede sağlanıp sağlanmadığının test edilmesi gereklidir²¹⁰.

Protokol'ün denetim makamları ("*supervisory authorities*") başlıklı 1. maddesi, üye ülkelerin Sözleşme'de ve Protokol'de belirtilen veri koruma ilkelerine uyulup uyulmadığının denetimi için bağımsız bir denetim makamı kurmalarını öngörmektedir.

G. AB Temel Haklar Şartı

AB Temel Haklar Şartı²¹¹ ("**ABTŞH**")²¹², 2000 yılının Aralık ayında Fransa'da (Nice) ilan edilmiştir. Ancak bu şart bağlayıcılığını 2009 Lizbon Anlaşması ile kazanmıştır. Bu vesileyle, temel hak olarak kabul edilen kişisel verilerin korunması hakkının AB Hukuku'ndaki kabulü sağlamlaştırmıştır²¹³.

Kişisel verilerin korunması hususu müstakil olarak 8.maddede düzenlenmiştir. Buna göre, "*Herkes, kendisini ilgilendiren kişisel verilerin korunması hakkına sahiptir. Bu veriler, adil bir şekilde, belirli amaçlar için ve ilgili kişinin rızasına veya yasa ile öngörülmüş diğer meşru bir temele dayanarak tutulur. Herkes, kendisi hakkında toplanmış verilere erişme ve bunları düzelttirme hakkına sahiptir. Bu kurallara uyulması, bağımsız bir makam tarafından denetlenir.*" Hükümden anlaşıldığı gibi, ABTŞH, kişisel verilerin korunması hakkını temel bir hak olarak kabul etmiştir.

²¹⁰ **Akıncı**, Veri Mahremiyeti, s. 64.

²¹¹ OJ. 26.10.2012, c. 326, V. 55, p. 391-407.

²¹² Metnin Türkçe çevirisi için bkz. http://www.sbb.gov.tr/wp-content/uploads/2018/11/Avrupa_Birligi_Temel_Haklar_Sarti%E2%80%8B.pdf (E.T.: 09.03.2020)

²¹³ **Fuster**, s. 2.

Veri koruma hükmü, insan hakları temelini onaylamak ve güçlendirmek amacıyla ABTHŞ'ye eklenmiştir²¹⁴. Ayrıca ABTHŞ m. 8/1'de hak süjesi olarak “*her kişi*” ifadesinin kullanılması tüzel kişilerin de bu hakkın sahibi olabileceği konusunda dikkat çekicidir. Ancak diğer AB düzenlemeleri de göz önüne alındığında söz konusu hakkın korumasından gerçek kişilerin yararlanması gerektiği belirtilmiştir²¹⁵.

H. 2016/679 AB Genel Veri Koruma Tüzüğü (GDPR)

1. Genel Olarak

Öncelikle belirtmek gerekir ki, GDPR²¹⁶, AB Direktifi'nin güncellenmiş sürümü olarak ifade edilebilir. 1995 tarihli AB Direktifi'nin kişisel verilerin korunması hukukuna katkısı paha biçilemez. Zira söz konusu Direktif, Türkiye de dahil olmak üzere birçok ülkenin kişisel veri mevzuatına ışık tutmuştur. Ancak gelişen ve dönüşen bir toplum yapısında hiçbir hukuki düzenleme baki kalmaz. Hele ki kişisel veri gibi teknolojik gelişmelerle bu kadar iç içe bir konuda 1995 yılındaki düzenlemenin günümüz değişen ihtiyaçlarına tam olarak cevap verememesini garipsememek gerekir.

AB Direktifi, özellikle kişisel verilere ilişkin temel ilkelerin oluşmasında öncü rol üstlenmiştir. Temel ilkelerin kişisel veriler için önemini TMK başlangıç hükümlerinin özel hukuktaki önemine benzetebiliriz. Bu temel ilkeler, ileride de detaylıca inceleyeceğimiz gibi, kişisel veri ile ilgili faaliyetlerin her aşamasında ilk bakılması gereken ana prensiplerdir. Söz konusu temel ilkeler, hala hem ülkemiz kişisel veri düzenlemeleri hem de yabancı ülke düzenlemelerinde baz alınmaktadır. Daha önce de

²¹⁴ **Bergkamp**, s. 33.

²¹⁵ **Şimşek**, s. 73.

²¹⁶ OJ. 4.5.2016, L. 119, V. 59, p. 1-88.

ifade ettiğimiz gibi, AB Direktifi'nin ana amaçlarından biri, ulusal veri mevzuatlarındaki farklılıkların giderilmesi ve tekliğin sağlanmasıdır. Zira ülkelerin hukuki düzenlemelerindeki farklılıklar ülkeler arası veri akışını sekteye uğratabilecektir. Ancak Direktif'in söz konusu amacına tam anlamıyla ulaştığı söylenemez. Zira her bir ülkenin veri korunması ile ilgili uygulamalarındaki farklılıklar kişisel verilerin korunması konusunda teklik ve birlik amacının tam olarak gerçekleştirilemediğini gözler önüne sermektedir²¹⁷. Yasalardaki ve uygulamalardaki farklılıklar ülkeler arasında veri akışını zorlaştırmaktadır. AB üyesi ülkelerdeki veri koruma yasalarının gerek içerik gerekse bakış açısı bakımından aralarında çok ciddi farklar olduğu öne sürülmüştür²¹⁸. Söz konusu farklılıklar ise kişisel verilerin ekonomik anlamdaki değeri düşünüldüğünde ekonomik alanda olumsuz sonuçlara yol açmaktadır²¹⁹. Ülkelerde veri koruma hususunda farklılıklar olması veri akışını engelleyecek ve bunun sonucunda ekonomi olumsuz anlamda etkilenecektir. Söz konusu ikilemler 95 tarihli AB Direktifi'nin uygulamasındaki çeşitlilikten kaynaklanmaktadır²²⁰. Saydığımız nedenler *data protection* konusunda yeni düzenlemelerin yapılması ihtiyacına işaret etmektedir.

GDPR'ın amacı kişisel verilerin korunması konusunda AB Direktifi'nde olmayan uyumun sağlanmasıdır²²¹. Bu uyum sonucunda ülkeler arası veri akışı hızlı ve rahat bir zeminde gerçekleşebilecektir. Ülkeler arasındaki uyumu sağlayacak yeni bir

²¹⁷ **Başalp, Nilgün**, “Avrupa Birliği Veri Koruması Genel Regülasyonu’nun Temel Yenilikleri”, MÜHF-HAD, 2015, C. 21, S. 1, s. 81-82.

²¹⁸ **Kuner**, s. 33.

²¹⁹ GDPR’ın 2. paragrafında ekonomik birliğin güçlendirilmesinin amaçlandığı vurgulanmıştır.

²²⁰ GDPR, 9. paragraf.

²²¹ GDPR, 3. paragraf.

düzenlemenin, AB'deki işletmelerin, yıllık 2 milyar Euro civarında bir yükten kurtulmalarını sağlayacağı düşünülmektedir²²².

Teknolojik gelişmelerin geldiği boyut ve küreselleşme, halihazırda olan kişisel verilerin korunması ihtiyacını arttırmıştır. Zira kişisel verilerin işlenmesi çok ciddi boyutlara ulaşmıştır. Gün geçtikçe de kişilerin bilgilerindeki işlenme miktarı artmaya devam etmektedir. Kişisel verilerin işlenmesindeki artış, haliyle bu verilerin paylaşılma miktarını da arttırmıştır. Saydığımız teknolojik gelişmelerle kişisel verilerin ülkeler arasındaki akışı artmış ve hızlanmıştır. Bu gelişmeler, birçok fayda sağladığı gibi kişiler açısından riskleri de beraberinde getirmektedir. İşlenen ve paylaşılan veri miktarı ne kadar artarsa verilerin korunmasıyla ilgili riskler de o kadar artacaktır. Bu nedenle kişisel verilerin yeni gelişmelere cevap verecek şekilde etkin olarak korunması gerekmektedir²²³. Günümüzde nerdeyse herkesin birden çok sosyal medya hesabının olması ve sosyal medya kullanımındaki dehşet artış kişisel verilerinin korunması açısından güncel bir düzenlemeyi mecbur kılmıştır²²⁴.

Saydığımız tüm nedenlerle, AB, AB Direktifi gibi verilerin korunmasındaki düzenleme serbestini üye ülkelere bırakmak yerine ülkelerde direkt olarak bağlayıcı olacak şekilde GDPR'ı yürürlüğe sokmuştur²²⁵. Bu noktada, GDPR'ın neden AB Direktifi gibi direktif olarak değil de tüzük olarak kabul edildiğinin irdelenmesi gerekmektedir. AB'nin hukuki tasarrufları "*Avrupa Birliği'nin İşleyişi Hakkındaki*

²²² Akıncı, AB Tüzüğü, s. 5.

²²³ GDPR, 6. paragraf.

²²⁴ Başalp, AB Regülasyonu, s. 85.

²²⁵ Başalp, AB Regülasyonu, s. 83.

*Antlaşma*²²⁶” (“**ABİHA**”)’nın 288. maddesinde sayılmıştır²²⁷. ABİHA m. 288/1 uyarınca “Kurumlar, Birliğin yetkilerinin kullanılması için tüzük, direktif, karar, tavsiye ve görüşler kabul eder.”

ABİHA m. 288/3’de ise direktifler düzenlenmiştir. Buna göre “Direktifler, muhatap alınan her üye devleti, ulaşılması gerekli sonuçları itibarıyla bağlar, şekil ve yöntem seçimini ise ulusal otoritelere bırakır.” Görüldüğü üzere direktifler temel hususları belirtip düzenlemeler konusunda üye ülkelere serbesti tanımaktadır. Bu da farklı düzenlemelerin, farklı uygulamaların ve farklı yorumların temel sebebidir. Üye ülkeler tarafından ulusal anlamda düzenleme yapılmazsa direktifler, ülkede yürürlüğe girmeyecektir. Ancak tüzükler doğrudan uygulama gücünü taşıdığından ayrıca ülke içinde söz konusu konuda bir düzenleme yapılmasına gerek kalmamaktadır. Başka bir ifadeyle, tüzüklerin üye ülkelerde yürürlüğe girmesi için herhangi bir iç hukuk düzenlemesine gerek yoktur. ABİHA m 288/2’ye göre “Tüzükler genel uygulama alanına sahiptir. Bütünüyle bağlayıcıdır ve tüm üye devletlerde doğrudan uygulanır.” Tüzük, AB çapında yürürlüğe girdiği zaman üye ülkelerde de otomatikman yürürlüğe girmektedir²²⁸. Bu da AB çapında kişisel verilerin korunması mevzuatını tekleştirecek ve temel kaynak olan GDPR’a bağlayacaktır²²⁹.

²²⁶ ABİHA’nın Türkçe metni için bkz. <https://www.ab.gov.tr/files/pub/antlasmalar.pdf> (E.T.: 15.04.2020).

²²⁷ Bu konuda detaylı bilgi için bkz. **Baykal, Sanem/Göçmen, İlke**, “Avrupa Birliği Hukukunun Kaynakları Bakımından Normlar Hiyerarşisi”, Prof. Dr. Erdal Onar’a Armağan, C. I, Ankara 2013, s. 325 vd.

²²⁸ **Başalp**, Kişisel Veri, s. 28.

²²⁹ **Akıncı**, AB Tüzüğü, s. 14.

GDPR hazırlık çalışmalarına 2012 yılında başlanmış ve söz konusu çalışmalar 4 yıl sonra 2016 yılında tamamlanmıştır²³⁰. GDPR AB Resmi Gazetesi olan OJ'de 04.05.2016 tarihinde yayımlanmıştır. GDPR m. 99 gereğince işbu tüzük 25 Mayıs 2018 tarihinden itibaren uygulanacaktır. GDPR'ın yürürlüğe girmesi ile birlikte “95 tarihli 95/46/EC Sayılı AB Direktifi” yürürlükten kalkmıştır²³¹.

Kişisel veri alanındaki son düzenleme olması, bilişim alanındaki son gelişmeler göz önüne alınarak düzenlenmiş olması ve birçok ülke tarafından kabul görmesi GDPR'ı önemli kılmaktadır. Her ne kadar KVKK hazırlanırken 95 tarihli AB Direktifleri esas alınmış olsa da aradan 20 yıldan fazla bir süre geçmiştir. Bu nedenle en güncel düzenleme olan GDPR'ın hem hukuki düzenlemelerde hem de uygulamada dikkate alınması gerekmektedir. Biz de bu nedenle ilgili yerlerde GDPR ilgili hükümlerine değinmeye çalıştık. Ancak burada tarafımızca mühim görülen ve yenilikler getiren GDPR hükümlerine değinilecektir.

2. GDPR'ın Kapsamı

GDPR incelendiğinde uygulama alanının²³² geniş tutulduğu söylenebilecektir. GDPR m. 3/2'ye göre “Veri sorumlusu veya veri işleyen AB sınırlarında olmasa dahi, AB'deki ilgili kişilerin kişisel verilerinin işlendiği iki durumda:

a- AB'deki ilgili kişilere mal ya da hizmet sunulması durumunda veya

b- AB'deki ilgili kişilerin AB içindeki davranışların izlenmesi durumunda GDPR

²³⁰ Akıncı, AB Tüzüğü, s. 5.

²³¹ GDPR, 171. paragraf; GDPR m. 94.

²³² GDPR'ın uygulama alanı ile ilgili detaylı bilgi için bkz. Çekin, Mesut Serdar, Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku, 2.Baskı, İstanbul 2019, s. 32-39.

uygulanır.”

GDPR’ın uygulanması için veri sorumlusu ya da veri işleyen illaki AB sınırları içinde olması gerekmemektedir. Yukarıda saydığımız bazı durumlar söz konusu olduğunda AB sınırları dışındaki veri sorumlusu ya da veri işleyenler de GDPR kapsamına dahil olacaktır. Bu durumlardan ilki “*AB’deki ilgili kişilere mal ya da hizmet sunulması*” durumudur. Buna göre AB’deki kişilerin kişisel verilerinin işlenmesi durumunda GDPR uygulanacaktır. AB’deki kişilerin illaki AB vatandaşı olması gerekmemektedir²³³. Ancak GDPR’ın uygulanabilmesi için bu işleme, mal ya da hizmet sunumuna ilişkin olmalıdır.

Veri sorumlusu veya veri işleyen AB dışında da olsa GDPR’ın uygulama alanı bulması çok önemli bir düzenlemedir. Örneğin Türkiye’deki bir veri sorumlusu şirketin AB’deki ilgili kişilere internet üzerinden satış yapması durumunda GDPR uygulanacaktır. Keza Türkiye’den AB’ye ihracat yapılması durumunda GDPR uygulama alanı bulacaktır. Bu nedenle AB dışında olup da AB’deki ilgili kişilere mal ya da hizmet sunanların GDPR’a riayet etmesi önem arz etmektedir.

AB dışındaki veri sorumlusu ya da veri işleyenlere GDPR’ın uygulanacağı 2. durum ise “*AB’deki ilgili kişilerin AB içindeki davranışlarının izlenmesi*” durumudur. Veri işleyenler tarafından kişilerin özellikle internetteki dolaşımı, davranışları, gezindiği internet siteleri izlenebilmektedir. Bu davranışlar analiz edilerek kişiler hakkında kimi sonuçlara varılabilmektedir. Çerezler ve kişilere özgü reklamlar vb. yöntemlerle günümüzde sıklıkla karşılaşılmaktadır. İşte kişilerin davranışlarının izlenmesi anlamına gelen her durumda GDPR uygulanacaktır²³⁴. Örneğin kişilerin internette yaptığı

²³³ Çekin, Kişisel Veri, s. 36.

²³⁴ Çekin, Kişisel Veri, s. 39.

aramaları izleyen Google'a GDPR uygulanacaktır²³⁵.

3. Rıza Koşulları ve Çocuğun Rızası

Rıza (consent), detaylı bir şekilde GDPR m. 7'de hüküm altına alınmıştır²³⁶. GDPR m. 7/1 uyarınca veri işlenmesi rızaya dayandırılıyorsa; veri sorumlusu, rızanın alındığını ispatlamalıdır. GDPR m. 7/3'e göre ilgili kişi dilediği an rızasını geri alabilir. Veri işleme birden fazla amaca dayanıyorsa hepsi için rıza gösterilmelidir²³⁷.

Çocuklara özgü düzenleme ne AB Direktifi'nde ne de KVKK'da yer almıştır. Ancak GDPR'da çocukların kişisel verilerine özel olarak yer verilmiştir. Çocuklar, verilerin işlenmesinin sonuçları ve riskleri konularında daha bilinçsizdir. Bu nedenle çocukların kişisel verilerinin yetişkinlerden farklı olarak özel bir şekilde korunması gerekmektedir²³⁸. Çocuk söz konusu olduğunda şeffaflık ilkesi daha dikkatle uygulanmalıdır. Çocukların kişisel verileri işlenirken tercih edilen dil, çocukların anlayabileceği şekilde sade ve net olmalıdır²³⁹.

GDPR, çocuğun rızasını 8. maddede özel olarak düzenlemiştir. Buna göre,

²³⁵ Taştan, s. 16.

²³⁶ GDPR'daki rıza düzenlemesi ile ilgili detaylı bilgi için bkz. **Data Protection WP, Guidelines on Consent under Regulation 2016/679**, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051 (E.T.: 07.04.2020); **EDPB, Guidelines 05/2020 on consent under Regulation 2016/679**, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en (E.T.: 11.05.2020).

²³⁷ GDPR, 32. paragraf.

²³⁸ GDPR, 38. paragraf.

²³⁹ GDPR, 58. paragraf.

“Çocuğun 16 yaşından küçük olması durumunda, bilgi toplumu hizmetleri ile ilgili veri işlenmesi halinde rızanın çocuğun velisi tarafından (ana-baba) verilmesi gerekmektedir. Aksi halde bu işleme hukuka aykırı olacaktır. Üye devletler, bu hükümle ilgili olarak daha küçük bir yaş belirleyebilir. Ancak her halükarda veli rızasının aranmaması 13 yaşın altına indirilemez.”

KVKK’da çocuğun rızasıyla ilgili herhangi bir özel hüküm bulunmamaktadır. GDPR’a göre, aksine düzenleme yapılmamışsa 16 yaşından küçük çocukların verilerinin işlenmesinde velilerinin rızası aranacaktır. Üye devletler bu yaş sınırını aşağı çekebilirler. Ancak bunun da sınırı 13 yaştır. Yani GDPR’a göre, her halükarda 13 yaşından küçük çocukların verilerinin işlenmesinde velilerinin rızası gerekmektedir. Fikrimce söz konusu hüküm yerindedir. Bu nedenle benzer bir hükmün ülkemize uygun bir şekilde düzenlenerek KVKK’ya eklenmesi yerinde olacaktır. Çünkü çocuklar, internette yetişkinler kadar ve hatta daha fazla vakit geçirmektedir. Çocuklar sosyal medya hesaplarını ve oyun sitelerini sıklıkla kullanmaktadır. İnternet kullanım yaşı ise gün geçtikçe daha da aşağıya inmektedir. Çocukların internet kullanımlarında ise sayısız şekilde kişisel verileri işlenmektedir. Bu nedenle öncelikle çocuklara kişisel verilerin korunmasıyla ilgili eğitimler verilerek çocuklar bilinçlendirilmelidir. Aynı zamanda KVKK hükümleri ile de geleceğimiz olan çocukların kişisel verilerini korumaya özgü daha sıkı düzenlemeler getirilmelidir.

4. Unutulma Hakkı

Her insan hata yapar. İnsan hata yapmasa dahi geçmişte yaşadığı olumsuzlukları hatırlamak istemeyebilir. Her insanın hayatında hatırlamak istemeyeceği kötü anıları olabilir. Geçmişteki olumsuzlukların sürekli gün yüzüne çıkarılması ise gelecekteki olumlu davranışların önünde aksi kabul edilemez bir engeldir. Her insana geçmişteki yanlışları düzeltme şansı verilmelidir. Geçmişin sürekli insanın karşısına çıkması ise kötü

anılarının canlanmasına yol açacaktır. Kötü anıların ve geçmişin olumsuzlukların insanın ömür boyu önüne çıkacak olması ise toplumda korku ortamı yaratır. Teknolojik gelişmelerle birlikte, özellikle internette, uçsuz bucaksız bir bilgi denizi oluşmuştur. Bu veri denizinin büyük bir kısmını ise kişiler hakkında olumsuz çağrışım yaratabilecek bilgiler oluşturmaktadır. Örneğin işe alımlarda dahi, işverenler, başvuranları özellikle arama motorlarından araştırmaktadır. Kişinin çok uzun yıllar önce yaşadığı bir olayın dahi bu veri denizinde bulunması kişi hakkında olumsuz sonuçlar doğurabilmektedir. En basitinden verdiğimiz örnekte, kişi işe alınmama tehlikesiyle karşılaşabilecektir. Kişi hiçbir hata yaşamamış olsun ya da hakkındaki bilgiler olumsuz olmamış olsun. Buna rağmen kişi hatırlanmak istemeyebilir. Zira kişi hakkında yalan bilgiler de bu veri denizinde yer alabilmektedir. Bu nedenle bu veri denizi bazen veri çöplüğüne dönüşmektedir. Diğer bir deyişle, bu deniz, ucu bucağı olmayan sonsuz bir çöplük haline dönüşmeye başlamıştır. İşte tüm bu olumsuzluklar karşısında kişinin geçmişinin hatırlanmamasının istenmesi kişinin en doğal hakkıdır. Tabiri caizse, unutulma hakkı, “geçmişe sünger çekmek” olarak ifade edilebilir. Kişi hayatına yeni bir sayfa açmak istiyor olabilir. Bunun en doğal sonucu da geçmişte kalan eski sayfaları ortadan kaldırmaktır. Bu açıklamalarımız unutulma hakkının sınırsız bir hak olduğu sonucunu doğurmamalıdır. Unutulma hakkından geçmişteki her türlü bilginin yok edilmesi sonucu çıkarılmamalıdır. Her hakta olduğu gibi, unutulma hakkının da sınırları vardır. Yani unutulma hakkı da elbette belirli sebeplerle sınırlanabilecektir. Örneğin, haberleşme hürriyeti veya basın hürriyeti nedenleri. Bu hak mevzuatımızda henüz tanınmadığından hakkın sınırlarından da net bir şekilde bahsedilememektedir. Ancak aralarındaki yakın ilişki nedeniyle, kanaatimizce, kişisel verilerin korunması hakkının sınırları unutulma hakkında da uygulanabilir.

Unutulma hakkının ortaya çıkış serüvenine bakıldığında, İsviçre Federal Mahkemesi’nin, içtihatlarıyla, unutulma hakkının kabul edilmesine önayak olduğu

gözlemlenebilir²⁴⁰. Unutulma hakkı (“*right to be forgotten*”), GDPR m. 17’de açıkça koruma altına alınmıştır. Buna göre ilgili kişinin, gecikmeksizin verilerinin silinmesini veri sorumlusundan isteme hakkı bulunmaktadır. Unutulma hakkı gereği, işlenen verilere artık gerek duyulmaması, veri işlenmesi için gerekli olan rızanın geri alınması, hukuka aykırı bir işleme olması gibi durumlarda veri sorumlusunun söz konusu verileri silmesi gerekmektedir. Unutulma hakkı kısaca veri sahibi kişinin verisinin işlenmesini istememesi, unutulmak istemesi hakkıdır. İlgili kişinin her hakkının karşısında veri sorumlusunun bir yükümlülüğü bulunmaktadır. İlgili kişinin unutulma hakkı karşısında veri sorumlusunun kişisel verileri silme yükümlülüğü bulunmaktadır.

Unutulma hakkı, kişisel verilerin korunması hakkı ile yakından ilişkilidir. Daha önce bahsettiğimiz gibi, kişisel verilerin temeli insan onuruna ve kişiliğin serbestçe geliştirilmesine dayanmaktadır. Unutulma hakkının temelini de aynı değerlere dayandığı söylenebilir²⁴¹. Unutulma hakkının kişisel verilerin korunması hakkıyla kesiştiği birçok nokta bulunmaktadır. Ancak yine de unutulma hakkının, bağımsız bir hak olarak kabul edilmesi gerektiği düşünülmektedir²⁴².

GDPR m. 17/2 gereğince veri sorumlusu, ilgili kişinin kişisel verilerini herkese açık hale getirmesi durumunda (örneğin internet sitesinden yayımlaması ve Google arama motorunda arama yapanların bu bilgilere ulaşabilmesi) kişisel verilerin silinmesi için (söz

²⁴⁰ İsviçre Federal Mahkemesi’nin unutulma hakkıyla ilgili “BGE 109 II 353”, “BGE 111 II 209”, “BGE 122 III 449”, “BGE 127 I 145ff”, “BGE 129 III 529” kararları için bkz. **Başalp**, AB Regülasyonu, s. 93-97.

²⁴¹ **Akgül, Aydın**, “*Kişisel Verilerin Korunmasında Yeni Bir Hak: Unutulma Hakkı ve AB Adalet Divanı’nın Google Kararı*”, TBB Dergisi, 2015, Y. 27, S. 116, s. 14.

²⁴² **Yavuz, Can**, İnternet’teki Arama Sonuçlarından Kişisel Verilerin Kaldırılması-Unutulma Hakkı, Güncellenmiş ve Genişletilmiş 2. Baskı, Ankara 2018, s. 57.

konusu verilerin kullanıldığı, çoğaltıldığı yerler de dahil olmak üzere) gerekenleri yapmalıdır. Yani kişisel verileri kamuya açıklayan veri sorumlusunun unutulma hakkı gereği işlediği kişisel verileri silmesi de yükümlülüğünü tam olarak yerine getirmesi için yeterli olmamaktadır. Veri sorumlusu ayrıca söz konusu verileri işleyen başka veri sorumlularını da nüshaları ve bağlantıları silmeleri için bilgilendirmelidir²⁴³. Günümüzde bilgilerin yayılma hızı düşünüldüğünde, bu düzenleme yerinde olmuştur. Zira veri sorumlusu tarafından işlenen veri paylaşıldığında çok hızlı bir şekilde yayılabilmektedir. Örneğin veri sorumlusu (A), internet sitesinde (B) kişinin kişisel verilerini işlemiş olsun. Veri sorumlusu (A), işlediği bu verileri kendi çapında imha etse dahi arama motorlarına yazıldığında (B)'nin imha edilen verilerine ulaşılabilir. Zira gelişen teknolojide kişisel veri özellikle internet ortamında bir kere paylaşıp yayıldıktan sonra tamamen imha edilmesi neredeyse imkansız hale gelmektedir. Birçok sitede söz konusu veri paylaşılabilmektedir. Bu nedenle veri sorumlusu, kişisel verileri herkese açık hale getiriyorsa yalnızca kendisinin imha etmesi yetmemektedir. Aynı zamanda söz konusu verileri işleyen başka veri sorumlularını da verileri silmeleri konusunda bilgilendirmelidir. Verilerin internetteki yayılım hızı düşünüldüğünde veri sorumlusunun veri işleyen herkese bu bilgilendirmeyi nasıl yapacağı merak konusudur. Ancak GDPR m. 17/2 bu konuda bir açık kapı bırakarak, veri sorumlusu tarafından *“mevcut teknoloji ve uygulama maliyetinin göz önünde bulundurularak”* bilgilendirilme yapılmasını öngörmüştür.

Unutulma hakkı, çocuklar için özel önem teşkil etmektedir. Özellikle internette kişisel verilerinin işlenmesinin yol açabileceği riskleri ve sonuçları öngöremeyen çocuklar tarafından rıza verilmesi ve sonrasında söz konusu bilgilerin internetten kaldırılmasını istemeleri durumunda, unutulma hakkı gereği bu talepleri karşılanmalıdır.

²⁴³ GDPR, 66. paragraf.

İlgili kiři söz konusu talebi sunduđu zaman yetiřkin olmuř olsa dahi unutulma hakkı geređince talebi yerine getirilmelidir²⁴⁴. Daha önce de belirttiđimiz gibi, veri koruma ile ilgili koruyucu düzenlemeler çocuklar söz konusu olduđuunda daha sıkı uygulanmalıdır. Çocuđuun bilinçsizken kişisel verilerinin işlenmesine dair verdiđi rızalar geleceđini olumsuz yönde etkilememelidir. Eđer etkiliyorsa unutulma hakkı geređi bu veriler silinmelidir.

Unutulma hakkının sınırsız olarak kullanımı 3. kişilerin haklarını ihlal edebilir. Unutulma hakkının kullanılması durumunda başka bir hak ihlal edilebilir. Bu nedenle karşı karşıya gelen iki hak arasında adil bir denge kurulmalıdır²⁴⁵. “*Haberleşme ve ifade özgürlüğü*”²⁴⁶, “*kitle iletişim özgürlüğü*”²⁴⁷ ve “*basın özgürlüğü*”²⁴⁸, bu hakla karşı karşıya gelebilecek değere örnek olarak verilebilir. Unutulma hakkı, sınırsız ve mutlak bir hak değildir. GDPR m. 17/3’de unutulma hakkının kullanılamayacağı haller sayılmıştır. Haberleşme ve ifade özgürlüğüünün kullanılması bu hallere dahil edilmiştir²⁴⁹. Yine halk sağlığı alanındaki kamu yararı nedeniyle işleme yapılmasında unutulma hakkı sınırlanabilecektir²⁵⁰. Kanunun verdiđi yetkinin kullanılması nedeniyle de bu hak

²⁴⁴ GDPR, 65. paragraf.

²⁴⁵ **Akkurt, Sinan Sami**, “17.06.2015 Tarih, E. 2014/4-56, K. 2015/1679 Sayılı Yargıtay Hukuk Genel Kurulu Kararı ve Mukayeseli Hukuk Çerçevesinde Unutulma Hakkı”, AÜHFD, 2016, C. 65, S. 4, s. 2624.

²⁴⁶ **Akkurt**, s. 2617.

²⁴⁷ **Akkurt**, s. 2619.

²⁴⁸ **Akkurt**, s. 2621.

²⁴⁹ GDPR, m. 17/3/a.

²⁵⁰ GDPR, m. 17/3/c.

sınırlanabilecektir²⁵¹. Kamu yararına arşiv, bilimsel-tarihi araştırma veya istatistiki nedenlerle²⁵² işleme yapılmasında da unutulma hakkı sınırlanabilecektir. Ancak saydığımız son nedene dayanarak unutulma hakkının sınırlandırılabilmesi için unutulma hakkının kullanılması durumunda işleme amacına ulaşılmasının imkansız hale gelmesi gerekmektedir.

Ülkemiz mevzuatında, ne KVKK da ne de başka bir hukuki düzenlemede unutulma hakkı açıkça yer almamakta ve korunmamaktadır. 5651 sayılı Kanun'da internette “*içeriğin kaldırılması ve erişimin engellenmesi*” düzenlemeleri mevcuttur. Ancak söz konusu düzenlemenin GDPR’da düzenlenen unutulma hakkını ifade ettiği söylenemez²⁵³. Kanımızca ülkemizde ileride yapılacak düzenlemelerde unutulma hakkının açıkça bir hak olarak tanınması, korunması ve KVKK’ya eklenmesi elzemdir.

Ülkemiz mevzuatında “*unutulma hakkı*” açıkça bulunmasa da hem AYM hem de Yargıtay söz konusu hak ile ilgili çok önemli kararlara imza atmışlardır. Yargıtay’ın ünlü kararında²⁵⁴ unutulma hakkı detaylı bir şekilde incelenmiş, tanımı yapılmış ve kişisel verilerin korunması hakkı ile ilişkisi üzerinde durulmuştur. Davanın konusu, cinsel saldırı suçu mağduru olan kişinin isminin gizlenmeden, açıkça bir kitapta yer almasıdır. Davacı, mağdur olduğu olayla ilgili olarak ismine açıkça yer verilmesi sebebiyle manevi tazminat talebinde bulunmuştur. Kararda unutulma hakkının ihlal edilmesi sebebiyle manevi tazminat talebinin kabul edilmesi gerektiğine karar verilmiştir. Görüldüğü üzere bu kararda Yargıtay, unutulma hakkını açıkça kabul etmiş, ve söz konusu hakka dayanarak

²⁵¹ GDPR, m. 17/3/b.

²⁵² GDPR m. 17/3/d.

²⁵³ **Henkoğlu**, s. 108.

²⁵⁴ Yargıtay HGK., 17.06.2015 T., 2014/4-56 E., 2015/1679 K., (Kazancı, E.T.: 22.04.2020).

kişiyne manevi tazminat verilmesi gerektiğine hükmetmiştir. Kararda unutulma hakkı açıkça kabul edilmiş ve detaylarıyla incelenmiştir. Bu karara göre “Unutulma hakkına gelince; unutulma hakkı ve bununla ilişkili olan gerektiği ölçüde ve en kısa süreliğine kişisel verilerin depolanması veya tutulması konuları, aslında kişisel verilerin korunması hakkının çatısını oluşturmaktadır. Her iki hakkın temelinde bireyin kişisel verileri üzerinde serbestçe tasarruf edebilmesini, geçmişin engeline takılmaksızın geleceğe yönelik plan yapabilmesini, kişisel verilerin kişi aleyhine kullanılmasının engellenmesini sağlamak yatmaktadır. Unutulma hakkı ile geçmişinde kendi iradesi ile veya üçüncü kişinin neden olduğu bir olay nedeni ile kişinin geleceğinin olumsuz bir şekilde etkilenmesinin engellenmesi sağlanmaktadır. Bireyin geçmişinde yaşadığı olumsuz etkilerden kurtularak geleceğini şekillendirebilmesi bireyin yararına olduğu gibi toplumun kalitesinin gelişmişlik seviyesinin yükselmesine etkisi de tartışılmazdır. Unutulma hakkı; üstün bir kamu yararı olmadığı sürece, dijital hafızada yer alan geçmişte yaşanan olumsuz olayların bir süre sonra unutulmasını, başkalarının bilmesini istemediği kişisel verilerin silinmesini ve yayılmasının önlemesini isteme hakkı olarak ifade edilebilir.” Genel olarak unutulma hakkı tanımları, dijital ortamı kapsamaktadır²⁵⁵.

Ancak bu davanın konusu internet üzerinde işlenen veriler değildir. Zira mağdurun ismine basılı kitapta yer verilmiştir. Yargıtay burada da isabetli olarak sadece dijital ortamın değil, herkesin rahatlıkla ulaşabileceği yerlerdeki veriler için de unutulma hakkının geçerli olması gerektiğini belirtmiştir. Karara göre,²⁵⁶ “Ayrıca şunun da ifade edilmesi gereklidir ki; unutulma hakkı tanımlarına bakıldığında her ne kadar dijital

²⁵⁵ **Gülener, Serdar**, “Dijital Hafızadan Silinmeyi İstemek: Temel Bir İnsan Hakkı Olarak Unutulma Hakkı”, TBB Dergisi, 2012, Y. 25, S. 102, s. 226.

²⁵⁶ Yargıtay HGK., 17.06.2015 T., 2014/4-56 E., 2015/1679 K., (Kazancı, E.T.: 22.04.2020).

veriler için düzenlenmiş ise de, bu hakkın özellikleri ve bu hakkın insan haklarıyla arasındaki ilişkisi dikkate alındığında; yalnızca dijital ortamdaki kişisel veriler için değil, kamunun kolayca ulaşabileceği yerde tutulan kişisel verilere yönelik olarak da kabul edilmesi gerektiği açıktır.” Söz konusu kabul, sadece internet ortamında değil, kitap gibi açık erişimin olduğu ortamlarda da unutulma hakkına uyulması açısından elzemdir. Başka bir ifadeyle, bu bakış, unutulma hakkının sadece dijital ortama indirgenmesini engellemiş olacaktır.

AYM’nin de ünlü bir unutulma hakkı kararı²⁵⁷ bulunmaktadır. Bu karara yansıyan olayda, başvuru, yıllar önce uyuşturucu kullandığı şüphesiyle yargılanmasına ilişkin haberlerin hala internette ulaşılabilir olduğunu belirtmekte ve ilgili haberlerin kaldırılmasını istemektedir. AYM, bu kararında unutulma hakkına dayanarak söz konusu haberlere erişimin engellenmesi gerektiğini belirtmiştir. Daha önce de belirttiğimiz gibi, unutulma hakkı, mevzuatımızda açıkça hüküm altına alınan bir hak değildir. Ancak AYM, Anayasa’nın 5, 17 ve 20. maddelerinden unutulma hakkına ulaşılabilceği sonucuna varmıştır. Karara göre, “Unutulma hakkı kişilerin manevi varlıklarını geliştirmelerine bir fırsat vermek açısından devletin pozitif yükümlülüğünün bir sonucudur.” Kararda AYM, kişisel verilerin korunması hakkı ile unutulma hakkı ilişkisine özel vurgu yapmıştır. AYM’ye göre “Özellikle kişisel verilerin korunması hakkı kapsamında kişisel verilerin silinmesini talep edebilme hakkı, kişilerin geçmişlerinde yaşadıkları olumsuzlukların unutulmasına imkân tanımayı kapsamaktadır.” Yine karara göre, devlet tarafından, bireylere, geçmişte kalan olayların 3. kişilerce öğrenilmesi önlenerek, bireylere “yeni bir sayfa açma” şansı verilmelidir.

Kanaatimizce bu karar gerçek manada önemli ve değerlidir. 2000’li yılların ilk çeyreğinde artık kişilerin unutulma hakkı ulusal ve uluslararası alanda kabul görmektedir.

²⁵⁷ AYM, 03.03.2016 T., 2013/5653 Başvuru N., RG. 24.08.2016, S. 29811.

Doktrin ve içtihat tarafından unutulma hakkının kabul edilmesi değerlidir. Yine de bu hakka hem Anayasa’da hem de KVKK’da yer verilmesi gerekmektedir. Zira bu hakkı açıkça mevzuatta tanıma, hak ve özgürlükler açısından, ülkemiz adına atılan büyük bir adım olacaktır.

5. Kısıtlama Hakkı

İlgili kişinin bazı durumlarda veri sorumlusundan kişisel verilerin kullanımının kısıtlanmasını talep etme hakkı bulunmaktadır. Kişisel verilerin işlenmesini kısıtlama hakkı (*“right to restriction of processing”*)²⁵⁸ GDPR m. 18’de hükme bağlanmıştır. Buna göre, ilgili kişi tarafından kişisel verinin doğruluğuna, silinmesine itiraz edilmesi gibi durumlarda bu hak söz konusu olabilir. İlgili kişi tarafından verinin doğru olmadığı yönünde bir iddia varsa bu iddia sonuçlanana kadar veri sorumlusu veri işlemeyi kısıtlamalıdır. Böyle bir durumda kişisel veriler, saklama hariç, yalnızca GDPR m. 18/2’de sayılan bazı durumlarda işlenebilir.

Son olarak belirtmek gerekir ki, unutulma hakkı ve kısıtlama hakkına karşılık veri sorumlusunun bir yükümlülüğü de bildirim yükümlülüğüdür. Kural olarak veri sorumlusu, kişisel verilerin kısıtlandığını, silindiğini veya düzeltildiğini verilerin paylaşıldığı alıcılara bildirmelidir. Ancak bu bildirim imkansızsa veya aşırı bir efor gerektiriyorsa yükümlülük söz konusu olmaz²⁵⁹.

²⁵⁸ *“Restriction of processing, saklanan kişisel verilerin gelecekte işlenmelerini sınırlandırmak için işaretlenmesidir.”* GDPR m. 4/3.

²⁵⁹ GDPR, m. 19.

6. Veri Taşınabilirliği Hakkı

Veri taşınabilirliği hakkı (*“right to data portability”*) GDPR m. 20’de hüküm altına alınmıştır. Hükme göre *“İlgili kişinin, kendisiyle ilgili işlenen kişisel verileri, yapılandırılmış, yaygın olarak kullanılan ve makine tarafından okunabilen bir formatta alma hakkı ve başka bir veri sorumlusuna iletme hakkı bulunmaktadır. Bu hakkın kullanılabilmesi için veri işleme, rızaya veya sözleşmeye dayanmalıdır. Ayrıca bu hakkın kullanılabilmesi için veri işleme faaliyetinin otomatik yolla gerçekleştirilmesi gerekmektedir.”* Kişisel verilerin işlenmesinin rıza ya da sözleşme dışında bir sebebe dayanması durumunda söz konusu hak kullanılamaz. Otomatik olmayan bir yolla veri işlenmesi durumunda da hak kullanılamayacaktır. Hakkın gereği gibi kullanılabilmesi için veri sorumluları, veri taşınabilirliğini kolaylaştıran formatlar geliştirmelidir²⁶⁰. Maddenin 3. fıkrasında hakkın kullanılamayacağı haller sayılmıştır²⁶¹.

7. Veri Koruma Etki Değerlendirmesi ve Ön Danışma

AB Direktifi’nin 18. maddesi ile kişisel verilerin işlendiğinin denetim makamına haber verilmesi için genel bir bildirim yükümlülüğü getirilmiştir. Söz konusu zorunluluğun idari ve mali külfetler getirmesine rağmen kişisel verilerin korunmasına kayda değer bir katkı sağladığı söylenemez. Bu vesileyle, fayda sağlamayan genel bildirimin GDPR ile kaldırılması yerinde olmuştur. Zira Direktif’teki genel bildirim, kişisel veri işleme açısından hiçbir ayırım gözetmemektedir. GDPR’a göre her türlü veri

²⁶⁰ GDPR, 68. paragraf.

²⁶¹ Veri taşınabilirliği hakkıyla ilgili detaylı bilgi için bkz. **Data Protection WP**, Guidelines on the right to data portability, https://edpb.europa.eu/our-work-tools/our-documents/guideline/right-data-portability_en (E.T.: 07.04.2020).

işleme değil, kişiler açısından yüksek miktarda risk teşkil edebilecek olan işlemler için aşağıda açıklayacağımız değerlendirme ve denetleme kuruluna bildirim yapılmalıdır²⁶². Geline son aşamada, AB nezdinde genel bildirim yerine, spesifik bildirim tercih edilmektedir. Ancak bizde ise veri sorumlularının yükümlülüklerinden olan VERBİS kaydı genel bildirim niteliğindedir. Fikrimce ileride KVKK’da yapılacak revizelerde bu kadar genel nitelikteki bir bildirim yükümlülüğü yerine GDPR m. 35’e benzer bildirim yükümlülüğünün getirilmesinin amaca daha iyi hizmet edip etmeyeceği tartışılmalıdır.

Veri koruma etki değerlendirmesi (*“VKED”*) (*“data protection impact assessment”*) yapmak, bazı durumlarda veri sorumlusu tarafından yerine getirilmesi gereken bir yükümlülüktür. Söz konusu değerlendirme GDPR m. 35’de düzenlenmiştir. Buna göre *“Kişisel verilerin işlenmesinin gerçek kişilerin temel hak ve özgürlükleri açısından risk oluşturabilme ihtimalinin bulunduğu hallerde, veri sorumlusu, kişisel verileri işlemeye başlamadan önce öngörülen işleme faaliyetinin kişisel verilerin korunması üzerindeki etkisinin bir değerlendirmesini yapar.”* VKED’in özellikle yeni teknolojiler kullanan ve kişiler açısından veri işlemenin risk oluşturma ihtimalinin olabileceği hallerde yapılması gerektiği unutulmamalıdır. Başka bir ifadeyle VKED, her veri işleme durumunda değil, özellikle *“profilleme gibi otomatik işlemlerde, hassas verilerin veya suçlara ilişkin kişisel verilerin işlenmesi durumlarında, halka açık bir alanın sistematik olarak izlenmesi gibi durumlarda”* yapılmalıdır²⁶³.

VKED, veri sorumlu tarafından, kişisel veri işlemeden önce, işleme yapılması durumunda kişilerin haklarının ihlal edilip edilmeyeceğinin değerlendirmesinin yapılmasıdır. VKED’ in yapılması ve veri sorumlusu tarafından verilerin bu değerlendirme çerçevesinde işlenmesi hem veri sorumlusunun hem de ilgili kişinin yararına olacaktır.

²⁶² **Akıncı**, Veri Mahremiyeti, s. 154-155; GDPR, 89. paragraf;

²⁶³ GDPR m. 35/3.

Zira VKED sonucuna göre veri sorumlusu hukuka aykırı veri işlemeden kaçınabilecek ve yaptırım veya tazminat talebiyle karşılaşma riski azalacaktır. Öte yandan değerlendirme yapıp ilgili kişinin haklarının ihlaline sebep olacak risklerin tespit edilmesi ve değerlendirmeye riayet edilmesi kişisel verilerin korunmasını sağlayacaktır.

Ön danışma (*“prior consultation”*), GDPR m. 36’da hüküm altına alınmıştır. Buna göre *“Veri sorumlusu tarafından yapılan veri koruma etki değerlendirmesi sonucunda kişisel verilerin işlenmesi durumunda yüksek bir riskle sonuçlanacağı (gerçek kişilerin hak ve özgürlükleri bakımından) öngörüliyorsa, kişisel veriler işlenmeden önce denetleme makamına danışılmalıdır.”* Etki değerlendirmesi ve ön danışma birbirini takip eden işlemlerdir. Ön danışma, veri işlenmeden önce veri işlemenin yaratacağı riskler konusunda bir kez daha düşünülmesini sağlayacaktır.

8. Veri Koruma Görevlisi

Veri koruma görevlisi (*“data protection officer”*) (**“DPO”**), GDPR’da düzenlenmiştir²⁶⁴. GDPR m. 37/1 uyarınca *“Veri sorumlusu ve veri işleyen tarafından; kişisel veri işlenmesinin mahkemeler haricindeki bir kamu kuruluşu veya organı tarafından gerçekleştirilmesi durumunda; veri sorumlusunun veya veri işleyenin ana faaliyetlerin doğası, kapsamı veya amaçları gereği ilgili kişinin büyük ölçekte, düzenli ve sistematik bir şekilde izlenmesini gerektiren bir veri işleme olması durumunda; veri sorumlusunun veya veri işleyenin ana faaliyetinin hassas veri veya suçlara ilişkin kişisel verilerin işlenmesinden oluşması durumlarında veri koruma görevlisi atanması*

²⁶⁴ Veri koruma görevlileri ile ilgili detaylı bilgi için bkz. **Data Protection WP, Guidelines on Data Protection Officers** (‘DPOs’), https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A (E.T.: 07.04.2020).

gerekmektedir.” Bu hükümde sayılan veri sorumlularının DPO ataması zorunludur.

GDPR m. 37/6’da belirtildiği üzere “*Veri koruma görevlisi, veri sorumlusunun veya veri işleyen personeli olabileceği gibi hizmet sözleşmesine göre görevlerini yerine getirebilir.*”

DPO’nun görevleri GDPR m. 39’da sayılmıştır. DPO’nun asıl görevi, atandığı veri sorumlusu ya da veri işleyen tarafından gerçekleştirilen veri işleme sürecinin GDPR ile uyumunu izlemektir²⁶⁵. Bu vesileyle, işlenen verilerin hukuka uygunluğu noktasında DPO atanması otokontrol bakımından faydalı olacaktır²⁶⁶. Ayrıca DPO’ya, veri sorumlusu ve veri işleyenleri kişisel verilerin korunması konusunda bilinçlendirme görevi verilmiştir. DPO denetim makamıyla işbirliği içerisinde olmalı, denetim makamı ile veri sorumlusu arasındaki teması sağlamalıdır²⁶⁷.

Ülkemizde veri koruma görevlisine ilişkin bir yasal düzenleme mevcut değildir. Kanımızca da KVKK’da özellikle büyük miktarda veri işleyen işletmelerde DPO atanma zorunluluğu getirilmesi yerinde olacaktır²⁶⁸.

9. Avrupa Veri Koruma Kurulu

GDPR ile birlikte, tüzel kişiliğe sahip, bağımsız bir organ olarak Avrupa Veri Koruma Kurulu²⁶⁹ (“*European Data Protection Board*”) kurulmuştur²⁷⁰. EDPB, AB

²⁶⁵ GDPR, 97. paragraf.

²⁶⁶ Başalp, s. 59.

²⁶⁷ GDPR, m. 39.

²⁶⁸ Akıncı, Veri Mahremiyeti, s. 153.

²⁶⁹ Bundan böyle EDPB olarak anılacaktır.

²⁷⁰ GDPR m. 68.

Direktifi'nin 29. maddesi ile kurulan “*Working Party*”nin karşılığıdır²⁷¹. EDPB’de her üye ülkenin denetim makamı başkanı yer alacaktır. EDPB’nin asıl görevi GDPR’ın tutarlı bir şekilde uygulanmasını sağlamaktır. EDPB’nin görevleri GDPR m. 70’de sayılmıştır. Önceden AB’de veri koruma konusunda farklılaşan yaklaşımlar varken EDPB ile birlikte tekdüze bir uygulamaya geçileceği düşünülmektedir²⁷². GDPR’ın çeşitli yerlerinde kişisel verilerin korunmasıyla ilgili hususlarda EDPB’nin rehberler (“*guidelines*”) hazırlayabileceğinin altı çizilmiştir²⁷³. EDPB tarafından hazırlanan ve hazırlanacak olan söz konusu rehberler, AB’nin veri korumasıyla ilgili görüşlerini yansıtmaları bakımından önem arz etmektedir²⁷⁴.

10. İdari Para Cezası

GDPR m. 83’de veri ihlali durumunda idari para cezası (“*imposition of administrative fine*”) kesileceği hükme bağlanmıştır²⁷⁵. Denetim makamları, söz konusu cezaların caydırıcı ve orantılı olmasına özen göstermelidir²⁷⁶. 83. madde incelendiğinde

²⁷¹ GDPR, 139. paragraf.

²⁷² Başalp, AB Regülasyonu, s. 86.

²⁷³ GDPR 72.-77.-124. paragraflar.

²⁷⁴ EDPB tarafından hazırlanan rehberlere ulaşmak için bkz. https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en (E.T.: 07.04.2020).

²⁷⁵ GDPR’da düzenlenen idari para cezaları ile ilgili detaylı bilgi için bkz. **Data Protection WP**, Guidelines on the application and setting of administrative fines for the purpose of the Regulation 2016/679, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237 (E.T.: 07.04.2020).

²⁷⁶ GDPR m. 83/1.

idari para cezaları miktarlarının caydırıcı olması amacıyla yüksek olarak belirlendiği gözlemlenmektedir. Denetim makamları tarafından verilebilen söz konusu cezalar 20 Milyon Euro’ya kadar çıkabilmektedir²⁷⁷. Veri ihlali yapan şirketin dünya çapındaki yıllık cirosunun 20 Milyon Euro’dan fazla olması halinde ise bu şirketin dünya çapındaki yıllık cirosunun %4’üne kadar idari para cezası uygulanabilecektir. Bu cezaların düzenlenmesinin asıl amacı GDPR’ın uygulanmasını güçlendirmektir.

GDPR’da idari para cezalarının sadece alt ve üst sınırı belirlenen belirli bir miktar olarak değil, aynı zamanda ciroya bağlı oransal olarak da belirlenmesi yerinde olmuştur. KVKK incelendiğinde ise cezaların alt ve üst sınırı belirlenen belirli bir miktar olarak belirlendiği görülecektir. Cezaların oransal olarak belirlenmesi ise çok yüksek gelir elde edilen şirketler için caydırıcı olmaktadır. Zira çok büyük şirketlerin yıllık cirosunun %4’üne kadar kesilecek ceza çoğu zaman KVKK’daki sabit miktarların üstünde olacaktır. Fikrimce şirketlerin dünya çapındaki yıllık cirosuna göre oransal bir para cezası öngören GDPR düzenlemesine benzer bir hüküm KVKK’ya eklenmelidir. Aksi halde büyük şirketler, kişisel verileri işlemekten elde edecekleri kar yanında çok küçük kalan para cezalarını ödemeyi göze alarak hukuka aykırı olarak veri işlemeye devam edeceklerdir.

III. Ulusal Düzenlemeler

A. 5237 Sayılı TCK

Türk Ceza Kanunu (**“TCK”**) 9. bölümünde (TCK m. 132-140) *“özel hayata ve hayatın gizli alanına karşı suçlar”* düzenlenmiştir. Kişisel verilerle ilgili suçlar (TCK m. 135-140) bu bölümde hüküm altına alınmıştır. TCK m. 135’de *“kişisel verilerin kaydedilmesi suçu”*, TCK m. 136’da *“kişisel verileri hukuka aykırı olarak verme veya*

²⁷⁷ GDPR m. 83/4-5-6.

ele geçirme suçu” ve TCK m. 138’de “*kişisel verileri yok etmeme suçu*” düzenlenmiştir. Ancak belirtmek gerekir ki, TCK’nın kabul tarihi olan 2004’de kişisel verilerin korunmasıyla ilgili bir kanun mevzuatımızda bulunmamaktaydı. TCK’nın kişisel veriyle ilgili suçlarla ilgili bölümü incelendiğinde kişisel veri tanımı yapılmadığı görülmektedir. TCK 135. madde gerekçesinde kişisel veri tanımlanmaya çalışılmış ve suçun tanımı ile ilgili olarak AK 108 No.lu sözleşmeye atıf yapılmıştır. Ayrıca o tarihte KVKK gibi kişisel verilere özgü bir yasa bulunmadığından, TCK’da sayılan fiillerin ne zaman hukuka aykırı kabul edeceği hususunda soru işaretleri bulunmaktaydı²⁷⁸. KVKK’nın yürürlüğe girmesiyle birlikte bu soru işaretleri giderilmiştir. KVKK m. 17’de kişisel veriyle ilgili suçlar açısından TCK’ya atıf yapmıştır. Bu nedenle kişisel verilere ilişkin suçlarda her iki kanun beraber değerlendirilmelidir.

B. T.C. Anayasa Hükümü

Anayasamızda 2010 yılına kadar kişisel verilerin korunmasına ilişkin bir hüküm yer almamaktaydı. Haliyle bu tarihe kadar kişisel verilerin korunması hakkı da düzenlenmemiş ve Anayasa tarafından korunmamıştır. Anayasa’nın 2. bölümünde “*kişinin hakları ve ödevleri*”ne yer verilmiştir. Özel hayatın gizliliğini düzenleyen 20. madde hükmü de bu bölümde yer almaktadır. Bu maddeye 2010 yılında 5982 sayılı kanun ile getirilen ek fıkra, kişisel verilere ilişkin ilk anayasal düzenlemedir. Söz konusu ek fıkraya göre “*Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin*

²⁷⁸ KVKK, genel gerekçe.

korunmasına ilişkin esas ve usuller kanunla düzenlenir.” Bu hükmün getirilmesiyle birlikte “*kişisel verinin korunması hakkı*” anayasa tarafından güvence altına alınmıştır²⁷⁹. Kişisel veriler elbette özel hayatın gizliliğiyle ilişkilidir. Ancak kanımca “*kişisel verilerin korunması hakkı*”nın ayrı bir maddede hüküm altına alınması, kişisel veri koruma kültürünün oluşması için daha anlamlı olurdu. Başka bir hakkın alt bendi olarak düzenlenmiş de olsa, kişisel verilerin korunması hakkı, Anayasa’da korunan temel bir haktır. Söz konusu temel hak, kişisel verilerin korunması hakkıdır. Ancak buradan verinin korunması anlaşılmamalıdır. Korunacak olan ilgili kişidir. Nitekim söz konusu temel hak, kişisel verilerin işlenmesi karşısında, kişinin korunması olarak ifade edilebilir²⁸⁰.

Kişisel verilerin korunması hakkı sınırsız bir hak değildir²⁸¹. Temel hak ve hürriyetlerin sınırlandırılması Anayasa m. 13’de hüküm altına alınmıştır²⁸². Kişisel verilerin korunması hakkının sınırlandırılması için de söz konusu hükme uygun olarak sınırlandırma yapmak gerekmektedir. Kişisel verilerin işlenmesinin açık rıza halinde yapılabileceği Anayasa’da düzenlenmiştir. Açık rıza dışındaki veri işleme halleri ise ancak Kanun ile düzenlenebilir. Ayrıca bu haller kanunla düzenlense dahi Anayasa m. 13

²⁷⁹ **Kılınç, Doğan**, “*Anayasal Bir Hak Olarak Kişisel Verilerin Korunması*”, AÜHFD, 2012, C. 61, S. 3, s. 1132.

²⁸⁰ **Şimşek**, s. 4-5.

²⁸¹ **Çekin, Mesut Serdar**, “*6698 Sayılı Kişisel Verilerin Korunması Hakkına Kanun’un Big Data (Büyük Veri) ve İrade Serbestisi Açısından Değerlendirilmesi*”, İÜHFM, 2016, C. 74, S. 2, s. 640.

²⁸² 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 laik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz.*”

gereği hakkın özüne dokunacak mahiyette olamayacağı gibi Anayasaya da aykırı olamaz²⁸³. Örneğin açık rıza dışında kişisel veri işleme sebebi Kurum'un hazırlayacağı bir düzenlemeyle getirilemez. Aksi kabul kişisel verilerin korunması hakkının Anayasaya aykırı olarak kısıtlanması anlamına gelecektir.

C. 6698 Sayılı Kişisel Verilerin Korunması Kanunu

KVKK'ya duyulan gereksinim sadece temel hak ve özgürlüklerin korunması bağlamında değil, aynı zamanda ticari, ekonomik, sosyal vb. birçok alanda önem arz etmektedir. KVKK genel gerekçesi incelendiğinde kanunun yürürlüğüne girmesinin ivedi olarak yapılması gerektiği ve bunun nedenlerine yer verildiği görülecektir.

KVKK'nın genel gerekçesinde kişisel verilerin korunmasına özgü bir kanuna gereksinim duyulduğu belirtilmiştir. Veri koruma düzenlemelerinin çeşitli kanunlara serpiştirilmiş olması, tek bir yerde düzenlenmemiş olması, dağınıklığa sebep olarak veri korumasında sıkıntılar yaratmaktaydı²⁸⁴. Gerekçede veri koruma alanını düzenleyen tek bir kanun bulunmadığına dikkat çekilmiştir. Ayrıca kişisel verilerin işlenmesinde meydana gelebilecek hukuka aykırılıkları ve bunun sonucunda ortaya çıkabilecek kişisel verilerin korunması hakkının ihlalini kontrol altına alabilecek bir Kurum olmadığına dikkat çekilmiştir. Ayrıca Türkiye-AB üyelik görüşmelerinde Türkiye'deki kişisel veri mevzuat eksikliği ifade edilmiştir. KVKK'nın düzenlenmesinin bir başka sebebi ise kişisel verileri düzenleyen temel bir kanun olmadığından, EUROPOL²⁸⁵ ve ülkemizin

²⁸³ Ayözger Öngün, s. 39; Henkoğlu, s. 73.

²⁸⁴ Henkoğlu, s. 20.

²⁸⁵ EUROPOL, uluslararası suçlarda etkin ve güçlü bir kuruluştur. Zaten asıl kurulma amacı da ülkeler arası bilgi akışının sağlanarak suçla etkin bir şekilde mücadele edilmesidir. Şimşek, s. 75-78.

kolluk birimleri arasında bilgi aktarımı yapılamamasıdır. Aynı sebeple EUROJUST ve yargı makamlarımız arasında da veri aktarımı konusunda problemler ortaya çıkmıştır²⁸⁶.

KVKK'nın kabul edilmesinin ekonomik ve ticari sebepleri de bulunmaktadır. Kişisel verilerin ekonomik kıymetinden söz etmeye gerek dahi bulunmamaktadır. Zira günümüzde şirketler ekonomik gayelerle veri işlemekte, işledikleri verileri yurt içinde veya yurt dışına aktarmaktadır. Yabancı sermayenin ülkemize yatırım yapması için de kişisel veri işlemenin ve aktarmanın belli bir düzen ve sistematik içinde olması önem taşımaktadır. Zira kişisel verilerin korunmasını düzenleyen temel bir kanun olmaması yerli ve yabancı yatırımların önüne set çekmektedir.

Daha önce de belirttiğimiz gibi, dünyada kişisel veri ile alakalı çalışmalar ve düzenlemeler 1970'li yıllarda yapılmaya başlanmıştır. Türkiye ise kişisel verilere ilişkin uluslararası anlaşmaları imzalamaya bile iç hukukuna dahil etmemiştir. 2004'de TCK'da kişisel verilerle ilgili hükümler olsa da bu sadece ceza alanında bir koruma sağlamaktaydı. Yine İş Kanunu'ndaki ("**İK**") İş Hukuku'na özgü ve sınırlı düzenlemeler de yeterli olmamaktaydı. Ayrıca kişisel verilerin korunması hakkı Anayasa'da ve diğer kanunlarla tam anlamıyla yer almadığından TCK kişisel veri düzenlemeleri biçare olarak kalmaktaydı. 2010'daki değişikliklerle kişisel verilerin korunmasına dair fıkra Anayasa'ya eklendi. Anayasa'nın yaptığı atıf gereği sadece veri koruma alanını düzenleyen özel bir kanunun yapılması gerekiyordu. Buna ek olarak AK 108 sayılı Sözleşme'nin 2016 yılında Türk hukukuna katılması da yeni bir kanunu gerekli kılıyordu. Tüm bu gerekçelerle yıllardır beklenen KVKK 24.03.2016 tarihinde kabul edildi. Söz konusu "*6698 sayılı Kişisel Verilerin Korunması Kanunu*" 07.04.2016 tarihli RG'de²⁸⁷ yayımlanarak yürürlüğe girdi.

²⁸⁶ KVKK, genel gerekçe.

²⁸⁷ RG. 07.04.2018, S. 29677.

KVKK'nın yürürlüğe girmesi Türkiye için kişisel verilerin korunması konusunda çok önemli bir adımdır. Zira KVKK ile birlikte Türkiye, AB açısından kişisel verilere ilişkin yeterli korumanın bulunduğu ülke²⁸⁸ sayılma noktasında önemli bir adım atmıştır²⁸⁹.



²⁸⁸ Yeterli korumanın bulunduğu ülke, güvenli ülke olarak da ifade edilmektedir. Söz konusu tasnif (güvenli ülke-güvenli görülmeyen ülke) kişisel verilerin korunması kapsamında yapılmaktadır.

²⁸⁹ **Akıncı**, AB Tüzüğü, s. 4.

İKİNCİ BÖLÜM

6698 SAYILI KİŞİSEL VERİLERİN KORUNMASI KANUNU KAPSAMINDA

KİŞİSEL VERİLERİN KORUNMASI

§4. Kanunun Amacı, Kapsamı ve Terimler

I. Kanunun Amacı

Daha önce de belirttiğimiz gibi, kişisel verilerin korunması hakkı, 2010 yılında Anayasa'ya eklenen fıkıyla güvence altına alınmıştır. İlgili 20. maddenin son cümlesine göre, “*Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.*” Görüldüğü üzere Anayasa, hak ile ilgili olarak genel çerçeveyi çizdikten sonra hakkın korunmasıyla ilgili detaylar için kanuni düzenlemeye atıf yapmıştır. Anayasa'nın aynı maddesinde ilgili kişinin hakları sayılmış, kişisel verilerin işlenmesinde temel hususlara değinilmiştir. Bu nedenle ilgili kişinin bu haklarını nasıl kullanacağı, kişisel verilerin korunmasını talep hakkının detayları ve veri işlemenin ne zaman hukuka uygun olup ne zaman olmayacağı sorunsalına çözüm bulmak KVKK'nın temel amaçları arasındadır. Kanun ile ulaşılmak istenen sonuç veri işlemenin modern ölçütlere bağlanarak korunmasıdır. Başka bir ifadeyle, kanunun hedefi, kişisel verilerin korunmasında modern standartların yakalanmasıdır²⁹⁰. Bu hedefin gerçekleşmesiyle birlikte verilerin rastgele

²⁹⁰ **Kurum**, Kişisel Verilerin Korunması Kanunu Hakkında Sıkça Sorulan Sorular, Ankara 2018, s. 16. <https://www.kvkk.gov.tr/Icerik/4196/Kisisel-Verilerin-Korunmasi-Kanunu-Hakkinda-Sikca-Sorulan-Sorular> (E.T.: 02.04.2020).

işlenmesi ve kötü amaçlarla kullanılması engellenebilecektir²⁹¹.

