

T.C KOCAELİ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
ÖZEL HUKUK ANABİLİM DALI
ÖZEL HUKUK BİLİM DALI

AB VE TÜRK ÖZEL HUKUKUNDA KARŞILAŞTIRMALI OLARAK
KİŞİSEL VERİLERİN KORUNMASI

YÜKSEK LİSANS TEZİ

GUNAY MAMMADOVA

KOCAELİ 2022

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

**AB VE TÜRK ÖZEL HUKUKUNDA KARŞILAŞTIRMALI OLARAK
KİŞİSEL VERİLERİN KORUNMASI**

YÜKSEK LİSANS TEZİ

Gunay MAMMADOVA

Dr. Öğretim Üyesi Duygu KOÇAK DİKER

KOCAELİ 2022

İÇİNDEKİLER

İÇİNDEKİLER	i
ÖZET.....	iv
ABSTRACT	v
KISALTMALAR	vi
GİRİŞ	1

BİRİNCİ BÖLÜM

1. KİŞİSEL VERİ KAVRAMI VE KİŞİSEL VERİLERİN KORUNMASI HAKKININ TARİHİ GELİŞİMİ

1.1. KİŞİSEL VERİ.....	3
1.1.1. Tanımı.....	3
1.1.2. Unsurlar	4
1.1.2.1. Her Türlü Bilgi.....	4
1.1.2.2. Kimliği Belirli veya Belirlenebilir Kişi.....	6
1.1.2.3. Bilginin Kişiye İlişkin Olması	10
1.1.3. Türleri.....	11
1.1.4. Hukuki Niteliği.....	14
1.1.4.1. Mülkiyet Hakkı Görüşü	14
1.1.4.2. Fikri Hak Görüşü.....	17
1.1.4.3. Kişilik Hakkı Görüşü.....	18
1.2. KİŞİSEL VERİLERİN KORUNMASINDA TARİHİ SÜREÇ	22
1.2.1. Avrupa Birliği Hukuku (GVKT).....	23
1.2.2. Türk Hukuku	26

İKİNCİ BÖLÜM

2. KİŞİSEL VERİLERİN KORUNMASI HUKUKUNDA TEMEL KAVRAMLAR, GENEL İLKELER VE VERİ SORUMLUSUNUN YÜKÜMLÜLÜKLERİ, İLGİLİ KİŞİNİN HAKLARI

2.1. TEMEL KAVRAMLAR	28
2.1.1. Veri Sahibi.....	28
2.1.2. Veri İşleme.....	30
2.1.3. Veri Sorumlusu ve Veri İşleyen.....	30
2.2. KİŞİSEL VERİLERİN İŞLENMESİNE İLİŞKİN İLKELER	34
2.2.1. Genel İlkeler	34
2.2.1.1. Hukuka ve Dürüstlük Kurallarına Uygun Olma İlkesi	35
2.2.1.2. Doğru ve Gerekliğinde Güncel Olma İlkesi	37

2.2.1.3. Belirli, Açık ve Meşru Amaçlar İçin Kullanma İlkesi.....	38
2.2.1.4. Amaçla Bağlantılı, Sınırlı ve Ölçülü Olma İlkesi.....	40
2.2.1.5. Belirli ve Sınırlı Süre Muhafaza Edilmesi İlkesi.....	41
2.2.1.6. Bütünlük ve Gizlilik İlkesi	43
2.2.1.7. Hesap Verebilirlik İlkesi	44
2.2.2. Veri Aktarımına İlişkin İlkeler.....	44
2.3. VERİ SORUMLUSUNUN YÜKÜMLÜLÜKLERİ.....	47
2.3.1. Genel Olarak	47
2.3.1.1. Aydınlatma Yükümlülüğü	47
2.3.1.2. Temsilci Atama Yükümlülüğü.....	50
2.3.1.3. İş Bölümü Anlaşması Yapmak	51
2.3.1.4. Zararı Tazmin Yükümlülüğü	52
2.3.1.5. İspat Yükümlülüğü.....	52
2.3.1.6. Denetim Yükümlülüğü	53
2.3.1.7. Kurul Kararlarına Uyuma Yükümlülüğü	54
2.3.2. Veri Kayıt ile İlgili Yükümlülükler.....	54
2.3.2.1. Veri Koruma Politikaları Oluşturma	54
2.3.2.2. Veri Saklama ve Kayıt Yükümlülüğü.....	55
2.3.2.3. Veri İhlali Açıklaması ve Bildirimi	57
2.3.2.4. Veri Güvenliğini Sağlama Yükümlülüğü	60
2.4. İLGİLİ KİŞİNİN HAKLARI.....	61
2.4.1. Bilgilendirilme Hakkı	61
2.4.2. Erişim hakkı.....	63
2.4.3. Düzeltme Talep Hakkı.....	64
2.4.4. Silinmeyi Talep Hakkı (Unutulma Hakkı)	65
2.4.5. İşlemenin Sınırlandırılması Hakkı.....	67
2.4.6. Veri Taşınabilirliği Hakkı.....	68
2.4.7. İşlemeye İtiraz Hakkı	68

ÜÇÜNCÜ BÖLÜM

3. KİŞİSEL VERİLERİN HUKUKA AYKIRI İŞLENMESİ VE BUNA KARŞI VERİ SAHİBİNİN KORUNMASI	
3.1. VERİ İŞLEMENİN HUKUKA UYGUNLUK ŞARTLARI.....	70
3.1.1. Genel Olarak	70
3.1.2. İlgili Kişinin Açık Rızası	71
3.1.2. Veri İşlemenin Kanunda Açıkça Öngörülmüş Olması	76
3.1.3. İlgili Kişinin veya Üçüncü Kişinin Üstün Özel Yararı.....	77
3.1.4. Sözleşmenin Kurulması ve İfası İçin Gerekli Olması.....	79

3.1.5. Veri Sorumlusunun Hukuki Yükümlülüğünü Yerine Getirebilmesi İçin Zorunlu Olması.....	79
3.1.6. Kişisel Verilerin İlgili Kişi Tarafından Alenileştirilmiş Olması.....	80
3.1.7. Kişisel Verilerin İşlenmesinin Bir Hakkın Tesisi, Kullanılması veya Korunması İçin Zorunlu Olması.....	82
3.2. KVKK ve GVKT BAKIMINDAN KİŞİSEL VERİLERİN KORUNMASI	83
3.2.1. GVKT Kapsamında Kişisel Verilerin Korunması.....	83
3.2.1.1. Denetim Otoriteleri ve Avrupa Veri Koruma Kurulu	83
3.2.1.1.1. Denetim Otoritesi.....	83
3.2.1.1.2. Avrupa Veri Koruma Kurulu.....	87
3.2.1.2. Kişisel Verilerin Korunma Yolları.....	89
3.2.1.2.1. İdari Başvuru Yolları	90
3.2.1.2.2. İdari Para Cezası	92
3.2.1.2.3. Hukuki Yaptırımlar.....	93
3.2.2. Kişisel Verilerin Korunması Kanunu Kapsamında Kişisel Verilerin Korunması.....	94
3.2.2.1. Veri Sorumlusuna Başvuru	94
3.2.2.2. Kurula Şikayet	96
3.2.2.3. İdari Yaptırımlar	97
3.3. TÜRK MEDENİ KANUNU IŞIĞINDA KİŞİSEL VERİLERİN KORUNMASI	98
3.3.1. Genel Olarak	98
3.3.2. Kişisel Verilerin Hukuka Aykırı Olarak İşlenmesi Halinde Açılacak Davalar	101
3.3.2.1. Önleme Davası	101
3.3.2.2. Durdurma Davası	102
3.3.2.3. Tespit Davası	103
3.3.2.4. Sebepsiz Zenginleşme Davası.....	104
3.3.2.5. Vekaletsiz İş Görme Davası	106
3.3.2.6. Maddi Tazminat Davası	106
3.3.2.7. Manevi Tazminat Davası.....	108
SONUÇ.....	111
KAYNAKÇA	114

ÖZET

Günümüzde çeşitli teknoloji türlerinin yüksek oranda gelişmesi dünyanın her bir yanından insanların bir birleriyle iletişim içerisinde olmasını sağlamaktadır. “*Kişiyeye ait her türlü bilgi*” olarak tanımlanan kişisel veri kavramı ise bahsettiğimiz iletişim ve etkileşimin en önemli parçalarından birine çevrilmiştir. Kişisel verilerin öneminin artması ve ekonomik değeri kazanması onlara ilişkin düzenlemelerin de güncellenmesine, yeni düzenlemelerin kabul edilmesine yol açmıştır. Çalışmamız kapsamında; kişisel verilerin korunmasına ilişkin olarak son yıllarda kabul edilmiş iki hukuki düzenleme Avrupa Birliği Genel Veri Koruma Tüzüğü ve Kişisel Verileri Koruma Kanunu karşılaştırılmıştır. Üç bölümden oluşan çalışmamızın ilk bölümünde kişisel veri kavramı, unsurları, türleri ve hukuki niteliği anlatılırken, ikinci bölümde veri koruma alanına ilişkin kavram haritası, yükümlülükler ve haklar mukayeseli şekilde açıklanmış, farklar ortaya koyulmuştur. Sonuncu bölümde ise kişisel verilerin hukuka aykırı işlenmesi ve buna karşın veri sahibinin korunması yollarından bahsedilmiştir.

Anahtar kelimeler: Kişisel veri, Kişisel Verilerin İşlenmesi, Genel Veri Koruma Tüzüğü, Kişisel Verilerin Korunması Kanunu

ABSTRACT

In our modern world the highly developed various types of technology enable people from all over the world to communicate with each other and increase the effects of each other's lives. If the concept of personal data, which is referred to as “*all kinds of personal information related to the natural person*” in legal regulations, is transformed into one of the most important parts of the communication and interaction. In this period when its importance has increased and being a part of it has become a necessity, legal regulations regarding this field have started to gain more importance as well. Within the scope of our thesis, the legal regulations on the subject were compared within the scope of the European Union, especially the General Data Protection Regulation, and Personal Data Protection Law in the Turkish Private Law. Then, the functioning of the legal regulations and the awareness of the data owners on this subject were investigated compared to the topicality of the subject. In the first part of our study, which consists of three parts, the concept of personal data, its elements, types and legal nature are explained, in the second part, the concept map, obligations and rights related to the field of data protection are explained in a comparative way and the differences are revealed. In the last part, the ways of illegal processing of personal data and the protection of the data owner are mentioned.

Key words: Personal data, Processing of Personal Data, General Data Protection Regulation, Turkish Data Protection Law no. 6698.

KISALTMALAR

AB	: Avrupa Birliđi
AAD	: Avrupa Adalet Divanı
ABAD	: Avrupa Birliđi Adalet Divanı
AEA	: Avrupa Ekonomik Alanı
a.g.e.	: Adı geen eser
a.g.m.	: Adı geen makale
a.g.t.	: Adı geen tez
AİHM	: Avrupa İnsan Hakları Mahkemesi
AVKK	: Avrupa Veri Koruma Kurulu
AYM	: Anayasa Mahkemesi
Bkz	: Bakınız
BKK	: Bađlayıcı Kurumsal Kurallar
CJEU	: Court of Justice of the European Union
CNIL	: Comission Nationale Informatique & Libertes
DPA	: Data Protection Authority
DPC	: Data Protection Commision
EctHR	: European Court of Human Rights
EC	: European Comission
EDPB	: European Data Protection Board
ET	: Eriřim Tarihi
GDPR	: General Data Procetion Regulation
GVKT	: Genel Veri Koruma Tüzüğü
HAD	: Hukuk Arařtırmaları Dergisi
İK	: İş Kanunu
ISS	: Information Systems & Services
KEP	: Kayıtlı Elektronik Posta
KVKK	: Kiřisel Verileri Korunması Kanunu
m	: Madde
MESS	: Metal Sanayicileri Sendikası
MÜHF	: Marmara Üniversitesi Hukuk Fakóltesi
OECD	: Organisation for Economic Cooperation and Development

Par	: Paragraf
PVSK	: Polis Vazife ve Salahiyet Kanunu
SA(s)	: Supervisory Authorities
SBF	: Siyasal Bilimler Fakóltesi
S	: Sayı
s	: Sayfa
T	: Tarix
TBK	: Türk Borçlar Kanunu
TBMM	: Türkiye Büyük Millet Meclisi
TDK	: Türk Dil Kurumu
TFEU	: Treaty on the Functioning of the European Union
TMK	: Türk Medeni Kanunu
Vd	: Ve devamı
WP	: Working Party

GİRİŞ

Bilindiği üzere küresel gelişimin sonuçlarından biri olarak kişisel verilerin önemi gün geçtikçe artmaktadır. Kişisel veriler artık bir kişiye ait herhangi bilgi olmaktan çıkmış, ekonomik yarışların bir parçasına çevrilmiştir. Bunu özellikle çeşitli şirketlerin faaliyetlerinde açıkça görmek mümkündür. Şöyle ki verilerin ele geçirilmesi sonucu insanların ilgi alanları, ihtiyaçları öğrenilmekte ve bu ihtiyaçlara uygun teklifler oluşturmaktadırlar. Bu bağlamda teknolojinin gelişimi veri dolaşımını ve verilerin ele geçirilmesini hızlandıran faktörler arasında yer almaktadır. Neredeyse herkesin sosyal medya platformlarında hesapları bulunmakta, alışverişler online şekilde yapılmaktadır. Teknolojik gelişimin veri sahiplerine ulusal sınırların dışına çıkabilme imkanı vermesi, aynı şekilde veri depolayan büyük şirketlerin bir çoğunun uluslararası olması kişisel verilerin korunmasına ilişkin daha gelişmiş düzenlemelere ihtiyacı beraberinde getirmiştir. Çalışmamız kapsamında karşılaştıracığımız iki düzenleme; 2016 senesinde Türkiye’de kabul edilen, Kişisel Verilerin Korunması Kanunu (“KVKK”) ve Avrupa’da kabul edilen Genel Veri Koruma Tüzüğü (“GVKT”) de söz konusu ihtiyaç doğrultusunda meydana çıkmıştır.

Tarihi akış içerisinde kişiye ait bilgilerin korunmasına dair hükümlere çeşitli ulusal ve uluslararası düzenlemelerde yer verilmiştir. 1970 yılında Almanya’da kişisel verilerin korunmasına ilişkin ilk ulusal kanun kabul edilirken, İspanya, Portekiz gibi ülkeler kendi anayasalarına kişisel verilerle ilgili hükümler getirmişler¹. Aynı şekilde uluslararası düzenlemelerde; Avrupa Konseyi tarafından 4 Kasım 1950 yılında kabul edilen Avrupa İnsan Hakları Sözleşmesi’nin (“AİHS”) 8. maddesi ile “*özel ve aile hayatına saygı hakkı*” düzenlenmiştir. Bu hak uyarınca “*herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir*”. Kişisel verilerin korunması hakkı da, bu hak ile korunan bir kavramdır². Daha sonra 1995 yılında Avrupa Veri Koruma Direktifi kabul edilmiş ve uzun süre ilgili alanda esas düzenleme olmuştur. Güncel gelişimler, hızla artan ticaret ve iletişim, özellikle online işlemlerin hayatımızda büyük bir yer edinmesi sonucu yeni bir düzenleme ihtiyacı oluşmuş ve bunun sonucunda 2016 yılında GVKT kabul

¹ Oğulcan Özkan, Kişisel Verilerin Korunması, 1. Baskı, Ankara, Yetkin Yayınları, 2020, s. 42.

² Murat Volkan Dülger, “Avrupa Birliği Veri Koruma Tüzüğü Bağlamında Kişisel Verilerin Korunması”, Yaşar Hukuk Dergisi, Cilt 1, Sayı 2, 2019, s. 78.

edilmiştir. Türk hukukunda ise kişisel verilerin korunması hakkı, ilk defa 5982 sayılı kanun ile 2010 yılında yapılan Anayasa değişikliği ile gündeme gelmiş, Anayasa'nın 20. maddesine eklenen son fıkra ile kişisel verilerin korunması, ayrı bir hak alanı olarak korunmaya başlamıştır. Bu alana ilk özel düzenleme ise yine 2016 senesinde kabul edilen 6698 sayılı Kişisel Verilerin Korunma Kanunu olmuştur.

Çalışmamızda kişisel verilerin korunmasına ilişkin bu iki özel düzenleme üç bölümde incelenmiş ve araştırma metodu olarak karşılaştırma (mukayese) metodu tercih edilmiştir. Birinci bölümde; ilk olarak kişisel veri kavramı, onun unsurları ve hukuki niteliğine ilişkin açıklamalar yapıldıktan sonra; kişisel verilerin korunmasının tarihsel gelişimi ele alınmıştır. Özellikle; kişisel verilerin hukuki niteliğine dair mülkiyet hakkı, fikri mülkiyet hakkı ve kişilik hakkı görüşleri bu başlık kapsamında anlatılmıştır. Son olarak; KVKK ve GVKT'nin kabul serüvenine ilişkin bilgi verilerek bölüm tamamlanmıştır.

İkinci bölümde; kişisel verilerin korunması hukukuna ilişkin temel kavramlar, veri işleme faaliyeti ve bu faaliyetde yer alan aktörler ele alınmıştır. Buna ek olarak; veri işleme faaliyeti yerine getirilirken uyulması gereken genel ilkeler mukayese edilen iki düzenleme kapsamında karşılaştırmalı olarak açıklanmaya çalışılmıştır. Bu bölüm kapsamında son olarak veri sorumlusunun yükümlülükleri ve ilgili kişinin haklarına yer verilmiştir.

Son bölümde ise, kişisel verilerin hukuka aykırı şekilde işlenmesi ve buna karşı veri sahibinin korunması yollarından bahsedilmiştir. Bu bağlamda ilk olarak veri işlemenin hukuka uygunluk şartları açıklanmıştır. Daha sonra KVKK ve GVKT kapsamında veri sorumlusuna, denetim otoritelerine, Avrupa Veri Koruma Kurulu ve Kişisel Verileri Koruma Kurulu'na başvuru yolları, hukuki yaptırımlar, idari para cezalarına ilişkin bilgilendirme yapılmıştır. Türk Medeni Kanunu'nda yer alan genel hükümler kapsamında öngörülen koruma yollarından; saldırının önlenmesi davası, saldırının durdurulması davası, saldırının tespiti davası, sebepsiz zenginleşme davası, vekaletsiz iş görme davası, maddi ve manevi tazminat davaları anlatılarak çalışmamız sonlandırılmıştır.

Çalışmamız kapsamında verilen teorik bilgilerin yanında karar örneklerine de yer verilerek kişisel verilerin korunması alandaki teorik bilgilerin uygulamaya nasıl geçirildiği anlatılmaya çalışılmıştır.

BİRİNCİ BÖLÜM

1. KİŞİSEL VERİ KAVRAMI VE KİŞİSEL VERİLERİN KORUNMASI HAKKININ TARİHİ GELİŞİMİ

1.1. KİŞİSEL VERİ

1.1.1. Tanımı

Kişisel verilerin korunmasından bahsedebilmemiz için ilk önce “*kişisel*” ve “*veri*” kavramlarının sözlük anlamlarını tespit etmek gereklidir. “*Kişisel*” kavramı “*kişi ile ilişkili, kişiye ilişkin olan, şahsi*”³, “*bir grup yerine tek ya da belirli bir kişiye ait olan*”⁴ anlamına gelir. Türk Dil Kurumu’na göre “*bilgi, data*” olarak ifade edilen “*veri*” kelimesi ise bir araştırmanın, veya herhangi bir tartışmanın, muhakemenin temeli olan ana öge, muta, done, bilişimde ise “*olgu, kavram veya komutların, iletişim, yorum ve işlem için elverişli biçimli gösterimi*”⁵ olarak tanımlanmaktadır.

Karşılaştırdığımız mevzuat genel olarak incelendiğinde iki düzenlemede de tanımların çok geniş tutulduğu gözükmemektedir. Kişisel Verilerin Koruması Kanunu (“*KVKK*”) madde 3 ve Genel Veri Koruma Tüzüğü (“*GVKT*”) madde 4 ile kişisel veriler “*Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi*” olarak tanımlanmıştır. Hem KVKK’da, hem de GVKT’de hangi tür bilgilerin kişisel veri kapsamına dahil olduğu sınırlı şekilde sayılmamıştır. Dolayısıyla doktrin veya uygulamada yapılabilecek herhangi bir yorum kişisel verilerin kapsamını genişletebileceği gibi de daraltabilir⁶. 1980 tarihli Ekonomik Kalkınma ve İşbirliği Örgütü (“*OECD*”) Rehber İlkelerine göre kişisel veriler, “*Kimliği belirli ya da*

³ Türk Dil Kurumu (“*TDK*”), Güncel Türkçe Sözlük, <https://sozluk.gov.tr/>, (E.T.: 24.10.2021).

⁴ Cambridge Dictionary, <https://dictionary.cambridge.org/dictionary/english/personal>, (E.T.: 24.10.2021).

⁵ TDK, <https://sozluk.gov.tr/>, E.T.: 30.10.2021.

⁶ Hüseyin Can Aksoy, Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması, Ankara, Çakmak Yayınevi, 2010, s. 12.

*belirlenebilir bir gerçek kişi (ilgili kişi) hakkındaki tüm bilgiler”*⁷ şeklinde tanımlanmıştır. Avrupa Konseyi (“AK”) tarafından hazırlanan 108 No.lu Sözleşme’nin⁸ 2/a maddesinde de kişisel veri kavramı aynı şekilde açıklanmıştır⁹. Konuyla ilgili Avrupa Birliği (“AB”) düzenlemelerinden olan 95/46/EC sayılı Direktif’in 29. maddesi uyarınca kurulmuş 25 Mayıs 2018 tarihine kadar (GVKT’nin uygulamaya girişi) mahremiyetin ve kişisel verilerin korunmasına ilişkin konulardan sorumlu bağımsız¹⁰ Çalışma Grubu (“Working Party”) / (“WP”) kişisel veri kavramının anlamı, unsurları ve somut durumlarda Direktif’in nasıl anlaşılması gerektiği ile ilgili bir rapor hazırlamıştır¹¹.

1.1.2. Unsurlar

Kişisel veri kavramına ilişkin yapılan tanımlar doğrultusunda kişisel verinin unsurları, “bilgi”, “kimliği belirli veya belirlenebilir kişi” ve “bilginin kişiye ilişkin olması” olarak sayılmaktadır. Adı geçen üç unsurun varlığı halinde kişisel verilerden ve onların korunmasından söz edilebilir.

1.1.2.1. Her Türlü Bilgi

KVKK (madde 3/e) ve GVKT (madde 4/1) ile kişisel verilere yapılan tanımlardan görüldüğü üzere her iki düzenlemede “her türlü bilgi” terimine yer verilmiş, nelerin kişisel veri sayılacağı tek tek sayılarak sınırlama yapılmamıştır. Dolayısıyla herhangi bir bilginin kişisel veri olarak kabul edilmesi için niteliği,

⁷ 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.), 2013, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, E.T. 11.09.2022.

⁸ 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.), 1981, Details of Treaty No.108, E.T.: 10.09.2022.

⁹ “Personal data means any information relating to an identified or identifiable individual (data subject).”

¹⁰ Article 29 Working Party, https://edpb.europa.eu/about-edpb/more-about-edpb/article-29-working-party_en, E.T.: 11.07.2022. Bundan böyle “Çalışma Grubu” olarak anılacaktır.

¹¹ 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.: 31.10.2021).

formatı ve sair diğer özelliklerine bakılmaksızın “*kişiyi tanımlayabilme kabiliyeti*”¹² dikkate alınarak geniş yorumlanması¹³, her somut olayın özelliğine göre kişisel verinin kapsamının genişletilmesi mümkündür.

“*Her türlü bilgi*” ifadesi yalnızca kişiye ait olan ad, soyad ya da doğum tarihi gibi onu tanınır kılan verileri değil, aynı zamanda bireyin belirlenebilir kılınmasını sağlayan aile ile ilgili, sosyal, fiziksel ve ekonomik yaşamla ilgili bilgileri de kapsamaktadır¹⁴. Günümüz teknolojilerindeki ilerlemeler sonucu banka hesap numarası, müşterinin bankaya talimat verirken kaydedilen ses kaydı¹⁵, T.C. kimlik numarası, e-posta adresi gibi bilgiler de kişisel veri sayılmaya başlamıştır¹⁶. Tek bir veri bazı durumlarda kişiyi belirlenebilir yapmaya yetmezken, bazı ek bilgiler ile birlikte kişinin kimliğinin saptanmasını sağlayabilir. Bu nedenle verinin tekbaşına kişisel veri niteliğinde olup olmayacağı öğretide tartışmalıdır¹⁷. Özetle kişisel veriler ait olduğu kişiyi dolaylı yolla ya da doğrudan olarak tanımlayan bilgilerdir¹⁸.

Bununla birlikte kişinin hakkındaki herhangi bir bilginin kişisel veri sayılması için o verinin mutlaka gizli olması gerekmeyebilir. Gizli bilgiler kişisel veri olduğu gibi gizli olmayan, herkes tarafından bilinen bilgiler de kişisel veridir¹⁹. Örnek olarak; kişinin cinsel yaşamı, kredi kartı şifresi gibi bilgileri kişisel veri sayıldığı gibi, fiziksel özellikleri, kullandığı arabanın markası, kamuya açık alanda yapılan bir toplantıda giydiği kıyafetin rengi gibi herkes tarafından ulaşılabilir olan bilgiler kişisel veri olarak değerlendirilebilir²⁰. Anayasa Mahkemesinin bazı

¹² Kişisel Verileri Koruma Kurumu (bundan böyle “Kurum” olarak anılacaktır), 100 Soruda Kişisel Verilerin Korunması Kanunu, Ankara, KVKK Yayınları, 2018, s. 18, <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/185c2130-8070-4b2b-a91e-1d48322ca352.pdf>, E.T.: 17.04.2022.

¹³ Data Protection WP, Concept, s. 1.

¹⁴ Kişisel Verileri Koruma Kurumu, Örneklerle Kişisel Verilerin Korunması, s. 1, Ankara, 2019, ÖRNEKLERLE KİŞİSEL VERİLERİN KORUNMASI, E.T.: 09.11. 2021.

¹⁵ Torre Lydia F de la, “What is ‘personal data’ under EU data protection law?”, <https://medium.com/golden-data/what-is-personal-data-under-eu-data-protection-law-a9983fb2e483>, E.T.: 16.04.2022.

¹⁶ Murat Volkan Dülger, Kişisel Verilerin Korunması Hukuku, 2. Baskı, İstanbul, Hukuk Akademisi yayınevi, 2019, s. 1.

¹⁷ Naifiye Yücedağ, “Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu’nun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri”, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Cilt 72, Sayı 2, 2017, s. 767-768.

¹⁸ Faruk Bilir, “Kişisel Verilerin Korunması Kişinin Kendisinin Korunmasıdır”, TRT Akademi, Cilt 6, Sayı 11, 2021, s. 172.

¹⁹ Aksoy, a.g.e, s. 14.