KVKK m.1'e göre *“Kanunun amacı, kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektir.”* Söz konusu maddede genel manada Anayasa'nın atfına riayet edildiği görülmektedir. Ancak Anayasa'da kişisel verilerin korunması hakkının açıkça düzenlendiğinden söz ettik. Buna rağmen KVKK'da söz konusu bağımsız hak yerine özel hayatın gizliliğine yer verilmesi eleştirilmektedir²⁹². Madde gerekçesinde²⁹³ de 1. maddeye benzer amaçlardan bahsedilmiş, ayrıca *“kişinin mahremiyet hakkı ve bilgi güvenliği hakkının korunmasına”* da özellikle vurgu yapılmıştır.

II. Kanunun Kapsamı

KVKK'nın ne zaman uygulanabileceğini tespit etmek için kanunun kapsamının belirlenmesi gerekmektedir. Zira veri işleyenlerin bütünü değil sadece madde kapsamında sayılan kişiler kanun kapsamına girecektir. KVKK m. 2'ye göre *“KVKK 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.”* Kanunun kapsamının sınırlarının GDPR m.2/1 ile benzer olduğu görülmektedir.

²⁹¹ **Kurum**, 100 Soruda Kişisel Verilerin Korunması Kanunu, Ankara 2018, s.12.

²⁹² **Çekin**, Kişisel Veri, s. 21-22.

²⁹³ KVKK gerekçe, m. 1.

A. Kanun Kapsamına Giren Haller

1. Kişi Bakımından

Öncelikle belirtmek gerekir ki, verisi işlenen gerçek kişiler KVKK kapsamında korunsa da tüzel kişiler bu korumadan yararlanamamaktadır. Başka bir ifadeyle, eğer bir tüzel kişinin bilgileri işleniyorsa bu kanuna başvurulamayacaktır. Ancak verisi işlenen gerçek kişiye işbu kanun kuşkusuz uygulama alanı bulacaktır. Zira kanun açıkça bu hususu belirtmiştir. Ayrıca KVKK m.3’de “*ilgili kişi, kişisel verisi işlenen gerçek kişi*” olarak tanımlanmıştır. Görüleceği üzere, KVKK, tüzel kişilere ait verilerin korunmasını düzenlememektedir. Bu anlayış GDPR ve AB Direktifi gibi uluslararası düzenlemelerle uyumludur. Lakin tüzel kişiye ait bilgiler gerçek kişinin tespit edilmesine yol açıyorsa, bu durumda söz konusu veriler tüzel kişiye de ait olsa KVKK kapsamında değerlendirilmelidir. Zira burada artık gerçek kişiye ait bilgi sınırına geçilmiştir²⁹⁴. Örneğin Anonim Şirket yönetim kurulu liste bilgisinin kaydedilmesi artık şirkete özgü bilgi olmaktan çıkacak, etkisi gerçek kişilere sirayet edeceği için KVKK korumasında olacaktır.

Veri işleyen, gerçek kişi de tüzel kişi de olsa kanun kapsamına girecektir. Veri işleyen bakımından herhangi bir ayırım söz konusu değildir. Bu hususta kamu tüzel kişileri için herhangi bir ayırım yapılmadığı için hem özel hem kamu tüzel kişileri kapsama dahildirler²⁹⁵. Örneğin işçileriyle ilgili bilgileri işleyen anonim şirket, bu kanun

²⁹⁴ **Başalp**, Kişisel Veri, s. 35; **Kurum**, Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi, Ankara 2018, s. 37.
<https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/0517c528-a43d-49f5-b1eb-33dc666cb938.pdf> (E.T.: 10.03.2020).

²⁹⁵ KVKK gerekçe, m.2.

kapsamında değerlendirileceği gibi personel alımı için ilan veren kamu kuruluşunun adaylardan topladığı bilgiler de kanun kapsamındadır.

2. Konu Bakımından

Öncelikle belirtmek gerekir ki, KVKK'nın uygulanacağı alanların tespitini yapabilmek için otomatik-otomatik olmayan işleme terimlerinin açıklanması gerekmektedir. KVKK m. 3/1/e'de kişisel verilerin işlenmesi tanımlanmıştır. Buna göre, “*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 hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleşen her türlü işlemi ifade eder.*” KVKK'daki tanım maddesi incelendiğinde görüleceği üzere, verinin elde edilmesinden itibaren akla gelebilecek her türlü işlem veri işleme kapsamında değerlendirilmiştir. Maddedeki “gibi” ifadesiyle sayılanların sadece örnek mahiyetinde olduğu, burada yazılanlar dışındaki işlemlerin de kişisel verilerin işlenmesi kapsamında değerlendirilebileceği ifade edilmek istenmiştir.

Kanundaki ayrıma göre kişisel verilerin işlenmesi iki şekilde gerçekleşmektedir. Bunlardan ilki *otomatik işlemedir*. KVKK otomatik işlemenin tanımını yapmamıştır. Otomatik işleme; bilgisayar, laptop, cep telefonu gibi elektronik aletlerde, insan etkisi olmaksızın bizatihi olan işleme olarak tanımlanabilir²⁹⁶.

Daha öncede ifade ettiğimiz gibi uluslararası düzenlemelerin bazılarında²⁹⁷ “*verilerin otomatik yolla işlenmesi*” üzerinde durulmuştur ve bu durum koruma altına

²⁹⁶ **Kurum**, 6698 Sayılı Kanun'da Yer Alan Temel Kavramlar, s.14.

²⁹⁷ Örneğin AK 108 No.lu sözleşme, OECD Rehber İlkeleri vb.

alınmıştır. Açıkçası bilişim sistemlerinin ulaştığı boyutlar düşünüldüğünde ilk korunması gereken durum “*otomatik yolla işleme durumu*”dur. KVKK da bu hususu gözeterek “*tamamen veya kısmen otomatik olan yolla*” işlenen verileri kapsamına almıştır.

Tamamen-kısmen otomatik yolla işleme ayırımında bakılması gereken herhangi bir insan müdahalesinin olup olmamasıdır. Tamamen otomatik işlemede, veri işlenirken insan müdahalesinden söz edilemez. Bu durumda, sistem yapısı gereği verilerin işlenmesini kendiliğinden gerçekleştirmektedir. Kısmen otomatik işlemede ise insan müdahalesi vardır. Sisteme verileri giren insandır. Kişisel verilerin işlenmesi bilgisayar aracılığıyla gerçekleştiğinde tamamen ya da kısmen otomatik yolla işleme kaçınılmaz olacaktır²⁹⁸. Başka bir ifadeyle, kişisel verilerin işlenmesinde bilgisayar vb. vasıtalar kullanılıyorsa otomatik veri işleme (tamamen-kısmen ayırımı fark etmeksizin) söz konusu olacaktır.

KVKK, kapsam bakımından tamamen-kısmen otomatik işlemede herhangi bir ayırım yapmamıştır. Yani kişisel veri otomatik yolla işleniyorsa KVKK uygulanacaktır. Bu nedenle kısmen ya da tamamen otomatik işlemenin, KVKK kapsamı bakımından bir farkı kalmayacaktır. Sonuç olarak, otomatik işleme söz konusuysa kısmen-tamamen ayırımı yapılmaksızın KVKK kapsamında değerlendirilecektir.

Otomatik olmayan işlemede ise KVKK kapsamının belirlenmesi için bir ayırım yapmak gerekmektedir. KVKK, “*otomatik olmayan yolla işlenen (yani manuel işlenen)*” tüm verileri kapsamı dışına çıkartmamıştır. Burada kanun “*veri kayıt sisteminin*²⁹⁹ *parçası*” olarak işleme kriterini kullanmıştır. Eğer “*otomatik olmayan yolla işlenen veri*” VKS’nin parçası olarak işleniyorsa KVKK kapsamına girecek, VKS dışında bir işleme mevcutsa kapsam dışında kalacaktır. “*Otomatik olmayan yolla işlenen ve veri kayıt*

²⁹⁸ Çekin, Kişisel Veri, s. 24.

²⁹⁹ Bundan böyle VKS olarak anılacaktır.

sisteminin de parçası olmayan kişisel veriler” KVKK kapsamında sayılmasa da vasfı gereği kişisel veri olduğundan TCK kapsamına girecek ve suç sayılacaktır³⁰⁰.

VKS kanunun 3. maddesinde şu şekilde tanımlanmıştır: *“Veri kayıt sistemi, kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemidir.”* VKS, GDPR m. 2’de *“dosyalama sistemi (filing system)”* olarak ifade edilmiştir. KVKK 2. maddenin gerekçesinde VKS şu şekilde ifade edilmiştir: *“Bir dosyalama sistemi olarak nitelenebilecek veri kayıt sistemi sadece dijital yahut elektronik ortamda oluşturulması gereken bir sistem değildir.”*

Otomatik olmayan işleme denilince akla özellikle kağıt üzerine kişisel veri işlenmesi gelmektedir. Kağıt üzerine işlenen her türlü kişisel veri, KVKK kapsamında değerlendirilecek midir? Eğer kişisel veriler belirli kriterlere göre, VKS’nin parçası olarak işleniyorsa değerlendirilecektir. Başka bir ifadeyle, KVKK kapsamından söz edebilmek için kişisel verilerin sistemli bir şekilde işlenmesi gerekmektedir. Ancak bir kağıt üzerine gelişigüzel yazılmış, herhangi bir kriterden söz edilemeyen veri işlemler KVKK kapsamında değildir.

Örneğin bir kağıdın üzerine gelişigüzel ad-soyad yazılması durumunda VKS’den bahsedilemeyecektir. Ancak ad-soyad belirli kriterlere göre kağıda yazılıyorsa KVKK uygulama alanı bulacaktır³⁰¹. Örneğin bir şirketi ziyaret edenlerin ad-soyad, meslek ve ziyaret tarihi bilgilerinin ziyaret defterine belirli kriterlere göre kaydedilmesi durumunda bu işleme bakımından VKS’den bahsedilebilecek ve işleme KVKK kapsamında değerlendirilecektir.

³⁰⁰ **Kurum**, Uygulama Rehberi, s. 39.

³⁰¹ **Kurum**, 6698 Sayılı Kişisel Verilerin Korunması Kanununun Amacı ve Kapsamı, s. 4-5.

Kayıt sisteminin dahilinde manuel olarak işlenen kişisel verilerin de KVKK kapsamına dahil olması KVKK'nın uygulama alanını oldukça genişletmektedir. Zira bu halde, ad-soyad ve borç olarak belirli bir kriterle işlenen bakkal veresiye defteri bile KVKK kapsamında değerlendirilebilecektir. Bu vesileyle de bakkalın veri sorumlusu olarak KVKK'dan kaynaklanan yükümlülöklere uyması gerekecektir³⁰².

Sonuç olarak bir verinin KVKK kapsamına girip girmediğini tespit etmek için öncelikle işlemenin niteliğine (otomatik-otomatik olmayan) bakılır. Otomatik işleme varsa KVKK zaten uygulanır. Ancak veri, otomatik olmayan yolla işlendiyse bu sefer de VKS çerçevesinde işlenip işlenmediğı tespit edilir. Eğer veri VKS'nin parçası değilse yani belirli kriterlere göre yapılandırılarak işlenmiyorsa KVKK kapsamında değildir.

B. Kanun Kapsamına Girmeyen Haller

Tüzel kişilerle ilgili verilerin KVKK kapsamına girmeyeceğinden, KVKK korumasından yararlanamayacağından yukarıda bahsettik. Ayrıca “*otomatik olmayan yolla işlenen ve veri kayıt sisteminin de parçası olmayan kişisel veriler*”in de KVKK kapsamında olmadığına değindik. Bunlar dışında KVKK “*istisnalar*” başlıklı 28. maddesinde kanun hükümlerinin uygulanmayacağı haller sayılmıştır. 28. madde bütün kanun hükümlerinin uygulanmayacağı ve bazı kanun hükümlerinin uygulanmayacağı haller olarak ikili bir ayrım yaptığı için bu haller aşağıda ikiye ayrılarak incelenmiştir.

1. Tamamen Kanun Kapsamına Girmeyen Haller

Madde 28/1'de büsbütün istisna olan haller hükme bağlanmıştır. Bu hallerin söz konusu olması durumunda KVKK'nın hiçbir hükmü uygulanmayacaktır. Ancak her ne

³⁰² Çekin, Kişisel Veri, s. 26.

kadar aşağıda sayılan haller söz konusu olup KVKK'nın tamamen ya da kısmen uygulanmaması şartları oluşsa da yine de kişisel veriler temel veri işleme ilkelerine uygun, orantılı ve ölçülü olarak işlenmelidir³⁰³. Özellikle kişisel verilerin işlenmesine dair genel ilkelere her koşulda riayet edilmelidir.

Madde 28/1/a uyarınca *“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 halinde KVKK hükümleri uygulanmaz.”* Örneğin aile içinde çekilen ve aile içinde kalacak olan fotoğraflarda KVKK uygulanmaz. Ancak çocuğun, anne ve babasının fotoğrafını Instagram'da paylaşması durumunda artık bu veri KVKK kapsamında değerlendirilecektir.

Madde 28/1/b'ye göre, *“Kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi halinde KVKK hükümleri uygulanmaz.”* Örneğin Türkiye İstatistik Kurumu'nun (**“TÜİK”**) bilgileri resmi istatistik kapsamında işlenmesi halinde, anonim duruma getirilmek şartıyla, işlenen verilerde KVKK uygulanmayacaktır.

Madde 28/1/c uyarınca *“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 halinde KVKK hükümleri uygulanmaz.”* *“İfade özgürlüğü kapsamında işlenen kişisel veriler”*de KVKK uygulanmayacaktır. Ancak ifade özgürlüğü ve kişisel verinin korunması arasındaki dengenin iyi kurulması gerekir³⁰⁴. Terazinin ifade özgürlüğü tarafının fazla şekilde ağır

³⁰³ **Kurum**, Örnekler, s. 50.

³⁰⁴ **Kurum**, Örnekler, s. 52.

basması ilgili kişinin zarar görmesine yol açabilir.

Madde 28/1/ç’de belirtildiği gibi, “*Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliğini sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi halinde KVKK uygulanmaz.*” Örneğin Milli İstihbarat Teşkilatı (“**MIT**”) tarafından kişisel veri işlenmesi durumunda KVKK uygulanmayacaktır.

Yine salgın hastalık durumunda kamu tarafından işlenen veriler bu fıkra kapsamında değerlendirilmektedir. Kurul tarafından yapılan açıklamada da COVID-19 sebebiyle yetkili kamu kurum ve kuruluşlarınca yapılan veri işlemler bu fıkra kapsamında değerlendirilmiştir³⁰⁵.

Madde 28/1/d’ye göre, “*Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi*” halinde de KVKK’nın hiçbir hükmü uygulanmayacaktır. Örneğin ilgili savcının soruşturma aşamasında (Soruşturma aşaması fiilin ve şüphelinin araştırıldığı aşama olduğundan kişisel veri işlenmemesi zaten kaçınılmazdır.) edindiği ve kaydettiği kişisel veriler KVKK kapsamına dahil olmayacaktır.

2. Kısmen Kanun Kapsamına Girmeyen Haller

KVKK 28. madde bütün olarak kanun kapsamına girmeyen halleri saydıktan sonra aynı maddenin 2. bendinde kısmen kanun kapsamına dahil olmayan durumları

³⁰⁵ **Kurul**, 09.04.2019 T., <https://www.kvkk.gov.tr/Icerik/6726/COVID-19-ILE-MUCADELEDE-KONUM-VERISININ-ISLENMESI-VE-KISILERIN-HAREKETLILIKLERININ-IZLENMESI-HAKKINDA-BILINMESI-GEREKENLER-2-> (E.T.: 17.05.2020).

saymıştır. Buna göre aşağıda sayacağımız hallerde KVKK m. 28/2 gereği “*bu kanunun amacına ve temel ilkelerine uygun ve orantılı olmak kaydıyla veri sorumlusunun aydınlatma yükümlülüğünü düzenleyen 10., zararın giderilmesini talep etme hakkı hariç, ilgili kişinin haklarını düzenleyen 11. ve Veri Sorumluları Siciline kayıt yükümlülüğünü düzenleyen 16. maddeleri*” uygulanmaz. Ancak bu 3 madde dışındaki diğer KVKK maddelerine ise tabidirler. Somut olay aşağıda sayacağımız durumlara da girse bu üç maddenin uygulanmaması için “*kanunun amacına ve temel ilkelerine uygun ve orantılı olma*” şartının yine de gerçekleşmesi zorunludur.

KVKK m. 10, m. 11 (“*zararın giderilmesini talep hakkı hariç*”) ve m. 16’nın uygulanmayacağı hallerden ilki KVKK m. 28/2/a’da düzenlenen “*kişisel veri işlemenin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması*” halidir. Örneğin ilgili savcılık tarafından yapılan soruşturmada kolluk tarafından şüpheliye ait uyuşturucu madde olduğu düşünülen ev bilgisinin aydınlatma yükümlülüğü kapsamında öncesinde şüpheliye açıklanması zaten mantık kurallarıyla bağdaşmayacaktır. Bu ve bunun gibi nedenlerle kanunun bazı maddeleri uygulanmaz.

KVKK m. 28/2/b’ye göre “*verinin ilgili kişinin kendisi tarafından alenileştirilmesi durumunda*” saydığımız KVKK maddeleri uygulanmaz. Avukatın kendi ofisine özgü internet sitesinde paylaştığı mail bilgisi buna örnek olarak verilebilir.

KVKK m. 28/2/c gereği “*kişisel veri işlemenin kanunun verdiği yetkiye dayanılarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olması*” durumunda yine KVKK ilgili hükümleri uygulanmaz. Örneğin barolar kamu kurumu niteliğindeki meslek kuruluşu niteliğinde olduğundan yapacağı disiplin soruşturması kapsamındaki kişisel veriler bu madde kapsamında değerlendirilecektir.

Kısmen kanun kapsamına girmeyen son durum ise KVKK m.28/2/ç'de düzenlenmiştir. Buna göre *“kişisel veri işlemenin bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olması”* halinde yine belirttiğimiz KVKK maddeleri dikkate alınmayacaktır.

III. Terimler

A. Genel Olarak

KVKK'nın 3. maddesinde kanunda sıklıkla kullanılan ve önemli olan bazı terimlerin tanımlarına yer verilmiştir. Burada tanımı yapılan terimlerle ilgili tanım ve açıklamalar ilgili yerlerde yapıldığı için burada sadece veri sorumlusu ve veri işleyen terimleri açıklanacaktır.

B. Veri Sorumlusu ve Veri İşleyen

Veri koruma hukukunun ana aktörlerinden olan veri sorumlusu ve veri işleyen terimlerinin açıklığa kavuşturulması gerekmektedir. Bu iki kavram tanımlandıktan sonra aralarındaki fark tespit edilmeye çalışılacaktır. Söz konusu tespit önemlidir. Zira KVKK'da düzenlenen yükümlülükler, sorumluluklar ve yaptırımlarla kimin karşılaşacağını bu tespit belirleyecektir. Veri sorumlusu ve veri işleyeni ayırt etmek bazen çok kolaydır. Ancak bazı durumlarda net bir ayırım yapmak oldukça zorlaşmaktadır³⁰⁶. Bazı durumlarda her ikisi de aynı kişi sıfatında birleşebilmektedir.

Veri sorumlusu (*“data controller”*) KVKK m. 3/1/ı'da *“kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve*

³⁰⁶ Kuner, 72.

yönetilmesinden sorumlu olan gerçek veya tüzel kişi” olarak tanımlanmıştır. Burada sayılan kişiler kapsamına hem gerçek kişiler hem de kamu tüzel kişileri ve özel hukuk tüzel kişileri (dernekler, vakıflar, şirketler) girmektedir. Kanun bu açıdan herhangi bir ayırım yapmamıştır³⁰⁷.

Tüzel kişilerde veri sorumlusu doğrudan tüzel kişiliğin kendisidir. TMK m. 50’ye göre, *“Tüzel kişinin iradesi organları aracılığıyla açıklanır”*. Tüzel kişiler tüm hukuki işlemleri organları vasıtasıyla gerçekleştirirler³⁰⁸. Ancak tüzel kişiliğin çatısı altında bulunan organların tüzel kişiliği olmadığından veri sorumlusu yine tüzel kişilik olacaktır³⁰⁹. Keza şubenin de tüzel kişiliği bulunmadığından³¹⁰ şubeler veri sorumlusu olarak kabul edilemez. Bu durumda da veri sorumlusu şirket tüzel kişiliği olacaktır. Yine tüzel kişilik bünyesindeki birimler kişilik vasfına haiz olmadığından KVKK hükümlerinden sorumlu olacak yine tüzel kişiliktir. Örneğin X Mağazacılık A.Ş.’den kıyafet alan bir kişinin kimlik ve adres bilgilerini işleyen X Mağazacılığın işçisi, şubesi ya da herhangi bir temsilcisi veri sorumlusu olarak kabul edilmeyecektir. KVKK yükümlülüklerine tabi olması gereken veri sorumlusu X Mağazacılık A.Ş tüzel kişiliğidir. Yine bir üniversitenin akademik personeline ilişkin verilerin tutulduğu personel birimi sorumlu olarak nitelendirilmeyecek, üniversite tüzel kişiliğinin kendisi veri sorumlusu olacaktır.

³⁰⁷ KVKK gerekçe, m.3.

³⁰⁸ **Ayan/Ayan**, s. 207.

³⁰⁹ Veri Sorumluları Sicili Hakkındaki Yönetmelik, m. 11/1.

³¹⁰ *“Anonim şirketler tüzel kişiliğe sahip sermaye şirketlerindendir. Yürütülen ticari faaliyetlerin yaygınlaşması sebebiyle işlerin tek bir merkezden yönetiminin zorlaşması halinde kurulan ve şirketi temsil eden şubelerin ise ayrı bir tüzel kişiliği yoktur.”* Yargıtay 6. HD., 14.12.2016 T., 2016/7517 E., 2016/7471 K., (Kazancı, E.T.: 11.03.2020).

Kamu kurum ve kuruluşlarında veri sorumlusu doğrudan kamu kurum ve kuruluşudur. Bakanlığa bağlı, ilgili ve ilişkili birimler için ise bir ayırım yapılması gerekmektedir. Burada bakılacak olan veri sorumlusu tanımındaki veri işleme amaç ve vasıtalarının kim tarafından belirlendiğidir. Bu tespit yapılırken veri kayıt sistemini kurup yönetenin de kim olduğuna bakılır. Saydığımız birimler tanımdaki unsurları karşılamıyorlarsa veri sorumlusu sayılmazlar. Söz konusu birimlerin veri işlemeden kaynaklanan yükümlülüklerini ilişkili oldukları Bakanlık yapar³¹¹.

Veri işleyen (**“data processor”**) ise KVVK m.3/1/ğ’ye göre *“veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi”*dir.

Veri işleyen, kendi adına veri işlememekte, veri sorumlusunun talimatı ile veri işlemektedir. Veri sorumlusu ile veri işleyeni ayırt etmek için işlenecek verilere karar verenin kim olduğu, verilerin hangi yolla işleneceği veya hangi süreyle muhafaza edileceği gibi hususlara karar verenin kim olduğuna bakmak gerekir. Bu hususlara karar verecek olan veri sorumlusudur. Yani kişisel verilerin işlenmesinde asıl karar alıcı veri sorumlusudur. Kısacası veri işlenmesi durumunda bunun *“neden”* ve *“nasıl”* olacağına karar verecek olan veri sorumlusudur. Veri işleyen ise aldığı emirler doğrultusunda yetkilendirildiği ölçüde veri işleyen kişidir³¹².

Veri işleyen mutlaka veri sorumlusu organizasyonu dışındaki bir 3. kişi olmalıdır. Şirketin işçileri, çalışanları veya şirketin veri işleyen birimleri veri işleyen olarak

³¹¹ **Kurum**, 6698 sayılı Kişisel Verilerin Korunması Kanunu Hakkında Doğru Bilinen Yanlışlar, Yayın No: 31, Ankara 2020, s. 19-20.
<https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/28d8adba-2b41-41b2-bf36-d0ff0d845666.pdf> (E.T.: 13.05.2020).

³¹² **Kurum**, Örnekler, s. 62.

nitelendirilmemektedir³¹³.

Sorumluluğun belirlenmesi bakımından veri sorumlusu ile veri işleyen ayrımını iyi yapmak gerekir. Kurum tarafından hazırlanan rehberde bu konuda bazı örneklerle yer verilmiştir. Her somut olayda belirttiğimiz kıstaslara göre belirleme yapılması gerekmele birlikte, biz de rehberdeki birkaç örneğe değineceğiz. “*Bulut hizmet sağlayıcıları*” ile verilerin saklanması konusunda sözleşme akdedilirse, bulut hizmet sağlayıcısı veri işleyen konumundadır. “*Mali müşavirler*”in müşterileriyle ilgili bilgileri işlemesi durumunda veri sorumlusu mali müşavirler olacaktır. Zira mali müşavirlerin sorumluluk kapsamında mesleklerinden kaynaklanan yasal yükümlülükleri vardır. Bu sebeple bu yükümlülükleri ve sorumluluğu müşterilerine yükleyemezler. Şirketin işçisiyle ilgili bir hukuki uyuşmazlığında hukuki sürecin yürütülebilmesi için işçi ile ilgili verilerin “*avukat*”a verilmesi durumunda şirketle birlikte avukat da veri sorumlusu olacaktır. Zira avukat, işçiyle ilgili kendisine verilen verileri “*neden*” ve “*nasıl*” işleyeceğine kendisi karar verecektir. Keza yine “*ödeme servisleri*” ve “*pazar araştırma şirketleri*” verilerin işleme yöntemine, hangi verilerin işleneceğine vs. karar verdikleri sürece veri sorumlusu olarak kabul edilirler³¹⁴. “*Kişisel verilerin veri sorumlusu bir avukat tarafından kısa mesaj yoluyla üçüncü kişilere ifşa edilmesi hakkında*”ki kararda Kurul, avukatın veri sorumlusu olduğu tespitini yapmıştır³¹⁵.

³¹³ **Kurum**, Doğru Bilinen Yanlışlar, s. 21.

³¹⁴ Bu konuda detaylı örnekler için bkz., **Kurum**, Veri Sorumlusu ve Veri İşleyen, s. 5-10.)

³¹⁵ Avukatın veri sorumlusu olarak değerlendirildiği Kurul kararı için bkz. **Kurul Kararı**, 14.01.2020 T., 2020/26 K. <https://www.kvkk.gov.tr/Icerik/6697/2020-26> (E.T.: 17.03.2020). Kurul tarafından “*Şikayete konu olayda, Bankaya borçlu olan ve bu borca ilişkin işlemlerin yürütülmesini teminen kişisel verileri Banka tarafından avukata*

Verdiğimiz bütün örnekler örnek mahiyetindedir. Somut olaya göre bu sıfatların değişebileceğine dikkat etmek gerekir. Örneğin veri işleyen sıfatıyla belirttiğimiz kişi kendi adına veri işlemeye başlarsa veri sorumlusu olabilecektir. En önemli kıstas olan verilerin “neden” ve “nasıl” işleneceğine karar veren kişi yani veri sorumlusu tespit edildikten sonra iki sıfat da kolaylıkla ayrılabilir.

Veri işleyen, veri sorumlusunun sözleşmeyle veri işleme konusunda yetkili kıldığı gerçek ya da tüzel kişidir. Kişisel veri işleme sözleşmesi³¹⁶, veri işleme konusunda veri sorumlusunun veri işleyeni yetkilendirdiği sözleşmedir. Örneğin veri depolama hizmeti sunan bir şirket (bulut bilişim) ile otomotiv sektöründeki bir şirket arasında müşterilerin verilerini işleme yetkisini veren bir sözleşme olsun. Depolama hizmeti sunan şirket verileri kendi adına değil otomotiv şirketi adına işlemektedir. Bu olayda otomotiv şirketi veri sorumlusudur. Veri depolayan şirket ise veri işleyendir. Otomotiv şirketinin, araç satın aldığı kişilerin (hangi kişiler), adını, soyadını, IBAN bilgilerini (hangi veriler), satış işleminin yapılması ve sözleşme kurulabilmesi amacıyla (işleme amacı) alması veri işlemede asıl merciin ve sorumlunun otomotiv şirketi olmasına örnektir. Bulut bilişim şirketi ise sadece otomotiv şirketinden gelen verileri işlediği için veri işleyen sıfatını taşımaktadır.

aktarılan ve avukat tarafından kişisel verileri işlenen ilgili kişi, Banka adına icra işlemlerini yürüten ve bu işlemle ilgili olmak üzere ilgili kişinin kişisel verilerini işleyen avukatın veri sorumlusu, ilgili kişinin bankaya olan borcunu tahsil edebilmek için avukat tarafından ilgili kişiye ait iletişim bilgileri ve diğer ilgili bilgilerinin işlenmesi eyleminin ise veri işleme faaliyeti olduğu” tespitleri yapılmıştır.

³¹⁶ Kişisel veri işleme sözleşmesiyle ilgili detaylı bilgi için bkz. **Taştan**, s. 112-146.

Bankanın kredi kartını müşteriye kurye ile göndermesine ilişkin bir Kurul kararına göre³¹⁷, banka, kredi kartı ile ilgili verileri “*kendi belirlediği amaçlar ve vasıtalar ile tuttuğundan*” veri sorumlusudur. Kredi kartı kapalı zarfta olduğundan kuryenin kart bilgilerine erişmesi mümkün değildir. Bu nedenle kurye kapalı zarftaki bilgiler kapsamında veri sorumlu addedilmeyecektir. Ancak kartı müşteriye teslim edebilmesi için işlediği ad, soyad ve adres gibi verileri kendi için işlediğinden ve kendi sisteminde tuttuğundan dolayı veri sorumlusudur. Aynı olayda kurye şirketi, kredi kartı bilgileri açısından veri sorumlusu kabul edilmezken, taşıma bilgileri (adres, ad gibi) açısından veri sorumlusu kabul edilmektedir. Somut olayda da görüldüğü üzere tek bir olayda dahi kişiler bir bakımdan veri sorumlusu sayılırken diğer bakımdan sayılmayabilir. Bu nedenle tespit yapılırken özellikle “*kendi belirlediği amaçlar ve vasıtalar ile veri tutanın*” kim olduğuna bakılmalı ve bu kişi veri sorumlusu sayılmalıdır.

Hukuken bir kimsenin ne kadar yetkisi varsa o kadar da yükümlülüğü vardır. Veri işlemede asıl karar verici olanın, “*verilerin işleme amacını ve vasıtalarını*” belirleyecek olanın veri sorumlu olduğunu inceledik. İşte bu sebeple KVKK’dan kaynaklanan yükümlülüklerden asıl sorumlu olan kişi de veri sorumlusudur³¹⁸.

Son olarak belirtmek gerekir ki, veri sorumluluğu sıfatı ile veri işleyen sıfatı mutlaka farklı kişiler üzerinde olmak zorunda değildir. Veri sorumlusu ve veri işleyen sıfatı aynı kişi üzerinde birleşebilir. Yani bir gerçek ya da tüzel kişi aynı anda hem veri sorumlusu hem de veri işleyen olabilir. Örneğin bir muhasebe şirketi kendi çalışanları

³¹⁷ **Kurul Kararı**, 16.01.2020 T., 2020/32 K. <https://www.kvkk.gov.tr/Icerik/6700/2020-32> (E.T.: 24.03.2020).

³¹⁸ Ayrıca kişisel verinin veri işleyen tarafından işlenmesi durumunda KVKK m.12 “*veri güvenliği*” hükmü uyarınca alınması gereken idari ve teknik tedbirler hususunda veri işleyen de veri sorumluyla birlikte müştereken sorumludur. (KVKK m.12/1)

hakkında işlediği veriler açısından veri sorumlusudur. Ancak müşteri ilişkisi olan başka şirketler hakkında işlediği veriler açısından veri işleyen olacaktır³¹⁹. Örnekte görüldüğü gibi her iki sıfat aynı kişide birleşebilmektedir.

§5. Kişisel Verilerin İşlenmesi

I. Genel Olarak

KVKK m.3/1/e düzenlemesine göre, “*Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi ifade etmektedir.*” Görüldüğü üzere KVKK’da baştan sona tüm süreci kapsayan bir tanımlama yoluna gidilmiştir. Bu sebeple bu sürecin her noktasını ayrıntılarıyla incelemek gerekmektedir. Hükümde “*gibi veriler üzerinde gerçekleştirilen her türlü işlem*” ifadesinden işlenmenin kapsamının hükümde yer verilen işlemlerle sınırlı olmadığı anlaşılmaktadır. Hükümde yer verilenler örnekleme niteliğindedir. Zira hükümde yer almasa dahi veriler üstünde gerçekleşen bütün işlemler kişisel verilerin işlenmesi kapsamında değerlendirilecektir.

II. Kişisel Verilerin İşlenmesine İlişkin Genel İlkeler

Kişisel verilerin korunması bir insan vücudu olsaydı genel ilkeler bu vücutta kalp olarak yerini alırdı. Teşbihte hata olmaz mottosuyla, kalbin durmasının insan vücudunda

³¹⁹ KVKK gerekçe, m. 3.

yaratacağı etkiyi, genel ilkelere uyulmadığında veri işlemenin hukuka uygunluğuna yaratacağı etkiye, benzetebiliriz. Gerçekten de Türk Özel Hukuku için TMK “*Başlangıç Hükümleri*”nin önemi ne kadarsa Kişisel Verilerin Korunması Hukuku’nda da “*kişisel verilerin işlenmesinde genel ilkeler*”in önemi o kadardır. Bu ilkeler veri hukukunun yapı taşı olduğu için “*temel ilkeler*” olarak da ifade edilmektedir. Ancak biz KVKK’da ifade edildiği gibi “*genel ilkeler*” ifadesini kullanmayı tercih ettik. İlkeleri bu kadar önemli kılan husus KVKK’nın uygulamasında ilk bakılacak ana kurallar olmalarıdır. Kurul bir kararında³²⁰ veri işleme faaliyetinde KVKK m.4’deki ilkelerin tümüne dikkat edilmesi gerektiğini belirtmiştir. Yine “*Aday Puanlarının Rıza Alınmaksızın, İnternet Sitesinde Paylaşılması Hakkındaki Görüş Talebi*” ile ilgili başka bir Kurul kararında³²¹ “*İnternet ortamında yayımlanan kişisel verilerin tamamen kaybolmadığı göz önüne alındığında değerlendirme puanlarının, Kanunun 4 üncü maddesinde yer alan genel ilkelere uyumlu şekilde, yalnızca akademik kadrolara müracaat eden ilgili kişilerce görüntülenebildiği bir yöntemle ve kimlik doğrulaması yapılmak suretiyle sorgulamasına imkân verecek şekilde ilan edilmesi gerektiğine karar verilmiştir.*” İlgili kararda kişilerin kimliğinin belirli ya da belirlenebilir olmasını engellemek için akademisyen adaylarının bilgilerine maskeleye yapılması (bilgilerin üstünün çizilmesi yahut yıldızlanması) gerektiğine karar verilmiştir. Görüldüğü üzere, Kurul kararlarında temel ilkelere sıklıkla dayanmaktadır. Bu ilkelere aykırı veri işleme faaliyeti tespit ettiğinde ise ihlal kararı vermektedir.

Günlük hayatımızda kişisel verilerin işlenmesi kaçınılmazdır. Ancak veri işleme; baştan savma bir şekilde değil, KVKK’daki temel ilkelere uygun olarak

³²⁰ **Kurul Kararı**, 25.03.2019 T., 2019/78 K. <https://www.kvkk.gov.tr/Icerik/5434/2019-78> (E.T.: 13.02.2020).

³²¹ **Kurul Kararı**, 26.12.2019 T., 2019/389 K. <https://www.kvkk.gov.tr/Icerik/6668/2019-389> (E.T.: 17.03.2020).

gerçekleştirilmelidir³²².

Ayrıca belirtmek gerekir ki, bu genel ilkelerin önemi ilgili kişilerin haklarının korunması bakımından paha biçilemez değerdedir. Zira çok hızlı bir şekilde gelişen bilişim ve teknoloji sektörü karşısında KVKK'nın yetersiz kalacağı durumlar olabilecektir. Kanun'u her yeni teknolojik ilerlemede değiştirmek mümkün olmadığı için bu temel ilkeler her durum ve koşulda ilgili kişinin haklarını koruyucu etki yaratacaktır, yaratmalıdır. Aşağıda da açıklayacağımız üzere Kurul da başvurularda temel ilkelere uyulup uyulmadığını kontrol etmekte eğer bu ilkelere uyulmuyorsa ihlal kararı vermektedir.

KVKK m.4/1'e göre *“Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir.”* Görüldüğü üzere verilerin işlenmesinde sadece KVKK değil, tüm kanunlar ve hukukun genel ilkeleri esas alınacaktır. Bu hükümle diğer kanunlara yapılan atıf, verileri işlerken ilgili kanunlara da riayet edilmesi anlamına gelmektedir.

KVKK m. 4/2 ise *“Kişisel verilerin işlenmesinde aşağıdaki ilkelere uyulması zorunludur.”* düzenlemesiyle uyulması gereken beş ilkeyi şu şekilde saymıştır: *“hukuka ve dürüstlük kurallarına uygun olma”, “doğru ve gerektiğinde güncel olma”, “belirli, açık ve meşru amaçlar için kullanma”, “işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma” ve “ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme.”* Biz de sırasıyla KVKK'nın tüm hükümleri incelenirken dikkate alınması gereken bu beş ilkeyi inceleyeceğiz. İşlenen veriler kaliteli olmalıdır. Bir veriyi kaliteli yapan husus ise işte bu beş temel ilkeye riayet edilerek kişisel verilerin işlenmesidir.

³²² **Kurum**, KVKK ve Getirdikleri, s. 5.

A. Hukuka ve Dürüstlük Kuralına Uygun Olma İlkesi

Söz konusu ilke en genel nitelikte olan ve diğer ilkelerin de temeli niteliğinde olan bir ilkedir. Aslında diğer dört ilkeye aykırılık olması durumunda da bu ilke ihlal edilmiş olacaktır. Zira diğer dört ilkeden herhangi birine aykırı bir veri işleme söz konusuysa KVKK m.4 ihlal edilmiş olacaktır. KVKK m.4'ün ihlali de hukuka aykırılık oluşturacağı için *“hukuka uygun olma ilkesinin”* de ihlaline sebep olacaktır. Yine KVKK m.5 ve m.6'daki şartlara uyulmadan yapılan veri işlemler otomatikman hukuka uygunluk ilkesine de aykırı olacaktır.

Bu ilke *“hukuka uygun olma ilkesi”* ve *“dürüstlük kuralına uygun olma ilkesi”* şeklinde ikiye ayrılarak incelenebilir.

“Hukuka uygunluk”, kanunlar ve diğer tüm hukuki düzenlemelere uyulması gerektiği anlamına gelir. Daha önce de belirttiğimiz gibi *“kişisel verinin işlenmesi”* çok geniş bir süreci ifade ettiğinden, bu sürecin tamamında bu ilkeye riayet edilmelidir³²³.

Hukuka uygunluk, sadece mevzuata uygunluğu ifade etmemekte, daha geniş bir anlamı ifade etmektedir. Örneğin hukuka uygunluk kanuna uygunluğu da sağlar. Ancak her zaman kanuna uygunluk hukuka uygunluk anlamına gelmez³²⁴.

Veri işlemenin KVKK ve diğer tüm hukuk kurallarına uygun olması yetmez. Ayrıca bu işleme dürüstlük kuralına da uygun olarak yapılmalıdır. KVKK açısından *“dürüstlük kuralına uygun olma ilkesi”* ise TMK m. 2'deki dürüstlük kuralının³²⁵

³²³ **Küzeci**, s. 201; **Özdemir, Hayrunnisa**, Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması, Ankara 2009, s. 137.

³²⁴ **Kurum**, Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler, s.2.

³²⁵ *“Dürüstlük kuralı, herkesin, haklarını kullanırken ve borçlarını yerine getirirken ortalama zeka seviyesine sahip, makul ve dürüst kişiden aynı hal ve şartlarda beklenecek*

karşılığı olarak ifade edilebilir³²⁶. “*Dürüst davranma*” başlıklı TMK m. 2’de “*Herkes, haklarını kullanırken ve borçlarını yerine getirirken dürüstlük kurallarına uymak zorundadır. Bir hakkın açıkça kötüye kullanılmasını hukuk düzeni korumaz.*” hükmü yer almıştır. Burada 1. fıkra “*dürüstlük kuralını*” düzenlerken 2. fıkra “*hakkın kötüye kullanılması yasağını*” düzenlemektedir.

TMK ilgili hükmünün asıl amacı, tüm sözleşmeleri ve yasa hükümlerini dürüstlük kuralı çerçevesinde yorumlamaktır. Ayrıca somut olaya uygulanan yasa hükmündeki maksadın aşılmasını önlemektir³²⁷. Bu nedenle veri sorumlusu, veri işleme faaliyetinde bu kurala riayet etmeli, veri işlemenin amacının aşılmasından kaçınmalıdır. Somut olayda veri işlemenin amacının aşılması durumunda işleme hukuka aykırı hale gelecektir.

KVKK açısından ise “*dürüstlük kuralına uygun olma ilkesi*” veri sorumlusunun, veri işlerken “*ilgili kişinin çıkarlarını ve makul beklentilerini*” nazara alması olarak ifade edilebilir³²⁸. Ayrıca bu ilke kapsamında işleme ilgili kişi açısından “*şeffaf*” olmalıdır. Kurul bir kararında³²⁹ veri sorumlusunun ilgili kişiye ait veriye sahip olmasına rağmen elinde olmadığını söylemesinin şeffaflıkla bağdaşmadığına, bunun da dürüstlük kuralına aykırı olduğuna karar vermiştir.

davranış haline uygun biçimde davranma yükümlülüğüdür.” Antalya, O. Gökhan/

Topuz, Murat, Medeni Hukuk C. I, Genişletilmiş 3. Baskı, Ankara 2019, s. 494.

³²⁶ **Özdemir**, Elektronik Haberleşme, s.138.

³²⁷ **Altaş, Hüseyin**, Medeni Hukuk Başlangıç Hükümleri, Ankara 2018, s. 259.

³²⁸ **Küzeci**, s. 201.

³²⁹ **Kurul Kararı**, 01.10.2019 T., 2019/294 K.

<https://www.kvkk.gov.tr/Icerik/6556/2019-294> (E.T.: 17.03.2020).

Dürüstlük kuralı gereği veri sorumlusu sadece gerektiği kadar veri işlemelidir. Ayrıca veri sahibi kişinin öngöremeyeceği işlemlerden kaçınmalıdır³³⁰.

Genel ilkeler ve özellikle bu ilke veri işlemede her durumda uyulması gereken ilkeler olduklarından Kurul tarafından birçok kararda bu ilkeye uyulmadığı için veri ihlali tespit edilmiştir. Kurulun Facebook hakkında verdiği kararda³³¹ *“Facebook platformu uygulamalarının daha ilk aşamada, oyunun, kişinin açık profiline ve kişinin bu oyunu oynayan tanıdığı kişilere erişiminin olması için izin aldığı, ilgili kişilerin paylaşmaya izin verecekleri kişisel verilerin neler olması gerektiği ve yükleme aşamasında gizlilik ayarlarıyla ilgili seçimlere imkan sağlanmayarak kişisel verilerin işlenmesinin açık rızaya dayandırıldığı, açık rızanın özgür iradeyle açıklanması gerekirken ilgili kişinin açık rızasının alınmasının bir ürün veya hizmetin sunulmasının ön şartı olarak ileri sürüldüğü ve bu durumun KVKK m.4/2/a hukuka ve dürüstlük kuralı ilkesine aykırılık teşkil ettiğine karar verilmiştir.”* ifadeleriyle bu ilke açısından ihlal tespiti yapılmıştır.

Yine başka bir kurul kararında³³² *“Şirket tarafından ilgili kişinin telefon numarasına aynı içerikteki mesajların farklı tarihlerde birden fazla kez gönderilmesinin veri sorumlusunun sahip olduğu hakkı kötüye kullanımı olduğu ve bu durumun da hukuka ve dürüstlük kurallarına aykırı olduğuna karar verilmiştir.”* ifadeleriyle hakkın kötüye kullanılması yasağına uyulmadığı tespit edilmiştir.

³³⁰ **Kurum**, Madde ve Gerekçesi İle Kişisel Verilerin Korunması Kanunu Bilgi Notu & Kişisel Verilerin Korunmasına İlişkin Terimler Sözlüğü, Ankara 2019, s. 14.

³³¹ **Kurul Kararı**, 11.04.2019 T., 2019/104 K.

<https://www.kvkk.gov.tr/Icerik/5450/2019-104> (E.T.: 12.02.2020).

³³² **Kurul Kararı**, 31.05.2019 T., 2019/159 K.

<https://www.kvkk.gov.tr/Icerik/5494/2019-159> (E.T.: 13.02.2020).

B. Doğru ve Gerektiğinde Güncel Olma İlkesi

Veriler işlenirken uyulması gereken bir diğer ilke “*doğru ve gerektiğinde güncel olma*” ilkesidir. Bu ilke, ilgili kişinin verilerinin düzeltilmesini isteme hakkının karşılığıdır. KVKK m. 11/1/d uyarınca “*İlgili kişi, verilerin eksik veya yanlış işlenmiş olması halinde bunların düzeltilmesi hakkına sahiptir.*” Görüldüğü üzere eğer veriler doğru ve güncel olarak tutulmazsa ilgili kişinin düzeltme talep hakkı doğacaktır.

Veriler gerçeğe uygun şekilde işlenmelidir. Verilerin doğru olması, sadece veri ilk kez işlenirken değil tüm süreçte sağlanmalıdır. İlgili kişiler bilgilerin gerçeğe uyumlu olup olmadıklarını düzenli aralıklarla denetleyebilir. Gerçeğe bağdaşmayan, yalan veya güncel olmayan kişisel verilerin düzeltilmesi ya da kaldırılması gerekmektedir³³³.

Söz konusu ilkeye uygun veri işlenmesi için bilgilerin salt doğru olması yetmemektedir. Veriler işlenirken doğruyken sonrasında doğruluğunu kaybetmiş olabilir. Bu sebeple veri sorumlusu, bilgilerin güncelliğini sürekli olarak kontrol etmelidir³³⁴. Veri sorumlusunun söz konusu bu ilke kapsamındaki “*aktif özen yükümlülüğü*”, işlenen verilerin veri sahibi açısından olumlu ya da olumsuz bir netice yaratacağı durumlarda söz konusu olur. Bu duruma kredi verme işlemi örnek olarak verilebilir³³⁵.

İlgili kişi, yanlış veya güncel olmayan veriler sebebiyle hem maddi hem de manevi zararlara uğrayabilir³³⁶. Örneğin kişi hakkında gerçeğe uygun olmayan şekilde tutulan sağlık durumu bilgileri kişiyi hak kaybına uğratacağı gibi manen de zarara uğratabilir. Yine fazla satılan malların satış fiyatı üzerinden prim alınan bir şirkette satış sorumlusu olarak çalışan bir kişinin mail adresinin yanlış işlenmesi ve müşterilerle yanlış

³³³ **Özdemir**, Elektronik Haberleşme, s. 138.

³³⁴ **Özdemir**, Elektronik Haberleşme, s. 139.

³³⁵ **Kurum**, Sorular, s. 44.

³³⁶ **Kurum**, Temel İlkeler, s. 6.

olan mail adresinin paylaşılması sonucu ilgili kişi prim alamayacağı için zarara uğrayacak, veri sorumlusu şirket de satış yapılamadığı için zarara uğrayacaktır. Görüldüğü gibi işbu ilke ilgili kişinin hakkını koruduğu kadar veri sorumlusunun da çıkarlarını korumaktadır.

C. Belirli, Açık ve Meşru Amaçlar İçin İşlenme İlkesi

Bu ilke gereği veri işlenirken veri sorumlusunun amacı, net olarak ortaya koyulmalı ve belirsiz olmamalıdır. Ayrıca bu açıkça anlaşılabilen amacın meşru da olması gerekmektedir. Kişisel verilerin işlenmesinde veri sorumlusunun hangi veri işleme şartına dayandığı ilgili kişiye açıkça belirtilmelidir. Belirtilmezse bu ilkeye aykırılık söz konusu olacağından işleme hukuka aykırı bir hal alır³³⁷.

Amacın belirli ve açık olması için veri sorumlusundan önce kanun koyucunun konuyla ilgili belirli ve açık hukuki düzenlemeler yapması gerekir. Veri sorumlusu işleme amacını net bir şekilde belirlemelidir. Veri sorumlusunun belirlediği amaçla işlediği amaç bağdaşmazsa bu ilkeye aykırılık söz konusu olur. Bunun sonuçlarına elbette veri sorumlusu katlanacaktır³³⁸. Bunun dışında kişisel bilgilerin ileride işe yarayabileceği ihtimaline karşı saklanması da amacın belirliliğini ve açıklığını ihlal edecektir³³⁹.

İşleme amacının belirliliği ve açıklığı veri işleme faaliyetinin her iki tarafı açısından da geçerli olmalıdır. Başka bir ifadeyle ilgili kişi açısından da amacın anlaşılabilir olması gerekir. İşleme amacının belirtildiği metinlerde, bu ilkeye uyumun sağlanabilmesi için -dürüstlük kuralı gereği olarak da- ilgili kişinin anlayamayacağı

³³⁷ **Kurul Kararı**, 01.10.2019 T., 2019/294 K.

<https://www.kvkk.gov.tr/Icerik/6556/2019-294> (E.T.: 17.03.2020).

³³⁸ KVKK gerekçe, m.4.

³³⁹ **Küzeci**, s. 203.

belirsiz ifadelere yer vermemeye azami gayret gösterilmelidir³⁴⁰.

KVKK m. 4 gerekçesine göre “*Amaçın meşru olması, veri sorumlusunun işlediği verilerin, yapmış olduğu iş veya sunmuş olduğu hizmetle bağlantılı ve bunlar için gerekli olması anlamına gelmektedir.*” Örneğin kütüphane üyelik işleminde, kurumun ilgili kişinin kimlik ve eğitim bilgilerini işlemesi meşru amaç olarak değerlendirilebilirken, kişinin sosyal güvenlik numarası bilgisinin işlenmesi meşru amaç kapsamında değerlendirilemez. Yine veri sorumlusu tarafından düzenlenen sempozyum katılımcılarının iletişim bilgilerinin işlenmesi meşru amaç olarak nitelendirilebilirken, katılımcıların anne kızlık soyadı bilgilerinin toplanıp işlenmesi meşru amaç olarak nitelendirilemez.

Kurul bir kararında³⁴¹ “*Şikâyetçinin müşterisi olduğu Bankaya kendisine ait iş ve işlemlerde ulaşılması adına vermiş olduğu telefon numarası bilgisinin, eşine ulaşılmasında yardımcı olunabilmesi adına işlenmesinin, KVKK m.4/2/c-ç’de yer alan kişisel verilerin işlenmesinde belirli, açık ve meşru amaçlar için işlenme ve işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ilkelerine uyulması zorunluluğuna aykırı olduğuna karar vermiştir.*”

D. Amaçla Bağlantılı, Sınırlı ve Ölçülü Olma İlkesi

Kişisel verilerin işlenmesinde dikkat edilmesi gereken ve yukarıdaki ilkeyle ilişkili dördüncü ilke, “*kişisel verilerin işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma*” ilkesidir. KVKK 4. madde gerekçesinde belirtildiği üzere, “*Kişisel verilerin, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması ilkesi, işlenen verilerin, belirlenen*

³⁴⁰ **Kurum**, Temel İlkeler, s. 8.

³⁴¹ **Kurul Kararı**, 18.09.2019 T., 2019/277 K.

<https://www.kvkk.gov.tr/Icerik/5545/2019-277> (E.T.: 13.02.2020).

amaçların gerçekleştirilebilmesine elverişli olmasını, amacın gerçekleştirilmesiyle ilgili olmayan veya ihtiyaç duyulmayan kişisel verilerin işlenmesinden kaçınılmasını gerektirmektedir. Ayrıca işlenen veri, sadece amacın gerçekleştirilmesi için gerekli olanla sınırlı tutulacaktır.”

“Veri minimizasyonu” (data minimisation) olarak da adlandırılan bu ilke³⁴² gereği veri sorumlusu, kişisel veri işlemenin zorunlu olup olmadığını gözden geçirmelidir. Şayet bu veri işlenmeden de amaç elde edilebilecekse veri işlenmemelidir. Eğer mutlaka veri işlenmesi gerekiyorsa da bu en az oranda veri işleme şeklinde gerçekleşmelidir. Kurul kararları incelendiğinde “veri minimizasyonu ilkesine aykırılık sebebiyle” veri ihlali kararları verildiği görülmektedir³⁴³. Veri minimizasyonu, kişisel veriler işlenirken yeterli minimum miktarla sınırlama olarak tanımlanabilir³⁴⁴. Bu durum “veri ekonomisi” olarak adlandırılır³⁴⁵. Veri ekonomisi gereği, veri sorumluları kişisel verileri işlerken adeta tutumlu olmalı, aşırı veri kullanımından kaçınmalıdır. Bu konuyla ilgili bir Kurul kararında³⁴⁶ “Bir havayolu taşımacılık şirketinin (veri sorumlusu) sunduğu sadakat

³⁴² Veri minimizasyonu ilkesi GDPR m. 5/1/c’de hüküm altına alınmıştır.

³⁴³ “İşlenme amacının gerektirdiğinden fazla kişisel veri işlenmesi/aktarılması (veri minimizasyonu ilkesine aykırılık) sebebiyle KVKK m/4/1/ç’de yer alan amaçla bağlantılı, sınırlı ve ölçülü olma ilkesine aykırılık teşkil ettiğine karar verilmiştir.” **Kurul Kararı**, <https://www.kvkk.gov.tr/Icerik/5413/Islenme-Amacinin-Gerektirdiginden-Fazla-Kisisel-Veri-Islenmesi-Aktarilmasi-Veri-Minimizasyonu-Ilkesine-Aykirilik-> (E.T.: 14.03.2020).

³⁴⁴ **Kuner**, s. 74.

³⁴⁵ **Küzeci**, s. 208.

³⁴⁶ Kurulun ilgili kararına göre “İlgili kişinin kimliğinin teyidi noktasında ek bilgi istemesinin yerinde olduğu değerlendirilmekle birlikte, ilgili kişinin din ve kan grubu gibi

programını kullanan ilgili kişinin kullanıcı adı ve parola bilgilerini değiştirme talebi karşısında ilgili kişiden arkalı önlü kimlik görüntüsü talep eden veri sorumlusu”nun bu ilkeye aykırı işlem yaptığı tespit edilmiştir.

Verilerin işleme amacının sonradan değişmesi halinde ilgili kişiden yeni amaç için tekrardan rıza alınmalıdır³⁴⁷. KVKK m. 4 gerekçesinde de aynı yönde “Yine, sonradan ortaya çıkması muhtemel ihtiyaçların karşılanmasına yönelik veri islenebilmesi için, işlemeye ilk kez başlıyor gibi, 5 inci maddede düzenlenmiş olan kişisel verilerin işleme şartlarından birinin gerçekleşmesi gerekecektir.” ifadelerine yer verilmiştir. Kurul’un da kararlarında benzer görüşte olduğu görülmektedir³⁴⁸.

*özel nitelikli kişisel verilerini de içeren arkalı önlü kimlik görüntüsünün talep edilmesi, Kanunun Genel İlkeler başlıklı 4. maddesinde düzenlenen işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ilkesine uygun değildir.” Kurulun bu kararında temel ilkelerin hepsine aykırılık tespit edilmiştir. Kararı incelemek için bkz. **Kurul Kararı**, 01.10.2019 T., 2019/294 K. <https://www.kvkk.gov.tr/Icerik/6556/2019-294> (E.T.: 14.03.2020).*

³⁴⁷ **Özdemir**, Elektronik Haberleşme, s. 141.

³⁴⁸ Bu konuyla ilgili Kurul kararında “*kışisel verilerin ilk kez işlenmesi için gereken amaçtan farklı olarak başka bir amaca yönelik yeni bir veri işleme faaliyetinin gerçekleştirilmesinin, Kanunun 5. maddesinde sayılan veri işleme şartlarından en az birine dayanması ve ilk amaçtan bağımsız olarak Kanunun 4. maddesinde sayılan kişisel verilerin işlenmesinde aranan ilkelerin tümüne uyumlu olması gerektiği*”ne karar verilmiştir. Bu karar için ve amacın sonradan değişmesi ile ilgili somut örnek için bkz. **Kurul Kararı**, 25.03.2019 T., 2019/78 K., <https://www.kvkk.gov.tr/Icerik/5434/2019-78> (E.T.: 18.03.2020).

Verinin işlenme amacı dışında başka bir amaç için kullanılması “*amaçla bağlantılı ve sınırlı olma ilkesi*”ne aykırılık oluşturacaktır. Bu hususla ilgili Kurul kararına³⁴⁹ konu olan olayda ilgili kişinin dergi aboneliği sebebiyle telefon numarası işlenmiştir. Ancak kişi aranarak başka bir şirketin reklamı yapılmıştır. Görüldüğü üzere kişisel verinin baştaki işlenme amacıyla sonradan kullanım amacı farklılık arz etmektedir. Amaçtaki bu değişiklik söz konusu ilkeye aykırılık sonucu doğuracaktır. Başka bir amaç için sağlanan veri işleme şartları yeni amacı kapsamamaktadır. Her amaç için ayrı ayrı veri işleme şartlarının sağlanması gerekmektedir.

“*Ölçülülük ilkesi*” veri işleme amacıyla işlenen veri arasında makul bir denge kurulması gerekliliğidir. İşlenen veri sadece amacı sağlayacak miktarda olmalıdır³⁵⁰. *Ölçülülük ilkesi*, hukuk devleti ilkesinin unsurlarındandır. Bu ilke gereği kişisel verilerin korunması hakkına karşı yapılacak veri işleme faaliyeti ölçülü olmalıdır³⁵¹. Kişisel veri işleme amacına başka bir şekilde (veri işleme dışında) ulaşılabiliriyorsa bu ilkeye riayet edildiği söylenemez. Başka bir ifadeyle, bu ilke gereğince amaca ulaşmak için tek araç işlemeyse o halde işleme yapılabilir³⁵². Örneğin dans kursu üyelik başvurusunda kişinin çalışma hayatına ilişkin veri istenmesi ölçülülük ilkesiyle bağdaşmayacaktır.

³⁴⁹ **Kurul Kararı**, 16.01.2020 T., 2020/34 K., <https://kvkk.gov.tr/Icerik/6713/2020-34> (E.T.: 02.04.2020).

³⁵⁰ **Kurum**, Temel İlkeler, s. 10.

³⁵¹ **Şimşek**, s. 98.

³⁵² **Çekin**, Kişisel Veri, s. 72.

Kurul ölçölülük ilkesine aykırı bulduğu bir kararında³⁵³ “*Spor kulübünde giriş çıkış kontrolünün yapılabilmesi ve kulüp hizmetlerinden faydalanmak isteyen kişilere ilişkin giriş kontrolünün alternatif yollar ile sağlanması mümkün iken kişilerin biyometrik veri niteliğindeki avuç içi izi verisinin alınmasının KVKK m.4/2’de yer alan işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ilkesi ile bağdaşmadığına karar vermiştir.*”

Danıştay bir kararında³⁵⁴ çalışanların işe giriş saatlerinin tespiti amacıyla kullanılan “*parmak izi taraması uygulaması*”nın hukuka aykırı olduğuna hükmetmiştir.

E. Belirli ve Sınırlı Süre Muhafaza Edilmesi İlkesi

Temel ilkeler içindeki sonuncu ilke “*İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkesi*”dir. İlkenin amacı belirsiz ve sınırsız bir süre verilerin veri sorumlusunun elinde olmasını engellemektir.

Bu ilke gereği veriler “*bir gün gerekli olur*” mantığıyla stoklanmamalı, ihtiyacın

³⁵³ Kurul’un bu ilke ile ilgili verdiği detaylı kararlar için bkz. **Kurul Kararı**, 25.03.2019 T., 2019/81 K. ve 31.05.2019 T., 2019/165 K.

<https://www.kvkk.gov.tr/Icerik/5496/2019-81-165> (E.T.: 14.03.2020). Benzer örnek ve görüş için bkz. **Data Protection WP**, Opinion 3/2012 on developments in biometric technologies, s. 8. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf (E.T.: 14.03.2020).

³⁵⁴ “*İlgililerden kişisel veri alınması niteliğinde olan, parmak izi taramasının, özel hayatın gizliliği ilkesi kapsamında bulunması karşısında Anayasal ilkeler ve uluslararası sözleşme kuralları ile bağdaşmayan parmak izi sistemiyle yürütülen mesai takibi uygulamasına ilişkin işlemde hukuka uygunluk bulunmadığı kararı verilmiştir.*” Danıştay İDDK., 09.12.2015 T., 2014/2242 E., 2015/4991 K. (Kazancı, E.T.: 11.05.2020).

üzerindeki miktarda veri saklanmamalıdır. Kişisel verilerin muhafaza edildiği her bir gün veri güvenliği bakımından risk yaratmaktadır. Bu ilke “*unutulma hakkı*” ve “*veri minimizasyonu ilkesi*” ile doğrudan bağlantılıdır³⁵⁵. “*Unutulma hakkı*” gereği verilerin sınırsız süre tutulmaması gerekir. Zira her kişi, unutulma hakkına sahiptir. Ayrıca verilerin tutulması gerekli olan süre geçince artık saklanmaması tutulan veri sayısını azaltacağından “*veri minimizasyonu*” ilkesinin de gerçekleşmesini sağlayacaktır.

KVKK’da belirtilen “*gerekli olan süre*” ifadesinin ne kadarlık bir süre olduğu tespit edilmelidir. Zira bu tespit yapılmazsa veri sorumlusunun bir veriyi gereğinden fazla ya da gereğinden az sakladığı tespit edilemez. KVKK bu konuda ikili bir ayrım yapmıştır. Bu süre “*mevzuatta öngörülen süre*” olabilir. Eğer mevzuatta gerekli olan süre açıkça hükme bağlanmışsa veri sorumlusu bu süreyi aşamayacaktır.

Bu duruma, ilgili Kurul kararında³⁵⁶ da belirtilen “*5411 sayılı Bankacılık Kanunu*” m. 42 “*Alınan yazılar ve faaliyetler ile ilgili belgelerin asılları ... ilgili banka nezdinde on yıl süreyle saklanır.*” ve “*Bankaların Muhasebe Uygulamalarına ve Belgelerin Saklanması İlişkin Usul ve Esaslar Hakkında Yönetmelik*” m. 17/1 “*Bankaların, müşterilerinden ... aldıkları mektup, telgraf, elektronik posta mesajı, ilam ve tebligatları ... istenildiğinde ibraz edilebilecek şekilde nezdlerinde on yıl süreyle saklamaları zorunludur.*” düzenlemeleri örnek olarak verilebilir. Kurul’un bu kararında ilgili kişi, veri sorumlusu bankaya verilerinin silinmesi için başvuruda bulunmuş, ancak

³⁵⁵ **Küzeci**, s. 337.

³⁵⁶ **Kurul Kararı**, 05.12.2018 T., 2018/142 K. <https://www.kvkk.gov.tr/Icerik/5424/-Ilgili-mevzuatta-ongorulen-veya-islendikleri-amac-icin-gerekli-olan-sure-kadar-muhafaza-edilme-ilkesi-geregince-kisisel-verilerin-silinmemesi-hakkinda-Kisisel-Verileri-Koruma-Kurulunun-05-12-2018-tarihli-ve-2018-142-sayili-Karari-Ozeti> (E.T.: 14.03.2020).

mevzuatta belirtilen 10 yıllık saklama süresi geçmediğinden Kurul tarafından ihlal tespit edilmemiştir.

Mevzuatta herhangi bir süre belirlenmemişse bu süre “*işlendikleri amaç için gerekli olan süre*”dir³⁵⁷. Veri sorumlularının bu hükmü geniş yorumlaması uygulamada haksız ve hukuka aykırı veri stoklanması önünü açacaktır. Bunu öngören kanun koyucu veri sorumlularının VERBİS’e kaydolurken “*kişisel verilerin işlendikleri amaç için gerekli olan azami süre*”nin bildirilmesi gerektiğini hükme bağlamıştır³⁵⁸. Bildirilecek olan bu süre “*makul bir süre*” olmalıdır.

“Mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre”nin geçmesi halinde veri sorumlularının söz konusu veriye ne kendilerinin ne de 3. kişilerin ulaşamayacakları şekilde eylemde bulunmaları gerekmektedir. İleride de tekrar değineceğimiz gibi bu eylem verileri silme ya da anonim hale getirmedir³⁵⁹. Sürenin geçmesi, amacın gerçekleşmesi veya veri işleme şartının artık bulunmaması durumlarından sonra veri muhafaza edilemeyecektir³⁶⁰. Örneğin alışveriş merkezi

³⁵⁷ Bu husus KVKK m.4 gerekçesinde şu şekilde ifade edilmiştir: “*Kişisel verilerin, ancak ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi zorunludur. Buna göre, veri sorumluları, ilgili mevzuatta verilerin saklanması için öngörülen bir süre varsa bu süreye uyacak; yoksa verileri, ancak işlendikleri amaç için gerekli olan süre kadar muhafaza edebilecektir.*”

³⁵⁸ KVKK m. 16/3/f.

³⁵⁹ Bu husus m.4 gerekçesinde de ifade edilmiştir: “*Bir verinin daha fazla saklanması için geçerli bir sebep olmaması durumunda, o veri silinecek veya anonim hale getirilecektir. Gelecekte kullanma ihtimalinin varlığına dayanarak veri saklanamayacaktır.*”

³⁶⁰ **Kurum**, Örnekler, s.9

tarafından düzenlenen, belirli bir miktar alışveriş yapılması durumunda katılınabilecek araba çekilişi için müşterilerin bazı kişisel verilerinin işlenmesi durumunda, çekiliş gerçekleştikten sonra bu veriler artık muhafaza edilemeyecektir.

III. Kişisel Verileri İşleme Şartları

Anayasa m. 20/3’de “*kişisel verilerin ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebileceği*” hükme bağlanmıştır. Yani veri işlenebilmesi için ilgili kişinin açık rızasının gerekmesi anayasal güvence altındadır. Açık rıza dışında bir sebeple kişisel veri işlenecekse bu hallerin kanunda belirtilmesi gerektiği de Anayasa’da düzenlenmiştir. Anayasa hükmüyle uyumlu olarak, kişisel verilerin işlenebilmesi için gerekli olan şartlar KVKK m. 5’de hüküm altına alınmıştır. KVKK m. 5/1’de kişisel verilerin açık rıza olmadan işlenemeyeceği düzenlenmiştir. Maddenin devamında ise açık rızanın olmadığı hallerde verilerin işlenebileceği haller sayılmıştır. Ancak burada belirtmek gerekir ki, kural kişisel verilerin işlenmemesidir. Kişisel verilerin işlenmesi istisnadır³⁶¹. Bu nedenle bu şartların tümü dar yorumlanmalıdır. Her zaman zayıf durumda olan “*ilgili kişi lehine yorum*” yapılmalıdır. Kişisel veri işleme şartlarının oluşup oluşmadığı hususunda tereddüt varsa şartın olmadığı kabul edilerek kişisel veri işlenmemelidir.

Kişisel verilerin hukuka uygun olarak işlenebilmesi için KVKK m.5’de sayılan hallerden herhangi birinin olması yeterlidir. Hepsinin bir arada olması gerekmez. Kanunda kişisel verilerin işlenebileceği haller sınırlı sayıda sayılmış olup, bu haller dışında veri işlenmesi hukuka aykırı olacaktır. Eğer açık rıza ya da açık rıza gerekmeyen haller mevcut değilse somut olayda kişisel verilerin işlenmesi mümkün değildir. Bir kurul

³⁶¹ Şimşek, s. 208.

kararında³⁶² da “Bir Eğitim Kurumu tarafından ilgili kişinin cep telefonu numarasının herhangi bir veri işleme şartına dayanmaksızın işlenmesi ve ilgili numaraya reklam/bilgilendirme içerikli mesaj gönderilmesinin; kişinin açık rızasına veya KVKK m. 5/2’de sayılan diğer veri işleme şartlarına dayanmadığından” hukuka aykırı bir veri işleme olduğu yönünde karar verilmiştir. Yine benzer bir kararda³⁶³ “X Eğitim kurumunun kişisel veri işleme şartları olmaksızın ilgili kişinin cep telefonuna reklam amaçlı kısa mesaj göndermesi” sebebiyle veri sorumlusu hakkında idari para cezası uygulanmıştır.

Günlük yaşantıda sıklıkla veri sorumluları tarafından herhangi bir veri işleme şartına dayanmadan SMS veya mail ile ilgili kişilerle iletişim kurulmaktadır. Sıklıkla karşılaşılan söz konusu veri ihlalini dikkate alan Kurum, bu konuda ilke kararı yayımlamıştır³⁶⁴. “Veri sorumluları ve veri işleyenler tarafından ilgili kişilerin e-posta adreslerine veya SMS ya da çağrı ile cep telefonlarına reklam bildirimleri/aramaları

³⁶² **Kurul Kararı**, 14.01.2020 T., 2020/20 K. <https://www.kvkk.gov.tr/Icerik/6699/2020-20> (E.T.: 17.03.2020). Veri sorumlusu doktor hakkında verilen aynı yönde başka bir karar için bkz. **Kurul Kararı**, 07.11.2019 T., 2019/332 K.

<https://www.kvkk.gov.tr/Icerik/6624/2019-332> (E.T.: 17.03.2020). Benzer yönde kararlar için bkz. **Kurul Kararı**, 08.07.2019 T., 2019/204 K.

<https://www.kvkk.gov.tr/Icerik/5517/2019-204> (E.T.: 17.03.2020), **Kurul Kararı**, 31.05.2019 T., 2019/162 K. <https://www.kvkk.gov.tr/Icerik/5495/2019-162> (E.T.: 18.03.2020).

³⁶³ **Kurul Kararı**, 18.09.2019 T., 2019/276 K.

<https://www.kvkk.gov.tr/Icerik/6558/2019-276> (E.T.: 17.03.2020).

³⁶⁴ **Kurul İlke Kararı**, 16.10.2018 T., 2018/119 K.

<https://www.kvkk.gov.tr/Icerik/5299/2018-119> (E.T.: 19.03.2020).

yönlendirilmesinin önüne geçilmesi "ne ilişkin kararıyla Kurul, uygulamada sıklıkla karşılaşılan veri ihlallerinin önlenmesi gereğini belirtmiştir.

Çalışmada ilk önce açık rıza kavramı incelenecek, sonrasında ise açık rıza dışındaki kişisel verilerin işlenebilmesi için olması gerekli olan şartlar üzerinde durulacaktır. Hassas kişisel verilerin işlenmesi ise ayrı şartlara tabi olduğu için ayrı başlık altında incelemeye tabi tutulacaktır.

A. Açık Rıza

1. Genel Olarak

Açık rıza (*"explicit consent"*), kavramıyla uluslararası metinlerde de sıklıkla karşılaşılmaktadır. AB Direktifi'ne göre rıza, kişinin özgür iradesiyle, belirsizlik olmadan net bir şekilde belirttiği onay beyanıdır. AB Direktifi'nde sadece hassas kişisel verilerin işlenmesi açık rıza şartına bağlanmıştır. Ancak KVKK ve GDPR'da kişisel veri türü fark etmeksizin verilerin işlenebilmesi için açık rıza gerekmektedir³⁶⁵.

KVKK m. 3/1/a'ya göre *"Açık rıza; belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanan rızadır."* Kanunda yapılan tanımda görüldüğü üzere açık rızanın unsurları *"belirli bir konuya ilişkin olma"*, *"bilgilendirmeye dayanma"* ve *"özgür iradeyle açıklanma"* olarak sayılabilir. Biz de açık rıza ile ilgili genel açıklamalarımızdan sonra sırasıyla bu üç unsura değineceğiz.

Kural olarak kişisel veriler işlenemez. Başka bir ifadeyle kural, veri işlemenin yasak oluşudur³⁶⁶. Kişisel verilerin işlenmesi yasağının istisnaları yukarıda da belirttiğimiz gibi açık rıza veya Kanun'da sayılan diğer hallerdir. Kişisel verilerin

³⁶⁵ **Kurum**, Temel Kavramlar, s. 2.

³⁶⁶ **Çekin**, İrade Serbestisi, s. 635.

işlenmesinde hukuka aykırılığı ortadan kaldıracak, en önemli hukuka uygunluk sebebi açık rızadır³⁶⁷. Ancak bu önem açık rızanın KVKK m. 5/2'deki diğer hukuka uygunluk hallerine nazaran üstün olması şeklinde anlaşılmamalıdır. Zira hukuka uygunluk nedenlerinin tamamı işlemeyi eşit düzeyde hukuka uygun hale getirmektedir³⁶⁸.

Açık rıza, KVKK'nın birçok maddesinde düzenlenmiş hukuka aykırılığı ortadan kaldıran bir haldir. KVKK m. 5/1 gereği "*Kişisel veriler ilgili kişinin açık rızası olmadan işlenemez.*" KVKK m. 6/2 uyarınca "*Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmadan işlenmesi yasaktır.*" Ayrıca KVKK m. 8/1 gereği "*Kişisel veriler, ilgili kişinin rızası olmadan aktarılamaz.*" KVKK m. 9/1 gereği "*Kişisel veriler, ilgilinin açık rızası olmaksızın yurt dışına aktarılamaz.*" Görüldüğü üzere birçok kanun maddesinde verilerin işlenmesi ve aktarılması durumlarında açık rızanın hukuka aykırılığı giderdiği görülmektedir. Bu nedenle "*açık rıza*" kavramının detaylıca incelenmesi önem arz etmektedir.

İlgili kişinin açık rızasının alınması, veri sorumlusunun KVKK m. 4'de düzenlenen genel ilkelere uyma yükümlülüğünü ortadan kaldırmayacaktır. Başka bir deyişle, ilgili kişinin açık rızası alınsa dahi temel veri işleme ilkelerine uyulması gerekecektir. Örneğin kişisel veri işlenirken ilgili kişinin açık rızası alınsa dahi aşırı miktarda veri işlenmesi genel ilkelerle bağdaşmayacağından hukuka aykırı olacaktır. Açık rıza, veri koruma ilkelerinden bir muafiyet olarak değil, kişisel verilerin işlenmesinde bir güvence olarak benimsenmelidir³⁶⁹.

³⁶⁷ **Başalp**, Kişisel Veri, s.39.

³⁶⁸ **Çekin**, Kişisel Veri, s. 73.

³⁶⁹ **Data Protection WP**, Opinion 15/2011 on the definition of consent, s.7.

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf (E.T.: 16.03.2020).

“Açık rıza”nın varlığı için ilgili kişinin beyanında şüpheyi yer olmamalıdır. Veri sahibi kişinin rıza beyanı net değilse, makul bir şüphe varsa belirsizlik olduğundan açık rızadan söz edilemez. Bu nedenle veri sorumluları ilgili kişilerin verilerin açık rızasını almada ehemmiyet göstermelidir. Zira gereken özeni göstermemeleri durumunda veri işleme hukuka aykırı bir hal alacaktır. Özellikle telefon veya internet üzerinden açık rızanın alınması durumunda rızayı veren kişinin gerçek veri sahibi olup olmadığına dikkat edilmelidir. Zira herhangi bir uyuşmazlık çıkması durumunda açık rızanın alındığını ispat edecek olan ilgili kişi değil, veri sorumlusudur³⁷⁰.

Kişi, kendisi hakkındaki bilgilerin işlenmesini istemiyorsa rıza vermemesi yeterlidir. Ayrıca neden rıza vermediğini gerekçelendirmesi gerekmemektedir³⁷¹. Aksine kişinin rızası olmamasına rağmen işlemenin yapıldığı durumda veri sorumlusunun gerekçelendirme yapması gerekmektedir.

2. Sessiz Kalınması

İlgili kişinin iradesini aktif bir şekilde belirtmediği durumda açık rızanın varlığından söz edilemez. Veri sahibi kişinin susması, sessiz kalması gibi pasif kaldığı bir durumda KVKK kapsamında bir açık rıza verildiğinden söz edilemez. İnternet sitesindeki önceden işaretlenmiş kutular veya ilgili kişinin sessizliği rıza verildiği anlamına gelmez. Rıza, açıkça olumlu bir eylem (affirmative act) şeklinde verilmelidir³⁷². Sonuç olarak kişisel verilerin açık rızaya dayanarak işlenebilmesi için zımni irade beyanı yeterli

³⁷⁰ **Data Protection WP**, Consent, s.21.

³⁷¹ **Şimşek**, s. 107.

³⁷² GDPR, 32. paragraf.

değildir³⁷³.

Örneğin ilgili kişiye gelen bir yazıda “*yazıya cevap verilmediği takdirde kişinin rıza vermiş sayılacağı*” beyanı olsun. Kişinin bu yazıya cevap vermemesi durumunda rıza verip vermediği belirsizdir. Bu nedenle bireyin pasif olan susma eylemi açık rıza olarak sayılamaz³⁷⁴. Kişisel verilerin işlenmesi, kişinin temel hakkına müdahale anlamına geleceğinden ilgili kişi lehine yorum yapmak gerekir. Kanaatimce açık rızanın olup olmadığı konusunda belirsizlik olması durumunda veri işlemede açık rızanın bulunmadığı kanaatine varılmalıdır.

Açık rızadan söz edebilmek için kişinin iradesinin aktif olması gerektiğinden bahsettik. Bu husus özellikle internette çerez (cookies) kullanımı hususunda önem arz etmektedir. Çerezler kişilerin internette dolaşımları sırasında hareketlerini izleme işlevi görmektedir³⁷⁵. Kişiler çerezler vasıtasıyla internette gezinirken izlenmektedir. Kişilerin dolaştığı sitelerden, yaptığı aramalardan çıkarımlar yapılmaktadır. Kişilerin alışveriş tercihleri, zevkleri, hobileri gibi bilgiler çerezler sayesinde elde edilebilmektedir. Bu sayede de kişilere özgü reklamlar sunularak şirketler ciddi anlamda gelir elde etmektedir. Bu uygulamaların ekonomik anlamda faydaları bulunmaktadır. Ancak kişisel verilerin korunması bakımından söz konusu uygulamalara mesafeli yaklaşılması gerekmektedir. Özellikle ilgili kişinin açık rızasının mevzuata uygun şekilde alınıp alınmadığı değerlendirilmelidir.

³⁷³ Kurul, Amazon kararında benzer şekilde “*zımni irade beyanı ile onay alınmasının mevzuata uygun kabul edilemeyeceği*”ni belirtmiştir. **Kurul Kararı**, 27.02.2020 T., 2020/173 K. <https://kvkk.gov.tr/Icerik/6739/2020-173> (E.T.: 12.05.2020).

³⁷⁴ **Data Protection WP**, Consent, s.23-24.

³⁷⁵ **Keser Berber, Leyla**, Çevrimiçi Davranışsal Reklamcılık (Online Behavioral Advertising) Uygulamaları Özelinde Kişisel Verilerin Korunması, İstanbul 2014, s. 23.

İnternet siteleri tarafından “Sizlere daha iyi hizmet sunabilmek için çerez kullanıyoruz. Sitemizi kullanmaya devam etmeniz bu kullanımı kabul anlamına gelmektedir.” benzeri ifadelerle uygulamada sıklıkla karşılaşılmaktadır. Söz konusu uygulamalar açık rızanın özgür iradeye dayanması unsuruyla ve açık rızanın aktif bir hareketle verilmesi gerekliliğiyle bağdaşmamaktadır. Zira kişinin salt siteyi kullanması kişinin iradesini aktif olarak belirtmesi olarak değerlendirilemez. Bu ifadelerin altında ise “kabul ediyorum”, “anladım” şeklinde kutucuklar yer alabilmektedir. Kişiye seçim hakkı tanımayan bu uygulamaların da açık rıza ile uyduğu söylenemez. Benzer şekilde önceden tıklanmış kutucuklar da açık rızayla bağdaşmamaktadır³⁷⁶.

Kurul da Amazon kararında³⁷⁷ açık rıza alınırken opt-out sisteminin değil opt-in sisteminin kullanılması gerektiğini belirtmiştir. Karara göre, “*Kanunda yer verilen tanım çerçevesinde veri sorumluları tarafından ilgili kişilerden alınacak açık rıza beyanlarında opt-out yani bireyin önceden onayını almaksızın kişisel verilerinin işlenmesine otomatik onay verdiklerinin kabul edildiği ve kişilere bu onayı kaldırmaları yönünde imkân veren bir sistemin değil, opt-in yani bireyin bilinçli eylemi ile kişisel verilerinin işlenmesine onay vereceği bir sistemin kullanılması gerekmektedir.*” Opt-out sisteminde kişiler karşı çıkmadıkça verilerinin işlenmesine rıza verdikleri kabul edilir. Opt-in sisteminde ise kişi açık rızasını bilinçli eylemi ile açıklamalıdır. KVKK’daki açık rıza düzenlemesi opt-in sisteminin tercih edildiğini göstermektedir. Zira açık rızanın veri işlemeye başlanmadan önce alınması gerekmektedir. Bu nedenle Kurul’un yaptığı tespit kanımızca yerinde olmuştur.

³⁷⁶ Çekin, Kişisel Veri, s. 189-190.

³⁷⁷ **Kurul Kararı**, 27.02.2020 T., 2020/173 K. <https://kvkk.gov.tr/Icerik/6739/2020-173> (E.T.: 12.05.2020).

3. Açık Rızayı Açıklama Ehliyeti

Tam ehliyetli olan kişilerin rıza beyanında bulunabileceği aşikardır. Ancak doktrinde tartışmalı olan husus tam ehliyetli olmayan kişilerin özellikle küçüklerin veri işlenmesine rıza gösterip gösteremeyecekleri hususudur. Çalışma Grubu'na göre tam ehliyete sahip olmayan kişilerin rızasının geçerli sayılma hususu her ülkeye göre değişecektir³⁷⁸.

Kişilik hakkı, kişiye sıkı sıkıya bağlı bir haktır. Kişisel verilerin korunması hakkının temelinde kişilik hakkı olduğunu ayrıntılarıyla tespit ettik. Bu nedenle “*kişisel verilerin işlenmesine rıza gösterme hakkı*”nın da kişiye sıkı sıkıya bağlı bir hak olduğu tespiti yapılabilir³⁷⁹. Tam ehliyetlilerin bu hakkı bizzat kullanacağı açıktır. Tam ehliyetsizler ise kişiye sıkı sıkıya bağlı hakları bizzat kullanamazlar³⁸⁰. Sınırlı ehliyetsizler yani ayırt etme gücüne sahip küçük ve kısıtlıların söz konusu hakkıyla ilgili düzenleme TMK m. 16'dadır. Buna göre “*Ayırt etme gücüne sahip küçükler ve kısıtlılar,*

³⁷⁸ Çalışma Grubu'nun çocukların kişisel verileri ile ilgili yayımladığı görüşleri için bkz.

Data Protection WP, Working Document 1/2008 on the protection of children's personal data (General guidelines and the special case of schools) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2008/wp147_en.pdf (E.T.: 18.03.2020). Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp160_en.pdf (E.T.: 18.03.2020).

³⁷⁹ **Aksoy, Hüseyin Can**, “*Kişisel Verilerin İşlenmesi Kapsamında Rıza Unsuru ve Sınırlı Ehliyetsizlerin Durumu*”, Haluk Konuralp Anısına Armağan, C. 3, Ankara 2009, s. 57.

³⁸⁰ **Dural/Öğüz**, s. 79; **Gezder, Ümit**, Türk Medeni Hukuku-Başlangıç-Kişiler-Aile Hukuku Soruları ve Cevapları, C. 1, İstanbul 2014, s. 39.

yasal temsilcilerinin rızası olmadıkça, kendi işlemleriyle borç altına giremezler. Karşılıksız kazanmada ve kişiye sıkı sıkıya bağlı hakları kullanmada bu rıza gerekli değildir.” Hükümde görüldüğü üzere sınırlı ehliyetsizler açısından kural ehliyetsizlik, istisna ehliyettir³⁸¹. Başka bir ifadeyle, kural olarak sınırlı ehliyetsizler ehliyetsizdirler. Ancak kişiye sıkı sıkıya bağlı hakları kullanmada ehliyetlidirler³⁸². Yani kişiye sıkı sıkıya bağlı hakları kullanma istisna kapsamındadır. Bu nedenle sınırlı ehliyetsizler kişiye sıkı sıkıya bağlı hakları bizzat kullanabilirler. Yasal temsilcilerinin rızası gerekmez. Ancak kanunda belirtilen bazı durumlarda sınırlı ehliyetsizler tarafından kişiye sıkı sıkıya bağlı hakların kullanımında yasal temsilcisinin rızası aranmaktadır. Evlenme, evlat edinilme de kişiye sıkı sıkıya bağlı haklardandır. Ancak kanun gereği bu hakların kullanımı için yasal temsilcinin rızası gerekmektedir³⁸³. Yani sınırlı ehliyetsizlerin zarar görme tehlikesinin olduğu durumlarda kişiye sıkı sıkıya bağlı haklarda dahi yasal temsilcinin izni aranmaktadır³⁸⁴. Kişisel verilerin işlenmesi durumunda sınırlı ehliyetsizlerin zarar görme tehlikesi bulunmaktadır. Aksoy, bu temele dayanarak bu hususta kanunda örtülü boşluk olduğunu öne sürmektedir. Aksoy’a göre “*kişisel verilerin işlenmesine rıza gösterme hakkı*” her ne kadar kişiye sıkı sıkıya bağlı bir hak da olsa, sınırlı ehliyetsizlerin korunması amacıyla sınırlı ehliyetsizlerin verileri işlenirken yasal temsilcilerinin rızası alınmalıdır³⁸⁵. Bu görüşün sınırlı ehliyetsizlerin korunması açısından daha faydalı olacağını kabul etmekle birlikte biz bu görüşe katılmıyoruz. Zira TMK m. 16’da kişiye sıkı sıkıya bağlı hakları kullanmada yasal temsilcinin rızasının gerekmediği açıkça

³⁸¹ Dural/Öğüz, s. 85.

³⁸² Helvacı, s. 78.

³⁸³ Dural/Öğüz, s. 93; Helvacı, s. 83.

³⁸⁴ Aksoy, Rıza, s. 59.

³⁸⁵ Aksoy, Rıza, s. 59 vd.

düzenlenmiştir. Kişiyi sıkı sıkıya bağlı hak olmasına rağmen yine de yasal temsilcinin rızasının arandığı haller de kanunda belirtilmiştir. Ancak ne TMK’da ne de KVKK’da sınırlı ehliyetsizlerin kişisel verilerinin işlenmesine dair bir hüküm bulunmamaktadır. Bu nedenle mevcut durumda TMK m. 16 gereği sınırlı ehliyetsizlerin kişisel verilerinin işlenmesinde yasal temsilcilerinin rızasının alınması gerekmekte, ayırt etme gücüne sahip çocuğun açık rızası yeterli olmaktadır. Ancak bu durumun hakkaniyete aykırı sonuçlar doğurabileceği bizim de kabulümüzdür. Yetişkinler kişisel verilerin korunması bilincine ne kadar sahiptir ki sınırlı ehliyetsizler bu bilince sahip olsun! Özellikle çocuklar, kişisel verilerinin işlenmesinin ileride doğurabileceği olumsuzlukları tam olarak tahayyül edemez. Bu nedenle fikrimce GDPR m. 8’dekine benzer bir madde KVKK’ya eklenerek, özellikle belli bir yaştaki küçüklerin kişisel verilerinin işlenmesinde yasal temsilcilerinin de açık rızası aranmalıdır.

4. Açık Rızanın Şekli

Açık rızanın verilmesinde herhangi bir şekil şartı bulunmamaktadır. Genel olarak açık rıza yazılı olarak açıklansa da bu bir zorunluluk değildir. Açık rıza, yazılı veya sözlü olarak verilebilir. Bu rıza, kağıt üzerinde olabileceği gibi elektronik ortamda da beyan edilebilir. Ancak belirtmek gerekir ki, rızanın sözlü olarak açıklanması durumunda ispatı güçleşecektir. Bu nedenle kanıtlanabilirlik açısından bizim de tavsiyemiz açık rızanın yazılı olarak alınmasıdır³⁸⁶. Zira açık rızanın alındığını kanıtlayacak olan veri sorumlusudur.

³⁸⁶ **Data Protection WP**, Consent, s.25.

5. Açık Rızanın Açıklanacağı Zaman

İlgili kişinin açık rızası kişisel veri işlenmeye başlanmadan önce alınmalıdır. Bu hususun bilhassa çerez (cookies) yerleştirilmesi gibi çevrimiçi davranışsal reklamcılık uygulamalarında göz önünde bulundurulması gerekmektedir³⁸⁷. Veri işleme amacının değişmesi durumunda da rıza tekrardan alınmalıdır. Rıza alınmadan veri işlenmesi durumunda veri işleme hukuka aykırı olacağından sonradan rıza alınması hukuka aykırılığı ortadan kaldırmaz.

6. Açık Rızanın Geri Alınması

Açık rıza beyanında bulunan ilgili kişi sonrasında bu beyanını geri alabilir³⁸⁸. Rızanın geri alınması, rıza beyanında bulunmak kadar zahmetsiz olmalıdır³⁸⁹. Kişi istediği zaman verdiği rızayı geri alabilir. Ancak rızanın geri alınması geçmişe etki etmez. Yani rızanın geri alınması, geri almadan önce rızaya dayanarak yapılan veri işlemenin hukuka uygunluğuna halel getirmez. Geri alma ileriye yönelik sonuç doğuracaktır. Rızanın geri alınması isteği veri sorumlusuna vardıktan sonra açık rıza sebebine bağlı olan tüm işlemlere veri sorumlusu tarafından son verilmelidir³⁹⁰. Rızanın geri alındığı aşamadan sonra veri işlenmesine devam edilmesi hukuka aykırı olacaktır.

³⁸⁷ **Ayözger Öngün**, s. 137. Çevrimiçi davranışsal reklamcılık konusunda detaylı bilgi için bkz. **Keser Berber**, s. 1 vd.

³⁸⁸ **Data Protection WP**, Consent, s.34.

³⁸⁹ GDPR m. 7/3.

³⁹⁰ **Kurum**, Data Protection In Turkey, s. 14.

<https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/5c02cb3c-7cc0-4fb0-b0a7-85cb90899df8.pdf> (E.T.: 02.04.2020).

7. Açık Rızanın Unsurları

a. Belirli Bir Konuya İlişkin Olma

Açık rızanın geçerli olabilmesi için ilk koşul “*belirli bir konuya ilişkin*” yani spesifik (specific) olmasıdır. Spesifik bir konuyla ilgili olmayan, “*battaniye rıza (blanket consent)*” geçerli bir açık rıza olarak kabul edilemez³⁹¹. Örneğin ilgili kişi tarafından yapılan “*kişisel verilerimin işlenmesini kabul ediyorum*” beyanı çok geniş kapsamlı olduğundan geçerli bir “*açık rıza*” değildir³⁹². Bu şekilde bir ifade çok geneldir. Oysa açık rızadan bahsedebilmek için hangi amaç için rıza verildiği belirli olmalıdır³⁹³. Yine “*gelecekteki talepler*”, “*daha fazla iş*” ve “*diğer şirketlerle işbirliği*” gibi gelecekteki sebeplerle veri işlenmesi için verilen rıza belirli konuya ilişkin olmadığı için geçersizdir³⁹⁴.

Açık rızanın belirli ve anlaşılabilir olması gerekir. Açık rızada veri işlemenin detaylı bir şekilde kapsamı ve işlemenin sonuçları belirtilmelidir³⁹⁵. Farklı kategorilerdeki verilerin işlenmesi için açık rıza verilecekse her bir kategori için ayrı ayrı rıza verilmesi gerekmektedir. İşlendikten sonraki işlemler için de (verilerin 3.kişilerle paylaşımı gibi) ayrı bir açık rıza alınması gerekmektedir³⁹⁶.

³⁹¹ **Data Protection WP**, Consent, s.17.

³⁹² **Kurum**, Açık Rıza, s. 4.

³⁹³ **Çekin**, İrade Serbestisi, s. 637.

³⁹⁴ **Ochsenfeld, Michael F.**, Datenschutz für Betriebsräte: Kurz und knackig, 2. Auflage, 2017, s. 38.

³⁹⁵ **Data Protection WP**, Consent, s.17.

³⁹⁶ **Kurum**, Açık Rıza, s.4.

b. Bilgilendirmeye Dayanma

Açık rızanın “*bilgilendirmeye dayanması (informed)*” KVKK m. 10 uyarınca veri sorumlusunun yerine getirmesi gereken “*aydınlatma yükümlülüğü*” ile yakından ilişkilidir. KVKK m. 10 gereği “*Kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişi, ilgili kişilere; veri sorumlusunun ve varsa temsilcisinin kimliği, kişisel verilerin hangi amaçla işleneceği, işlenen kişisel verilerin kimlere ve hangi amaçla aktarılacağı, kişisel veri toplamanın yöntemi ve hukuki sebebi, 11. maddede sayılan diğer hakları, konusunda bilgi vermekle yükümlüdür.*” Açık rızası alınacak kişiye veri sorumlusu tarafından bu bilgilendirmelerin yapılması gerekmektedir.

İlgili kişinin açık rıza verebilmesi için kişinin kendisiyle ilgili bilgilerden hangilerinin işlenmesine rıza gösterdiğini bilmesi, kavraması gerekmektedir. Kişinin bunları tam olarak anlayabilmesi için teknik jargon kullanılmamalı, yazıların okunaklı olmasına ve küçük puntolarda olmamasına dikkat edilmelidir. Bilgilendirme kesinlikle veri işlenmeye başlamadan önce yapılmalıdır. Bu unsurun yerine getirilmesi “*kişinin kendi geleceğini belirleme hakkı*”nın da bir göstergesidir³⁹⁷.

Rızanın bu unsuru “*şeffaflıkla (transparency)*” ilgilidir. Veri sorumlusu, ilgili kişiyi şeffaf bir şekilde bilgilendirmelidir. Şeffaflık, kişisel verilerin işlenmesinin yasallığını sağlayan tek koşul olmasa da rızanın geçerli olması için ana koşullardan biridir. Rızanın geçerli olması için bilgilendirmeye dayanması gerekmektedir. Bu bilgilendirme, veri işlemenin önemli yönlerini içermelidir³⁹⁸.

³⁹⁷ **Kurum**, Açık Rıza, s.5.

³⁹⁸ **Data Protection WP**, Consent, s.9.

c. Özgür İradeyle Açıklanma

Açık rızanın “*özgür iradeyle açıklanması (freely given)*” gerekmektedir. TDK’nın da özgür tanımı³⁹⁹ gibi, ilgili kişinin iradesi, “*herhangi bir kısıtlamaya, zorlamaya, şarta bağlı olmayan hür bir irade*” olmalıdır.

Bu unsur gereği ilgili kişinin gerçekten seçim yapabilecek durumda olması gerekir. İlgili kişinin bu seçimi; cebir, hata, hile veya tehdit sebebiyle olmamalıdır. Ayrıca rıza göstermediği takdirde kendisiyle ilgili olumsuz sonuçlar ortaya çıkacağı düşüncesine dayanmamalıdır. Rıza beyanının yol açacağı sonuçların ilgili kişinin seçim özgürlüğünü engellemesi durumunda rızanın özgür iradeyle açıklandığından söz edilemez. Bu duruma işçi-işveren ilişkisinde işçinin rızası örnek olarak verilebilir. İşçi-işveren ilişkisi⁴⁰⁰ bağımlılık esaslı bir ilişki olduğundan “*özgür iradenin*” daha detaylı bir şekilde irdelenmesi gerekmektedir. Zira işten çıkma korkusuyla rızasını açıklayan bir işçinin beyanının özgür iradeye dayanması beklenemez⁴⁰¹.

Sözleşmenin ifası için rızanın gerekmediği bir durumda, ifanın rıza şartına bağlanması rızayı geçersiz kılacaktır⁴⁰². Yine bu unsurun gereği olarak, veri sahibinden rıza beyanı alınması, bir hizmetten faydalanma veya bir mal temininin koşulu olarak

³⁹⁹ **TDK**, <https://sozluk.gov.tr> (E.T.: 16.03.2020).

⁴⁰⁰ İş ilişkisinde rızanın özgür iradeyle açıklanması ile ilgili detaylı bilgi için bkz. **Data Protection WP**, Consent, s.13-14.

⁴⁰¹ **Kuner**, s. 68; **Data Protection WP**, Consent, s.12-13.

⁴⁰² **Yücedağ, Nafiye**, “*Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu’nun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri*”, İÜHFM, 2017, C. 75, S. 2, s. 774.

sunulamaz⁴⁰³. Bu konuyla ilgili bir kurul kararında⁴⁰⁴ “herhangi bir ürün ve/veya hizmetin sunumunun, açık rıza verme ön şartına bağlanmaması gerektiği ve eğer yapılan seçimin sonuçları, kişisel veri sahibinin seçim özgürlüğünü etki altında bırakıyorsa, bu durumda rızanın özgürce verildiğini söylemenin mümkün bulunmadığı” ifadelerine yer verilmiştir. Söz konusu kararda “üyelere sunulan online üyelik sözleşmesinde, özel nitelikli kişisel veri olan avuç içi izinin alınmasına onay verilmesinin sözleşmenin kurulması için zorunlu bir şart olarak sunulduğu ve kurala uyulmaması halinde firmaya fesih hakkı tanınmış olduğu hususları birlikte değerlendirildiğinde üyelerin kulüplere girişlerde avuç içi izi bilgilerinin alınmasına rıza göstermemeleri halinde söz konusu hizmetten yararlanamayacakları dikkate alındığında, üyeler tarafından verilen açık rızaların özgür iradeye dayalı olduğunu söylemenin mümkün bulunmadığı” saptanmıştır.

Örneğin bir fitness salonuna üyelik şartı olarak kişinin “retina ve iris görüntüleri”nin alınması zorunlu tutulamaz. Zira kişi özgür iradesiyle değil, salt üye olma gayesiyle bu verilerin işlenmesine rıza vereceğinden özgür iradeyle açıklanan bir rızadan söz edilemez. Bu sebeple de kişinin bu bilgilerinin işlenmesi hukuka aykırı olacaktır.

B. Açık Rıza Gerekmeyen Haller

Veri sorumlusu, kişisel verileri işlerken öncelikle KVKK m.5/2’de sayılan açık rıza gerekmeyen hallerden biri olup olmadığını kontrol edecek, eğer veri işlemek için herhangi bir hale dayanılamıyorsa kişinin açık rızası alınarak veri işlenebilecektir. Kısaca veri işlenirken ilk bakılacak KVKK m.5/2dir. Eğer somut hal buradaki hallerden biri

⁴⁰³ **Kurum**, Açık Rıza, s.6.

⁴⁰⁴ **Kurul Kararı**, 25.03.2019 T., 2019/81 K. <https://www.kvkk.gov.tr/Icerik/5496/2019-81-165> (E.T.: 18.03.2020).

değilse o zaman KVKK m.5/1 gereği ilgili kişinin açık rızası aranacaktır. Kişisel verileri işlemek için açık rıza dışında başka bir sebebe dayanılabilecekken açık rızaya dayanılması, “*hakkın kötüye kullanımı*” anlamına gelecek ve temel ilkelerden olan “*hukuka ve dürüstlük kuralına uygun işleme*”ye aykırılık oluşturacaktır⁴⁰⁵. Kurul da aynı görüştedir. Kurul’un bu husustaki kararına⁴⁰⁶ göre, “*Kişisel veri işleme faaliyetinin, Kanunda bulunan açık rıza dışındaki şartlardan birine dayanıyorsa, bu durumda ilgili kişiden açık rıza alınmasına gerek bulunmadığı ve veri işleme faaliyetinin, açık rıza dışında bir dayanakla yürütülmesi mümkün iken açık rızaya dayandırılmasının, aldatıcı ve hakkın kötüye kullanımı niteliğinde olacağı; nitekim ilgili kişi tarafından verilen açık rızanın geri alınması halinde veri sorumlusunun diğer kişisel veri işleme şartlarından birine dayalı olarak veri işleme faaliyetini sürdürmesinin hukuka ve dürüstlük kurallarına aykırı işlem yapılması anlamına geleceği dikkate alınarak karar verilmiştir.*”

Aynı zamanda Kurul’a göre, açık rıza gerekmeyen hallerden birine dayanılarak veri işleniyorsa ayrıca ilgili kişiden açık rıza alınmamalıdır⁴⁰⁷.

KVKK 5. maddede “*açık rıza gerekmeyen haller*” 7 bent halinde sayılmıştır. Şimdi sırasıyla bunları inceleyelim.

1. Kanunlarda Açıkça Öngörülmesi

Bu hallerden ilki KVKK m.5/2/a’da düzenlenen “*kanunlarda açıkça öngörülmesi*” halidir. Buna göre ilgili kişinin açık rızası olmasa dahi “*kanunlarda açıkça*

⁴⁰⁵ **Kurum**, Doğru Bilinen Yanlıklar, s. 26; **Kurum**, Kişisel Verilerin İşlenme Şartları, s. 3-6.

⁴⁰⁶ **Kurul Kararı**, 08.07.2019 T., 2019/206 K. <https://kvkk.gov.tr/Icerik/6709/2019-206> (E.T.: 03.04.2020).

⁴⁰⁷ **Kurum**, Doğru Bilinen Yanlıklar, s. 25.

öngörülen bir hal” varsa kişisel veri işlenebilir. Örneğin 2559 sayılı PVSİ m.5 “*şüphelilerden parmak izi alınması*” hali kanunda açıkça hükme bağlanmıştır. Kişinin kişisel verisi niteliğinde olan parmak izi, kanunda açıkça hükme bağlandığından açık rızası olmasa da bu verisinin işlenmesi olanaklıdır. Yine İK m. 75⁴⁰⁸ gereğı işveren “*işçi özlük dosyası*” tanzim etmek zorundadır. İşçinin rızası olması dahi işveren tarafından tanzim edilen dosya kapsamında veri işleme hukuka uygun olacaktır⁴⁰⁹. Yine veri sorumluları tarafından KVKK m. 16 gereğı VERBİS’e yapılan veri bildirimi “*kanunda açıkça düzenlenen veri işleme hali*”ne örnek olarak verilebilir⁴¹⁰.

2. Fiili İmkansızlık

KVKK’da düzenlenen ikinci hal (KVKK m. 5/2/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*” halidir. Örneğin trafik kazası sonucu bilinç kaybı yaşayan kişiye hastanede müdahale yapılabilmesi amacıyla işlenen veriler bu kapsamda değerlendirilecektir. Zira böyle bir durumda kişi rızasını istese de açıklayamayacağından zarurilik söz konusudur. Yine gözetim altında bulunduğu yerden kaçan akıl hastasının yakalanması durumunda iadesi ve korunması için gerekli bilgilerin işlenmesi (adı, soyadı, T.C. kimlik numarası vb.) hali de bu kapsamda değerlendirilebilir. Zira burada da rızasına

⁴⁰⁸ İK m. 75 “*İşveren çalıştırdığı her işçi için bir özlük dosyası düzenler. İşveren bu dosyada, işçinin kimlik bilgilerinin yanında, bu Kanun ve diğer kanunlar uyarınca düzenlemek zorunda olduğu her türlü belge ve kayıtları saklamak ve bunları istendiği zaman yetkili memur ve mercilere göstermek zorundadır.*”

⁴⁰⁹ Başalp, s. 41.

⁴¹⁰ Kurum, Örnekler, s. 11.

hukuki geçerlilik tanınmayan bir kişi bulunmaktadır. Başka bir örnek olarak yaşadığı şehirde meydana gelen deprem sonucu enkaz altında kalan kişinin kurtarılabilmesi için cep telefonu bilgisi ve konum bilgisinin işlenmesi hali örnek olarak verilebilir. Burada da kişinin hayatının korunması için zorunluluk olduğu gibi kişinin rızasının beklenmesi de abes kaçacaktır. Söz konusu bent kapsamında en çok dikkat edilmesi gereken husus “zorunlu olma hali”dir. Diğer tüm koşullar gerçekleşse bile verinin işlenmesin gerçekten zorunlu olup olmadığı dikkatle incelenmelidir.

Kişisel verilerin işlenmesi başkasının hayatının korunması için zorunlu olabilir. Salgın hastalıkların yayılmasını önlemek için veri işlenmesi buna örnek olarak verilebilir⁴¹¹. Örneğin COVID-19 testi pozitif çıkan ve yoğun bakımda tedavi altında tutulan bir kişiye ait aile bilgileri, virüsü kaptıktan sonraki konum verileri, hastalığı yayabileceği potansiyel çevre bilgileri gibi hastalığın yayılmasını önlemek için işlenen veriler bu kapsamda değerlendirilebilir. Kişinin COVID-19 virüsünü taşıdığına ilişkin bilgi, hassas veri olan kişisel sağlık verisi olduğundan KVKK m. 6/3 kapsamında açık rıza aranmadan işlenebilir. Burada kastettiğimiz ise hastalığın topluma yayılmasını önlemek için işlenen verilerdir. Hastalığa yakalan kişinin son 10 günlük konum bilgilerinin tespit edilmesi gibi.

Kurul tarafından bu konu ile ilgili bir duyuru yapılmıştır. Bu duyuruda salgın hastalıklarla mücadele amacıyla işlenen konum verilerinin KVKK m. 28/1/ç kapsamında olduğu ve bu nedenle KVKK’ nın uygulanmayacağı belirtilmiştir⁴¹². Kanımızca KVKK

⁴¹¹ GDPR, 46. paragraf.

⁴¹² **Kurul**, 09.04.2020 T. <https://www.kvkk.gov.tr/Icerik/6726/COVID-19-ILE-MUCADELEDE-KONUM-VERISININ-ISLENMESI-VE-KISILERIN-HAREKETLILIKLERININ-IZLENMESI-HAKKINDA-BILINMESI-GEREKENLER-2-> (E.T.: 06.05.2020).

uygulama alanı bulsa dahi söz konusu veriler açık rıza aranmadan işlenebilir. Ancak bu kadar büyük çapta kişisel veri işleme faaliyetini KVKK koruması dışında bırakmanın ne kadar isabetli olduğu tartışılabilir. Kanaatimce söz konusu verilerin işleme dayanağı ne olursa olsun veri güvenliği tedbirleri alınmalı ve salgın hastalık sona erdiğinde söz konusu veriler imha edilmelidir. Ayrıca her zaman olduğu gibi kişisel verilerin işlenmesi faaliyetinin her aşamasında temel ilkelere tam uyum sağlanmalıdır.

3. Sözleşmenin Kurulması veya İfası İçin Gerekli Olması

KVKK m.5/2/c'ye göre *“bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması”* durumunda da kişisel veriler işlenebilecektir. Burada dikkat edilmesi gereken husus bu bent kapsamında sadece sözleşme taraflarının verileri işlenebilir, 3. kişilerin verileri işlenemez. Ayrıca hükümde *“sözleşmenin kurulması”* veya *“sözleşmenin ifası”* olarak iki farklı durum söz konusudur.

Yukarıda da ifade edildiği gibi bent kapsamında hem sözleşmenin kurulması hem de ifası ile ilgili olan veriler işlenebilecektir. Her iki durumda da doğrudan ilgili olmak ve gerekli olmak kaydıyla veriler işlenebilecektir. İlk durum *“sözleşmenin kurulması aşaması”*yla ilgilidir. Sözleşmenin kurulması amacıyla sözleşme öncesi verilerin işlenmesi hukuka uygun olacaktır. Örneğin aracına kasko yaptırmak isteyen bir kişinin kasko şirketinden fiyat teklifi talep etmesi durumunda, kasko şirketinin bu teklifi hazırlamak amacıyla aracın markası, yaşı, araç hasar kaydı vb. gerekli verileri işlemesi hukuka uygundur⁴¹³. Yine iş kurmak amacıyla bankadan kredi almak isteyen bir kişiden

⁴¹³ **Data Protection WP**, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, s. 18.

banka tarafından istenen maaş bordrosu, ipotek olarak verilebilecek gayrimenkul bilgisi, araç ruhsat bilgisi veya ek gelir belgesinin işlenmesi sözleşmenin kurulması aşamasıyla ilgilidir.

İkinci durum ise “*sözleşmenin ifası aşaması*”yla ilgilidir. Sözleşme kurulduktan sonra tarafların IBAN bilgilerinin veya teslimat adreslerinin işlenmesi de bu bent kapsamındadır. Zira ifanın sözleşmeye uygun olarak yerine getirilebilmesi için doğru yerde yapılması gerekmektedir.

Veri işlemenin sözleşme kapsamında yapılabilmesi için “*gereklilik (necessary)*” kısmına dikkat etmek gerekir. Hukuka uygun olarak veri işlenebilmesi için işleme, sözleşme için gerekli bir işleme olmalıdır. Örneğin internet sitesinden alışveriş yapılması (ayakkabı siparişi gibi) durumunda kredi kartı bilgilerinin işlenmesi bu kapsamda değerlendirilebilir. Ancak satın alınan mallara göre ilgili kişinin alışveriş tercihleri ve zevkleri hakkında profillemeye⁴¹⁴ yapılması KVKK m.5/2/c kapsamında değerlendirilerek hukuka uygun bir işleme sayılamaz. Zira veri sorumlusu bu somut olayda mal temininden (ayakkabıyı göndermek) sorumludur ve müşteri profilinin çıkarılmasının hükümde yer alan bir “*gereklilik*” olduğu söylenemez. Başka bir ifadeyle, müşterinin alışveriş tercihlerinden profilinin çıkarılması sözleşmenin ifası için gerekli değildir. Somut olayda veri işleme gerekliliğinin olup olmadığını ayırt edebilmek için sözleşmenin asıl amacının tespit edilmesi gerekmektedir⁴¹⁵. Taraflar arasında birden fazla sözleşme söz konusu olabilir. Böyle bir durumda “*gereklilik*” unsuru her sözleşme açısından bağımsız olarak

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf (E.T.: 19.03.2020).

⁴¹⁴ Ayrıca belirtmek gerekir ki, profillemeye karşı ilgili kişiye itiraz etme hakkı tanınmalıdır. GDPR, 70. paragraf.

⁴¹⁵ **Data Protection WP**, Legitimate Interests, s. 16-17.

değerlendirilmelidir. Bir sözleşme için gerekli olan veri diğer sözleşme için gerekli olmayabilir⁴¹⁶.

KVKK m. 5/2/c'ye dayalı bir işleme, bir Kurul kararına yansımıştır. Kurul'a yapılan şikayette, seyahat ile ilgili bir mobil uygulamada yapılan yolculukların puanlandığı belirtilmiştir. Veri sorumlusu söz konusu puanlama ile ilgili bilgilerin KVKK m. 5/2/c kapsamında sözleşme gereğince işlendiği savunmasını yapmıştır. Ancak Kurul söz konusu verilerin işlenmesinin sözleşmenin kurulması veya ifası için zorunlu olmadığına kanaat getirmiş ve söz konusu verilerin işlenmesini hukuka aykırı bulmuştur⁴¹⁷.

4. Veri Sorumlusunun Hukuki Yükümlülüğünü Yerine Getirebilmesi İçin Zorunlu Olması

KVKK'da kişisel verilerin işlenebilmesi için düzenlenen dördüncü hal (KVKK m. 5/2/ç), “*veri sorumlusunun hukuki yükümlülüğünü (legal obligation) yerine getirebilmesi için zorunlu olması*” halidir. Veri sorumlusunun KVKK dışında da bazı kanunlarla kendisine yüklenmiş bazı yükümlülükler olabilir. Ve bu yükümlülüklerin yerine getirilmesi için kişiyle ilgili verilerin işlenmesi zorunluluğu doğabilir. Veri sorumlusunun hukuki yükümlülüğünü yerine getirmesi için ilgili kişinin rızasının alınması, yükümlülüğe uyulamamasına yol açabilir⁴¹⁸. Bu nedenle böyle bir durumda ilgili kişinin rızası aranmayacaktır. Bentteki zorunluluk unsurunun somut olayda gerçekleşip gerçekleşmediğine dikkat edilmesi gerekir. Bu hususla ilgili bir kurul

⁴¹⁶ Çekin, Kişisel Veri, s. 92.

⁴¹⁷ **Kurul Kararı**, 27.01.2020 T., 2020/65 K. <https://kvkk.gov.tr/Icerik/6717/2020-65> (E.T.: 03.04.2020).

⁴¹⁸ Küzeci, s. 344.

kararına⁴¹⁹ göre avukatın veri sorumlusu olması durumunda Avukatlık Kanunu ve İcra İflas Kanunundan kaynaklanan hukuki yükümlülükleri gereği açık rıza olmasa da veri işleyebileceğine karar verilmiştir. Karara göre “Somut olayda, veri sorumlusu bir avukat olup, vekili olduğu Banka adına, Bankanın haklarını ve menfaatlerini korumak amacıyla hareket ettiği, bu anlamda Avukatlık Kanunundan kaynaklanan yükümlülükleri ve yürütmekte olduğu icra işlemleri bakımından İcra İflas Kanunu ve ikincil mevzuat düzenlemelerinden kaynaklanan hukuki yükümlülüklerini yerine getirmek amacıyla borçluya ait bilgileri, kanuna uygun olarak işleme ve ilgili birim/mercilere bildirme yetkisi olduğu ve bu bağlamda işlediği kişisel verilerin Kanunun m.5/2 çerçevesinde ilgili kişinin açık rızası olmaksızın işlenmesinin kanuna uygun olacağına karar verilmiştir.” Söz konusu karara göre borçluya ait kişisel veriler açık rıza olmadan KVKK m. 5/2 gereği işlenebilirken, borçlunun kardeşine ait bilgiler bu kapsamda işlenemez.

Yine veri sorumlusu şirketin, işçisine ödeyeceği ücretin tespiti amacıyla veri işlemesi, bu bende örnek olarak gösterilebilir⁴²⁰.

KVKK m. 5/2/ç hükmünde kamu-özel ayrımı yapılmamıştır. Zaten yukarıda da değindiğimiz gibi, veri sorumlusu hem kamu hukuku hem de özel hukuk tüzel kişisi olabilir. Bu nedenle kamu kurumlarının da hukuki yükümlülükleri sebebiyle veri işlemesi bu bent kapsamındadır. Örneğin KTK m. 61 gereği “park etmenin yasaklanmış olduğu yerler”e araç park edilmesi durumunda araca ceza yazılabilmesi için veri işlenmesi bu

⁴¹⁹ **Kurul Kararı**, 14.01.2020 T., 2020/26 K. <https://www.kvkk.gov.tr/Icerik/6697/2020-26> (E.T.: 17.03.2020).

⁴²⁰ KVKK m.5 gerekçesine göre “Örneğin bir şirketin çalışanına maaş ödeyebilmesi için, banka hesap numarası, evli olup olmadığına bakmakla yükümlü olduğu kişiler, eşinin çalışıp çalışmadığı, sosyal sigorta numarası gibi verileri işlemesi bu bendin verdiği yetkiye istinaden olacaktır.”

bent kapsamında hukuka uygundur⁴²¹.

KVKK m. 5/2/ç'ye dayanılarak veri işlenmesi için veri sorumlusunun yükümlülüğü kanun hükmünden kaynaklanmalıdır. Sözleşme hükmünden kaynaklanan yükümlülük bu kapsamda değerlendirilemez. Bu durumda sözleşmeden kaynaklanan veri işlemeye (KVKK m. 5/2/c) dayanılabilir. Ayrıca belirtmek gerekir ki, veri sorumlusunun kanun hükmünde belirtilen hukuki yükümlülüğü yerine getirmesi zorunlu olmalıdır. Bu yükümlülüğü yerine getirip getirmeme konusunda bir seçim şansı olmamalıdır. Dolayısıyla hukuki yükümlülüğün ötesinde gönüllü olarak veri işlenmesi bu bent kapsamına girmeyecek ve hukuka uygun olmayacaktır. Örneğin internet servis sağlayıcılarının, herhangi bir hukuki yükümlülükleri olmadığı halde illegal dosya indirmeyi engellemek amacıyla kullanıcılarının verilerini işlemeleri hukuka uygun bir veri işleme faaliyeti sayılamayacaktır⁴²².

5. Kişisel Verilerin İlgili Kişinin Kendisi Tarafından Alenileştirilmesi

Bir başka hal (KVKK m.5/2/d) ise *“ilgili kişinin kendisi tarafından alenileştirilmiş olması”* halidir. Buna göre veri sahibi kendi isteğiyle veriyi alenileştirdiyse açık rıza olmaksızın veri işlenebilecektir. Zira kişi, kendisine ait verilerini kamuya paylaşmıştır. Bu nedenle de veri herkes tarafından ulaşılabilir hale geldiğinden artık *“verilerin işlenmesinde korunması gereken hukuki yarar ortadan kalkmıştır.”*⁴²³ Kişisel verilerin alenileştirilmiş sayılabilmesi için ilgili kişi *“alenileştirme iradesi”*ne sahip olmalıdır. Yani verinin kamuya açık alanda olması yetmez. Ayrıca veri sahibi

⁴²¹ **Data Protection WP**, Legitimate Interests, s.19.

⁴²² **Data Protection WP**, Legitimate Interests, s.19.

⁴²³ KVKK gerekçe, m.5.

tarafından kamuya açıklığın istenmiş olması gerekir⁴²⁴. Bu çıkarıma KVKK'nın “*kendisi tarafından*” ifadesiyle varılmaktadır. Örneğin bir avukatın kendi internet sitesinde iletişim bilgilerini paylaştığı durumda alenilik kabul edilecektir. Ancak 3. kişiler tarafından avukatın iradesi olmadan iletişim bilgilerinin paylaşılması durumunda söz konusu kişisel veri alenileştirilmiş kabul edilemeyecek ve bu bent kapsamında değerlendirilemeyecektir.

Verinin bu sebebe dayanarak işlenebilmesi ve kullanılabilmesi için ilgili kişinin alenileştirme amacı çerçevesinde kalınması gereklidir. Aksi halde veri işleme hukuka aykırı hal alacaktır. Örneğin şirket temsilcisinin cep telefonu numarasının şirket internet sitesinde paylaşılıp alenileştirilmesi durumunda; ilgili kişi yalnızca şirketle ilgili sorular için aranabilecektir. Söz konusu kişinin başka bir sebeple aranması veya verisinin işlenmesi durumunda alenileştirilme amacı aşılabacağından işleme hukuka aykırı olacaktır⁴²⁵. Benzer bir örnek olarak, arabasını satmak isteyen kişinin internet üzerinden verdiği ilanda paylaştığı iletişim bilgileri araç satışıyla ilgili işlenecekse bu bent kapsamında değerlendirilir. Ancak bu iletişim bilgilerinin başka amaçlarla işlenmesi durumunda (örneğin reklam amaçlı) veri işlemenin hukuka aykırı olacağı

⁴²⁴ **Kurum**, İşlenme Şartları, s. 11.

⁴²⁵ “İlgili kişi tarafından alenileştirilen kişisel verinin, alenileştirme amacı dışında işlenmesi (ilgili kişinin Sigorta Şirketi tarafından aranması)” konulu bir Kurul kararında da “İlgili kişinin kişisel verilerine kendisi tarafından daha önce alenileştirilen internet sitesinden ulaşılması halinde dahi Sigorta Şirketi tarafından ilgili kişinin bilgilerinin internet sitesinde bulunma ve alenileştirilme amacıyla kullanılmadığı anlaşıldığından, Sigorta Şirket’i tarafından gerçekleştirilen veri işleme faaliyetinin KVKK m.5/2/d çerçevesinde değerlendirilemeyeceğine karar verilmiştir.” **Kurul Kararı**, 07.11.2019 T., 2019/331 K. <https://www.kvkk.gov.tr/Icerik/6623/2019-331> (E.T.: 17.03.2020).

tartışmasıdır⁴²⁶. Yine bu kapsamda avukatın ofis sitesinde yer alan cep telefonu numarasına hukuki danışmanlık sebebiyle SMS atılabilir. Zira avukatın alenileştirme iradesi bu yöndedir. Ancak avukatın özel hayatına ilişkin bir soru yöneltmek amacıyla bu iletişim bilgileri kullanılamayacaktır.

Kurul tarafından verilen başka bir karara⁴²⁷ göre önemli olan husus kişinin alenileştirme niyetidir. Kişiye SMS yoluyla reklam gönderen bir şirket tarafından internet üzerinden kişinin iletişim bilgilerine ulaşıldığı iddia edilmiştir. Ancak kişinin internette iletişim bilgilerini paylaşma niyeti reklam gönderilme amacına yönelik değildir. Bu nedenle alenileştirme iradesine aykırı kullanımın hukuka aykırı olacağı aşikardır.

6. Veri İşlemenin Bir Hakkın Tesisi, Kullanılması veya Korunması İçin Zorunlu Olması

KVKK m. 5/2/e’de ise *“bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması”* hali düzenlenmiştir. Örneğin mülkiyet veya rehin gibi hakların kurulabilmesi için tapuya yapılan tescilde kişinin verileri bu bent kapsamında işlenebilir⁴²⁸. Yine çalışanı tarafından veri sorumlusuna açılan davada çalışana ait bazı verilerin kullanılması örnek olarak verilebilir⁴²⁹. Başka bir örnek ise, müvekkil tarafından vekalet verilen avukatın, davanın takibi için gerekli işlemleri yapabilmesi amacıyla müvekkilinin bilgilerini işlemesidir⁴³⁰.

⁴²⁶ **Kurum**, Doğru Bilinen Yanlışlar, s. 29.

⁴²⁷ **Kurul Kararı**, 27.01.2020 T., 2020/67 K. <https://kvkk.gov.tr/Icerik/6718/2020-67> (E.T.: 03.04.2020).

⁴²⁸ **Kurum**, İşlenme Şartları, s. 5.

⁴²⁹ KVKK gerekçe, m.5.

⁴³⁰ **Kurum**, Örnekler, s. 17.

7. Veri İşlemenin Veri Sorumlusunun Meşru Menfaatleri İçin Zorunlu Olması

Açık rıza olmaksızın kişisel verilerin işlenebileceği son hal ise KVKK m.5/2'nin son bendi olan f bendinde düzenlenen *“ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması”*dır.

Bu şarta dayanarak veri işlenmesi için veri sorumlusunun *“meşru menfaati (legitimate interests)”* olmalıdır. Buna ek olarak veri işleme, *“ilgili kişinin temel hak ve özgürlüklerine zarar verilmemelidir.”* Bu bende dayanılabilmesi için her iki koşulun da birlikte sağlanması gerekir. Veri sorumlusunun *“meşru menfaati”* ile ilgili kişinin *“temel hak ve özgürlükleri”* arasında bir *“dengeleme testi (balancing test)”* yapılmalıdır. Bu test sonucunda meşru menfaat daha ağır basarsa KVKK m.5/2/f'ye dayanan veri işleme, yasal zemine oturacaktır. Ancak denge temel hak ve özgürlükler lehine ise meşru menfaate dayanarak veri işleme yapılamaz⁴³¹.

Veri işlenmesi neticesinde veri sorumlusunun sağlayacağı fayda, meşru menfaati ifade eder. Bu fayda; meşru, belirli ve halihazırda var olan bir menfaate dayanmalıdır. Ayrıca meşru menfaat ciddi ve mühim olmalıdır. Veri işleme, veri sorumlusuna ya güncel olarak fayda sağlamalı ya da yakın bir zamanda fayda sağlayacak olmalıdır. Meşru menfaat ve amaç kavramları birbirleriyle karıştırılmamalıdır. Veri sorumlusunun meşru menfaati, işleme sonunda ulaşılabilecek çıkara yöneliktir. Ancak amaç, verinin işleme nedeniyle ilgilidir. Meşru menfaat ise daha geniş bir kavramdır⁴³².

Örneğin bir şirketi devralmak isteyen kişinin şirketin güncel durumunu veya çalışanlarına ait verileri incelemesi meşru menfaat kapsamında değerlendirilebilecektir.

⁴³¹ **Data Protection WP**, Legitimate Interests, s. 9.

⁴³² **Kurum**, İşlenme Şartları, s. 16.

Zira kiři bu inceleme sonucunda satın almaya ilişkin karar verecektir. Bu da kiřinin yakın gelecekte elde edeceęi faydayla ilişkindir⁴³³. Bu durumda meşru menfaatin varlığını tespit için denge testi yapılmalıdır. Öncelikle veri sorumlusunun menfaatinin olup olmadığına bakmak gerekir. Somut olayda veri sorumlusu elde ettięi bilgilerle yatırımına karar verecek, řirketi satın alma kararını gözden geçirecektir. Bu nedenle veri sorumlusunun menfaatinin olduęu sonucuna varılabilir. Sonrasında bakılması gereken söz konusu menfaatin meşru olup olmadığıdır. Bu menfaat, mevcut ya da yakın gelecekte doęacak bir menfaatse meşru olduęu kabul edilir. Somut olayda bu şartın da saęlandığı görülür. Son olarak veri sorumlusunun meşru menfaati ile ilgili kiřinin temel hak ve özgürlüğünün kıyası yapılmalıdır. Denge testi işte bu noktada önem kazanmaktadır. Meşru menfaatin tespitinden sonra veri sahibinin temel hak ve özgürlüklerinin neler olduęu değerlendirilmelidir. Kanımızca somut olayda yapılan denge testi sonucu, veri sorumlusunun menfaati daha güçlüdür. Bu nedenle somut olayımızda veri sorumlusu meşru menfaatine dayanarak kişisel veri işleyebilecektir.

Yine işverenin kaliteli çalışan işçilerine terfi vermek amacıyla onların verilerini işlemesi bu kapsamda değerlendirilebilir⁴³⁴. Zira terfi alan işçiler motive olacak, terfi

⁴³³ **Kurum**, Örnekler, s. 17.