²⁰ Aksoy, a.g.e, s. 14, “Kişisel veri” kavramının telefon koordinatları, çalışma koşulları ve hobileri de kapsayacağı ile ilgili Avrupa Adalet Divanı (“AAD”) (“European Court of Justice”) kararı için bkz: CJEU, *Directive 95/46 / EC - Scope - Publication of personal data on the Internet - Place of publication - Concept of transfer of personal data to third countries - Freedom of expression -*

kararlarında kişisel verilerle ilgili tanımlar yer almaktadır. Bahsi geçen kararlardan birinde bir kişinin imzası, kimlik, abonelik ve ailesine ilişkin bilgilerin, ev veya iş adresinin de kişisel veri kapsamında olduğu belirtilmiştir. İlgili karar uyarınca,

“Belirli veya kimliği belirlenebilir olmanın yanısıra, kişisel veri kavramı, herhangi bir kişiyle ilgili bilgilerin tamamını ifade eder. Bu kapsamda kişinin adı, soyadı, doğum tarihi ve yeri gibi şahsın yalnızca kimliğini açıklayan bilgiler değil, motorlu taşıt plakası, sosyal güvenlik, telefon, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgileri, IP veya e-posta adresi, hobileri, tercihleri, onun etkileşimde bulunduğu kişiler, grup üyelikleri, aile bilgileri gibi kişiyi doğrudan yada dolaylı olarak belirlenebilir yapan bütün veriler kişisel veri sayılacaktır”²¹.

Kişiyile ilgili nesnel bilgilerin yanı sıra bir kişinin hakkında mevcut görüşler ve değerlendirmeler gibi öznel bilgiler de kişisel veri sayılmaktadır²². Örnek olarak; kişide herhangi bir virüsün varlığı ile ilgili bilgi kişinin nesnel sağlık bilgisidir. Kişinin iş ya da arkadaş ortamında onun hakkındaki görüş ve değerlendirmeler ise kişiye dair öznel bilgiler olacaktır

Bilginin kişisel veri olarak sayılabilmesi için her zaman doğru bilgi olması gerekmemektedir. Doğru olmayan bilgiler de kişisel veri olabilir. Böyle bir durumda verisi yanlış işlenen bireyin işlenmekte olan veriye ilişkin bilgilendirilme hakkı ve ilgili verinin düzeltilmesini talep etme hakkı mevcut olacaktır²³. Bu hakkın kullanılması için yanlış bilgilerin de kişisel veri gibi kabul edilmesi gerekmektedir²⁴.

1.1.2.2. Kimliği Belirli veya Belirlenebilir Kişi

Kişisel verinin diğer unsuru kimliği belirli veya belirlenebilir kişidir. Burada öncelikle kişi kavramı üzerinde durulacak, ardından kişi bakımından belirli veya belirlenebilir olma unsurunun anlamı anlatılacaktır. Kişi kavramı etimolojik olarak,

Compatibility with directive 95 / 46 stronger protection of personal data by the legislation of a Member State”, C-101/01, 06.11.2003, 62001CJ0101 - EN - EUR-Lex, E.T.: 10.09.2022.

²¹ Anayasa Mahkemesi, Basın Duyurusu, 29.07.2021, Başkasına Ait Bilgilerin Sosyal Medya Hesabında Paylaşılması Nedeniyle Kişisel Verilerin Korunmasını İsteme Hakkının İhlal Edilmesi | Anayasa Mahkemesi, E.T.: 11.09.2022

²² Özkan, a.g.e, s. 11.

²³ Bu hususa “Veri sahibinin hakları” bölümünde değinilecektir.

²⁴ Data Protection WP, Concept, s. 6.

insan, kimse, şahıs, eş, koca, erkek, bir eserde (oyun, roman, hikaye) yer alan kimse, çekimli fiillerde, zamirlerde konuşan, dinleyen, sözü edilen varlık, şahıs, insan olarak tanımlanmaktadır²⁵.

Türk Medeni Kanunu (“TMK”) uyarınca, “*Kişilik çocuğun sağ olarak tamamıyla doğduğu anda başlar ve ölümle sona erer*”²⁶. TMK’ya göre kişi, gerçek kişi ve tüzel kişi olarak iki ayrı kısımda incelenmiştir. İnsanlar gerçek kişilerdir ve madde 8 uyarınca “*Her insan hak ehliyetine sahiptir*”. Aynı kanunun 47. maddesi uyarınca gerçek kişiler dışında kalan ve hak ehliyetine sahip olan, belirli ve sürekli bir amacı gerçekleştirmek için kurulmuş ama onu kuran kişiden bağımsız olan kişi veya mal toplulukları tüzel kişilerdir²⁷.

Avrupa Birliği (GVKT) ve Türk özel hukukundaki (KVKK) düzenlemelere bakıldığında kişisel verilerinin korunması kapsamına tüzel kişilerin değil, gerçek kişilerin verilerinin dahil olduğu görülmektedir. GVKT’de, 14. paragrafta kişisel verilerinin korunması kapsamına tüzel kişilerin girmediği açıkça vurgulanmıştır. Aynı şekilde, KVKK’da madde 2’de kanunun “*kişisel verileri işlenen gerçek kişiler*”e uygulanacağı açıkça belirtilmiştir. Ancak tüzel kişilere dair bilgiler gerçek bir kişiye dair kişisel verileri ulaşılabilir kıldığı durumda bu bilgiler de koruma kapsamında olacaktır²⁸. Örneğin; bir hastahanenin hasta kayıt sisteminin ele geçirilmesi durumunda hastalara ilişkin kişisel veriler bahsettiğimiz veri koruma düzenlemeleri kapsamında değerlendirilecektir.

Konuya ilişkin önem arzeden hususlardan bir diğeri ceninin kişisel verinin korumasından yararlanıp yararlanamayacağıdır. TMK 28. madde uyarınca, “*Çocuk hak ehliyetini, sağ doğmak şartıyla anne rahmine düştüğü anda elde eder*”. Kanunun metninde ceninin hak ehliyetinin başlangıcı olarak “*ana rahmine düşmüş*” olma gösterilse de,²⁹ kişiliğin başlangıcı ile hak ehliyetinin kazanılması aynı anda gerçekleşmemektedir³⁰. Hak ehliyetinin kazanılması sağ doğma koşuluna bağlanmıştır. Çalışma Grubu’na göre ise doğumdan önceki dönemde ceninin kişisel

²⁵ Ömer Ergün, “Kişilik Kavramı ve Çeşitleri”, Dicle Üniversitesi Adalet Meslek Yüksekokulu Dicle Adalet Dergisi, Cilt 1, Sayı 1, 2017, s. 2-3.

²⁶ TMK, m. 28.

²⁷ Fahri Erdem Kaşak, “Tüzel Kişilik Kavramı ve Tüzel Kişilik Perdesinin Kaldırılması”, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, Cilt 26, Sayı 2, 2020, s. 1243.

²⁸ Özkan, a.g.e, s. 15-16.

²⁹ Leyla Müjde Kurt, “Cenin Mal Varlığı Hakları”, İnönü Üniversitesi Hukuk Fakültesi Dergisi, Cilt 2, Sayı 1, 2011, s. 184.

³⁰ Fatih Burak Uzun, “Gerçek Kişilerin Hak Ehliyeti ve Hak Ehliyetine Uygulanacak Hukukun Tespiti”, Hacettepe Hukuk Fakültesi Dergisi, Cilt 6, Say 2, 2016, s. 7.

verilerinin korunmasından yararlanması durumunun tespit edilmesi için devletlerin ulusal düzenlemelerine bakılmalıdır³¹.

Türk Medeni Kanunu madde 28 uyarınca kişilik ölümle sona erer. Bu nedenden ötürü ölmüş kişilerin bilgilerinin kişisel verilerin korunması kapsamında değerlendirilmediği savunulmaktadır³². Aynı şekilde GVKT 27. paragrafta da ölmüş kişilerin bu düzenleme kapsamına girmediğinden bahsedilmiştir. Ancak ölmüş kişilere ilişkin bilgilerin yaşayan kişilere ilişkin bilgileri etkileyeceği durumlarda artık bu bilgilerin de kişisel verilerin korunması kapsamına girmesi mümkündür. Örneğin; ölmüş kişinin taşıdığı herhangi genetik hastalığın doktoru ve sair kişiler tarafından açığa çıkarılması sonucu bu kişinin yaşayan yakınlarına ilişkin kişisel verilerin açıklanması durumu söz konusu olacağından ölmüş kişiye ait bilginin de kişisel verilerin korunması kapsamında muhafaza edilmesi gerekmektedir³³.

Bir kişinin kimliğinin belli olması onun diğer insanlardan ayrıt edilmesi amlamına gelir. Kişinin kimliğinin belirlenebilir olması ise kişinin kimliği henüz belli olmasa bile kişinin diğer insanlardan farkedilmesinin mümkün olması demektir³⁴. Kişinin kimliğinin belirlenmesi bir takım tanımlayıcılar ile gerçekleştirilir. Kişinin ismi de bu tanımlayıcılar arasındadır. Fakat kişinin belirlenmesi ve tespiti için her zaman ismi gerekmemektedir³⁵. Kişiye ait çeşitli bilgiler yalnız bir şekilde kişiyi belirlemeye yeterli olmasa bile hepsi bir araya gelerek kişi belirleyebilir³⁶. Yukarıda, kişisel veri kavramının tanımı sırasında belirtilen “fiziksel, fizyolojik, genetik, ruhsal, ekonomik, kültürel veya toplumsal kimliğine özgü bir ya da daha fazla sayıda faktör” birbaşına herhangi bir kişiyi belirlemeye yetmese de, hepsi veya birkaçı birleşirse bir kişi tespit edilebilir³⁷.

Diğer bir durumda tam aksine kesin bir şekilde tanımlayıcı nitelikte olduğunu düşündüğümüz verilerin kişisel veri olmaması mümkündür. Örneğin, ülkede çok

³¹ Data Protection WP, Concept, s. 23.

³² Özkan, a.g.e, s. 16.

³³ Özkan, a.g.e, s. 17.

³⁴ Data Protection WP, Concept, s. 22.

³⁵ Data Protection WP, Concept, s. 14.

³⁶ Aksoy, a.g.e, s. 23; Murat Develioğlu, 6698 Sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku, İstanbul, On İki Levha Yayıncılık, 2017, s. 33.

³⁷ Data Protection WP, Concept, s. 13.

insanın kullandığı yaygın bir isimden söz edildiğinde bu bilgi kişisel veri niteliğinde değerlendirilmeyecektir³⁸.

Konuya ilişkin olarak Avrupa Birliği Adalet Divanı (“ABAD”) Kasım 2003 yılında kabul edilen C-101/01 sayılı, “*Lindqvist*” kararında bir internet sayfasında çeşitli kişilere atıfta bulunulması, bu kişilerin adlarıyla veya başka yollarla, örneğin telefon numaralarının veya çalışma koşulları ve hobileri ile ilgili bilgilerin verilmesi suretiyle kişinin dolaylı yoldan tespit edildiğini, bu nedenle bu tür verilerin kişisel veri olduğunu vurgulamıştır³⁹.

Biyometrik sayılan, parmak izi ve iris gibi veriler de kişiyi başkalarından ayıran ve onu belirlenebilir yapan özelliklerdendir. Günümüzde parmak izi ve iris gibi yalnız kişiye özel olan bu veriler bazı güvenlik sistemlerince kullanılmaktadır. Konuya ilişkin Kişisel Verileri Koruma Kurulu⁴⁰ kararında “*üstün güvenlik önlemi alınmasına ihtiyaç duyulmayan alanlarda yalnızca mesai kontrolü amacıyla parmak izi alınmasına yönelik uygulamaların*” ölçülülük⁴¹ ilkesine aykırı olduğu belirtilmiştir⁴².

Kişiyi belirlenebilir kılma olasılıklarından dolayı takma adlar, anonim veriler ve diğer bilgiler ile birleştirildiğinde kişi tanımlanabiliyorsa mahlas ve lakap da⁴³ kişisel veri olarak kabul edilir⁴⁴. Anonim veriler kişisel veriler öyle verilerdir ki, onlar başka verilerle eşleştirilirse dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemezler. Takma adların kullanıldığı veriler ise, bir ek bilgiler ile biraraya geldiklerinde kişinin belirlenebilmesini mümkün kılan verilerdir⁴⁵. Bunun esas nedeni takma ad ile kişi arasında bağlantı kurulması ihtimalinin mevcut olmasıdır⁴⁶.

³⁸ Jenna Kersten, “What is GDPR Personal Data and Who is a GDPR Data Subject?”, What is GDPR Personal Data and Who is a GDPR Data Subject? | GDPR Compliance, E.T.: 16.04.2022.

³⁹ Avrupa Birliği Adalet Divanı, C-101/01 sayılı ve 06.11.2003 tarihli kararı, 62001CJ0101 - EN - EUR-Lex, E.T.: 11.09.2022.

⁴⁰ Bundan böyle “*Kurul*” olarak anılacaktır.

⁴¹ Kişisel verilerin işlenmesine ilişkin temel ilkelerden biridir. Çalışmamızın sonraki bölümlerinde daha detaylı anlatılacaktır.

⁴² Kurul Kararı, 01.12.2020, <https://kvkk.gov.tr/Icerik/6872/2020-915>, E.T: 12.07.2022.

⁴³ Kurum, Örnekler, s. 4.

⁴⁴ Ezgi Çabuk, Avrupa Birliği düzenlemeleri ışığında Türk hukukunda kişisel verilerin korunması, Yüksek Lisans Tezi, Bahçeşehir Üniversitesi, Sosyal Bilimler Enstitüsü, İstanbul, 2020.

⁴⁵ Develioğlu, a.g.e, s. 36.

⁴⁶ Özkan, a.g.e, s. 19.

1.1.2.3. Bilginin Kişiyeye İlişkin Olması

Genel anlamıyla kişiyeye alakalı olan, yani onun karakterine, davranışlarına, hislerine ve saire kişiyeye bağılı olan her şeye atıf yapan, onu belirlenebilir kılan bilgiler kişiyeye ilişkin bilgilerdir⁴⁷. Bahsi geçen bilgi direkt olarak kişinin kendi ile ilgili olmasa bile, kişinin kendisine dair bilgilere erişilmesine, dolayısıyla ona ulaşılmasına yol açıyorsa, bu bilgiler kişiliğe ilişkin bilgilerdir⁴⁸.

Bilginin kişiyeye ait olması durumu üç unsurun: içerik, amaç ve sonuç unsurlarından herhangi birinin olması halinde tespit edilebilir. Bu unsurlardan herhangi birinin varlığı yeterli olup, üçünün aynı anda mevcut olması beklenmemektedir⁴⁹.

İçerik unsuru bakımından bilgi ve bireyin arasında ilişki kurulması için bilginin kişi “*hakkında*” olması gerekmektedir. Örneğin, herhangi bir giyim mağazasında müşterinin kaydedilmiş bilgileri onu ulaşılabilir kılıyorsa, bu bilgiler kişisel veri sayılacaktır⁵⁰. Benzer diğere bir örnekte, online alışveriş yaparken mağaza sahibine müşteri tarafından verilen bilgilerin içeriği kişisel veri sayılacaktır.

Bilgi ve kişi arasındaki ilişkinin belirlenmesi “*amaç*” hususu ile de ilgili olabilir. Burada önemli olan bilginin kullanılma amacıdır⁵¹. Kurul konuya ilişkin bir kararında, “*Hastalardan alınan kan, serum ve doku örneklerinin bilimsel amaçlarla kaydedildiği ve manunun 28. maddesi kapsamında bu verilerin işlenmesinin milli savunmayı, milli güvenliğı, kamu güvenliğini, kamu düzenini, ekonomik güvenliğı, özel hayatın gizliliğini veya kişilik haklarını ihlal etmediğı ya da suç teşkil etmediğı değerlendirildiğinden şikayet hakkında bu aşamada yapılacak bir işlem olmadığına*” karar vermiştir⁵².

Bilginin kişiyeye ilişkin olması durumunun belirlenmesinde sonuncu ve daha zor olanı “*sonuç*” unsurudur. Bu hususta dikkat edilmesi gereken mesele bilginin kullanılması durumunun kişinin haklarına etki etmesidir⁵³. Online alışveriş esnasında

⁴⁷ Data Protection WP (2005), 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.: 04.12.2021.

⁴⁸ Özkan, a.g.e, s. 20.

⁴⁹ Data Protection WP, Concept, s. 10.

⁵⁰ Data Protection WP, Concept, s. 10.

⁵¹ Data Protection WP, Concept, s. 10.

⁵² Kurul Kararı, 30.10.2019, <https://www.kvkk.gov.tr/Icerik/6876/2019-316>, E.T.: 12.07.2022.

⁵³ Data Protection WP, Concept, s. 10.

kişinin kendi kart veya adres bilgilerini paylaşması sonrası satıcı tarafından bu bilgilerin kişinin iradesi dışında kullanılması duruma örnek olarak gösterilebilir.

1.1.3. Türleri

GVKT’de ve KVKK’da yer alan düzenlemelere bakıldığında kişisel verilerden bahsedilirken “*özel nitelikli kişisel veriler*” kavramına yer verildiğini görülmektedir. Bu bağlamda kişisel verilerin genel nitelikli ve özel nitelikli olarak ayrıldığını söylemek mümkündür. Özel nitelikli kişisel veriler öyle verilerdir ki, bu verilerin başka kişilerce kullanılması veri sahibini diğer kişilerden farklı davranışlara, ayrımcılığa maruz koyabilir⁵⁴. Bu nedenle bu tür verilerin özel olarak korunması gereklidir.

Öncelikle türk hukukunda özel nitelikli kişisel verilere nazaran özel ayırım yapılmış, hangi verilerin özel nitelikli veri sayıldığı sayma yoluyla “*sınırlı sayıda (numerus clausus)*” belirlenmiştir⁵⁵. Şöyle ki, KVKK ile özel nitelikli veriler “*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*”⁵⁶ olarak sayılmıştır.

Aynı şekilde GVKT ile bazı kişisel verilerin işlenmesinin daha riskli olabileceğini kabul edilerek bu tarz verileri “*özel nitelikli kişisel veriler*” olarak belirlenmiş ve bu verilerin işlenme şartları özel olarak düzenlenmiştir. GVKT’nin 9. maddesine göre ırk veya etnik köken, siyasi görüşler,,dini veya felsefi inançlar, sendika üyeliği, genetik veriler, biyometrik veriler, sağlık ile ilgili veriler, cinsel yaşama veya cinsel eğilime ilişkin veriler özel nitelikli kişisel verilerdir. Dolayısıyla burada gösterilmeyen diğer bütün bilgiler özel nitelikli olmayan (genel nitelikli) kişisel veri olarak değerlendirilecektir.

Herhangi bir verinin özel nitelikli olup olmadığının somut olaya nazaran değerlendirilmesi mümkündür. Kişinin uçak bileti alırken dini inancına bağlı yaptığı

⁵⁴ Kişisel Verilerin Korunması Kanunu Tasarısı ve Adalet Komisyonu Raporu, (1/541) s. 9, <https://www.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf>, E.T.: 23.04.2022.

⁵⁵ Özkan, a.g.e, s. 22.

⁵⁶ KVKK, m. 6/1.

yemek seçimi bilgisi kişinin özel nitelikli verilerine örnek olarak gösterilebilir⁵⁷. Zira kişiye ilişkin din veya mezhep bilgileri doğası gereği hassastır. Burada dikkat edilmesi gereken verinin kullanım amacıdır. Yani verinin kullanılması bu veriyi özel nitelikli veri gibi kullanma isteği ile ilgili olmalıdır⁵⁸. Bahsi geçen verinin kullanılması ile kişinin ayrımcılığa maruz kalma durumu ortaya çıktığı durumlarda özel nitelikli kişisel verilerden bahsetmemiz mümkün olacaktır.

KVKK'nın 6. maddesinin ikinci fıkrası ve GVKT'nin 9. maddesi uyarınca veri sahibinin açık rızası olmaksızın özel nitelikli verilerin işlenmesi kesinlikle yasaktır. Açık rızanın mevcutluğu işleme faaliyetine konu verinin özel nitelikli ait olup olmamasından bağımsızdır ve veriler söz konusu olduğunda veri sahibinin rızasının açık (bariz) biçimde verilmesi gerekmektedir⁵⁹. Açık rızanın bulunmadığı durumlarda özel nitelikli verilerin işleme şartları her iki düzenlemeye ayrıca düzenlemiştir⁶⁰. GVKT özel nitelikli verilere ilişkin işleme şartlarını KVKK'ya nazaran daha geniş tutmuştur⁶¹.

Karşılaştırdığımız her iki düzenleme uyarınca kişinin sağlığı ve cinsel hayatı ile ilgili bilgileri de özel nitelikli bilgilerdendir ve bu bilgilerin de başka kişiler tarafından bilinmesi, kullanılması veri sahibi için olumsuz sonuçlara neden olabilir. Özel nitelikli veriler KVKK'da sayılmakla birlikte, kanunda bu verilerin tanımı yapılmamıştır. Herhangi bir verinin özel veri kategorisinde olup olmadığının belirlenmesi için sağlık verileri, genetik ve biyometrik veriler gibi teknik anlamı olan hassas veri türlerinin tanımlarının yapılması gereklidir⁶².

KVKK'dan farklı olarak GVKT ile kişisel sağlık verisinin tanımı yapılmıştır. İlgili maddeye göre kişinin fiziksel veya ruhsal sağlığıyla ilgili her türlü bilgi kişisel sağlık verisidir⁶³. “*Kişisel Sağlık Verileri Hakkında Yönetmelik*” ile yapılan tanıma

⁵⁷ Cemil Kaya, “Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas Kişisel Veriler ve İşlenmesi”, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Cilt 69, Sayı 1-2, 2011, s. 322.

⁵⁸ Kaya, a.g. m, s. 317.

⁵⁹ Handbook, 2018, s. 161.

⁶⁰ KVKK'nın 6. maddesi uyarınca Veri sahibinin sağlığına ve cinsel hayatına ilişkin verileri hariç olmak üzere diğer kişisel veriler; kanunlarda belirlenmiş istisnai durumlarda açık rıza olmasa dahi işlenebilirler. İlgili kişinin sağlığına ve cinsel hayatına ilişkin kişisel veriler ise yalnızca kamu sağlığını korumak, koruyucu hekimlik, 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 aranmadan işleme tabi tutulabilir.

⁶¹ İşleme şartlarının tamamı için bkz. GVKT, m. 9(b).

⁶² Özkan, a.g.e, s. 23.

⁶³ GVKT, m. 4/15.

göre ise kimliği belirli veya belirlenebilir gerçek kişinin fiziksel ve ruhsal sağlığı ile ilgili kişiye sunulan sağlık hizmetlerine ilişkin bilgiler kişisel sağlık verisidir⁶⁴.

GVKT ile genetik verilerin de tanımı yapılmıştır. İlgili madde uyarınca genetik veriler, “*gerçek kişiye ait fizyoloji ya da sağlık hakkında benzersiz bilgi veren ve özellikle söz konusu kişiden alınan bir biyolojik numunenin analizinden kaynaklanan ve söz konusu kişinin kalıtsal özellikleri ile ilgili kişisel veriler*”⁶⁵, biyometrik veriler ise, *gerçek kişiye ait fiziksel, fizyolojik veya davranışsal özelliklerine ilişkin olan, yüz görüntüleri gibi gerçek kişinin benzersiz olarak tanınmasını sağlayan, özel teknik işlemekten kaynaklanan*” kişisel verilerdir.⁶⁶

GVKT ve KVKK’da özel nitelikli kişisel verilerin işlenmesi bakımından bazı farklılıklar mevcuttur. Şöyle ki, GVKT ile kişinin cinsel yönelime ilişkin veriler de özel nitelikli sayılmasına rağmen KVKK kapsamında bu konuya ilişkin ayrıca bir koruma belirlenmemiştir. Ancak cinsel hayata ilişkin veriler KVKK’da özel nitelikli olarak düzenlendiğinden cinsel yönelimine ilişkin verilerin kanunla özel nitelikli kişisel veri sayılacağını söylemek mümkündür⁶⁷.

Avrupa Birliği hukuku ve Türk özel hukukunda özel nitelikli kişisel verilerin korunması arasında bir diğer farklılık kılık ve kıyafete ilişkin veriler KVKK ile özel nitelikli kişisel veri sayılırken, GVKT’de böyle bir hususun olmamasıdır. Kılık ve kıyafete ilişkin verilerin özel nitelikli sayılması kültürle, sosyal yaşamda kılık kıyafetin kimlik belirleyici niteliğe sahip olmasıyla ilgilidir. Hatta çokuluslu yapıda olan Osmanlı Devleti’nde giyim ve kuşam sosyal, ekonomik, hatta dini bakımdan insanları tanımak için bir araç olarak görülmekteydi⁶⁸. Günümüzde de kişinin kılık kıyafetine ilişkin verilerin kişinin açık rızası olmaksızın işlenmesi sonucu kişinin özellikle din ve vicdan hürriyetinin ihlali söz konusu olabilir⁶⁹.

⁶⁴ Resmi Gazete, 21.06.2019, Kişisel Sağlık Verileri Hakkında Yönetmelik, Sayı 30808.

⁶⁵ GDPR, m. 4/13.

⁶⁶ GDPR, m. 4/14.

⁶⁷ Yüksel Tolun, Kişisel Verilerin KVKK ve GVKT Kapsamında Korunması, Yüksek Lisans Tezi, Kırıkkale Üniversitesi, Sosyal Bilimler Enstitüsü, Kırıkkale, 2020, s. 71.

⁶⁸ Necdet Aysal, “*Tanzimat’tan Cumhuriyet’e Giyim ve Kuşamda Çağdaşlaşma Hareketleri*”, Çağdaş Türkiye Tarihi Araştırmaları Dergisi, Cilt 10, Sayı 22, 2011, s. 3,4.

⁶⁹ Tolun, a.g.t, s. 71, Kılık kıyafete ilişkin ayrımcılık konusu ile ilgili AIHM karar örnekleri için bkz. European Court of the Human Rights (“ECHR”),(2021), “*Factsheet – Religious symbols and clothing*”, 2021, https://www.echr.coe.int/documents/fs_religious_symbols_eng.pdf, E.T.: 03.09.2022.

1.1.4. Hukuki Niteliği

Kişisel verilerin korunması hukukunda korunan yalnızca veriler değil, aynı zamanda veri sahibi gerçek kişilerdir. Bu bağlamda gerçek kişilere dair birçok bilgi, özel hayat, insanın şerefi, onuru ve saire gibi birçok kavramın korunmasından bahsetmemiz mümkündür. Aynı şekilde bu verilerin hangi amaçla korunuyor olduğu önem arz etmektedir. Doktrinde kişisel verilerin hukuki niteliğine dair çeşitli görüşler bulunmaktadır. Konuya mukayeseli hukuk çerçevesinde bakıldığında Anglo–Amerikan hukuk sisteminde kişisel veri kavramının genel olarak “*ekonomik ve iktisadi bir yaklaşımla mülkiyet ve/veya fikri haklar*” kapsamında, Kıta Avrupası hukuk sisteminde ise “*sosyal ve hümanist bir yaklaşımla temel insan hakları ve/veya kişilik hakkı*” kapsamında ele alındığı görülmektedir⁷⁰. Çalışmamızın bu bölümünde ilgili üç görüşü inceleyecek, kişisel verilerin korunma amacına ilişkin hukuki niteliğini anlatmaya çalışacağız.