⁴³⁴ “Örneęin bir řirket sahibi, çalışanlarının temel hak ve özgürlüklerine zarar vermemek kaydıyla, onların terfileri, maaş zamları yahut sosyal haklarının düzenlenmesinde ya da işletmenin yeniden yapılandırılması sürecinde görev ve rol dağıtımında esas alınmak üzere çalışanların kişisel verilerini işleyebilecektir. Burada, işletmenin yeniden yapılandırılması ya da ehliyetli ve liyakatli çalışanların terfi almaları, veri sorumlusu statüsündeki řirket sahibinin meşru menfaati cümlesindendir. Kişisel verilerin korunmasına ilişkin temel ilkelere uyulması ve veri sorumlusu ile ilgili kiřinin menfaat dengesinin gözetilmesi gerekmektedir.” KVKK gerekçe, m. 5.

almayanlar ise daha verimli çalışmak için gayret edecek, bütün bunlar da işveren açısından fayda sağlayacaktır.

Meşru menfaat şartı, diğer altı şartın olmadığı hallerde veya beklenmedik hallerde başvurulacak “*son çare (a last resort), en zayıf halka (the weakest link) ya da açık kapı (open door)*” olarak görülmemelidir⁴³⁵. “*Meşru menfaat*” kavramı geniş yorumlanmaya müsaittir. Bu kavram yorumlanırken hakkın özüne zarar verme tehlikesi bertaraf edilmelidir⁴³⁶. Bu kavram ne kadar geniş yorumlanırsa veri sorumluları her fırsatta veri işlemeye çalışacaktır. Zira geniş yorum durumunda veri sorumlularının her türlü veri işleme faaliyetini bu kapsamda değerlendirip yasallaştırma riski mevcuttur. Bu nedenle veri işlemede KVKK m/2/f’ye dayanılması durumunda özel olarak dikkat etmek gerekmektedir. Zira diğer bentler daha somut olarak ortaya konulabilmektedir.

Kamu tüzel kişileri tarafından “*meşru menfaat*” sebebine dayanılarak veri işlenmesine ise ihtiyatla yaklaşılmalıdır. Kamu tarafından bu sebebe dayanarak veri işlenemeyeceği öne sürülmektedir. Zira “*meşru menfaat*” soyut ve genel bir kavramdır. Kamu tarafından temel haklara yapılan müdahaleler için ise hukuki bir dayanak gerekmektedir. Meşru menfaat kavramının bu gerekliliğe ne kadar dayanak konusu olabileceği ise şüphelidir⁴³⁷.

Kurul “*veri sorumlusunun meşru menfaatleri için veri işlemenin zorunlu olması*” halinin somut olayda gerçekleşip gerçekleşmediğini tespit ederken belirlediği kriterlere⁴³⁸ göre karar vermektedir. Veri işlemenin KVKK m. 5/f kapsamında hukuka uygun işleme

⁴³⁵ **Data Protection WP**, Legitimate Interests, s. 3, s. 9.

⁴³⁶ **Küzeci**, s. 347.

⁴³⁷ **Çekin**, Kişisel Veri, s. 96.

⁴³⁸ **Kurul Kararı**, 25.03.2019 T., 2019/78 K. <https://www.kvkk.gov.tr/Icerik/5434/2019-78> (E.T.: 18.03.2020).

sayılabilmesi için kurulun belirlediği kriterler şunlardır.

“- Kişisel verinin işlenmesi sonucunda elde edilecek menfaat ile ilgili kişinin temel hak ve hürriyetlerinin yarışabilir düzeyde olması,

- Söz konusu menfaate ulaşılabilmesi bakımından kişisel veri işlenmesinin zorunluluk arz etmesi,

- Meşru menfaatin halihazırda mevcut, belirli ve açık olması,

- İlgili kişinin temel hak ve hürriyetleri ile yarışabilir nitelikte olan meşru menfaatin elde edilmesi halinde bir yarar sağlanacak olması ve kişisel veri işlenmeksizin başkaca bir yol ve yöntemle bu yararın ortaya çıkmasının mümkün olmaması,

- Meşru menfaat belirlenirken söz konusu yararın çok sayıda kişiyi etkilemesi, yalnızca kâr elde edilmesi ya da ekonomik yararın sağlanması amacına yönelik olmaması, iş süreçlerini ya da bir işleyişi kolaylaştırması (örneğin bir birim ya da az sayıda personel nezdinde değil, kurumsal olarak geneli etkileyecek şekilde) gibi şeffaf ve hesap verilebilir nitelikleri haiz kriterlerin esas alınması,

- Bu açıdan ilgili kişinin başta kişisel verilerinin korunması olmak üzere temel hak ve hürriyetlerinin zarar görmesini engellemek amacıyla öngörülebilir, açık ve yakın her türlü tehlikeden uzak tutulması,

- Kişisel verilerin bir veri kayıt sisteminde amaçla sınırlı olarak hukuka uygun işleyişinin temini ile zararı ve ihlalleri engellemek için her türlü teknik ve idari tedbirin alınması,

- Kişisel verilerin işlenmesinde genel ilkelere uygunluğun sağlanması,

- Bu kapsamda, kişinin temel hak ve hürriyetleri ile veri sorumlusunun meşru menfaatinin karşılaştırılarak denge testinin yapılması hususlarının değerlendirilmesi gerekmektedir.”

Bu kriterler önemlidir. Her somut olay bu kriterler kapsamında ayrı ayrı değerlendirilmeli, ayrıca denge testine sokularak veri işlemenin hukuka uygun olup

olmadığına karar verilmelidir.

C. Özel Nitelikteki (Hassas) Kişisel Verilerin İşlenme Şartları

Özel nitelikteki kişisel verilerin niteliğinden daha önce bahsedildiği için burada bu verilerin işlenme şartları üzerinde durulacaktır. Daha önce de belirttiğimiz gibi, KVKK m.5’de veri işleme şartları düzenlenmişken KVKK m.6’da şartlara ayrıca yer verilmesi özel nitelikteki verilere daha yüksek düzeyde koruma sağlamak amacıyla⁴³⁹. KVKK m. 6/1’de⁴⁴⁰ özel nitelikteki kişisel verilerin neler olduğu sınırlı sayma yoluyla belirtilmiştir. Şimdi de sayılan bu narin verilerin nasıl işlenebileceklerini inceleyelim.

KVKK m. 6’da belirtilen istisnalar dışında hassas kişisel verilerin işlenmesi yasaktır⁴⁴¹. Bu yasak kanunda “*Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır.*” şeklinde ifade edilmiştir⁴⁴². Ancak bu mutlak bir yasak değildir. Hassas verilere özgü bu koruma sınırlanabilir. Ancak bu sınırlamanın Anayasa m. 13 çerçevesinde yapılması gerekmektedir⁴⁴³. KVKK m.6’da da bu yasağın istisnaları sayılmıştır.

⁴³⁹ **Data Protection WP**, Legitimate Interests, s. 15.

⁴⁴⁰ KVKK m. 6/1 “*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.*”

⁴⁴¹ Bu yasak, “*hassas verilerde kesin işlem yasağı*” olarak ifade edilmektedir. **Başalp**, Kişisel Veri, s. 42; **Kaya**, s. 323; **Özdemir**, Elektronik Haberleşme, s. 127.

⁴⁴² KVKK m. 6/2.

⁴⁴³ **Kurum**, Özel Nitelikteki Kişisel Verilerin İşlenme Şartları, s. 2.

Açık rıza, hassas verilerde de hukuka uygunluk sebebi teşkil eder. Bu konu bakımından genel-özel nitelikli kişisel veriler arasında bir ayrım yoktur. Açık rıza ile ilgili yukarıda yaptığımız açıklamalar burada da geçerlidir. Tekrara düşmemek amacıyla atıf yapmakla yetiniyoruz.

Açık rıza dışındaki şartlarda KVKK hassas kişisel veriler arasında ikili bir ayrım yapmıştır. Bunlardan ilk kategori sağlık ve cinsel hayata ilişkin verilerdir. Diğer kategori ise sağlık ve cinsel hayat dışındaki tüm hassas kişisel verilerdir. Bu iki kategori de hassas verilerdir. Ayrıca her iki kategoriye giren veriler de açık rıza olması durumunda işlenebilecektir. Ancak açık rıza dışında işlenme şartları farklılaşmaktadır.

“Sağlık ve cinsel hayat dışındaki hassas veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. ” (KVKK m.6/3). Yani eğer herhangi bir kanun hükmü varsa verinin (sağlık ve cinsel hayat dışındaki) işlenebilmesi için açık rızaya ihtiyaç kalmayacaktır. Hükümdeki kanunlar ibaresinden sadece kişisel veri ile ilgili olanlar değil, her türlü kanun anlaşılmalıdır. Başka bir ifadeyle söz konusu verilerin işlenebilmesi için yalnız KVKK’da değil, diğer kanunlarda öngörülen haller de yeterli olacaktır. Sonuç olarak hassas verilerden, *“sağlık ve cinsel hayat dışındaki hassas veriler”*in işlenmesinin hukuka uygun olabilmesi için ya açık rıza ya da kanun hükmü olması gerekmektedir.

“Sağlık ve cinsel hayata ilişkin kişisel verilerin” de açık rıza ile hukuka uygun olarak işlenebileceğini belirttik. Açık rıza olmaması durumunda ise bu verilerin hukuka uygun işlenmiş sayılabilmesi için KVKK m. 6/3 hükmüne bakmak gerekir. Hükme göre *“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.”* Hükümde açık rıza olmaması durumunda sağlık ve cinsel

hayata ilişkin verilerin işlenebileceği hukuka uygunluk halleri düzenlenmiştir. Hüküm, sağlık ve cinsel hayata ilişkin kişisel verilerin işlenmesini hem amaç hem de kişi bakımından sınırlamıştır. Kişi bakımından söz konusu verileri işlemeye sadece “*sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar*” yetkilidir. Kişisel verilerin işleme amacı da hükümde sınırlı sayıda sayılan amaçlardan birinin kapsamı dahilinde olmalıdır. Amaç ve kişi unsurunun ikisinin birden sağlanmaması durumunda veri işleme hukuka aykırı hale gelecektir.

Sağlık ve cinsel hayata ilişkin verilerin hükümde belirtilen amaçlarla yetkili kurum ve kuruluşlar tarafından işlenebileceği öngörülmüştür. Bunun yanında söz konusu verilerin aynı amaçlarla “*sır saklama yükümlülüğü altında bulunan kişiler*” tarafından işlenebileceği öngörülmüştür. Söz konusu düzenlemenin irdelenmesi gerekmektedir. Öncelikle sır saklama yükümlülüğü altında bulunan kişiler mevzuat tarafından belirlenen kişiler olmalıdır. Sözleşmesel bir ilişkiyle böyle bir kişinin tespit edilmesi durumunda, KVKK açısından bu belirlemeye bir sonuç bağlanmayacaktır. Başka bir ifadeyle bu kişi KVKK m. 6/3 kapsamında hassas veri işleyemez.

İkinci bir sorun ise “*sır saklama yükümlülüğü altında bulunan bir kişi*” bulunmayan veri sorumlularında ortaya çıkmaktadır. Hükümün açık ifadesine göre bu nitelikte bir kişi yoksa sağlık-cinsel hayat verileri işlenemeyecektir. Örneğin veri sorumlusu işveren nezdinde bir işyeri hekimi varsa bir sıkıntı söz konusu olmayacaktır. İşyeri hekimi açık rıza olmasa dahi hükümde sayılan amaçlarla sağlık ve cinsel hayata ilişkin veri işleyebilecektir. Zira doktorlar “*sır saklama yükümlülüğü altında bulunan kişiler*”dendir. Ancak her işyerinde işyeri hekimi bulunmamaktadır. Bu nedenle de bu veri sorumluları KVKK m. 6/3 kapsamında veri işleyemeyecektir. Bu noktada veri sorumlusu işverenlerin açık rızaya başvurmadan başka bir seçeneği kalmamaktadır. Ancak işçi-işveren ilişkilerinde açık rızanın özgür iradeye dayanıp dayanmadığı hususu ayrı bir tartışma konusudur. Ayrıca bazı durumlarda veri sorumluları KVKK m. 5/2/a

gereği veri işleyebilmektedir. Örneğin veri sorumlusu işverenin İK m. 75 gereği özlük dosyası düzenlemesi gerekmektedir. Söz konusu dosyada da sağlık verileri yer alabilmektedir. İşyeri hekimi bulunmayan veri sorumlusu işverenlerin bir yandan İK gereği veri işlemesi gerekirken KVKK m. 6/3 buna engel olmaktadır. Fikrimce KVKK özel kanun olduğundan KVKK m. 6/3 düzenlemesi öncelenmelidir. Yani bahsettiğimiz örnekte, işyeri hekimi bulunmayan yerlerde veri sorumlusu açık rıza yoksa sağlık-cinsel hayat verisi işleyemez. Bu sonuç ise veri sorumlularını işçiden açık rıza alma yoluna itecektir. İşçinin açık rızasının ise bu şartlarda ne kadar özgür iradeye dayandığı şüphelidir. KVKK m. 6/3 kişisel verilerin korunması açısından sıkı bir hükümdür. Ancak uygulamada çıkabilecek sorunlar bakımından yumuşatılması gerekmektedir. Bu nedenle fikrimce KVKK'da bir değişiklik yapılarak sağlık-cinsel hayat verilerinin de tıpkı diğer hassas veriler gibi kanunlarda öngörülen hallerde açık rıza aranmadan işlenebilmesi sağlanmalıdır.

Kanunun gerekçesine göre *“Sağlık Bakanlığı ile her türlü sağlık kuruluşunun ve Sosyal Güvenlik Kurumunun bu bentte yazılı amaçlarla tuttukları veriler ve kayıtlar bu kapsamda değerlendirilecektir.”* Örneğin bir kişinin hastanede yapılan tetkikler sonucu kalp ameliyatı olması gerektiğinin tespit edilmesi ve kişinin ameliyat için başka bir hastaneyi tercih etmesi durumunda iki hastane arasında kişinin sağlık verilerini içeren tetkiklerinin paylaşılması bu kapsamda değerlendirilebilir.

Örneğin ülkede COVID-19 salgınının görülmesi durumunda, virüsün yayılma hızı göz önüne alındığında kamu sağlığı ciddi tehdit altında olduğundan, kamu sağlığının korunması ve virüsün yayılmasını engellemek için hükümde sayılan kişiler ve kuruluşlar açık rıza aranmaksızın kişinin COVID-19 virüsünü taşıdığına ilişkin bilgileri işleyebilirler. Örneğin söz konusu veriler açık rıza olmasa dahi işyeri hekimleri tarafından işlenebilecektir. Zira burada kamu yararı ön plana çıkmaktadır. Yine de kişinin rızası olmadan işlenen bu sağlık verileri için özel koruma önlemleri alınmalıdır.

Kurul bir kararında⁴⁴⁴ KVKK m.6 gereği veri işleme şartları bulunmadığından “bir gazete tarafından ilgili kişinin özel nitelikli kişisel verileri (babasının kanser olduğu bilgisi) hakkında haber yapılmasını hukuka aykırı olarak” nitelendirmiştir.

KVKK m.6/4 uyarınca “Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır.” KVKK burada yeterli önlemlerin ne olacağının saptanması konusunda Kurul’a atıf yapmıştır. Yine Kurul’un görev ve yetkilerinin sayıldığı KVKK 22. maddesinin 4 bendinde “özel nitelikli kişisel verilerin işlenmesini için aranan yeterli önlemleri belirlemek” Kurul’un görevleri arasında belirtilmiştir. Kurul da bu sebeple “Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler” ile ilgili kararını⁴⁴⁵ RG’de yayımlamıştır⁴⁴⁶. Bu kararda öncelikle hassas kişisel veri işleyen çalışanlarla ilgili alınacak tedbirlere yer verilmiştir. Sonrasında veri işlemenin elektronik ortamda yapılması durumunda alınacak önlemlerden söz edilmiştir. Veriler elektronik ortamda saklanacaksa bahsedilen veri güvenliği araçları; kriptografik yöntemler kullanılması, loglama, güvenlik testlerinin yapılması ve kimlik doğrulama sistemi olarak sayılabilir. Ayrıca verilerin saklandığı fiziksel ortamın da güvenliğinin sağlanması gerektiği ifade edilmiştir. Hassas verilerin aktarımında ise; kurumsal posta hesabı veya KEP kullanımı, CD-DVD ile aktarımda kriptografik şifreleme kullanımı gibi gerekliliklere yer

⁴⁴⁴ “Gazete tarafından Kanunun 6. maddesinde sayılan şartlardan birine dayanmaksızın ilgili kişinin özel nitelikli kişisel verilerinin, köşe yazısında paylaşılmasının hukuka aykırı olduğuna karar verilmiştir.” **Kurul Kararı**, 09.12.2019 T., 2019/372 K. <https://www.kvkk.gov.tr/Icerik/6663/2019-372> (E.T.: 17.03.2020).

⁴⁴⁵ **Kurul Kararı**, 31.01.2018 T., 2018/10 K. <https://www.kvkk.gov.tr/Icerik/4110/2018-10> (E.T.: 14.03.2020).

⁴⁴⁶ RG. 07.03.2018, S. 30353, s. 23-25.

verilmiştir. Kurul tarafından karar verilen bu yeterli önlemler, veri işlenmesinde alınacak asgari önlemler olarak görülmelidir. Başka bir ifadeyle, hassas veriler işlenirken Kurul kararındaki önlemlerin alınması zaten zorunluluktur. Ancak hassas verilerin narin yapısı düşünüldüğünde veri sorumluları daha sıkı koruma politikaları izleyerek daha koruyucu yapıda önlemler elbette alabilecektir.

IV. Kişisel Verilerin Silinmesi, Yok Edilmesi ve Anonim Hale Getirilmesi

Kişisel verilerin silinmesi yok edilmesi veya anonim hale getirilmesi KVKK m. 7’de düzenlenmiştir. KVKK m. 7/1 uyarınca *“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.”* Bu hüküm, veri sorumlusuna yükümlülük getirmektedir. Zira veri sorumlusu verilerin işlenmesini hukuka uygun olarak yapmış olsa bile verilerin işlenme nedenleri ortadan kalktığında veriyi artık elinde tutamaz. Böyle bir durumda kişisel verileri imha⁴⁴⁷ etmesi zorunludur. Bu zorunluluk veri sorumlusuna bu madde gereği yüklenmiştir. Veri sorumlusunun yükümlüğünün karşılığı olarak ilgili kişiye talep ve kontrol hakkı verilmiştir. Zira bu husus ilgili kişinin haklarının sayıldığı KVKK m. 11’de *“KVKK 7. Maddesinde öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme hakkı”* şeklinde ifade edilmiştir.

Veri işleme başlangıçta KVKK m. 4’deki genel ilkelere uygun olarak yapılsa da sonrasında bu ilkelere aykırı hale gelebilir. Bu aykırılık kişisel veri işlemenin artık

⁴⁴⁷ *“Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi” işlemlerinin hepsini bir arada ifade etmek için KVSİYAY m. 4’de “imha” sözcüğünü kullanılmıştır. Biz de bu üç işlemi ifade edeceğimiz yerlerde bu sözcüğü kullanacağız.*

hukuka aykırı olması sonucunu doğuracaktır. Bu hukuka aykırılığın engellenmesi için veri sorumlusu tarafından kişisel veriler imha edilmelidir. Veri işlemede *“ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme”* ilkesinden daha önce bahsettik. Bu ilke gereği veri işleme için gerekli sürenin geçmesi halinde veri sorumlusu KVKK m. 7 yükümlülüklerine riayet ederek verileri imha etmelidir.

Aynı şekilde KVKK m. 5 ve m. 6’daki veri işleme şartları ortadan kalktığında veri sorumlusunun işlediği verileri imha etmesi gerekecektir. Keza buna bağlı olarak kişinin açık rızasıyla işleme yapıldığı durumda, kişi rızasını geri alırsa veri sorumlusunun veri işlemeye son vermesi gerekmekte ve KVKK m. 7’deki işlemleri yapması gerekmektedir.

Örneğin sözleşme gereği veri işlendiyse sözleşmenin geçersiz olması durumunda da veri sorumlusu KVKK m. 7 yükümlülüklerini yerine getirmelidir. Yani sözleşme gereği işlediği kişisel verileri silmeli, yok etmeli veya anonim hale getirmelidir⁴⁴⁸.

KVKK m. 7/2’ ye göre *“Kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesine ilişkin diğer kanunlarda yer alan hükümler saklıdır.”* Örneğin 5352 sayılı Adli Sicil Kanunu (**“ASK”**)⁴⁴⁹ m. 9’da adli sicil bilgilerinin silineceği haller düzenlenmiştir. Keza yine ASK 12. maddesinde arşiv bilgilerinin silinmesi hüküm altına alınmıştır. Bu nedenle ASK’daki söz konusu hükümlerin dikkate alınması gerekmektedir.

KVKK m. 7/3 uyarınca *“Kişisel verilerin silinmesine, yok edilmesine veya anonim hâle getirilmesine ilişkin usul ve esaslar yönetmelikle düzenlenir.”* Bu hükmün yaptığı atıf çerçevesinde *“Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale*

⁴⁴⁸ **Kurum**, Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi, s. 1-3

⁴⁴⁹ RG. 01.06.2005, S. 25832.

*Getirilmesi Hakkında Yönetmelik*⁴⁵⁰ (**KVSYAY**)” yayımlanmıştır⁴⁵¹. KVKK genel olarak veri sorumlusunun yükümlülüğünü düzenledikten sonra bu yükümlülükle ilgili detayları KVSYAY düzenlemesine bırakmıştır. KVKK “anonim hale getirme”nin tanımını yapsa da “silinme ve yok edilme”nin tanımını yapmamıştır. Bu nedenle bu kavramların tanımında KVSYAY esas alınacaktır.

KVKK ve KVSYAY hükümleri esas alınarak, uygulamada veri sorumlularına kılavuzluk etmesi amacıyla Kurum tarafından rehber hazırlanmıştır⁴⁵². Söz konusu rehberde veri sorumlularına silme, yok etme ve anonim hale getirme yöntemleri gösterilmiştir.

VERBİS’e kayıt olacak veri sorumlularına KVSYAY m. 5 ile “*veri saklama ve imha politikası hazırlama yükümlülüğü*” getirilmiştir. Yönetmelik ve KVKK düzenlemeleri dikkate alınarak veri sorumluları tarafından söz konusu politika hazırlanmalıdır⁴⁵³. “*Kişisel veri saklama ve imha politikası*” KVSYAY m. 4/1/f’de “*Veri sorumlularının, kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi belirleme işlemi ile silme, yok etme ve anonim hale getirme işlemi için dayanak yaptıkları politika*”

⁴⁵⁰ Bundan böyle KVSYAY olarak anılacaktır.

⁴⁵¹ RG. 28.10.2017, S. 30224.

⁴⁵² **Kurum**, Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi, Ankara 2018.

<https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/bc1cb353-ef85-4e58-bb99-3bba31258508.pdf> (E.T.: 23.03.2020).

⁴⁵³ Kurum tarafından hazırlanmış olan “*Kişisel Verileri Koruma Kurumu Kişisel Veri Saklama ve İmha Politikası*” için bkz. **Kurum**, Kişisel Veri Saklama ve İmha Politikası, <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/a556b331-4910-4a77-9794-83cba2ba74e1.pdf> (E.T.: 02.04.2020).

olarak tanımlanmıştır. KVSİYAY m. 6’da bu politikanın içereceğı asgari bilgiler sayılmaktadır. Yani veri sorumluları m. 5’de getirilen “*veri saklama ve imha politikası hazırlama yükümlülüğü*”nü m. 6 çerçevesinde yerine getirmelidirler.

Kişisel verilerin silinmesi KVSİYAY m. 8’de tanımlanmıştır. Buna göre, “*Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.*” İlgili kullanıcı, KVKK m. 4/1/b’de tanımlanmıştır⁴⁵⁴.

Kişisel verilerin silinmesinde, veri sorumluları belli bir süreci takip etmelidir. Öncelikle veri sorumluları tarafından silinecek veri tespit edilmelidir. Sonrasında “*ilgili kullanıcı*” sıfatıyla verileri işleyen kişiler belirlenmelidir. Son olarak ilgili kullanıcıların verilere ulaşp müdahale etme yetkilerine son verilmelidir. Bu sürecin izlenmesi sonucunda kişisel veriler silinmiş olacaktır⁴⁵⁵.

Kişisel verilerin silinmesi, verinin tutulduğu ortama göre farklılık arz edecektir. Verinin elektronik ortamdan silinmesiyle kağıttan silinmesi aynı yöntemle olmayacaktır. Örneğın ilgili kişi tarafından kişisel verilerini içeren dosya veri sorumlusuna verilmiş olsun. Bu verilerin işlenmesini gerektiren sebep ortadan kalktığında imha edilmesi gerekecektir. Bu durumda veri sorumlusu, kişisel bilgileri içeren dosyadaki kağıtlara

⁴⁵⁴ İlgili kullanıcı KVSİYAY m. 4/1/b’de “*Verilerin teknik olarak depolanması, korunması ve yedeklenmesinden sorumlu olan kişi ya da birim hariç olmak üzere veri sorumlusu organizasyonu içerisinde veya veri sorumlusundan aldığı yetki ve talimat doğrultusunda kişisel verileri işleyen kişiler*” olarak tanımlanmıştır.

⁴⁵⁵ **Kurul**, İmha Rehberi, s. 6.

karartma işlemi uygulayarak silebilir⁴⁵⁶.

Kişisel verilerin yok edilmesi, KVSİYAY m.9’da tanımlanmıştır. Buna göre, “Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.”

Örneğin bir kuruluş tarafından hukuk fakültesi öğrencileri arasında kurgusal duruşma düzenleniyor olsun. Kuruluş, bu organizasyonun düzen ve tertibi için katılımcı öğrenciler arasından bazı bilgileri işleyecektir. İşlenen tüm bu bilgiler bir CD’de tutulmuş olsun. Bir öğrenci grubunun yarışmadan çekilmesi durumunda sadece onların bilgilerinin olduğu kısımlar CD’den silinecektir. Ancak yarışmanın iptal olması veya sona ermesi durumunda, gerekli muhafaza süresi de geçince CD’nin tamamen parçalanma gibi yollarla yok edilmesi gerekmektedir.

Kişisel verilerin anonim hale getirilmesi ise KVKK’nın tanımlar maddesi olan m.3’de “Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesi” olarak tanımlanmıştır. Kişisel verilerin anonim hale getirilmesi KVSİYAY m. 10’da tamamen aynı şekilde tanımlanmıştır. Ayrıca KVSİYAY m. 10/2 gereğince, “Kişisel verilerin anonim hale getirilmiş olması için; kişisel verilerin, veri sorumlusu, alıcı veya alıcı grupları tarafından geri döndürme ve verilerin başka verilerle eşleştirilmesi gibi kayıt ortamı ve ilgili faaliyet alanı açısından uygun tekniklerin kullanılması yoluyla dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemez hale getirilmesi gerekir.” Burada ifade edilmek istenen, hangi yol ve yöntem kullanılırsa kullanılsın o verinin kişiyle ilişkilendirilememesi gerekmektedir. Aksi halde kişisel verinin anonim

⁴⁵⁶ “Karartma; kişisel verilerin bütünüünün, kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek şekilde silinmesi, üstlerinin çizilmesi, boyanması ve yıldızlanması gibi işlemlerdir.” **Kurul**, İmha Rehberi, s. 3.

hale getirildiğinden söz edilemez.

Kişisel verilerin anonim hale getirildiğinin söylenilebilmesi için kişiyi ayırt edilebilir kılan “*doğrudan tanımlayıcıların*” ve “*dolaylı tanımlayıcıların*” etkisiz hale getirilmesi gerekmektedir. “*Doğrudan tanımlayıcılar*”, münferiden bir kişiyi tarif eden ve ayırt edilebilir kılan tanımlayıcılardır. “*Dolaylı tanımlayıcılar*” ise münferiden bir kişinin net bir şekilde ortaya konulmasına olanak tanımasa da başka tanımlayıcılarla birlikte kişiyi ayırt edilebilir kılan tanımlayıcılardır⁴⁵⁷. Veriden kişi tespit edilebiliyorsa veya başka verilerle beraber değerlendirildiğinde verilerin bir kişiye ait olduğu tespit edilebiliyorsa, verilerin anonimleştirildiğinden söz edilemez. Nitekim bu husus big data (büyük veri) kavramıyla birlikte değerlendirilmelidir. Verilerin miktarı arttıkça ilgili kişinin de tespiti o oranda kolaylaşmaktadır⁴⁵⁸.

Verinin anonimleştirilmesinden tam anlamıyla söz edebilmek için hiçbir türlü ilgili kişiye ulaşılamamalıdır. Böyle bir durumda bilgi, kişiyi “*belirli veya belirlenebilir kılma*” niteliğini kaybedeceğinden bu veri artık kişisel veri sayılamayacaktır. Bu nedenle de artık KVKK kapsamında değerlendirilemeyecektir⁴⁵⁹.

Verilerin anonimleştirilmesi amacıyla maskeleye⁴⁶⁰, bilgileri gizleme, çıkarma gibi bazı anonimleştirme teknikleri (“*anonymisation techniques*”) kullanılabilir⁴⁶¹.

⁴⁵⁷ **Kurum**, İmha Rehberi, s. 16.

⁴⁵⁸ **Çekin**, İrade Serbestisi, s. 635.

⁴⁵⁹ **Kuner**, s. 66; **Kurum**, 100 Soru, s. 47.

⁴⁶⁰ “*Maskeleye, kişisel verilerin belli alanlarının, kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek şekilde silinmesi, üstlerinin çizilmesi, boyanması ve yıldızlanması gibi işlemleri ifade eder.*” **Kurum**, İmha Rehberi, s. 3.

⁴⁶¹ Verileri anonim hale getirme yöntemleri hakkında detaylı bilgi için bkz. **Data Protection WP**, Opinion 05/2014 on Anonymisation Techniques,

Örneğin bir anket şirketince, kişilere, harcama alanlarının tespiti amacıyla aylık ortalama gelirleri sorulmuş olsun. Bunun sonucunda kişilerden ad, soyad, yaş, cinsiyet, aylık kazanç, harcama alanları gibi veriler toplanmış olsun. Söz konusu anketin, şirket internet sitesinde paylaşılması durumunda; ad, soyad gibi ilgili kişiyi belirli kılacak bilgiler maskeleye gibi yöntemlerle anonimleştirilebilir. Zira söz konusu olayda ad, soyadın anketten çıkarılması durumunda elde kalan diğer verilerle kişilerin tespitinin yapılması mümkün görünmemektedir. Ancak bu hususun her somut olayda ayrı ayrı kontrol edilmesi gerekmektedir. Bir veri; çok geniş bir çevrede anonimleştirilmiş sayılabilirken, dar bir çevrede kişiyi belirli kılacak niteliğe sahip olabilir. Anketin tüm Türkiye’de uygulanması durumunda ad, soyad dışında elde kalan verilerle veri sahibi kişi tespiti yapılamayabilir. Ancak bu anketin sadece belirli bir apartmanda yapılması ve paylaşılması halinde ad, soyad dışındaki verilerle dahi gerçek kişinin tespiti yapılabilir. Bu nedenle anonim hale getirme hususunda her somut olay kendi şartlarıyla değerlendirilmelidir.

Kurul’un “*öğretim görevlisi ve araştırma görevlisi kadrolarına yapılacak atamalarda adaylardan talep edilen kişisel veri niteliğindeki bilgilerin internet ortamında yayımlanması uygulaması hakkında*”ki kararında 3. kişilerin adayla ilgili tüm bilgileri görebilmesinde bir yarar görülmediği belirtilmiştir. Karara göre ilan edilen puanlardan kişinin tespit edilemeyeceği şekilde maskeleye yapılması gerekmektedir⁴⁶². Karara göre, “*İlgili kişiler ile sınav puanları arasındaki bağlantının, maskeleye*

<https://ec.europa.eu/justice/article-29/documentation/opinion->

[recommendation/files/2014/wp216_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf) (E.T.: 24.03.2020); **Kurum**, İmha Rehberi, s.16-37.

⁴⁶² **Kurul Kararı**, 26.12.2019 T., 2019/389 K.

<https://www.kvkk.gov.tr/Icerik/6668/2019-389> (E.T.: 24.03.2020).

*yöntemleriyle kaldırılmasının uygun olacağına, bu kapsamda adaylara ait ad, soyad, T.C. kimlik numarası gibi verilerin, kişiyi belirli ya da belirlenebilir kılabilme özelliğinin ortadan kaldırılabilmesi adına, anılan bilgilerin açık şekilde yazılması yerine, kişinin kendisinin anlayabileceği şekilde harflerin ya da rakamların A**** B****, 11*****11 şeklinde yıldızlanarak yukarıda sözü edilen yöntemlerle yayımlanabileceğine karar verilmiştir.”*

Anonim hale getirilme diğerlerinden kolayca ayırt edilebilir. Ancak kişisel verilerin silinmesi ve yok edilmesi karıştırılabilir. Bu ayrımı yapabilmek için her iki kavramın da tanımlarının kıyaslanması gerekmektedir. Kişisel verilere erişilme hususunda; silinmede ilgili kullanıcılar tarafından erişilemeyeceğinden söz edilmişken, yok edilmede hiç kimse tarafından erişilemeyeceğinden söz edilmiştir. Ayrıca kişisel verilerin yok edilmesi maddesinde (KVSİYAY m. 9), verilerin “geri getirilememesinden” söz edilmişken, kişisel verilerin silinmesi maddesinde (KVSİYAY m. 8) böyle bir ibare yer almamaktadır. Buradan çıkan sonuç; kişisel veriler yok edildikten sonra geri getirilemez. Ancak kişisel veriler silindikten sonra geri getirilebilir.

Ayrıca belirtmek gerekir ki, KVSİYAY m.8, 9 ve 10 hükümlerinin her birinde “*veri sorumlusunun, kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesi hususunda gereken her türlü teknik ve idari tedbiri alma yükümlülüğü*” düzenlenmiştir.

Son olarak belirtmek gerekir ki, KVSİYAY m.11 ve m. 12 de sırasıyla kişisel verilerin resen imha edilmesi ve ilgili kişinin talebiyle imha edilmesi süreleri düzenlenmiştir. Veri sorumlusunun bu sürelere uyması gerekmektedir.

Veri sorumlusu “*periyodik imha süreleri*” belirlemelidir. Verilerin imha edilmesi gerekiyorsa bu işlem, ilk periyodik imhada gerçekleştirilir. Ayrıca periyodik imha süresinin 6 ayı geçemeyeceği m. 11/2’de belirtilmiştir.

İmha talebi ilgili kişiden geliyorsa, kişisel verileri işleme şartlarının ortadan kalkıp kalkmadığına bakılır. Veri işleme şartları ortadan kalkmışsa veriler 30 gün içinde imha

edilmelidir. Ayrıca bu veriler 3. kişilere aktarılmışsa, bu kişiler, veri sorumlusu tarafından bilgilendirilir. İşleme şartlarının ortadan kalkmadığı durumda ise 30 gün içinde ilgili kişiye verilecek ret cevabı gerekçeli olmalıdır. Görüldüğü üzere, olumlu ya da olumsuz cevap verilmesi fark etmeksizin, ilgili kişiye 30 gün içinde dönüş yapılmalıdır.

V. Kişisel Verilerin Aktarılması

KVKK m. 3/1/e gereği kişisel verilerin işlenmesinin, verilerle ilgili her türlü işlemi kapsadığını daha önce ifade ettik. Bu nedenle kişisel verilerin aktarılması da kişisel verilerin işlenmesi işlemleri arasındadır. KVKK m. 8 kişisel verilerin aktarılması başlıklıdır. 9. maddede ise kişisel verilerin yurt dışına aktarılması ayrıca düzenlenmiştir. Kanun'un düzenleniş sistemi göz önüne alındığında KVKK m. 8'in kişisel verilerin yurt içinde aktarımını hükme bağladığı anlaşılmaktadır. Ayrı düzenleme sebebiyle yurt içinde veri aktarımıyla yurt dışına veri aktarımı şartları ve izlenmesi gereken süreç farklılaşmaktadır. Bu nedenle bu aktarımların birbirlerinden ayrı olarak değerlendirme konusu yapılması gerekmektedir. Sonuç olarak kişisel verilerin aktarımı, yurt içinde aktarılması ve yurt dışına aktarılması olarak ikiye ayrılarak incelenecektir.

A. Yurt İçinde Aktarılması

Kişisel verilerin yurt içinde aktarılma şartları, KVKK m. 5'de hüküm bulan kişisel verilerin işleme şartlarıyla aynıdır. Burada da açık rıza olması halinde kişisel verilerin aktarılabilceği hüküm altına alındıktan sonra, açık rıza olmaması durumunda veri aktarımı yapılabilmesi için gereken şartlar konusunda KVKK m. 5 ve KVKK m. 6'ya atıf yapılmıştır. Zaten kişisel verilerin aktarımı da kişisel verilerin işlenmesi faaliyeti sayıldığından, bu atıf makuldür.

KVKK m. 8/1 uyarınca “*Kişisel veriler, ilgili kişinin açık rızası olmaksızın aktarılamaz.*” Görüldüğü üzere açık rıza kişisel verilerin aktarılmasında da hukuka uygunluk sebebi olarak kabul edilmiştir. Eğer ilgili kişinin açık rızası varsa kişisel veriler 3. kişilere aktarılabilecektir.

Açık rıza olmaması durumunda ise kişisel veri aktarımının yapılabilmesi için KVKK 8/2’ye bakmak gerekir. Bu hükme göre “*Kişisel veriler; 5 inci maddenin ikinci fıkrasında veya yeterli önlemler alınmak kaydıyla, 6 ncı maddenin üçüncü fıkrasında, belirtilen şartlardan birinin bulunması hâlinde, ilgili kişinin açık rızası aranmaksızın aktarılabilir.*” Genel nitelikli (hassas olmayan) verilerin aktarımında KVKK m. 5/2’ye bakılacak ve o hallerden birinin olması halinde hukuka uygun olarak aktarım yapılabilecektir. Hassas (özel nitelikli) kişisel verilerin aktarımında ise “*yeterli önlemler alınmak kaydıyla*” KVKK m. 6/3’deki şartlara uyulması gerekecektir. Güzelce ifade etmek gerekirse, kişisel verilerin işleme şartları (KVKK m.5-6) ile kişisel verilerin yurt içinde aktarımı şartları (KVKK m.8) aynıdır.

Hangi hallerin KVKK kapsamında yurt içinde veri aktarımı sayılacağı hususunda uygulamada karışıklıklar olabilir. Zira KVKK m.8’e uyulması için bu kapsamda bir veri aktarımı söz konusu olmalıdır. Veri sorumlusu olan tüzel kişinin kendi içinde yaptığı aktarımlar (örneğin organlar arasında) KVKK kapsamında bir veri aktarımı kabul edilmeyecektir. Ancak aktarım bir 3. kişiye yani farklı bir tüzel kişiliğe olursa bu kapsamda veri aktarımı kabul edilecektir. Örneğin Türk Ticaret Kanunu (“**TTK**”) m. 195’de hüküm altına alınan “*şirketler topluluğu*”nda⁴⁶³ birden fazla şirket ve haliyle

⁴⁶³ TTK m. 195/4: “*Hâkim şirkete doğrudan veya dolaylı olarak bağlı bulunan şirketler, onunla birlikte şirketler topluluğunu oluşturur. Hâkim şirketler ana, bağlı şirketler yavru şirket konumundadır.*” Bu hükme göre şirketler topluluğundan bahsedebilmek için hakim şirketten başka bağlı şirkete ihtiyaç vardır. Yani şirketler topluluğundan bahsedebilmek

birden fazla tüzel kişilik vardır. Şirketler topluluğundaki şirketler arasında yapılan veri aktarımı KVKK m.8’de düzenlenen veri aktarımıdır. Zira burada farklı tüzel kişilikler arasında veri aktarımı yapılmaktadır⁴⁶⁴. Bu nedenle KVKK m. 8 şartlarına uyulması gerekmektedir. Şirketler topluluğunda veri işleme şirketlerden yalnızca biri tarafından yapılıyor olabilir. Söz konusu şirketler arasında veri aktarımı açık rıza halinde pek tabi yapılacaktır. Ancak açık rıza olmasa dahi şirketler topluluğundaki şirketler arasındaki veri işlemlerin KVKK m. 5/f “*meşru menfaat*” şartına dayandırılması değerlendirilmelidir⁴⁶⁵.

Bizim de katıldığımız görüşe göre, veri sorumlusu tarafından veri işleyene yapılan yurt içindeki aktarım KVKK m. 8 kapsamında değerlendirilmemelidir. Zira veri işleyen söz konusu ilişkide 3. bir kişi değil, ana aktörlerden biridir. Ayrıca veri işleyen veri sorumlusuyla arasındaki sözleşme gereği veri işlemektedir. Bu nedenle veri işleyene yapılan aktarım KVKK m. 8’de zikredilen şartlara tabi olmamalıdır⁴⁶⁶.

KVKK m. 8/3 gereğince “*Kişisel verilerin aktarılmasına ilişkin diğer kanunlarda yer alan hükümler saklıdır.*” Kişisel verilerin yurt dışına aktarımında da KVKK dışındaki kanun hükümlerinin saklı olduğu KVKK m. 9/6’da hüküm altına alınmıştır.

için en az 2 şirket bulunmalıdır. Alt sınır bu olmakla birlikte şirket sayısı açısından bir üst sınır bulunmamaktadır. **Şener, Oruç Hami**, Teorik ve Uygulamalı Ortaklıklar Hukuku Ders Kitabı, Gözden Geçirilmiş 4. Bası, Ankara 2019, s. 172. Adı üstünde hakim şirket hakimiyet kuran, bağlı şirket üstünde hakimiyet kurulan şirkettir. **Çelik, Aytekin**, Ticaret Hukuku, Güncellenmiş 8. Baskı, Ankara 2018, s. 140.

⁴⁶⁴ **Kurum**, Uygulama Rehberi, s. 89-90.

⁴⁶⁵ **Çekin**, Kişisel Veri, s. 100-101.

⁴⁶⁶ **Çekin**, Kişisel Veri, s. 107 vd.

B. Yurt Dışına Aktarılması

1. Genel Olarak

Günümüzde teknolojik gelişmelerle birlikte çok ciddi boyutlara ulaşan veri aktarımı miktarı, özellikle ekonomik sebeplerle sınırlar ötesi boyutta da gün geçtikçe artmaktadır. Kişisel verilerin korunmasının amacı, bu veri dolaşımını engellemek değildir. Amaç, ciddi boyutlara ulaşan bu veri dolaşımının kişilerin temel hak ve özgürlüklerine zarar vermeyecek şekilde yapılmasının sağlanmasıdır. Bu nedenle kişisel verilerin yurt dışına aktarımı, mutlak olarak yasaklanamaz⁴⁶⁷. Ancak bir ülke kişisel verilerin korunmasında ne kadar hassas olursa olsun, ne kadar kişisel verilerin işlenmesini ve aktarılmasını sıkı şartlara bağlarsa bağlasın, diğer ülkelerde veri koruma hassasiyeti gelişmemiş olabilir. Bir ülkenin mevzuatında kişisel verilerin korunması detaylarıyla düzenlenmişken diğer ülkede kişisel verilerin korunması için mevzuat yeterli olmayabilir. Tüm bu durumlarda kişilerin verilerinin bir ülkede korunurken başka ülkelerde korunmaması sonucu doğabilir. Bu sonuç da kişilerin temel hak ve özgürlüklerin ihlaline yol açacaktır. Bu nedenle kişisel verilerin yurt dışına aktarımında özel şartlar ve kurallar belirlemek gereklidir. Kanun koyucu da bu hususu gözeterek kişisel verilerin yurt dışına aktarımını ayrı bir madde de düzenlemeyi uygun görmüştür.

Açık rıza, kişisel verilerin yurt dışına aktarılmasında da temel hukuka uygunluk sebebidir. İlgili kişilerin açık rızası varsa kişisel veriler yurt dışına aktarılabilir. Bu husus KVKK m. 9/1’de “*Kişisel veriler, ilgili kişinin açık rızası olmaksızın yurt dışına aktarılamaz.*” şeklinde ifade edilmiştir. Görüldüğü üzere kişisel verilerin yurt içinde aktarımında olduğu gibi, verilerin aktarımı için açık rıza hukuka uygunluk sebebidir. Açık rızanın aranmadığı diğer durumlar ise 2. bentte hükme bağlanmıştır.

⁴⁶⁷ Küzeci, s. 357.

Açık rızanın aranmadığı durumlarda KVKK m. 9/2 ikili bir ayırım yapmıştır. Kişisel verilerin yurt dışına aktarımı kuralları veri aktarılabilecek ülkede “yeterli koruma”nın bulunup bulunmamasına göre farklı şekilde düzenlenmiştir.

2. Yeterli Korumanın Bulunması

Yeterli korumanın bulunduğu ülkeler, kişisel verilerin korunması konusunda bilinçli olarak değerlendirilen ve kişisel verilerin korunması hakkına saygılı olan ülkelerdir. Bu nedenle bu ülkelere veri aktarımında ek şartlar aranmamaktadır. Kurul bu ülkeleri güvenli ülkeler olarak kabul etmektedir.

KVKK m. 9/2 uyarınca “*Kişisel veriler, 5 inci maddenin ikinci fıkrası ile 6 ncı maddenin üçüncü fıkrasında belirtilen şartlardan birinin varlığı ve kişisel verinin aktarılabileceği yabancı ülkede yeterli korumanın bulunması kaydıyla ilgili kişinin açık rızası aranmaksızın yurt dışına aktarılabılır.*” Aynı kişisel verilerin yurt içinde aktarımında olduğu gibi burada da kişisel verilerin işleme şartlarının düzenlendiği KVKK m. 5 ve m. 6’ya atıf yapılmıştır. Yeterli korumanın bulunduğu yabancı ülkeye kişisel verilerin aktarılabilmesi için KVKK m. 5 ve KVKK m. 6’da düzenlenen veri işleme şartlarından birinin gerçekleşmesi yeterlidir. Başka bir ifadeyle, eğer atıf yapılan iki hükümdeki şartlardan herhangi biri varsa, kişisel veri, yeterli koruma bulunan ülkeye aktarılabilecek, açık rıza veya başka bir şart aranmayacaktır.

Yeterli korumanın bulunduğu ülkelerin tespitini KVKK Kurul’a bırakmıştır. KVKK m. 9/3’e göre “*Yeterli korumanın bulunduğu ülkeler Kurulca belirlenerek ilan edilir.*” Ancak halihazırda Kurul tarafından herhangi bir ilan yapılmamıştır. Başka bir ifadeyle, Kurul tarafından ilan edilmesi gereken güvenli ülkeler henüz ilan edilmemiştir. Bu nedenle Kurul tarafından herhangi bir ilan ya da duyuru yapılana kadar bütün ülkeler güvenli olmayan ülke olarak değerlendirilerek aktarım yapılmalıdır. Zira hangi ülkede

yeterli korumanın bulunup bulunmadığı tespit edilmemiştir. Mevcut durumun veri sorumlularını yurt dışına veri aktarımı için açık rıza aramaya iteceği aşıkardır.

Ayrıca Kurul yabancı ülkede yeterli koruma bulunup bulunmadığına, *“Türkiye’nin taraf olduğu uluslararası sözleşmeleri, kişisel veri talep eden ülke ile Türkiye arasında veri aktarımına ilişkin karşılıklılık durumunu, her somut kişisel veri aktarımına ilişkin olarak kişisel verinin niteliği ile işlenme amaç ve süresini, kişisel verinin aktarılacağı ülkenin konuyla ilgili mevzuatı ve uygulamasını, kişisel verinin aktarılacağı ülkede bulunan veri sorumlusu tarafından taahhüt edilen önlemleri, değerlendirmek ve ihtiyaç duyması hâlinde, ilgili kurum ve kuruluşların görüşünü de”* olarak karar verecektir⁴⁶⁸. Kurul kişisel verilerin yurt dışına aktarımında yeterli korumanın bulunduğu ülkelerin tespiti için KVKK m. 9/4’deki kriterleri genişleterek bir form yayımlamıştır⁴⁶⁹. Bu formda KVKK m. 9/4 hükmünde sayılan kriterlere ek olarak bazı kriterler daha eklenmiştir. Örneğin veri korumayla ilgili genel ilkeler, aktarım yapılacak ülkede bağımsız veri otoritesinin (Kurum gibi) bulunması, bu konuda uluslararası belgelere taraf olma gibi. Ayrıca *“ilgili ülke ile yürütülen ticaret hacmi”*ne formda yer verilmiştir. Bu hususa, güvenli ülke tespitinde bakılacak olması dikkat çekicidir.

3. Yeterli Korumanın Bulunmaması

Yeterli korumanın bulunmadığı ülkeler, kişisel verilerin korunması açısından yeterli bulunmayan ülkelerdir. Bir ülkede yeterli koruma bulunup bulunmadığına karar

⁴⁶⁸ KVKK m. 9/4.

⁴⁶⁹ **Kurul Kararı**, 02.05.2019 T., 2019/125 K. <https://www.kvkk.gov.tr/Icerik/5469/-Yeterli-korumanin-bulundugu-ulkelerin-tayininde-kullanilmak-uzere-olusturulan-form-hakkindaki-02-05-2019-tarihli-ve-2019-125-sayili-Kurul-Karari> (E.T.: 25.03.2020).

verecek olan makam Kuruldur. Yeterli koruma bulunmayan ve aktarım için ek koruma önlemleri getirilen ülkeler Kurul tarafından güvensiz bulunan ülkelerdir. Ancak bu değerlendirme (güvenli-güvensiz) şüphesiz salt kişisel veriler bakımından yapılan bir değerlendirmedir.

Daha önce de belirttiğimiz gibi, açık rızanın olması durumunda yeterli koruması olan ülke ayrımı yapmaya gerek yoktur. Zira veri aktarılabilecek ülke yeterli koruması olmayan bir ülke de olsa açık rıza varsa veri yurt dışına aktarılabilecektir. Açık rızanın olmadığı durumlarda ise yeterli korumanın bulunmadığı ülkelere veri aktarımı için ek şartlar aranmaktadır.

Veri aktarımı yapılacak ülke yeterli korumanın bulunmadığı ülkeyse öncelikle KVKK m. 9 gereği KVKK m. 5 ve m. 6'daki veri işleme şartlarından birinin bulunması gerekir. Bu gereklilik yeterli korumanın bulunduğu ülkeyle aynıdır. Ülkeler açısından yeterli-yetersiz korumanın olduğu ülke ayrımı ek şartlarda önem kazanacaktır. KVKK m. 9/2/b gereğince *“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.”* Yani kişisel verilerin yeterli korumanın bulunmadığı ülkeye (güvenli olmayan) aktarımı için gerekli ek şartlar:

- Veri sorumlusu tarafından yeterli korumanın olduğuna dair yazılı taahhütname verilmesi ve
- Kurul’un izninin olmasıdır.

Yurt dışına veri aktarımının hukuka uygun gerçekleşmesi için bu iki şartın da sağlanması gerekir. Kurul tarafından izin verilirken, tıpkı bir ülkede yeterli koruma bulunup bulunmadığına karar vermesinde olduğu gibi, KVKK m. 9/4'deki kriterler göz önüne alınarak karar verilir.

Açık rızaya dayanılarak yurt dışına veri aktarımı yapılıyorsa veri sorumlusu tarafından taahhütname verilmesi gerekmemektedir⁴⁷⁰.

Kurul tarafından “*yurt dışına veri aktarımında veri sorumlularınca hazırlanacak taahhütnamede yer alacak asgari unsurlar*” yayımlanmıştır⁴⁷¹. Kurul daha sonra yaptığı bir açıklamada bu taahhütnamelelerin “*çok uluslu şirket toplulukları*” bakımından yetersiz olabileceğine dikkat çekmiştir. Kurul bu durumu göz önünde bulundurarak bu şirketlerce yapılacak yurt dışı veri aktarımında geçerli olmak üzere “*Bağlayıcı Şirket Kuralları*” belirleyerek yayımlamıştır⁴⁷². Kurul son olarak “*yurt dışına kişisel veri aktarımında hazırlanacak taahhütnamelelerde dikkat edilmesi gereken hususlara ilişkin duyuru*” yayımlamıştır⁴⁷³. Taahhütnameleler hazırlanırken Kurul’un belirttiği hususlara riayet

⁴⁷⁰ **Kurum**, Doğru Bilinen Yanlışlar, s. 34.

⁴⁷¹ **Kurul**, 16.05.2018 T., <https://www.kvkk.gov.tr/Icerik/4236/Yurtdisina-Veri-Aktariminda-Veri-Sorumlularinca-Hazirlanacak-Taahhutnamede-Yer-Alacak-Asgari-Unsurlar> (E.T.: 25.03.2020).

⁴⁷² “*Bağlayıcı Şirket Kuralları, yeterli korumanın bulunmadığı ülkelerde faaliyet gösteren çok uluslu grup şirketleri için kişisel verilerin yurt dışına aktarımında kullanılan ve yeterli bir korumanın yazılı olarak taahhüt edilmesini sağlayan veri koruma kurallarıdır. Bu kapsama giren şirketlerin, ilgili formu doldurup gerekli talimatları izleyerek Kuruma, Bağlayıcı Şirket Kuralları başvurusu yapması gerekmektedir.*” **Kurul**, 10.04.2020 T. <https://www.kvkk.gov.tr/Icerik/6728/YURT-DISINA-KISISEL-VERI-AKTARIMINDA-BAGLAYICI-SIRKET-KURALLARI-HAKKINDA-DUYURU> (E.T.: 06.05.2020).

⁴⁷³ **Kurul**, 07.05.2020 T., <https://www.kvkk.gov.tr/Icerik/6741/YURT-DISINA-KISISEL-VERI-AKTARIMINDA-HAZIRLANACAK-TAAHHUTNAMELEDERDE->

edilmesi Kurul'un yurt dışına aktarım izni vermesi açısından önem arz etmektedir.

Yeterli koruma bulunan ülke-bulunmayan ülke ayrımından bağımsız olarak KVKK m. 9/5'e göre *"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."* Bu hüküm veri aktarılacak ülke de yeterli koruma bulursa da bulunmasa da uygulanır. Kişisel verilerin aktarılacağı ülkede yeterli koruma bulursa ve KVKK m.5-6 veri işleme şartları gerçekleşse bile *"ciddi anlamda menfaat ihlali"*⁴⁷⁴ nin olacağı durumlarda kişisel verilerin yurt dışına aktarımı için Kurul'un izni gerekmektedir.

§6. Tarafların Hak ve Yükümlülükleri

I. Veri Sorumlusunun Yükümlülükleri

A. Aydınlatma Yükümlülüğü

Veri sorumlusunun en önemli yükümlülüklerinden birisi aydınlatma yükümlülüğüdür. Bu yükümlülük gereğince veri sorumluları tarafından ilgili kişiler bilgilendirilmelidir. Aydınlatma yükümlülüğü, *"ilgili kişinin işlenen kişisel veri ile ilgili bilgilendirilme hakkı"*nın karşılığıdır. Bu yükümlülük ile ilgili kişinin kendi kişisel verileri üzerinde denetim yapabilme şansı doğar. İlgili kişinin verisi üzerinde yapacağı

DIKKAT-EDİLMESİ-GEREKEN-HUSUSLARA-İLİSKİN-DUYURU

(E.T.:

07.05.2020).

⁴⁷⁴ KVKK m. 9/5'deki *"Türkiye'nin veya ilgili kişinin menfaatinin ciddi bir şekilde zarar göreceği"* ifadesi muğlak bir ifade olduğundan eleştirilmektedir., **Küzeci**, s. 356-357.

bu denetim “*kişisel verilerin geleceğini belirleme hakkı*”nın bir gereğidir⁴⁷⁵. Aydınlatma yükümlülüğü yerine getirilmeden yapılacak bir veri işleme (her ne kadar veri işleme şartlarını taşısa da) hukuka aykırı olacaktır. Söz konusu yükümlülük KVKK m. 10’da hükme bağlanmıştır. Hükme göre “*Kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişi, ilgili kişilere; veri sorumlusunun ve varsa temsilcisinin kimliği, kişisel verilerin hangi amaçla işleneceği, işlenen kişisel verilerin kimlere ve hangi amaçla aktarılabilmesi, kişisel veri toplamanın yöntemi ve hukuki sebebi, 11. maddede sayılan diğer hakları, konusunda bilgi vermekle yükümlüdür.*” Veri sorumluları tarafından ilgili kişilere yapılacak bilgilendirme, en azından hükümde yer alan hususları içermelidir.

Veri sorumluları, bu yükümlülüklerini yerine getirirken ayrıca Kurum tarafından RG’de⁴⁷⁶ yayınlanan “*Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ*”e⁴⁷⁷ riayet etmelidirler.

Kişisel veriler, KVKK m. 5 veya m. 6’daki hangi veri işleme şartına bağlı olarak işlenirse işlensinler bu yükümlülüğe uyulmak zorunludur. İlgili kişinin açık rızasıyla veri işlendiği durumlarda da kişi bu yükümlülük gereği aydınlatılmalıdır. Kısacası nerede kişisel verilerin işlenmesi varsa orada aydınlatma yükümlülüğü vardır⁴⁷⁸.

AYT m. 5/f gereği “*Kişisel veri işleme faaliyetinin açık rıza şartına dayalı olarak gerçekleştirilmesi halinde, aydınlatma yükümlülüğü ve açık rızanın alınması işlemlerinin ayrı ayrı yerine getirilmesi gerekmektedir.*” Bu maddedeki “*ayrı ayrı*” ibaresine özellikle

⁴⁷⁵ **Kurum**, Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi, Yayın No: 24, Ankara 2019, s. 8.

⁴⁷⁶ RG. 10.03.2018, S. 30356.

⁴⁷⁷ Bundan böyle AYT olarak anılacaktır.

⁴⁷⁸ AYT, m. 5/1/a

dikkat çekilmesi gerekmektedir. Bu faaliyetlerin her birinin ayrı olarak yapılması veri işlenmesine onay verecek ilgili kişinin iki kez düşünmesini sağlayacaktır. Ayrıca veri sorumlusunun aynı anda hem bir yükümlülüğünü yerine getirmesi hem de işleme için rıza alması engellenmiş olacaktır.

Aydınlatma yükümlülüğünün gerçekleştirilmesi sırasında “*hukuki sebebin*” net bir şekilde ilgili kişiye açıklanması gereklidir. KVKK m. 10’da belirtilen “*hukuki sebep*”, verileri işlerken KVKK m. 5 ve m. 6 kapsamında hangi işleme sebebine dayanıldığıdır. Hangi işleme şartına dayanılarak veri işlendiğinin de aydınlatmada belirtilmesi gereklidir (AYT m. 1/h).

Aydınlatma yükümlülüğünde kişisel verilerin hangi işleme şartına dayanılarak işlendiği (KVKK m. 5 ve 6’da sayılan şartlar) tereddüde yer vermeyecek bir şekilde net olarak yer almalıdır. Özellikle aydınlatma metninde “*gibi amaçlar için işlenmektedir*” şeklinde belirsiz ifadeler yer almamalıdır⁴⁷⁹.

Aydınlatma yükümlüğü icra edilirken uyulması gereken herhangi bir şekil şartı bulunmamaktadır. Bu yükümlülük sözlü veya yazılı şekilde fiziksel ya da elektronik ortamda gerçekleştirilebilir. Ancak aydınlatma yükümlülüğünün gerçekleştirildiğini kanıtlayacak olan veri sorumlusudur. Bu sebeple tarafımızca aydınlatma yükümlülüğünün yazılı olarak yerine getirilmesi tavsiye edilmektedir. Ayrıca veri sorumlusu tarafından aydınlatma tek taraflı olarak yapılmalıdır. Bu konuda ilgili kişinin herhangi bir başvurusuna veya talebine gerek yoktur⁴⁸⁰.

⁴⁷⁹ **Kurul Kararı**, 02.05.2019 T., 2019/122 K. <https://kvkk.gov.tr/Icerik/5461/2019/122> (E.T.: 03.04.2020).

⁴⁸⁰ AYT, m. 5/1

Veri sorumluları tarafından “katmanlı aydınlatma” yapılarak da aydınlatma yükümlülüğü gerçekleştirilebilmektedir. Kurum’un yayınladığı rehberde göre⁴⁸¹, “Katmanlı aydınlatma; kişisel verilerin elde edilmesi sırasında ilgili kişiye, kişisel verilerin elde edildiği konusunda ön bilgilendirme yapılarak, ilgili kişinin KVKK 10. maddesine uygun aydınlatmaya yönlendirilmesini ifade eder.” Bu uygulamada aydınlatma metninden önce ön bir bilgi verilmekte, isteyen kişiler istemesi durumunda ön bilgilendirmede atıf yapılan asıl metne ulaşabilmektedir. Örneğin kamera kaydı yapılan bir iş yerinde bu yola başvurulabilir. Ancak yine de veri sorumlusunun kimliği ve ön bilgilendirme yapılmalıdır. “X. A.Ş olarak güvenliğinizin sağlanması için şirket binamız 7/24 kamera ile kayıt altına alınmakta ve izlenmektedir. Detaylı bilgi için şuraya bkz.” minvalindeki bir metin katmanlı aydınlatma metnine örnek olarak gösterilebilir⁴⁸². Bir kozmetik firmasının mobil uygulamasından alışveriş yaparken öncelikle “veri sorumlusunun kimliği ve ön aydınlatma bilgilerinin” kısaca belirtilip ardından “Detaylı aydınlatma metni için tıklayınız.” ibaresinin bulunması da örnek teşkil eder. Yine kurumun sitesinde VERBİS kaydına başlanmadan önce yer alan “Kurumumuzca hazırlanmış olan Veri Sorumluları Sicil Bilgi Sistemi Aydınlatma Metnine bu linke tıklayarak ulaşabilirsiniz.” ibaresi katmanlı aydınlatmaya örnek olarak gösterilebilir.

Kanaatimizce ilgili kullanıcıya uzun ve karmaşık aydınlatma metinleri sunmak yerine katmanlı aydınlatma yöntemi tercih edilmelidir. Zira uygulamada karmaşık ve uzun metinlerin ilgili kullanıcılar ve hatta biz hukukçular tarafından dahi okunmadığı gözlemlenmektedir. Ancak kısa ve öz bilgilere ilk metinde yer verilmesi yerinde olacaktır. Bu sayede ilgili kullanıcı en önemli ve net bilgilere sahip olacaktır. Eğer ilgili kişi, kişisel verilerin işlenmesiyle ilgili detayları incelemek istiyorsa ilk metnin atıf

⁴⁸¹ Kurum, Aydınlatma Yükümlülüğü, s. 8.

⁴⁸² Kurum, Aydınlatma Yükümlülüğü, s. 19.

yaptığı detaylı metinde bu isteğini gerçekleştirebilecektir.

Aydınlatma yükümlülüğü, ilgili kişinin anlayacağı bir dille yapılmalıdır. Teknik ve hukuki tabirlere yer verilmesinden kaçınılmalı, yer verilecekse bu ifadeler ilgili kişinin anlayacağı bir şekilde açıklanmalıdır. Zira aksi durum veri sorumlularının kanuni bir prosedürü aşma çabasından öteye gidemeyecektir.