1.1.4.1. Mülkiyet Hakkı Görüşü

Kişisel verinin, sahibinin bir parçası olmasının yanı sıra onun bir ürünü olarak kabul edilmesi gerekliliği düşüncesine dayanan bu yaklaşım daha çok Anglo–Amerikan hukuk sisteminde kabul edilmektedir. Bu yaklaşıma göre kişisel veri, yalnızca sahibinin kişiliğinin bir uzantısı (parçası) değil, aynı zamanda ilgili kişiliğin ürünü olarak kabul edilmelidir⁷¹. Kişisel verilerin mülkiyet hakkı olması görüşü genel olarak Amerika Birleşik Devletleri menşeli olup kişisel verinin, kural olarak eşya hukukundaki “şey” kavramıyla aynı olduğu yönündedir. Mülkiyet hakkı mutlak bir haktır⁷². Mülkiyet hakkının sahibine eşya üzerinde tanıdığı haklar “*kullanma yetkisi*”, “*yararlanma yetkisi*” ve “*tasarruf yetkisi*” olarak sayılabilir⁷³. Bu görüşe göre ilgili kişi, yani veri sahibi, kendi kişisel verileri üzerinde kullanma, yararlanma ve tasarruf yetkilerine sahiptir. Eşya hukuku esaslarına göre hak sahibi, malik her nasıl mülkiyetini haiz olduğu eşyaları kullanabiliyor, onlardan yararlanabiliyor

⁷⁰ Sinan Sami Akkurt, “Kişisel Veri Kavramının Hukuki Niteliğine İlişkin Yaklaşımlara Mukayeseli Bir Bakış”, *Kişisel Verileri Koruma Dergisi*, Cilt 2, Sayı 1, 2020, s. 21-22.

⁷¹ Akkurt, a.g.m, s. 22; Aksoy, a.g.e, s. 215.

⁷² Rona Serozan, *Eşya Hukuku I*, Genişletilmiş 3. Bası, İstanbul, Filiz Kitap Evi, 2014, s. 202.

⁷³ Jale Akipek / Turgut Akıntürk / Derya Ateş, *Eşya Hukuku*, 15. Baskı, İstanbul, Beta Yayıncılık, 2019, s. 380, O. Gökhan/ Murat Topuz, *Eşya Hukuku*, C. IV/1, Genişletilmiş 3. Baskı, Ankara, Seçkin Yayıncılık, 2019, s. 110, A. Lale Sirmen, *Eşya Hukuku*, 6. Baskı, Ankara, Legal Kitabevi, 2018, s. 29.

ve/veya bunlar üzerinde tasarrufta bulunabiliyorsa kişisel verileri üzerinde de aynı hak ve yetkileri kullanabilmelidir. Yani ilgili kişi, hukuka aykırı şekilde ihlal edildikleri takdirde mülkiyet hakkının sağladığı koruyucu yetkileri/imkanları kullanarak verileri üzerinde tam bir denetime kavuşabileceği gibi, bunların kullanımını karşılıklı yada karşılıksız olarak devredebilir, verileri üzerindeki yetkilerini satış, kira gibi borç ilişkilerine konu edebilir⁷⁴. Özetle bu görüşe göre mülkiyet hakkının kişiye sağladığı tüm haklar kişisel veriler üzerinde de sağlanmalıdır.

“Verilerin mülkleştirilmesini”⁷⁵ destekleyen görüşe göre, kişiler kendi kişisel verilerini “*adil bir bedel*”⁷⁶ karşılığında satabilirler⁷⁷. Günümüzde kişisel verilerin maddi değeri yükselmektedir. Buna bağlı olarak şirketler bu verileri kendi faaliyetlerinde kullanıp yarar elde etmenin yanı sıra bu verilerin satılması yoluyla da ciddi gelir elde etmektedirler⁷⁸. Nitekim veri sahipleri de bu verilerin satılmasından bir kazanç elde etmektedirler. Ancak veri toplayanlar verilerin alınması karşılığında bir bedel vermeyebilir ya da verdikleri bedel çok az olabilir. Bu görüşü destekleyenlere göre kişisel verileri işleyen kuruluşlar işledikleri veriler karşılığında veri sahiplerine uygun bir bedel ödemek zorunda bırakıldıklarında işleyecekleri veri miktarı da daha az olacaktır. Doktrinde veri işleyen şirketlerin işledikleri veriler karşılığında bedel ödememek için daha az veri işleyecekleri ve sonuç olarak kişisel verilerin korunacağı düşünülmektedir⁷⁹. Verilerin sahiplerinden satın alınması veri toplayanlar için ek maliyete neden olacak ve böylelikle şirketler daha az veri işleyecektir. Bunun sonucunda veri sahipleri daha iyi korunacaktır. Aynı şekilde günümüzde mevcut olan hukuk düzenlemelerinde mülkiyet hakkına ilişkin sistem mevcut olduğundan ülkeler mali ve hukuki yönden veri korumaya ilişkin bir

⁷⁴ Akgül Aydın, “Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması”, 2. Basım, İstanbul, Beta Basım Yayın, 2014, s. 74, Jagner Edward J, “Privacy Property, Information Costs and the Anticommons”, Hastings Law Journal, Cilt 54, Sayı 4, 2003, s. 899; Prins Jej., “The Propertization of Personal Data and Identities”, Electronic Journal of Comparative Law, Cilt 8, Sayı 3, 2004, s. 1.

⁷⁵ Elif Küzeci, “Kişisel verilerin Korunması” Yenilenmiş ve Gözden Geçirilmiş 3. Baskı, Ankara, On İki Lehta Yayıncılık, 2019, s. 60.

⁷⁶ Prins, a.g.m, s. 1.

⁷⁷ Kanf Jerry, “Information Privacy in Cyberspace Transactions”, Standorf Law Review, 50, s. 1193-1294, 2004, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=631723, E.T.: 10.09.2022., s. 1256.

⁷⁸ Özkan, a.g.e, s. 27.

⁷⁹ Aksoy, a.g.e, s. 59.

maliyetten kurtulmuş olacaktırlar⁸⁰. Ayrıca mülkiyet hakkı görüşünün kabul edilmesi sonucunda verilerin verileri toplayanlara değil, veri sahiplerine ait olması da netlik kazanacaktır⁸¹.

Söz konusu görüşün eleştirildiği ilk konu verilerini satan kişilerle verilerin satıldığı kişiler arasında çıkar eşitliğinin olmaması⁸², taraflardan birinin daha çok kazaması⁸³ sonucu adaletsiz durumların ortaya çıkması ihtimalidir. Örnek olarak bu tür durumlarda taraflardan birinin işveren, şirketler, kamu veya diğer kuruluşlar olması durumunda adil bir alış verişi söz konusu olmayacaktır.

Konuya ilişkin temel eleştiri ise kişisel verilerin mülkiyet hakkı kavramı bağdaşmaması ile ilgilidir. Şöyle ki, mülkiyet hakkının sahibine sağladığı kullanma, yararlanma, tasarrufta bulunma yetkileri kişiye hakka konu olan eşya üzerinde direkt yetkiler sağlamakla beraber, kişiye hakkını başkalarına karşı ileri sürebileceği yetkilerdir. Burada özellikle tasarruf yetkisinin kişisel verilerle uyuşmadığı görülmektedir. Veri sahibinin maliki olduğu veriye ilişkin tasarruf yetkisini kullanması ile beraber verinin başkasına devredilmesi sonucu veri sahibi artık o veri üzerinde herhangi bir yetkiye sahip olmayacak ve kendi verileri üzerinde kontrolü kaybedecektir. Bu veri sahibinin kendi verilerinden tamamen soyutlandığı, “*kişi*” ve “*veri*” arasında mevcut bağın kopması anlamına gelecektir⁸⁴.

Kanaatimizce, kişisel verilerin mülkiyet hakkı niteliği taşımasına ilişkin eleştiriler haklıdır. Her şeyden önce kişisel verilerin mülkiyet hakkı olması kişisel verilerin taşıdığı öz anlam ile bağdaşmamaktadır. Çünkü kişisel verilerin özünde yalnızca kişiye ait olan ve maddi değer taşıyan konular değil hem de onun sağlığına, cinsel yaşamına, özel yaşamına, ırkına, siyasi ve dini görüşlerine ait, özetle kişiyi insan olarak nitelendirebilecek tüm bilgiler dahil olabilir. Bu bilgilerin kendi sahipleri tarafından pazarlık konusuna çevrilmesi, kişinin kendisine ait verileri satması ve bu verilere dair yetkilerini devretmesi ona maddi ve manevi zarar gelmesine neden olabilir. Sonuç olarak mülkiyet hakkı görüşünün kişinin haklarından soyutlanması nedeniyle kabul edilmesi mümkün görünmemektedir.

⁸⁰ Furkan Güven Taştan, Türk Sözleşme Hukukunda Kişisel Verilerin Korunması, İstanbul, On İki Lehva Yayıncılık, 2017, s. 53, Aksoy, a.g.e, s. 58.

⁸¹ Prins, a.g.m, s. 279.

⁸² Bibas Steven A.,(1994) “A Contractual Approach to Data Privacy”, Harvard Journal of Law & Public Policy, 17(2), s. 591-611.

⁸³ Küzeci, a.g.e, s. 61.

⁸⁴ Aksoy, a.g.e, s. 65.

1.1.4.2. Fikri Hak Görüşü

Kişisel verilerin hukuk niteliğine dair görüşlerden bir diğer kişisel verilerin fikri mülkiyet hakkı olduğu yönündedir. Teoride kişisel verilerin fikri haklar gibi telif hakları ile korunduğu fikri mevcuttur⁸⁵. Manevi haklar kişiye herhangi bir getirisi olmayan, onun manevi bağları ile ilgili haklardır⁸⁶. Fikri mülkiyet hakkının korunması kapsamında kişi kendi eserine kazandırdığı özelliklerin değiştirilmesini önleyebilir, onu kamuya tanıtabilir. Aynı şekilde eserin kamuya tanıtılmasına, ne zaman ve hangi şekilde, kimin adı ile savunulmasına dair kararlar verebilir⁸⁷. Dolayısıyla esas benzerlik bilginin korunması ve dağılımının kontrolde tutulmasıdır⁸⁸.

Bu görüşü destekleyenlere göre kişinin kendi verileri üzerine hakim olduğu hakları ile fikri mülkiyet hakkı kapsamında sahip olduğu “*eseri umuma arz yetkisi*” ve “*eserde değişiklik yapılmasını yasaklama yetkisi*” gibi hakları benzemektedirler⁸⁹. Bu haklardan ilki çerçevesinde eser sahibi kendi eserini umma arz edebilme, yayımlanma zamanını ve şeklini belirleyebilme yetkilerine sahiptir⁹⁰. Eserde değişiklik yapılmasını yasaklama yetkisi kapsamında ise eğer eser sahibi izin vermezse, onun sahibi olduğu eserde ya da eserin adında kısaltma, ekleme veya diğer değişiklikler yapılamaz⁹¹. Bu benzerlik doğrultusunda, eser sahiplerinde olduğu gibi, kişisel veri sahipleri de verilerinin hangi kişilerle ve ne şekilde paylaşılacağını belirleyebilir. Hatta verileri kendi elinde olmazsa dahi bu verilerin bütünlük ve doğruluğunun korunması talebinde bulunabilir⁹².

Kişisel verilerin fikri mülkiyet hakkı ile eşleştiğini eleştirenler fikri mülkiyet hakkının konusu olan eserlerin bilinçli bir çaba sonucu üretildiğini, kişisel verilerin ise tamamen kişinin insan olmasından kaynaklanan, hiçbir çaba sarfetmeden günlük yaşama dair bilgiler, veriler olduğunu savunmaktadırlar⁹³.

Fikri mülkiyet hakkı görüşüne ilişkin diğer fark ise bu hakların kullanım amaçları ile ilgilidir. Şöyle ki, eserlerin kullanım ve korunma sebeplerinin temelinde

⁸⁵ Aksoy, a.g.e, s. 60, Küzeci, a.g.e, s. 62.

⁸⁶ Ahmet Kılıçoğlu Sınai Haklarla Karşılaştırmalı Fikri Haklar, Genişletilmiş-Gözden Geçirilmiş 2. Bası, Ankara, Turhan Kitabevi, 2013, s. 260.

⁸⁷ Kılıçoğlu, 2013, a.g.e, s. 262.

⁸⁸ Aksoy, a.g.e, s. 60.

⁸⁹ Aksoy, a.g.e, s. 61.

⁹⁰ Kılıçoğlu, 2013, a.g.e, s. 265.

⁹¹ Kılıçoğlu, 2013, a.g.e, s. 271.

⁹² Aksoy, a.g.e, s. 61.

⁹³ Aksoy, a.g.e, s. 66.

ekonomik nedenler mevcutken ve bu nedenler eser sahibini yeni eserler meydana getirmeye teşvik ederken, kişisel verilerin korunmasında ise esas amaç veri sahibinin rızası dışında ona ait verilerin toplanmasını, kullanılmasını, yayılmasını engellemek, özetle veri dolaşımının kontrolüdür⁹⁴.

1.1.4.3. Kişilik Hakkı Görüşü

Kişisel verilerin hukuki niteliği ile ilgili başka bir görüş kişilik hakkı görüşüdür. Kişilik hakkı kavramını oluşturan değerlerin tek tek sayılması mümkün olmasa da⁹⁵, bu hak kişinin kişiliğini oluşturan, onu insan kılan tüm maddi ve manevi değerlere, sağlığına, onuruna, saygınlığına, özel yaşamının gizliliğine, sözüne, resmine, eserine, özgürlüğüne, ekonomik serbestliğine ilişkin⁹⁶, dolayısıyla kişiliği oluşturan ve diğer kişiler ile arasındaki farklılığı ortaya koyan⁹⁷ tüm değerler üzerindeki haktır⁹⁸. Hangi değerlerin kişilik hakkına konu olabileceği sınırlı olarak belirtilmediğinden bu tespit hakim tarafından somut olay bazında yapılmaktadır⁹⁹. Kişilik hakkı yalnızca sahip olduğu kişi tarafından kullanılmalıdır. Çünkü bu hak sahibine sıkıca bağlıdır¹⁰⁰. Hakkın kendisinin ve ona ilişkin değerlerin devredilmesi mümkün değildir¹⁰¹. Kişilik hakkı miras olarak geçmeyeceği gibi kişinin ölümüyle son bulur. Kişilik hakkına konu değerler malvarlığı haklarına değil, şahıs varlığı haklarına dahildir¹⁰². Ancak bu kişilik hakkına karşı yapılmış saldırıların malvarlığına her zaman etkisiz olacağı anlamına gelmemektedir. Zira kişilik hakkına

⁹⁴ Çabuk, a.g.t, s. 46.

⁹⁵ Nihat Yavuz, Borçlar Hukuku El Kitabı, Ankara, Adalet Yayınevi, 2018, s. 257, Mine Kaya, Elektronik Ortamda (Elektronik haberleşme – İnternet – Sosyal Medya) Kişilik Hakkının Korunması, 1. Baskı, Ankara, Seçkin Yayınları, 2015, s. 32.

⁹⁶ Rona Serozan, Kişilik hakkının korunmasıyla ilgili bazı düşünceler, İstanbul Üniversitesi Mukayeseli Hukuk Araştırmaları Dergisi, Sayı 14, 1997, s. 93.

⁹⁷ Sibel Özel, Uluslararası Alanda Medya ve İnternette Kişilik Hakkının Korunması, 1. Baskı, Ankara, Seçkin Yayıncılık, 2004, s. 27.

⁹⁸ Serap Helvacı, Gerçek Kişiler, 9. baskı, İstanbul, Legal Kitabevi, 2021, s. 69; Aydın/Acabey Zevkiler, Mehmet Beşir/ K. Emre Gökyayla, Medeni Hukuk, Gözden Geçirilmiş ve Genişletilmiş 6. Baskı, Ankara, Seçkin Yayıncılık, 2000, s. 395.

⁹⁹ Helvacı, 2021, s. 103; Ahmet M Kılıçoğlu, Şeref, Haysiyet ve Özel Yaşama Basın Yoluyla Saldırılarından Hukuksal Sorumluluk, Yeniden Gözden Geçirilmiş, Güncelleştirilmiş 5. Bası, Ankara, Turhan Kitabevi, 2016, s. 5.

¹⁰⁰ Rona Serozan, Medeni Hukuk-Genel Bölüm/Kişiler Hukuku, 7. Bası, İstanbul, Filiz Kitab evi, 2017, s. 455.

¹⁰¹ Helvacı, 2021, s. 106.

¹⁰² Helvacı, 2021, s. 105.

karşı yapılmış saldırılar sonucunda kişinin sahip olduğu mal varlığı da maddi bakımdan zarar görebilir¹⁰³. Saydığımız özellikler kişisel verilere de aittir.

Kişisel verilerin korunmasının kişilik hakkının bir uzantısı olduğundan bahsetmeden önce bu hakkın temel bir insan hakkı olup olmaması tartışması üzerinde durulması gerekmektedir. Öncelikle şunu belirtmek gerekir ki kişisel veriler de insan hakları gibi insanın doğası gereği sahip olduğu ve onu belirleyebilecek her türlü bilgilerdir. Bu nedenle kişisel veriler insan hakları ile paralellik oluşturmaktadırlar¹⁰⁴. İlk başlarda kişisel verilerin korunması kişinin temel hak ve özgürlüklerinden olan “*özel hayatın gizliliği*” veya “*özel ve aile hayatına saygı*” başlıkları altında düzenlenmiştir. Daha sonra gelişen teknoloji, kişisel veriler kullanılarak hukuka uygun veya aykırı fiillerin gerçekleştirilmesi imkanını artırdığından özel yaşamın gizliliği ilkeleri kişinin kendi kişisel verileri üzerindeki çıkarlarının korunmasında yetersiz kalmıştır¹⁰⁵. Bu nedenle kişisel verilerin korunması zamanla temel haklardan biri gibi ayrıca bir düzenlenme konusu olmuş ve özel hayatın korunmasından ayrılmıştır¹⁰⁶.

Türkiye Cumhuriyeti Anayasa’sı madde 20 uyarınca kişisel verilerin korunması hakkının “*özel hayatın gizliliği ve korunması*” hakkı kapsamında düzenlenmesinden görüldüğü üzere kişisel veriler ile özel hayat arasında bağlantı kurulmuştur. Dolayısıyla kanun kişisel verilerin temelini kişilik hakkından geldiğini belirten görüşle bir nevi uzlaşmıştır¹⁰⁷.

Kişisel verilerin kişilik hakkı olduğuna dair görüş “*kişisel verilerin korunması*”nı “*mahremiyetin ve özel hayatın korunması*” ile eşleştirildiği için eleştirilmektedir. Nitekim kişisel verilerin korunmasını yalnızca özel hayat korunması ile bağdaştırmak yetersiz olabilir. Çünkü bu kavramlar benzer olsalar bile tam olarak eşanlamlı değildirler. Şöyle ki, kişilik hakkı üç alandan oluşmaktadır ve bu alanlardan yalnız ikisine, özel ve gizli hayat alanına ilişkin korumayı

¹⁰³ Serap Helvacı, Türk ve İsviçre Hukuklarında Kişilik Hakkını Koruyucu Davalar, İstanbul, Beta Basım Yayın Dağıtım, 2001, s. 44.

¹⁰⁴ Murat Volkan Dülger, “İnsan Hakları ve Temel Hak ve Özgürlükler Bağlamında Kişisel Verilerin Korunması”, İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi, Cilt 5, Sayı 1, 2018, s. 109.

¹⁰⁵ Dülger, 2018, s. 78.

¹⁰⁶ Bart van der Sloot, Data Protection and Privacy: (In)visibilities and Infrastructures, “Legal fundamentalism: is data protection really a fundamental right?”, https://link.springer.com/chapter/10.1007/978-3-319-50796-5_1, E.T.: 25.07.2022.

¹⁰⁷ Aksoy, a.g.e, s. 54.

kapsamaktadır¹⁰⁸. Böylelikle, kişisel veriler yalnızca özel hayatla eşleştirildiğinde kamuya açık olan veriler korunamayacaktır¹⁰⁹. Konuya ilişkin olarak Avrupa İnsan Hakları Mahkemesi (“AİHM”) kişinin kimliğini, onur ve şöhretini, kişisel verilerini, fiziksel ve psikolojik bütünlüğünü ve cinsel hayatını özel hayat kapsamında değerlendirmektedir¹¹⁰. Ancak kişisel verilerin korunması “*özel hayata ve aile hayatına saygı hakkı*”nın ötesine geçebilir. Şöyle ki özel hayat kapsamında olmayan değerler de kişisel veri sayılabilir ve hukuki sonuç doğurabilir. Kişinin müşterilere hizmet amaçlı kendi telefon numarasını paylaşması sonucu aynı numaranın paylaşım amacı dışında kullanılması örneğinde özel hayat kapsamında değerlendirilmeyen numara veri sayılırken, numaranın kullanımı ise veriye ilişkin hak ihlalini doğuracaktır. Aynı şekilde bir bilginin kişisel veri sayılması için bu bilginin doğru veya kanıtlanmış olmasına ilişkin bir zorunluluk yoktur. Bilgi gerçek bir kişiye aitse, yanlış da olsa kişisel veridir ve kanunla korunur¹¹¹. Burada esas olan, sosyal ve maddi olarak gerekli olsa bile, verilerin belirli amaca bağlı olarak ve gerektiği kadar paylaşılmasıdır¹¹². “*Bireyin kişisel verilerinin geleceğini belirleme hakkı*”, kişisel verileri ile ilgili karar merciinin kişinin kendisi olmasıdır¹¹³. Bu hak kapsamında kişi verilerinin ne zaman, kimlerce, hangi ölçüde işlenmesine karar verebilir¹¹⁴, sınırsız olarak toplanmasına ve depolanmasına engel olabilir¹¹⁵. Bu nedenlerle kişinin kendisi hakkında doğru olmayan bilgilerden zarar görmemesi için kişisel veri kavramının özel hayatla eşleştirilmesi yerinde olmayacaktır. Özel hayat alanına dahil olmayan kişisel veriler de kanunla korunduğu için kişisel verilerin özel hayatın gizliliği ile tam olarak aynı olmadığını¹¹⁶, dolayısıyla kişisel verilerin korunması hakkının özel hayatın gizliliği ve diğer temel insan haklarıyla olan yakın

¹⁰⁸ Helvacı, 2021, a.g.e, s.122-125.

¹⁰⁹ Prins, a.g.m, s. 281.

¹¹⁰ Yaşar Salihpaşaoğlu, Özel Hayatın Kapsamı: Avrupa İnsan Hakları Mahkemesi İçtihatları Kapsamında Bir Değerlendirme, Gazi Üniversitesi Hukuk Fakültesi Dergisi, Cilt 17, Sayı 3, 2013, s. 243.

¹¹¹ Data Protection WP, Concept, s. 6-7.

¹¹² Damla Gürpınar, Kişisel Verilerin Korunamamasından Kaynaklanan Hukuki Sorumluluk, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, Cilt 19, Sayı 2, 2017, s. 683.

¹¹³ Oğuz Şimşek, Anayasa Hukukunda Kişisel Verilerin Korunması, İstanbul, Beta Basım Yayım, 2008, s. 115.

¹¹⁴ Paul Schwartz, “The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination”, The American Journal of Comparative Law, Cilt 37, Sayı 4, 1989, s. 690.

¹¹⁵ Kemal Atasoy, Kişilik Hakkı Kapsamında Sosyal Medyada Kişisel Verilerin Korunması ve Veri Sahibinin Rızası, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, Cilt 22, Sayı 3, 2016, s. 277.

¹¹⁶ Aksoy, a.g.e, s. 62.

ilişkinine rağmen ayrı bir başlık altında düzenlenmesi gerektiğini¹¹⁷ söylemek mümkündür.

Sonuç olarak, kanaatimizce kişisel verilerin korunmasını yalnızca özel hayatın korunmasıyla eşleştirmek yerinde değildir. Kişisel verilerin kişilik hakkını oluşturan değerlerden biri gibi, yani kişinin kendi verilerinin geleceğini belirleme hakkı gibi kabul etmek daha doğru olacaktır.

Kişisel verileri koruma hakkı, Türkiye Cumhuriyeti Anayasa'sı madde 17'de yer alan "*kişinin maddi ve manevi varlığını koruma ve geliştirme hakkı*" ve "*insan onuru ilkesi*" ile de bağdaşmaktadır. Anayasa'ya göre bu hak sayılan hakların başka bir şeklidir ve verilerin işlenmesi sırasında bu haklara da uyulmalıdır¹¹⁸. Örnek olarak, bir AYM kararında¹¹⁹ "*Kişisel verilerin korunmasını isteme hakkı, insanın onurunun korunması ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimidir. Bu hakkın amacı kişisel verilerin işlenmesi anında şahsın hak ve özgürlüklerini korumaktır*". ifadeleri yer almaktadır.

Bunların beraberinde bazı durumlarda kişisel verilerin yasadışı kullanımı sonucu yalnız veri sahibi kişi değil başkaları da zarar görebilir. Örneğin, kişinin sicil kaydı ile ilgili bilgiler de onun kişisel verileridir. Fakat bu bilgilerin öğrenilmesi durumunda yalnız ona dair bilgiler değil, kişi suç işlemişse mağdura ilişkin bilgiler de başkalarınca öğrenilmiş olacaktır. Diğer bir örnekte anaokuluna giden bir çocuğa dair bilgilere erişilmesi durumunda acil durumlarda irtibat kurulabilecek yetişkinin kişisel verileri ele geçirilebilir¹²⁰. Bu örneklerden de görüldüğü üzere kişisel verilerin boyutları, ihlalleri sonuçları bazı durumlarda yalnızca bir kişiye ilişkin kişilik hakkı ile örtüşmemektedir.

Böylelikle, kişisel verilerin hukuki niteliğine ilişkin görüşleri incelediğimizde verilerin mülkiyet hakkı ve fikri haklar bağlamında korunması mümkün değilken kişilik haklarının içerisinde yer aldığını görüyoruz. Fakat kişisel veriler kişilik hakkı kapsamında tam korunmamaktadır. Bundan dolayı kişilerin kendilerine ait bilgilerin

¹¹⁷ Dülger, 2018, s.79.

¹¹⁸ Şimşek, a.g.e, s. 114.

¹¹⁹ Anayasa Mahkemesi Kararı , 09.04.2014,

<https://normkararlarbilgibankasi.anayasa.gov.tr/Dosyalar/Kararlar/KararPDF/2014-74-nrm.pdf>, E.T.: 11.09.2022.

¹²⁰ Information Commissioner's office (2012), "Determining what is personal data",

<https://ico.org.uk/media/for-organisations/documents/1554/determining-what-is-personal-data.pdf>, E.T: 26.01.2022

geleceğini tayin etmek hakkını saklı tutmak kaydıyla yeni bir hak alanının yaratılmasının daha doğru bir yaklaşım olacağı kanaatindeyiz.

1.2. KİŞİSEL VERİLERİN KORUNMASINDA TARİHİ SÜREÇ

Kişisel verilerin korunması ilk olarak kişilerin kendi mahremiyetini koruma çabasına ilişkin ortaya çıkmıştır. Çağımızda kişisel veriler bağlamında ele alınan mahremiyet kavramı kişilerin yalnız kaldıkları, düşündükleri, davrandıkları, diğer kişilerle hangi sınırlarda ilişki ve iletişim kuracaklarına kendilerinin karar verdikleri bir alanı ifade etmektedir¹²¹. Mahremiyet yakın zamanda geliştirilmiş bir kavram gibi görünse de, hem antropolojik hem de sosyolojik söylemlerde uzun eski kökleriyle tarihi antik Yunan, Roma zamanlarına dayanmaktadır¹²². Milattan önce Antik Yunan’da hasta doktor ilişkilerinde doktorun sır saklama yükümlülüklerini kapsayan mahremiyet kavramı “*Hipokrat Yemini*”nde daha sonra “*Hammurabi Kanunları*”nda, milattan sonra beşinci yüzyılda ise “*Justinianus Kanunları*”nda¹²³ karşımıza çıkmaktadır.