Kişisel verilerin ileride farklı amaçlarla da işlenebileceği çağrıştıran ibareler kullanılmamalıdır. Örneğin “*Kişisel verilerinizi yeni hizmetler geliştirmek için kullanabiliriz.*” şeklinde genel ve belirsiz ifadeler yer verilmemelidir⁴⁸³. Ayrıca veri sorumlusunca VERBİS’e girilen bilgilerle ilgili kişiye verilen bilgiler arasında tutarsızlık olmamalı, bilgiler uyusmalıdır.

Kural olarak, işlenecek kişisel veriler ilgili kişilerden elde edilir. KVKK, aksi durumu düzenlememiştir. Ancak AYT m. 6’da “*Kişisel verilerin ilgili kişiden elde edilmemesi halinde aydınlatma yükümlülüğü*” düzenlenmiştir. Buna göre ilgili kişiden verilerin toplanmadığı, ilgili kişiye ulaşılamaması gibi haller söz konusu olabilir. Bu hallerde işlenen veriler doğrudan ilgili kişiden elde edilemiyorsa, “*kişisel verilerin elde edilmesinden itibaren makul bir süre içerisinde*” ilgili kişiyi aydınlatma yükümlülüğü gerçekleştirilmelidir.

Daha önce de ifade ettiğimiz gibi, KVKK m. 28/1’de düzenlenen hallerde zaten KVKK uygulama alanı bulmayacaktır. KVKK m. 28/2’deki hallerde ise KVKK’nın bazı hükümlerinin uygulanmayacağı hükme bağlanmıştır. Bu hükümler arasında aydınlatma yükümlülüğü (m. 10) maddesi de vardır. Sonuç olarak KVKK m. 28/2’ye giren hallerde KVKK m. 10 uygulanmayacaktır. Bu nedenle söz konusu hallerde veri sorumlusunun aydınlatma yapma zorunluluğu doğmayacaktır.

⁴⁸³ **Kurum**, Aydınlatma Yükümlülüğü, s. 14-15.

Aydınlatma yükümlülüğün yerine getirilmemesi, KVKK m. 18’de kabahat olarak nitelendirilmiş ve idari para cezası yaptırımına bağlanmıştır. Buna göre, “KVKK 10. maddesinde öngörülen aydınlatma yükümlülüğünü yerine getirmeyenler hakkında 5.000 Türk lirasından 100.000 Türk lirasına kadar idari para cezası verilir.”

B. Veri Güvenliğine İlişkin Yükümlülükler

1. Teknik ve İdari Tedbirleri Alma Yükümlülüğü

Kişisel verilerin tam olarak korunmasından bahsedebilmek için veri güvenliğinin sağlanması gerekmektedir. Bu güvenliği sağlamakla yükümlü olan veri sorumlusudur. Veri güvenliğinin sağlanması için sadece verilerin hukuka uygun işlenmesi yetmez. Veriler hukuka uygun işlendikten sonraki aşamada da yetkisi olmayan 3. kişilerin verilere erişimi engellenmelidir. Kötü niyetli 3. kişiler çeşitli sebeplerle verilere ulaşmak isteyebilir. Bu ulaşımı engellemekle mükellef olan veri sorumlusudur. Veri güvenliğinin sağlanması için veri sorumlusu teknik ve idari önlemler almalıdır. Bu önlemler alınırken Kurul tarafından hazırlanan rehber de göz önünde bulundurulmalıdır⁴⁸⁴. KVKK m. 12’de düzenlenen bu yükümlülüğe göre “Veri sorumlusu;

- (1) kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,
- (2) kişisel verilere hukuka aykırı olarak erişilmesini önlemek,
- (3) kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.”

Görüldüğü üzere veri sorumlusunun bu hüküm kapsamında üç adet yükümlülüğü bulunmaktadır. Bu yükümlülüklerin yerine getirilmesi için de gerekli veri güvenliğini

⁴⁸⁴ **Kurum**, Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler), Yayın No: 5, Ankara 2019.

sağlamak zorundadır.

Veri güvenliğine ilişkin önlemlerin alınmaması KVKK m. 18/1/b kapsamında kabahat teşkil eder. Bu hüküm gereği, “KVKK 12. maddesinde öngörülen veri güvenliğine ilişkin yükümlülükleri yerine getirmeyenler hakkında 15.000 Türk lirasından 1.000.000 Türk lirasına kadar idari para cezası verilir.” Görüldüğü gibi veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi idari para cezası yaptırımına bağlanmıştır. Uygulamada ne yazık ki veri güvenliği yükümlülüğünün tam anlamıyla yerine getirildiği söylenememektedir. Bu nedenle Kurul birçok kararında söz konusu yükümlülüğün yerine getirilmemesi sebebiyle veri sorumluları hakkında idari para cezasının uygulanmasına karar vermiştir. Kurul’un “bir sigorta acentesinin müşterilerine ait kişisel verileri herkese açık sosyal medya platformlarında müşterilerinden habersiz olarak ve reklam amacıyla paylaşması hakkında”ki kararında veri güvenliği yükümlülükleri yerine getirilmediğinden veri sorumlusu hakkında idari para cezasına hükmedilmiştir⁴⁸⁵. Yine bir başka Kurul kararına yansıyan somut olayda veri sorumlusu; bir müşterisine, başka bir müşteriye ait faturaları göndermiştir. Söz konusu olayda Kurul, veri sorumlusunun gereken teknik önlemleri almadığını belirterek para cezası yaptırımını uygulanmasına karar vermiştir⁴⁸⁶.

⁴⁸⁵ **Kurul Kararı**, 27.01.2020 T., 2020/58 K. <https://kvkk.gov.tr/Icerik/6716/2020-58> (E.T.: 02.04.2020). Başka bir Kurul kararında da bankada gerçekleşen veri ihlalinde, veri sorumlusunun teknik ve idari tedbirleri alma yükümlülüğüne riayet etmediği saptanmıştır. **Kurul Kararı**, 26.11.2019 T., 2019/352 K. <https://kvkk.gov.tr/Icerik/6656/2019-352> (E.T.: 02.04.2020).

⁴⁸⁶ **Kurul Kararı**, 07.11.2019 T., 2019/333 K. <https://www.kvkk.gov.tr/Icerik/6712/2019-333> (E.T.: 02.04.2020).

Veri güvenliğinde alınması gereken *idari tedbirler* kapsamında öncelikle risk ve tehditlerin saptanması gerekmektedir. Bunun yanı sıra çalışanlara veri güvenliği konusunda eğitimler verilmelidir. Çalışanlarda farkındalık yaratılması, sadece dışarıdan gelecek saldırılarla mücadele için değil aynı zamanda kişisel verilerin hukuka aykırı şekilde kullanılmaması için de önem arz etmektedir. Veri sorumluları, veri güvenliğiyle ilgili politikalar hazırlamalı ve bu politikalar çerçevesinde, sistematik bir şekilde, belirli periyotlarda kontrol ve denetimler yapılmalıdır. Kişisel verilerin minimal miktara indirilmesine gayret edilmelidir. Zira kişisel veri sayısı arttıkça güvenlik açısından risk ve tehditler de o oranda artacaktır. Bu nedenle artık gereksinim duyulmayan verilerin imha edilmesi gerekmektedir. Veri sorumluları, veri işleyenlerle birlikte müştereken sorumlu olduklarından; veri sorumluları, veri işleyen tarafından gerekli güvenlik önlemlerinin alındığını kontrol etmelidir. Zira veri işleyenin yeterli önlemleri almaması durumunda veri sorumlusu gereken her türlü önlemi alsa da müştereken sorumluluk gereği sorumluluğu devam edecektir⁴⁸⁷.

Veri güvenliğinde alınması gereken *teknik tedbirler* kapsamında siber güvenliğin sağlanmasına gayret edilmelidir⁴⁸⁸. Örneğin antivirüs programı yüklenmesi, SSL⁴⁸⁹ sertifikasıyla korumanın sağlanması gibi. Ayrıca kişisel veri hangi ortamda muhafaza

⁴⁸⁷ **Kurum**, Veri Güvenliği, s. 8-14.

⁴⁸⁸ Kurul kararına yansıyan bir olayda veri sorumlusunun sistemine siber saldırı gerçekleştirilmiş ve birtakım kişisel verilere erişilmiştir. Kurul yaptığı inceleme sonucu şirket nezdinde idari ve teknik yetersizlik olduğuna kanaat getirmiştir. **Kurul Kararı**, 27.08.2019 T., 2019/255 K. <https://kvkk.gov.tr/Icerik/5537/2019-255> (E.T.: 02.04.2020).

⁴⁸⁹ SSL (Secure Sockets Layer) (Güvenli Giriş Katmanı): “*Sunucu ile istemci arasında akan veri güvenliğini ve bütünlüğünü mümkün kılan sertifika*”dır. **Kurum**, Veri Güvenliği, s. 4.

ediliyorsa o ortam güvenli tutulmalıdır. Verilerin kağıt, CD gibi fiziksel ortamlarda tutulması durumunda bu ortama girişin sadece belli kişilerde bulunan kartla yapılması örnek olarak verilebilir. “*Bulut depolama hizmet sağlayıcıları*” ile verilerin saklanması konusunda sözleşme akdedilirse, bu sağlayıcının veri işleyen konumunda olacağından söz ettik. Bu şekilde verilerin bulutta depolanması veri sorumlusu açısından kolaylık sağlasa da bazen güvenlik riski teşkil edebilmektedir. Bu nedenle veri sorumlusu, anlaştığı bulut şirketinin yeterli önlemleri almasına dikkat etmelidir⁴⁹⁰.

Uygulamada sıklıkla karşılaşılan veri güvenliğini tehdit sebebi veri sızıntısıdır. Veri sızıntısı, 3. kişiler tarafından verilere erişilerek kişilere ait bilgilerin elde edilmesidir. 3. kişiler tarafından yapılan bu erişim genellikle kötü amaçlarla yapılmaktadır. Veri sorumlusu verilerin dışarı sızmasını önlemek için gerekli teknik önlemleri almalıdır. Buna veri sızıntısını önleme yazılımı olan DLP örnek olarak verilebilir⁴⁹¹. Veri sızıntısı özellikle veri sorumlusu bakımından ekonomik kayba yol açabilir. Bu nedenle veri sorumlusu sızıntıya karşı önlemleri öncelikle kendisi için almalıdır. Daha da önemlisi veri sızıntısı durumunda çok ciddi biçimde temel hak ihlalleri söz konusu olabilir. Söz konusu tehlikelerin en az düzeyde olumsuz sonuca yol açması amacıyla veri sorumluları öncelikle veri ihlalinin etkilenen ilgili kişilere bu ihlali bildirmelidir. Veri sorumluları zararların en alt düzeyde tutulması için ayrıca Kurul’a bildirimde bulunmalıdır⁴⁹². Veri sorumlusunun söz konusu bildirim yükümlülüğü aşağıda ayrıca incelenecektir. Kurul kararlarına yansıyan veri sızıntısının söz konusu olduğu birçok somut olayda veri

⁴⁹⁰ **Kurum**, Veri Güvenliği, s. 18-27.

⁴⁹¹ **Kurum**, Veri Güvenliği, s. 5.

⁴⁹² **Küzeci**, s. 358-359.

sorumluları gereken önlemleri almadıklarından yaptırımla karşılaşmışlardır⁴⁹³. Kurul'un Facebook hakkında verdiği kararda, sistem hatasından kaynaklı veri ihlali olduğu tespit edilmiştir. Bu hatadan kaynaklı binlerce kullanıcının verilerine yetkisiz erişim sağlanmıştır. Kurul bu nedenle veri güvenliği yükümlülüğünün yerine getirilmediğinden bahisle para cezasına karar vermiştir⁴⁹⁴.

Yine uygulamada sıklıkla karşılaşılan veri güvenliğini ihlal tehlikesi, müşterilerin sıraya girerek vs. toplu olarak bulunduğu ortamda (banko, gişe gibi) kişilerin birbirleriyle ilgili kişisel verileri öğrenmesidir. Örneğin kargo hizmetinin sunulduğu bir şubede bir müşterinin ad, soyad veya T.C. kimlik numarası bilgileri işlenirken başka bir müşterilerin bu bilgileri duyması veri güvenliğinin ihlal edilmesi anlamına gelecektir. Bu nedenle Kurul *“banko, gişe, masa gibi hizmet alanlarında kişisel verilerin korunmasına yönelik ilke kararı”*nı yayınlamıştır⁴⁹⁵. Karara göre, *“Bankacılık ve sağlık sektörleri başta olmak üzere birden fazla çalışan ile birlikte bitişik düzende hizmet veren posta ve kargo hizmetleri, turizm acenteleri, zincir mağazaların müşteri hizmetleri bölümleri, çeşitli abonelik işlemlerinin yapıldığı kuruluşlar ile belediye, vergi ve nüfus ile ilgili işlemler gibi hizmetlerin verildiği kamu ve özel sektör kurum ve kuruluşlarının, 6698 sayılı Kişisel Verilerin Korunması Kanununun 12 nci maddesi uyarınca kişisel verilerin korunması ile ilgili olarak; banko/gişe/ masa gibi bölümlerde yetkisi olmayan kişilerin yer almasını önleyecek ve aynı anda birbirlerine yakın konumda hizmet alanların birbirlerine ait*

⁴⁹³ **Kurul Kararı**, 27.08.2019 T., 2019/254 K. <https://kvkk.gov.tr/Icerik/5535/2019-254> (E.T.: 03.04.2020).

⁴⁹⁴ **Kurul Kararı**, 18.09.2019 T., 2019/269 K. <https://kvkk.gov.tr/Icerik/5534/2019-269> (E.T.: 03.04.2020).

⁴⁹⁵ **Kurul İlke Kararı**, 21.12.2017 T., 2017/62 K.

<https://www.kvkk.gov.tr/Icerik/4114/2017-62> (E.T.: 04.04.2020).

kişisel verileri duymasını, görmesini, öğrenmesini veya ele geçirmesini engelleyecek nitelikte gerekli teknik ve idari tedbirleri almasına karar verilmiştir.” Kurulun bu kararı sıklıkla karşılaşılan ihlallerle ilgili aldığı ilke kararına güzel bir örnektir. Buna göre söz konusu ortamlarda veri sorumlusunun gerekli idari ve teknik önlemleri alması gerekmektedir. Özellikle müşterilerinin birbirlerinin verilerini öğrenmesinin önüne geçilmelidir. Aksi halde veri sorumlusunun Kurul tarafından yaptırımla karşılaşacağı kuşkusuzdur.

Kişisel verilerin veri işleyen tarafından işlenmesi durumunda; yukarıdaki önlemlerin alınmasında veri işleyen ve veri sorumlusu müştereken sorumlu olacaklardır. Yani veri işleyenlerin de veri güvenliğine ilişkin önlemleri alma yükümlülükleri vardır. Bu müştereken sorumluluk hali KVKK m. 12/2’de hüküm altına alınmıştır. Buna göre *“Veri sorumlusu, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, yukarıda belirtilen tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumludur.”* Örneğin veri sorumlusu bir limited şirketin bazı belgelerinin, muhasebe şirketi tarafından işlenmesi konusunda anlaşma yapılmış olsun. Bu durumda her iki şirketin de güvenliği sağlamak amacıyla gerekli önlemleri alması gerekmektedir. Bu nedenle limited şirket, muhasebe şirketi ile beraber müştereken sorumludur⁴⁹⁶.

2. Denetim Yükümlülüğü

KVKK m. 12/3’de ise *“veri sorumlusunun denetim yükümlülüğü”* düzenlenmiştir. Veri sorumlusunun gerekli önlemlerin alınıp alınmadığını kontrol etmesi gerekmektedir. Bu hükme göre *“Veri sorumlusu, kendi kurum veya kuruluşunda, bu Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorundadır.”* Hükümden anlaşılacağı üzere veri sorumlusu bu kontrol ödevini kendisi

⁴⁹⁶ KVKK gerekçe, m. 12.

yapabileceği gibi başkasına da yaptırabilecektir.

3. Sır Saklama Yükümlülüğü

Veri sorumluları ve veri işleyenlerin ortak olan bir diğer yükümlülüğü “*sır saklama yükümlülüğüdür.*” Buna göre “*Veri sorumluları ile veri işleyen kişiler, öğrendikleri kişisel verileri bu Kanun hükümlerine aykırı olarak başkasına açıklayamaz ve işleme amacı dışında kullanamazlar. Bu yükümlülük görevden ayrılmalarından sonra da devam eder.*” Veri sorumlusu ile veri işleyen arasındaki veri işleme sözleşmesi sona erse dahi veri işleyen bu yükümlülüğü devam edecektir.

4. Kurul’a Bildirim Yükümlülüğü

Veri sorumlusunun veri güvenliğine ilişkin son yükümlülüğü KVKK m. 12/5’de düzenlenen “*Kurul’ a bildirim yükümlülüğü*”dür. Buna göre, “*İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.*” Bu yükümlülüğe göre veri ihlali durumunda “*en kısa sürede*” verisi ihlal edilen kişiye ve Kurul’a veri sorumlusu tarafından bildirim yapılmalıdır. Buradaki “en kısa süre” Kurul kararında 72 saat olarak belirlenmiştir⁴⁹⁷. GDPR 85. paragrafta da benzer şekilde veri

⁴⁹⁷ **Kurul Kararı**, 24.01.2019 T., 2019/10 K., <https://www.kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirimi> (E.T.: 12.05.2020). Kurul birçok kararında veri ihlali bildirimi en kısa sürede Kurul’a bildirilmediğinden bahisle veri sorumlularına para cezası vermektedir. **Kurul Kararı**, 16.05.2019 T., 2019/144 K. <https://kvkk.gov.tr/Icerik/5480/2019-144> (E.T.: 03.04.2020). Veri ihlali bildiriminin 72 saat içinde yapılması gerektiği ve bu

ihlali durumunda veri sorumlusunun ihlali fark eder etmez bildirmesi, bu bildirimin 72 saati geçmemesi gerektiği ifade edilmiştir. Eğer söz konusu bildirim 72 saati geçerse veri sorumlusu gecikmenin sebepleriyle birlikte Kurul’a bildirimde bulunmalıdır. Kişisel veri ihlali bildirimde Kurul’a bildirim sürelerinin kısa tutulması makul olandır. Zira veri ihlaline zamanında müdahale edilmediğinde, Kurul ve ilgili kişilere haber verilmediğinde hasarın boyutu büyüyebilecektir⁴⁹⁸.

Kurul, bu veri ihlali bildirimlerini, gerekli gördüğü hallerde internet sitesinde veya başka bir vasıta ile duyurabilir. Kurul, veri sorumluları tarafından yapılacak veri ihlali bildiriminin usul ve esasları hakkında kararını yayınlamıştır. Kararda ayrıca veri ihlali Kurul’a bildirilirken “*Kişisel Veri İhlal Bildirim Formu*”nun kullanılması gerektiği belirtilmektedir. Bu forma kararda ek olarak yer verilmiştir. Bu nedenle veri ihlali tespit eden veri sorumluları, bu detaylı formu doldurarak Kurul’a bildirimde bulunabilirler⁴⁹⁹. Karara göre bildirim yapılmasının amacı, veri ihlalini olabildiğince çabuk engellemek, hukuka aykırı neticelerin oluşmaması için önlemler almaktır. Kanımızca da bu bildirimlerin asıl amacı veri ihlalini engellemek ve bilgilerine hukuka aykırı ulaşılan kişilerin olumsuz anlamda etkilenmesini en aza indirmektir. Veri işleyenlerin işlediği verilere 3. kişiler tarafından hukuka aykırı erişim olması durumunda veri işleyenlerin veri sorumlularına gecikmeksizin bildirimde bulunması gerektiği de kararda ifade edilmiştir. Böyle bir durumda veri işleyen veri sorumlusuna, veri sorumlusu da Kurul’a bildirim

gerekliliğe uymayan veri sorumlusu hakkında para cezası verilmesi hakkındaki karar için bkz. **Kurul Kararı**, 26.11.2019 T., 2019/352 K. <https://kvkk.gov.tr/Icerik/6656/2019-352> (E.T.: 02.04.2020).

⁴⁹⁸ GDPR 85. paragraf.

⁴⁹⁹ **Kurul Kararı**, 24.01.2019 T., 2019/10 K. <https://www.kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirimi> (E.T.: 12.05.2020).

yapacaktır.

Veri sorumlularının bildirim yükümlülüğü Kurul'a yapılan bildirimle sınırlı değildir. Kişisel verilere 3. kişiler tarafından haksız erişim olduğunda bundan en çok etkilenecekler ilgili kişilerdir. Bu nedenle veri ihlalinin etkilenecek kişilere veri sorumlusu tarafından bildirimde bulunulması gerekmektedir. Veri sorumlusunca ilgili kişilere yapılacak olan bildirimde hangi hususların yer alması gerektiği ve ilgili kişilerin hangi konularda bilgilendirileceği Kurul kararı ile belirlenmiştir⁵⁰⁰. Söz konusu bildirim teknik terimler içermemeli, ilgili kişinin hangi verisine, hangi yolla hukuka aykırı erişildiği ve bu anlamda alınan önlemler net bir şekilde yer almalıdır. Nitekim daha önce de belirttiğimiz gibi, kötü niyetli 3. kişiler tarafından verilere erişildiği zaman Kurul'a ve ilgili kişiye yapılan bildirim yükümlülüğünün getirilme sebebi, veri ihlali gerçekleşikten sonraki süreci en az hasarla atlatmaktır.

C. Veri Sorumluları Sicili'ne Kayıt Yükümlülüğü

1. VERBİS

Veri Sorumluları Sicili, veri işleyen gerçek veya tüzel kişilerin veri işlemeye başlamadan önce kaydolmalarının zorunlu olduğu bir sicildir⁵⁰¹. Sicil KVKK m. 16'da düzenlenmiştir. KVKK m. 16/1'de "*Kurulun gözetiminde, Başkanlık tarafından kamuya açık olarak Veri Sorumluları Sicili tutulacağı*" hükme bağlanmıştır. Bu hükümde öngörüldüğü üzere Başkanlık tarafından Veri Sorumluları Sicil Bilgi Sistemi (VERBİS) kurulmuştur. Bu nedenle sicille ilgili işlemler VERBİS vasıtasıyla yapılır. Veri işleyen

⁵⁰⁰ **Kurul Kararı**, 18.09.2019 T., 2019/271K.

<https://www.kvkk.gov.tr/Icerik/5547/2019-271> (E.T.: 04.04.2020).

⁵⁰¹ KVKK m. 16/2.

bu kişilerin işledikleri verilerle ilgili bilgileri “*kategorik bazda*” VERBİS’e girmeleri gerekmektedir⁵⁰². İleride tekrar değineceğimiz gibi, burada çok karıştırılan bir hususa değinmek gerekir. Veri sorumlularınca sicile bilgi girişinde, kişisel verilerin kendisi girilmeyecek, hangi kategorilerde veri işlendiği girilecektir.

VERBİS’e kayıt, Kurum’un internet sitesi üzerinden olmaktadır⁵⁰³. Yine internet sitesinde “*sicil sorgulama*” kısmından veri sorumlularınca VERBİS’e girilmiş bilgilerin ilgili kişilerce görülebilmesi kamuya açıklığın bir göstergesidir. VERBİS’in kamuya açık tutulması isteyen herkesin sicili inceleyebilmesini sağlamaktadır. “*Kamuya açıklık ilkesi*”, kişisel verilerin korunması bakımından elzemdir. Zira isteyen kişinin veri sorumlularını göreceğ olması veri sorumluların hukuka uygun veri işleme konusunda itici güç olmaktadır⁵⁰⁴. Ayrıca kamuya açıklık, kişisel verilerin işlenmesinde “*şeffaflık*”⁵⁰⁵ ve “*hesap verebilirlik*”⁵⁰⁶ ilkelerinin gereğidir. Sicilin kamuya açık olarak tutulması ayrıca “*veri işleme faaliyetinin açık olması ilkesi*” ile ilişkilidir. İlgili kişi, VERBİS’e ulaşmasaydı veri işleme faaliyetinin açık olduğundan söz edilemezdi⁵⁰⁷.

⁵⁰² **Kurum**, Sorularla Veri Sorumluları Sicil Bilgi Sistemi (VERBİS), Yayın No: 22, Ankara 2019, s. 6.

⁵⁰³ VERBİS kaydı yapmak için bkz. <https://verbis.kvkk.gov.tr>

⁵⁰⁴ **Kurum**, Veri Sorumluları Sicili, s. 1.

⁵⁰⁵ Şeffaflık ilkesi gereğince kişi, kendisi ile ilgili işlenen kişisel verilere kolaylıkla ulaşabilmeli; ulaştığı bilgileri ise net bir şekilde anlayabilmelidir. GDPR, 39. paragraf.

⁵⁰⁶ GDPR m. 5/2 hesap verebilirlik (accountability) gereği veri sorumlusunun, kişisel veri işlerken temel ilkelere uyması yetmemekte, ayrıca veri sorumlusu, temel ilkelere uygun davrandığını gösterebilmelidir.

⁵⁰⁷ **Şimşek**, s. 100.

Sicile kayıt yükümlülüğüne riayet etmemek kabahat teşkil edecektir. Bu nedenle KVKK m. 18/1/ç hükmü uyarınca “*Veri Sorumluları Siciline kayıt ve bildirim yükümlülüğüne aykırı hareket edenler hakkında 20.000 TL’ den 1.000.000 TL’ ye kadar idari para cezası verilir.*” Ancak VERBİS’e yapılan bildirimler salt yaptırımdan kaçınmak maksatlı olmamalı, söz konusu yükümlülük kapsamında doğru ve güncel bilgilerin sicile bildirilmesi gerekmektedir. Bu yükümlülüğün getirilmesinin asıl amacı veri sorumluları tarafından veri işlenmesinin bir sicile bağlanarak düzen çerçevesinde işlenmenin sağlanmasıdır. Kurul da bir kararında⁵⁰⁸ salt yaptırımdan kaçınma amaçlı yapılan ve KVKK ve ikincil düzenlemelere aykırılık teşkil eden VERBİS kayıt bildirimlerinin yükümlülüğün yerine getirilmesi anlamına gelmeyeceğini ve KVKK’ya aykırı olacağını belirtmiştir. Kurul kararında, VERBİS’e kayıt yükümlülüğünün asıl amacının “*kişisel verilerin işlenmesinde şeffaflığın sağlanması, veri sorumlularının Kanuna uyumu konusunda özen göstermeleri, kişisel veri işlenmesinin disiplin altına alınması, kişisel verisini işlediği kişilere hesap verebilmesi, kişisel verilerin gelişigüzel işlenmesinin önüne geçilmesi ve bu konuda bir kültür ve farkındalık oluşmasının sağlanması*” olduğu ifade edilmiştir.

KVKK m. 16/5’e göre, “*Veri Sorumluları Siciline ilişkin usul ve esaslar yönetmelikle düzenlenir.*” Sicile ilişkin usul ve esasları belirlemek üzere “*Veri Sorumluları Sicili Hakkında Yönetmelik*⁵⁰⁹” RG’de⁵¹⁰ yayımlanmıştır.

⁵⁰⁸ **Kurul Kararı**, 27.12.2019 T., 2019/387 K.

<https://www.kvkk.gov.tr/Icerik/6631/Veri-Sorumlulari-Siciline-Kayit-Yukumlulugune-Iliskin-Kurulca-Belirlenen-Tarihler-Hakkinda-2019-387-Sayili-Kurul-Karar-Ozeti>
(E.T.: 25.03.2020).

⁵⁰⁹ Bundan böyle VSSY olarak anılacaktır.

⁵¹⁰ RG. 30.12.2017, S. 30286.

2. VERBİS'e Kayıt Yükümlülüğü ve İstisnaları

Kural olarak veri sorumlularının hepsinin VERBİS'e kaydolmaları zorunludur. Gerçek ve tüzel kişi olan veri sorumluları gibi kamu kurum ve kuruluşu olan veri sorumlularının da VERBİS'e kayıt olması gerekmektedir⁵¹¹. Ayrıca veri sorumlularının veri işlemeye başlamadan önce kayıt yükümlülüğünü yerine getirmiş olması gerekir. Ancak kayıt işlemi gerçekleştikten sonra veri işlenmeye başlanabilecektir.

Her kuralda olduğu gibi VERBİS'e kayıt zorunluluğu kuralının da istisnaları mevcuttur. Öncelikle belirtmek gerekir ki, KVKK tarafından m. 28/2'de sayılan haller söz konusu olduğunda m. 16 uygulanmayacağından sicile kayıt yükümlülüğü de söz konusu olmayacaktır. Söz konusu bu istisna KVKK'dan kaynaklanmaktadır.

VERBİS'e kayıt zorunluluğunun bir diğer istisnası ise hükmün (m. 16) devamında düzenlenmiştir. Bu istisnanın iskeleti ise Kurul tarafından alınan kararlarla oluşturulacaktır. Buna göre objektif kriterler göz önüne alınarak Kurul tarafından VERBİS'e kayıt zorunluluğuna istisna getirilebilecektir. Görüldüğü üzere objektif kriterleri gözeterek VERBİS'e kayıt zorunluluğuna istisna getirme yetkisi Kuruldadır. Kurul'un kayıt zorunluluğuna istisna getirirken gözeteceği objektif kriterler (istisna kriterleri) VSSY m. 16 da sayılmıştır⁵¹². Kurul tarafından alınan çeşitli kararlarda VERBİS'e kayıt zorunluluğundan istisna tutulan veri sorumluları belirlenmiştir. Buna göre Kurul tarafından alınan ve RG'de yayınlanan kararlarla “*herhangi bir veri kayıt*

⁵¹¹ **Kurum**, Sorularla VERBİS, s. 16.

⁵¹² “*Buna göre Kurul, şu kriterleri göz önünde bulundurarak kayıt yükümlülüğüne istisna getirebilir: kişisel verinin niteliği, kişisel verinin sayısı, kişisel verinin işleme amacı, kişisel verinin işlendiği faaliyet alanı, kişisel verinin üçüncü kişilere aktarılma durumu, kişisel veri işleme faaliyetinin kanunlardan kaynaklanması, kişisel verilerin muhafaza edilmesi süresi, veri konusu kişi grubu veya veri kategorileri.*”

sisteminin parçası olmak kaydıyla yalnızca otomatik olmayan yollarla kişisel veri işleyenler; 1512 sayılı Noterlik Kanunu uyarınca faaliyet gösteren noterler; 2820 sayılı Siyasi Partiler Kanununa göre kurulmuş siyasi partiler; Avukatlık Kanunu uyarınca faaliyet gösteren avukatlar; 3568 sayılı Serbest Muhasebeci Mali Müşavirlik ve Yeminli Mali Müşavirlik Kanunu uyarınca faaliyet gösteren Serbest Muhasebeci Mali Müşavirler ve Yeminli Mali Müşavirler⁵¹³”, “4458 sayılı Gümrük Kanunu uyarınca faaliyet gösteren gümrük müşavirleri ve yetkilendirilmiş gümrük müşavirleri⁵¹⁴”, “arabulucular⁵¹⁵”, “yıllık çalışan sayısı 50’den az ve yıllık mali bilanço toplamı 25 milyon TL’den az olan gerçek veya tüzel kişi veri sorumlularından ana faaliyet konusu özel nitelikli kişisel veri işleme olmayanlar⁵¹⁶” ve “yalnızca ilgili mevzuat ve amaçlarına uygun, faaliyet alanlarıyla sınırlı olmak üzere kişisel veri işleyen Türkiye’de yerleşik dernek, vakıf ve sendikalar⁵¹⁷” VERBİS’e kayıt yükümlülüğünden istisna tutulmuşlardır. Kararlarda sayılan veri sorumlularının VERBİS’e kaydolması gerekmemektedir. Ancak VERBİS’e kayıt yükümlülüğünden istisna tutulan veri sorumlularının KVKK kapsamındaki diğer

⁵¹³**Kurul Kararı**, 02.04.2018 T., 2018/32 K., <https://www.kvkk.gov.tr/Icerik/4233/2018-32> (E.T.: 27.03.2020).

⁵¹⁴**Kurul Kararı**, 28.06.2018 T., 2018/68 K., <https://www.kvkk.gov.tr/Icerik/5269/2018-68> (E.T.: 27.03.2020).

⁵¹⁵**Kurul Kararı**, 05.07.2018 T., 2018/75 K., <https://www.kvkk.gov.tr/Icerik/5270/2018-75> (E.T.: 27.03.2020).

⁵¹⁶**Kurul Kararı**, 19.07.2018 T., 2018/87 K., <https://www.kvkk.gov.tr/Icerik/5271/2018-87> (E.T.: 27.03.2020).

⁵¹⁷**Kurul Kararı**, 22.04.2020 T., 2020/315 K., <https://www.kvkk.gov.tr/Icerik/6740/2020-315> (E.T.: 18.05.2020). RG. 09.05.2020, S. 31122.

yükümlülükleri devam etmektedir⁵¹⁸. Kurul'un istisna getirme yetkisi yalnızca VERBİS'e kayıt ile sınırlıdır. Yoksa Kurul tarafından veri sorumlularının KVKK'dan doğan diğer yükümlülüklerine istisna getirilemez⁵¹⁹. Ayrıca kayıt yükümlülüğü olmayan bu veri sorumluları kendi istekleriyle VERBİS'e kaydolabilirler⁵²⁰.

3. VERBİS'e Kayıt Bildirimi

Kural olarak veri sorumlularının VERBİS'e kaydolmaları gerektiğinden bahsettik⁵²¹. Peki veri sorumluları VERBİS'e kaydolurken hangi bilgileri bildirecektir? Veri sorumlularının VERBİS'e kayıt bildiriminin bazı bilgileri içermesi gerekmektedir. Söz konusu kayıt bildiriminde yer alması gereken bilgiler KVKK m. 16/3'de sayılmıştır. Buna göre, *“Veri Sorumluları Siciline kayıt başvurusu aşağıdaki hususları içeren bir bildirimle yapılır:*

- a) Veri sorumlusu ve varsa temsilcisinin kimlik ve adres bilgileri.*
- b) Kişisel verilerin hangi amaçla işleneceği.*
- c) Veri konusu kişi grubu ve grupları ile bu kişilere ait veri kategorileri hakkındaki açıklamalar.*
- ç) Kişisel verilerin aktarılabilceği alıcı veya alıcı grupları.*
- d) Yabancı ülkelere aktarımı öngörülen kişisel veriler.*

⁵¹⁸ VSSY m. 5/1/e.

⁵¹⁹ Çekin, Kişisel Veri, s. 171.

⁵²⁰ Kurum, Sorularla VERBİS, s. 19.

⁵²¹ VERBİS'e kayıt işlemi, sistemin nasıl kullanılacağı, veri kategorileri ile ilgili detaylı bilgi için bkz., Kurum, VERBİS Kılavuzu.

<https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/a1fca030-7f7e-4e61-bd70-8da57160199b.PDF> (E.T.: 02.04.2020).

e) Kişisel veri güvenliğine ilişkin alınan tedbirler.

f) Kişisel verilerin işlendikleri amaç için gerekli olan azami süre.”

Sicile bildirilen söz konusu bilgilerin doğru ve güncel olmalarından veri sorumlusu sorumludur⁵²².

KVKK ilgili hükmünde de görüldüğü üzere VERBİS’e kayıta kişisel veri kategorileri yer alacaktır. Yani VERBİS’de doğrudan kişisel verilerin yer alması söz konusu değildir. VERBİS’de yer alacak olan bilgiler ilgili kişilere ait kişisel veriler olmayacak, veri sorumlusu tarafından sadece başlık halinde “*kategorik bazda*” kişisel veriler işlenecektir. Bu nedenle kamuya açık olan sicilde, kişisel verilerin ifşa edilmesi gibi bir durum yoktur⁵²³. Örneğin veri sorumlusu bir şirket tarafından ilgili kişilerin telefon numaralarının ve e-maillerinin işlenmesi durumunda; veri sorumlusu, VERBİS’e direkt olarak ilgili kişinin telefon numarasını ya da mail adresini girmeyecek, iletişim kategorisi başlığında iletişim verileri işlediğini belirtecektir.

Yabancı ülkede yerleşik olan veri sorumlularının *veri sorumlusu temsilcisi*⁵²⁴ ataması gerekmektedir. Veri sorumlusu temsilcisi, Türkiye’de yerleşik tüzel kişi ya da T.C. vatandaşı gerçek kişi olabilir. Veri sorumlusu temsilcisi VSSY m. 11’de belirtilen durumlarda veri sorumlusunu temsile yetkilidir.

VERBİS kaydı yapılırken veri sorumluları tarafından *irtibat kişisi* bildirilmelidir. İrtibat kişisi, veri sorumlusu ya da onun temsilcisi tarafından belirlenen Kurum ile irtibat

⁵²² VSSY m. 5/1/e.

⁵²³ **Kurum**, 100 soru, s. 71.

⁵²⁴ Veri sorumlusu temsilcisi, “*Türkiye’de yerleşik olmayan veri sorumlularını bu Yönetmelik m. 11/3’de belirtilen konularda asgari temsile yetkili Türkiye’de yerleşik tüzel kişi ya da Türkiye Cumhuriyeti vatandaşı gerçek kişi*” olarak tanımlanabilir. (VSSY 4/1/p).

kurulmasını sağlanması için belirlenen gerçek kişidir⁵²⁵. Bu gerçek kişinin Türkiye’de yaşayan bir T.C vatandaşı olması zorunludur. İrtibat kişisi, Kurum ile ilgili iş ve işlemleri yürütecektir. Veri sorumlusu, irtibat kişisi olarak kendisini de belirleyebilir⁵²⁶. Veri sorumlusu bir kişiden fazla irtibat kişisi belirleyemez. Benzer şekilde bir gerçek kişi birden fazla veri sorumlusunun irtibat kişisi olamaz⁵²⁷. Veri sorumlusu temsilcisi VSSY m. 11’de belirtilen durumlarda veri sorumlusunu temsile yetkiliyken, irtibat kişinin böyle bir temsil yetkisi bulunmamaktadır.

Veri sorumluları tarafından sicile bildirilen bilgilerde bir değişiklik olması durumunda bu husus derhal Kurum Başkanlığına bildirilmelidir⁵²⁸. Kanun’da derhal olarak ifade edilen bu süre VSSY m. 13’de 7 gün olarak düzenlenmiştir. Yani VERBİS’e daha önceden bildirilen bilgilerde bir değişiklik olması durumunda 7 gün içinde Kurum’a bildirim yapılmalıdır.

4. Kişisel Veri İşleme Envanteri Hazırlama Yükümlülüğü

VERBİS’e kaydolma yükümlülüğü olan veri sorumlularına VSSY m. 5/1/ç ile getirilen bir başka yükümlülük “*Kişisel Veri İşleme Envanteri*” hazırlama yükümlülüğüdür. Bu yükümlülüğün Kanun ile değil Yönetmelik ile getirilmesi ilginçtir. Kişisel veri işleme envanteri, veri sorumluları tarafından veri işlenmesinin başlangıcından sonuna kadar bütün süreçleri içeren, adeta işlenen kişisel veri ile ilgili her türlü bilgi ve detayın yer aldığı rapordur. VSSY m. 4/1/h’de kişisel veri işleme envanteri şu şekilde tanımlanmıştır: “*Veri sorumlularının iş süreçlerine bağlı olarak*

⁵²⁵ VSSY m. 4/1/ç.

⁵²⁶ **Kurum**, Sorularla VERBİS, s. 19.

⁵²⁷ **Kurum**, Sorularla VERBİS, s. 20.

⁵²⁸ KVKK m. 16/4.

gerçekleştirmekte oldukları kişisel veri işleme faaliyetlerini; kişisel veri işleme amaçları ve hukuki sebebi, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami muhafaza edilme süresini, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları envanterdir.”

Veri sorumlusuna böyle bir rapor düzenleme zorunluluğu yüklenmesindeki amaç; veri sorumlusunun veri işlerken KVKK’ya uyup uymadığı konusunda kendisini test etmesinin sağlanmasıdır⁵²⁹. Başka bir ifadeyle, veri sorumlusu, işlediği kişisel verilerle ilgili detaylı bir rapor hazırladığında eğer KVKK’ya aykırı bir veri işleme varsa bunu kendiliğinden görebilecek ve düzeltebilecektir. Her ne kadar Envanter hazırlama külfet olarak görülse de veri sorumlusunun yararınadır. Zira Envanter hazırlayan veri sorumlusu, bu yükümlülük sayesinde işlediği kişisel verilerle ilgili her detaya vakıf olacağından KVKK’ya aykırı bir husus varsa bunu düzeltebilecek ve yaptırımlardan kaçınabilecektir. Yine ilgili kişi tarafından başvuru yapılması durumunda detaylı bir şekilde Envanter hazırlayan veri sorumlusu kısa süre içerisinde rahatlıkla cevap verebilecektir. Bu nedenle tarafımızca tüm veri sorumlularına Kişisel Veri Envanteri hazırlaması önerilmektedir.

Hangi kişisel verilerin işlendiği, bu verilerin hangi kategoriye dahil oldukları, verilerin hangi işleme şartına dayandığı, verilerin hangi amaçla işlendiği, verilerin saklanması için öngörülen süre, verilerin 3. kişilere aktarılıp aktarılmayacağı ve bu kişilerin kimler olduğu, yurt dışına veri aktarımı yapılıp yapılmayacağı, alınan idari ve teknik önlemlerin ne olduğu gibi hususların Envanter’de yer alması gerekir.

⁵²⁹ **Kurum**, Kişisel Veri İşleme Envanteri Hazırlama Rehberi, Yayın No: 30, Ankara 2019, s. 10.

Envanter hazırlama yükümlülüğü olanlar VERBİS’e kayıt yükümlülüğü olanlardır. Bu nedenle VERBİS kaydı yükümlülüğü ve istisnaları konusunda yaptığımız açıklamalar burada da geçerlidir.

VERBİS’e bildirilecek bilgiler bu envantere uygun olarak hazırlanmalıdır. Kurul’un bir kararına⁵³⁰ göre, *“Veri sorumluları, VERBİS’e kayıt ve bildirim yükümlülüğünü yerine getirirken öncelikle kişisel veri işlenmekte olan tüm süreçleri içerecek şekilde kişisel veri işleme envanteri hazırlamalı ve VERBİS’e bildirim yapılırken gelişigüzel değil söz konusu envanter baz alınarak giriş yapılması gerekmektedir.”* Yani ilk önce envanter hazırlanmalı daha sonra hazırlanan bilgiler doğrultusunda VERBİS kaydı yapılmalıdır. VERBİS’deki bilgiler ile Envanter’de yer alan bilgiler arasında tutarsızlık söz konusu olmamalıdır. Söz konusu Envanter ne kadar düzgün, hukuka uygun, güncel ve güzel hazırlanırsa VERBİS’e bildirilen bilgiler de o oranda doğru ve hukuka uygun olacaktır. Envanter’in bu şekilde doğru, güncel ve hukuka uygun olarak hazırlanması çok önemlidir. Zira gerek aydınlatma yükümlülüğünde gerekse ilgili kişilerin başvuruları yanıtlanırken temel alınacak bilgiler Envanter’deki bilgilerdir.

VERBİS ve Envanter özellikle içerdiği bilgiler konusunda birbirlerine benzese de bazı noktalarda farklılaşmaktadır. Daha önce defalarca ifade ettiğimiz gibi, VERBİS’de kişisel verilerin kendisi değil başlık halinde işlenen verilerin hangi kategoride oldukları yer alacaktır. Ancak Envanter’de kişisel veriler sadece veri kategorisi şeklinde yer almayacak, çok daha detaylı bir şekilde o veri ile ilgili tüm işleme sürecine yer verilecektir. VERBİS, kamuya açıktır. Ancak Envanter kamuya açık olmayıp, veri

⁵³⁰ **Kurul Kararı**, 27.12.2019 T., 2019/387 K.

<https://www.kvkk.gov.tr/Icerik/6631/Veri-Sorumlulari-Siciline-Kayit-Yukumlulugune-Iliskin-Kurulca-Belirlenen-Tarihler-Hakkinda-2019-387-Sayili-Kurul-Karar-Ozeti>
(E.T.: 11.05.2020).

sorumlusunun nezdinde bulunmaktadır⁵³¹.

II. İlgili Kişinin Hakları

Kişisel verilerin korunmasını isteme hakkının Anayasa m. 20/3’de düzenlendiğinden bahsettik. Söz konusu hükümde *“kişisel verilerin korunmasını isteme hakkının, kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsayacağı”* ifade edilmiştir. Görüldüğü üzere ilgili kişinin sayılan hakları anayasal güvence altındadır. İlgili kişinin bu hakları KVKK m.11’de hüküm altına alınmıştır.

A. Öğrenme ve Bilgi Talep Etme Hakkı

Kişisel verilerin korunmasında ilgili kişinin en temel hakkı bilgi edinme hakkıdır⁵³². İlgili kişi kendisi hakkında işlenen kişisel verilerle ilgili her türlü bilgiye erişebilmeli ve bilgi edinebilmelidir. Bu hakkın önemli oluşu, çoğu zaman, bu hak olmadan ilgili kişinin diğer haklarını kullanamamasından kaynaklanmaktadır. İlgili kişi, kendisi hakkında işlenen kişisel verilerle ilgili bilgi sahibi olmaması durumunda nasıl kişisel verilerin düzeltilmesi, imhası hakkını veya aşağıda belirteceğimiz diğer haklarını kullanabilecektir? Misalen kişi, işlenen verisiyle ilgili her türlü bilgiye haiz olmalıdır ki, eğer yalnızca düzeltilmesini talep edebilsin. Diğer hakların kullanılabilmesi için ön koşul olan bilgi edinme hakkı, hakların en önemlisi ve vazgeçilmezidir. Bu nedenle kanun koyucu da KVKK m. 11’de bu hakka etkin bir biçimde yer vermiştir. KVKK m. 11/1/a-

⁵³¹ **Kurum**, Envanter, s. 18.

⁵³² **Kuner**, s. 63 vd.

b-c-ç düzenlemeleri uyarınca “Herkes, veri sorumlusuna başvurarak kendisiyle ilgili; kişisel veri işlenip işlenmediğini öğrenme, kişisel verileri işlenmişse buna ilişkin bilgi talep etme, kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme, yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme haklarına sahiptir.”

Hükümde de görüldüğü üzere, ilgili kişi, öncelikle hakkında kişisel veri işlenip işlenmediğini bilmelidir. Eğer hakkında veri işlenmişse bu verilerle ilgili her türlü bilgiyi isteyebilir. Ayrıca Anayasa’da da ifade edildiği gibi işlenme amacını ve bu amaca riayet edilerek mi verilerin kullanıldığını öğrenme hakkına sahiptir. Eğer veriler 3. kişilere aktarılıyorsa hangi verilerin hangi 3. kişilere aktarıldığını da bilme hakkı vardır. İlgili kişinin saydığımız bu haklarının karşısında veri sorumlusunun bu hakların gereği gibi yerine getirilmesi yükümlülüğü vardır. İlgili kişi, kişisel verisiyle ilgili bilgi talep ettiğinde veri sorumlusu tarafından bu talep hukuka uygun bir şekilde karşılanmalıdır. Veri sorumlusu tarafından yapılan karmaşık ve göstermelik bilgilendirmeler ilgili kişinin söz konusu haklarına ihanet etmesi anlamına gelecektir.

TMK uyarınca kişiliğin ölümle sona ereceğinden söz ettik. Kişisel verinin bir unsuru da bilginin gerçek kişiye ait olmasıdır. Bu nedenle ölümlerin bilgileri kişisel veri olarak sayılmayacaktır. Peki ölümlerin yakınları KVKK m. 11 kapsamında ölüyle ilgili bilgilere erişebilirler mi? İlgili kişinin haklarının sayıldığı KVKK m. 11’de kişinin “kendisiyle ilgili” veriler hakkında bilgi edinme hakkı olduğu belirtilmiştir. Bu nedenle ölenin yakınlarının KVKK m. 11 çerçevesinde bilgi edinme hakkı bulunmamaktadır. Kurul da bir kararında⁵³³ ölünün eşinin ölü ile ilgili bilgiler için veri sorumlusuna yaptığı başvuruyu KVKK m. 11 kapsamında değerlendirmemiştir. Sonuç olarak ölünün

⁵³³ **Kurul Kararı**, 18.09.2019 T., 2019/273 K. <https://kvkk.gov.tr/Icerik/6710/2019-273> (E.T.: 02.04.2020).

yakınlarının ölü ile ilgili bilgileri talep etme hakkı yoktur.

B. Kişisel Verilerin Düzeltilmesini, Silinmesini veya Yok Edilmesini İsteme Hakkı

İlgili kişinin bir diğer hakkı Anayasa’da da yer verilen “*kişisel verilerin düzeltilmesini, silinmesini veya yok edilmesini isteme hakkı*”dır. KVKK m.11’de bu hak iki bent halinde düzenlenmiştir. Kişisel verilerin düzeltilmesini isteme hakkı ile silinmesini ve yok edilmesini isteme hakkı ayrı bentlerde düzenlenmiştir.

KVKK m. 11/d uyarınca ilgili kişi, “*kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme hakkı*”na sahiptir. Kişisel verilerin doğru ve güncel olması ilkesi, kişisel verilerle ilgili temel ilkelerdendir. Bu ilkeye uyulmadığında, yani kişisel veriler doğru ve güncel olarak tutulmadığında, ilgili kişi bu hakkını kullanarak verilerin düzeltilmesini isteyebilir. Zira kişiyle ilgili yanlış ve eksik tutulan bilgiler kişinin zarara uğramasına yol açabilir. Örneğin çalışanlara çocuk sayısı kadar ek ödeme yapılan bir şirkette dört çocuğu olan bir çalışanın çocuk sayısının iki olarak işlenmesi halinde, çalışan ekonomik olarak hak kaybına uğrayacaktır. Çalışan bu durumda veri sorumlusu şirkete başvurarak yanlış işlenen kişisel verisinin düzeltilmesini talep edebilir. Çalışanın bu hakkı karşısında veri sorumlusu şirketin de yanlış olan kişisel veriyi düzeltme yükümlülüğü bulunmaktadır.

Yukarıda da belirttiğimiz gibi, kişinin, hakkında işlenen verilerin yanlış veya eksik olarak işlendiğini bilebilmesi için kişi, hakkında işlenen kişisel veriler hakkında bilgi sahibi olmalıdır. Ancak bu mutlaka bilgi edinme hakkının kullanılarak bilgi edinileceği anlamına gelmez. Başka bir ifadeyle, bilgi edinme hakkının kullanılması, burada bahsettiğimiz hakların kullanılabilmesi için ön şart değildir⁵³⁴. Kişi, veri

⁵³⁴ Şimşek, s. 92.

sorumlusuna karşı bilgi edinme hakkına başvurmadan da kendisi hakkında işlenen bilgilerin yanlış veya eksik olduğunu öğrenebilir. Sonuç olarak kişinin hakkında işlenen bilgileri öğrenme yolu önemli değildir. Kişi, verilerinin yanlış veya eksik işlendiğini nerden duyarsa duysun düzeltme hakkını kullanabilir. Yine kişi, KVKK m. 7 çerçevesinde işleme sebebinin ortadan kalktığı bir durumu öğrendiği zaman silinmesini veya yok edilmesini talep edebilecektir.

Kişinin düzeltme istemi herhangi bir şekil şartına bağlanmamıştır. İstemden düzeltme isteminin anlaşılması yeterlidir. Eksik veya yanlış verilerin düzeltilmesi istemine karşın veri sorumlusu söz konusu verileri düzeltmelidir. Aksi halde kişisel verilerin işlenmesi hukuka aykırı bir hal almış olacaktır. Nitekim söz konusu işleme faaliyeti *doğru ve güncel olma ilkesine* aykırı bir nitelik taşıyacaktır⁵³⁵.

KVKK m.11/e'ye göre ilgili kişi, *“7. maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme hakkı”*na sahiptir. Burada KVKK m. 7 hükmüne atıf yapılmıştır. KVKK 7. maddesi *“kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi”* maddesidir. Bu madde ilgili bölümde detaylı bir şekilde açıklandığından burada değinilmekle yetinilecektir.

KVKK m. 11/f gereğince ilgili kişi, kişisel verilerin düzeltilmesi, silinmesi veya yok edilmesini talep hakkı çerçevesinde yerine getirilen işlemlerin, verilerin aktarıldığı 3. kişilere bildirilmesini isteyebilir. Zira veri sorumlusu, başvuru üzerine yanlış olan kişisel veriyi düzeltse dahi veri aktarılan 3. kişi yanlış olan bu veriyi kullanabilir. Yine ilgili kişinin talebi doğrultusunda silinen bir kişisel verinin olması durumunda, bu durumu bilmeyen 3. kişi kişisel veriyi kullanmaya devam edebilir. Bu ihtimalleri öngören kanun koyucu da ilgili kişiye, 3. kişiye bildirilmesini talep hakkı tanımıştır.

⁵³⁵ Çekin, Kişisel Veri, s. 126-127.

C. İtiraz Etme Hakkı

İtiraz hakkı, KVKK m. 11/g’de hüküm altına alınmıştır. Buna göre ilgili kişinin, “işlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme hakkı” bulunmaktadır. İlgili kişiden toplanan verilerin özellikle otomatik sistemlerle incelenmesi sonucunda kişi ile ilgili olumsuz bir durum söz konusu olacaksa, ilgili kişi buna itiraz edebilir. Kişisel verilerin değerlendirilmesinde sadece otomatik sistemlerin kullanılması doğru olmayan sonuçlara ulaşılmasına yol açabilir. Bilgisayar sistemleri ne kadar gelişmiş olursa olsun bazı durumlarda insan tarafından değerlendirilme yapılması gerekebilir. Zira bu sistemlerin duygu ve düşünceleri yoktur.

Veri sorumluları otomatik sistemlere başvurmayı azaltarak olumsuz sonuçları azaltabilir. Bunun için de çalışanlara veya müşterilere menfaat sağlanacağı durumlarda nihai kararların makineden ziyade bir insan tarafından alınması yerinde olacaktır⁵³⁶.

İtiraz etme hakkının kullanılabilmesi için iki şartın bir arada gerçekleşmesi gerekmektedir. Bunlardan ilki, kişisel verilerin analizi özellikle otomatik sistemlerle yapılmalıdır. İkinci şart ise bu analiz sonucunda ilgili kişi hakkında olumsuz bir sonuç ortaya çıkmalıdır. Örneğin işçilerin yaptıkları işe göre ücret ödemesinin yapıldığı bir şirkette, işçilerin yaptıkları işler otomatik bir sistem tarafından değerlendirilip bir sonuca varılıyorsa işçi tarafından bu madde kapsamında değerlendirme sonucuna itiraz edilebilecektir⁵³⁷. Yine bir şirket tarafından yapılan personel alım mülakatında kişiye psikolojik bir test yapılması ve bu testin otomatik olarak değerlendirilmesi sonucunda

⁵³⁶ **Kuner**, s. 65.

⁵³⁷ 11. maddenin gerekçesindeki örneğe göre, “Bir çalışanın performansının, onun tarafından yapılan işlerin, otomatik bir sisteme işlenip analiz edilerek, analiz sonucuna göre değerlendirilmesine, çalışanın itiraz edebilmesi bu kapsamda değerlendirilecektir.”

mülakatın olumsuz sonuçlanması durumunda, kişi itiraz etme hakkına sahiptir⁵³⁸.

D. Zararın Giderilmesini Talep etme Hakkı

İlgili kişinin “zararın giderilmesini talep etme hakkı” KVKK m. 11/1/ğ’de hüküm altına alınmıştır. Buna göre ilgili kişi, “*kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme hakkı*”na sahiptir. Hükme göre bu hakkın söz konusu olabilmesi için, öncelikle kişisel verilerin işlenmesinin kanuna aykırı olarak gerçekleşmiş olması gerekir. Söz konusu kanuna aykırılık sonucu ilgili kişi bir zarara uğramalıdır. Bu zarar maddi ya da manevi bir zarar olabilir.

İlgili kişinin her bir hakkının karşısında veri sorumlusunun bir yükümlülüğü vardır. Bu nedenle ilgili kişinin bu hakkı karşısında veri sorumlusunun zararı giderme yükümlülüğü vardır⁵³⁹. Ancak ilgili kişinin zararın giderilmesi talebi veri sorumlusu tarafından karşılanmazsa, ilgili kişi, KVKK m. 14/1 gereği Kurul’a şikayet yoluna gidebileceği gibi KVKK m. 14/3 gereği genel hükümlere göre yargı yoluna başvurabilir.

E. Veri Sorumlusuna Başvuru Hakkı

İlgili kişilere kişisel verilerinin etkin bir şekilde korunmasının sağlanması amacıyla veri sorumlusuna başvuru hakkı ve Kurul’a şikayet hakkı verilmiştir. KVKK m. 14/2 uyarınca ilgili kişilerin öncelikle veri sorumlusuna başvuru yoluna gitmesi gerekmektedir. Bu yol tüketilmeden Kurul’a şikayet yoluna gidilemeyecektir. Veri

⁵³⁸ Başalp, s. 54.

⁵³⁹ Veri sorumlusu, kişisel verilerin kanuna aykırı işlenmesi sonucu ilgili kişinin uğradığı zararı tazmin etmelidir. GDPR, 146. paragraf.

sorumlusuna başvuru yapılmadan Kurul’a şikayet yoluna gidilemeyeceği için öncelikle veri sorumlusuna başvuru hakkını inceleyeceğiz.

Veri sorumlusuna başvuru hakkı KVKK m. 13’de hüküm altına alınmıştır. Buna göre, “İlgili kişi, KVKK’nın uygulanmasıyla ilgili taleplerini yazılı olarak veya Kurulun belirleyeceği diğer yöntemlerle veri sorumlusuna iletir.” Hükümde veri sorumlusuna başvuru yolu düzenlenmiştir. İlgili kişi tarafından yapılacak başvuru yazılı olabilir. Ayrıca hükümde yazılı başvuru dışında, Kurul’un belirleyeceği başka usullerle de başvurunun yapılabileceği ifade edilmiştir. Söz konusu usuller RG’de⁵⁴⁰ yayımlanan “Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ”de⁵⁴¹ yer almaktadır. VSBT m. 5’de yazılı başvuru dışındaki diğer usullere yer verilmiştir. Buna göre, “İlgili kişi, Kanunun 11 inci maddesinde belirtilen hakları kapsamında taleplerini, yazılı olarak veya kayıtlı elektronik posta (KEP) adresi, güvenli elektronik imza, mobil imza ya da ilgili kişi tarafından veri sorumlusuna daha önce bildirilen ve veri sorumlusunun sisteminde kayıtlı bulunan elektronik posta adresini kullanmak suretiyle veya başvuru amacına yönelik geliştirilmiş bir yazılım ya da uygulama vasıtasıyla veri sorumlusuna iletir.” İlgili kişi burada belirtilen usullerden herhangi birini kullanarak başvurusunu yapabilecektir.

Başvuruda bulunması gereken zorunlu bilgiler VSBT m. 5/2’de sayılmıştır. Başvurunun burada yazılan bilgileri içermesi gerekmektedir⁵⁴².

⁵⁴⁰ RG. 10.03.2018, S. 30356.

⁵⁴¹ Bundan böyle VSBT olarak anılacaktır.

⁵⁴² VSBT m. 5/2: “Başvuruda; ad, soyad ve başvuru yazılı ise imza, T.C. kimlik numarası (yabancılar için uyruğu, pasaport numarası veya varsa kimlik numarası), tebligata esas yerleşim yeri veya iş yeri adresi, varsa bildirime esas elektronik posta adresi, telefon ve faks numarası, talep konusu bulunması zorunludur.”

KVKK m. 13/2 uyarınca *“Veri sorumlusu başvuruda yer alan talepleri, talebin niteliğine göre en kısa sürede ve en geç otuz gün içinde ücretsiz olarak sonuçlandırır.”* İlgili kişi KVKK’dan doğan taleplerini başvuru yoluyla veri sorumlusuna bildirir. Veri sorumlusu bu talepleri olabildiğince çabuk bir sürede değerlendirmelidir. Ancak bu süre herhalde 30 günü aşamayacaktır. Yani veri sorumlusunun başvuruyu inceleyebileceği azami süre 30 gündür.

Bir diğer husus ise kural olarak başvurunun ücretsiz bir şekilde neticelendirilmesidir. Ancak KVKK m. 13/2 gereği *“İşlemin ayrıca bir maliyeti gerektirmesi hâlinde, Kurulca belirlenen tarifiedeki ücret alınabilir.”* Kurul tarafından belirlenen tarifeye VSBT ücret başlıklı 7. maddesinde yer verilmiştir. Buna göre *“İlgili kişinin başvurusuna yazılı olarak cevap verilecekse, on sayfaya kadar ücret alınmaz. On sayfanın üzerindeki her sayfa için 1 Türk Lirası işlem ücreti alınabilir. Başvuruya cevabın CD, flash bellek gibi bir kayıt ortamında verilmesi halinde veri sorumlusu tarafından talep edilebilecek ücret kayıt ortamının maliyetini geçemez.”* Özellikle ilgili kişi tarafından yapılan ısrarcı, aslı olmayan, ölçüsüz ve sırf veri sorumlusunu rahatsız etme maksatlı yapılan başvurulardan (söz konusu durum ispatlanmak şartıyla) makul bir ücret alınmalıdır⁵⁴³. Zira ilgili kişi tarafından temeli olmayan, aşırı ve sürekli tekrarlayan başvurular hakkın kötüye kullanılması teşkil edecektir.

Ayrıca KVKK m. 13/3 gereğince ilgili kişi tarafından başvuruda bulunulmasının sebebinin veri sorumlusunun hatası olması durumunda; ilgili kişiden başvuru sebebiyle herhangi bir ücret alındıysa, bu ücret geri verilmelidir.

Her zaman olduğu gibi ilgili kişinin veri sorumlusuna başvuru hakkı karşısında veri sorumlusunun yükümlülüğü bulunmaktadır. Veri sorumlusunun bu yükümlülüğü, *“ilgili kişi tarafından yapılan başvuruların cevaplanması”* yükümlülüğüdür. KVKK m.

⁵⁴³ GDPR, m. 12/5.

13/3 uyarınca “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.” İlgili kişinin başvurusunu alan veri sorumlusu bu başvuruyu cevaplandırmalıdır. Veri sorumlusu tarafından verilecek cevapta yer alması gereken hususlar VSBT m. 6/4’de sayılmıştır⁵⁴⁴. Veri sorumlusu ilgili kişinin taleplerini içeren başvuruyu aldıktan sonra iki şekilde davranabilir. Birincisi talebi kabul edebilir. Eğer talebi kabul ediyorsa talebin yerine getirilmesi için gereğini yapmalıdır. İkinci seçenek ise, veri sorumlusu tarafından talebin reddedilmesidir. Talebi reddeden veri sorumlusu, talebi neden reddettiğini de gerekçelendirmelidir. Veri sorumlusu tarafından verilecek cevap olumlu da olsa olumsuz da olsa ilgili kişiye bildirilmelidir⁵⁴⁵. Veri sorumlusu cevabını yazılı veya elektronik ortamda bildirebilir.

⁵⁴⁴ VSBT m. 6/4: “Cevap yazısının; veri sorumlusu veya temsilcisine ait bilgileri, başvuru sahibinin adı ve soyadını, T.C. kimlik numarasını (yabancılar için uyruğunu, pasaport numarasını veya varsa kimlik numarasını), tebligata esas yerleşim yeri veya iş yeri adresini, varsa bildirim esas elektronik posta adresini, telefon ve faks numarasını, talep konusunu, veri sorumlusunun başvuruya ilişkin açıklamalarını içermesi zorunludur.”

⁵⁴⁵ KVKK m. 13 gerekçesinde veri sorumlusu tarafından yapılacak bildirim açıklanmıştır. Buna göre “Veri sorumlusunun gerçek kişi veya özel hukuk tüzel kişisi olabileceği ve bunların 7201 sayılı Tebligat Kanununa tabi olmamaları dikkate alınarak, veri sorumlusunun cevabını ilgili kişiye bildirmesi hükme bağlanmaktadır. Bu bildirim, bir ispat sorunu olup gerektiğinde yargı mercilerince ele alınacaktır. 7201 sayılı Kanuna tabi kurum ve kuruluşların bu bildirimleri anılan Kanun hükümleri uyarınca resmi tebligat yoluyla yapacakları da açıktır.”

Veri sorumlu tarafından talebin kabul edilmesi durumunda gerekenin yapılması gerekir. Eğer cevap olumlu olmasına rağmen talep yerine getirilmezse, veri sorumlusunun talebi reddettiğini kabul etmek gerekmektedir. Zira bu kabul gereği cevap ret sayılacağından ilgili kişi, Kurul’a şikayet ederek yerine getirilmeyen talebi için hakkını aramaya devam edebilecektir⁵⁴⁶.

Veri sorumlusu, yapılan başvuruyu “*etkin, hukuka ve dürüstlük kuralına uygun*” bir şekilde neticelendirmelidir. Aynı zamanda veri sorumlusu başvuruların bu şekilde neticelendirilebilmesi için gerekli idari ve teknik tedbirleri almakla mükelleftir⁵⁴⁷.

F. Kurul’a Şikayet Hakkı

1. Kurul’a Şikayet

İlgili kişinin Kurul’a şikayet hakkını kullanabilmesi için öncelikle veri sorumlusuna başvuru hakkını kullanması gerekmektedir. Bu husus KVKK m. 14/2’de “*13. madde uyarınca başvuru yolu tüketilmeden şikayet yoluna başvurulamaz.*” şeklinde ifade edilmiştir. Bu nedenle veri sorumlusuna başvuru zorunlu bir yoldur. Ancak burada ifade etmek gerekir ki, bu zorunluluk Kurul’a şikayet yoluna gidecek ilgili kişiler için bir zorunluktur. Yoksa doğrudan yargı yoluna gidecek bir kişinin veri sorumlusuna başvuru zorunluluğu yoktur⁵⁴⁸. İlgili kişi veri sorumlusuna ya da Kurul’a herhangi bir talepte bulunmadan direkt olarak yargı yoluna gidebilmektedir. Kurul’a şikayet yolu ise ihtiyaridir. İlgili kişi, veri sorumlusuna başvuru sonucu ret cevabı almış ya da hiç cevap alamamış olabilir. Böyle bir durumda Kurul’a şikayet yoluna gidebileceği gibi yargı

⁵⁴⁶ **Kurum**, Uygulama Rehberi, s . 104.

⁵⁴⁷ VSBT m. 6/1.

⁵⁴⁸ **Kurum**, Uygulama Rehberi, s. 105.

yoluna da gidebilir⁵⁴⁹. Yani kiři veri sorumlusundan gelen cevaptan sonra ister hareketsiz kalır, ister yargı yoluna gider, istemesi durumunda Kurul’a řıkayet de edebilir.

İlgili kiřinin KVKK’nın uygulaması kapsamında bir talebi olduęunda öncelikle bunu veri sorumlusuna yöneltmesi gerekir. Zira veri sorumlusu tarafından talebin karřılanması halinde bir sorun kalmayacaęından Kurul’un devreye girmesine de gerek kalmayacaktır. Hedeflenen çözüm yolu bu olmakla birlikte çeřitli saiklerle veri sorumluları tarafından bu talepler her zaman karřılanmamaktadır. Böyle bir durumda ilgili kiřinin Kurul’a řıkayet hakkı bulunmaktadır.

Bu hakkın düzenlendięi KVKK m. 14/1’e göre, *“Bařvurunun reddedilmesi, verilen cevabın yetersiz bulunması veya süresinde bařvuruya cevap verilmemesi hâllerinde; ilgili kiři, veri sorumlusunun cevabını öğrendięi tarihten itibaren otuz ve her hâlde bařvuru tarihinden itibaren altmış gün içinde Kurula řikâyetle bulunabilir.”* Daha önce de belirttiğimiz gibi, veri sorumlusu bařvuruyu kabul edebilir, reddedebilir veya cevapsız bırakabilir. Veri sorumlusunun bařvuruyu kabul etmesi durumunda zaten gereęini yapması zorunlu olduęundan bir problem olmayacaktır. Ancak veri sorumlusunun bařvuruyu reddetmesi veya cevapsız bırakması durumlarında Kurul’a yapılacak řıkayet süresinin ne zaman başlayacaęı ve kaç gün olacaęının incelenmesi gereklidir. Veri sorumlusunun bařvuruyu reddetmesi veya verdięi cevabın yeterli bulunmaması halinde, ilgili kiři Kurul’a řıkayet yoluna gidebilir. Bu halde ilgili kiři açısından 30 günlük süre cevabı öğrendięi tarihten itibaren işleyecektir. Yani ilk ihtimal olarak, veri sorumlusu, bařvuruya 30 gün içinde bir cevap verirse, cevap tarihinden itibaren 30 gün içinde Kurul’a řıkayet yoluna gidilebilecektir. Yani böyle bir durumda Kurul’a řıkayet için veri sorumlusuna bařvurudan itibaren 60 günlük süre bulunmamaktadır.

⁵⁴⁹ KVKK gerekçe, m. 14.

İkinci hal ise veri sorumlusunun başvuruya cevap vermemesi, susması halidir. Bu halde ilgili kişi, başvuru tarihinden itibaren 60 gün içinde Kurul'a şikayet yoluna gidebilecektir.

Üçüncü bir ihtimal daha vardır. Veri sorumlusunun başvuruya 30 gün içinde cevap vermesi gerektiğinden söz ettik. Peki veri sorumlusu cevap süresi olan 30 gün geçtikten sonra cevap verirse Kurul'a şikayet süresi ne zaman başlayacaktır ve kaç gün olacaktır? Veri sorumlusunun cevap süresi olan 30 gün geçtikten sonra verdiği cevap, Kurul'a şikayet süresinin hesaplanmasında, hiç cevap vermemesi durumu olan 2. hal gibi değerlendirilecektir. Yani başvurudan 30 gün geçtikten sonra veri sorumlusunca verilen cevap, sürelerin hesaplanmasında dikkate alınmayacaktır. Sonuç olarak, ilgili kişi tarafından başvuru yapıldıktan sonra veri sorumlusu tarafından 30 günlük cevap süresinin geçmesinden sonra bir cevap gelmesi halinde, ilgili kişi başvuru tarihinden itibaren 60 gün içinde Kurul'a şikayet yoluna gidebilecektir⁵⁵⁰. Zira kanunda her halde 60 gün içinde Kurul'a şikayette bulunulacağı hükme bağlanmıştır.

Yukarıdaki 3 ihtimali örnek üzerinden inceleyelim. İlgili kişi tarafından veri sorumlusuna yapılan başvuru tarihi her üç ihtimal için de 16.01.2020 olsun.

İlk ihtimalde, veri sorumlusu tarafından 27.01.2020 tarihinde olumsuz cevap verilmiş olsun ya da verilen cevap yetersiz olsun. Cevap olumsuz da olsa yetersiz de olsa sonuçta bir cevap verilmiştir. Ayrıca görüldüğü üzere verilen cevap veri sorumlusunca cevap verilmesi gereken 30 günlük süre içerisinde verilmiştir. Yani 30 günlük cevap süresi geçmeden veri sorumlusu cevap vermiştir. Böyle bir durumda ilgili kişi tarafından veri sorumlusunun cevap tarihi olan 27.01.2020 tarihinden itibaren 30 gün içinde Kurul'a şikayet yoluna gidilebilecektir.

⁵⁵⁰ **Kurul Kararı**, 24.01.2019 T., 2019/9 K.

İkinci ihtimalde, veri sorumlusu tarafından hiçbir cevap verilmemiş olsun. Bu durumda veri sorumlusu susmaktadır. Veri sorumlusunun bu halde olumlu ya da olumsuz bir hareketi olmasa da ilgili kişinin Kurul’a şikayet hakkının engellenmemesi için veri sorumlusunun susmasına bir sonuç bağlamamız gerekmektedir. Söz konusu durumda ilgili kişi, veri sorumlusuna başvuru tarihi olan 16.01.2020 tarihinden itibaren 60 gün içerisinde Kurul’a şikayet yolunu izleyebilecektir.

Üçüncü ihtimalde, veri sorumlusu 28.02.2020 tarihinde başvuruya cevap vermiş olsun. Görüldüğü üzere veri sorumlusu, başvurudan sonra cevap vermesi gereken süre olan 30 günlük sürede değil, bu süre geçtikten sonra cevap vermiştir. Bu halde şikayet süresi 28.02.2020 tarihinde başlamayacaktır. Sonuç olarak, söz konusu durumda ilgili kişi tarafından veri sorumlusuna başvuru tarihi olan 16.01.2020 tarihinden itibaren 60 gün içinde Kurul’a şikayet yolu takip edilebilecektir.

KVKK dışındaki koruma yolları ileride inceleneceği için burada değinilmekle yetinilecektir. KVKK m. 14/3 uyarınca “*Kişilik hakkı ihlal edilenlerin, genel hükümlere göre tazminat hakkı saklıdır.*” KVKK’nın öncesinde de kişilik hakkı ihlal edilenler Medeni Hukuk çerçevesinde tazminat talep edebilmekteydi. Ancak KVKK m. 14/3 düzenlemesinden sonra söz konusu talebin artacağı öngörülmektedir⁵⁵¹. Hükme göre ilgili kişi, kişilik hakkı ihlal edildiğinde veri sorumlusuna başvuru (KVKK m. 11/1/ğ) ve sonrasında Kurul’a şikayet yoluna gidebileceği gibi, bunlardan ayrı olarak genel hükümlere yargı yoluna giderek tazminat talep edebilecektir. Ancak Kurul kararları incelendiğinde, Kurul’a yapılan şikayetlerde tazminat talebinin incelenmediği ve genel mahkemelere başvurulması gerektiği yönünde kararlar verildiği görülmektedir. Zira bu husus bir kurul kararında “*İlgili kişinin zarara uğraması ve buna yönelik bir tazminat talebi söz konusuysa, KVKK m. 14/3 hükmü çerçevesinde, söz konusu talebini genel*

⁵⁵¹ Küzeci, s. 373.

mahkemeler huzurunda kullanması gerekir.” şeklinde ifade edilmiştir⁵⁵².

2. Kurul Tarafından Yapılan İncelemenin Usul ve Esasları

Kurul tarafından yapılacak incelemenin usul ve esasları KVKK m. 15’de hüküm altına alınmıştır. Öncelikle belirtmek gerekir ki, Kurul tarafından inceleme yapılabilmesi için ilgili kişinin şikayeti şart değildir. Kurul, ihlal iddiasını resen öğrenmesi durumunda da inceleme yapabilecektir⁵⁵³.

KVKK m. 15/2 gereği “3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanunun 6. maddesinde belirtilen şartları taşımayan ihbar veya şikâyetler incelemeye alınmaz.” Buna göre, ilgili kişi tarafından Kurul’a yapılan şikayetin belli şartları taşıması gereklidir. Söz konusu şekil ve esas şartlarını taşımayan şikayetlere Kurul tarafından itibar edilmeyecektir. Söz konusu hükümde üç bent halinde dilekçelerin incelenemeyeceği düzenlenmiştir. Buna göre “*belli bir konuyu ihtiva etmeyen, yargı mercilerinin görevine giren konularla ilgili olanlar ve dilekçede bulunmayan zorunlu şartları taşımayan*” şikayetler Kurul tarafından incelenmeyecektir. Örneğin Kurul’un

⁵⁵² **Kurul Kararı**, 16.01.2020 T., 2020/41 K. <https://kvkk.gov.tr/Icerik/6714/2020-41> (E.T.: 02.04.2020). Yine benzer bir kararda “*ilgili kişinin başvurusunda manevi zarara uğradığı yönünde bir iddia ve buna ilişkin bir tazminat talebinin söz konusu olduğu dikkate alınarak, KVKK m. 14/3 hükmü çerçevesinde, talebin genel mahkemeler huzurunda kullanılması gerektiğinden, Kurul tarafından tesis edilecek bir işlem bulunmadığına*” karar verilmiştir. **Kurul Kararı**, 16.01.2020 T., 2020/43 K. <https://kvkk.gov.tr/Icerik/6715/2020-43> (E.T.: 02.04.2020).

⁵⁵³ KVKK m. 15/1.

verdiği bir kararda⁵⁵⁴ ilgili kişi tarafından Kurul’a yapılan başvuruda TCK kapsamına girecek suç iddialarının olduğu saptanmıştır. Bu nedenle söz konusu başvuru yargı merciinin görev alanına girdiğinden Kurulca incelenmemiştir.

Kurul’un şikayet ile ilgili inceleme yapabilmesi için veri sorumlusunun elindeki bazı bilgi ve belgelere ihtiyacı olabilir. Peki Kurul, veri sorumlusunun elindeki her türlü bilgiyi isteyebilir mi? Eğer isterse veri sorumlusu bu bilgileri Kurul’a vermek zorunda mıdır? Bu soruların cevabını KVKK m. 15/3 hükmü vermektedir. Buna göre veri sorumlusu, *“Devlet sırrı niteliğindeki bilgi ve belgeler hariç; Kurulun, inceleme konusuyla ilgili istemiş olduğu bilgi ve belgeleri on beş gün içinde göndermek ve gerektiğinde yerinde inceleme yapılmasına imkân sağlamak zorundadır.”* Hükümde görüldüğü üzere Kurul tarafından şikayet ile ilgili bilgi ve belge talebi olursa veri sorumlusunun bu talebi karşılama yükümlülüğü bulunmaktadır. Buradaki tek istisna bilgilerin devlet sırrı niteliğinde olmasıdır. Bu nitelikte bilgi ve belgelerin olması durumunda veri sorumlusunun, Kurul’a söz konusu bilgi ve belgeleri verme yükümlülüğü ortadan kalkmaktadır. Bu istisna dışında Kurul tarafından veri sorumlusundan istenen bilgi ve belgeler 15 gün içinde Kurul’a verilmelidir. Şikayet konusu, Kurul’un yerinde inceleme yapmasını gerektiriyorsa, veri sorumlusu, bu incelemeyi engelleyecek eylemlerden kaçınmalıdır.

İlgili kişinin Kurul’a şikayeti halinde Kurul, şikayeti değerlendirerek olumlu ya da olumsuz bir cevap vermelidir. Yani başvuruyu ya kabul eder ya da reddeder. Ancak bir diğer durum Kurul’un cevap vermeyerek sessiz kalmasıdır. Kurul tarafından belirli

⁵⁵⁴ **Kurul Kararı**, 24.12.2018 T., 2018/156 K. <https://kvkk.gov.tr/Icerik/5425/-Yargi-mercilerinin-gorev-alanina-giren-konularla-ilgili-Kuruma-yapilan-basvurular-hakkinda-Kisisel-Verileri-Koruma-Kurulunun-24-12-2018-tarihli-ve-2018-156-sayili-Karari-Ozeti> (E.T.: 04.04.2020).

bir süre cevap verilmemesi KVKK m. 15/4 uyarınca “*zımnî ret*” sayılmaktadır. Buna göre “*Şikâyet tarihinden itibaren altmış gün içinde cevap verilmezse talep reddedilmiş sayılır.*”⁵⁵⁵ Yani KVKK, Kurul’un sessizliğine ve eylemsizliğine bir sonuç bağlamıştır. Söz konusu hükümde Kurul’un şikâyet üzerine inceleme yaptığı zaman 60 günlük süre söz konusudur. Ancak Kurul incelemesini resen yapıyorsa herhangi bir süreyle bağlı değildir⁵⁵⁶.

Kurul sessiz kalma dışında, yaptığı incelemede herhangi bir ihlal görmeyebilir. Bu durumda ilgili kişinin şikâyetine Kurulca olumsuz cevap verilmiş olacaktır. Bir diğer durum ise Kurul’un yaptığı inceleme sonucu ihlal olduğuna kanat getirmesidir. Yani Kurul yaptığı değerlendirmede hukuka aykırılık tespit edebilir. Bu durum KVKK m. 15/5’de düzenlenmiştir. Buna göre “*Şikâyet üzerine veya resen yapılan inceleme sonucunda, ihlalin varlığının anlaşılması hâlinde Kurul, tespit ettiği hukuka aykırılıkların veri sorumlusu tarafından giderilmesine karar vererek ilgililere tebliğ eder.*” Hükümde de görüldüğü üzere Kurul yaptığı incelemede hukuka aykırılık tespit ederse ilgili kişinin başvurusu olumlu sonuçlanmış olacaktır. Kurul bu durumda ilgililere kararını tebliğ eder. Veri sorumlusu tarafından 30 gün içinde bu kararın gereği yerine getirilmelidir⁵⁵⁷. Veri sorumlusu kendisine tebliğ edilen karardan sonra hukuka aykırılığa son vermelidir. Veri sorumlusu, 30 gün içinde karar gereği yapılması gerekenleri yapmalıdır. KVKK m. 15 uyarınca “*Kurul tarafından verilen kararları yerine getirmeyenler hakkında 25.000 Türk lirasından 1.000.000 Türk lirasına kadar idari para cezası verilir.*” Görüldüğü üzere Kurul kararlarını yerine getirmemek KVKK çerçevesinde kabahat olarak

⁵⁵⁵ KVKK 15. madde gerekçesine göre, “*Şikâyet tarihinden itibaren altmış günlük sürenin geçmesiyle idari yargıda dava açma süresi başlayacaktır.*”

⁵⁵⁶ KVKK gerekçe, m. 15.

⁵⁵⁷ KVKK m. 15/5.

değerlendirilmiş ve idari para cezası yaptırımına bağlanmıştır.

Kurul tarafından yapılan değerlendirmelerde (şikayet üzerine ya da resen fark etmeksizin) söz konusu olan hukuka aykırılıkların çok sık gerçekleştiği fark edilirse “*ilke kararı*” alınacaktır. İlke kararı, KVKK m. 15/6’da düzenlenmiştir. Buna göre, “*Şikâyet üzerine veya resen yapılan inceleme sonucunda, ihlalin yaygın olduğunun tespit edilmesi hâlinde Kurul, bu konuda ilke kararı alır ve bu kararı yayımlar. Kurul, ilke kararı almadan önce ihtiyaç duyması hâlinde, ilgili kurum ve kuruluşların görüşlerini de alabilir.*” Kurul tarafından alınan ilke kararları yayımlanarak sıklıkla karşılaşılan hukuka aykırılıkların engellenmesi amaçlanmaktadır. Kurul bu madde çerçevesinde ilke kararlarını yayınlamaya başlamıştır. Gerçekten de veri koruma bilincinin yeni yeni oluştuğu ülkemizde Kurul ilke kararları ciddi manada yol göstericidir.

Kurul bazı durumlarda “*kişisel verilerin işlenmesinin durdurulması kararı verebilir.*” Yukarıda sayılan kararlardan farklı olarak Kurul tarafından verilebilecek başka bir karar olan durdurma kararı KVKK m. 15/7’de hüküm altına alınmıştır. Buna göre “*Kurul, telafisi güç veya imkânsız zararların doğması ve açıkça hukuka aykırılık olması hâlinde, veri işlenmesinin veya verinin yurt dışına aktarılmasının durdurulmasına karar verebilir.*” Örneğin Kurul tarafından yapılan incelemede hukuka aykırılık olduğuna kanaat getirilirse; Kurul, KVKK m. 18 gereği veri sorumlusu hakkında idari para cezası uygulayabilir. Ancak telafisi güç ve imkansız bir zarar doğacaksa, Kurul kişisel veriyle ilgili işlemlerin durdurulmasına karar verebilir⁵⁵⁸. Örneğin Kurul tarafından yayınlanan “*rehberlik hizmeti veren uygulamalarla(numaradan isim sorgulama ya da isimden numara sorgulama gibi imkanlar veren uygulamalar)*” ilgili ilke kararda kişiler tarafından uygulamalar aracılığıyla başkalarının iletişim bilgilerine yetkisiz olarak erişildiği tespit edilmiştir. Kurul tarafından verileri paylaşan bu tarz uygulamalar

⁵⁵⁸ **Kurul**, Örnekler, s. 40.

tarafından yapılan veri işlemenin KVKK m. 15/7 kapsamında durdurulmasına karar verilmiştir⁵⁵⁹.

Kurul tarafından “*kabahatler*” başlıklı KVKK m. 18’e dayanılarak idari para cezasına karar verilmesi halinde, 15 gün içinde Sulh Ceza Mahkemesi’ne başvurulabilir. Zira 5326 sayılı Kabahatler Kanunu’nu m. 27’ye göre, “*İdarî para cezası ve mülkiyetin kamuya geçirilmesine ilişkin idarî yaptırım kararına karşı, kararın tebliği veya tefhimi tarihinden itibaren en geç onbeş gün içinde, sulh ceza mahkemesine başvurulabilir. Bu süre içinde başvurunun yapılmamış olması halinde idarî yaptırım kararı kesinleşir.*”

Ancak örneğin Kurul tarafından kişisel verilerin işlenmesinin durdurulmasına karar verilmesi halinde idari yargı yoluna gidilecektir⁵⁶⁰.

§7. Kişisel Verileri Koruma Kurumu

I. Kişisel Verileri Koruma Kurumu

KVKK’nın 6. bölümünde Kurum ve teşkilat yapısı düzenlenmiştir. KVKK m. 19’a göre “*Bu Kanunla verilen görevleri yerine getirmek üzere, idari ve mali özerkliğe sahip ve kamu tüzel kişiliğini haiz Kişisel Verileri Koruma Kurumu kurulmuştur.*” Kurum’un kurulma amacı, KVKK kapsamında öngörülen görevleri yerine getirmek olarak belirlenmiştir. Kurum kamu tüzel kişiliğine sahiptir. AK 108 sayılı Sözleşme ve AB Direktifi gibi uluslararası belgelere uygun olarak Kurum’un bağımsız bir otorite

⁵⁵⁹ **Kurul İlke Kararı**, 21.12.2017 T., 2017/61 K.

<https://www.kvkk.gov.tr/Icerik/4113/2017-61> (E.T.: 04.04.2020).

⁵⁶⁰ İlgililer Kurul tarafından verilen kararlara karşı idare mahkemelerinde dava açabilirler. KVKK, gerekçe, m. 15.

olduđu hüküm altına alınmıştır⁵⁶¹. Kurum’un görevleri KVKK m. 20’de sayılmıştır. Kurum’un; kişisel verilerin hukuka uygun işlenmesini sağlamak, kişisel veri konusunda düzenleyici işlem oluşturmak gibi görevleri vardır⁵⁶². Kurum, veri sorumlusunun kişisel verilerin korunmasına saygı duymasını sağlayacak düzenlemeleri yapmalı ve bunun için gerekli tedbirleri almalıdır.

KVKK m. 19/4’e göre Kurum, Kurul ve Başkanlıktan oluşmaktadır.

II. Kişisel Verileri Koruma Kurulu

Kurul, Kurumun karar organıdır⁵⁶³. KVKK m. 21/1’e göre “*Kurul, bu Kanunla ve diğer mevzuatla verilen görev ve yetkilerini kendi sorumluluđu altında, bağımsız olarak yerine getirir ve kullanır. Görev alanına giren konularla ilgili olarak hiçbir organ, makam, merci veya kişi, Kurula emir ve talimat veremez, tavsiye veya telkinde bulunamaz.*” Kurul da uluslararası belgelerde öngörüldüğü şekilde bağımsız olarak düzenlenmiştir. Bu hüküm gereği, Kurul hiçbir yere bağımlı olmadığı gibi kararlarını hiçbir kişi veya kurumun etkisi altında kalmadan vermelidir. Yine aynı maddede Kurul’un yapısı, Kurul üyesi olma şartları sayılmıştır (KVKK m. 21/3). Buna göre Kurul 9 üyeden oluşur. 5 üyeyi TBMM, 4 üyeyi ise Cumhurbaşkanı seçecektir (KVKK m. 21/2). Yine TBMM tarafından yapılacak üye seçimi detaylı bir şekilde maddede yer bulmuştur (KVKK m. 21/5). Kurul/Kurum başkanı ise Kurul üyeleri tarafından yapılan oylamayla seçilecektir (KVKK m. 21/7). Üyelerin görev süresi 4 yıldır ve tekrar seçilebilirler (KVKK m. 21/8). Kurul üyelerinin bu görev süreleri sona ermeden herhangi bir sebeple üyelikleri sona erdirilemez (KVKK m. 21/13). Bu hüküm, Kurul’un kişisel verilerin

⁵⁶¹ KVKK, gerekçe, m. 19.

⁵⁶² **Kurum**, KVKK ve Getirdikleri, s. 3.

⁵⁶³ KVKK m. 19/4.

korunmasına ilişkin görevlerini yerine getirirken bağımsız olmaları ve verecekleri kararlar sonucunda görevlerinin sona ereceği korkusu yaşamamaları amacıyla getirilmiştir.

Kurul'un görev ve yetkileri KVKK m. 22'de detaylı bir şekilde sayılmıştır. Çalışmamızın ilgili yerlerinde Kurul'un görevleri sayılmıştır. Ancak Kurul'un en önemli görevlerinden birinin maddede belirtilen *“kişisel verilerin, temel hak ve özgürlüklere uygun şekilde işlenmesini sağlamak”* olduğunu tekrar vurgulamak gerekir.

Kurul'un çalışma esasları KVKK m. 23'de hüküm altına alınmıştır. Kurul'un çalışma esaslarına ilişkin *“Kişisel Verileri Koruma Kurulu Çalışma Usul ve Esaslarına Dair Yönetmelik”* RG'de⁵⁶⁴ yayımlanmıştır. KVKK m. 23/4 gereği, Kurul üyelerinin sır saklama yükümlülüğü vardır. Görevleri nedeniyle öğrendikleri bilgileri açıklayamazlar.

Son olarak belirtmek gerekir ki, Kurum ve teşkilat yapılanmasına ilişkin yönetmelikler yayımlanmıştır. *“Kişisel Verileri Koruma Uzmanlığı Yönetmeliği”*⁵⁶⁵, *“Kişisel Verileri Koruma Kurumu Personeli Görevde Yükselme ve Unvan Değişikliği Yönetmeliği”*⁵⁶⁶, *“Kişisel Verileri Koruma Kurumu Teşkilat Yönetmeliği”*⁵⁶⁷ ve *“Kişisel Verileri Koruma Kurumu Disiplin Amirleri Yönetmeliği”*⁵⁶⁸ RG'de yayımlanmıştır.

⁵⁶⁴ RG. 16.11.2017, S. 30242.

⁵⁶⁵ RG. 09.02.2018, S. 30327.

⁵⁶⁶ RG. 05.05.2018, S. 30412.

⁵⁶⁷ RG. 26.04.2018, S. 30403.

⁵⁶⁸ RG. 17.05.2019, S. 30777.

ÜÇÜNCÜ BÖLÜM

6698 SAYILI KİŞİSEL VERİLERİN KORUNMASI KANUNU DIŞINDA

KİŞİSEL VERİLERİN KORUNMASI YOLLARI

§8. Kişisel Verilerin Korunması

Çalışmamızda sürekli olarak ifade ettiğimiz gibi, kişisel verilerin yaşadığımız dönemdeki öneminden bahsetmeye gerek dahi yoktur. Kişisel veriler “*çağdaş ekonominin hammaddesi*⁵⁶⁹” olarak ifade edilmektedir. Bunun önemini kavrayan birçok şirket ise çok büyük miktarlarda veri toplayarak veri bankaları oluşturmuş ve söz konusu bankalardan ciddi anlamda kazanç elde etmişlerdir⁵⁷⁰. Özel teşebbüsler kadar devlet de vatandaşlarına daha iyi hizmet sunmak gibi çeşitli sebeplerle çok yüksek miktarlarla veri işlemiştir ve işlemeye devam etmektedir. Verilerimizin işlenmesi bakımından özel-devlet ayrımı bulunmamaktadır. Yaşadığımız dönemde attığımız her adımda verilerimiz işlenmektedir. Sonuç olarak artık insanlar verilerinin nerede, ne kadar işlendiğini, kimlerle paylaşıldığını ve kimlerin erişebildiğini dahi bilemez hale gelmiştir. Buna karşın kişisel verilerin korunma ihtiyacı elzem hale gelmiştir. Söz konusu korumada ise ne özel hukuk ne de kamu hukuku ayrımı yapılabilir. Yani kişisel verilerin korunmasını sağlayacak her hukuki düzenlemenin irdelenmesi ve koruma kapsamında değerlendirilmesi gereklidir. Kişisel verilerin etkin bir şekilde korunması için Anayasa Hukuku, İdare Hukuku, Ceza Hukuku, Medeni Hukuk, Borçlar Hukuku ve İş Hukuku gibi birçok hukuk alanında hukuki düzenlemeler yapılmıştır ve yapılmaya da devam

⁵⁶⁹ Aksoy, Kişisel Veri, s. 77.

⁵⁷⁰ Aksoy, Kişisel Veri, s. 78.

etmektedir. Tüm hukuk alanlarındaki korumanın incelenmesi çalışma konumuzun boyutlarını ciddi anlamda genişletecektir. Bu nedenle yukarıda detaylıca incelediğimiz KVKK'ya ek olarak TMK ve TCK hükümleri inceleme konusu yapılacak, iş ilişkisindeki özel durumlara da değinilecektir.

KVKK kapsamında kişilere tanınan koruma yollarından yukarıda bahsettik. Buna göre, ilgili kişinin veri sorumlusuna başvuru, Kurul'a şikayet gibi gidebileceği koruma yolları bulunmaktadır. Söz konusu kanun ülkemiz veri koruma hukuku için çok büyük bir atılımdır. Ancak kişisel verilerin korunmasında sadece bu kanunun göz önünde bulundurulması yetersiz kalacaktır. Kişisel verilerin korunmasıyla ilgili hem özel hem de genel kanunlarda birçok düzenleme mevcuttur. Birey gerçekten veri işleme faaliyetine karşı korunmak isteniyorsa ülkemiz mevzuatındaki tüm koruma yollarının bir arada değerlendirilmesi gerekmektedir.

Yine Anayasamızda 2010 yılında yapılan değişiklikle “*kişisel verilerin korunmasını isteme hakkı*”nın tanınması ülkemiz veri hukuku açısından ciddi anlamda önem teşkil etmektedir.

§9. İş İlişkisinde Kişisel Verilerin Korunması

İşçinin, işverene bağımlı olarak emir ve talimatları kapsamında iş görmesi İş Hukuku'nda işçinin kişilik hakkının dolayısıyla kişisel verilerinin korunma nedeni olarak belirlenebilir⁵⁷¹. İşverenin iş ilişkisinin güçlü tarafı olması kişisel verilerin hukuka aykırı

⁵⁷¹ **Kaplan, Emine Tuncay**, “*İş Hukukunda Kişilik Haklarının Özellikle Bilgisayarda Toplanan Bilgilere Karşı Korunması*”, AÜSBFD, 1997, C. 52, S. 1, s. 371.

olarak işlenmesine yol açmamalıdır⁵⁷². Kişisel verilerin korunmasında kabul görmüş tüm kurallar ve ilkeler iş ilişkisine de uygulanacaktır. Ancak bu uygulamada iş ilişkisinin ve İş Hukuku'nun kendine has yapısının göz önünde bulundurulması gerekmektedir⁵⁷³. İşverenin aralarındaki hukuki ilişki gereği işçiye ait işlemesi gerekli olan kişisel veriler elbette mevcuttur. Zira işçinin kişisel verilerinin işlenmesi aralarındaki iş ilişkisi ile de sınırlı değildir. Ayrıca iş ilişkisi başlamadan önceki aşama olan işe başvuru aşamasında ve söz konusu ilişkisi sona erdikten sonra da işçinin bilgileri işlenebilmektedir⁵⁷⁴. Bu nedenlerle elbette işçinin kişisel verileri işlenebilecektir. Ancak bu işlemenin hukuka uygun ve bir düzen çerçevesinde yapılması gerekmektedir. Ayrıca işçi-işveren ilişkilerinde, bu ilişkinin hassas yapısı gereği, kişisel verilerin korunmasının daha dikkatli olarak değerlendirilmesi gerekmektedir. Örneğin işçinin açık rızasına dayanarak işveren tarafından veri işlenmesi durumunda aralarındaki hassas ve bağımlı⁵⁷⁵ ilişki nedeniyle işçisinin rızasının özgür iradesine dayanıp dayanmadığının adaletli bir şekilde değerlendirilmesi gereklidir. Nitekim özgür iradeye dayanmayan rıza beyanı açık rıza olarak nitelendirilemeyeceğinden veri işleme faaliyeti hukuka aykırı olacaktır. İşten çıkarılma korkusu, işte yükselememe korkusu veya mobbing uygulanacağı endişesiyle verilen rızaların özgür bir şekilde verildiği bahis konusu dahi değildir. Eğer rızanın özgür

⁵⁷² **Uncular, Selen**, Kişisel Verilerin Korunması Kanunu ve AB Genel Veri Koruma Tüzüğü Kapsamında İş İlişkisinde İşçinin Kişisel Verilerinin Korunması, Güncellenmiş ve Genişletilmiş 2. Baskı, Ankara 2018, s. 121.

⁵⁷³ **Uncular**, s. 119.

⁵⁷⁴ **Gürsel, İlke**, “*Kişisel Verilerin Korunması Hakkının İşçi ve İşveren İlişkisine Etkileri*”, Legal İSGHD, 2016, C. 13, S. 50, s. 765.

⁵⁷⁵ İK m. 8/1: “*İş sözleşmesi, bir tarafın (işçi) bağımlı olarak iş görmeyi, diğer tarafın (işveren) da ücret ödemeyi üstlenmesinden oluşan sözleşmedir.*”

olup olmadığı konusunda ikilem varsa (işçi lehine yorum da göz önüne alınarak) rızanın geçerli olmadığı kabul edilmelidir.

İşveren, işçinin kişisel verilerini işlerken elbette KVKK'ya riayet etmelidir. Bu verilerin işlenmesinin hukuka uygun olarak yapılması isteniyorsa KVKK m.5 ve 6'daki veri işleme şartlarına uyulmalıdır. Ayrıca kişisel verilerin korunmasının beyni ve kalbi niteliğinde olan temel ilkelere de veri sorumlusu işveren riayet etmelidir. Yine işçi, KVKK m. 13 kapsamında veri sorumlusu işverene başvuru hakkına sahiptir. İsteğinin kabul edilmemesi halinde yine Kurum'a şikayet hakkı vardır. Uzun lafın kısası işçi, KVKK'dan kaynaklanan tüm korumalardan yararlanabilir. Yine kişisel verilerin hukuka aykırı olarak işlenmesi durumunda aşağıda detaylarıyla inceleyeceğimiz TMK⁵⁷⁶ ve TCK hükümlerinden de yararlanabilir. Bunun dışında iş ilişkisine özgü bazı özel düzenlemeler de mevcuttur.

İşçinin kişisel verilerinin korunması, işverenin yükümlülüklerinden olan “*işçinin kişiliğini gözetme borcu*”nun bir uzantısı olarak değerlendirilmektedir⁵⁷⁷. Türk Borçlar Kanunu (“**TBK**”) m. 417'de işçinin kişilik hakkının korunması hüküm altına alınmıştır. Buna göre “*İşveren, hizmet ilişkisinde işçinin kişiliğini korumak ve saygı göstermek ve işyerinde dürüstlük ilkelerine uygun bir düzeni sağlamakla, özellikle işçilerin psikolojik ve cinsel tacize uğramamaları ve bu tür tacizlere uğramış olanların daha fazla zarar görmemeleri için gerekli önlemleri almakla yükümlüdür.*” Görüldüğü üzere, kanun koyucu, işverene, işçinin kişilik hakkını koruma ve bu hakka saygı gösterme yükümlülüğü getirmiştir. Bu nedenle kişisel verileri hukuka aykırı olarak işleyen işveren

⁵⁷⁶ Detaylı bilgi için bkz. **Sevimli, Ahmet**, “*İşçinin Özel Yaşam Hakkı Bağlamında İşçi-İşveren İlişkisi*”, MESS Sicil İş Hukuku Dergisi, 2008, S. 10, s. 60 vd.

⁵⁷⁷ **Süzek, Sarper**, İş Hukuku, Yenilenmiş 12. Baskı, İstanbul 2016, s. 438.

işçiyi gözetme borcunu da yerine getirmemiş olacaktır⁵⁷⁸.

TBK m. 419 ise doğrudan kişisel verileri düzenlemiştir. Buna göre “İşveren, işçiye ait kişisel verileri, ancak işçinin işe yatkınlığıyla ilgili veya hizmet sözleşmesinin ifası için zorunlu olduğu ölçüde kullanabilir. Özel kanun hükümleri saklıdır.” Hükümde geçen özel kanun 2016 yılında yürürlüğe giren KVKK’dır⁵⁷⁹.

İş Kanunu incelendiğinde “işçi özlük dosyası” ile ilgili işçiye bir koruma getirildiği gözlemlenmektedir. İK m. 75’de işverene işçi özlük dosyası düzenleme yükümlülüğü getirilmiştir. Söz konusu özlük dosyasında işçiye ait kişisel veriler yer alacaktır. Bunu öngören kanun koyucu 75. maddenin 2. fıkrasında koruma getirmiştir. Buna göre “İşveren, işçi hakkında edindiği bilgileri dürüstlük kuralları ve hukuka uygun olarak kullanmak ve gizli kalmasında işçinin haklı çıkarı bulunan bilgileri açıklamamakla yükümlüdür.” İşçinin kişisel verilerinin hükümde öngörülen şekilde hukuka uygun kullanılmaması halinde işçi İK m. 24/2’ye dayanarak iş sözleşmesini haklı nedenle feshedebilir. Aynı zamanda işçinin genel hükümler uyarınca tazminat talep etme hakkı da vardır⁵⁸⁰.

Hem TBK m. 419 hem de İK m. 75 incelendiğinde kişisel verilerin işlenmesinden bahsedilmediği, “kullanılmasının” hüküm altına alındığı görülmektedir⁵⁸¹. Kişisel

⁵⁷⁸ Gürsel, İşçi ve İşveren İlişkisi, s. 837.

⁵⁷⁹ Sevimli, Ahmet, “Veri Koruma Hukuku İlkeleri Işığında Türk Borçlar Kanunu Madde 419”, MESS Sicil İş Hukuku Dergisi, 2011, S. 24, s. 133.

⁵⁸⁰ Manav, A. Eda, “İş İlişkisinde İşçinin Kişisel Verilerinin Korunması, GÜHFD, 2015, C. 19, S. 2, s. 106; Belge, Ayşe Merve, “Özellikle Kişisel Verilerin Korunması Kanunu Çerçevesinde İşçilerin Kişisel Verilerinin İhlali ve Korunması Yolları, DEÜHFD, 2017, Prof. Dr. Şeref ERTAŞ’a Armağan, C. 19, Özel Sayı, s. 1046.

⁵⁸¹ Süzek, s. 443.

verilerin kullanılması da bir veri işleme türüdür. Ancak daha önce de bahsettiğimiz gibi, kişisel verilerin işlenmesi çok daha geniş bir kavramdır. Kişisel veri üzerinde gerçekleştirilen her türlü işlem, işleme sayılmaktadır. İK'nın düzenlendiği tarihte KVKK gibi kişisel verilere özgü bir kanunumuzun bulunmaması “işleme” yerine “kullanma” kelimesinin tercih edilmesine yol açmış olabilir. Kanaatimizce kişisel verilerin gerçek anlamda korunmasında samimi olmak için söz konusu hükümler kişisel veri işlenmesinin her türlü faaliyetini kapsayacak şekilde geniş olarak yorumlanabilir⁵⁸². Söz konusu hükümlerdeki korumalar geniş olarak yorumlanmasa ve kanunun sözüne riayet edilerek sadece kişisel verilerin *kullanılmasının* düzenlenmiş olduğu kabul edilse bile KVKK hükümleri gereğince kişisel veri işleme faaliyetinin her aşamasında genel ilkelere ve işleme şartlarına uyulması gerektiğinden herhangi bir koruma açığı söz konusu olmayacaktır.

Yukarıda da bahsettiğimiz gibi, iş ilişkisinin birçok aşamasında işçinin kişisel verileri işlenebilmektedir. İşçi adaylığı sürecinde ve iş ilişkisi devam ederken adaya veya işçiye sağlığı, kişiliği, dini, sendika üyeliği, siyasi görüşü, eskiden herhangi bir suçtan hüküm giyip giymediği gibi birçok soru sorulmaktadır. Yine işçiye alkol, uyuşturucu, HIV/AIDS veya psikolojik testler uygulanabilmektedir⁵⁸³. İşverenler tarafından çeşitli sebeplerle işçinin gözetlenmesi ve izlenmesi uygulamaları da söz konusu

⁵⁸² Aynı görüş için bkz. **Sevimli**, Veri Koruma, s. 134.

⁵⁸³ İşçinin kişisel verilerinin işlendiği uygulamalarla ilgili detaylı bilgi için bkz., **Gürsel, İlke**, İşçinin Kişisel Verilerinin Korunması Hakkı, Ankara 2016, s. 277 vd.; **Uncular**, s. 186-304.

olabilmektedir⁵⁸⁴. Buna; işçinin e-postalarının izlenmesi, internette dolaşımının izlenmesi, işçinin GPS araçlarıyla izlenmesi gibi uygulamalar örnek olarak verilebilir. Örnek niteliğinde saydığımız söz konusu uygulamaların hepsi işçinin kişisel verilerinin işlenmesine yol açmaktadır. Bu nedenle bu tür uygulamalarda KVKK m. 5 ve 6 kişisel verileri işleme şartları, KVKK m. 10 aydınlatma yükümlülüğü gibi KVKK'dan doğan her türlü sorumluluk yerine getirilmelidir. Aksi halde kişisel verilerin işlenmesi hukuka aykırı olduğundan yukarıda da bahsettiğimiz gibi işçi, İK m. 24/2'ye dayanarak sözleşmeyi haklı nedenle feshedebileceği gibi tazminat talep etme hakkına da sahip olacaktır.

İşçinin Whatsapp konuşmaları gerekçe gösterilerek sözleşmesinin feshedildiği bir olay Yargıtay kararına⁵⁸⁵ yansımıştır. Yargıtay'a göre, *“Whatsapp konuşmaları gizlilik içeren kişisel veri niteliğinde olduğundan, salt nasıl temin edildiği anlaşılamayan bu yazışmalara dayanılarak iş aktinin feshi haksız olup, kıdem tazminatı ve ihbar tazminatı taleplerinin kabulü gerekmektedir.”*

⁵⁸⁴ Bu konuda detaylı bilgi için bkz. **Özdemir, Hayrunnisa**, *“İşyerinde İşçilerin İzlenmesi ve İşçinin Kişilik Haklarının Korunması”*, EÜHFD, 2010, C.14, S. 1-2, s. 231-270.

⁵⁸⁵ Yargıtay 9. HD., 10.01.2019 T., 2018/10718 E., 2019/559 K. Benzer yöndeki karar için bkz. Yargıtay 9. HD., 01.06.2017 T., 2016/14205 E., 2017/9526 K. (Kazancı, E.T.: 25.04.2020).

§10. 4721 Sayılı Türk Medeni Kanunu Kapsamında Kişisel Verilerin Korunması

I. Genel Olarak

Kişisel verilerin temelinde bir kişilik hakkı olduğuna dair açıklamalarımızı kişisel verilerin hukuki niteliği kısmında belirttik. Bu nedenle kişisel verilerin korunmasında TMK m. 23, 24, 25’de öngörülen kişiliğin korunmasına ilişkin hükümlere dayanılabilecektir. Kişilik hakkına ilişkin açıklamalar daha önce yapıldığı için tekrara düşmemek amacıyla burada atıf yapmakla yetiniyoruz.

KVKK m. 11/1/ğ maddesi kişinin uğradığı zararın giderilmesini talep hakkı vermiştir. KVKK m. 14/3’e göre de “*Kişilik hakları ihlal edilenlerin, genel hükümlere göre tazminat hakkı saklıdır.*” İşte burada sözü edilen “*genel hükümler*” TMK ve TBK’daki kişilik hakkını koruyan hükümlerdir⁵⁸⁶. Yani KVKK’da açıkça belirtilmese de dolaylı olarak TMK’ya atıf yapıldığı kabul edilebilir.

KVKK ile birlikte kişisel verilerin korunması ile ilgili farkındalık artacağından TMK kişiliğin korunması hükümlerine daha sık başvurulacağı düşünülmektedir⁵⁸⁷.

Kişiliği, hukuki işlemle (kişinin rızasıyla) gerçekleştirilen saldırılara koruyan hüküm TMK m. 23’tür. Kişiliği, hukuka aykırı fiille (kişinin rızası dışında)

⁵⁸⁶ **Gürpınar, Damla**, “*Kişisel Verilerin Korunamamasından Doğan Hukuki Sorumluluk*”, DEÜHFD, 2017, Prof. Dr. Şeref ERTAŞ’a Armağan, C. 19, Özel Sayı, s. 689.

⁵⁸⁷ **Küzeci**, s. 388.

gerçekleştirilen saldırılara karşı koruyan hüküm ise TMK m. 24'tür⁵⁸⁸. TMK m. 25'de ise hukuka aykırı fiille kişilik ihlali durumunda başvurulabilecek hukuki yollar hüküm altına alınmıştır⁵⁸⁹.

II. Kişisel Verilerin Hukuki İşlemle Gerçekleştirilen Saldırlara Karşı Korunması

TMK m. 23'ün koruma alanını kişinin hak ve fiil ehliyeti ile özgürlükleri oluşturmaktadır⁵⁹⁰. TMK m. 23 uyarınca *“Kimse, hak ve fiil ehliyetlerinden kısmen de olsa vazgeçemez. Kimse özgürlüklerinden vazgeçemez veya onları hukuka ya da ahlâka aykırı olarak sınırlayamaz.”*

TMK m. 23 korumasında aslında kişi bir hukuki işlem yapmaktadır ve rızası vardır. Ancak kanun koyucu buna rağmen (kişinin rızası olmasına rağmen) kişiliği koruyucu bir hüküm getirmiştir. Bu hükmün getirilmesinin sebebi sözleşmenin zayıf tarafının, sözleşmenin güçlü tarafı karşısında haklarından vazgeçmesinin veya aşırı sınırlandırılmasının engellenmesidir⁵⁹¹.

Hükme göre hak-fiil ehliyeti ve özgürlükleri sınırlandıran sözleşmeler geçerlidir. Ancak bu sözleşmelerin hukuka ve ahlaka aykırı olmaması gerekmektedir. Örneğin kişi, özel yaşamıyla ilgili bilgilerin beyanına dair bir sözleşme yapabilir. Ancak bu

⁵⁸⁸ **Dural/Öğüz**, s. 148; **Helvacı**, Koruyucu Davalar, s. 13; **Helvacı**, Gerçek, s. 139; **Özsunay, Ergun**, Gerçek Kişilerin Hukuki Durumu, Genişletilmiş ve Gözden Geçirilmiş 4. Baskı, İstanbul 1979, s. 151.

⁵⁸⁹ **Kılıçoğlu**, Basın, s. 12; Yargıtay 4. HD., 03.07.2019 T., 2017/763 E., 2019/3735 K. (Kazancı, E.T.: 22.04.2020).

⁵⁹⁰ **Dural/Öğüz**, s. 148; **Özsunay**, s. 152; **Tekinay**, s. 252.

⁵⁹¹ **Helvacı**, Gerçek, s. 139.

sözleşmenin hukuka ve ahlaka aykırı olmaması gerekmektedir⁵⁹².

TBK m. 26 gereğince *“Taraflar, bir sözleşmenin içeriğini kanunda öngörülen sınırlar içinde özgürce belirleyebilirler.”* Buna göre bir sözleşmenin içeriğini kişisel veriler de oluşturabilir. TBK m. 26’da öngörülen sözleşme özgürlüğünün sınırlarını TMK m. 23 ve TBK m. 27 oluşturmaktadır. Başka bir ifadeyle, TMK m. 23, sözleşme özgürlüğünü, kişilik hakkını korumak için sınırlamaktadır⁵⁹³. TBK m. 27’de sözleşme özgürlüğüne getirilen sınırlamalar belirtilmiştir. Buna göre *“Kanunun emredici hükümlerine, ahlaka, kamu düzenine, kişilik haklarına aykırı veya konusu imkânsız olan sözleşmeler kesin olarak hükümsüzdür.”* Hükümde de görüleceği üzere kişilik haklarına aykırı olan sözleşmeler kesin hükümsüzlük yaptırımına bağlanmıştır. Kişilik hakkıyla ilgili düzenlemeler zaten emredici hükümlerdir. Ancak buna rağmen kanun koyucu kişilik hakkını özel olarak koruma ihtiyacı hissetmiş ve *“kişilik hakkına aykırı sözleşmelerin”* geçersiz olacağını ayrıca belirtmiştir⁵⁹⁴. TMK m. 23’de *“vazgeçme ve aşırı sınırlamanın”* yaptırımı açıkça belirtilmemiştir. TBK m. 27 gereği bu yaptırım kesin hükümsüzlüktür⁵⁹⁵.

⁵⁹² **Kılıçoğlu, Ahmet M.**, Borçlar Hukuku Genel Hükümler, Genişletilmiş 23. Bası, Ankara 2019, s. 142.

⁵⁹³ **Serozan, Medeni**, s. 457; *“TMK’nın 23/2. maddesi uyarınca kimsenin özgürlüklerinden vazgeçemeyeceği veya onları hukuka ya da ahlaka aykırı olarak sınırlayamayacağı, dolayısıyla hukuk sistemimizde sözleşme serbestisi ilkesi yanı sıra bu özgürlüğün sınırlarının da belirlenmiş durumda olduğu...”* Yargıtay 11. HD., 04.03.2019 T., 2017/5343 E., 2019/1793 K. (Kazancı, E.T.: 22.04.2020).

⁵⁹⁴ **Kılıçoğlu**, Borçlar, s. 141.

⁵⁹⁵ **Antalya, O. Gökhan**, Borçlar Hukuku Genel Hükümler, C. V/1, 1, Genişletilmiş 2. Baskı, Ankara 2019, s. 462.

Yargıtay kararları da bu yöndedir⁵⁹⁶.

Ayrıca belirtmek gerekir ki, bir sözleşmenin bağlayıcılığı için çok uzun yıllar öngörülmüşse bu sözleşme kişilik hakkına aykırılık nedeniyle geçersiz olacaktır⁵⁹⁷. Kanaatimizce bir sözleşmede kişisel verilerin işlenmesi rıza sebebine dayanıyorsa, verilen rızaların çok uzun bir süreyi kapsaması da rızanın ve sözleşmenin geçersiz olmasına yol açacaktır.

Tüm hükümler birlikte değerlendirildiğinde kişisel verilerin korunması hakkından vazgeçilemeyeceği sonucuna ulaşılmaktadır. Ayrıca kişisel veriler hukuka ya da ahlaka aykırı olarak sınırlandırılmayacaktır. Aksi halde bu sözleşme kesin hükümsüz olacaktır.

III. Kişisel Verilerin Hukuka Aykırı Fiille Gerçekleştirilen Saldırlara Karşı Korunması

A. Genel Olarak

TMK m. 24 kişiliği hukuka aykırı olarak gerçekleştirilen saldırılara karşı korumaktadır. TMK m. 23'de kişiliğin, kişinin kendi rızası ile saldırıya uğraması

⁵⁹⁶ “Bir bütün olarak kişilik hakkı ve içerdiği değerler sözleşme özgürlüğünün sınırını oluşturduğundan bu hakka ve bu hakkın içerdiği değerlere aykırı sözleşmeler kesin hükümsüzdür. Bu durumda kişilik hak ve özgürlüklerini konu edinen sözleşmesel kısıtlamalar hakkında TMK'nın 23. ve TBK'nın 27/1'inci maddeleri gözetilerek değerlendirme yapılacak ve sözleşme hükümleri anılan kanun maddelerinin koruma amaçlarına aykırı düştüğü ölçüde kişilik hakkını ihlâl nedeniyle geçersiz olacaktır.” Yargıtay HGK., 04.07.2019 T., 2019/11-25 E., 2019/874 K. (Kazancı, E.T.: 22.04.2020).

⁵⁹⁷ **Oğuzman, Kemal/ Öz, Turgut**, Borçlar Hukuku Genel Hükümler, C. 1, Gözden Geçirilmiş 16. Bası, İstanbul 2018, s. 84.

düzenlenmişken, TMK m. 24’de kişiliğin, kişinin rızası dışında saldırıya uğraması düzenlenmiştir. TMK m. 25’de ise kişiliğe saldırı halinde açılacak davalar hüküm altına alınmıştır. Yani kişisel verilerin hukuka aykırı olarak işlenmesi durumunda kişi, TMK m. 24 korumasından yararlanabilecektir. Bu kişi TMK m. 25’de düzenlenen davaları da açabilecektir.

TMK m. 24/1’e göre *“Hukuka aykırı olarak kişilik hakkına saldırılan kimse, hâkimden, saldırıda bulunanlara karşı korunmasını isteyebilir.”* Kişilik hakkının mutlak hak olması hasebiyle, kişilik hakkına saldırılar koruma altına alınmıştır. Görüldüğü üzere koruma talep edebilmek için öncelikle hukuka aykırılığın söz konusu olması gerekmektedir. Kişilik hakkına saldırı gerekçesiyle hakimden korunma istenmesi durumunda, hakim öncelikle kişilik hakkına herhangi bir saldırının vuku bulup bulmadığını inceleyecektir. Bundan sonraki aşamada ise hakim, saldırının hukuka aykırı olup olmadığı tespiti yapacaktır⁵⁹⁸. Kişisel verilerin hukuka aykırı olarak işlendiği iddiası varsa, hakim öncelikle *“kimliği belirli veya belirlenebilir gerçek kişiye ilişkin bir bilgi”* yani kişisel veri olup olmadığı tespiti yapacaktır. Ondan sonra ise söz konusu kişisel veriye müdahalenin hukuka aykırı olup olmadığını değerlendirecektir.

TMK m. 24/2 uyarınca *“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.”* Hükümden anlaşılacağı üzere, kural olarak kişilik hakkına müdahale hukuka aykırıdır. Bu kural kişilik hakkının mutlak hak olmasından kaynaklanmaktadır. Kişilik hakkına saldırı haksız fiil teşkil etmektedir. Ancak hukuka uygunluk sebeplerinin olması

⁵⁹⁸ Dural/Öğüz, s. 152.

halinde, müdahale, hukuka aykırı kabul edilmeyecektir⁵⁹⁹. Fiilin hukuka aykırı olup olmadığı bütün hukuk düzeni dikkate alınarak tespit edilebilir⁶⁰⁰. Hukuka uygunluk nedenlerinden herhangi birinin somut olayda yer alması halinde kişisel verilerin işlenmesi de hukuka uygun bir hal alacak ve söz konusu işleme hukuka aykırı bir işleme olarak değerlendirilmeyecektir.

Rızanın bu çerçevede değerlendirilebilmesi için hukuka ve ahlaka aykırı olmaması gerekir. Aksi halde rıza, hukuka uygunluk nedeni olmayacağı için hukuka aykırılığı ortadan kaldırmayacaktır. Hukuka aykırı olarak verilen rıza ancak tazminatın indirilmesi hususunda dikkate alınır⁶⁰¹.

Hukuka uygunluk sebepleri, TMK m. 24/2’de sayılmıştır. Buna göre, hukuka uygunluk sebepleri; “*kişilik hakkı zedelenen kimsenin rızası*”, “*daha üstün nitelikte özel yarar*”, “*kamusal yarar*” ve “*kanunun verdiği yetkinin kullanılması*”dır. Kişisel verilere özgü hukuka uygunluk sebepleri ise KVKK m. 5 ve 6’da sayılmıştır. Yani KVKK m. 5 ve 6’daki hallerden birinin olması durumunda kişisel verilerin işlenmesi hukuka uygun hale gelecektir. Bu haller detaylarıyla ilgili kısımda anlatıldığından burada değinilmekle yetinilecektir. KVKK, TMK’ya göre özel nitelikte bir kanun olduğundan hukuka uygunluk sebeplerinde KVKK m. 5 ve 6’daki hükümler öncelenmelidir. Ancak bu kabul TMK m. 24/2’deki hukuka uygunluk nedenlerinin tamamen ekarte edileceği anlamına gelmemektedir. Yani kişisel verilerin işlenmesi durumunda öncelikle KVKK m. 5 ve 6 hukuka uygunluk halleri incelenmelidir. Sonrasında TMK’da düzenlenen hukuka uygunluk sebeplerine bakılmalıdır. Burada sayılanlar da niteliğine uygun düştüğü ölçüde

⁵⁹⁹ **Günay, Erhan**, Kişilik Haklarına Saldırıdan Kaynaklanan Tazminat Davaları, Güncellenmiş 2. Baskı, Ankara 2017, s. 86; **Helvacı**, Gerçek, s. 145.

⁶⁰⁰ **Kılıçoğlu**, Borçlar, s. 368.

⁶⁰¹ **Helvacı**, Koruyucu Davalar, s. 103-104.

uygulanır⁶⁰². Eğer hukuka uygunluk nedenleri olarak nitelendirdiğimiz kişisel verilerin işlenme şartlarından (KVKK m.5-6) herhangi biri varsa veri işleme hukuka uygundur. Kişisel verilerin işlenmesinin hukuka uygun olması durumunda da TMK m. 25’de öngörülen davalar açılmayacaktır.

B. Kişisel Verilerin Hukuka Aykırı Olarak İşlenmesi Halinde Açılacak Davalar

Kişisel verilerin hukuka aykırı olarak işlenmesi halinde açılacak davalar TMK m. 25’de sayılmıştır. Hükümde sayılan davaları koruyucu davalar ve tazminat davaları olarak ikiye ayırarak incelemek mümkündür.

1. Koruyucu Davalar

TMK m. 25/1 uyarınca *“Davacı, hâkimden saldırı tehlikesinin önlenmesini, sürmekte olan saldırıya son verilmesini, sona ermiş olsa bile etkileri devam eden saldırının hukuka aykırılığının tespitini isteyebilir.”* Koruyucu davalar, *“saldırı tehlikesinin önlenmesi davası”, “saldırıya son verilmesi davası”* ve *“saldırının hukuka aykırılığının tespiti davası”* şeklinde sıralanabilir.

Koruyucu davaların açılabilmesi için hepsinin ortak özelliği, kişilik hakkına hukuka aykırı bir saldırı gerçekleştirilmesidir. Söz konusu saldırı, bitmiş, devam ediyor veya gelecekte gerçekleşmesi muhtemel olabilir. Koruyucu davalarda failin kusurlu olması gerekmez⁶⁰³. Ayrıca saldırı nedeniyle bir zarar olması da gerekmez. Kişilik hakkı

⁶⁰² Taştan, s. 150.

⁶⁰³ Serozan, Medeni, s. 477; Zevkliler/Acabey/Gökyayla, s. 460.

ihlal edilen zarara uğramamış olsa dahi koruyucu davaları açabilir⁶⁰⁴. Başka bir ifadeyle, maddi-manevi herhangi bir zarara uğramayan kişi bile söz konusu davaları açabilmektedir⁶⁰⁵. Kısaca, bu davalarda kusur ve zarar aranmaz⁶⁰⁶.

Koruyucu davaların etkisini arttırmak için kanun koyucu kişilik hakkı ihlal edilen kişiye bir hak vermiştir. Söz konusu bu hak TMK m. 25/2’de düzenlenmiştir. Buna göre *“Davacı koruyucu davalarla birlikte, düzeltmenin veya kararın üçüncü kişilere bildirilmesi ya da yayımlanması isteminde de bulunabilir.”* Kişilik hakkı, saldırıya uğrayan kişi, kişiliği koruyucu davaları açıp kazansa dahi saldırının sonuçlarının tam olarak bertaraf edildiği söylenemez. Zira saldırı, örneğin, internet üzerinde gerçekleştiyse, konu ile ilgili-ilgisiz herkesin söz konusu ihlalden haberi olacaktır. Sadece mahkeme önünde saldırının önlenmesi, son verilmesi ya da tespitine karar verilmiş olması, hakkı ihlal edilen kişinin tam olarak tatmin olmasını sağlamadığı gibi vicdanları da rahatsız edecektir. Bu nedenle herkes tarafından mahkeme kararının bilinmesi ve hukuka aykırılığın sona erdirilmesi için TMK m. 25/2 öngörülmüştür. Amaç, saldırıya uğrayanın kişisel tatmininin sağlanmasıdır⁶⁰⁷. Hükme göre kişi, açacağı koruyucu dava ile birlikte kararın 3. kişilere bildirilmesini ya da yayımlanmasını isteyebilecektir. Söz konusu talep koruyucu davalarla birlikte öne sürülebilecektir. Bu nedenle bu talebin yapılabilmesi için koruyucu davaların açılabilme şartları gerçekleşmelidir⁶⁰⁸. Hükümden

⁶⁰⁴ **Helvacı**, Gerçek, s. 157.

⁶⁰⁵ **Helvacı**, Koruyucu Davalar, s. 86.

⁶⁰⁶ **Bulut, Harun**, Kişilik Hakları ve Kişilik Haklarına Saldırıdan Kaynaklanan Hukuk Davaları, İstanbul 2006, s. 177.

⁶⁰⁷ **Bulut**, s. 179.

⁶⁰⁸ **Helvacı**, Koruyucu Davalar, s. 141.

anlaşıldığı üzere, davacının bu konuda talebi gereklidir⁶⁰⁹. Hakim resen kararın bildirilmesine ya da yayımlanmasına hükmedemeyecektir⁶¹⁰. Ayrıca belirtmek gerekir ki, TMK m. 25/2'deki imkan koruyucu davaların hepsi için geçerlidir. Zira hükümde davalar arasında herhangi bir ayırım yapılmamıştır⁶¹¹.

a. Saldırı Tehlikesinin Önlenmesi Davası

Önleme davası, şuan kişiliğe yönelik bir saldırı vuku bulmasa da ileride gerçekleşebilecek bir saldırı tehlikesinin bulunduğu durumlarda açılacak bir koruyucu davadır. Yani kişiliğe yönelik saldırı henüz meydana gelmemiştir. Ancak ileride gerçekleşebilecek bir saldırı tehlikesi vardır⁶¹². Söz konusu tehlike ciddi⁶¹³ ve yakın olmalıdır⁶¹⁴. Saldırı tehlikesi varsa önleme davası açılabilir⁶¹⁵. Bu tehlike son bulmuşsa, yani artık herhangi bir tehlike yoksa yahut saldırı halihazırda gerçekleşmişse önleme davası açılamaz⁶¹⁶. Davacı, saldırı tehlikesinin bulunduğunu ispatlamalıdır⁶¹⁷.

⁶⁰⁹ **Helvacı**, Koruyucu Davalar, s. 142.

⁶¹⁰ **Dural/Öğüz**, s. 159.

⁶¹¹ **Bulut**, s. 179.

⁶¹² **Serozan**, Medeni, s. 476; **Tekinay**, s. 269.