Günümüzdeki anlamıyla mahremiyet yani kişisel verilerin korunması konusu 1960’lı yılların sonunda ve 1970’li yılların başında gündeme gelmeye başlamıştır¹²⁴. Bu yıllarda sanayi devrimiyle birlikte devletlerin ağırlığı hissedilmeye başlamış ve devletlerin getirdiği vergiler ve uyguladığı sosyal politikalar sonucu elde edilen veri miktarı gün geçtikçe artmıştır¹²⁵. Dolayısıyla kişisel verilerinin korunması, ilk olarak devlete karşı başlamıştır. Kişisel verilerin korunmasının bu yıllarda gündeme gelmesinin en önemli nedeni hem özel hem de kamu sektöründe bilgisayar ve elektronik veri iletme yöntemlerinin çok kullanılmaya başlaması olmuştur¹²⁶.

¹²¹ Mehmet Yüksel, “Mahremiyet hakkı ve Sosyo – Tarihsel Gelişimi”, Ankara Üniversitesi, SBF dergisi, Cilt 58, Sayı 01, 2003, s. 187-188, https://doi.org/10.1501/SBFder_0000001619, E.T.: 23.07.2022.

¹²² Toriql Islam, Mohammad Ershadul Karim, “A brief historical account of global data privacy regulations and the lessons for Malaysiya”, Journal of History Department, University of Malaya, Cilt 28, Sayı 2, 2019, s. 171.

¹²³ “*Code of Justinian (Codex Justinianus)*”, XIV kısım için bkz. <http://thelatinlibrary.com/law/institutes.html>, E.T.: 28.01.2022.

¹²⁴ Kadir Can Özel, Ana Hatlarıyla Kişisel Verilerin Korunmasının Tarihsel Süreci ile Amacı ve Kişisel Verilerin Korunması Hakkı, İstanbul Barosu Dergisi, Cilt 94, Sayı 2, 2020, s. 242.

¹²⁵ Cemil Kaya, İdare Hukukunda Bilgi Edinme Hakkı, Ankara, Seçkin Yayıncılık, 2005, s. 88

¹²⁶ Nuri Tortop, “Çağımızın Önemli Sorunu: Kişisel Bilgilerin Güvenliği Sorunu”, Amme İdaresi Dergisi, Cilt 33, Sayı 3, 2000, s. 2.

Verilerin güvenliğini korunması ile ilgili ilk yasal düzenlemeler bahsi geçen dönemlere aittir. 1967 yılında ABD’de kabul edilen “*Bilgi Edinme Özgürlüğü Yasası*” ile bu doğru yönde büyük bir gelişme gibi görünse de, bu kanun yalnızca insanların devlet kurumlarından kendileri hakkında bilgi talep edebilme haklarını kapsamaktaydı¹²⁷. Tarih boyu kişisel verilerin korunmasına ilişkin kabul edilmiş ilk yasal düzenleme Almanya’nın Hessen eyaletinde 1970 yılında kabul edilmiş Veri Koruma Kanunu (“*Hessisches Datenschutzgesetz*”) olmuştur¹²⁸. İsveç’te, 1973’te veri hırsızlığını suç haline getiren ilk federal gizlilik yasası, daha sonra 1978’de Almanya’da kişisel verilerin işlenmesi için rıza dahil olmak üzere temel veri koruma standartlarını oluşturan Alman Federal Veri Koruma Kanunu kabul edilmiştir¹²⁹.

Yukarıda belirtilen örneklerde olduğu gibi AB’ye dahil olan bazı ülkelere kişisel verilerin korunmasına ilişkin özel kanunlar kabul etmiş, Portekiz, Avusturya ve İspanya gibi devletler ise kendi anayasalarına verilerin korunması ile ilgili hükümler eklemiştir. Bu devletler içerisinde yalnız Avusturya’da veri koruma hakkı ilk defa anayasada kullanılmıştır¹³⁰. Sonraki on yıl içinde bilgisayar teknolojisinde oluşan büyük gelişmeler AB’nin 1995’teki Veri Koruma Direktifi’nin kabulü ile sonuçlanmıştır¹³¹. Veri koruma alanındaki ulusal çabalar uluslararası örgütleri sonralar da konuya ilgili düzenlemeler yapmaya tetiklemiş ve bu süreç GVKT’niin kabulü ile noktalanmıştır.

1.2.1. Avrupa Birliği Hukuku (GVKT)

Teknolojinin değişmesi ve gelişmesi sonucu meydana gelen yenilikler ve riskler hukukun yeknesaklaştırılmasını gerekli kılmıştır. Bu nedenle kişisel verilerin korunması alanında Genel Veri Koruma Tüzüğü’nün düzenlenmesi ihtiyacı ortaya çıkmıştır. Zira Birlik üyesi ülkelerdeki veri korumaya ilişkin düzenlemeler arasındaki

¹²⁷ “History of data privacy” (2021), <https://www.accountablehq.com/post/history-of-data-privacy-laws>, E.T.: 30.01.2022.

¹²⁸ Gonzalez Gloria Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Springer, 2014, s. 55.

¹²⁹ Kanun ile ilgili ayrıntılı bilgi için bkz. LEE J. Riccardi, “The German Federal Data Protection Act of 1977: Protecting the Right to Privacy?”, *Boston College International and Comparative Law Review*, Cilt 6, Sayı 1, 1983, s. 243-271.

¹³⁰ Özkan, a.g.e, s. 42.

¹³¹ 95/46/EC sayılı *Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktif*’i 24 Ekim 1995 tarihinde yayınlanmış ve Avrupa Birliği Genel Veri Koruma Tüzüğüyle yürürlükten kaldırılana kadar AB’de veri korumasına ilişkin başlıca yasal düzenleme olmuştur. Bundan böyle “Direktif” olarak anılacaktır.

farklılıklar ile veri koruma düzeyleri arasındaki eşitsizlikler, ülkelerarası veri aktarımı konusunda sıkıntılar yaratmaktaydı. Birtakım ülkeler iç hukuklarındaki yasal düzenlemelerinde Direktif'teki temel düzeyi baz alırken, bazı ülkelerde ise çok daha yüksek veri koruma düzeyine ilişkin ulusal düzenlemeler yapılmaktaydı¹³². Kişisel veriler maddi değere sahip olduğundan hukuki düzenlemelerdeki ayrımlar ekonomik kayıplara neden olmaktaydı. Örneğin, GVKT'nin 2. paragrafında düzenlemenin amaçlarından biri olarak güçlü ekonomik birliğin oluşturulması gösterilmiştir. Ayrıca günümüzde çoğu insanın birden fazla sosyal medya hesabının olması ve bu hesapların kullanımının hızla artmasıyla kişisel verilerinin korunması için güncel bir düzenlemeyi gerekli kılmıştır¹³³. Yeni oluşturulan bu düzenlemenin herhangi bir üye devletin kişisel veri yasalarını benimsemeye, değiştirmeye çalışmayacağı, 24 Mayıs 2018'den itibaren bütün veri koruma hükümleri alanındaki uygulama eksikliği sona ereceği, AB için birleşik ve doğrudan uygulanabilir tek bir veri koruma yasası olacağı beklenmekteydi. Düzenlemenin diğer özelliği ise mevcut üye devletlerin hemen hemen tüm ulusal hükümlerinin yerini alması ve ulusal hukuka aktarılmadan işletmeler, bireyler, mahkemeler ve yetkililer tarafından uygulanacak olmasıydı¹³⁴.

Direktif'in yenilenmesi 2012 senesinden başlayarak AB'nin gündeminde olmuş ve bu alandaki çalışmaların sonunda ilk kez 2012 yılında Avrupa Birliği Komisyon'u Direktif'e değişiklikler yapılması ile ilgili bir öneri hazırlamıştır. Bu öneriyi Avrupa Komisyonu adından Komisyon'un o dönemki Başkan Yardımcısı Viviane Reding açıklamıştır¹³⁵. Reding açıklamasında 17 yıl önce Avrupalıların %1'inden daha azının interneti kullandığını ve bugün dünyanın her yerinde çok büyük miktarda kişisel veri aktarıldığını, ancak vatandaşların kendi kişisel verileri üzerinde her zaman tam kontrol sahibi hissetmediklerini belirtmiştir. Reding önerilerin çevrimiçi hizmetlere güven oluşturmaya yardımcı olacağını, veri

¹³² Küzeci, a.g.e, s. 193; Nilgün Başalp, "Avrupa Birliği Veri Koruması Genel Regülasyonu'nun Temel Yenilikleri", Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, Cilt 21, Sayı 1, 2015, s. 83.

¹³³ Başalp, 2015, a.g.m, s. 85.

¹³⁴ Albretch, J. (2015) "How the GDPR Will Change the World" European Data Protection Law Review, Cilt 2, Sayı 3, 2015, s. 287.

¹³⁵ European Commission (2012), "Viviane Reding Vice-President of the European Commission, EU Justice Commissioner The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age Innovation Conference Digital, Life, Design", https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_12_26, E.T.: 24.09.2022.

sahiplerini daha fazla kontrol sahibi yapacağını, ancak bunu işletmeler için kolay ve daha az maliyetle gerçekleştireceğini vurgulamıştır¹³⁶.

Nihayet çalışmaların sonucunda 27 Nisan 2016'da Avrupa Birliği GVKT kabul edilmiş, 4 Mayıs 2016 tarihinde Avrupa Birliği Resmi Gazetesi'nde yayımlanmıştır. Tüzük 173 paragraflık giriş bölümü ve 99 maddeden oluşmaktadır. Daha sonra uyum çalışmalarının tamamlanmasından dolayı iki yıllık bir geçiş süreci belirlenmiş ve 25 Mayıs 2018 tarihinde Tüzük yürürlüğe girmiştir.

Önceden Direktif hükümlerinin doğrudan uygulanma kabiliyeti olmadığından üye devletler ulusal mevzuatlarında gerekli düzenlemeler yapmakla yükümlüydüler¹³⁷. GVKT ise üye devletler için genel uygulama alanına sahip bir düzenlemedir. Bu nedenle Tüzük herhangi bir iç hukuka geçirme prosedürüne gerek duymaksızın Topluluk Resmi Gazetesi'nde yayımlandıktan sonra tüm AB üyesi ülkelerde doğrudan doğruya bağlayıcı metin halini almıştır¹³⁸.

Tüzüğün kişisel verilerin korunması alanında kapsamı ve uygulama alanı oldukça geniş tutulmuştur. Şöyle ki Tüzüğün 3. maddesi gereği Tüzük yalnızca Birlik sınırları içerisinde veri işleyenleri değil, Birlik sınırlarında bulunmasa bile sınırlarında ikamet eden, hizmet sunan kişilere ve onları gözlemleyen veri sorumlusu ya da veri işleyenlere uygulanmaktadır. Yani burada önemli olan kişinin kim olduğu ya da nereli olması değildir. Şirket merkezinin nerede olduğu değil¹³⁹, şirketin nerede faaliyet gösterdiği, verisi işlenen kişinin AB vatandaşı olması değil, AB sınırlarında mukim olması¹⁴⁰, Tüzüğün uygulanması için yeterlidir. Örneğin Türkiye'den AB'ye ihracat yapılması durumunda GVKT uygulanacaktır. Bu hüküm hem GVKT'nin global uygulanabilme imkanını, hem de uygulama alanının oldukça geniş olduğunu göstermektedir. AB içerisinde olmayan veri sorumlusu ya da veri işleyenlere Tüzüğün uygulanacağı diğer bir durum ise *“AB'deki ilgili kişilerin AB içindeki davranışlarının izlenmesi”* durumudur. Şöyle ki günümüzde veri işleyenler kişilerin

¹³⁶ European Commission (2012), Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses, https://ec.europa.eu/commission/presscorner/detail/en/IP_12_46, E.T.: 14.04.2022

¹³⁷ Direktif ile Tüzüğün farkları ile ilgili daha detaylı bilgi için bkz: European Union, “Types of legislation”, https://european-union.europa.eu/institutions-law-budget/law/types-legislation_en, E.T.: 03.09.2022, European Union, 2022, “Sources and Scope of European Union Law”, https://www.europarl.europa.eu/ftu/pdf/en/FTU_1.2.1.pdf, E.T.: 03.09.2022.

¹³⁸ Mehmet Nuri Tapan, “Avrupa Birliği (AB) Hukukunun Kaynakları ve Ulusal Hukuka Etkileri: Avrupa Adalet Divanı”, Türkiye Barolar Birliği Dergisi, Sayı 3, 1998, s. 993.

¹³⁹ Başalp, 2015, a.g.m, s. 83.

¹⁴⁰ Mesut Serdar Çekin, Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku, İstanbul, On İki Levha Yayıncılık, 2019, s. 5.

özellikle internet ortamındaki dolaşımını, davranışlarını, gezindiği internet sitelerini izlemekte ve bu davranışları analiz ederek kişiler hakkında bazı sonuçlar elde edilebilmektedir. Bu kapsamda kişilerin davranışlarının izlendiği her durumda GVKT uygulanacaktır¹⁴¹. Örneğin, internette yapılan aramaları izleyen Google'un, icloud, google drive gibi depolama hizmeti sunan bulut bilişim sistem sağlayıcılarının¹⁴² GVKT'nin uygulama alanına gireceğini belirtmek gerekmektedir¹⁴³.

1.2.2. Türk Hukuku

Türkiye Cumhuriyeti Anayasası'nda 2010 yılına kadar kişisel verilerin korunması ile ilgili bir hükme yer verilmemiştir. 2010 yılında Anayasa'nın "*kişinin hakları ve ödevleri*" bölümünde yer alan ve özel hayatın gizliliğini düzenleyen 20. maddesine 2010 tarihli 5982 sayılı kanun ile ek fıkra getirilmiştir. Bu fıkra kişisel verilere dair Anayasa'daki ilk düzenleme olmuştur. İlgili ek fıkra aşağıdaki şekildedir:

"Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir"¹⁴⁴.

Kişisel verilerin korunması hakkı yalnızca kişisel verinin korunması demek değildir¹⁴⁵. Bahsettiğimiz hak kişisel verilerinin işlenmesine karşı veri sahibinin korunmasını ifade etmektedir¹⁴⁶.

¹⁴¹ Çekin, a.g.e, s. 35.

¹⁴² Bulut hizmetleri ile ilgili daha detaylı bilgi için bkz: The Evolution Of Data Storage, <https://www.securedatarecovery.com/infographics/the-evolution-of-data-storage>, bulut bilişim sistemlerinde kaydedilen kişisel veriler ile ilgili bkz.: P. M. Schwartz, "Information Privacy in the Cloud", University of Pennsylvania Law Review, https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1024&context=penn_law_review, E.T.: 31.07.2022.

¹⁴³ Taştan, a.g.e, s. 16.

¹⁴⁴ Doğan Kılınç, "Anayasal Bir Hak Olarak Kişisel Verilerin Korunması", Ankara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, Cilt 61, Sayı 3, 2012, s. 1132.

¹⁴⁵ Özkan, a.g.e, s. 81.

¹⁴⁶ Şimşek, a.g.e, s. 4-5.

Kişisel veriler özel hayatın gizliliğiyle ilişkili olsa da, Anayasa’da “*kişisel verilerin korunması hakkı*” özel olarak ayrı bir maddede düzenlenmemiştir. Elbette münhasır bir hukuki dayanağın oluşması için konuya ilişkin bir hükmün bulunması daha anlamlı olurdu.

Kişisel verilerin korunması hakkı Anayasa ile düzenlense de bazı nedenler konuya ilişkin özel bir kanunu gerektiriyordu. Siyasal nedenler KVKK’yı gerekli kılan nedenlerden biriydi. Şöyle ki Türkiye’nin AB’ne üyelik görüşmelerinde Türkiye’deki kişisel verilerin korunması alanında mevzuat eksikliği ifade edilmişti¹⁴⁷. Ayrıca bahsedilen nedenlerden dolayı Türkiye’nin kolluk birimleri ile EUROPOL arasında bilgi aktarımı yapılamamaktaydı. Benzer sebeplerden dolayı EUROJUST ve yetkileri yargı makamları arasında da veri nakli hususunda problemler oluşmaktaydı¹⁴⁸.

Günümüzde şirketler maddi nedenlerle veri işletmekte ve bu verileri yurt içine ve dışına aktarmaktadırlar. Veri korumaya dair ekonomik ve ticari sebepler özel kanunu gerekli kılan nedenlerden bir diğeri. Veri korumaya dair özel bir kanunun olmaması yerel ve yabancı yatırımlara da engel olabilirdi¹⁴⁹.

Diğer bir gerekçe sağlık kuruluşlarında hastalara ilişkin çok sayıda verinin tutulması ve bu verilerin tutulmasına dair herhangi bir hukuki dayanağın bulunmaması, veri güvenliğine ilişkin tedbirlerin alınmaması ve yetkisiz kişilerce bu verilerin ifşa edilmesinin AIHM tarafından özel hayatın gizliliğine müdahale olarak nitelendirilmesi ve ihlal kararlarının verilmesiydi¹⁵⁰.

Bahsedilen gerekçeler ışığında Kişisel Verilerin Korunması Kanunu 24 Mart 2016 tarihinde TBMM tarafından kabul edilmiş ve 7 Nisan 2016 tarihinde Resmi Gazetede yayımlanmıştır¹⁵¹.

¹⁴⁷ Türkiye 2015 Yılı İlerleme Raporu, s. 4, Türkiye 2014 Yılı İlerleme Raporu, s. 6, Türkiye 2013 Yılı İlerleme Raporu, s. 6, https://www.ab.gov.tr/ilerleme-raporlari_46224.html, E.T.: 24.07.2022.

¹⁴⁸ Özkan, a.g.e, s. 82.

¹⁴⁹ Özkan, a.g.e, s. 83.

¹⁵⁰ Mustafa Baysal, Kişisel Verilerin Korunması Kanunu El Kitabı, 5. Baskı, Ankara, Seçkin Yayınları, 2022, s. 27.

¹⁵¹ 7 Nisan 2016 tarihli ve 29677 sayılı Resmi Gazete, <https://www.resmigazete.gov.tr/eskiler/2016/04/20160407-8.pdf>, E.T.: 15.04.2022.

İKİNCİ BÖLÜM

2. KİŞİSEL VERİLERİN KORUNMASI HUKUKUNDA TEMEL KAVRAMLAR, GENEL İLKELER VE VERİ SORUMLUSUNUN YÜKÜMLÜLÜKLERİ, İLGİLİ KİŞİNİN HAKLARI

2.1. TEMEL KAVRAMLAR

2.1.1. Veri Sahibi

Veri sahibi, GVKT’de ve KVKK’da kişisel verileri bakımından korunan kişiyi, hakkın süjesini ifade eder.

Verisi işlenen gerçek kişi KVKK kapsamında “*ilgili kişi*” olarak, GVKT’de ise “*verileri toplanan veya işlenen ve doğrudan veya dolaylı olarak tanımlanabilen gerçek kişi*” olarak tanımlanmıştır. Görüldüğü üzere veri sahibi kavramı KVKK’da olduğu gibi Tüzük ile de daraltılmış ve kişiler verilerin tanımında (4. madde) açıkça “*gerçek kişi*”lerin verilerinin korunduğu belirtilmiştir.

TMK uyarınca kişiliğin sağ ve tam doğum ile kazanılması, bazı durumlarda ilgili kişinin kim olduğuna ilişkin belirsizliklere sebep olabilir. Bu durum bazı soruları ortaya çıkarmaktadır. Örneğin, bebeğin doğumundan önce bebeğe ilişkin elde edilmiş tıbbi verileri veya, ultrason gibi yöntemlerle elde edilmiş görüntüleri de KVKK uyarınca kişisel veri kapsamında değerlendirilebilir mi? Söz konusu verilerin kişisel veri olarak kabul göreceği takdirde ilgili kişi tam ve sağ doğumdan sonra kişilik hakkını kazanan bebek mi olacaktır? Bununla ilgili henüz doğum gerçekleşmediğinden anne karnındaki ceninin yasal temsilcisi tarafından kişilik haklarının ve kişisel verilerinin korunmasına ilişkin yollara başvurma imkanı olmayacaktır. Etkili bir hukuki koruma sadece çocuğun doğumundan sonra mümkün olabilecektir¹⁵².

¹⁵² Kurt, a.g.m, s. 181-183.

Her ne kadar çocukların kişisel verilerinin korunmasına yönelik bir engel bulunmasa bile bahsi geçen durumda ilgili kişinin kim olacağına dair doktrinde fikir birliği sağlanılamamıştır¹⁵³.

GVKT ile KVKK'dan farklı olarak veri sahibinin çocuk olması durumunda işleme faaliyetleri ve buna yönelik verilecek rızanın niteliği konusunda bazı özel düzenlemeler getirilmiştir. GVKT'nin kabul gerekçesinin 38. maddesinde gösterildiği üzere çocuklar kişisel verilerinin işlenmesinin risklerini ve işleme faaliyetlerinin sonuçlarını kavrayamayabilirler. Bu nedenle çocukların kişisel verilerinin özel olarak korunması gerekmektedir. Bu hüküm gereği çevrimiçi pazarlama faaliyetleri, sosyal kişilik yaratma veya kullanıcı profili oluşturma ya da çocuklara doğrudan hizmet vermeyi amaçlayan uygulamaların kullanılması sırasında çocukların kişisel verilerinin toplanması gibi işlemler çocukların özellikle koruma altına alınması gereken durumlardır¹⁵⁴. GVKT'nin 8. maddesine göre işleme faaliyetlerinin hukuka uygunluğunun ve bu faaliyetin veri sahibinin rızasına dayalı olduğu durumlarda rızanın geçerli olabilmesi için çocuğun en az 16 yaşında olması gerekir. Çocuğun 16 yaşından küçük olması durumunda ise söz konusu işleme faaliyeti, yalnızca rızanın çocuk üzerinde velayet hakkı bulunan kişi tarafından verildiği veya onaylandığı durumda rızanın verildiği veya faaliyetin onaylandığı ölçüde hukuka uygun olacaktır. Aynı hükümle bu durum için GVKT'ye uygun ispat yükü veri sorumlusuna verilmiştir. Şöyle ki veri sorumlusu, rızanın çocuğun velisi tarafından verildiğini doğrulamak için *“mevcut teknolojiyi dikkate alarak”* *“makul çaba”* sarf etmelidir. Mevcut teknolojinin hangi unsurlarının nasıl etkili olacağı yada *“makul çabanın”* kapsamının ne olduğu konuları ise GVKT ile düzenlenmemiştir¹⁵⁵. Bununla birlikte çocukların rızasına geçerlilik tanınmasına ilişkin yaş sınırını belirleme yetkisi bir ölçüde üye devletlere bırakılmıştır. İlgili hüküm gereği üye devletler yaş sınırını 13 yaşına kadar indirebilirler¹⁵⁶. Nitekim Birleşik Krallık'ta bu sınırı 13 yaşına indirilmiştir¹⁵⁷.

Ayrıca GVKT'nin 75. resitalinde *“gerçek kişilerin hak ve özgürlüklerine yönelik yüksek risk oluşturmaları muhtemel kişisel verileri işleme faaliyetlerine”*

¹⁵³ Tolun, a.g.t, s. 22.

¹⁵⁴ GDPR, Recital 38, <https://www.privacy-regulation.eu/en/recital-38-GDPR.htm>, E.T.: 04.09.2022.

¹⁵⁵ Tolun, a.g.t, s. 58.

¹⁵⁶ GVKT, m. 8(1).

¹⁵⁷ Information Commissioner's Office, Children and GDPR, What are the rules about an ISS and consent? | ICO, E.T.: 04.09.2022.

toplumun daha savunmasız grubunu oluşturan çocuklara ilişkin verilerin işlenmesi örnek olarak gösterilmiştir¹⁵⁸. Aynı şekilde 58. resital’de şeffaflık ilkesi¹⁵⁹ gereği, işlemenin bir çocuğa yönelik olduğu durumlarda çocuğa yönelik her türlü bilgi ve iletişimin çocuğun kolayca anlayabileceği açık ve sade bir dilde olması gerektiği belirtilmiştir¹⁶⁰.

Yukarıda belirtildiği üzere çocukların kişisel verilerinin korunmasına ilişkin KVKK’da özel hükümler bulunmamaktadır. Bu kapsamda kişisel verilerin korunmasına ilişkin KVKK’da yer alan genel düzenlemelerden, TMK’da kişiliği koruyan madde 24-25 hükümleri ve çocuğun korunmasına ilişkin madde 346 hükmünden yararlanılabilir¹⁶¹.

2.1.2. Veri İşleme

KVKK madde 3(1)(e) ve GVKT madde 4(2) uyarınca veri işleme faaliyeti kişisel veri veya kişisel veri setleri üzerinde gerçekleştirilen toplama, kaydetme, düzenleme, yapılandırma, saklama, uyarılama veya değiştirme, elde etme, danışma, kullanma, iletim yoluyla açıklama, yayma veya kullanıma sunma, uyumlaştırma ya da birleştirme, kısıtlama, silme veya imha gibi herhangi bir işlem veya işlem dizisidir. Kısaca, kişisel veri üzerinde ve onunla ilgili gerçekleştirilen her türlü faaliyet veri işleme faaliyetidir. Her iki düzenleme uyarınca veri işleme faaliyeti otomatik veya otomatik olmayan yollarla gerçekleştirilebilir.

2.1.3. Veri Sorumlusu ve Veri İşleyen

Veri sorumlusu KVKK madde 3 uyarınca “*Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi*” olarak tanımlanmıştır. Kanunun ilgili hükmü uyarınca veri sorumlusu hem gerçek hem de tüzel kişi olabilir. GVKT’ye göre ise veri sorumlusu başka bir deyişle “*kontrolör*”, kişisel verilerin hangi amaç ve yöntemler ile işleneceklerini belirleme yetkisine sahip gerçek ya da

¹⁵⁸ GDPR, Recital 38.

¹⁵⁹ “*the principle of transparency*”

¹⁶⁰ GDPR, Recital 58, <https://www.privacy-regulation.eu/en/recital-58-GDPR.htm>, E.T.: 04.09.2022.

¹⁶¹ Murat Uçak, “Kişisel Verilerin Hukuka Uygun İşlenmesinde Çocuğun Rızası”, Kişisel Verilerin Koruma Dergisi, Cilt 3, Sayı 1, 2021, s. 47-48.

tüzel kişi, yahut kamu kuruluşları ya da herhangi diğer kurumdur¹⁶². KVKK’da olduğu gibi GVKT’ye göre de veri sorumlusu gerçek kişilere ilişkin verilerin toplanmasını ve işlenmesini gerçekleştirse de, veri sorumlusunun gerçek kişi olma zorunluluğu bulunmamaktadır. GVKT’nin 4. maddesi uyarınca veri sorumlusu, gerçek kişi olabileceği gibi tüzel kişi de olabilmektedir.

Yukarıda belirtildiği üzere veri sorumlusu hem gerçek hem de tüzel kişi, aynı şekilde kamu kuruluşu ya da başka bir organ olabilir. Bu durumda Madde 29 Çalışma Grubu’nun görüşüne göre, kamu kurumu ya da diğer bir organ olmasına bağımsız olarak veri sorumlusu bir tüzel kişi olduğu durumda, ilgili organın içerisindeki belirli bir kişi değil, organın kendisi veri sorumlusu sayılacaktır. Veri sorumlusunun gerçek kişi olması halinde ise kendisi veri işlemeden ve buna ilişkin tüm faaliyetlerden sorumlu olacaktır. Örneğin; popüler müzik dinleme uygulaması Spotify müşterilerinin dinleme geçmişlerini depolayıp daha sonra Google Cloud tarafından sağlanan bulut hizmetlerini kullanarak müşterilerinin müzik zevklerine uygun yeni şarkılar önermektedir. Bu durumda işleme faaliyetinin amacına ve yöntemine ilişkin kararları veren Spotify veri sorumlusu, işleme faaliyetini Spotify adına gerçekleştiren Google Cloud veri işleyendir¹⁶³. Diğer bir örnekte bir hastanenin web sitesindeki formu kişisel bilgileriniz ile doldurursanız, formu siteye web sitesini yapan kişi koysa da, veri sorumlusu hastane olacaktır¹⁶⁴.

Veri sorumlusu kanuni düzenlemelerde yer alan kişisel verilerin işlenmesine ilişkin bütün ilkelerin uygulayıcısı, kanunun gerektirdiği yükümlülüklerle sahip ve meydana gelen zararların sorumlusu olan kişidir¹⁶⁵. Başka bir deyişle kontrolör kavramının ilk ve en önemli rolü veri koruma kurallarına uyulmasından kimin sorumlu olacağını belirlemek, kısaca sorumluluk dağıtmaktır¹⁶⁶.

Veri sorumlusunun mutlaka veriyi doğrudan işleyen veya kişisel verileri elinde bulunduran kişi veya kuruluş olması gerekmez. Tanımda belirtildiği üzere *“kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin*

¹⁶² GVKT, m. 4.

¹⁶³ Supreeth Shastri, Wasserman Melissa, Chidambaram Vijay, “The seven sins of personal-data processing systems under GDPR”, <https://www.usenix.org/system/files/hotcloud19-paper-shastri.pdf>, E.T.: 16.04.2022

¹⁶⁴ Tolun, a.g.t, s. 33.

¹⁶⁵ Memiş Tekin, “Veri Sorumlusu ve Veri İşleyen Arasındaki İlişkiler ve Sorumluluk Düzeni”, Beykent Üniversitesi Hukuk Fakültesi Dergisi, Cilt 3, Sayı 6, 2017, s. 1

¹⁶⁶ Article 29 Working Party (2010), Opinion 1/2010 on the concepts of “controller” and “processor”, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf, E.T.: 16.04.2022

kurulması ve yönetilmesinden sorumlu olan kişi” verileri kendisi işlemese ve elinde bulundurmaya bile veri sorumlusu olarak değerlendirilecektir¹⁶⁷. Bu durumda veri sorumlularının sorumluluğu, veri işlenmesine ilişkin amaçlar ve yöntemleri belirleyerek bu konuda veri işleyenlere talimat vermek ve verilerin bu talimatlara uygun işlenip işlenmediğini denetlemek olacaktır¹⁶⁸. Veri sorumlusunun belirlenmesinde kullanılacak esas ölçüt, kişisel verilerin işleme amaçları ve yöntemleri üzerinde kimin kontrol sahibi olmasıdır¹⁶⁹.

GVKT uyarınca veri sorumlusunun adına veri işleme faaliyetini gerçekleştiren kişi veri işleyendir. Veri işleyen de veri sorumlusu gibi gerçek ya da tüzel kişi, yahut kamu kurumu ya da başka bir organ olabilir¹⁷⁰. Veri işleyen kavramı KVKK’da GVKT ile aynı yönde, “*Veri sorumlusu adına kişisel verileri işleyen bir gerçek ya da tüzel kişi, kamu kuruluşu, kurumu veya diğer herhangi bir organ*” şeklinde ifade edilmiştir. Bu tanımlara göre veri işleyen “*verilerin işleme amaçlarını ve veri işlemede kullanılacak araçları*” tek başına belirleyemeyen, “*veri kayıt sisteminin kurulmasında ve yönetilmesinde*” tek başına sorumluluğu olmayan, sadece olarak veri sorumlusu tarafından yetkilendirilerek, onun verdiği talimatlar doğrultusunda onun namı ve hesabı ile kişisel verileri işleyen gerçek veya tüzel kişi olarak ifade edilebilir¹⁷¹.

Veri sorumlusunun ve veri işleyenin kim olması sorumlulukların belirlenmesi bakımından oldukça önemlidir. Veri işleyen veri işleme faaliyetini veri sorumlusunun talimatlarına uygun olmayan biçimde gerçekleştirdiği takdirde, yaptığı uygunsuzluğun ölçüsünde sorumlu olacaktır¹⁷². Madde 29 Çalışma Grubu’nun görüşüne göre ise bu durumda ortak veri sorumluluğu mevcut olacaktır. Bununla birlikte, veri sorumlusu veri işleyene belirli bir derecede takdir yetkisi verebilir.

¹⁶⁷ Buse Doğan, Kişisel Verilerin İşlenme Şartları Bağlamında Açık Rıza, Yüksek Lisans Tezi, İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü, İstanbul, 2019, s. 40.

¹⁶⁸ Serdar Çelikel, Kişisel Verilerin Korunması Hukuku Kapsamında Veri Sorumlusu ve Veri Sorumlusunun Yükümlülükleri, 1. Baskı, Ankara, Seçkin Yayınları, 2021, s. 87.

¹⁶⁹ Canan İmançlı, Kişisel Sağlık Verilerinin Korunamamasından Doğan Özel Hukuk Sorumluluğu, Yüksek Lisans Tezi, İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü, İstanbul, 2019, s. 75.

¹⁷⁰ GVKT, m. 4(7), 4(8)

¹⁷¹ Turan Metin, Karşılaştırmalı Hukukta Kişisel Verilerin Korunması, 2. Baskı, Ankara Seçkin Yayınevi, 2019, s. 64.

¹⁷² Dülger, 2019 (a), a.g.m, s. 91.

Burada amaç veri sorumlusu işleyicinin en uygun olanı seçmesine izin vererek onun çıkarlarına hizmet etmesini talep etmektir¹⁷³.

Konuya ilişkin diğer bir mühim mesele, veri işleyenin eğer veri sorumlusunun önceden vermiş olduğu bir yazılı onayı yoksa, diğer bir veri işleyenle çalışamayacak olmasıdır¹⁷⁴.

GVKT kendi haleflerinin aksine hem veri sorumlusuna, hem de veri işleyene belirli ölçüde sorumluluk getirmiştir. Şöyle ki, veri sahipleri, GVKT'ın 79. ve 82. maddeleri gereği yalnızca veri sorumlusuna karşı değil, veri işleyene karşı da dava açabilirler. Ayrıca, GVKT madde 33/1-2 uyarınca, veri sorumlusu ve veri işleyen herhangi bir ihlal mevcut olduğu durumda bunu gecikmeden denetim otoritesine bildirmekle yükümlüdürler.

Tüzüğe göre “*ortak veri sorumluları*”nın tanımı yapılmıştır. İlgili madde uyarınca birden fazla veri sorumlusunun veri işlemeye dair ortak amaç ve yöntemleri belirledikleri durumlarda onlar ortak veri sorumluları sayılacaktırlar¹⁷⁵. KVKK uyarınca belirlenmiş veri sorumlusu kavramının GVKT'den esas farkı burada veri sorumlularına ilişkin “*ortak veri sorumluluğu*” kavramının tespit edilmemiş olmasıdır.

Diğer bir esas farklılık KVKK ile veri sorumlusunun tanımı yapılırken “*veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olma ölçütü*” arandığı halde, GVKT ile böyle bir ölçüte yer verilmemiştir.

Karşılaştırdığımız her iki düzenleme kapsamında yalnızca veri sorumluları değil veri işleyenler de hukuki sorumluluğa tabi tutulmuştur. Ancak GVKT ile veri sorumlularının ve veri işleyenlerin veri işleme faaliyetine ilişkin sorumluluklarının kapsamını genişletilmiştir¹⁷⁶. Her iki mevzuata göre veri işleyenler de veri güvenliğini sağlamaya yönelik olarak işletmelerinde teknik ve idari işleyişe ilişkin gereken tedbirleri gecikmeksizin almakla yükümlüdürler. Ancak GVKT ile ek olarak veri sorumlularına gerekli olan hallerde veri işleme faaliyetini gözlemlemek, tavsiyelerde bulunacak veri koruma görevlisi belirlemek ve veriler kendi elindeyken

¹⁷³ Article 29 Working Party (2010), Opinion 1/2010 on the concepts of “controller” and “processor”, s. 25

¹⁷⁴ GVKT, m. 28(2)

¹⁷⁵ GVKT, m. 26(1)

¹⁷⁶ SSRN Electronic Journal, “GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy?”, 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3212210, E.T.: 18.04.2022

ihlale uğramışsa gecikmeye neden olmadan ve en geç 72 saatlik bir süre içinde durumu veri sorumlusuna bildirmek yükümlülükleri düzenlenmiştir¹⁷⁷.

KVKK'dan farklı olarak GVKT ile tespit edilmiş veri sorumlusu ve işleyen arasındaki sözleşme (veya diğer hukuki tasarruf) yasal bir zorumluluk olup, veri işleyenin ilgili veri sorumlusu tarafından ona verilmiş talimatların dışında hareket etmesini engellemek içindir¹⁷⁸. Bu sözleşme, veri sorumlusu ile ilgili veri işleyen açısından bağlayıcıdır. İşleme faaliyetinin konusu, süresini, mahiyetini, amacını, kişisel verilerin türlerini, veri sahiplerinin kategorilerini, veri sorumlusunun yükümlülüklerini ve haklarını kapsar¹⁷⁹.

2.2. KİŞİSEL VERİLERİN İŞLENMESİNE İLİŞKİN İLKELER

2.2.1. Genel İlkeler

Kişisel verilerin işlenmesine ilişkin ilkeler KVKK'nın uygulaması esnasında bakılacak temel kurallardır. Kurul'un bazı kararlarında da KVKK 4. madde ile belirlenmiş genel ilkelerin önemi vurgulanmıştır. Örneğin, Kurul'un 25 mart 2019 tarihli kararında “*Kişisel verilerin işlenmesinde genel ilkelere uygunluğun sağlanmasının önemi*” vurgulanmıştır¹⁸⁰. Daha sonra yine 26 Aralık 2019 tarihli kararında Kurul “*değerlendirme puanlarının Kişisel verilerin Korunması Kanunun 4. maddesinde yer alan genel ilkelere uyumlu şekilde ilan edilmesi gerektiğine*” karar vermiştir¹⁸¹.

KVKK madde 4/1. madde uyarınca, “*Kişisel veriler, yalnızca Kişisel Verileri Koruma Kanunu'nda ve diğer kanunlarda öngörülen yöntemlere ve esaslara uygun bir şekilde işlenebilir.*” Kanunun maddesinden de görüldüğü üzere kişisel veri işleme faaliyetinde yalnızca KVKK değil, tüm hukuki düzenlemeler ve hukukun genel ilkeleri esas alınmalıdır.

Kişisel verilerin işlenmesinde uyulması gereken ilkeler KVKK madde 4/2 ile tespit edilmiştir. Söz konusu ilişkin temel ilkelere GVKT 5. madde ile yer verilmiştir. Bu ilkeler GVKT'nin devamında belirlenmiş kurallar için de başlangıç noktası

¹⁷⁷ Handbook on European Data Protection, 2018, s. 102, https://www.echr.coe.int/documents/handbook_data_protection_eng.pdf, E.T.: 16.04.2022.

¹⁷⁸ GVKT, m. 28(3).

¹⁷⁹ GVKT, m. 28(3).

¹⁸⁰ Kurul Kararı, 25.03.2019, <https://www.kvkk.gov.tr/Icerik/5434/2019-78>, E.T.: 21.04.2022.

¹⁸¹ Kurul Kararı, 26.12.2019, <https://www.kvkk.gov.tr/Icerik/6668/2019-389>, E.T.: 21.04.2022.

oluşturmaktadır. Bu prensiplere ilişkin istisnalar ancak AB seviyesinde veya ulusal düzeyde çıkarılacak kanunlar ile, temel haklar ve özgürlüklere saygı göstererek, demokratik bir toplumda meşru menfaatlerin güvence altına alınması için gerekli ve orantılı olmak kaydıyla mümkündür¹⁸².

İlkeleri tek tek irdelemeden önce veri işleme faaliyetleri esnasında hem kendisinin hem de anlaştığı tüm veri işleyicilerinin söz konusu ilkeleri gözetmesinden sorumlu olan esas tarafın veri sorumlusu olduğunu belirtmek gerekir¹⁸³.

2.2.1.1. Hukuka ve Dürüstlük Kurallarına Uygun Olma İlkesi

KVKK'ya göre kişisel veriler ilk olarak hukuka ve dürüstlük kurallarına uygun olarak işlenmelidir¹⁸⁴. Hukuka ve dürüstlük kurallarına uygunluk, sadece verilerin korunmasının değil, aynı zamanda hukukun genel ilkelerindendir. Türk Medeni Kanunu'nun 2. maddesine göre hukuk, hakkın kötüye kullanılmasını korumaz.

Dürüstlük kuralının ve hukuka uygunluğun gereği olarak, veri işleyen, kişisel verileri neden topladığını, ne şekilde topladığını, hangi amaçlarla ve hangi biçimde kullanacağını kişisel verilere ilişkin her hangi davranışta bulunmadan önce veri sahibine açıklamalıdır. Bilgilendirmenin yapılmaması durumunda ise veri işlemenin dürüstlük kuralına uygun olmasından bahsetmek de mümkün olmayacaktır¹⁸⁵.

Bazı durumlarda işleme faaliyeti hukuka uygun olarak görünse bile dürüstlük kuralına uygunluk ilkesine aykırı olabilir. Örneğin, veri işlemenin hukuka uygunluk sebebi rıza olarak görünse de aslında veri işleme, kanunla belirlenmiş başka bir hukuka uygunluk sebeplerinden birine dayanarak yapılıyorsa, ilgili kişinin rızasını geri çektiğinde işlemenin duracağını sanması dürüstlük kuralına uygunluk ilkesini ihlali sayılacaktır¹⁸⁶. Aynı şekilde kişinin rıza gösterdiği veri işleme amacı sonradan

¹⁸² Handbook, 2018, s. 116.

¹⁸³ Tolun, a.g.t, 40.

¹⁸⁴ KVKK, m. 4(2)(a).

¹⁸⁵ Oğuz Habip, "Elektronik Ortamda Kişisel verilerin Korunması, Bazı Ülke Uygulamaları ve Ülkemizdeki Durum", Uyuşmazlık Mahkemesi Dergisi, Cilt 0, Sayı 3, 2014, s. 23.

¹⁸⁶ Yücedağ, a.g.m, s. 84.s

değiştii taktirde yeni durum makul beklenenin dışında kalacağından veri sahibinin yeniden rızası alınması gerekecektir¹⁸⁷.

Bu ilke kapsamında veri işleme faaliyetinin veri sahibi açısından “şeffaf” olması gerekmektedir. Örneğin, Kurul’un 01 Ekim 2019 tarihli kararında elinde kişisel veriler bulunmadığı halde aksini söyleyen veri sorumlusunun dürüstlük kuralını ihlal ettiği yönde karar vermiştir¹⁸⁸.

Dürüstlük kuralına uygunluğun beraberinde kişisel verilerin işlenmesinde hukuka uygunluk şartının da sağlanmış olması gereklidir. Bundan dolayı, kişisel verilerin işlenmesi ancak KVKK 5. madde gösterilmiş hukuka uygunluk sebeplerinin varlığı halinde mümkündür.

GVKT uyarınca da “*Kişisel veriler hukuka uygun, adil ve şeffaf bir biçimde işlenmelidir*¹⁸⁹.” Dolayısıyla veri işlemeye dair ilk kural kişisel veriler işlenirken hukuka uygun hareket edilmeli, adil ve şeffaf davranılmalıdır. Hukuka uygunluk, adalet ve şeffaflık farklı ilkeler gibi ifade edilmiş olsa bile aslında birbirleriyle ilişkilidirler¹⁹⁰.

GVKT’nin 6. maddesi uyarınca veri işleme faaliyetinin hukuka uygun olabilmesi için bu işleme veri sahibinin rızası altında veya veri sahibinin taraf olduğu bir sözleşmenin, veri sorumlusunun uyması gereken bir yasal yükümlülüğün, ilgili kişinin yahut diğer bir gerçek kişinin hayati menfaatlerinin, kamu yararına gerçekleştirilen bir görev, ya da (veri sahibinin başka hakları ağır basmadığı takdirde) kontrolün veya üçüncü kişinin meşru menfaatlerinin doğrultusunda gerçekleştirilmelidir¹⁹¹. Veri işlemenin hukuka uygun olması için bu işlemenin kişisel verilerin korunmasının temel ilkelerine uygun olması gerekmektedir¹⁹². Veri işleme temel ilkelere uygun şekilde yapıldığında hukuka da uygun olacaktır.

Bu ilkeye göre kişisel veri işleme faaliyetlerinin sahip olması gereken “*adil olma*” özelliğine ilişkin doktrinde her ne kadar tanımı GVKT içerisinde doğrudan yapılmasa da “*adillik*” ve “*farkındalık*”a atıf yaptığı düşünülmektedir¹⁹³. Başka bir

¹⁸⁷ Murat Altındere, *Kişisel Verilerin Korunması Hukuku ve Uygulaması*, 1. Basım, Adalet Yayınevi, İstanbul, 2020, s. 38.

¹⁸⁸ Kurul Kararı, 01.10.2019, <https://www.kvkk.gov.tr/Icerik/6556/2019-294>, E.T.: 22.04.2022.

¹⁸⁹ GVKT, m. 5/1-a.

¹⁹⁰ Senem Ovalıoğlu, *Avrupa Birliği hukukunda Kişisel Verilerin Korunması*, Yüksek Lisans Tezi, Dokuz Eylül Üniversitesi, Sosyal Bilimler Enstitüsü, İzmir, 2021, s. 25.

¹⁹¹ Tolun, a.g.t, s. 52.

¹⁹² Ovalıoğlu, a.g.t, s. 26.

¹⁹³ Tolun, a.g.t, s. 52.

deyişle veri sahibi kişisel verileri üzerinde yürütülen işleme faaliyetlerine dair farkındalığa sahip olmalıdır. Veri sorumlusu ise işleme faaliyetlerini gizli olarak gerçekleştirmemeli ve veri sahiplerini olası risklere karşı bilgilendirmelidir¹⁹⁴.

GVKT ile açıkça düzenlenmiş şeffaflık unsuru ise işleme faaliyetleri öncesinde veri sahibine bilgi vermeyi içermesinin yanı sıra, süreç boyunca da veri sahibinin talebi üzerine kendisini bilgilendirmeyi ve gerektiğinde veri sahibinin kendi verilerine erişimini mümkün kılmayı da içermektedir¹⁹⁵.

2.2.1.2. Doğru ve Gerektiğinde Güncel Olma İlkesi

Kişisel verilerin işlenmesine ilişkin ilkelerden bir diğeri “*doğru ve gerektiğinde güncel olma*” ilkesidir. KVKK’ya göre veri sahibi kendisine ait verilerin eksik ya da yanlış işlenmesi durumunda bunların düzeltilmesini talep edebilir¹⁹⁶. Eğer veriler doğru ve güncel tutulmazsa, veri sahibi kanunun ona tanıdığı hakkını kullanabilecektir.

İşlenen verilerin doğru olması şartı yalnızca, verileri ilk kez işlendiği zaman için değil, tüm süreç boyunca geçerlidir ve bu süre boyunca veri sorumluları tarafından verilerin gerçekliği kontrol edilmelidir. Gerçekle uzlaşmayan, yalan ya da güncel olmayan kişisel veriler düzeltilmeli ya da ortadan kaldırılmalıdır¹⁹⁷.

Kişisel verilerin yanlış olduğunda ya da güncel olmadığında veri sahipleri maddi ve manevi zarara maruz kalabilir. Örneğin, veri sorumlusu hastahane tarafından hastaya dair bilgilerin güncel tutulmaması ya da yanlış işlenmesi sonucunda hasta manevi zarara uğrayabilir. Diğer bir örnekte mağaza görevlisinin mal satışından prim eldeceği bir mağazada görevlinin numarasının yanlış işlenmesi ya alıcılara yanlış numaranın paylaşılması sonucunda görevli alamayacağı para için maddi zarara uğrayacaktır. Bu durumda veri sorumlusu mağaza sahibi de satış yapılmadığından maddi zarara uğrayacaktır. Böylelikle söz konusu ilkenin veri sahibini koruduğu kadar veri sorumlusunun çıkarlarını da koruduğu gözükmetedir¹⁹⁸.

¹⁹⁴ Handbook, 2018, s. 118.

¹⁹⁵ Handbook, 2018, s. 120.

¹⁹⁶ KVKK, m. 11/1/d.

¹⁹⁷ Özkan, a.g.e, s. 107.

¹⁹⁸ Özkan, a.g.e, s. 108.

Doğruluk ve güncellik ilkesi uyarınca doğru ve güncel olmayan kişisel verilerin gecikmezsizin silinmesi veya düzeltilmesi için gerekli adımlar atılmalıdır. Ancak burada verilerin işlenme amaçları da göz önünde bulundurulmalıdır¹⁹⁹.

Söz konusu ilkeye göre kişisel verileri elinde bulunduran veri sorumlusu ilgili verinin gerçek ve güncel olmasını doğrulamak için çaba göstermediği takdirde bu bilgiyi kullanmamalıdır²⁰⁰. Bunun yanı sıra, veriler ilk defa elde edildiği anda veriyi doğrudan ve bilgisi dahilinde veren ilgili kişiden alınıyorsa, bahsi geçen kişi de bu veriyi doğru bir şekilde verilmelidir²⁰¹.

Bazı kişisel verilerin her zaman için mutlak bir şekilde kontrol edilerek güncellenmesi gereklidir. Bazı veriler ise yalnızca gerekli olduğunda güncellenmelidir. Hatta önceden kaydedilmiş bazı kişisel verilerin güncellenmesi hukuken yasaklanmıştır. Örneğin, bir hastaya ait medikal kayıtlardaki bilgiler daha sonra doğru olmadıkları anlaşılrsa dahi güncellenmemelidir. Böyle bir durumda yeni bilgiler yalnızca bu işlem açıkça yapıldığı takdirde eklenebilir. Diğer bir örnekte ise, bir kişi kredi çekmek için bankaya başvurduğunda, banka tarafından bu kişi hakkında oluşturulan veri tabanlarından kişinin kredi verilebilir durumda olmasını incelediği zaman veri tabanı güncel olmayan veriler içerirse bu kişi için olumsuz sonuçlara yol açabilir²⁰². Böyle gibi durumların yaşanmaması için bu tarz veri tabanlarını kontrol edenler kişiler verileri güncel tutmakla yükümlüdürler²⁰³.

2.2.1.3. Belirli, Açık ve Meşru Amaçlar İçin Kullanma İlkesi

Bu ilke gereği kişisel verilerin işleme amacı açık, anlaşılır ve meşru olmalıdır. Veriler hukuki amaçlar için toplansa dahi, toplanma amaçlarına aykırı şekilde kullanılamazlar. Kişisel verilerin işlenmesinde veri sorumlusu veri sahibine işleme faaliyetinin hangi veri işleme şartına dayandığı belirtilmelidir. Aksi halde ilkeye aykırılıktan dolayı veri işleme faaliyeti hukuka aykırı olacaktır²⁰⁴.

Veri sorumlusunun amacının belirli ve açık olması için kanun koyucu tarafından konuya ilişkin düzenlemeler yapılmalıdır. Veri sorumlusunun belirlediği

¹⁹⁹ GVKT, m 5(1)(d).

²⁰⁰ Dülger, 2019 (a), s. 104.

²⁰¹ Dülger, 2019 (b), s. 133.

²⁰² A Guide for Policy Engagement on Data Protection, Part 3 – “Data Protection Principles”, Data Protection Principles, E.T.: 04.09.2022.

²⁰³ Dülger, 2019 (a), s. 104.

²⁰⁴ Kurul Kararı, 01.10.2019, <https://www.kvkk.gov.tr/Icerik/6556/2019-294>, E.T.: 22.04.2022.

amaçla verilerin işleme amacı farklı olursa ilkeye aykırılık söz konusu olacaktır. Böyle bir durumda meydana gelen ihlalden dolayı veri sorumlusu sorumlu olacaktır²⁰⁵.

KVKK 4. madde gerekçesi uyarınca, veri sorumlusunun işlediği veriler onun yaptığı iş ya da sunduğu hizmetle ilgili ve bunlar için zaruri olduğu takdirde amaç meşru sayılabilir. Aynı şekilde GVKT'nin 5/1-b maddesi gereği; *“Kişisel veriler belirtilen, açık ve meşru amaçlara yönelik olarak toplanmalıdır ve bu amaçlara zıt olarak işlenmemelidir. İlgili maddeye göre yalnızca kamu yararına arşivlemek ya da, bilimsel veya tarihi araştırmalar için, ayrıca istatistiki amaçlarla gerçekleştirilen veri işleme faaliyeti de 89(1) maddesi uyarınca, başta belirtilen amaçlara uygun olmalıdır”*.

Örneğin, veri sorumlusunun düzenlediği bir sempozyumun katılımcılarının iletişim bilgilerinin işlenmesi meşru amaç sayılacaktır. Fakat toplanması ve işlenmesi için aynı katılımcılara annelerinin kızlık soyadı sorulduğu takdirde bu amaç meşru olmayacaktır²⁰⁶. Başka bir örnekte bir banka ticaret amaçlı hizmetlerini göstermesi sırasında güvenlik amacıyla müşterilerinin parmak izlerini alabilir. Bu veri kişinin rızasına bağlı olarak işlenir ve gerekli olan durumlarda kullanılır. Aksi durumda, eğer banka bu verileri ihtiyaç duyulmaksızın kullanırsa ya da gelecekte ihtiyaç duyacağı ihtimaliyle saklıyorsa bu faaliyet hukuka aykırı sayılacaktır²⁰⁷.

Konuya ilişkin olarak Kurul'un 18 Eylül 2019 tarihli kararında *“bankanın işlemlerde kendisine ulaşılması için verdiği bilgileri müşterinin eşine ulaşılması için işleme faaliyetinin KVKK madde 4/2/c-ç’de yer alan kişisel verilerin işlenmesinde belirli, açık ve meşru amaçlar için işleme ve işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ilkelerine aykırı olduğuna karar verilmiştir”*²⁰⁸.

Bunun için ilk olarak veri işleme faaliyetinin amacı belirlenmeli ve bu amacın gerçekleştirilmesine yetecek kadar veri işlenmelidir. Daha sonra ise belirli olan amaca karşı gerçekleştirilen veri işleme faaliyetinin gerekliliği belirlenmelidir. Bu

²⁰⁵ Kişisel Verileri Koruma Kurumu, “Madde ve Gerekçesi ile KVKK ve Kişisel Verilerin Korunmasına İlişkin Terimler Sözlüğü”, Ankara, 2019, Madde ve Gerekçesi ile Kişisel Verilerin Korunması Kanunu (Bilgi Notu) ve Kişisel Verilerin Korunmasına İlişkin Terimler Sözlüğü, E.T.: 31.08.2022

²⁰⁶ Özkan, a.g.e, s. 109.