⁶¹³ **Özsunay**, s. 154.

⁶¹⁴ **Helvacı**, Koruyucu Davalar, s. 128.

⁶¹⁵ Saldırı tehlikesi devam ediyor olmalıdır. “TMK 25/1 maddesi gereğince davanın açıldığı tarihte saldırı tehlikesinin devam ettiği anlaşıldığından mahkemece davanın kabulüyle saldırı tehlikesinin önlenmesi kararının verilmesi gerekir.” Yargıtay 4. HD., 23.12.2019 T., 2017/2589 E., 2019/6238 K. (Kazancı, E.T.: 22.04.2020).

⁶¹⁶ **Helvacı**, Koruyucu Davalar, s. 129; **Kılıçoğlu**, Basın, s. 325.

⁶¹⁷ **Bulut**, s. 178.

Davanın açılma nedeni, mağduru, ileride gerçekleşebilecek olan saldırılara karşı korumaktır. Bu davayla muhtemel saldırılar, meydana gelmeden engellenebilecektir⁶¹⁸. Bu davanın açılabilmesi için failin kusuru gerekmediği gibi herhangi bir zarar tehlikesinin bulunması da gerekmez⁶¹⁹. Kısaca, önleme davasının açılabilmesi için, öncelikle, diğer koruyucu davalarda da şart olan hukuka aykırılık bulunmalıdır. Kişilik hakkına saldırı tehlikesi olmalı ve bu tehlike ciddi ve yakın olmalıdır.

Kişisel verilerin hukuka aykırı olarak işleme tehlikesi varsa önleme davası açılabilir. Örneğin bir internet sitesinde kişisel bilgilerinin paylaşılacağını öğrenen bir kimse saldırı tehlikesinin önlenmesi davası açabilmelidir. Ancak belirtmek gerekir ki, hukuka uygunluk sebeplerinin bulunması halinde söz konusu veri işleme hukuka aykırı olmayacaktır. Yani somut olayda KVKK m. 5 ve 6'daki kişisel verileri işleme şartlarından herhangi biri bulunuyorsa önleme davası sonuç doğurmayacaktır.

b. Saldırıya Son Verilmesi Davası

Kişiliğe karşı bir saldırı varsa ve bu hukuka aykırı saldırı sürmekteyse bu dava açılabilir. Davanın açılma nedeni, kişiliğe yönelen hukuka aykırı saldırıya son vermektir⁶²⁰. Bu davanın açılabilmesi için saldırının hukuka aykırı olması gerekli ve yeterlidir. Ayrıca failin kusuru ya da zararın meydana gelmiş olması gerekmez. Saldırı durumu sürdüğü müddetçe bu dava açılabilirdiğinden, saldırı devam ettikçe zamanaşımı söz konusu olmayacaktır. Saldırı henüz başlamamış yahut başlamış ve sona ermişse saldırıya son verilmesi davası açılmayacaktır⁶²¹. Bu davanın açılabilmesi için mutlaka

⁶¹⁸ **Helvacı**, Koruyucu Davalar, s. 175.

⁶¹⁹ **Dural/Öğüz**, s. 157; **Helvacı**, Gerçek, s. 158.

⁶²⁰ **Kılıçoğlu**, Basın, s. 336.

⁶²¹ **Eren, Fikret**, Borçlar Hukuku Genel Hükümler, 22. Baskı, Ankara 2017, s. 807.

süren bir saldırı olmalıdır⁶²². Henüz bir saldırı yoksa bu dava açılmaz. Ancak şartlar sağlanırsa önleme davası açılabilir⁶²³.

Kişisel verilerin hukuka aykırı olarak işlenmesi halinde, işleme faaliyeti devam ediyorsa son verme davası açılabilir. Kişisel verilerin KVKK m. 5 ve 6'daki şartlardan hiçbirini olmadan işlenmesi halinde işleme hukuka aykırı nitelik taşıyacağından bu dava açılabilir.

Örneğin dağıtımdaki bir kitapta kişisel verilerin hukuka aykırı olarak işlenmesi söz konusuysa söz konusu dava açılabilir.⁶²⁴

KVKK m. 7'de belirtildiği gibi kişisel veriler hukuka uygun olarak işlenmiş olmasına rağmen, sonradan hukuka aykırı hale gelebilir. Buna neden olan durum, kişisel verinin işlenme sebebinin sonradan ortadan kalkmasıdır. Böyle bir durumda kişisel veriler, kendiliğinden ya da ilgili kişinin talebi ile imha edilmelidir. İşlemenin hukuka aykırı hale bürünmesi durumunda ilgili kişi KVKK m. 7 ve KVKK m. 11'den kaynaklanan haklarını kullanarak silme, düzeltme, yok etme talebinde bulunabileceği gibi saldırıya son verme davası⁶²⁵ da açılabilir. Fikrimce kişisel verilerin hukuka aykırı olarak işlendiği veya sonradan hukuka aykırı hale geldiği durumda kolay bir yol olması açısından ilgili kişi, veri sorumlusuna başvurmayı tercih edebilir. Talep reddedilirse, Kurul'a şikayet yoluna gidilebileceği gibi aynı zamanda hukuka aykırı veri işlenmesine son verilmesi amacıyla dava açılabilir. Ancak kişinin talebiyle ya da resen kişisel verinin hukuka aykırı olarak işlenmesi sonlandırılırsa son verilme davası açılmayacaktır.

⁶²² **Dural/Öğüz**, s. 156; **Helvacı**; Gerçek, s. 159.

⁶²³ **Bulut**, s. 178.

⁶²⁴ **Helvacı**, Koruyucu Davalar, s. 130.

⁶²⁵ Söz konusu dava ile kişisel verilerin imhası sağlanabilecektir. **Serozan**, Medeni, s. 476.

Zira burada artık saldırı devam etmemektedir.

Tutulan verilerin güncelliğini yitirmesi veya yanlış olması ayrıca kişinin zarara uğramasına da yol açabilir. Kişi, verilerinin bu şekilde işlenmesi sebebiyle maddi-manevi zarara da uğrayabilir⁶²⁶. Örneğin kişinin adres bilgisi yanlış işlenmiş olabilir. Yine kişi eski adresinden taşınmış olabilir. Verilerin güncelliğini kaybetmesi kişiyi zarara uğratabilir. Kişi bu durumda yukarıda belirttiğimiz gibi elbette saldırıya son verilme davası açabilir. Ancak zarara uğraması durumunda, aşağıda detaylarıyla inceleyeceğimiz tazminat davalarını da açabilecektir.

c. Saldırının Hukuka Aykırılığının Tespiti Davası

Bu davanın açılabilmesi için de hukuka aykırı bir saldırı olmalıdır. Söz konusu dava, hukuka aykırı saldırının son bulduğu ancak etkisinin sürdüğü durumlarda açılabilir⁶²⁷. Henüz gerçekleşmemiş bir saldırı için tespit davası açılmayacaktır⁶²⁸. Tespit davasının açılabilmesi için yine failin kusuru veya zararın oluşması gerekmez. Davanın açılma nedeni, hukuka aykırılığın tespit edilerek saldırının etkilerini sona erdirmektir⁶²⁹. Yani amaç, hukuka aykırı saldırının mahkeme kararıyla tespitini sağlamaktır⁶³⁰. Özellikle hukuka aykırı saldırının 3. kişiler tarafından öğrenildiği

⁶²⁶ **Özbakır, Ali Fuat**, Sosyal Medyada ve İnternette Hukuki Sorumluluk, Ankara 2019, s. 223.

⁶²⁷ **Eren**, s. 807; **Reisoğlu, Safa**, Türk Borçlar Hukuku Genel Hükümler, 24. Bası, İstanbul 2013, s. 230.

⁶²⁸ **Ayan/Ayan**, s. 126.

⁶²⁹ **Helvacı**, Koruyucu Davalar, s. 132.

⁶³⁰ **Ayan/Ayan**, s. 126.

durumlarda saldırının etkisinin devam ettiği söylenebilir⁶³¹.

Kişisel verilerin hukuka aykırı olarak işlenmesi sona ermiş ancak söz konusu hukuka aykırı işlemenin kişi bakımından etkileri devam ediyorsa kişi, saldırının hukuka aykırılığının tespiti davası açabilecektir. Örneğin kişisel veri işleme şartlarına riayet edilmeden kişinin kişisel bilgilerinin paylaşılması veya 3. kişilere aktarılması halinde, işleme sona erdirilse dahi kişi açısından etkileri devam edeceğinden söz konusu dava açılabilirdir.

2. Tazminat Davaları

TMK m. 25/3 uyarınca *“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.”* Tazminat davaları; *“maddi tazminat davası”, “manevi tazminat davası”* ve *“kazancın geri verilmesi davası”* olarak sıralanabilir. Aşağıda bu 3 dava incelenecektir. Burada ise söz konusu 3 davanın ortak özelliklerine değinilecektir.

Tazminat davasının açılma nedeni, bitmiş saldırının neticelerini ortadan kaldırmak ya da onarmaktır. Tazminat davalarının açılabilmesi için saldırı son bulmuş olmalıdır. Gerçekleşmemiş veya gerçekleşmeye devam eden saldırılara karşı tazminat davası açılmayacaktır⁶³².

Kişisel veriler açısından bakıldığında ilgili kişi söz konusu tazminat davalarını açabilecektir. Nitekim KVKK m. 14/3’de *“kişilik hakkı ihlal edilenlerin genel hükümlere göre tazminat hakkının saklı olduğu”* belirtilmiştir. KVKK incelendiğinde kişisel verilerin hukuka aykırı olarak işlenmesi halinde tazminat davaları için özel bir

⁶³¹ **Dural/Öğüz**, s. 158; **Helvacı**, Gerçek, s. 160-161; **Helvacı**, Koruyucu Davalar, s. 132.

⁶³² **Helvacı**, Gerçek, s. 161; **Helvacı**, Koruyucu Davalar, s. 178.

düzenlemenin yer almadığı, genel hükümlere atıf yapıldığı gözlemlenmektedir. Bu vesileyle, kişisel verileri hukuka aykırı olarak işlenmiş olan ilgili kişi TMK ve TBK hükümleri çerçevesinde tazminat davası açabilecektir.

a. Maddi Tazminat Davası

Kişilik hakkı saldırıya uğrayan kimse, saldırı nedeniyle malvarlığında oluşan eksikliğin ortadan kaldırılması için maddi tazminat davası açabilir⁶³³. Maddi zarar, saldırı nedeniyle kişinin malvarlığında oluşan eksilme olarak tanımlanabilir⁶³⁴. Kişilik hakkı malvarlığı kapsamında değildir. Ancak kişilik hakkına dahil değerlerin ihlali malvarlığında olumsuz sonuçlara yol açabilir⁶³⁵. Özetle bu dava ile maddi zararın⁶³⁶ tazmini amaçlanır. Koruyucu davalarda kusur ya da zarar şartının aranmadığından bahsettik. Ancak maddi tazminat davası açılabilmesi için kusur (ya da kusursuz sorumluluk hali) ve zarardan bahsedilebilmelidir. Kısaca, maddi tazminat davasının açılabilmesi için haksız fiil ya da borca aykırılığın şartları meydana gelmiş olmalıdır⁶³⁷. Maddi tazminat davasının açılabilmesi şu şartlarının gerçekleşmesine bağlıdır⁶³⁸.

- Hukuka aykırı bir saldırı olmalıdır. (Kişisel verilerin hukuka aykırı olarak işlenmesi).

- Kusur (ya da kusursuz sorumluluk hallerinden biri) var olmalıdır.

⁶³³ **Helvacı**, Koruyucu Davalar, s. 177.

⁶³⁴ **Eren**, s. 545; **Kılıçoğlu**, Borçlar, s. 392.

⁶³⁵ **Eren**, s. 546.

⁶³⁶ Maddi zarar kavramıyla ilgili detaylı bilgi için bkz. **Büyüksağış, Erdem**, Yeni Sosyo-Ekonomik Boyutuyla Maddi Zarar Kavramı, İstanbul 2007, s. 45 vd.

⁶³⁷ **Dural/Öğüz**, s. 161.

⁶³⁸ **Helvacı**, Gerçek, s. 162; **Kılıçoğlu**, Basın, s. 362.

- Zarar meydana gelmedir.
- Hukuka aykırı saldırı ile meydana gelen zarar arasında illiyet bağı olmalıdır.

KVKK, kişisel verilerin hukuka aykırı işlenmesi durumuna özgü bir sorumluluk hali düzenlememiştir. Başka bir ifadeyle, bu durumda kusurun aranıp aranmayacağı KVKK'da düzenlenmemiştir. Haksız fiil sorumluluğu için ise kural olarak kusur aranmaktadır⁶³⁹. Yani fail kusurlu olması durumunda sorumludur. Kusursuz sorumluluk halleri ise istisnadır⁶⁴⁰. Bu hallerde sorumluluğun kusur şartı aranmamaktadır. KVKK'da sadece genel hükümlere atıf yapılmış ve sorumlulukta kişisel verilere özgü bir düzenlemeye yer verilmemiştir. Bu nedenle kanaatimizce kişisel verilerden doğan sorumlulukta da kusur şart olarak aranmalıdır. Kişisel verilerin hukuka aykırı işlenmesinden doğan sorumluluğun, kusursuz sorumluluk hallerinden olan tehlike sorumluluğu⁶⁴¹ ya da özen sorumluluğu⁶⁴² olup olmadığı da doktrinde tartışılmaktadır.

Maddi zarar, fiili zarar ya da yoksun kalınan kar olarak kendini gösterir⁶⁴³. Kişisel verilerin hukuka aykırı işlenmesinde yoksun kalınan kar ile daha sık karşılaşılır. Örneğin meşhur bir şarkıcının doktoru tarafından HIV virüsü testinin pozitif çıktığına dair yapılan

⁶³⁹ **Kılıçoğlu**, Borçlar, s. 414.

⁶⁴⁰ **Oğuzman, Kemal/Öz, Turgut**, Borçlar Hukuku Genel Hükümler, C. 2., Gözden Geçirilmiş 14. Bası, İstanbul 2018, s. 1.

⁶⁴¹ **Gürpınar**, s. 691.

⁶⁴² **Çekin**, Kişisel Veri, s. 138-139.

⁶⁴³ **Antalya, O. Gökhan**, Borçlar Hukuku Genel Hükümler, C. V/1, 2, Genişletilmiş 2. Baskı, Ankara 2019, s. 146; **Ayan, Mehmet**, Borçlar Hukuku Genel Hükümler, Gözden Geçirilmiş 11. Baskı, Ankara, 2016, s. 319; **Eren**, s. 550; **Feyzioğlu, Feyzi Necmeddin**, Borçlar Hukuku Genel Hükümler, C. I, Yenilenmiş ve Genişletilmiş 2. Bası, İstanbul 1976, s. 473; **Kılıçoğlu**, Borçlar, s. 398.

açıklama nedeniyle şarkıcının ileri tarihteki konserlerinin iptal edilmesi yoksun kalınan kara yol açar⁶⁴⁴. Yine kişisel verilerin hukuka aykırı olarak işlenmesi sebebiyle müşterilerin azalması durumunda, yoksun kalınan kar talep edilebilecektir⁶⁴⁵. Örnekte görüldüğü gibi kişinin malvarlığında oluşması beklenen artışın haksız saldırı nedeniyle engellenmesi söz konusudur⁶⁴⁶. Online alışveriş sitesinde müşterilerin kayıtlı kredi kartı bilgilerinin çalınarak harcama yapılması ise fiili zarara örnek olarak verilebilir⁶⁴⁷.

Kişiliğe saldırı, haksız fiil şeklinde gerçekleşebileceği gibi, borca aykırılık (TBK m. 112 vd.) şeklinde de gerçekleşebilir. Yani maddi tazminat talebi, haksız fiilden ya da sözleşmeden kaynaklanabilir⁶⁴⁸. Bu nedenle maddi tazminat davasının zamanaşımı süreleri de farklılaşmaktadır. Yani süre, sorumluluğun kaynağına göre tespit edilecektir⁶⁴⁹. Söz konusu dava haksız fiilden kaynaklanıyorsa TBK m. 72 uyarınca *“Tazminat istemi, zarar görenin zararı ve tazminat yükümlüsünü öğrendiği tarihten başlayarak iki yılın ve her hâlde fiilin işlendiği tarihten başlayarak on yılın geçmesiyle zamanaşımına uğrar.”* Ancak tazminat talebi sözleşmeden kaynaklanıyorsa TBK m. 146 uyarınca 10 yıllık zamanaşımı söz konusu olacaktır.

Kişisel verilerin hukuka aykırı olarak işlenmesi halinde ilgili kişinin malvarlığında eksilmenin meydana gelmesi durumunda ilgili kişi maddi tazminat davası açabilecektir. Örneğin kişisel verilerin hukuka aykırı olarak işlenmesi sebebiyle kişi işini kaybetmişse uğradığı zararların tazminini maddi tazminat davası açarak talep

⁶⁴⁴ **Özdemir**, Elektronik Haberleşme, s. 209.

⁶⁴⁵ **Gürpınar**, s. 690.

⁶⁴⁶ **Feyzioğlu**, s. 473.

⁶⁴⁷ **Taştan**, s. 177.

⁶⁴⁸ **Dural/Öğüz**, s. 161; **Helvacı**, Gerçek, s. 162.

⁶⁴⁹ **Bulut**, s. 219.

edebilecektir.

b. Manevi Tazminat Davası

Manevi tazminatın hukuki niteliği konusunda doktrinde çeşitli görüşler bulunmaktadır⁶⁵⁰. Manevi tazminat davası, kişilik hakkına yapılan saldırı sonucu manevi zarara uğrayan kişinin başvuracağı hukuki yoldur. Başka bir ifadeyle, bu dava ile manevi acı, üzüntü ve ızdırabın giderilmesi amaçlanmaktadır⁶⁵¹. Manevi tazminat talebi⁶⁵², TMK m. 25/3 hükmünün yanında TBK m. 58’de hüküm altına alınmıştır. Manevi tazminat davası bazı konularda özel olarak (TMK m. 26/2, TMK m. 158/2, TBK m. 56 gibi) düzenlenmiştir. Ancak bu şekilde özel olarak düzenlenmeyen durumlar için TBK m. 58

⁶⁵⁰ Görüşler hakkında detaylı bilgi için bkz. **Antalya**, Borçlar 2, s. 214 vd; **Erlüle**, s. 39 vd. Doktrinde bu görüşler sübjektif görüş ve objektif görüş olarak ayrılmaktadır. Karma görüş ise objektif görüşün sübjektif görüş ile tamamlanması gerektiğini savunmaktadır. Detaylı bilgi için bkz. **Antalya, O. Gökhan**, “*Manevi Zararın Belirlenmesi ve Manevi Tazminatın Hesaplanması-Türk Hukukuna Manevi Zararın İki Aşamalı Olarak Belirlenmesine İlişkin Bir Model Önerisi*”, MÜHF-HAD, 2016, C. 22, S. 3, s. 229.

⁶⁵¹ **Dural/Öğüz**, s. 162; **Feyzioğlu**, s. 473; **Helvacı**, Gerçek, s. 163; **Kılıçoğlu**, Basın, s. 397; **Kılıçoğlu**, Borçlar, s. 552; **Reisoğlu**, s. 228; **Yavuz**, Borçlar, s. 258.

⁶⁵² Yargıtay tarafından verilen bir kararda bu davanın tanımı yapılmıştır. “*Kişilik haklarının korunması için açılacak davalardan olan manevi tazminat davası, genel olarak kabul edilen görüşe göre, zarar görenin kişilik değerlerinde iradesi dışında meydana gelen eksilmeye karşılık ya da kişilik hakkı hukuka aykırı olarak saldırıya uğrayan kimsenin duyduğu acı, elem ve ızdırabın giderilmesi amacıyla açılan bir davadır.*” Yargıtay HGK., 25.04.2018 T., 2018/19-374 E., 2018/943 K. (Kazancı, E.T.: 22.04.2020).

ve TMK m. 25/3 hükümlerine başvurulacaktır⁶⁵³. Kişisel verilerin hukuka aykırı olarak işlenmesine özgü bir düzenleme olmadığı için, böyle bir işlemeden dolayı manevi zarar doğmuşsa TMK m. 25/3 ve TBK m. 58 uyarınca manevi tazminat davası açılabilir.

TBK m. 58 uyarınca “*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.*” Hüküm bütün olarak değerlendirildiğinde, kişilik hakkı ihlal edilen kişi, davayla yalnızca para ödenmesini talep edebilecektir⁶⁵⁴. Yani kişinin burada seçim şansı yoktur. Ancak kişiye verilmeyen bu seçim şansı hakime verilmiştir. Hakim para ödenmesi yerine başka bir yaptırıma karar verebileceği gibi, para+başka bir yaptırım kararı da verebilir. Hükümde para ödenmesinden başka karara örnek olarak, hakimin saldırıyı kınayan bir karar vermesi ve söz konusu kararın yayımlanması örnek olarak verilmiştir. Sosyal medyanın ve internetin günümüz iletişiminde geldiği nokta ortadadır. Bu nedenle kararın söz konusu mecralarda yayımlanması önem teşkil etmektedir. Zira salt gazete veya televizyonda yapılan ilan hükmün amacını tam anlamıyla karşılamayabilir⁶⁵⁵. TMK m. 58/2 düzenlemesi kişisel verilerin korunması açısından önemlidir. Zira kişisel verilerin hukuka aykırı olarak işlenmesi durumunda, daha önce de belirttiğimiz gibi, sadece davaların açılması hukuka aykırılığın yahut kişinin uğradığı zararların tam anlamıyla giderilmesine (en azından azaltılmasına) yardımcı olmamaktadır. Gerçekten de özellikle kişisel verilerin 3. kişilerle

⁶⁵³ **Dural/Öğüz**, s. 162; **Helvacı**, Gerçek, s. 163.

⁶⁵⁴ Aynı yönde görüş için bkz. **Dural/Öğüz**, s. 163; **Oğuzman/Öz**, Borçlar 2, s. 278.

⁶⁵⁵ **Atasoy, Kemal**, “*Kişilik Hakkı Kapsamında Sosyal Medyada Kişisel Verilerin Korunması ve Veri Sahibinin Rızası*”, MÜHF-HAD, 2016, C. 22, S. 3, s. 275.

paylaşıldığı durumlarda sadece davanın kazanılması davacıyı tatmin etmeyecektir. Örneğin kişinin evlilik dışı ilişki yaşadığına dair iddiaların paylaşılması, kişinin hem iş ilişkilerinde hem de aile ilişkilerinde maddi-manevi zarara uğramasına yol açabilir. Söz konusu iddianın gerçek veya yalan olması da kişisel veriler açısından önem taşımaz. Kişi hakkındaki bu bilgi gerçek dışı da olsa kişisel veridir ve korunması gerekmektedir. Somut olay gibi bir durumda kişinin maddi-manevi tazminat davaları açarak kazanması durumunda dahi karardan büyük ihtimalle (davacı çok tanınan biri değilse) taraflar haberdar olacaktır. Ancak TBK m. 58 gereğince kararın yayımlanması 3. kişilerin de kişisel verilerin hukuka aykırı olarak işlenmesini öğrenmesini sağlayacaktır. Aksi halde “çamur at izi kalsın” mantığı işlemeye devam edecektir.

Manevi tazminat davasının açılabilmesi şu şartlarının gerçekleşmesine bağlıdır⁶⁵⁶. Kısaca, manevi tazminat davasının açılabilmesi için haksız fiil ya da borca aykırılığın şartları meydana gelmiş olmalıdır.

- Hukuka aykırı bir saldırı olmalıdır. (Kişisel verilerin hukuka aykırı olarak işlenmesi).
- Kusur (ya da kusursuz sorumluluk hallerinden biri) var olmalıdır.
- Manevi zarar meydana gelmelidir⁶⁵⁷.
- Hukuka aykırı saldırı ile meydana gelen zarar arasında illiyet bağı olmalıdır.

⁶⁵⁶ **Günay**, s. 22; **Helvacı**, Gerçek, s. 163; **Reisoğlu**, s. 232 vd.

⁶⁵⁷ “*Türk Borçlar Kanunu’nun 58. maddesi hükmüne göre, manevi tazminata karar verilebilmesi için 4721 Sayılı Türk Medeni Kanununun 24. maddesi hükmünde genel olarak açıklanan kişilik haklarına bir saldırı bulunması, hukuka aykırı fiil sonucunda kişilik haklarının zarar görmüş olması zorunludur.*” Yargıtay 3. HD., 15.05.2019 T., 2017/8390 E., 2019/4510 K. (Kazancı, E.T.: 22.04.2020).

Manevi tazminat talebinin devri ve mirasçılara intikali TMK m. 25/4’de hüküm altına alınmıştır. Buna göre *“Manevî tazminat istemi, karşı tarafça kabul edilmiş olmadıkça devredilemez; mirasbırakan tarafından ileri sürülmüş olmadıkça mirasçılara geçmez.”* Hükümde görüldüğü üzere, kişinin yaşarken tazminat talebini devredebilmesi için ihlal yapan tarafından devrin kabul edilmesi gerekmektedir. Kişi talebi ileri sürmeden ölürse mirasçılara geçmez. Ancak bu talebi ileri sürdükten sonra ölürse mirasçılara geçecektir. Burada *“ileri sürülmüş olma”*nın neyi kastettiğini belirlemek gerekir. TMK m. 25’in gerekçesinde *“Maddeye göre ileri sürmenin mutlaka dava yoluyla gerçekleşmesi şart olmayıp saldırıya uğrayan kişinin bunu ortaya koyan ve kanıtlanabilen hür iradesi yeterli görülmüştür.”* ifadeleri yer almıştır. Yani kişi, hayattayken dava açma iradesini belirtmesi *“ileri sürülmüş olma”* şartının gerçekleşmesi için yeterlidir. Manevi tazminat isteminin mirasçılara geçmesi için kişinin illaki sağlığında dava açmış olması gerekmemektedir. Örneğin mağdur, yaşarken çevresindekilere manevi tazminat talebinde bulunacağını beyan etmişse ve bu beyan kanıtlanmışsa, söz konusu talep mirasçılara geçecektir⁶⁵⁸.

Manevi tazminat davasındaki zamanaşımı süresi, maddi tazminat davasındaki süreler ile birebir aynıdır. Yani söz konusu dava haksız fiilden kaynaklanıyorsa TBK m. 72 uyarınca *“Tazminat istemi, zarar görenin zararı ve tazminat yükümlüsünü öğrendiği tarihten başlayarak iki yılın ve her hâlde fiilin işlendiği tarihten başlayarak on yılın geçmesiyle zamanaşımına uğrar.”* Ancak tazminat talebi sözleşmeden kaynaklanıyorsa TBK m. 146 uyarınca 10 yıllık zamanaşımı söz konusu olacaktır.

⁶⁵⁸ **Gezder**, s. 42.

c. Kazancın Geri Verilmesi Davası

Kişiliğe hukuka aykırı saldırı sonucunda saldıran kişinin elde ettiği kazanç neticesinde saldıranın malvarlığında bir artış oluşabilir. Söz konusu artışın kişiliğine saldırılan kişiye ödenmesi için açılan dava “kazancın geri verilmesi davası”dır. Bu davanın açılabilmesi şu şartlarının gerçekleşmesine bağlıdır⁶⁵⁹.

- Hukuka aykırı bir saldırı olmalıdır. (Kişisel verilerin hukuka aykırı olarak işlenmesi).

- Failin, mağdurun “elde etmek istemediği veya elde edemeyeceği kazancı” elde etmesi gerekir⁶⁶⁰.

- Hukuka aykırı saldırı ile elde edilen kazanç arasında illiyet bağı olmalıdır.

Maddi tazminat ve manevi tazminat davasında kusur şartı aranırken, söz konusu davada aranmamaktadır. Yani söz konusu davanın açılabilmesi için failin kusurlu olması gerekmez⁶⁶¹. Kazancın iade edilmesi davasının hukuki temeli gerçek olmayan vekaletsiz iş görmeye dayanmaktadır. Bu nedenle, söz konusu davada, kazanç TBK m. 530’a (gerçek olmayan vekaletsiz iş görme hükmü) dayanılarak istenebilecektir⁶⁶². Gerçek olmayan vekaletsiz iş görmede de kusur bir şart olarak aranmamaktadır⁶⁶³.

Kişisel verilerin hukuka aykırı olarak işlenmesi sonucunda veri sorumlusu bir kazanç elde ediyorsa, ilgili kişi kazancın geri verilmesi davası açarak bu kazancı talep

⁶⁵⁹ **Helvacı**, Gerçek, s. 165.

⁶⁶⁰ **Dural/Öğüz**, s. 160.

⁶⁶¹ **Helvacı**, Gerçek, s. 165; Detaylı bilgi için bkz. **Helvacı, Serap/Aydın, Gülşah Sinem**, “Kişilik Hakkı İhlalinden Doğan Vekaletsiz İşgörmede Kusurun Bir Şart Olarak Aranıp Aranmayacağı Sorunu”, MÜHF-HAD, 2017, C. 23, S. 1.

⁶⁶² **Ayan/Ayan**, s. 138; **Bulut**, s. 195; **Dural/Öğüz**, s. 160; **Serozan**, Medeni, s. 477.

⁶⁶³ **Helvacı/Aydın**, s. 281 vd.

edebilir. Sürekli vurguladığımız gibi, kişisel verilerin ekonomik değeri günümüzde paha biçilemez hale gelmiştir. Kişisel veriler kullanılarak şirketler politikalarını ayarlamakta ve dolaylı da olsa kişisel veriler üzerinden ciddi miktarda kazanç elde etmektedir. Ayrıca kişisel veriler tek başına şirketler arasında el değiştirerek kazanç elde edilebilmektedir. Saydığımız durumlarda, kişisel verilerin işlenmesi hukuka aykırıysa, yani veri işleme şartlarına dayanmıyorsa, ilgili kişi, veri sorumlusunun elde ettiği kazancı TBK m. 530 çerçevesinde isteyebilecektir.

3. Davacı ve Davalı Taraf

a. Davacı Taraf

Kişilik hakkına saldırı durumunda açılacak davalarda davacı ve davalı tarafın, kimlerin dava açıp yürütebileceğinin ve kimlere karşı dava açılabilirliğinin belirlenmesi gerekmektedir. Davada taraf olabilme ehliyeti, taraf ehliyetidir. Hak ehliyeti olan tüm gerçek kişiler ve tüzel kişiler taraf ehliyetine sahiptir. Yani davada taraf olabilirler. Dava ehliyeti ise kişinin davayı, davalı ya da davacı olarak takip etme ehliyeti olarak tanımlanabilir. Dava ehliyeti, fiil ehliyetine göre belirlenir. Başka bir ifadeyle, fiil ehliyetine haiz olan gerçek kişi ve tüzel kişilerin dava ehliyeti de vardır⁶⁶⁴.

Hak ve fiil ehliyetine sahip gerçek ve tüzel kişilerin, taraf ve dava ehliyetinin olduğunu belirttik. Medeni usul hukukuna ilişkin genel açıklamalardan sonra, gerçek veya tüzel kişilerin, kişilik hakkına ilişkin yukarıdaki davaları açabileceği tespitini yapabiliriz. Ancak kişisel verilerin hukuka aykırı olarak işlenmesi halinde söz konusu davaların açılacak olması durumunda durum farklılaşmaktadır. Defalarca belirttiğimiz

⁶⁶⁴ Arslan, Ramazan/Yılmaz, Ejder/Taşpınar Ayvaz, Sema/Hanağası, Emel, Medeni Usul Hukuku, 5. Baskı, Ankara 2019, s. 258.

gibi, KVKK’da kişisel veri tanımına tüzel kişiler alınmamış ve tüzel kişiler, kişisel verilerin korunması kapsamına alınmamıştır. Bu nedenle, tüzel kişiler, kişisel verilerin hukuka aykırı işlenmesi durumunda açılacak davaları (yukarıda bahsi geçen davalar) açamazlar. Nitekim tüzel kişiler kişisel verilerin korunmasına dahil değildirler. Sonuç olarak davacı taraf gerçek kişilerdir. Yukarıda bahsi geçen davalarda tüzel kişiler davacı olamaz.

Gerçek kişilerin tamamının hak ehliyeti vardır. Yani gerçek kişilerin tamamı davada taraf olabilirler. Ancak gerçek kişilerin dava ehliyetinin irdelenmesi gerekmektedir. Bu irdeleme gerçek kişilerin fiil ehliyeti üzerinden yapılmalıdır. Tam ehliyetliler (ergin, ayırt etme gücüne haiz, kısıtlı olmayan), tam dava ehliyetine de sahiptir. Bu kişiler dava açabilir ve yürütebilir. Dava ehliyeti olmayan kişiler, tam ehliyetsizlerdir (ayırt etme gücünden yoksun kişiler). Bu kişiler adına yasal temsilciler dava açabilir. Zira tam ehliyetsizler kişiye sıkı sıkıya bağlı hakları da bizzat kullanamaz⁶⁶⁵. Sınırlı ehliyetsizlerin (ayırt etme gücüne haiz küçükler ve kısıtlılar) dava ehliyeti de sınırlıdır. Bu kişilerin kural olarak dava ehliyeti yoktur. Bazı istisnai durumlarda dava ehliyetleri vardır⁶⁶⁶. Bu istisnai durumlardan biri, kişiye sıkı sıkıya bağlı haklarda ortaya çıkar. Sınırlı ehliyetsizler, kişiye sıkı sıkıya bağlı hakları kendileri kullanabilirler. Bu haklar bakımından yasal temsilcinin rızasına ihtiyaç bulunmamaktadır⁶⁶⁷. Yukarıda bahsi geçen koruyucu davalar ve manevi tazminat davasını açma, kişiye sıkı sıkıya bağlı haklardandır. Bu nedenle sınırlı ehliyetsiz bu davaları tek başına açabilir⁶⁶⁸.

⁶⁶⁵ **Gezder**, s. 39.

⁶⁶⁶ **Arslan/Yılmaz/Taşpınar Ayvaz/Hanağası**, s. 259.

⁶⁶⁷ **Helvacı**, Koruyucu Davalar, s. 157.

⁶⁶⁸ **Helvacı**, Gerçek, s. 84.

Sonuç olarak, kişisel verilerin hukuka aykırı olarak işlenmesi halinde açılacak davalarda, davacı, kişisel verisi hukuka aykırı olarak işlenen gerçek kişidir.

b. Davalı Taraf

Yukarıda bahsi geçen davalarda davalı taraf, kişilik hakkına saldırıda bulunan kişidir. Bu kişi, gerçek kişi olabileceği gibi tüzel kişi de olabilir. Kişisel verilerin korunması bakımından davalı kural olarak veri sorumlusudur. Zira kişisel verilerin işleme amacını belirleyen asıl kişi odur. KVKK m. 12/1’de veri sorumlusu, kişisel verilerin hukuka aykırı olarak işlenmesini önlemekle sorumlu tutulmuştur. Ancak KVKK m. 12/2’de “*veri sorumlusu, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumlu*” tutulmuştur. Bu hüküm gereği, veri işleyen ve veri sorumlusu, kişisel verilerin hukuka aykırı olarak işlenmesinden müştereken sorumludur. Bu nedenle davalı tarafta veri sorumlusu da veri işleyen de olabilir. KVKK’nın 3. maddesinde yapılan tanımlarda görüleceği üzere veri sorumlusu da veri işleyen de gerçek kişi veya tüzel kişi olabilir. Bu nedenle yukarıda bahsi geçen davalarda, davalı tarafta, hem gerçek kişi hem tüzel kişi yer alabilir.

Sonuç olarak, kişisel verilerin hukuka aykırı olarak işlenmesi halinde açılacak davalarda, davacı, kişisel veriyi hukuka aykırı olarak işleyen, gerçek veya tüzel kişidir.

4. Yetkili Mahkeme

Kişilik hakkına saldırı halinde açılacak yukarıda bahsi geçen bütün davalarla ilgili yetkili mahkeme TMK m. 25’in son fıkrasında hüküm altına alınmıştır. Yani hem koruyucu davalar hem tazminat davaları için yetkili mahkeme TMK m. 25/5’de düzenlenmiştir. Buna göre “*Davacı, kişilik haklarının korunması için kendi yerleşim yeri*

veya davalının yerleşim yeri mahkemesinde dava açabilir.” Kişilik hakkının korunmasında davacıya seçim hakkı tanınmıştır. Davacı (kişilik hakkı ihlal edilen) söz konusu davaları kendi yerleşim yeri mahkemesinde açabileceği gibi davalının (kişilik hakkını ihlal eden) yerleşim yeri mahkemesinde de açabilir. Kişisel verilerin hukuka aykırı olarak işlenmesi durumunda da ilgili kişi, TMK m. 25’den kaynaklanan tüm davaları, veri sorumlusuna (ve/veya veri işleyene) karşı ister kendi yerleşim yerinde isterse davalının yerleşim yerinde açabilecektir.

TMK m. 25/5 düzenlemesi kesin yetki kuralı değildir. Yani kesin olmayan bir yetki kuralıdır. Ayrıca bu hüküm özel yetkiye ilişkin bir hükümdür⁶⁶⁹. Özel yetki, genel yetkiyi bertaraf etmez. Davacı ister genel yetkiye isterse özel yetkiye dayanır⁶⁷⁰. Hükümün ifadesinden TMK m. 25/5’in kesin olmayan yetki kuralı olduğu anlaşılmaktadır⁶⁷¹. Zaten medeni usulde kesin olmayan yargı kuralları kural, kesin yargı kuralları istisnadır⁶⁷². Bu nedenle Hukuk Muhakemeleri Kanunu’nda (“**HMK**”) haksız fiilden ve sözleşmeden doğan davalardaki yetki hükümlerine de bakmak gerekmektedir. Başka bir ifadeyle, TMK m. 25/5 hükmü kesin yetki kuralı olmadığından⁶⁷³, davacı, HMK’da yetkili

⁶⁶⁹ **Pekcanıtez, Hakan/Atalay, Oğuz/Özekes, Muhammet**, Medeni Usul Hukuku Ders Kitabı, 6. Bası, İstanbul 2018, s. 75.

⁶⁷⁰ **Pekcanıtez/Atalay/Özekes**, s. 72.

⁶⁷¹ Aksi görüş için bkz. **Helvacı, Serap**, “*Kişilik Hakkına Hukuka Aykırı Saldırı Halinde Açılacak Davalarda Yetkili Mahkeme*”, Doç. Dr. Mehmet Somer’in Anısına Armağan, İstanbul 2006, s. 657-659.

⁶⁷² **Arslan/Yılmaz/Taşpınar Ayvaz/Hanağası**, s. 228.

⁶⁷³ Yargıtay HGK., 22.01.2016 T., 2014/4-213 E., 2016/70 K., (Kazancı, E.T.: 22.04.2020).

gösterilen mahkemelerde de dava açabilecektir⁶⁷⁴. Eğer dava, *sözleşmeden* doğuyorsa HMK m. 10' da⁶⁷⁵ düzenlenen sözleşmeler için özel yetki kuralına da bakmak gerekir. Ancak burada önemli bir hususa dikkat etmek gerekir. HMK m. 10'da bahsi geçen sözleşmeler, borçlar hukuku sözleşmeleridir. Yoksa kişiler hukuku ve aile hukuku sözleşmeleri için HMK m. 10 yetki hükmü geçerli değildir⁶⁷⁶. Eğer dava, *haksız fiilden* doğuyorsa, kişi yukarıda bahsi geçen davaları HMK m. 16'da⁶⁷⁷ yer verilen mahkemelerde de açabilecektir⁶⁷⁸. Davacının burada seçimlik bir hakkı vardır⁶⁷⁹.

§11. 5237 Sayılı Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması

I. Genel Olarak

Kişisel verilerin korunmasına ilişkin suçlar KVKK'da açıkça düzenlenmemiştir. Söz konusu suçlarla ilgili düzenleme TCK 135-140 maddeleri arasındadır. Bu nedenle

⁶⁷⁴ **Özdemir**, Elektronik Haberleşme, s. 234.

⁶⁷⁵ HMK m. 10: “*Sözleşmeden doğan davalar, sözleşmenin ifa edileceği yer mahkemesinde de açılabilir.*”

⁶⁷⁶ **Arslan/Yılmaz/Taşpınar Ayvaz/Hanağası**, s. 216.

⁶⁷⁷ HMK m. 16: “*Haksız fiilden doğan davalarda, haksız fiilin işlendiği veya zararın meydana geldiği yahut gelme ihtimalinin bulunduğu yer ya da zarar görenin yerleşim yeri mahkemesi de yetkilidir.*”

⁶⁷⁸ **Dural/Öğüz**, s. 166; **Tekinay**, s. 279.

⁶⁷⁹ Yargıtay 4. HD., 14.02.2017 T., 2016/15646 E., 2017/885 K. (Kazancı, E.T.: 22.04.2020).

KVKK m. 17’de⁶⁸⁰ TCK’nın ilgili hükümlerine atıf yapılmış, kişisel veri suçları bakımından TCK hükümlerinin uygulanacağını belirtilmiştir. Kişisel verilerle ilgili suçlar TCK’da hüküm altına alındığında KVKK gibi bir kanunumuz bulunmadığından uygulamada sıkıntılar ortaya çıkmaktaydı. Kişisel verilere özgü bir kanunun kabul edilmesiyle birlikte söz konusu sorun ortadan kalkmıştır. TCK’nın ilgili hükümleri KVKK ile birlikte uygulanmalıdır.

Kişisel verilere ilişkin suçlar, TCK özel hükümlerin “*kişilere karşı suçlar*” kısmında düzenlenmiştir. Bu kısmın 9. bölümünde “*özel hayata ve hayatın gizli alanına karşı suçlar*”a yer verilmiştir. Kişisel verilere ilişkin suçlar da işte bu bölümde yer almıştır. Söz konusu suçların kanundaki yerine dikkat edilirse, Anayasa’daki anlayışın TCK’da da olduğu görülecektir. Zira kişisel verilerin korunması hakkı Anayasa’da, TCK’ya benzer şekilde “*özel hayatın gizliliği*” maddesinde düzenlenmiştir. Tabii ki özel hayatla-kişisel verilerin arasında yakın bir ilişki olduğu bizce de kabul edilmektedir. Ancak kişisel verilerin korunmasının özel hayata indirgenmemesi ile ilgili yukarıda belirttiğimiz düşünce burada da geçerlidir. Kanaatimizce daha etkin bir koruma sağlanması için söz konusu hakkın Anayasa’da ayrı bir maddede düzenlenmesi gerekmektedir. Aynı gerekçeyle “*kişisel verilere ilişkin suçlar*”ın TCK’da da ayrı bir bölümde düzenlenmesi yerinde olacaktır.

TCK’da kişisel verilerle ilgili 3 adet suça yer verilmiştir. TCK m. 135’de “*kişisel verilerin kaydedilmesi suçu*” yer almıştır. TCK m. 136’da “*verileri hukuka aykırı olarak verme veya ele geçirme suçu*” düzenlenmiştir. TCK m. 138’de ise “*verileri yok etmeme*” suç olarak yer almıştır. Şimdi sırasıyla bu suçları inceleyelim.

⁶⁸⁰ KVKK m. 17: “*Kişisel verilere ilişkin suçlar bakımından 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununun 135 ila 140 ıncı madde hükümleri uygulanır.*”

Yukarıda saydığımız 3 madde doğrudan kişisel verilerin korunmasına ilişkin olup, açıkça kişisel verilerle ilgili suçlar düzenlenmektedir. Ancak dolaylı bir koruma sağlaması bakımından TCK m. 132,133 ve 134’de düzenlenen suçlar da önemlidir⁶⁸¹. Bu suçlar sırasıyla; “*haberleşmenin gizliliğini ihlal suçu*”, “*kişiler arasındaki konuşmaların dinlenmesi veya kayda alınması suçu*” ve “*özel hayatın gizliliğini ihlal suçu*” olarak sayılabilir. Ancak çalışmamızın sınırlarını oldukça genişleteceğinden bu hükümler inceleme konusu yapılmayacaktır.

II. Kişisel Verilerin Kaydedilmesi Suçu

TCK m. 135/1’e göre, “*Hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir.*” Suçun konusu, kişisel verilerdir⁶⁸². Hukuka aykırılığın tespiti, KVKK hükümleri kapsamında yapılmalıdır⁶⁸³.

⁶⁸¹ **Korkmaz, İbrahim**, Kişisel Verilerin Ceza Hukuku Kapsamında Korunması, Güncellenmiş 2. Baskı, Ankara 2019, s. 377.

⁶⁸² TCK gerekçe, m. 135. Yargıtay bir kararında her türlü kişisel verinin m. 135 ve m. 136 suçları kapsamında değerlendirilmesi gerektiğini belirtmiştir. “*TCK 135 ve 136. maddelerindeki kişisel verilerin korunmasına ilişkin düzenlemelerde sadece sır niteliğinde kişisel verilerin korunacağına ilişkin bir hükmün bulunmaması ve aksine 135. maddenin gerekçesinde gerçek kişiyle ilgili her türlü bilginin kişisel veri olarak kabul edilmesi gerektiğinin belirtilmesi karşısında, her türlü kişisel verinin hukuka aykırı olarak başkasına verilmesi, yayılması ve ele geçirilmesi fiillerinin kanunun 136. maddesindeki suçu oluşturduğu kabul edilmelidir.*” Yargıtay CGK., 17.06.2014 T., 2012/12-1510 E., 2014/331 K. (Kazancı, E.T.: 25.04.2020).

⁶⁸³ **Küzeci**, s., 407.

Suçun faili herkes olabilecektir⁶⁸⁴. Ancak TCK m. 137’de sayılan kişiler olması durumunda ceza arttırılacaktır⁶⁸⁵. Buna göre, söz konusu suçun, *“Kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle ya da belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenmesi halinde, verilecek ceza yarı oranında artırılır.”*

Kişisel verisi kaydedilen kişinin rızası olması ya da KVKK m. 5 ve 6’daki diğer veri işleme şartlarının bulunması halinde suç oluşmayacaktır⁶⁸⁶. Zira KVKK m. 5 ve 6’daki şartların olması durumunda kişisel verinin kaydedilmesi hukuka aykırı bir nitelik taşımayacaktır. KVKK m. 28’de KVKK’nın uygulanmayacağı haller hüküm altına alınmıştır. Söz konusu haller kapsamında kişisel veri kaydedilmesi durumunda da bu suç oluşmayacaktır⁶⁸⁷. Yine TCK m. 24/1’de hüküm altına alınan *“kanun hükmünün yerine getirilmesi”* hukuka uygunluk nedeni olarak belirtilebilir⁶⁸⁸.

Kişisel veriler işlenirken KVKK m. 4’de yer alan genel ilkelerin hepsine riayet edilmesi gerektiğini defalarca kez vurguladık. Örneğin kişinin adı-soyadı verisi yeterliyken kişinin anne kızlık soyadı, adet günleri gibi verilerinin işlenmesi kişisel

⁶⁸⁴ **Özbek, Veli Özer/Doğan, Koray/Bacaksız, Pınar**, Türk Ceza Hukuku Özel Hükümler, Genişletilmiş ve Güncellenmiş 14. Baskı, Ankara 2019, s. 586.

⁶⁸⁵ **Artuç, Mustafa**, Kişilere Karşı Suçlar, Genişletilmiş ve Güncellenmiş 2. Baskı, Ankara 2018, s. 1626; **Hafızoğulları, Zeki/Özen, Muharrem**, Türk Ceza Hukuku Özel Hükümler-Kişilere Karşı Suçlar, 5. Baskı, Ankara 2016, s. 287; **Yokuş Sevük, Handan**, Türk Ceza Hukuku Özel Hükümler, Genişletilmiş ve Güncellenmiş 2. Baskı, Ankara 2019, s. 271.

⁶⁸⁶ **Korkmaz**, s. 411; **Yokuş Sevük**, s. 274.

⁶⁸⁷ **Korkmaz**, s. 392, s. 422.

⁶⁸⁸ **Özbek/Doğan/Bacaksız**, s. 593.

verilerin kaydedilmesi suçunun oluşmasına yol açabilir. Zira örnekteki olayda amaçla bağlılık ve ölçülülük ilkesine aykırı davranılmış olunacaktır⁶⁸⁹.

Suçun oluşması için kaydın nerede yapıldığının bir önemi bulunmamaktadır. Zira maddenin gerekçesinde de “Söz konusu suç tanımında kişisel verilerin bilgisayar ortamında veya kağıt üzerinde kayda alınması arasında bir ayırım gözetilmemiştir.” ifadelerine yer verilmiştir. Günümüzde verilerin otomatik olarak özellikle bilgisayar ortamında işlendiği bir gerçektir. Ancak elle tutulan dosyalarda kaydedilen veriler de kişiye zarar verebilir. Bu nedenle verinin otomatik-otomatik olmayan yolla kayda alınmasına bakılmaksızın bu suç kapsamında değerlendirme yapılmalıdır⁶⁹⁰.

Bu suç, icra hareketiyle işlenebilir. Zira kaydetmek, icra hareketidir. Ayrıca bu suç “salt hareket suçu”dur. Yani verinin hukuka aykırı olarak kaydedilmesi, suçun oluşumu için yeterlidir. Ayrıca bu verilerin kullanılması ya da yarar elde edilmesi gerekmez⁶⁹¹. Yani kaydetme sonucunda herhangi bir sonucun oluşması gerekmez⁶⁹². Verinin hukuka aykırı olarak kaydedilmesinden bir zarar doğması da gerekmez. Yani herhangi bir zarar doğmasa bile kişisel veri hukuka aykırı olarak kaydedildiği zaman bu suç oluşmaktadır. Bu sebeplerle bu suç bir tehlike suçudur. Suçun düzenlemesinde hareketin somut olarak bir tehlike meydana getirebilmesinden bahsedilmemiştir. Bu nedenle bu suç bir soyut tehlike suçudur⁶⁹³.

⁶⁸⁹ **Yılmaz, Sabire Sanem**, Tıp Alanında Kişisel Verilerin Açıklanması Suçu, Güncellenmiş 3. Baskı, Ankara 2019, s. 54.

⁶⁹⁰ **Akdağ, Hale**, Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması, Ankara 2013, s. 100; **Yokuş Sevik**, s. 272.

⁶⁹¹ **Artuç**, s. 1631.

⁶⁹² **Hafizoğulları /Özen**, s. 288.

⁶⁹³ **Özbek/Doğan/Bacaksız**, s. 587.

Kişisel verilerin kaydedilmesi, KVKK m. 3/e’de işlenmenin bir türü olarak sayılmıştır. Yani kaydetme, kişisel verilerin işlenmesinin sadece bir aşamasıdır. Kişisel verilerin işlenmesi ise KVKK’daki tanımdan⁶⁹⁴ anlaşıldığı üzere çok daha geniştir ve birçok aşamayı daha kapsamaktadır. Kanunilik ilkesi gereği kaydetme dışındaki veri işlemlerinin suç oluşturmaması tehlikesi söz konusudur. Zira TCK’da sadece kaydetme yaptırıma bağlanmıştır. Bu durumda ise kişisel verilerin etkin bir şekilde korunmasından bahsedilemeyecektir. Bu nedenle TCK’daki “*kişisel verilerin kaydedilmesi suçu*”nun “*kişisel verileri işleme suçu*” olarak değiştirilmesi yerinde bir düzenleme olacaktır⁶⁹⁵. Bu eleştiri sadece kaydedilme suçunda değil, TCK m. 136 açısından da yapılabilir. Zira aşağıda detaylıca inceleneceği üzere 136. maddedeki hareketler de KVKK gereğince kişisel verilerin işlenmesi sayılmaktadır. Yani hem 135 hem de 136 madde de kişisel verilerin birkaç türü düzenlenmiştir. Ancak işlenmenin tamamı suç olarak düzenlenmemiştir. Zira işleme TCK’da sayılan hareketlerden ibaret değildir. TCK’daki kişisel veri suçlarının, kişisel verilerin hukuka aykırı işlenmesinin tamamını kapsamına

⁶⁹⁴ KVKK m. 3/1/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.*”

⁶⁹⁵ **Ketizmen, Muammer**, Türk Ceza Hukukunda Bilişim Suçları, Ankara 2008, s. 238; **Korkmaz**, s. 397.

alacak şekilde revize edilmesi gerekmektedir⁶⁹⁶.

TCK m. 139’da bu suç, şikayete bağlı bir suç olarak sayılmamıştır. Bu nedenle söz konusu suç resen takip edilir.

TCK m. 135/2’ye göre, “*Kişisel verinin, kişilerin siyasi, felsefi veya dini görüşlerine, ırkı kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması durumunda birinci fıkra uyarınca verilecek ceza yarı oranında artırılır.*” İkinci fıkra bazı kişisel veriler ayrıca sayılmıştır. Burada sayılan kişisel verilerin kaydedilmesi durumunda ceza arttırılacaktır. İkinci fıkranın iki açıdan değerlendirilmesi önem arz etmektedir.

İlk olarak bu fıkra KVKK’daki “*hassas veri*”lere benzer bir sayım yapılmıştır. Ancak burada sayılan verilerin hassas verilerle birebir örtüşmediği görülmektedir. Başka bir ifadeyle, KVKK’da sayılan hassas verilerinin tamamının sayılmadığı görülmektedir. Cezanın arttırılmasını düzenleyen bu fıkra hassas verilerin sadece bir kısmı yer almıştır. Zira KVKK m. 6’ya göre “*Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir.*” KVKK’da hassas veri sayılmasına rağmen “*etnik köken*”, “*mezhep veya diğer inançlar*”, “*kılık kıyafet*” “*vakıf ya da dernek üyeliği*” ve “*ceza mahkumiyeti ve güvenlik tedbirleriyle ilgili veriler*” ile “*biyometrik ve genetik veriler*” TCK’da ceza artış sebebi olarak görülmemiştir. Ayrıca TCK 135/2’de sayılan “*kişinin ahlaki eğilimlerine ilişkin veriler*” de KVKK’da hassas veri olarak düzenlenmemiştir. Suçta kanunilik ilkesi gereği, KVKK’da hassas veri olarak

⁶⁹⁶ **Dülger, Murat Volkan**, “*Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması*”, İMÜHFD, 2016, C.3, S.2, s. 163.

düzenlenip, TCK'da düzenlenmeyen verilerin 135/2'deki arttırmaya girmeyecekleri sonucu çıkabilir⁶⁹⁷. Ancak hassas veriler arasında ayırım yapıp, bazılarının cezayı arttıracak olması tarafımızca mantıklı görülmemektedir. Bu nedenlerle KVKK'da sayılan tüm hassas verilerin TCK m. 135/2 kapsamına alınması gerektiği savunulmaktadır⁶⁹⁸. Fikrimce KVKK m. 6 ve TCK m. 135/2'de sayılan veri türleri eşitlenmelidir⁶⁹⁹. Yani her iki kanun hükmünün uyumlu hale getirilmesi gerekmektedir⁷⁰⁰. Bu uyumlaştırmada, TCK, özel kanun olan KVKK ilgili hükmünü kapsayacak şekilde düzenlenmelidir⁷⁰¹. Önerdiğimiz uyumlaştırmanın yapılması durumunda hassas verilerin tümü ağırlaştırıcı sebep olacak ve uygulamada soru işaretleri oluşmayacaktır.

İkincisi TCK m. 135/2'de sayılan verilerin bazılarının kaydedilmesinde “*hukuka aykırılık*” ibaresi yer almıştır. Ancak bazılarında ise yer almamıştır. Gerçekten hüküm incelendiğinde bu husus görülecektir. Fıkra ikiye ayrılmaktadır. Kişilerin “*ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin*” verilerde hukuka aykırılık ibaresi yer almıştır. Ancak kişilerin “*siyasi, felsefi veya dini görüşlerine, ırki kökenlerine*” ilişkin verilerde hukuka aykırılık ibaresine yer verilmemiştir. Oysa 1. fıkroda zaten verilerin kaydedilmesinin suç oluşunda “*hukuka aykırılık*” açıkça yer almıştır. Burada kanun koyucunun niyetini anlamak zordur. “*Hukuka aykırılık*” ifadesine yer verilmeyen verilerin kaydedilmesinin zaten, her

⁶⁹⁷ **Korkmaz**, s. 432.

⁶⁹⁸ **Yokuş Sevük**, s. 275.

⁶⁹⁹ Benzer öneri için bkz. **Sert, Şeyma**, Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması, Ankara 2019, s. 109.

⁷⁰⁰ Benzer yönde, **Göçmen Uyarer, Sinem**, Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması, Ankara 2019, s. 175.

⁷⁰¹ **Özbek/Doğan/Bacaksız**, s. 591.

halükarda hukuka aykırı olduğu tespiti yapılabilir⁷⁰².

III. Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme Suçu

TCK m. 136'ya göre “*Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır. Suçun konusunun, Ceza Muhakemesi Kanununun 236 ncı maddesinin beşinci ve altıncı fıkraları uyarınca kayda alınan beyan ve görüntüler olması durumunda verilecek ceza bir kat artırılır.*” Suçun konusu kişisel verilerdir. Bu hükümde, kişisel verileri, “*başkasına vermek*”, “*yaymak*” veya “*ele geçirmek*” suç olarak belirtilmiştir. Bu nedenle bu suç, *seçimlik hareketli bir suç*tür⁷⁰³. Yani hükümde sayılan hareketlerin birinin dahi yapılması suçun oluşmasını sağlayacaktır. Hareketlerin birden fazlasının yapılmasında da tek bir suç oluşacaktır⁷⁰⁴. Örneğin fail, verileri hem ele geçirip hem de başkasına verirse TCK m. 136 özelinde tek bir suçtan söz edilir⁷⁰⁵. Yoksa ayrı ayrı iki suç oluşmaz. Faile de tek suçun cezası verilecektir⁷⁰⁶. Ancak hareketin birden fazla olması cezayı etkileyebilecektir⁷⁰⁷.

⁷⁰² **Hafizoğulları /Özen**, s. 288.

⁷⁰³ **Ketizmen**, s. 239; Yargıtay CGK., 09.05.2019 T., 2015/12-708 E., 2019/414 K. Yargıtay CGK., 17.06.2014 T., 2012/12-1510 E., 2014/331 K. (Kazancı, E.T.: 25.04.2020).

⁷⁰⁴ **Özbek/Doğan/Bacaksız**, s. 597.

⁷⁰⁵ **Yokuş Sevük**, s. 285.

⁷⁰⁶ **Dülger**, Ceza Normlarıyla Korunma, s. 132.

⁷⁰⁷ **Hafizoğulları /Özen**, s. 290.

Suçun faili herkes olabilecektir⁷⁰⁸. Ancak TCK m. 137’de sayılan kişiler olması durumunda ceza arttırılacaktır⁷⁰⁹. Buna göre, söz konusu suçun, *“Kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle ya da belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenmesi halinde, verilecek ceza yarı oranında artırılır.”* Cezanın arttırılacağı hale, bir psikiyatristin, hastasına ait bilgileri boşanma davasında kullanması için hastasının eşiyle paylaşması örnek olarak verilebilir⁷¹⁰.

TCK m. 135’de düzenlenen *“verilerin kaydedilmesi”* ve TCK m. 136’da düzenlenen *“verme”*, *“yayma”* ve *“ele geçirme”* hareketleri KVKK m. 3/e’de kişisel verilerin işlenmesinin türleri arasında sayılmıştır. Yani bunların hepsi özünde bir veri işleme faaliyetidir. Yukarıda da belirtildiği gibi KVKK m. 5 ve 6’daki veri işleme şartlarının bulunması durumunda veri işleme hukuka uygun sayılacaktır. Yani kişisel veri işleme şartlarından birisi varsa *“verilerin kaydedilmesi”*, *“verme”*, *“yayma”*, ve *“ele geçirme”* hukuka uygun olacaktır. Hukuka uygun olduğu için de haliyle TCK m. 135 ve 136’daki suçlar oluşmayacaktır. Kısacası, KVKK m. 5 ve 6’daki haller, hem TCK m. 135 için hem de TCK m. 136 için hukuka uygunluk nedenleridir⁷¹¹. Söz konusu hallerin olması durumunda ne *“kişisel verilerin kaydedilmesi suçu”* ne de *“verileri hukuka aykırı olarak verme ya da ele geçirme suçu”* vücut bulacaktır.

Fail, verileri kaydetme suçundan sonra bu suçu işleyebilir. Yani kişi hukuka aykırı olarak kaydettiği veriyi, örneğin, 3. bir kişiye verebilir. Bu durumda hem TCK m. 135 hem de 136 suçu işlenmiş olacaktır. Burada gerçek içtima hükümleri uygulanmalıdır.

⁷⁰⁸ Artuç, s. 1645.

⁷⁰⁹ Hafizoğulları /Özen, s. 287.

⁷¹⁰ Yılmaz, s. 133.

⁷¹¹ Dülger, Ceza Normlarıyla Korunma, s. 145.

Yani iki suçtan da ceza verilebilecektir⁷¹². Yargıtay'ın da verdiği kararlarda bu görüşte olduğu görülmektedir.

Bazı durumlarda tek bir fiil ile birden fazla suç oluşabilir. TCK “fikri içtima” başlıklı 44. maddesine göre, “İşlediği bir fiil ile birden fazla farklı suçun oluşmasına sebebiyet veren kişi, bunlardan en ağır cezayı gerektiren suçtan dolayı cezalandırılır.” Yargıtay kararları incelendiğinde tek bir fiille hem “özel hayatın gizliliğini ihlal”⁷¹³, “hakaret”⁷¹⁴ hem de “verileri hukuka aykırı olarak verme veya ele geçirme” suçlarının

⁷¹² Artuç, s. 1634.

⁷¹³ “Sanık tarafından mağdureye ait kişisel veri niteliğindeki resimlerin rızası dahilinde çekilerek aktarıldığı hafıza kartının kaybedilmesinin ardından söz konusu kartı bulan sanık ...dan aldıkları karttaki resimleri hukuka aykırı şekilde temin eden sanıklar ... ile ...nin eylemlerinin hem özel hayatın gizliliğini ihlal hem de verileri hukuka aykırı olarak verme veya ele geçirme suçlarını oluşturup, 5237 Sayılı TCK'nın 44. maddesinde düzenlenen fikri içtima kuralı gereğince daha ağır yaptırım içeren aynı Kanunun 136. maddesinde düzenlenen suçu oluşturduğu gözetilerek hükümler kurulması gerekir.” Yargıtay 14. CD., 24.12.2019 T., 2019/5596 E., 2019/13580 K. (Kazancı, E.T.: 24.04.2020).

⁷¹⁴ “İkrar içeren savunmaya ve dosya kapsamına göre; eşinin kardeşi olan diğer sanık ...in şifresini bildiği facebook hesabından aralarında husumet bulunan katılanın cep telefonu numarasını, -05..... Selam beyler sorun yok isteyen beylere her zaman hizmet veririm, ister zevkine ister ücretli farketmez, yeterki beni mutlu edin, doyurun, kalacak yerim yok ama- şeklindeki ifadeler ile paylaşılan sanığın sübut bulan eylemlerinin, katılanın kişisel veri niteliğindeki cep telefonu numarasını rızası dışında paylaşması nedeniyle TCK'nın 136/1. madde ve fıkrasında düzenlenen verileri hukuka aykırı olarak verme veya ele geçirme suçu ile birlikte katılanın para karşılığı cinsel ilişki yaşadığı

oluştugu örnekler görülmektedir. Yargıtay'a göre böyle bir durumda TCK m. 44 gereği sadece cezası daha ağır olan suçtan ceza verilmelidir.