²⁰⁷ Göknül Özcan, Bankacılık İş ve İşlemlerinde Kişisel Verilerin Korunması, , İstanbul On İki Levha Yayınları, 2020, s.90.

²⁰⁸ Kurul Kararı, 18.09.2019, <https://www.kvkk.gov.tr/Icerik/5545/2019-277>, E.T.: 22.04.2022.

tespitlerin neticesinde veri sorumlusu yalnız kendi amacı için gerekli olacak kadar veriyi işlemeli, bu amacı aşan verilere dokunmamalıdır²⁰⁹.

2.2.1.4. Amaçla Bağlantılı, Sınırlı ve Ölçülü Olma İlkesi

GVKT’de düzenlenen “*veri minimizasyonu*” (*data minimisation*) ilkesinin KVKK’daki karşılığı olan bu ilke 4. maddenin gerekçesinde “*Kişisel verilerin, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması ilkesi, işlenen verilerin, belirlenen 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.*” şeklinde belirtilmiştir.

Bu ilke gereği veri sorumlusu işleme faaliyetinin gerekliliğini belirlemeli, eğer işleme faaliyetinin sonucunda amaca ulaşması mümkünse verileri işlemelidir. Eğer amaca ulaşılması için söz konusu verinin işlenmesi mutlaka gerekliyse, veri sorumlusu mümkün en az miktarda veriyi işlemelidir. Örnek olarak, Kurul’un 04 Kasım 2021 tarihli kararında veri sorumlusu üniversitenin yüksek lisans ve doktora öğrencilerine ait kişisel verilerin tamamının bilgilendirme amacını aşacak nitelikte üniversiteye ait internet sitesinde paylaşmasının amaçla bağlantılı, sınırlı ve ölçülü olma ilkesine aykırı olduğuna, dolayısıyla veri minimizasyonu ilkesine aykırılıktan dolayı ihlalin mevcut olduğuna karar verilmiştir²¹⁰.

İşlenen verilerin yeterli miktarla sınırlaması anlamına gelen veri minimizasyonu “*veri ekonomisi*” olarak da adlandırılmaktadır²¹¹. Veri ekonomisi kavramınca veri sorumluları kişisel veri işlenmesi sırasında tabiri caizse, tutumlu olmalı, aşırı veri kullanımından kaçınmalıdır. Konuyla ilgili diğer bir Kurul kararında “*Veri sorumlusu olan bir havayolu taşımacılık şirketinin sunduğu sadakat programının kullanımı sırasında kullanıcı adı ve parola bilgilerini değiştirmeye çalışan kişiden kimliğinin önlü arkalı görüntüsünü talep eden veri sorumlusu*”nun bahsettiğimiz ilkeye aykırı işlem yaptığı belirtilmiştir²¹².

²⁰⁹ Habip Bozkurt, Kişisel Verilerin İşlenmesinin Hukuki Boyutu, Yayınlanmamış Yüksek Lisans Tezi, Kadir Has Üniversitesi, Lisansüstü Eğitim Enstitüsü, İstanbul, 2019, s.93.

²¹⁰ Kurul Kararı, 04.11.2021, <https://www.kvkk.gov.tr/Icerik/7267/2021-1127>, E.T.: 06.08.2022.

²¹¹ Küzeci, a.g.e , s. 208.

²¹² Kurul Kararı, 01.10.2019, <https://www.kvkk.gov.tr/Icerik/6556/2019-294>, E.T.: 23.04.2022.

“Ölçülülük ilkesi” veri işleme faaliyeti ile gerçekleştirilmesi gereken amaç arasında makul bir dengenin kurulmasını hedeflemektedir²¹³. Eğer veri işleme faaliyetinin amacına bu faaliyeti gerçekleştirmeden ulaşmak mümkünse ölçülülük ilkesine aykırılık mevcut olacaktır. Diğer bir ifadeyle söz konusu amaca ulaşmak için tek yolun kişisel verilerin işlenmesi olduğu durumda işleme yapılmalıdır²¹⁴. Örnek olarak, dans kursuna gitmek isteyen kişiden üyelik başvurusu sırasında iş hayatına ilişkin verilerinin de istenilmesi durumunda bu durum ölçülülük ilkesiyle bağdaşmayacaktır²¹⁵.

Bu ilkeye göre veri sorumlusu tarafından toplanılan veriler yalnızca işleme faaliyetinin amaçları ile ilgili olarak yeterli, yerinde ve gerekli olacak miktar ile sınırlandırılmalıdır. İşleme faaliyetlerinin önceden belirlenmiş amaçları ile bağdaşmayan yahut bu amacın yerine getirilmesi için zorunlu olmayan kişisel verilerin toplanması durumunda veri işleme faaliyeti GVKT’ye ve KVKK’ya uygun olmayacaktır²¹⁶. Örneğin, özellikle büyük şehirlerde sıklıkla kullanılan toplu ulaşım kartlarının üzerinde ve içerisindeki çipte kartın sahibine ilişkin isim, soyisim, TC kimlik numarası gibi bilgilerin yer alması, toplu taşımayı kullanan kişinin kimliğinin ulaşım ücretinin ödenmesi işlemi için gerekli olmadığından sözkonusu bilgilerin işlenmesi söz konusu ilkeye aykırılık teşkil edecektir²¹⁷.

2.2.1.5. Belirli ve Sınırlı Süre Muhafaza Edilmesi İlkesi

Kişisel verilerin işlenmesine ilişkin diğer temel ilke “İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkesi”dir. Bu ilkenin temel maksadı veri sorumluları tarafından kişisel verilerin belli olmayan bir süreç içinde saklanmasıyla engellenmesidir. Bu ilkenin gereğince veriler gelecek bir zamanda gerekli olabilme ihtimali ile stoklanmamalı, ihtiyaç olmadıkça veya fazla miktarda veri saklanmamalıdır. Bu ilke “veri minimizasyonu ilkesi” ile de bağlantılıdır²¹⁸. Şöyle ki verilerin saklanması için gereken süre sona

²¹³ Tülay Selin Gener, Kişisel Verilerin İşlenmesine yönelik olarak Açık Rza Verilmesi ve Açık Rza Beyanında bulunma ehliyeti, Yüksek Lisans Tezi, Eskişehir Üniversitesi, Sosyal Bilimler Enstitüsü, Eskişehir, 2021, s. 64

²¹⁴ Çekin, a.g.e, s. 72.

²¹⁵ Özkan, a.g.e, s. 112.

²¹⁶ Tolun, a.g.t, s. 52.

²¹⁷ Handbook, 2018, s. 126.

²¹⁸ Küzeci, a.g.e, s. 337.

erdiğinde verilerin saklanmaması stoklanan veri sayısını da azaltacaktır. Bu durumda sonuç olarak “*veri minimizasyonu*” ilkesine de riayet edilecektir²¹⁹.

KVKK’da düzenlenmiş kişisel verilerin saklanması için “*gerekli olan süre*”nin taraflarca tespit edilmediği durumlarda bir verinin “*gerekli olan süre zarfında*” saklanıp saklanmayacağını belirlemek için KVKK ile ikili bir ayırım yapılmıştır. Bunlardan biri “*mevzuatta öngörülen süre*”, böyle bir sürenin belirlenmediği durumlarda ise “*işlendikleri amaç için gerekli olan süre*”dir.

Öncelikle mevzuatta veri saklama ile ilgili gereken süre açıkça düzenlendiği takdirde veri sorumlusu ilgili süreyi aşamamalıdır. Örnek olarak, bu konuyla ilgili bir Kurul kararında veri sahibi veri sorumlusu olan bankaya kendi verilerinin silinmesi için başvuru yaptığını belirtmiştir. Ancak *5411 sayılı Bankacılık Kanunu*” madde 42 uyarınca “*Alınan yazılar ve faaliyetler ile ilgili belgelerin asılları ... ilgili banka nezdinde on yıl süreyle saklanır.*” hükmü ile, aynı şekilde, “*Bankaların Muhasebe Uygulamalarına ve Belgelerin Saklanması İlişkin Usul ve Esaslar Hakkında Yönetmelik*” madde 17/1 uyarınca “*Bankaların, müşterilerinden ... aldıkları mektup, telgraf, elektronik posta mesajı, ilam ve tebligatları ... istenildiğinde ibraz edilebilecek şekilde..nezdlerinde on yıl süreyle saklamaları zorunludur.*” hükümleri ile veri saklama süresi kanunla açıkça belirlenmiş olduğundan Kurul tarafından ihlal tespit edilmemiştir²²⁰.

Verilerin saklanma süresine ilişkin “*gerekli olan süre*” kavramından anlaşılması gereken veri işlemenin amacının gerçekleştirilmesi için gereken süredir. Veri sorumluları tarafından kanunun bu maddesinin keyfi olarak yorumlanmaması ve uygulamada haksız ya da hukuka aykırı veri stoklanmasına neden olmaması için kanun koyucu KVKK madde 16/3/f. ile veri sorumlularına VERBİS’e kaydolurken veri işlemenin amaçları için gereken azami sürenin bildirilmesi yükümlülüğü getirilmiştir. Bildirilecek ilgili süre “*makul bir süre*” olmalıdır.

KVKK 4. madde gerekçesine göre “*Mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre*” bittiğinde veri sorumluları söz konusu veriyi kendilerinin ve ya başka kişilerin ulaşamayacakları hale getirmelidirler. Yine bu gerekçeye göre bu işlem silme ya da anonim hale getirme yolu ile yapılabilir.

²¹⁹ Özkan, a.g.e, s. 114.

²²⁰ Kurul Kararı, 05.12.2018, <https://www.kvkk.gov.tr/Icerik/5424/2018-142>, E.T.:23.04.2022.

KVKK'da olduğu gibi GVKT'de da sınırlı süre saklama ilkesi kişisel verilerin yalnızca işleme amaçlarının gerektirdiği süre içerisinde saklanabileceğini ifade etmektedir²²¹. Daha basit anlamıyla veriler amaç için gerekli olan kadar süre boyunca işlenmeli, bu süre sona erdiğinde veri işleme faaliyeti de son bulmalıdır.

Belirtmek gereklidir ki bu ilkeye aykırılık veriler veri sahiplerinin kimliklerini açığa çıkaracak şekilde saklandığı durumlarda uygulama alanı bulacaktır²²². Veri sorumluları verilerin işleme amaçları için gerekli olan süre bittikten sonra ilgili verileri veri sahibinin kimliğini açık edecek ek bilgiler kullanmamak kaydı ile anonimleştirerek saklamaya devam edebilirler²²³. Ancak Tüzüğün 89. maddesi uyarınca yalnızca kamu yararına arşivleme, bilimsel veya tarihi araştırma, ya da istatistiki amaçlarla işlendikleri sürece ve veri sahibinin hakları ve özgürlüklerinin güvence altına alınması için GVKT'y uygun teknik ve düzenlemeye ilişkin tedbirlerin alınması koşuluyla kişisel veriler daha uzun süreler boyunca saklanabilir²²⁴. Konuyla ilgili AİHM "*Peruzzo and Martens v. Germany*" davasında hücrel materyalin DNA profilinin kurulması amacı gerçekleştirildikten sonra artık ihtiyaç duyulmadığında verilerin derhal imha edilmesi gerektiğini ve elde edilen DNA profillerinin yalnızca cezai amaçlarla ilgili makamlara açıklanabileceği kanaatine gelmiştir²²⁵. Bununla birlikte "*P.N. v. Germany*" davasında mahkemece bir suçludan alınan verilerin polis tarafından en fazla beş yıl süreyle saklanabileceği belirtilmiştir²²⁶.

2.2.1.6. Bütünlük ve Gizlilik İlkesi

KVKK ile düzenlenmeyen ancak GVKT'de yer alan ilkelerden veri sorumlusunu finansal olarak en çok etkileyebilecek bütünlük ve gizlilik ilkesidir²²⁷. Bu ilkeye göre veri sorumlusu kişisel verilerin yetkisiz veya yasa dışı işlenmesine,

²²¹ GVKT, m. 5(1)(e).

²²² Dülger, 2019 (a), s. 105.

²²³ Data Protection Commission (2019), "Quick Guide to the Principles of Data Protection", Quick Guide to the Principles of Data Protection, E.T.: 04.09.2022.

²²⁴ GVKT, m. 5(1)(e).

²²⁵ EctHR, "*Peruzzo and Martens v. Germany*" No. 7841/08 and 57900/12, 04.06.2013, [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-121998%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-121998%22]}), E.T. 04.09.2022

²²⁶ EctHR, "*P.N. v. Germany*", No. 74440/17, 16.11.2020, [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-202758%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-202758%22]}), E.T.: 04.09.2022.

²²⁷ Handbook, 2018, s. 128.

kaybolmasına veya imha edilmesine veya tahribine karşı korunmasına ilişkin teknik veya yönetsel tüm tedbirleri almakla yükümlüdür.

Burada dikkat edilmesi gereken iki husus vardır. Birincisi, veri ihlalinin yaşanması ve bunun tek başına bu ilkenin ihlaline dair kanıt olmalıdır. İkincisi, teknik önlemlere ek olarak veriye erişimi zorumlu olmayan personelin de yönetsel tedbirler alınması kaydıyla veriye erişiminin kısıtlanmasıdır²²⁸.

2.2.1.7. Hesap Verebilirlik İlkesi

KVKK'da birebir karşılığı olmayan hesap verebilirlik ilkesi GVKT'nin 5/2. maddesi ile *“veri sorumlusu 1. paragrafa, yani veri işleme ilkelerine uygun davranmaktan sorumludur ve buna uygun davrandığını gösterebilmelidir.”* şeklinde tanımlamıştır. Bu ilkeye aykırı bir şekilde hareket etmediğini ispat edebilmek için veri sorumlusu ve işleyenler kendi faaliyetlerini kayıt altına alabilirler. Aynı şekilde bu kayıtları delil olarak denetim otoritesine takdim edebilirler²²⁹. Yine özel durumlar için veri sorumluları kişisel verilerin korunmasına ilişkin bir veri koruma görevlisi de atayabilir, işlemeye ilişkin herhangi bir faaliyetin veri sahibinin hakları yönünden yüksek risk içermesinin mümkün olabileceği ihtimaline karşın, işleme faaliyetinden önce veri koruma etki değerlendirmesi uygulayabilirler²³⁰.

GVKT ile hesap verme yükümlülüğü bir tek veri sorumlusuna getirilmiş olsa da, veri işleyen de muayyen yükümlülüklerle uymak zorundadır. Aynı şekilde veri işleyen de verilerle çalıştığı sırada yukarıda sayılan ilkelere uygun davrandığı ile ilgili hesap verebilir olmalıdır²³¹.

2.2.2. Veri Aktarımına İlişkin İlkeler

KVKK ile veri aktarımının ortaya çıkarabileceği negatif sonuçları engellemek amacıyla hem yurt içinde, hem de yurtdışında veri aktarımı ilgili kişinin açık rızası olmayan durumlarda kesinlikle yasaklanmıştır. Yalnızca KVKK kapsamında ilgili kişinin rızası olmaksızın hem yurt içinde hem de yurt dışında veri aktarımı

²²⁸ Develioğlu, a.g.e, s. 50, Tolun, a.g.t, s. 125.

²²⁹ GDPR, m. 30.

²³⁰ Dülger, 2019 (a), s. 107, GDPR, m. 35.

²³¹ Ovalıoğlu, a.g.t, s. 32, Dülger, 2019 (a), s. 106.

yapılmasını mümkün kılan bazı istisnalar mevcuttur. Şöyle ki yurt içinde veri aktarımının ilgili kişinin rızası olmaksızın yapılabilmesi için KVKK'nın 5. ve 6. maddelerinde öngörülen hukuka uygunluk sebeplerinden birinin varlığı, yurt dışına veri aktarımı için ise ilgili kişinin açık rızası olmayan hallerde yurtdışına veri aktarılabilmesi için hukuka uygunluk sebeplerine ek olarak aynı zamanda verilerin aktarılacağı ülkede yeterli korumanın bulunması veya yeterli korumanın veri sorumlularınca taahhüt edilmesi ve Kurul'un buna izin vermesi gerekmektedir²³². Yeterli korunmasının veri sorumlularınca taahhüt edilmesi için hazırlanacak taahhütnamelere ilişkin şartlar ve örnekler Kurum'un internet sitesinde yayınlanmıştır²³³. GVKT'de olduğu gibi taahhütnamelerin yanısıra Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmelerinde kullanılabilecek bir diğer yöntem “Bağlayıcı Şirket Kuralları”dır²³⁴.

GVKT uyarınca kişisel verilerin Avrupa Birliği içerisinde serbest dolaşımı için herhangi bir ek bir işlem talebi belirlenmemiştir. Ek olarak Avrupa Ekonomik Alanı Ortak Komitesinin aldığı karar ile birlikte GVKT hem de Avrupa Ekonomik Alanı (AEA) Anlaşması'nın bir parçası sayılarak verilerin serbest dolaşımı Norveç, İzlanda ve Lihtenştai gibi Birlik üyesi olmayan ülkeleri de kapsamaktadır²³⁵.

Verilerin AEA dışına aktarılması ihtimali öngörülerek GVKT ile bu tür aktarımların kişisel verilerin korunması açısından oluşturabileceği riskleri en aza indirmek için bazı ek tedbirler getirilmiştir. Bu konuda AEA içerisinde veri aktarımını serbest bırakılarak veri sorumlularına kısmi bir serbesti sağlanırken, yalnızca 3. ülkelere veri aktarımı konusunu zorlaştırmıştır. GVKT ile kişisel verilerin hukuka uygun olarak üçüncü ülkelere aktarılabilmesi için aktarımın bir yeterlilik kararına dayanmasını, uygun güvencelere tabi olarak yapılmasını, bağlayıcı kurumsal kurallar kapsamında yapılmasını ya da kanunda açıkça sayılan istisnai durumlardan birinin varlığını şart koşmuştur.

²³² KVKK, madde 9(2).

²³³ Kişisel Verileri Koruma Kurumu, “Yurtdışına Veri Aktarımında Veri Sorumlularınca Hazırlanacak Taahhütnamede Yer Alacak Asgari Unsurlar, <https://www.kvkk.gov.tr/Icerik/4236/Yurtdisina-Veri-Aktariminda-Veri-Sorumlularinca-Hazirlanacak-Taahhutnamede-Yer-Alacak-Asgari-Unsurlar>, E.T.: 23.04.2022.

²³⁴ Kişisel Verileri Koruma Kurumu, Yurtdışına Aktarım, <https://www.kvkk.gov.tr/Icerik/2053/Yurtdisina-Aktarim>, E.T.: 23.04.2022.

²³⁵ Decision of the EEA Joint Committee, No 154/2018, 06.07.2018, <https://eur-lex.europa.eu/legal-content/GA/ALL/?uri=CELEX:22018D1022>, E.T.: 21.04.2022

GVKT 45. madde uyarınca hakkında hukukun üstünlüğü, insan hakları ve temel özgürlüklere saygı, bağımsız denetim otoritesinin varlığı ve etkili bir şekilde işlev göstermesi gibi hususların da yer aldığı niteliklerin varlığı durumunda veri sahiplerinin haklarının etkin şekilde korunduğu ve onların haklarına ilişkin yeterli adli tazminin bulunduğu ülkeler ve uluslararası kuruluşlara veri aktarımı, herhangi başka bir izin aranmaksızın yapılabilir. Hakkında verilerin korunması bakımından yeterlilik kararı alınan ülkeler; Andora, Arjantin, Kanada (ticari kuruluşlar), Faroe Adaları, Guernsey, İsrail, Man Adası, Japonya, Jersey, Yeni Zelanda, Kore Cumhuriyeti, İsviçre ve Uruguay'dır²³⁶.

Yeterlilik kararı dışında veri aktarımı yapılmasına ilişkin belirlenmiş diğer şart, 46. maddede belirtildiği üzere uygun güvencelerin sağlamış olmasıdır. Örneğin, kamu kuruluşları ya da organlar arasında yasal anlaşmalar ve ya bağlayıcı diğer yasal kurallar “*uygun güvenceler*” kapsamında değerlendirileceklerdir²³⁷.

Ortak bir ekonomik faaliyette bulunan teşebbüsler ya da işletmeler grubunun faaliyetleri çerçevesinde kendi içerisinde AEA dışındaki ülkelere veri aktarımı yapması bağlayıcı kurumsal kurallarla mümkündür ve GVKT'nin 47. maddesine göre bağlayıcı kurumsal kuralların veri aktarımı için hukuki bir temel gibi sayılması için bu kurallar yetkin denetim otoritesi tarafından onaylanmış olmalıdır.

Bağlayıcı kurumsal kuralların (BKK) onaylanmaları için hukuksal olarak bağlayıcı, tüm veri koruma ilkelerini kapsayan ve tüm üyelerce uygulanan nitelikte olması gereklidir. Aynı şekilde, kuralların veri sahibinin haklarını açık uygulanabilir şekilde ifade etmeli, veri koruma şartlarını, onların uygulanma şekillerini açıklamalıdır. Ek olarak, bağlayıcı kurumsal kurallar hem de bu kuralların ihlali durumları için yaptırımları, sorumluluk ve tazminat kurumlarına ilişkin içeriği barındırıyor olmalıdır²³⁸.

GVKT'nin veri aktarımına ilişkin dikkat çeken diğer bir düzenlemesi bir yeterlilik kararı yahut güvencelerin sağlanması olmadan da AEA dışındaki ülkelere veri transferi yapılmasının mümkün olduğu istisnai hallerin belirlenmiş olmasıdır. Hukuki veri aktarımı için son çare olarak baş vurulan bu durum GVKT'nin 49. maddesiyle belirlenmiştir. Veri sahibinin verilerin transfer riskleri konusunda

²³⁶ European Commission, “Adequacy decisions”, Adequacy decisions | European Commission, E.T.: 11.09.2022.

²³⁷ Dülger, 2019 (a), s. 106.

²³⁸ Handbook, 2018, s. 263.

aydınlatılmasına rağmen açık rıza göstermesi, veri transferinin kamu yararına ilişkin önemli nedenlerden dolayı gerekiyor olması gibi istisnai hallerin mevcutluğu durumunda büyük çaplı yahut tekrarlanan veri aktarımları hukuka uygun sayılabilecektir²³⁹.

2.3. VERİ SORUMLUSUNUN YÜKÜMLÜLÜKLERİ

2.3.1. Genel Olarak

2.3.1.1. Aydınlatma Yükümlülüğü

Kişisel verilerin işlenmesi sırasında veri sahibinin aydınlatılması kişisel verilerin korunması hukukunun veri sorumlusuna yüklediği temel yükümlülüklerdendir. Kişisel verilerin korunması hakkının amacına uygun ve etkin bir şekilde kullanması bu yükümlülüğün yerine getirilmesi ile mümkündür²⁴⁰. Zira kendisiyle ilgili bir kişisel veri işleme faaliyetinin mevcut olmasından habersiz ilgili kişi kendisine tanınan bilgi alma, yanlış veya güncel olmayan verileri gerektiğinde düzelttirme, sildirme veya yok ettirme, veri işleme sürecine yönelik itirazda bulunma ve kendisi hakkındaki verilerin başkalarına aktarılmasını durdurma gibi haklarını kullanamayacaktır²⁴¹.

Aydınlatma yükümlülüğünün kapsamı KVKK'da 10. madde ile belirlenmiştir. Bu maddeye göre en geç kişisel verilerin elde edilmesi sırasında veri sorumlusu veya onun tarafından yetkilendirilmiş kişi, veri sahiplerine 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 ilgili ve veri sahibinin Kanunun 11. maddesinde sayılan diğer hakları konusunda bilgi vermekle yükümlü tutulmuştur.

²³⁹ Handbook, 2018, s. 264.

²⁴⁰ Dülger, 2019, (b), s. 297.

²⁴¹ Şimşek, a.g.e, s. 88.

Aydınlatma yükümlülüğü, KVKK’da açıkça gösterilmemiş kişisel verilerin korunması hukukunun genel ilkelerinden olan şeffaflık ve hesap verilebilirlik ilkelerinin de gereğidir²⁴².

Bu yükümlülüğün aynı zamanda verilerin doğru ve gerektiğinde güncel olması ilkesini (KVKK m. 4/2-b) hayata geçirmeye yönelik olduğu söylenebilir. Aksi halde kendi kişisel verilerinin işlenip işlenmediğinden haberdar olmayan veri sahibinin bu verilerin doğru ve güncel olup olmadığını da denetlemeyecektir.

Aydınlatma yükümlülüğü yalnızca kişise verilerin veri sahibinden değil, onun haricindeki başka kaynaklardan toplanması aşamasında da söz konusudur²⁴³.

Bu husus KVKK’da açıkça belirlenmemiş olsa da, GVKT’da madde 14/3’de ayrı bir maddede ayrıntılı olarak düzenlenmiştir. Maddeye göre, *“Kişisel verilerin ilgili kişiden elde edilmemesi halinde, veri sorumlusu, kişisel verilerin elde edilmesinden sonra makul bir süre içinde kişisel verilerin işlendiği koşullar dikkate alınarak en geç bir ay içinde, elde edilen kişisel veriler ilgili kişi ile iletişim kurmak için kullanılacaksa en geç ilgili kişi ile ilk iletişime geçildiğinde veya kişisel verilerin başka bir alıcıya aktarılması düşünüüyorsa, en geç veriler ilk aktarıldığında ilgili kişiyi bilgilendirmelidir”*.

Bahsi geçen gereklilik *“Kişisel Verileri Koruma Kurumu”* tarafından yayınlanan *“Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ”*in 6. maddesinde benzer biçimde vurgulanmıştır²⁴⁴. Tebliğin 5. maddesi uyarınca, *“Aydınlatma yükümlülüğünün yerine getirilmesine ilişkin metinlerde, muhatabın anlayacağı açıklıkta ve yalın bir yazım dili kullanılmalı, genel nitelikte ve muğlak ifadelerle yer verilmemelidir. Bu kapsamda gelecekte gündeme gelebilecek başka amaçlar için kişisel verilerin işlenebileceği kanaati uyandıran ifadelerle, eksik, ilgili kişileri yanıltıcı ve yanlış bilgilere yer verilmemelidir”*. Ancak Tebliğ’de yine GVKT’dan farklı olarak makul sürenin en fazla ne kadar olacağı gösterilmemiştir.

²⁴² Kişisel Verileri Koruma Kurumu, Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi, AYDINLATMA YÜKÜMLÜLÜĞÜNÜN YERİNE GETİRİLMESİ REHBERİ, Ankara, KVKK Yayınları, 2018, E.T.: 27.04.2022, Ş. İ Aşıkoğlu, “Veri Sorumlularının Aydınlatma Yükümlülüğü - Avrupa Birliği ve Türk Hukukunda”, Kişisel Verileri Koruma Dergisi, Cilt 1, Sayı 2, 2019, s.43, Şimşek, s.90.

²⁴³ Develioğlu, a.g.e, s. 85.

²⁴⁴ Resmi Gazete, 10.03.2018, Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ, Sayı: 30356.

KVKK ve GVKT’de aydınlatma yükümlülüğünün ne şekilde yerine getirileceği hususunda veri sorumlusunu sınırlayan bir yöntem ve şekil şartı öngörülme de, Tebliğ’de bu konuda kullanılabilecek bazı yöntemlerden örnekler verilmiştir. Örnek olarak, madde 5’e göre “*Veri sorumlusu ya da yetkilendirdiği kişi tarafından sözlü, yazılı, ses kaydı, çağrı merkezi gibi fiziksel veya elektronik ortam kullanılmak suretiyle aydınlatma yükümlülüğünün yerine getirilmesi mümkündür*”. Yinne aynı maddeye göre “*veri sorumlusunun aydınlatma yükümlülüğünün gereği gibi yerine getirildiğine dair ispat yükü olduğundan, veri sorumlusu aydınlatma işlemini gerçekleştirirken bunu kayıt altına alabilir ve aynı şekilde kendisine ispatta kolaylık sağlayacak yöntemlerin kullanabilir*”²⁴⁵.

GVKT madde 13/4 ve 14/5-a uyarınca KVKK’dan farklı olarak aydınlatma yükümlülüğünün istisnalarına yer verilmiştir. GVKT 13/4’e göre veri sahibi aydınlatma yükümlülüğü kapsamında ona verilmesi gereken bilgileri zaten biliyorsa veya madde 14/5 uyarınca kişisel verilerin kamu yararına, bilimsel çalışma ya da tarihi araştırma amacıyla veya arşivleme işlemi için işlendiği durumlarda, veri sorumlusunun aydınlatma yükümlülüğü olmayacaktır”.²⁴⁶ Benzer istisnalara KVKK’nın 28. maddesinde Kanunun hükümlerinin tamamen ve kısmen uygulanamayacağı durumların arasında yer verilmiştir.

Aydınlatma yükümlülüğünün yerine getirilmesi veri sahibinin talebine veya kabulüne yada veri sahibince verilecek bilgiye ilgi gösterilip gösterilmediğine ve veri sahibinin bu yönde talepte bulunup bulunmadığına bağlı değildir. Veri sorumlusunun, kendiliğinden aydınlatma yükümlülüğünü yerine getirmesi bunu ispatlaması için önem arz etmektedir²⁴⁷. Bu duruma örnek olarak Kurul’un 19.03.2022 tarihli kararı gösterilebilir. Bahsi geçen kararda; veri sorumlusu

“...bankanın aydınlatma metninin internet sitesinde herkes tarafından erişime açık şekilde yer aldığı, internet sayfasında “Bize Ulaşın” bölümünü kullanarak iletilen başvurularda “Kişisel Verilerin Korunması Kanunu kapsamında yapılan Bilgilendirmeyi okudum, anladım” kutucuğu ile, Çağrı Merkezi arandığında ilk olarak kayıp/çalıntı/şüpheli işlem bildirimi işlemleri ile birlikte Kişisel Verilerin Korunmasına ilişkin

²⁴⁵ Özkan, a.g.e, s. 170.

²⁴⁶ Handbook, s. 215.

²⁴⁷ Handbook, s. 207, Elif Gizem Koç, Kişisel Verilerin korunmasında Veri Sorumlusunun Medeni Hukuktan doğan Sorumluluğu, Yüksek Lisans Tezi, Marmara Üniversitesi, Sosyal Bilimler Enstitüsü, İstanbul, 2020, s. 76-77

bilgi alınması hususundaki işlem menüsüne yönlendirildiği, ilgili kişiye çağrı merkezi kanalıyla KVKK aydınlatma metni sunulduğu, ancak müşterinin dinlememeyi tercih ettiği, ilgili kişinin “Çağrı Merkezi” kanalıyla ve Banka web sayfasında “Bize Ulaşın” bölümünde oluşturduğu başvurusunda aydınlatma yükümlülüğünün yerine getirildiği” tespit edilmiştir²⁴⁸.

2.3.1.2. Temsilci Atama Yükümlülüğü

Çalışmamızın başında belirtildiği üzere GVKT’nin uygulama alanı yalnızca Avrupa Birliği devletlerini kapsamamaktadır. Eğer veri sorumlusu ve veri işleyen Birlik içerisindeki kişilerin verilerini işlerse, kendileri AB’de bulunmasa bile Tüzük yine uygulanacaktır. Bu durum için düzenleme veri sorumlusu veya işleyen tarafından yazılı olarak Birlik içerisinde bir temsilci atanması gerektiği yönündedir²⁴⁹. Atanacak olan temsilci verileri işlenmekte olan ve ya gösterilen hizmetlere ilişkin davranışları takip edilen veri sahiplerinin yerleştiği üye devletlerden birinde bulunacaktır²⁵⁰. Ancak Birlik içerisinde bulunmayan veri sorumlusu birden fazla üye devlette bulunan kişilerin verilerini işlerse, veri sorumlusu kendi temsilcisinin hangi ülkede yerleşeceğini belirlemek hakkına sahip olacaktır²⁵¹.

Veri sorumlusu kendi temsilcisini hangi ülkeye atayacak olmasına bağımsız olarak Birlik vatandaşlarının tamamına yönelik aydınlatma metinlerinde temsilcisine ait kimlik ve iletişim bilgilerine mutlaka yer vermelidir²⁵².

GVKT’nin 4/17. maddesi uyarınca temsilciler Birlik içerisinde bulunan veri sorumlusu ve veri işleyenlerin yükümlülüklerine ilişkin onları temsil eden gerçek veya tüzel kişi şeklinde tanımlanmıştır. Aynı şekilde 27. madde uyarınca temsilci

²⁴⁸ Kurul Kararı, 10.03.2022, <https://www.kvkk.gov.tr/Icerik/7296/2022-224>, E.T.: 05.09.2022

²⁴⁹ GVKT m. 27(1); Develioğlu, a.g.e, s. 98-99.

²⁵⁰ GVKT m. 27(3).

²⁵¹ EDPB, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - Version for public consultation, 2019, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) Version 2.1 12 November 2019 , E.T.: 25.04.2022

²⁵² Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - Version for public consultation, s. 12.

veri sorumlusu veya işleyen tarafından yazılı olarak belirlenir ve gerçek kişiler gibi tüzel kişiler de temsilci olabilir²⁵³.

KVKK uyarınca veri sorumlusuna temsilci atama yükümlülüğü direkt olarak belirlenmese de, 10. maddeye göre veri sorumluları veya yetkilendirdiği kişi kişisel verilerin elde edilmesi sırasında ilgili kişilere veri sorumlusunun ve varsa temsilcisinin kimliği konusunda bilgi vermekle yükümlü kılınmıştır.

2.3.1.3. İş Bölümü Anlaşması Yapmak

Tüzük uyarınca veri işleme faaliyetine dair amaçlarını ve usullerini ortak şekilde belirleyen birden fazla veri sorumlusu ortak veri sorumlusu olarak tanımlanmaktadır²⁵⁴. Birlik veya üye devlet hukukunda tespit edilmediği takdirde ortak veri sorumluları Tüzük'te yer alan yükümlülüklerini bir anlaşma ile açıkça belirlemelidirler²⁵⁵.

Ortak veri sorumluları kendi faaliyetlerinin hukuka uygun olmasından ve oluşabilecek herhangi bir ihlalden birlikte sorumlu olacaklardır. Veri sorumlularından biri diğer ortağın ihlallerinden sorumlu tutulmak istemiyorsa hangi yükümlülüğün kime ait olduğunu açıkça belirlemelidir²⁵⁶.

Ortak veri sorumlularının sorumluluklarını belirlemesi veri sahiplerinin mağduriyetine yol açacak, ya da kendi sorumluluklarına nazaran sorumsuzluğa neden olacak şekilde düzenlenemez. Böyle bir anlaşmanın yapılsa dahi hükümsüz sayılacaktır. Ortak sorumlular yine ayrı ayrı sorumlu olacaklardır. Veri sorumlularının veri sahiplerinin haklarını kullanmasına ilişkin yükümlülükleri ise ortak veri sorumluların hiç birine devredilemez²⁵⁷. Ortak sorumluları veri sahiplerinin haklarını kullanması için GVKT ile belirlenen uygun koşulları

²⁵³ Dülger, 2019 (a), s. 108.

²⁵⁴ GVKT, m. 26(1).

²⁵⁵ GVKT m. 26(1); Develioğlu, a.g.e, s. 102.

²⁵⁶ Information Commissioner's Office, "What does it mean if you are joint controllers?", <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-GDPR/controllers-and-processors/what-does-it-mean-if-you-are-joint-controllers/>, E.T.: 25.04.2022.

²⁵⁷ Gernot Fritz, Nadja Paulus, "CJEU rules on joint controllership – what does this mean for companies?", Freshfields Bruckhaus Deringer LLP, <https://technologyquotient.freshfields.com/post/102f0aw/cjeu-rules-on-joint-controllership-what-does-this-mean-for-companies>, E.T.: 25.04.2022.

oluşturulmalıdır²⁵⁸. GVKT'nin 28. maddesi uyarınca, veri sorumlusu veri işleme faaliyeti esnasında Tüzüğün hükümlerinin yerine getirilmesini temin etmelidir. Ayrıca veri sahibinin haklarının korunması için en uygun teknik tedbirleri ve yeterli güvenceleri sağlayacak veri işleyenleri kullanmalıdır²⁵⁹.

KVKK ile ortak veri sorumluları kavramına yer verilmemiştir. Ortak sorumluluk kişisel verilerin veri sorumlusu adına başka bir gerçek veya tüzel kişi tarafından işlenmesi durumunda veri sorumlularının veri güvenliğine ilişkin yükümlülükleri hususunda bu kişilerle birlikte müştereken sorumlu olacakları şeklinde düzenlenmiştir²⁶⁰.

2.3.1.4. Zararı Tazmin Yükümlülüğü

Veri sahiplerinin KVKK'nın 11/1-ğ ve 14/3. maddeleri ile kişisel verilerinin hukuka aykırı olarak işlenmesi sonucu zarara uğraması durumunda zararın giderilmesini talep etme hakkı vardır.

KVKK ile zararı tazmin yükümlülüğü sadece veri sorumluları için belirlenmişken, GVKT'nin 82/1. maddesi ile getirilen bir yenilik olarak hem veri sorumlusuna hem de veri işleyene belli ölçüde sorumluluk yüklenmiş ve veri işleyenlerin yükümlülükleri genişletilerek sorumluluk bakımından veri sorumlusuna yaklaştırılmıştır²⁶¹. KVKK'da ise tazminat sorumluluğu bakımından tek muhattap veri sorumlusu olduğundan veri sahibi zararın giderilmesini ilk olarak ondan talep edebilecektir²⁶².

2.3.1.5. İspat Yükümlülüğü

GVKT'de ispat hususu ayrı bir madde ile düzenlenmişken KVKK'da ise bu husus genel hükümlere bırakılmıştır. GVKT'ye göre veri sorumlusu veri işleme faaliyetini genel ilkelere uygun hale getirmeli ve gerektiğinde bunu ispat

²⁵⁸ Dülger, 2019 (a), s. 109.

²⁵⁹ GVKT m. 28(1).

²⁶⁰ KVKK, m. 12(2).

²⁶¹ Aşıkoğlu, a.g.m, s. 73, Tamer Soysal, "Unutulma hakkının Avrupa Birliği'nin Genel Veri Koruma Tüzüğü Çerçevesinde İncelenmesi", Cilt 0, Sayı 13, 2019, s. 371.

²⁶² Çelikel, a.g.e, s. 115.

edebilmelidir. Bu hüküm hesap verebilirlik ilkesinin gereğidir²⁶³. Genel hükümler uyarınca kişisel verilerin işlenmesi bir hukuka uygunluk nedeni bulunmadığı sürece hukuka aykırı olduğundan veri işlenmesinin hukuka uygun olduğunu ve ortada bir veri işleme nedeninin bulunduğunu ispat yükümlülüğü veri sorumlusunun üzerindedir²⁶⁴. Çünkü hukuka aykırılık bir karine olarak kabul edilmektedir ve karinenin aksi yani veri işleme faaliyetinin hukuka uygun olduğunu ispat ise veri sorumlusuna düşmektedir²⁶⁵. Ancak veri sorumlusu ispat yükümlülüğünü yerine getirmek için işleme faaliyetinin gerektirdiğinden fazla veri elde etmemeli ve işlememelidir²⁶⁶.

2.3.1.6. Denetim Yükümlülüğü

Veri sorumluları tarafından veri güvenliğinin sağlanması için yerine getirilmesi gereken bir diğer yükümlülük, denetim yükümlülüğüdür. KVKK'nın 12/3. maddesinde denetim yükümlülüğü, *“Veri sorumlusu, kendi kurum veya kuruluşunda, KVKK hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorundadır.”* şeklinde belirtilmiştir.

Veri sorumlusu söz konusu denetimi bizzat kendisi yapmak zorunda değildir. Çünkü madde *“denetimleri yapmak veya yaptırmak”* şeklindedir, yani veri sorumlusu bu konuda profesyonel denetim kuruluşlarından hizmet alabilir veya kendi adına denetim yapması için bir başkasını görevlendirebilir²⁶⁷.

GVKT'de ise kamu kurum ve kuruluşları gibi belirli veri sorumluları açısından bu denetimleri yapma görevi, KVKK'dan farklı olarak veri koruma görevlisine bırakılmıştır. KVKK'da böyle bir kavrama yer verilmemiştir. Türk hukuku bakımından hiç olmazsa, Veri Sorumluları Siciline kayıt yükümlülüğü bulunan veri sorumluları yönünden benzer bir uygulamaya gidilmesi, veri koruma hukuku kurallarına uyumun sağlanması için faydalı olabilirdi²⁶⁸.

²⁶³ GVKT, m. 5/2, Ozan Selek, “Genel Veri Koruma Tüzüğü Işığında Kişisel Verilerin İşlenmesinde Rıza Açıklaması”, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, Cilt 21, Sayı 2, 2019, s. 921.

²⁶⁴ Develioğlu, a.g.e, s. 117.

²⁶⁵ Çelikel, a.g.e, s. 130.

²⁶⁶ EDPB, Guidelines 05/20 Consent under Regulation 2016/679, s. 22-23, Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1, E.T.: 05.09.2022.

²⁶⁷ Özkan, a.g.e, s. 170.

²⁶⁸ Yasemin Avcı, “Kişisel Verilerin Korunması”, Yüksek Lisans Tezi, Selçuk Üniversitesi, Sosyal Bilimler Enstitüsü, Konya, 2019, s. 90.

2.3.1.7. Kurul Kararlarına Uyma Yükümlülüğü

KVKK'nın 15/5. maddesine göre eğer Kurul yapılan şikayet üzerine ya da resen yaptığı inceleme sonucunda ihlalin varlığı kanaatine gelirse tespit ettiği hukuka aykırılıkların veri sorumlusu tarafından ortadan kaldırılmasına karar vererek ve bu kararı ilgililere tebliğ edecektir. Kurul'un bu kararı, veri sorumlusunca tebliğden sonra gecikmeden ve en geç otuz gün içinde yerine getirilmelidir. Kurul kararlarına uymamanın yaptırımı KVKK'nın kabahat yaptırımlarına ilişkin 18/1-c maddesinde gösterilmiştir. Buna göre, *“Kanunun 15. maddesi uyarınca Kurul tarafından verilen kararları yerine getirmeyenler hakkında idari para cezası yaptırımı uygulanmasına”* karar verilecektir²⁶⁹.

GVKT'nin 60. maddesi uyarınca veri sorumlusu ya da veri işleyen baş denetim otoritesinin kararı hususunda bildirim yapıldıktan sonra Birlik içerisindeki tüm işletmeler içerisinde veri işleme faaliyetlerine ilişkin karara uyumluluk sağlanması için gereken tedbirleri alır. Aynı veri sorumlusu ya da veri işleyen denetim otoritesinin kararına uyumun sağlanması amacıyla alınan tedbirleri, diğer ilgili denetim otoritelerini de bilgilendirecek baş denetim otoritesine bildirir.

2.3.2. Veri Kayıt ile İlgili Yükümlülükler

2.3.2.1. Veri Koruma Politikaları Oluşturma

KVKK uyarınca Veri Sorumluları Siciline kayıt yükümlülüğüne tabi tutulan veri sorumlularına yüklenen diğer bir yükümlülük, *“Veri Sorumluları Sicili Hakkında Yönetmelik”* madde 5/1-ç ile yer verilen *“kişisel veri işleme envanteri hazırlama yükümlülüğü”*dür²⁷⁰. Yönetmeliğe göre,

“Kişisel veri işleme envanteri, veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirdikleri kişisel veri işleme faaliyetlerini, amaçlarını ve hukuki sebebi, veri kategorisi, verilerin aktarıldığı alıcı grubunu ve veri konusunu, kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin

²⁶⁹ Emine Hizarcı, “6698 Sayılı Kişisel Verilerin Korunması Kanununun AB Veri Koruma Hukuku Işığında Değerlendirilmesi”, 1. Baskı, İstanbul, Yetkin Yayınları, 2020, s. 143.

²⁷⁰ Resmi Gazete , 30.12.2017, Veri Sorumluları Sicili Hakkında Yönetmelik, Sayı 30286.

işlendikleri amaçlar için gerekli olan azami muhafaza edilme süresini, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları belgedir”²⁷¹.

Veri sorumlularına kişisel veri işleme envanteri hazırlama yükümlülüğünün belirlenmesinin nedeni, veri işleme faaliyetinin yürütüldüğü bütün süre boyunca hukuka aykırı bir durumun varlığında bunun kolayca ortaya çıkarılmasıdır²⁷².

Veri sorumlusunun ilgili yükümlülüğünün GVKT hükümlerindeki karşılığı ise madde 24/1 ile tespit edilmiştir. Maddeye göre, veri sorumlusu veri işleme faaliyetini GVKT hükümlerine uygun olarak gerçekleştirilmelidir ve bunu kanıtlamak için uygun teknik ve organizasyonel tedbirleri almalı ve uygulamalıdır. Bu amacın yerine getirilmesi için veri sorumlusu uygun veri koruma politikalarını uygular²⁷³.

2.3.2.2. Veri Saklama ve Kayıt Yükümlülüğü

KVKK’nın 12/4. maddesinde, veri sorumlusunun “*genel bir sır saklama yükümlülüğü*”ne yer verilmiştir. Bu maddeye göre,

“Veri sorumluları ile veri işleyen kişiler, öğrendikleri kişisel verileri KVKK hükümlerine aykırı olarak başkasına açıklayamaz ve işleme amacı dışında kullanamazlar ve bu yükümlülük bu kişilerin görevden ayrılmalarından sonra da devam eder”.

Bu hüküm gereğince veri sorumluları ve veri işleyenler elde ettikleri kişisel verileri bir hukuka uygunluk nedeni olmadan başkasına açıklayamaz ve işleme amacı dışında kullanamaz.

İlgili madde ile veri sorumlularına genel bir sır saklama yükümlülüğü getirilmiştir. Dolayısıyla veri sorumlularına başka kanunlarla daha spesifik alanlarda saklama yükümlülüğü getirilmesi mümkündür. Örneğin, 4857 Sayılı İş Kanunu’nda işçi verilerinin işlenmesi nedeniyle veri sorumlusu olan işverenin sır saklama yükümlülüğüne yer verilmiştir. Buna göre Kanun’un 75/2. maddesinde,

²⁷¹ Resmi Gazete , 30.12.2017, Veri Sorumluları Sicili Hakkında Yönetmelik, Sayı 30286, m. 4/1-h.

²⁷² Kişisel Verileri Koruma Kurumu, Kişisel Veri İşleme Envanteri Hazırlama Rehberi, Ankara, 2019, KİŞİSEL VERİ İŞLEME ENVANTERİ HAZIRLAMA REHBERİ, E.T: 28.04.2022, s. 10.

²⁷³ GVKT, m. 24/2.

“İşverenin, işçi hakkında edindiği bilgileri dürüstlük kuralları ve hukuka uygun olarak kullanmak ve gizli kalmasında işçinin haklı çıkarı bulunan bilgileri açıklamamakla yükümlü olduğu” belirtilmiştir.

Aynı şekilde, ilgili madde ile sır saklama yükümlülüğünden bağımsız olarak veri sorumlularına ve veri işleyenlere verileri işleme amacı dışında kullanmama yükümlülüğü yüklenmiştir. Bu yükümlülük, KVKK’nın 4/2-ç maddesinde yer verilmiş genel ilkelerden olan kişisel verilerin *“işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması”* ilkesinin de bir gereğidir²⁷⁴.

KVKK’nın 16/2. maddesi ile veri sorumluları için sicile kayıt yükümlülüğü düzenlenmiştir. Bu yükümlülüğe göre, kişisel verileri işleyen gerçek ve tüzel kişiler, veri işleme faaliyetine başlamadan önce Veri Sorumluları Sicili’ne kaydolmak zorundadırlar. Ancak işlenen kişisel verinin niteliği, sayısı veri işlemenin kanundan kaynaklanması veya üçüncü kişilere aktarılma durumu gibi objektifliği Kurul tarafından belirlenebilecek kriterlerle birlikte yine Kurul tarafından, Veri Sorumluları Sicili’ne kayıt yükümlülüğüne istisnalar getirilebilir. Örneğin; Kişisel Verileri Koruma Kurulu’nun 02.04.2018 tarihli kararıyla *“yalnızca ilgili mevzuat ve amaçlarına uygun, faaliyet alanlarıyla sınırlı olmak üzere kişisel veri işleyen Türkiye’de yerleşik dernek, vakıf ve sendikalar”* için Sicil’e kayıt yükümlülüğüne istisna getirilmiş,²⁷⁵ daha sonra 09.06.2021 tarihli kararla yapılan değişiklikle birlikte yeniden *“noterler, siyasi partiler, avukatlar, serbest muhasebeci ve yeminli mali müşavirler, yalnızca ilgili mevzuat ve amaçlarına uygun faaliyet alanlarıyla sınırlı olmak üzere kişisel veri işleyen Türkiye’de yerleşik dernek, vakıf ve sendikalar”*²⁷⁶ veri sorumluları siciline kaydolma yükümlülüğünden muaf tutulmuştur. Veri sorumlularının sicile kayıt yükümlülüğünden muaf tutulması Kanun’da öngörülen diğer yükümlülüklerden ve Kanun’dan muaf tutulması demek değildir²⁷⁷. Uygulamada bu konuya ilişkin bir yanlış anlaşılmanın mevcut olduğu gözükmektedir. Sicile kayıt olunsun veya olunmasın KVKK yürürlüktedir ve veri sorumluları veri işleme faaliyetlerini KVKK’ya uygun olarak yürütmelidir²⁷⁸. Zira

²⁷⁴ Çelikel, a.g.e, s. 115.

²⁷⁵ Kurul Kararı, 02.04.2018, <https://kvkk.gov.tr/Icerik/4233/2018-32>, E.T.: 28.04.2022.

²⁷⁶ Kurul Kararı, 09.06.2021, <https://www.kvkk.gov.tr/Icerik/6986/2021-571>, E.T.: 28.04.2022.

²⁷⁷ Güneysu Nilüfer Boran, Burak Memiş, “Kişisel Verilerin Korunması Kanunu Kapsamında Avukatın Yükümlülük ve Sorumlulukları”, Anadolu Üniversitesi Hukuk Fakültesi Dergisi, Cilt 5, Sayı 2, 2019, s. 327.

²⁷⁸ Çelikel, a.g.e, s. 121.

Anayasa Mahkeme'sinin KVKK'nın bazı maddelerinin iptali talebiyle açılmış dava ile ilgili kararında “

Bazı veri sorumlularının Kurul tarafından veri sorumluları siciline kayıt yükümlülüğünden muhaf tutulmasının, Kanun'un 12. maddesinde veri sorumluları için belirlenen yükümlülüklerin devam etmesi, bu yükümlülükler bakımından sicile kayıt zorunluluğunun bir öneminin bulunmadığı, bu nedenle bu durumun veri sorumlularının veri güvenliğine ilişkin yükümlülüklerine istisna getirmediği veya kişinin haklarını korumak bakımından öngörülen tedbirleri ortadan kaldıran bir düzenleme şeklinde değerlendirilemeyeceği”

gereğesiyle KVKK'nın 12. maddesine ilişkin iptal talebi reddedilmiştir²⁷⁹.

Kamuya açık bir sicil tutulması KVKK'da genel ilkeler arasında yer verilmesi de şeffaflık ilkesinin gereği yerine getirilmesidir²⁸⁰.

Sicile kayıt yükümlülüğü aynı zamanda ilgili kişilerin kendi verileri üzerinde denetim ve kontrol sağlamaları bakımından da önem arz etmektedir. Çünkü bir veri sorumlusu tarafından kişisel verilerinin işlenmesi için açık rıza talep edilen ilgili kişiler kamuya açık olan bu sicildeki bilgileri inceleyerek verilerine ilişkin açık rıza verip vermeyeceklerine yönelik daha sağlıklı kararlar alabilme imkanı elde edeceklerdir²⁸¹.

GVKT madde 30/1'e göre veri sorumlusunun işlediği verilerle ilgili kayıt tutma yükümlülüğü vardır. Bu kayıtlarda yazılı ya da elektronik olmasına bağımsız veri sorumlusu, veri koruma görevlisi, veri işleme amaçları, veri sahibi ve kişisel veri kategorileri, alıcılar, veri aktarımları, verilerin silinmesine ilişkin süre sınırları gibi açıklamalar yer almalıdır.

2.3.2.3. Veri İhlali Açıklaması ve Bildirimi

KVKK'ya göre işleme faaliyetinin konusu olan veriler hukuka aykırı şekilde başkaları tarafından elde edilirse veri sorumluları ilgili veri ihlalini veri sahibine ve Kurula bildirmelidir²⁸².

²⁷⁹ Anayasa Mahkemesi Kararı, 28.09.2017, <https://normkararlarbilgibankasi.anayasa.gov.tr/Dosyalar/Kararlar/KararPDF/2017-143-nrm.pdf>, E.T.: 28.04.2022.

²⁸⁰ Şimşek, a.g.e, s. 100, Güneysu / Memiş, a.g.m, s. 329, Çekin, a.g.e, s. 215.

²⁸¹ Özkan, a.g.e, s. 180, Çelikel, a.g.e, s. 122.

²⁸² KVKK, m. 12/5.

KVKK'nın tanımlar kısmında veri ihlali kavramı açıkça tanımlanmasa da, bu madde uyarınca veriler kanunsuz şekilde başkaları tarafından elde edilirse bunun ihlal olarak değerlendirileceği açıktır. GVKT'nin 4/12. maddesinde ise veri ihlali,

“Aktarılan, saklanan veya başka bir şekilde işlenen kişisel verilerin kazara veya yasa dışı olarak yok edilmesine, kaybolmasına, değiştirilmesine, yetkisiz ifşasına veya bunlara erişime yol açan bir güvenlik ihlali”

şeklinde tanımlanmıştır. KVKK'da başkaları tarafından sadece verilerin elde edilmesinden bahsedilse de, GVKT'ye benzer şekilde verilerin yok edilmesi, erişilmez kılınması, kaybolmasına neden olunması, değiştirilmesi ya da ifşası veri ihlali olarak gösterilmiştir²⁸³.