TCK m. 139 gereği bu suç da resen takip edilen bir suçtur.

Ayrıca bu suç da *salt hareket suçudur*. Hükümde yer alan hareketlerden birinin gerçekleşmesi ile suç tamamlanacaktır. Kişisel verileri kaydetme suçunda yaptığımız açıklamalar burada da geçerlidir. Yani bu suç da bir *soyut tehlike suçudur*⁷¹⁵. Hükümde belirtilen 3 hareketten biri gerçekleştiğinde suç tamamlanacağından, illaki zarar olması gerekmemektedir⁷¹⁶.

izlenimi oluşturmaları nedeniyle de TCK'nın 125/2. madde ve fıkrasında düzenlenen hakaret suçunun da oluştuğu, bir fiili ile birden fazla farklı suçun oluşmasına neden olan sanığın, TCK'nın 44. maddesi gereğince, daha ağır cezayı gerektiren verileri hukuka aykırı olarak verme veya ele geçirme suçundan cezalandırılması, hakaret suçundan ise hüküm kurulmasına yer olmadığına karar verilmesi gerekir.” Yargıtay 12. CD., 21.06.2018 T., 2018/1250 E., 2018/7024 K. Benzer yönde kararlar için bkz. Yargıtay 12. CD., 13.11.2019 T., 2019/532 E., 2019/10827 K., Yargıtay CGK., 09.05.2019 T., 2015/12-708 E., 2019/414 K., Yargıtay 12. CD., 27.02.2019 T., 2018/8087 E., 2019/2692 K., Yargıtay 12. CD., 24.01.2018 T., 2017/1357 E., 2018/834 K., Yargıtay 12. CD., 23.10.2017 T., 2016/10995 E., 2017/7760 K., Yargıtay 12. CD., 23.10.2017 T., 2016/10893 E., 2017/7762 K. (Kazancı, E.T.: 25.04.2020).

⁷¹⁵ Yargıtay CGK., 09.05.2019 T., 2015/12-708 E., 2019/414 K., Yargıtay CGK., 17.06.2014 T., 2012/12-1510 E., 2014/331 K. (Kazancı, E.T.: 25.04.2020).

⁷¹⁶ **Özbek/Doğan/Bacaksız**, s. 598.

Kurul, “Bir şirket sahibinin, çalışanının Whatsapp yazışmalarını hukuka aykırı olarak elde etmesi” konulu kararında⁷¹⁷, başvurunun TCK (m. 136) çerçevesinde değerlendirilmesi gerektiğini belirtmiştir. Bu konu KVKK m. 15/2 gereği “yargı mercilerinin görevine giren konulara ilişkin” olduğundan Kurul tarafından somut olayın TCK çerçevesinde yürütülmesi tespiti yapılmakla yetinilmiştir.

Şimdi TCK m. 136 suçunun oluştuğu birkaç somut örnek verelim. Vereceğimiz örnekler, adı üstünde sadece örnek niteliğindedir. Yoksa bu suçun oluşmasına kişisel verilerin hepsi sebep olabilir. Yine kişisel verinin yayıldığı veya ele geçirdiği ortamın da suçun oluşması açısından önemi bulunmamaktadır. Suçun özellikle internet üzerinde işlendiği görülmektedir. Ancak tabii ki bu şart değildir. Yargıtay kararları incelendiğinde, özellikle başkasına ait cep telefonu numarası veya fotoğraf gibi kişisel verilerin internette yayımlanması durumunda TCK m. 136 suçunun oluştuğu somut durumların sıklığı dikkat çekmiştir⁷¹⁸. Sosyal medya kullanımının bu denli arttığı günümüzde, yargı kararlarına

⁷¹⁷ **Kurul Kararı**, 16.05.2019 T., 2019/138 K. <https://kvkk.gov.tr/Icerik/6708/2019-138> (E.T.: 24.04.2020). Kurul başka bir kararda da olayı TCK kapsamında değerlendirmiştir.

“İlgili kişinin tarafına ait borç bilgilerinin rızası ve bilgisi dışında üçüncü kişilerle paylaşıldığı iddiası, sair mevzuat kapsamında hukuka aykırı bir fiil olduğundan ve bu fiiller Bankacılık Kanunu ve Türk Ceza Kanununun ilgili hükümlerinde de düzenlenmiş olduğundan, ilgili Banka ve personel hakkında Bankacılık Kanunu ve Türk Ceza Kanunu kapsamında işlem tesis edilmesi hususunun değerlendirilmesini teminen konunun Bankacılık Düzenleme ve Denetleme Kurumuna intikal ettirilmesine karar verilmiştir.”

Kurul Kararı, 16.01.2020 T., 2020/43 K. <https://kvkk.gov.tr/Icerik/6715/2020-43> (E.T.: 24.04.2020).

⁷¹⁸ “Dosya kapsamına göre; ... sanığın, görev yaptığı birimdeki bilgisayarını kullanarak, bir arkadaşlık sitesinde oluşturduğu ... isimli profil üzerinden, yaklaşık iki yıl önce bir

yansıyan olayların da sosyal medya vesilesiyle olmasına şaşırmmamak gerekir.

IV. Verileri Yok Etmeme Suçu

TCK m. 138/1'e göre *“Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde bir yıldan iki yıla kadar hapis cezası verilir.”* KVKK'da belirtilen temel ilkelerden biri gerekli süre kadar muhafaza edilmesi ilkesidir. TCK m. 138'in söz konusu temel ilkenin uzantısı olduğu söylenebilir. Ayrıca bu suç, unutulma hakkı ile de bağlantılıdır. Yani bu suç kişinin unutulma hakkını koruma altına almaktadır⁷¹⁹. Zira çok uzun süre geçmesine karşın kişisel verinin işlenmeye devam edilmesi unutulma hakkıyla bağdaşmayacaktır.

Suçun faili yalnızca *“ verileri yok etmekle yükümlü olan kişi ”* olabileceğinden, bu suç özgü suçtur⁷²⁰. Suçun faili kamu görevlisi olabileceği gibi kamu görevlisi olmayan

konuda tartışmalarından dolayı kızgın olduğunu ifade ettiği ... mağdura ait kişisel veri niteliğindeki cep telefonu numaralarını, mağdurun bilgisi ve rızası dışında, başkalarına yayması biçiminde sübut bulan eyleminin verileri hukuka aykırı olarak verme veya ele geçirme suçunu oluşturduğuna dair yerel mahkemenin kabulünde bir isabetsizlik görülmemiştir.” Yargıtay 12. CD., 26.06.2019 T., 2018/8312 E., 2019/7735 K. Benzer yönde kararlar için bkz., Yargıtay 12. CD., 19.06.2019 T., 2018/8331 E., 2019/7459 K., Yargıtay 12. CD., 11.09.2019 T., 2018/8381 E., 2019/8629 K., Yargıtay 12. CD., 10.07.2019 T., 2018/8369 E., 2019/8318 K., Yargıtay 12. CD., 10.07.2019 T., 2018/8327 E., 2019/8315 K., Yargıtay 12. CD., 15.05.2019 T., 2018/8198 E., 2019/6187 K., Yargıtay 12. CD., 24.04.2019 T., 2019/3534 E., 2019/5452 K., Yargıtay 18. CD., 13.02.2019 T., 2016/12443 E., 2019/2912 K., (Kazancı, E.T.: 25.04.2020).,

⁷¹⁹ **Yokuş Sevük**, s. 286.

⁷²⁰ **Ketizmen**, s. 204.

da olabilir⁷²¹. Ancak burada dikkat etmek gerekir ki kamu görevlisi olmak cezayı arttırmayacaktır⁷²². Zira TCK 137 “*nitelikli haller*” maddesi 135 ve 136. Maddedeki suçlar için geçerliyken 138. maddedeki suç için geçerli değildir.

TCK’da yalnızca sürenin geçmesi hali suç olarak belirlenmiştir. Ayrıca sadece “*yok etme*” ibaresi yer almıştır. Ancak sadece sürenin geçmesi göz önüne alınmamalıdır. Zira KVKK m. 7’de “*KVKK ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel verilerin resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silineceği, yok edileceği veya anonim hâle getirileceği*” düzenlenmiştir. Kişisel veriler KVKK m. 5 ve 6’daki şartlara riayet edilerek hukuka uygun olarak işlenmiş olabilir. Ancak işleme şartlarının ortadan kalkması hukuka uygun durumu bozacaktır. Bu durumda da veri sorumlusunun, verileri; silme, yok etme ve anonimleştirme zorunluluğu doğacaktır. Bunu öngören kanun koyucu TCK’ya atıf yapmıştır. KVKK’nın 17. maddesinde bu suça atıf yapıldığı görülmektedir. Buna göre “*KVKK m.7’ye aykırı olarak, kişisel verileri silmeyen veya anonim hale getirmeyenler TCK m. 138’e göre cezalandırılırlar.*” Sonuç olarak, veri sorumlusu, kişisel veri işleme şartları ortadan kalktığında “*kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesi*” yükümlülüğü yerine getirmezse TCK m. 138 kapsamında cezalandırılacaktır. Bu atıfla birlikte, suçun oluşumu için sadece sürenin geçmesi değil, veri işleme şartının ortadan kalkması halinde imha edilmemesi de yeterli olacaktır. Örneğin kişinin rızasına dayanılarak veri işlenmiş olsun. Kişi tarafından rıza geri alındığında veri işleme nedeni ortadan kalkmış olacaktır. Kişi bu durumda KVKK m. 11/1/e uyarınca veri sorumlusundan verisinin silinmesini talep etmiş olsun. Bu durumda veri sorumlusunun KVKK m. 7 gereği kişisel veriyi silmesi gerekecektir. Aksi

⁷²¹ **Hafızoğulları /Özen,** s. 292; **Yokuş Sevük,** s. 287.

⁷²² **Artuç,** s. 1686.

halde TCK m. 138 kapsamında cezalandırılması söz konusu olabilecektir.

TCK m. 135 ve 136'daki suçlar icrai hareketle işlenebilir. Ancak bu suç (TCK m. 138) yalnızca ihmal hareketiyle işlenebilir⁷²³. TCK m. 138'de “*yok etmekle yükümlü olanlar*” ibaresi yer almıştır. Böyle bir yükümlülüğü bulunmayanlar bu suçu işleyemeyecektir. Süre geçtikten sonra yok etme yükümlülüğünün yerine getirilmesi ise suçun oluşmasını engellemeyecektir⁷²⁴.

Suçun tamamlanması için zarar doğması şart değildir. Bu nedenle bu suç zarar suçu değildir. Sadece bazı durumlarda kişisel verilerin yok edilmemesi yeterlidir. Bu nedenle yukarıdaki diğer suçlar gibi bu suç da *soyut tehlike suçudur*⁷²⁵.

TCK m. 139 gereği bu suç da şikayete bağlı değildir. Yani resen takip edilen bir suçtur.

Hükümde yer alan “*sistem içinde*” ifadesi otomatik işleme çağrışımı yapmaktadır. Diğer iki suçta otomatik-olmayan işleme ayrımı yapılmazken bu suçta yapılacak olması hükümler arasında bir çelişki yaratır. TCK m. 138 ve TCK m. 135-136 arasında uyumun sağlanabilmesi için “*sistem içinde*” ifadesinin hükümden çıkarılması yerinde olacaktır⁷²⁶.

TCK m. 138/2'ye göre, “*Suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması hâlinde verilecek ceza bir kat artırılır.*” Hükme göre CMK kapsamında yok edilmesi gerekip, edilmeyen veri söz konusu olduğunda ceza arttırılacaktır. Bu hususa CMK m. 80/2, 81/2, 135/3, 139/6 ve 140/4 hükümleri örnek olarak verilebilir.

⁷²³ **Bük, Alaattin**, Bilişim Alanında Kişisel Verilerin Korunması, Ankara 2018, s. 104; **Ketizmen**, s. 204.

⁷²⁴ **Hafizoğulları /Özen**, s. 292.

⁷²⁵ **Dülger**, Ceza Normlarıyla Korunma, s. 135; **Özbek/Doğan/Bacaksız**, s. 603.

⁷²⁶ **Ketizmen**, s. 242.

SONUÇ

Kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade eder. Bu tanım hem ulusal mevzuatımızda hem de uluslararası düzenlemelerde kabul görmektedir. Kişisel verinin; bilgi, kimliği belirli veya belirlenebilir kişi ve bilginin kişiye ilişkin olması olmak üzere üç unsuru vardır. İşte bu üç unsurun bir arada olması koşuluyla bir bilgi, kişisel veri sayılabilir ve korumalardan yararlanabilir. Kişiyi doğrudan belirli kılan bilgiler kişisel veri sayıldığı gibi direkt olarak kişiyi belirlemese de belirlenebilir kılan bilgiler de kişisel veri sayılmaktadır. Alenileştirilen bilgi ya da doğru olmayan bilgi de kişisel veridir. Uluslararası düzenlemelerde olduğu gibi, KVKK da kişisel veri tanımına yalnızca gerçek kişilere ilişkin bilgileri almıştır. Başka bir ifadeyle, gerçek kişilerin bilgileri KVKK korumasına dahilken, tüzel kişilerin bilgileri kişisel verilerin korunmasına dahil değildir. Sağ doğmak koşuluyla, ceninin bilgileri de kişisel verilerin korunmasına dahildir. Ölüm ile birlikte kişilik sona ereceğinden ölümlere ilişkin bilgiler kişisel verilerin korunmasına dahil değildir. Ancak ölüye ilişkin bilgi, yaşayan bir kişiyle ilişkilendirilebiliyorsa o zaman veri koruma kapsamına girecektir. Kişinin mahlası (takma ad) ya da lakabı direkt olarak ya da başka verilerle birleşerek kişi tanımlanabiliyorsa söz konusu mahlas ve lakap kişisel veri kabul edilir. Anonim hale getirilmiş bir veri ise kişisel veri değildir. Bir bilginin kişiyle ilişkili olup olmadığı; içerik, amaç veya sonuç olarak üç unsurun varlığına bağlı olarak tespit edilebilir.

Yapısı gereği hassas olduğu düşünülen kişisel veriler özel nitelikli kişisel verilerdir. KVKK tarafından özel nitelikli kişisel veriler 6. maddede sınırlı sayma yoluyla belirlenmiştir ve genişletilemez. KVKK m. 6/1’de sayılmayan her türlü veri, özel nitelikli olmayan (genel nitelikli) kişisel veri sayılacaktır.

Kişisel verinin temelinde kişilik hakkı bulunmaktadır. Ancak bu salt özel hayatın gizliliği veya mahremiyetle bağdaştırılmamalıdır. Kişisel verinin temelindeki hak, Alman

Anayasa Mahkemesi'nin nüfus sayımı kararında da belirtildiği gibi, *“bireyin kişisel verilerinin geleceğini belirleme hakkı”*dır. Bu kararda mahkeme, isabetli olarak, kişisel verilerin korunması hakkını, insan onuruyla ve kişinin varlığını geliştirme hakkıyla ilişkilendirerek kişilik hakkının bir biçimi olarak belirlemiştir.

Dünya tarihinde kişisel verilerin korunması, ilk olarak Almanya'nın Hessen eyaletinde 1970 yılında kabul edilen Veri Koruma Kanunu (*“Hessisches Datenschutzgesetz”*) ile düzenlenmiştir. Bu tarihlerde çeşitli ülkelerde kişisel verilerin korunması ile ilgili ulusal düzenlemeler yapılmaya başlanmıştır. Daha sonra OECD, AK, AB ve BM tarafından yapılan düzenlemelerle Kişisel Verilerin Korunması Hukuku'nun temelleri atılmıştır. Bu kapsamda, KVKK hazırlanırken temel alınan 95/46/EC sayılı AB Direktifi ve bu direktifin revize edilen hali olan GDPR düzenlemeleri önem teşkil etmektedir. Ülkemizde ilk olarak 2004 tarihli TCK'da kişisel verilere ilişkin suçlara yer verilmiştir. Anayasamızda 2010 yılında yapılan değişiklikle “kişisel verilerin korunması hakkı” anayasal güvence altına alınmıştır. Bu alana has bir kanun olan 6698 sayılı Kişisel Verilerin Korunması Kanunu ise 07.04.2016 tarihinde yürürlüğe girmiştir.

KVKK'nın kişi bakımından kapsamına yalnızca gerçek kişiler girmekte, tüzel kişilere ait bilgiler KVKK korumasından yararlanamamaktadır. Kişisel verisi işlenen ilgili kişi, gerçek kişidir. Veri işleyen ve veri sorumlusu ise gerçek kişi olabileceği gibi tüzel kişi de olabilir. KVKK'nın konu bakımından kapsamını ise tamamen veya kısmen otomatik yolla işleme ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yolla işleme oluşturmaktadır. Herhangi bir veri kayıt sisteminin parçası olmayan otomatik olmayan yolla işleme ise kanunun kapsamı dışında kalmaktadır. KVKK m. 28/1'de sayılan haller tamamen kanun kapsamına girmeyen hallerdir. Bu haller tam istisna olarak değerlendirildiğinden söz konusu hallerde KVKK'nın hiçbir hükmü uygulanmayacaktır. KVKK m. 28/2'deki haller ise kısmen kanun kapsamına girmeyen hallerdir. Bu hallerin söz konusu olması halinde KVKK m. 10, 11 (zararın giderilmesini

talep hakkı hariç) ve 16. maddeleri uygulanmayacak, bunlar dışındaki maddeler ise uygulanmaya devam edecektir.

Veri sorumlusu, kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen gerçek veya tüzel kişidir. Başka bir ifadeyle, veri sorumlusu, veri işleme faaliyetinin neden ve nasıl olacağına karar veren kişidir. Tüzel kişilerde veri sorumlusu doğrudan tüzel kişiliğin kendisidir. Tüzel kişinin organları, çalışanları, şubesi, birimleri veri sorumlusu olmayıp; şirket tüzel kişiliği veri sorumlusudur. Bu nedenle KVKK kapsamında sorumluluk şirket tüzel kişiliğinin kendisindedir. Veri işleyen, veri sorumlusunun verdiği yetkiye dayanarak veri sorumlusu adına veri işleyen gerçek veya tüzel kişidir. Veri işleyen, mutlaka veri sorumlusu organizasyonu dışındaki bir 3. kişi olmalıdır. Şirketin işçileri, çalışanları veya şirketin veri işleyen birimleri veri işleyen olarak nitelendirilmemektedir. Kişisel veri işleme sözleşmesi, veri işleme konusunda veri sorumlusunun veri işleyeni yetkilendirdiği sözleşmedir.

Kişisel verilerin işlenmesi, veriler üzerinde gerçekleştirilen her türlü işlemi ifade eder. Kişisel verilerin işlenmesi sayılacak işlemler KVKK m. 3/1/e’de örnekleme yoluyla sayılmıştır. Maddede sayılmayan, veriler üzerinde gerçekleştirilen başka bir işlem de kişisel verilerin işlenmesi addedilecektir. Kişisel verilerin hukuka uygun olarak işlenebilmesi için KVKK m. 4’de sayılan kişisel verilerin işlenmesindeki genel ilkelere veri işleme faaliyetinin her aşamasında uyulması gerekmektedir. Aksi halde söz konusu veri işleme hukuka aykırı bir hal alacaktır. “*Kişisel verilerin işlenmesinde genel ilkeler*”in Kişisel Verilerin Korunması Hukuku için önemini TMK “*Başlangıç Hükümleri*”nin önemine benzetebiliriz. Veri işleme faaliyetinin her safhasında riayet edilmesi gereken temel ilkeler; “*hukuka ve dürüstlük kuralına uygun olma ilkesi*”, “*doğru ve gerektiğinde güncel olma ilkesi*”, “*belirli, açık ve meşru amaçlar için işlenme ilkesi*”, “*amaçla bağlantılı, sınırlı ve ölçülü olma ilkesi*” ve “*belirli ve sınırlı süre muhafaza edilme ilkesi*” olarak sıralanabilir.

Kişisel verilerin işlenebilmesi için genel nitelikteki kişisel veriler için KVKK m. 5, özel nitelikteki kişisel veriler için ise KVKK m. 6'daki kişisel verileri işleme şartlarından en az birisinin bulunması gerekmektedir. Aksi halde veri işleme faaliyeti hukuka aykırı olacaktır. Kişisel verileri işleme şartları yani hukuka uygunluk sebeplerinden birisi açık rızadır. Açık rıza; belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanan rızadır. Açık rızadan söz edebilmek için ilgili kişinin aktif bir hareketi olmalıdır. İlgili kişinin sessiz kaldığı durumlarda açık rızadan söz edilemez. Başka bir ifadeyle, kişisel verilerin açık rızaya dayanılarak işlenebilmesi için zımni irade beyanı yeterli değildir. Bu kapsamda, internet sitelerindeki önceden işaretlenmiş kutucuklar açık rıza verildiği anlamına gelmez. Açık rızanın verilmesinde herhangi bir şekil şartı bulunmamaktadır. Açık rızanın alındığını ispatlayacak olan veri sorumlusudur. İlgili kişinin açık rızası kişisel veri işlenmeye başlanmadan önce alınmalıdır. Açık rıza beyanında bulunan ilgili kişi, sonradan bu beyanını geri alabilir. Kişisel veriler işlenirken ilk bakılması gereken açık rıza dışındaki şartlardır. Kişisel veriler işlenirken açık rıza dışındaki başka bir sebebe dayanılabilecekken açık rızaya dayanılması, hakkın kötüye kullanımı anlamına gelecek, ve temel ilkelerden olan hukuka ve dürüstlük kuralına uygun işlemeye aykırı olacaktır. Kişisel verileri işleme şartlarının ortadan kalması halinde KVKK m. 7/1 uyarınca kişisel veriler veri sorumlusu tarafından silinir, yok edilir veya anonim hale getirilir. Kişisel verilerin yurt içinde aktarımında KVKK m. 8' da belirtilen şartlara, kişisel verilerin yurt dışına aktarımında ise KVKK m. 9'da belirtilen şartlara riayet edilmesi gerekmektedir.

Veri sorumlusunun ilgili kişiyi aydınlatma yükümlülüğü bulunmaktadır. Veri sorumlusunun bir diğer yükümlülüğü veri güvenliğine ilişkin yükümlülüktür. Bu kapsamda, veri sorumlusunun teknik ve idari tedbirleri alma yükümlülüğü, denetim yükümlülüğü, sır saklama yükümlülüğü ve Kurul'a bildirim yükümlülüğü bulunmaktadır. Veri sorumlusu açısından bir başka yükümlülük, Veri Sorumluları Sicili'ne kayıt

yükümlülüğüdür. Bu bağlamda, sicile kayıtla yükümlü olan veri sorumlusunun Kişisel Veri İşleme Envanteri hazırlaması gerekmektedir.

İlgili kişinin veri sorumlusuna başvurarak kullanabileceği hakları KVKK m. 11’de sayılmıştır. Bu kapsamda, ilgili kişinin, işlenen kişisel veri ile ilgili öğrenme ve bilgi talep etme hakkı bulunmaktadır. İlgili kişi, kişisel verilerinin düzeltilmesini, silinmesini veya yok edilmesini isteme hakkına sahiptir. İlgili kişiden toplanan verilerin özellikle otomatik sistemlerle incelenmesi sonucunda kişi ile ilgili olumsuz bir durumun söz konusu olması durumunda, ilgili kişinin itiraz etme hakkı vardır. İlgili kişi, kişisel verilerin hukuka aykırı olarak işlenmesi sonucunda bir zarara uğramışsa, zararın giderilmesini talep etme hakkına sahiptir. Ayrıca ilgili kişilere, kişisel verilerinin etkin bir şekilde korunmasının sağlanması amacıyla, veri sorumlusuna başvuru ve Kurul’a şikayet hakkı verilmiştir. Veri sorumlusuna başvuru yoluna gidilmeden Kurul’a şikayet yoluna gidilemez.

Kişisel verilerin korunması yolları KVKK’dan ibaret değildir. Kişisel verisi hukuka aykırı olarak işlenen ilgili kişi KVKK’daki koruma yollarına başvurabileceği gibi, KVKK dışındaki koruma yollarına da gidebilir. Bu bağlamda, kişisel verilerin korunması salt Kişisel Verilerin Korunması Hukuku’na indirgenmemeli, Ceza Hukuku, Medeni Hukuk, Borçlar Hukuku, İş Hukuku, Anayasa Hukuku ve İdare Hukuku gibi hukuk alanlarıyla birlikte değerlendirilmelidir. Zira kişisel verilerin korunması birçok hukuk alanıyla ilişkilidir. Ayrıca KVKK dışındaki kanunlar da kişisel verilerle ilgili hükümler içermektedir.

İş ilişkisinde, işçi, işverene bağımlı olarak, işverenin talimatları kapsamında iş görmektedir. İş ilişkisindeki bu narin yapı sebebiyle iş ilişkisinde kişisel verilerin korunmasına özel önem gösterilmelidir. Özellikle kişisel verinin işlenmesinde işçinin açık rızasına dayanılması durumunda, işçinin rızasının özgür iradeyle açıklanıp açıklanmadığı dikkatle incelenmelidir. Nitekim özgür iradeye dayanmayan rıza beyanı

açık rıza olarak nitelendirilemeyeceğinden veri işleme faaliyeti hukuka aykırı olacaktır. İşçinin kişisel verilerinin korunması, işverenin, işçinin kişiliğini gözetme borcunun bir uzantısı olarak değerlendirilmektedir. Kişisel verilerin işverence hukuka aykırı olarak işlenmesi, işçiyi gözetme borcunun yerine getirilmemesine sebep olacaktır. İK m. 75/2 gereği işveren, işçinin bilgilerini hukuka ve dürüstlük kuralına uygun olarak kullanmakla yükümlüdür. Bu yükümlülüğe riayet edilmemesi halinde, işçi, İK m. 24/2'ye dayanarak iş sözleşmesini haklı nedenle feshedebilir. Aynı zamanda işçi genel hükümler uyarınca tazminat talep etme hakkına sahiptir.

Kişisel veriler, temelinde bir kişilik hakkı olduğundan, kişisel verilerin korunmasında TMK m. 23, 24, 25'e yani kişiliğin korunmasına ilişkin hükümlere dayanılabilecektir. KVKK m. 14/3 gereği kişilik hakları ihlal edilenler, genel hükümlere göre tazminat talep edebilecektir. Hükümde bahsi geçen genel hükümler TMK ve TBK hükümleridir. Kişisel verilerin hukuki işlemle gerçekleştirilen saldırılara karşı korunması TMK m. 23 çerçevesinde sağlanır. Kişisel verilerin hukuka aykırı fiille gerçekleştirilen saldırılara karşı korunması ise TMK m.24 ve 25 çerçevesinde sağlanır. Kişisel verilerin hukuka aykırı olarak işlenmesi durumunda, ilgili kişi, TMK m. 24 korumasından yararlanabilecektir. Bu kişi aynı zamanda TMK m. 25'de düzenlenen davaları da açabilecektir.

KVKK m. 17 atfı gereği kişisel verilere ilişkin suçlarda TCK m. 135-140 arasındaki hükümler uygulanacaktır.

KAYNAKÇA

- Akdağ, Hale**, Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması, Ankara 2013.
- Akgül, Aydın**, “*Kişisel Verilerin Korunmasında Yeni Bir Hak: Unutulma Hakkı ve AB Adalet Divanı’nın Google Kararı*”, TBB Dergisi, 2015, Y. 27, S. 116, s. 11-38.
- Akıncı, Ayşe Nur**, “*Avrupa Birliği Genel Veri Koruma Tüzüğü’ nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi*”, Çalışma Raporu 6, T.C. Kalkınma Bakanlığı Yayın No: 2968, 2017. (Anılışı: AB Tüzüğü).
- Akıncı, Ayşe Nur**, Büyük Veri Uygulamalarında Kişisel Veri Mahremiyeti, Uzmanlık Tezi, T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı, Yayın No: 0001, Ankara 2019. (Anılışı: Veri Mahremiyeti).
- Akıntürk, Turgut/Ateş, Derya**, Medeni Hukuk, 25. Baskı, İstanbul 2019.
- Akipek, Jale/Akıntürk Turgut/Ateş, Derya**, Eşya Hukuku, 2. Baskı, İstanbul 2018.
- Akkurt, Sinan Sami**, “*17.06.2015 Tarih, E. 2014/4-56, K. 2015/1679 Sayılı Yargıtay Hukuk Genel Kurulu Kararı ve Mukayeseli Hukuk Çerçevesinde Unutulma Hakkı*”, AÜHFD, 2016, C. 65, S. 4, s. 2605-2635.
- Aksoy, Hüseyin Can**, “*Kişisel Verilerin İşlenmesi Kapsamında Rıza Unsuru ve Sınırlı Ehliyetsizlerin Durumu*”, Haluk Konuralp Anısına Armağan, C. 3, Ankara 2009, s. 47-68. (Anılışı: Rıza)
- Aksoy, Hüseyin Can**, Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması, Ankara 2010. (Anılışı: Kişisel Veri).
- Aksoy, Hüseyin Can**, “*The Right to Personality and Its Different Manifestations as the Core of Personal Data*”, Ankara Law Review, 2008, C. 5, S. 2, s. 235-249. (Anılışı: Personal Data).
- Altaş, Hüseyin**, Medeni Hukuk Başlangıç Hükümleri, Ankara 2018.

- Antalya, O. Gökhan**, Borçlar Hukuku Genel Hükümler, C. V/1, 1, Genişletilmiş 2. Baskı, Ankara 2019.
- Antalya, O. Gökhan**, Borçlar Hukuku Genel Hükümler, C. V/1, 2, Genişletilmiş 2. Baskı, Ankara 2019. (Anılışı: Borçlar 2).
- Antalya, O. Gökhan**, “*Manevi Zararın Belirlenmesi ve Manevi Tazminatın Hesaplanması-Türk Hukukuna Manevi Zararın İki Aşamalı Olarak Belirlenmesine İlişkin Bir Model Önerisi*”, MÜHF-HAD, 2016, C. 22, S. 3, s. 221-250.
- Antalya, O. Gökhan/Topuz, Murat**, Eşya Hukuku, C. IV/1, Genişletilmiş 3. Baskı, Ankara 2019.
- Antalya, O. Gökhan/ Topuz, Murat**, Medeni Hukuk C. I, Genişletilmiş 3. Baskı, Ankara 2019.
- Arbek, Ömer**, Fikir ve Sanat Eserlerine İlişkin Lisans Sözleşmesi, Ankara 2005.
- Arpacı, Abdülkadir**, Kişiler Hukuku (Gerçek Kişiler), Gözden Geçirilmiş ve Genişletilmiş 2. Bası, İstanbul 2000.
- Arslan, Ramazan/Yılmaz, Ejder/Taşpınar Ayvaz, Sema/Hanağası, Emel**, Medeni Usul Hukuku, 5. Baskı, Ankara 2019, s. 228.
- Artuç, Mustafa**, Kişilere Karşı Suçlar, Genişletilmiş ve Güncellenmiş 2. Baskı, Ankara 2018.
- Atasoy, Kemal**, “*Kişilik Hakkı Kapsamında Sosyal Medyada Kişisel Verilerin Korunması ve Veri Sahibinin Rızası*”, MÜHF-HAD, 2016, C. 22, S. 3, s. 269-301.
- Ayan, Mehmet**, Borçlar Hukuku Genel Hükümler, Gözden Geçirilmiş 11. Baskı, Ankara, 2016.
- Ayan, Mehmet**, Eşya Hukuku-II-Mülkiyet, Güncelleştirilmiş 9.Baskı, Ankara, 2016.
- Ayan, Mehmet/Ayan Nurşen**, Kişiler Hukuku, Gözden Geçirilmiş 8. Baskı, Ankara 2016.

Aydın Ünver, Tülay, Ceninin Hukuki Konumu, İstanbul 2011.

Ayözger Öngün, Çiğdem, Kişisel Verilerin Korunması Hukuku (Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil), Genişletilmiş 2. Baskı, İstanbul 2019.

Bartow, Ann, “*Our Data, Ourselves: Privacy, Propertization and Gender*”, University of San Francisco Law Review, 2000, C. 34, s. 633-704.

Başalp, Nilgün, “*Avrupa Birliği Veri Koruması Genel Regülasyonu’nun Temel Yenilikleri*”, MÜHF-HAD, 2015, C. 21, S. 1, s. 77-105. (Anılışı: AB Regülasyonu).

Başalp, Nilgün, Kişisel Verilerin Korunması ve Saklanması, Ankara 2004. (Anılışı: Kişisel Veri).

Baykal, Sanem/Göçmen, İlke, “*Avrupa Birliği Hukukunun Kaynakları Bakımından Normlar Hiyerarşisi*”, Prof. Dr. Erdal Onar’a Armağan, C. I, Ankara 2013, s. 317-365.

Belge, Ayşe Merve, “*Özellikle Kişisel Verilerin Korunması Kanunu Çerçevesinde İşçilerin Kişisel Verilerinin İhlali ve Korunması Yolları*”, DEÜHFD, 2017, Prof. Dr. Şeref ERTAŞ’ a Armağan, C. 19, Özel Sayı, s. 1025-1051.

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 Report, 2002, C. 18, S. 1, s. 31-47.

Bibas, Steven A., “*A Contractual Approach to Data Privacy*”, Harvard Journal of Law & Public Policy, 1994, C. 17, S. 2, s. 591-611.

Bilir, Faruk, “*Kişisel Verilerin Korunması Kanununa Genel Bir Bakış*”, İnşaat Sanayi Dergisi, 2018, S.165, s. 62-67.

Bulut, Harun, Kişilik Hakları ve Kişilik Haklarına Saldırıdan Kaynaklanan Hukuk Davaları, İstanbul 2006.

- Bük, Alaattin**, Bilişim Alanında Kişisel Verilerin Korunması, Ankara 2018.
- Büyüksağış, Erdem**, Yeni Sosyo-Ekonomik Boyutuyla Maddi Zarar Kavramı, İstanbul 2007.
- Bygrave, Lee A.**, “*Data Protection Pursuant to the Right to Privacy in Human Rights Treaties*”, International Journal of Law and Information Technology, 1998, C. 6, S. 3, s. 247-284.
- Cate, Fred H.**, “*The Changing Face of Privacy Protection in the European Union and The United States*”, Indiana Law Review, 1999, C. 33, s. 173-232.
- Çekin, Mesut Serdar**, “6698 Sayılı Kişisel Verilerin Korunması Hakkına Kanun’un Big Data (Büyük Veri) ve İrade Serbestisi Açısından Değerlendirilmesi”, İÜHFM, 2016, C. 74, S. 2, s. 629-644. (Anılışı : İrade Serbestisi).
- Çekin, Mesut Serdar**, Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku, 2.Baskı, İstanbul 2019. (Anılışı: Kişisel Veri).
- Çelik, Aytekin**, Ticaret Hukuku, Güncellenmiş 8. Baskı, Ankara 2018.
- Dural, Mustafa/Öğüz, Tufan**, Türk Özel Hukuku-Kişiler Hukuku, C.II, 20. Baskı, İstanbul 2019.
- Dülger, Murat Volkan**, Kişisel Verilerin Korunması Hukuku, 2. Baskı, İstanbul 2019. (Anılışı: Kişisel Veri).
- Dülger, Murat Volkan**, “*Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması*”, İMÜHFD, 2016, C.3, S.2, s. 101-167. (Anılışı: Ceza Normlarıyla Korunma).
- Eren, Fikret**, Borçlar Hukuku Genel Hükümler, 22. Baskı, Ankara 2017.
- Erlüle, Fulya**, Türk Borçlar Kanunu’na Göre Bedensel Bütünlüğün İhlalinde Manevi Tazminat, Gözden Geçirilmiş 2. Baskı, Ankara 2015.
- Ertaş, Şeref**, Eşya Hukuku, Gözden Geçirilmiş ve Genişletilmiş 14. Baskı, İzmir 2018.

- Feyzioğlu, Feyzi Necmeddin**, Borçlar Hukuku Genel Hükümler, C. I, Yenilenmiş ve Genişletilmiş 2. Bası, İstanbul 1976.
- Franzius, Claudio**, “*Das Recht auf informationelle Selbstbestimmung*”, Zeitschrift für das Juristische Studium, 3/2015, s. 259-270.
- Fuster, Gloria Gonzalez**, The Emergence of Personal Data Protection as a Fundamental Right of the EU, Springer, 2014.
- Gezder, Ümit**, Türk Medeni Hukuku-Başlangıç-Kişiler-Aile Hukuku Soruları ve Cevapları, C. 1, İstanbul 2014.
- Göçmen Uyarer, Sinem**, Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması, Ankara 2019.
- Gülener, Serdar**, “*Dijital Hafızadan Silinmeyi İstemek: Temel Bir İnsan Hakkı Olarak Unutulma Hakkı*”, TBB Dergisi, 2012, Y. 25, S. 102, s. 219-240.
- Günay, Erhan**, Kişilik Haklarına Saldırıdan Kaynaklanan Tazminat Davaları, Güncellenmiş 2. Baskı, Ankara 2017.
- Gür, İkbâl**, Kişisel Verilerin Korunması Hususunda AB ile ABD Arasında Çıkan Uyuşmazlıklar ve Çözüm Yolları, Ankara 2010.
- Gürpınar, Damla**, “*Kişisel Verilerin Korunamamasından Doğan Hukuki Sorumluluk*”, DEÜHFD, 2017, Prof. Dr. Şeref ERTAŞ’a Armağan, C. 19, Özel Sayı, s. 679-694.
- Gürsel, İlke**, İşçinin Kişisel Verilerinin Korunması Hakkı, Ankara 2016.
- Gürsel, İlke**, “*Kişisel Verilerin Korunması Hakkının İşçi ve İşveren İlişkisine Etkileri*”, Legal İSGHD, 2016, C. 13, S. 50, s. 763-848. (Anıltısı: İşçi ve İşveren İlişkisi).
- Hafizoğulları, Zeki/Özen, Muharrem**, Türk Ceza Hukuku Özel Hükümler-Kişilere Karşı Suçlar, 5. Baskı, Ankara 2016.
- Hatemi, Hüseyin**, Kişiler Hukuku, Güncellenmiş 7. Bası, İstanbul 2018.
- Helvacı, Serap**, Gerçek Kişiler, 7. Baskı, İstanbul 2016. (Anıltısı: Gerçek).

- Helvacı, Serap**, “*Kişilik Hakkına Hukuka Aykırı Saldırı Halinde Açılabilir Davalarda Yetkili Mahkeme*”, Doç. Dr. Mehmet Somer’in Anısına Armağan, İstanbul 2006, s. 653-659.
- Helvacı, Serap**, Türk ve İsviçre Hukuklarında Kişilik Hakkını Koruyucu Davalar, İstanbul 2001. (Anıltı: Koruyucu Davalar).
- Helvacı, Serap/Aydın, Gülşah Sinem**, “*Kişilik Hakkı İhlalinden Doğan Vekaletsiz İşgörmeye Kusurun Bir Şart Olarak Aranıp Aranmayacağı Sorunu*”, MÜHF-HAD, 2017, C. 23, S. 1, s. 265-301.
- Helvacı, Serap/Erlüle Fulya**, Medeni Hukuk, 5. Bası, İstanbul 2018.
- Henkoğlu, Türkay**, Bilgi Güvenliği ve Kişisel Verilerin Korunması, Ankara 2015.
- Hornung, Gerrit/Schnabel, Christoph**, “*Data Protection in Germany I: The Population Census Decision and The Right To Informational Self-Determination*”, Computer Law & Security Report, 2009, C. 25, S. 1, s. 84-88.
- Janger, Edward J.**, “*Privacy Property, Information Costs and the Anticommons*”, Hastings Law Journal, 2003, C. 54, S. 4, s. 899-929.
- Kang, Jerry**, “*Information Privacy in Cyberspace Transactions*”, Stanford Law Review, 1998, C. 50, s. 1193-1294.
- Kaplan, Emine Tuncay**, “*İş Hukukunda Kişilik Haklarının Özellikle Bilgisayarda Toplanan Bilgilere Karşı Korunması*”, AÜSBFD, 1997, C. 52, S. 1, s. 367-386.
- Kaya, Cemil**, “*Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi*”, İÜHFM, 2011, C. 69, S. 1-2, s. 317-334.
- Keser Berber, Leyla**, Çevrimiçi Davranışsal Reklamcılık (Online Behavioral Advertising) Uygulamaları Özelinde Kişisel Verilerin Korunması, İstanbul 2014.
- Keskin, A. Dilşad/Demircioğlu, H. Reyhan**, Medeni Hukuk-II (Eşya Hukuku – Miras Hukuku), Ankara 2018.
- Ketizmen, Muammer**, Türk Ceza Hukukunda Bilişim Suçları, Ankara 2008.

- Kılıçoğlu, Ahmet M.**, Borçlar Hukuku Genel Hükümler, Genişletilmiş 23. Bası, Ankara 2019. (Anılışı: Borçlar)
- Kılıçoğlu Ahmet M.**, Medeni Hukuk, Gözden Geçirilmiş-Güncellenmiş 3. Bası, Ankara 2019. (Anılışı: Medeni)
- Kılıçoğlu, Ahmet M.**, Şeref, Haysiyet ve Özel Yaşama Basın Yoluyla Saldırlardan Hukuksal Sorumluluk, Yeniden Gözden Geçirilmiş, Güncelleştirilmiş 4. Bası, Ankara 2013. (Anılışı: Basın).
- Kılınç, Doğan**, “*Anayasal Bir Hak Olarak Kişisel Verilerin Korunması*”, AÜHFD, 2012, C. 61, S. 3, s. 1089-1169.
- Kilian, Wolfgang**, “*Germany*”, James B. Rule and Graham Greenleaf, Global Privacy Protection, The First Generation, United Kingdom 2008.
- Kişisel Verileri Koruma Kurumu**, 100 Soruda Kişisel Verilerin Korunması Kanunu, Ankara 2018. (Anılışı: Kurum, 100 Soru).
- Kişisel Verileri Koruma Kurumu**, 6698 Sayılı Kanun’da Yer Alan Temel Kavramlar. (Anılışı: Kurum, Temel Kavramlar).
- Kişisel Verileri Koruma Kurumu**, 6698 Sayılı Kişisel Verilerin Korunması Kanununun Amacı ve Kapsamı.
- Kişisel Verileri Koruma Kurumu**, Açık Rıza.
- Kişisel Verileri Koruma Kurumu**, Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi, Yayın No: 24, Ankara 2019. (Anılışı: Kurum, Aydınlatma Yükümlülüğü).
- Kişisel Verileri Koruma Kurumu**, Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler), Yayın No: 5, Ankara 2019. (Anılışı: Kurum, Veri Güvenliği).
- Kişisel Verileri Koruma Kurumu**, Kişisel Veri İşleme Envanteri Hazırlama Rehberi, Yayın No: 30, Ankara 2019. (Anılışı: Kurum, Envanter).

Kişisel Verileri Koruma Kurumu, Kişisel Verilerin İşlenme Şartları. (Anılışı: Kurum, İşlenme Şartları).

Kişisel Verileri Koruma Kurumu, Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler. (Anılışı: Kurum, Temel İlkeler).

Kişisel Verileri Koruma Kurumu, Kişisel Verilerin Korunması Alanında Uluslararası ve Ulusal Düzenlemeler. (Anılışı: Kurum, Uluslararası ve Ulusal Düzenlemeler).

Kişisel Verileri Koruma Kurumu, Kişisel Verilerin Korunması Kanunu ve Getirdikleri, Yayın No: 26. (Anılışı: Kurum, KVKK ve Getirdikleri).

Kişisel Verileri Koruma Kurumu, Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi. (Anılışı: Kurum, İmha).

Kişisel Verileri Koruma Kurumu, Madde ve Gerekçesi İle Kişisel Verilerin Korunması Kanunu Bilgi Notu & Kişisel Verilerin Korunmasına İlişkin Terimler Sözlüğü, Ankara 2019.

Kişisel Verileri Koruma Kurumu, Örneklerle Kişisel Verilerin Korunması, Yayın No:29, Ankara 2019. (Anılışı: Kurum, Örnekler).

Kişisel Verileri Koruma Kurumu, Özel Nitelikteki Kişisel Verilerin İşlenme Şartları.

Kişisel Verileri Koruma Kurumu, Sorularla Veri Sorumluları Sicil Bilgi Sistemi (VERBİS), Yayın No: 22, Ankara 2019. (Anılışı: Sorularla VERBİS).

Kişisel Verileri Koruma Kurumu, Veri Sorumluları Sicili.

Kişisel Verileri Koruma Kurumu, Veri Sorumlusu ve Veri işleyen.

Korkmaz, İbrahim, Kişisel Verilerin Ceza Hukuku Kapsamında Korunması, Güncellenmiş 2. Baskı, Ankara 2019.

Kuner, Christopher, European Data Protection Law (Corporate Compliance and Regulation), Second Edition, Oxford 2007.

Kurt, Leyla Müjde, “*Ceninin Malvarlığı Hakları*”, İÜHFD, 2011, C. 2, S. 1, s. 177-207.

- Küzeci, Elif**, Yenilenmiş ve Gözden Geçirilmiş 3. Baskı, Ankara 2019.
- Litman, Jessica**, “*Information Privacy/Information Property*”, Stanford Law Review, 2000, C. 52, s. 1283-1313.
- Manav, A. Eda**, “*İş İlişkisinde İşçinin Kişisel Verilerinin Korunması*”, GÜHFD, 2015, C. 19, S. 2, s. 95-136.
- Nomer, Haluk Nami/Ergüne, Mehmet Serkan**, Eşya Hukuku, Gözden Geçirilmiş 7. Bası, İstanbul 2019.
- Ochsenfeld, Michael F.**, Datenschutz für Betriebsräte: Kurz und knackig, 2. Auflage, 2017.
- Oğuzman, Kemal/ Öz, Turgut**, Borçlar Hukuku Genel Hükümler, C. 1, Gözden Geçirilmiş 16. Bası, İstanbul 2018.
- Oğuzman, Kemal/ Öz, Turgut**, Borçlar Hukuku Genel Hükümler, C. 2, Gözden Geçirilmiş 14. Bası, İstanbul 2018. (Anılışı: Borçlar 2).
- Özbakır, Ali Fuat**, Sosyal Medyada ve İnternette Hukuki Sorumluluk, Ankara 2019.
- Özbek, Veli Özer/Doğan, Koray/Bacaksız, Pınar**, Türk Ceza Hukuku Özel Hükümler, Genişletilmiş ve Güncellenmiş 14. Baskı, Ankara 2019.
- Özdemir, Hayrunnisa**, Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması, Ankara 2009. (Anılışı: Elektronik Haberleşme).
- Özdemir, Hayrunnisa**, “*İşyerinde İşçilerin İzlenmesi ve İşçinin Kişilik Haklarının Korunması*”, EÜHFD, 2010, C.14, S. 1-2, s. 231-270.
- Özsunay, Ergun**, Gerçek Kişilerin Hukuki Durumu, Genişletilmiş ve Gözden Geçirilmiş 4. Baskı, İstanbul 1979.
- Pekcanitez, Hakan/Atalay, Oğuz/Özekes, Muhammet**, Medeni Usul Hukuku Ders Kitabı, 6. Bası, Ankara, 2018.
- Petek, Hasan**, Kişilik Değerlerinin Ölümünden Sonra Korunması, Ankara 2015.

- Prins, Corien**, “*When personal data, behavior and virtual identities become a commodity: Would a property rights approach matter?*”, SCRIPT-ed, 2006, C. 3, S. 4, s. 270-303. (Anılışı: Prins, Corien).
- Prins, J.E.J.**, “*The Propertization of Personal Data and Identities*”, Electronic Journal of Comparative Law, 2004, C. 8, S. 3, s. 1-7. (Anılışı: Prins, J.E.J.).
- Reisoğlu, Safa**, Türk Borçlar Hukuku Genel Hükümler, 24. Bası, İstanbul 2013.
- Riccardi, J. Lee**, “*The German Federal Data Protection Act of 1977: Protecting the Right to Privacy?*”, Boston College International and Comparative Law Review, 1983, C.6, S. 1, s. 243-271.
- Schwartz, Paul**, “*The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination*”, The American Journal of Comparative Law, 1989, C. 37, S. 4, s. 675-701. (Anılışı: Self Determination).
- Schwartz, Paul M.**, “*Property, Privacy and Personal Data*”, Harvard Law Review, 2004, C. 117, S. 7, s. 2055-2128.
- Serozan, Rona**, Eşya Hukuku I, Genişletilmiş 3. Bası, İstanbul 2014.
- Serozan, Rona**, Medeni Hukuk-Genel Bölüm/Kişiler Hukuku, 7. Bası, İstanbul 2017. (Anılışı: Medeni).
- Sert, Şeyma**, Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması, Ankara 2019.
- Sevimli, Ahmet**, “*İşçinin Özel Yaşam Hakkı Bağlamında İşçi-İşveren İlişkisi*”, MESS Sicil İş Hukuku Dergisi, 2008, S. 10, s. 53-79.
- Sevimli, Ahmet**, “*Veri Koruma Hukuku İlkeleri Işığında Türk Borçlar Kanunu Madde 419*”, MESS Sicil İş Hukuku Dergisi, 2011, S. 24, s. 120-139. (Anılışı: Veri Koruma).
- Sirmen, A. Lale**, Eşya Hukuku, 6. Baskı, Ankara 2018.
- Süzek, Sarper**, İş Hukuku, Yenilenmiş 12. Baskı, İstanbul 2016.

- Şener, Oruç Hami**, Teorik ve Uygulamalı Ortaklıklar Hukuku Ders Kitabı, Gözden Geçirilmiş 4. Bası, Ankara 2019.
- Şimşek, Oğuz**, Anayasa Hukukunda Kişisel Verilerin Korunması, İstanbul 2008.
- Taştan, Furkan Güven**, Türk Sözleşme Hukukunda Kişisel Verilerin Korunması, İstanbul 2017.
- Tekinalp, Ünal**, Fikri Mülkiyet Hukuku, Güncelleştirilmiş ve Genişletilmiş 5. Bası, İstanbul 2012.
- Tekinay, Selahattin Sulhi**, Medeni Hukukun Genel Esasları ve Gerçek Kişiler Hukuku, Gözden Geçirilmiş İlaveli 6. Bası, İstanbul 1992.
- Uncular, Selen**, Kişisel Verilerin Korunması Kanunu ve AB Genel Veri Koruma Tüzüğü Kapsamında İş İlişkisinde İşçinin Kişisel Verilerinin Korunması, Güncellenmiş ve Genişletilmiş 2. Baskı, Ankara 2018.
- Ünal, Mehmet/Başpınar, Veysel**, Şekli Eşya Hukuku, Güncellenmiş ve Genişletilmiş 8. Baskı, Ankara 2016.
- Yavuz, Can**, İnternet'teki Arama Sonuçlarından Kişisel Verilerin Kaldırılması-Unutulma Hakkı, Güncellenmiş ve Genişletilmiş 2. Baskı, Ankara 2018.
- Yavuz, Nihat**, Borçlar Hukuku El Kitabı, Ankara 2018. (Anıltı: Yavuz, Borçlar).
- Yılmaz, Sabire Sanem**, Tıp Alanında Kişisel Verilerin Açıklanması Suçu, Güncellenmiş 3. Baskı, Ankara 2019.
- Yokuş Sevük, Handan**, Türk Ceza Hukuku Özel Hükümler, Genişletilmiş ve Güncellenmiş 2. Baskı, Ankara 2019.
- Yücedağ, Nafiye**, “*Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu’nun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri*”, İÜHFM, 2017, C. 75, S. 2, s. 765-789.
- Zevkliler, Aydın/Acabey, M. Beşir/Gökyayla, K. Emre**, Medeni Hukuk, Gözden Geçirilmiş ve Genişletilmiş 6. Baskı, Ankara 2000.

ÇEVİRİM İÇİ KAYNAKLAR

AB Genel Sekreterliği, ABİHA, <https://www.ab.gov.tr/files/pub/antlasmalar.pdf> (E.T.: 15.04.2020).

Bundesanzeiger Verlag, <https://www.bundesanzeiger-verlag.de> (E.T.: 09.04.2020).

Bundesamt für Justiz, BDSG, https://www.gesetze-im-internet.de/bdsg_2018/BJNR209710017.html (E.T.: 09.04.2020).

Cambridge Dictionary, <https://dictionary.cambridge.org/dictionary/english/personal> (E.T.: 25.02.2020).

Council of Europe, “*Additional Protocol to the Convention for the Protection of Individuals with regard to Processing of Personal Data Regarding Supervisory Authorities and Transborder Data Flows*”, <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680080626> (E.T.: 09.04.2020).

Council of Europe, Avrupa İnsan Hakları Sözleşmesi, https://www.echr.coe.int/Documents/Convention_TUR.pdf (E.T.: 07.03.2020).

Council of Europe, “*Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*”, <https://rm.coe.int/1680078b37> (E.T.: 26.02.2020).

Council of Europe, European Convention on Human Rights, https://www.echr.coe.int/Documents/Convention_ENG.pdf (E.T.: 07.03.2020).

Council of Europe, Members of Council of Europe, <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005/signatures> (E.T.: 07.03.2020).

Council of Europe, “*Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data*” (“*Kişisel Verilerin İşlenmesi Karşısında Bireylerin Korunması İçin Modernize Edilmiş Sözleşme*”), <https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1> (E.T.: 08.03.2020).

Data Protection WP, Guidelines on Consent under Regulation 2016/679, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051 (E.T.: 07.04.2020).

Data Protection WP, Guidelines on Data Protection Officers (‘DPOs’), https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A (E.T.: 07.04.2020).

Data Protection WP, Guidelines on the application and setting of administrative fines for the purpose of the Regulation 2016/679, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237 (E.T.: 07.04.2020).

Data Protection WP, Guidelines on the right to data portability, https://edpb.europa.eu/our-work-tools/our-documents/guideline/right-data-portability_en (E.T.: 07.04.2020).

Data Protection WP, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf (E.T.: 19.03.2020). (Anılışı: Legitimate Interests).

Data Protection WP, Opinion 05/2014 on Anonymisation Techniques, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf (E.T.: 24.03.2020).

- Data Protection WP**, Opinion 3/2012 on developments in biometric technologies,
https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf (E.T.: 14.03.2020).
- Data Protection WP**, Opinion 15/2011 on the definition of consent,
https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf (E.T.: 16.03.2020). (Anılışı: Consent).
- Data Protection WP**, Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools),
https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp160_en.pdf (E.T.: 18.03.2020).
- Data Protection WP**, Opinion 4/2007 on the Concept of Personal Data,
https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf (E.T.: 03.03.2020). (Anılışı: Concept).
- Data Protection WP**, Opinions and Recommendations,
https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm (E.T.: 09.03.2020).
- Data Protection WP**, Working Document 1/2008 on the protection of children's personal data (General guidelines and the special case of schools),
https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2008/wp147_en.pdf (E.T.: 18.03.2020).
- Data Protection WP**, Working Document on Data Protection Issues Related to RFID technology,
https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp105_en.pdf (E.T.: 04.03.2020).

European Court of Human Rights,

[https://hudoc.echr.coe.int/tur#{\"fulltext\":\[\"Amann%20v%20Switzerland\"\],\"documentcodocumentco2\":\[\"GRANDCHAMBER\",\"CHAMBER\"\],\"itemid\":\[\"001-58497\"\]}](https://hudoc.echr.coe.int/tur#{\) (E.T.: 03.03.2020).

European Court of Justice,

<http://curia.europa.eu/juris/document/document.jsf?text=&docid=48382&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=125691> (E.T.: 03.03.2020).

European Data Protection Board, Guidelines 05/2020 on consent under Regulation

2016/679, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en (E.T.: 11.05.2020).

European Data Protection Board, Guidelines, Recommendations, Best Practices,

https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en (E.T.: 07.04.2020).

European Union, “*Charter of Fundamental Rights of the European Union*”, [https://eur-](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012P%2FTXT)

[lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012P%2FTXT](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012P%2FTXT) (E.T.: 09.03.2020).

European Union, “*Concerning the Processing of Personal Data and the Protection of*

Privacy in the Electronic Communications Sector-Directive on Privacy and Electronic Communication”, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN> (E.T.: 05.03.2020).

European Union, “*Directive 95/46/EC of the European Parliament and of the Council*

of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data”, <https://eur->

lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046 (E.T.: 02.03.2020).

European Union, “*Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR)*”, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679> (E.T.: 02.03.2020).

Kişisel Verileri Koruma Kurulu, 6698 sayılı Kişisel Verilerin Korunması Kanunu Hakkında Doğru Bilinen Yanlıklar, Yayın No: 31, Ankara 2020. <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/28d8adba-2b41-41b2-bf36-d0ff0d845666.pdf> (E.T.: 13.05.2020). (Anılışı: Doğru Bilinen Yanlıklar).

Kişisel Verileri Koruma Kurumu, Data Protection In Turkey, <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/5c02cb3c-7cc0-4fb0-b0a7-85cb90899df8.pdf> (E.T.: 02.04.2020).

Kişisel Verileri Koruma Kurumu, Kişisel Verilerin Korunması Kanunu Hakkında Sıkça Sorulan Sorular, Ankara 2018, <https://www.kvkk.gov.tr/Icerik/4196/Kisisel-Verilerin-Korunmasi-Kanunu-Hakkinda-Sikca-Sorulan-Sorular> (E.T.: 02.04.2020).

(Anılışı: Kurum, Sorular).

Kişisel Verileri Koruma Kurumu, Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi, <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/0517c528-a43d-49f5-b1eb-33dc666cb938.pdf> (E.T.: 10.03.2020). (Anılışı: Kurum, Uygulama Rehberi).

- Kişisel Verileri Koruma Kurumu**, Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi, Ankara 2018,
<https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/bc1cb353-ef85-4e58-bb99-3bba31258508.pdf> (E.T.: 23.03.2020). (Anılışı: Kurum, İmha Rehberi).
- Kişisel Verileri Koruma Kurumu**, Kişisel Veri, Saklama ve İmha Politikası,
<https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/a556b331-4910-4a77-9794-83cba2ba74e1.pdf> (E.T.: 02.04.2020).
- Kişisel Verileri Koruma Kurumu**, Kurul Karar Özetleri,
<https://www.kvkk.gov.tr/Icerik/5406/Kurul-Karar-Ozetleri> (E.T.: 17.03.2020).
- Kişisel Verileri Koruma Kurumu**, VERBİS Kılavuzu,
<https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/a1fca030-7f7e-4e61-bd70-8da57160199b.PDF> (E.T.: 02.04.2020).
- OECD**, “*Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*”,
<https://www.oecd.org/internet/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsofPersonalData.htm> (E.T.: 25.02.2020).
- OECD**, OECD e-Government Studies Turkey, https://read.oecd-ilibrary.org/governance/oecd-e-government-studies-turkey-2007_9789264028456-en#page1 (E.T.: 07.03.2020).
- OECD**, OECD e-Government Studies Turkey, https://read.oecd-ilibrary.org/governance/oecd-e-government-studies_9789264037700-tr#page1 (E.T.: 07.03.2020).
- OECD**, revision 2013,
https://www.oecd.org/internet/ieconomy/oecd_privacy_framework.pdf (E.T.: 07.03.2020).

TBMM, İnsan Hakları Evrensel Beyannamesi,
<https://www.tbmm.gov.tr/komisyon/insanhaklari/pdf01/203-208.pdf> (E.T.:
09.03.2020).

T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı, http://www.sbb.gov.tr/wp-content/uploads/2018/11/Avrupa_Birligi_Temel_Haklar_Sarti%E2%80%8B.pdf
(E.T.: 09.03.2020).

TDK, Güncel Türkçe Sözlük, <https://sozluk.gov.tr> (E.T.:25.02.2020).

United Nations, “*Guidelines for the Regulation of Computerized Personal Data Files*”,
<https://www.refworld.org/pdfile/3ddcafaac.pdf> (E.T.: 09.03.2020).



ÖZET

Bu çalışmanın konusunu “*Kişisel Verilerin Korunması*” oluşturmaktadır. Kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade eder. Gelişen teknoloji ve dönüşen toplum yapısında kişisel veriler kolayca işlenebilmekte ve işlenen kişisel verilerden ciddi manada gelir elde edilebilmektedir. Kişisel verilerin işlenmesi nitelik ve nicelik olarak her geçen gün artmaya devam etmiştir. Buna karşın kişisel verilerin korunması elzem hale gelmiştir. Kişisel verilerin korunması serüveni, 1970’lerde Avrupa’da başlamıştır. 50 yıllık bir geçmişe sahip olan bu konuda uluslararası alanda birçok düzenleme yapılmıştır. Ülkemizde ise bu alandaki mevzuat oluşumu çok yenidir. Anayasamızda 2010 yılında yapılan değişiklikle “*kişisel verilerin korunması hakkı*” anayasal güvence altına alınmıştır. Bu alana has bir kanun olan 6698 sayılı Kişisel Verilerin Korunması Kanunu ise 07.04.2016 tarihinde yürürlüğe girmiştir. Çalışmamızda öncelikle kişisel veri kavramı ayrıntılı bir şekilde irdelenmiş, kişisel verilerin hukuki niteliği incelenmiş, kişisel verilerin korunmasının tarihsel serüveni ve kişisel verilerin korunmasının hak olarak ortaya çıkışı açıklanmaya çalışılmıştır. Daha sonra Kişisel Verilerin Korunması Kanunu detaylarıyla incelenmeye çalışılmıştır. Bu kapsamda kişisel verilerin işlenmesi, genel ilkeler, kişisel verileri işleme şartları, kişisel verilerin imhası, veri sorumlusunun yükümlülükleri ve ilgili kişinin hakları incelenmiştir. Bu inceleme yapılırken Kişisel Verileri Koruma Kurulu kararlarına yer verilerek teorik bilgiler, uygulamadaki kararlarla perçinlenmeye çalışılmıştır. Son bölümde ise Kişisel Verilerin Korunması Hukuku dışındaki hukuk dallarındaki kişisel verilerin korunması yollarına yer verilmiştir.

Anahtar Kelimeler: Kişisel Veri, Kişilik Hakkı, Kişisel Verilerin Korunması, Veri Güvenliği.

ABSTRACT

The subject of this study is “*Protection of Personal Data*”. Personal data refers to any kind of information related to an identified or identifiable natural person. Through the developing nature of technology and transforming societal structure, personal data can be easily processed and a serious volume of income can be obtained from the processed personal data. Processing of personal data has continued to increase day by day in terms of quality and quantity. However, the protection of personal data has become essential. The history of personal data protection started in Europe in the 1970s. Within the fifty year history of the subject, many arrangements have been made internationally. In our country, the formation of legislated rules and regulations in this field is very new. With the amendment made in our constitution in 2010, “*right of personal data protection*” was guaranteed by the constitution. The Law on the Protection of Personal Data No. 6698, which is a legislation specific to this field, came into force on 07.04.2016. In our study, firstly, the concept of personal data has been examined in detail, the legal nature of personal data has been examined, and we have attempted to explain the historical process of protecting personal data and the emergence of personal data as a right. Then, the Law on the Protection of Personal Data is tried to be examined in detail. In this context, processing of personal data, general principles, terms of processing personal data, destruction of personal data, obligations of the data controller and the rights of the data subject are analysed. During this review, theoretical information was tried to be reinforced with inclusion of the Personal Data Protection Board decisions on practice. In the last section, other than the Personal Data Protection Law, the methods of protecting personal data in the other branches of law are included.

Keywords: Personal Data, Personality Rights, Protection of Personal Data, Data Security.