KVKK'nın 12/5. maddesi ile veri ihlali gerçekleştiğinde veri sorumlusunun ve Kurul'un ne yönde hareket etmesi belirlenmiştir. Buna göre, *“veri sorumlusu veri ihlali en kısa sürede ilgisine ve Kurul'a bildirmeli, Kurul ise gerekli gördüğü hallerde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan etmelidir”*. Bu ilan veri sorumlusu tarafından ulaşılamayan ve veri ihlali haberdar olmayan ilgili kişileri bilgilendirmekle veri sahiplerinin veri ihlali en az şekilde etkilenmesi için kendilerince gerekli tedbirleri almasını temin edecektir²⁸⁴.

GVKT 34/1. maddeye göre, oluşan ihlalden dolayı gerçek kişilerin hakları ve özgürlükleri açısından yüksek bir riskin olduğu durumda veri sorumlusu kişisel veri ihlali gecikmeksizin veri sahibine iletmelidir. Bu ihlalin bildirilmesi için veri sorumlusuna 72 saatlik bir süre tanınmıştır²⁸⁵. GVKT'den farklı olarak KVKK'da en kısa sürede bildirim yükümlülüğünün bahsedilse de bunun için belli bir süre belirlenmemiştir²⁸⁶. Ancak Kurul'un 24.01.2019 tarihli, *“Kişisel Veri İhlali Bildirim Usul ve Esasları Hakkındaki Kararında”*²⁸⁷ da GVKT ile uyumlu biçimde 72 saat olarak belirlenmiştir²⁸⁸.

²⁸³ Dülger, 2019 (a), s. 119.

²⁸⁴ Dülger, 2019 (a), s. 120

²⁸⁵ GVKT, m. 33/1.

²⁸⁶ Hizarcı, a.g.e, s. 139

²⁸⁷ Kurul Kararı, 24.01.2019, <https://www.kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirimi>, E.T.: 28.04.2022.

²⁸⁸ Avcı, a.g.t, s. 92.

Kişisel veri ihlalinin mümkün olan en kısa sürede ve gecikmeden bildirilmesi oldukça önemlidir. Aksi halde, bildirim zamanında yapılmadığında, ihlalin sonuçları ve oluşabilecek zarar ağırlaşabilir²⁸⁹. Örneğin, bildirimde gecikme, ayrımcılığa uğratma, dolandırıcılık, şantaj, takma adın öğrenilerek daha çok kişisel veriye ulaşılması veya özel nitelikli kişisel verilerin ifşa edilmesi sonucu ilgili kişinin maddi veya manevi zarara uğramasına sebep olabilir²⁹⁰.

GVKT madde 33/3 uyarınca, veri sorumlusu tarafından yapılan veri ihlali bildiriminde ilgili veri ihlalinin niteliği, veri koruma görevlisi veya daha fazla bilginin elde edilebileceği diğer bağlantı noktası ile ilgili gereken isim ve bilgiler, ihlalin olabilecek sonuçları ve olumsuz etkilerinin azaltılmasına yönelik alınan/önerilen tedbirler yer almalıdır.

GVKT'nin 85. Resital'inde, bildirim yükümlülüğüne uymayan veri sorumlusunun, hesap verebilirlik ilkesi gereği, kişisel veri ihlalinin gerçek kişilerin hak ve hürriyetlerine yönelik bir risk bulundurma ihtimalinin düşük olduğunu ileri sürebileceği" gösterilmiştir²⁹¹. Ancak KVKK'ya göre veri sorumluları gerçekleşmiş veri ihlalinin gerçek kişilerin temel hak ve hürriyetlerine zarar vermesinin düşük bir risk teşkil edip etmediğine bakmadan büyük küçük, önemli yada önemsiz her türlü veri ihlalinin ilgili kişiye ve Kurul'a bildirmelidirler²⁹².

KVKK'da veri sorumlusuna hem ilgili kişiye hem de Kurul'a bildirim yükümlülüğü getirilmiştir²⁹³. Uygulamada ise kişisel verilerin, veri sorumlusunun elinde olduğu zaman değil, veri sorumlusu adına veri işleyen tarafından veri işlenmesi sırasında ihlale uğraması halinde veri ihlal bildirimini kimin yapacağı hususunda bir sorun ortaya çıkabilir. KVKK bu konuda, açık ve net bir şekilde bildirimin veri sorumlusu tarafından yapılacağına işaret etmiştir. Böylelikle veri sorumlusu, veri işleyen kendisine geç bildirimde bulunsa bile oluşabilecek gecikmeden sorumlu tutulabilir ve yalnızca iç ilişkide veri işleyene karşı talep ileri sürebilecektir²⁹⁴.

²⁸⁹ Özkan, a.g.e, s. 108.

²⁹⁰ Avcı, a.g.t, s. 43.

²⁹¹ Dülger, 2019 (a), s. 124, GDPR, Recital 85, <https://www.privacy-regulation.eu/en/recital-85-GDPR.htm>, E.T.: 01.09.2022.

²⁹² KVKK, m. 12(4).

²⁹³ KVKK, m. 12(5).

²⁹⁴ Çekin, a.g.e, s. 207.

GVKT’de veri ihlal bildiriminde bulunma yükümlülüğü, veri işleyene de getirilmiştir.²⁹⁵ Konuyla ilgili Kurul’un Kişisel Veri İhlali Bildirim Usul ve Esaslarına ilişkin 24.01.2019 tarihli kararında bu duruma değinilmiş, GVKT’la uyumlu olacak biçimde,

“Veri işleyen nezdinde bulunan kişisel verilerin hukuka aykırı olarak başkaları tarafından elde edilmesi halinde, veri işleyenin bu konuda herhangi bir gecikmeye yer vermeden veri sorumlusuna bildirimde bulunması gerektiği”

belirtilmiştir.

2.3.2.4. Veri Güvenliğini Sağlama Yükümlülüğü

Veri sorumlusunun veri güvenliğini sağlama yükümlülüğüne, KVKK’nın 12. maddesi ile yer verilmiştir. İlgili madde uyarınca,

“Veri sorumlusu;

- *Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,*
- *Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,*
- *Kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbiri almak zorundadır”.*

KVKK’da veri güvenliğini sağlamak için veri sorumlusunun *“gerekli her türlü teknik ve idari tedbiri almak zorunda olduğu”* belirtilse de, çoğunlukla genel ifadelerle yer verilmiş, teknik ve idari tedbirler hakkında bir açıklama ve ayrıntılara yer verilmemiştir²⁹⁶.

Bu husus KVKK’nın bir eksikliği olarak görülmemektedir²⁹⁷. Çünkü bu tedbirlerin neler olduğu Kişisel Verileri Koruma Kurumu’nun yayınladığı Kişisel Veri Güvenliği Rehberinde ayrıntılı olarak gösterilmiştir²⁹⁸. Zira teknolojik alandaki hızlı gelişmelerden dolayı kanunda yer verilecek tedbirler zamanla veri güvenliğini

²⁹⁵ GVKT, m. 33/2.

²⁹⁶ Develioğlu, a.g.e, s. 107, Çelikle, a.g.e, s. 122.

²⁹⁷ Samet Saygı, “6698 Sayılı Kanun’un Sistematiğinde Yargısal Başvuru Yolları”, Kişisel Verileri Koruma Dergisi, Cilt 2, Sayı 2, 2020, s. 31.

²⁹⁸ Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler), KVKK Yayınları, Ankara, 2018, https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf, E.T.: 28.04.2022.

sağlamada yetersiz kalacak ve yeni tedbirler için sürekli kanun değişikliği yapmak gerekli olacaktır²⁹⁹.

GVKT'ye göre veri sorumlusu veya veri işleyen gerçek kişilerin hakları ve özgürlükleri açısından çeşitli olasılıklar ve ciddiyetlere sahip riskleri dikkate alarak uygun bir güvenlik seviyesi sağlamalıdır. İlgili düzenlemelere göre veri sorumlusu ve veri işleyen;

“....takma ad kullanımı ve şifreleme, veri işleme sistemleri ve hizmetlerinin gizliliği, bütünlüğü, elverişliliği ve esnekliğinin sürekli olarak sağlanabilmesi, fiziksel veya teknik bir olay durumunda, kişisel verilere erişimin vakitlice eski haline getirilebilmesi, veri işleme faaliyetinin güvenliliğinin sağlanmasına yönelik teknik tedbirlerin etkililiğinin düzenli sınanması, ölçülmesi ve değerlendirilmesine ve buna ilişkin süreç gibi tedbirler uygulamalıdır”³⁰⁰.

2.4. İLGİLİ KİŞİNİN HAKLARI

2.4.1. Bilgilendirilme Hakkı

Verileri işlenen ilgili kişi herhangi bir zaman kısıtlamasına tabi tutulmadan istediği an verilerinin işlenip işlenmediğini veri sorumlusuna başvurma yoluyla öğrenme hakkına sahiptir³⁰¹. Kişinin bu hakkı yalnızca kendi kişisel verisinin işlenip işlenmediği faaliyetiyle sınırlıdır, yani ilgili kişi kendisiyle ilgisi olmayan herhangi bir veri işleme faaliyeti hususunda bilgi alma hakkına sahip değildir. Örneğin 18.09.2019 tarihli Kurul kararında, kişinin ölmüş eşine ait bilgiler için veri sorumlusuna yaptığı başvuru KVKK m. 11 kapsamında değerlendirmemiştir³⁰².

Veri sahibinin kendisi hakkında hangi kişisel verilerin işlenip işlenmediğini öğrenmesi yasal haklarını kullanabilmesi için de önemlidir³⁰³. Örneğin, ilgili kişinin bilgi talep etme hakkı kişisel verileri üzerinde yapılan değişikliklerin öğrenmesiyle birlikte ilgili verilerin düzeltilmesini talep edebilecektir. Böylelikle, ilgili kişi verilerinin doğru ve güncel olup olmadığını tespit edebilecek ve yanlış işlenmiş veya

²⁹⁹ Hizarcı, a.g.e, s. 137.

³⁰⁰ GVKT, m. 30(1).

³⁰¹ Çekin, a.g.e, s. 90.

³⁰² Kurul Kararı, 18.09.2019, <https://kvkk.gov.tr/Icerik/6710/2019-273>, E.T.: 29.04.2022.

³⁰³ Develioğlu, a.g.e, s. 83.

güncelliğini yitirmiş verilerinin düzeltilmesini talep edebilecektir³⁰⁴. Bu hak kişisel verilerin işlenmesi faaliyetinin olabildiğince şeffaf olmasını hedeflemektedir³⁰⁵.

Yukarıda ifade edildiği üzere kişinin bu hakkını kullanma zamanına ilişkin Kanun’da herhangi bir düzenleme yer almamaktadır. Dolayısıyla ilgili kişinin bu hakkı tek kullanımlık bir hak değildir ve kişi amacına ulaşanadək kişisel verilerinin işlenip işlenmediğini öğrenme hakkını sahiptir³⁰⁶. Kişisel verinin elde edilmesi, paylaşılması, aktarılması, silinmesi, yok edilmesi gibi faaliyetlerin hepsi kişisel veri işleme faaliyetleri kapsamındadır ve buna göre kişisel veri işlenmeyip muhafaza edilse bile ilgili kişi muhafaza edilen veriler için de öğrenme hakkını kullanabilir³⁰⁷.

GVKT ile de KVKK’da olduğu gibi veri sorumlularının planladıkları veri işleme faaliyetine ilişkin veri sahiplerini bilgilendirme yükümlülüğü düzenlenmiştir³⁰⁸. Bu yükümlülük veri sahibinin bilgilendirmeyi talep etme hakkından doğmaktadır³⁰⁹. Veri sahipleri verilerin hangi biçimde toplandığını, kullanıldığını ya da işlendiğini, aynı şekilde bu faaliyetden doğan riskleri ve bu risklere karşı mevcut düzenlemeleri bilme hakkına sahiptirler³¹⁰.

Tüzüğün 12. maddesine göre, veri sorumlusu gerçekleştireceği işleme faaliyeti ile ilgili veri sahibine yapacağı bilgilendirmeyi “öz, şeffaf, anlaşılır ve kolayca erişilebilir” şekilde, açık ve sade bir dil kullanarak sağlamalıdır³¹¹.

GVKT ile yapılacak bilgilendirme işleminin şekli belirlenmiştir. Düzenlemeye göre bilgilendirme yazılı ya da uygun olduğu halde, “elektronik yollar da dahil olmak üzere diğer yollarla” yapılabilir. Ayrıca bilgilendirme veri sahibinin kimliğini doğrulaması şartıyla onun talebi karşılığında sözlü olarak da sağlanabilir³¹².

Veri sorumlusu veri işleme faaliyetine başlamadan önce belirttiği amaçtan farklı bir amaçla devam etmek istediğinde veri sahibine bu yeni amacı bildirmelidir. Eğer veri sahibinin yeni ve farklı amaca ilişkin onayı alınmazsa ek bir işlemin

³⁰⁴ Muhammet Aydın, Kişisel verilerin Korunması Bağlamında idarenin Sorumluluğu ve Yargısal Denetimi, Yüksek Lisans Tezi, Ufuk Üniversitesi, Sosyal Bilimler Enstitüsü, Ankara, 2020, s. 49.

³⁰⁵ Sedat Erdem Aydın, AİHM İçtihatları Bağlamında Kişisel Verilerin Kaydedilmesi Suçu, 1. Baskı, İstanbul, On İki Levha Yayıncılık, 2015, s.30.

³⁰⁶ Nilgün Başalp, Kişisel Verilerin Korunması ve Saklanması, 1. Baskı, Ankara, Yetkin Yayınları, 2004, s. 48

³⁰⁷ Çekin, a.g.e, s. 89.

³⁰⁸ GVKT, m. 12(1).

³⁰⁹ Dülger, 2019 (a), s. 150.

³¹⁰ GVKT, Gerekçe 39.

³¹¹ GVKT, m. 12(1).

³¹² GVKT, m. 12(1).

gerçekleştirmesi mümkün değildir³¹³. Bu hem amacın sınırlandırılması hem de şeffaflık ilkelerinin gereğidir.

GVKT'ye göre bilgilendirilmenin yapılması anı kişisel verilerin elde edildiği kaynağa göre değişecektir. Şöyle ki, veri sorumlusu verileri direkt veri sahibinden almışsa, veri toplama esnasında bilgilendirme yapılmalıdır. Eğer aksine, veriler veri sahibinin kendisinden alınmamıştırsa, bu durumda veri sorumlusu bilgilendirmeyi makul bir süre zarfında, fakat en geç bir ay içinde yapmalıdır³¹⁴. Bundan başka eğer veri sorumlusunun verileri başka bir alıcıyla paylaşması sözkonusuysa, en geç verileri ilk paylaştığı anda bu konuda veri sahibini haberdar etmelidir³¹⁵.

Bilgilendirme ücretsiz olarak sağlanmalı, ancak veri sahibinin talepleri asılsız ya da ölçüsüzdürse, özellikle bu taleplerin tekrarlandığı açıkça anlaşılıyorsa veri sorumlusu bunun karşılığında makul bir ücret talep edebilir ya da ilgili talebe ilişkin işlem yapmayı reddedebilir³¹⁶. Bilgilendirmenin şekline, süresine, elde edilme kaynağına göre yapılma anına ilişkin hükümler KVKK ile düzenlenmemiştir.

2.4.2. Erişim hakkı

GVKT madde 15(1)'e göre bireylerin kendi kişisel verilerine erişim hakları vardır. Bu hak uyarınca veri sahibi kişisel verilerinin işlenip işlenmediğini kontrol edebilir ve işleme faaliyetinin mevcutluğu durumunda işlenen verilere erişebilir. Aynı şekilde KVKK madde 11 hükümlerine göre veri sahipleri veri sorumlusuna başvurarak kişisel verilerinin işlenip işlenmediğini öğrenir ve verileri işlenmişse buna ilişkin bilgi talep etme hakkına sahiptir.

Erişim hakkı gereğince veri sorumlusu, işlenen verilerle ilgili belgelerin bir nüshasını verilerin sahibine vermekle yükümlüdür. Söz konusu bilgiler anlaşılır olmalıdır³¹⁷. Örnek olarak, veri sorumlusu teknik kısaltmalar yaptığı ama söz konusu kısaltmaları açıklamadığı takdirde veri sahibine verdiği bilgiler yeterli olmayacaktır³¹⁸.

³¹³ GVKT, m. 13(1).

³¹⁴ GVKT, m. 14(3)(a).

³¹⁵ GVKT, m. 14(3)(c).

³¹⁶ GVKT, m. 12(5).

³¹⁷ GVKT, m. 15(3).

³¹⁸ Dülger, 2019 (a), s. 154.

2.4.3. Düzeltme Talep Hakkı

KVKK madde 11/d'ye göre veriler yanlış ya da eksik olarak işlendiği takdirde verilerin sahibi düzeltme talebinde bulunabilir. Kanun'un 4. maddesinde işlenen kişisel verilerin doğru ve güncel olması gerektiği düzenlenmiştir. İlgili kişi kanun kapsamında hatalı veya eksik işlenmiş kişisel verisinin düzeltilmesini talep etme hakkına sahiptir³¹⁹. Örneğin, internet ortamında alışveriş yapan ilgili kişinin adresinin kayıtlı olduğu alışveriş sitesinden bir ürün aldığı sırada ürünün eski adresine gönderilmesi, ilgili kişinin adres bilgisini değiştirmesini gerektirecektir³²⁰. Bu durumda veri sahibi veri sorumlusudan alışveriş sitesinden adres bilgilerinin değiştirilmesini talep edebilecektir. Zira hatalı veya eksik tutulan kişisel veriler üzerinden bir veri işleme faaliyetinde bulunulması ilgili kişinin haklarını ihlal edebilir³²¹.

Veri sorumlusu tarafından verilerin düzeltilmesi hususunda direniş gösterilirse, hukuka aykırı veri işleme faaliyeti sebebiyle veri sahibi veri sorumlusundan ortaya çıkan zararın giderilmesini talep edebilir veya Kurul'a şikayette bulunabilir³²². Veri sahibi verisinin yanlış ya da eksik işlendiği bilgisine ulaştığı kaynak düzeltme hakkının kullanılmasına engel değildir. Veri sahibi mevzubahis durumu nereden duyarsa duysun ilgili hakkını kullanabilir³²³.

GVKT'ye göre de KVKK'da olduğu gibi veri sahipleri doğru olmayan verilerin “*gereksiz gecikmeye mahal verilmeden*” düzeltilmesini veri sorumlusundan talep edebilir³²⁴.

Düzeltmeyi talep etme hakkı hem de kişisel verilerin hukuka uygun işlenmesinin gereğidir. Bu kapsamda veri sahiplerinin bu konudaki talepleri için herhangi bir neden belirtme yükümlülükleri yoktur. Verilerin yanlış veya eksik olmasının ispatı yükü veri sahibindedir³²⁵.

Konuyla ilişkin olarak AİHM'nin “*Ciubotaru v. Moldova*” kararında devlet kayıtlarında Moldovalı etnik kimliğiyle kaydedilmiş olan başvuru, kendi entik

³¹⁹ Develioğlu, a.g.e, s. 90.

³²⁰ Bekir Gürses, AB ve Türk Hukukunda Kişisel Verilerin Korunması-Mevzuat Uyumuna Yönelik Bir Değerlendirme, 1. Baskı, İstanbul, Platon Hukuk, 2022, , s. 6

³²¹ M. Aydın, 2020, s. 51.

³²² Avcı, a.g.t, s. 84.

³²³ Özkan, a.g.e, s. 192.

³²⁴ GVKT, m. 16.

³²⁵ Dülger, 2019 (a), s. 154-155.

2.4.4. Silinmeyi Talep Hakkı (Unutulma Hakkı)

Kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesini düzenleyen KVKK'nın 7. maddesi uyarınca KVKK ve ya ilgili diğer kanun hükümlerine uygun bir biçimde işlenmesine rağmen işleme faaliyetini gerekli kılan sebeplerin ortadan kalkması sonucu kişisel veriler resen veya veri sahibinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hale getirilir³²⁸.

³³⁰ Kurum, Silme, Yok Etme, s. 9.

ulaşılamayacak şekilde silinebilir. Sempozyum tamamlandığında ve gerekli saklama süresinin sona ermesiyle verilerin yok edilmesi gerekecektir. Bu durumda veri sorumlusunun söz konusu taşınabilir belleği kırması veya metal öğütücüye atması yok etme işlemi olacaktır³³¹.

KVKK madde 11/f uyarınca veri sorumlusundan kişisel verilerinin silinmesini veya yok edilmesini isteyen veri sahibi bunun hem de ilgili verilerin bildirildiği üçüncü kişilerin de haberdar edilmesini isteyebilir. Bu işlem veri sahibinin menfaatleri için oldukça önemlidir. Şöyle ki, veri sorumlusu elindeki verileri yok etse, silse dahi bundan habersiz üçüncü kişiler tarafından bu veriler kullanılmaya devam edebilir³³². Örneğin gençlik döneminde paylaştığı uygunsuz fotoğraflar nedeniyle ilgili kişinin iş başvurusu reddedilebilir³³³. Bu tür durumlarla karşılaşmamak için Kanun ilgili kişiye, düzeltme veya silme taleplerinin üçüncü kişilere bildirilmesini isteme hakkını sunmuştur.

Veri sorumlusu kişisel verilerin silinmesi, yok edilmesi, anonim hale getirilmesi için gerekli her türlü teknik ve idari tedbirleri alarak veri güvenliğini sağlamakla, ve Kişisel Verileri Koruma Kurulu tarafından hazırlanmış “*Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik*”teki usul ve esaslara uymakla yükümlüdür³³⁴.

GVKT’ye göre kişisel veriler yalnızca onların işlenme amaçlarının gerektirdiği süre içinde veri sahiplerini belirleyecek biçimde tutulur³³⁵. Buna bağlı olarak GVKT madde 17 uyarınca kişisel verilerin toplanma veya işlenme amaçlarına ilişkin olarak artık gerekli olmaması, veri sahibinin işleme faaliyetinin dayandığı izni geri çekmesi ve işleme faaliyetiyle ilgili başka bir yasal gerekçe bulunmaması, veri sahibinin işleme faaliyetine itirazda bulunması ve işleme faaliyetine yönelik ağır basan meşru bir gerekçe bulunmaması, kişisel verilerin yasadışı biçimde işlenmiş olması gibi durumlarda veri sorumlusu elindeki verileri silmelidir. Ayrıca veri sorumlusu uymak zorunda olduğu yasal yükümlülüklerle uygunluğun sağlanması için verileri gecikmeksizin silmelidir. Örnek olarak tabi olduğu Birlik veya üye devlet hukukundaki bir yasal yükümlülüğe uygunluk sağlanması için kişisel verilerin

³³¹ Koç, a.g.t, s. 43.

³³² Özkan, a.g.e, s. 192.

³³³ Çekin, a.g.e, s. 96.

³³⁴ KVKK, m. 7.

³³⁵ GVKT, m. 5(1)(e).

silinmesi zorunlu olduğunda veriler herhangi bir gecikmeye mahal vermeden silinmelidir³³⁶.

GVKT’de kişisel verilerinin silinmesini yahut yok edilmesini isteme hakkı unutulma hakkı olarak da bilinmektedir³³⁷.

2.4.5. İşlemenin Sınırlandırılması Hakkı

GVKT ile veri sahibine bir takım kişisel veriler üzerindeki işleme faaliyetlerinin sınırlandırılması hakkı tanınmıştır. Veri sahibinin bu hakkı kullanması halinde veri işaretlenir ve işaretlenmiş veri üzerinde yasal iddiaların oluşturulması, veya savunulması, başka bir kişinin haklarının korunması veya kamu yararına olmaksızın, depolama dışında hiçbir işleme faaliyeti gerçekleştirilemez³³⁸.

GVKT’ye göre, aşağıdaki şartlardan biri mevcut olduğunda veri sahipleri, veri işleme faaliyetini geçici olarak kısıtlayabilir:

- veri sahibi verilerin doğru olduğuna itiraz ettiğinde veri sahibi verilerin doğruluğunu teyit edene kadar;
- veri işleme faaliyeti yasal olmadığında veri sahibi verilerin silinmesine itiraz ettiğinde ve onların kullanımını sınırlandırmasını talep ettiğinde;
- veri sorumlusunun veri işleme faaliyetinin amaçları artık işlenen veriler gerekli olmasa bile veri sahibi kendi yasal haklarını kullanmak için bu verilere ihtiyaç duyduğunda;
- veri sorumlusu kendi yasal meşru menfaatlerinin veri sahibinin yasal menfaatlerine üstün geldiğini kanıtlayana kadar veri sahibi işleme faaliyetine karşı çıktığında³³⁹.

İşleme faaliyetinin kısıtlanması çeşitli yollarla gerçekleştirilebilir. Örneğin, ilgili verilerin belirli bir süre için farklı bir sisteme aktarılmasıyla ilgili verilere ulaşım

³³⁶ GVKT, m. 17(1)(e).

³³⁷ M. Aydın, 2020, s. 52.

³³⁸ Torre Lydia F de la, “The right to restrict processing under EU data protection law”, <https://medium.com/golden-data/what-is-the-right-to-restrict-processing-under-eu-data-b6627db1319f>, E.T.: 16.04.2022

³³⁹ GVKT, m. 18(1).

engellenmiş olacaktır³⁴⁰. Veri sorumlusu uyguladığı kısıtlamaları kaldırmadan önce ilgili kişiyi haberdar etmelidir³⁴¹. Bahsettiğimiz hak KVKK'da tespit edilmemiştir.

2.4.6. Veri Taşınabilirliği Hakkı

KVKK'dan farklı olarak GVKT ile veri sahibine tanınmış olan bu hak kapsamında veri sorumlusu herhangi bir sözleşme uyarınca ya da sahibinin rızasıyla işlediği verileri veri sahibinin talebi üzerine yaygın kullanılan ve makine ile okunabilecek bir formatta ona vermelidir. Ayrıca hak veri işleme faaliyetinin otomatik yollarla gerçekleştirildiği durumlarda da kullanılabilir³⁴². Veri sahibi geri aldığı verilerini ilgili veri sorumlusunun bilgisi ya da engeli olmadan başka bir veri sorumlusuna verebilir³⁴³. GVKT'nin gerekçesine göre veri sorumluları veri taşınabilirliği hakkının kullanımını sağlamalıdır. Örneğin verilerin ilgili kişiye kolayca verilmesi için formatlar geliştirebilir³⁴⁴. Madde 29 Çalışma Grubu'nun rehberine göre, bu hak veri sahibinin seçimlerini ve kendi verilerini kontrol etme imkanını desteklemektedir³⁴⁵.

2.4.7. İşlemeye İtiraz Hakkı

Veri sahibi kişisel verileri pazarlama amaçlı işlendiğinde ya da kendi kişisel nedenleri olduğunda verilerinin işlenmesine itiraz edebilir³⁴⁶. Bu hak KVKK madde11/g ile;

“...işlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme hakkı”

şeklinde tespit edilmiştir.

³⁴⁰ Dülger, 2019(a), s. 158.

³⁴¹ GVKT, m. 18(3).

³⁴² GVKT, m. 20(1).

³⁴³ GVKT, m. 20(1).

³⁴⁴ GDPR, Recital 68, <https://www.privacy-regulation.eu/en/recital-68-GDPR.htm>, E.T.: 11.09.2022.

³⁴⁵ Article 29 Working Party, “Guidelines on the right to data portability”, 13.12. 2016, s. 13, https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf, E.T.: 29.04.2022.

³⁴⁶ Dülger, 2019 (a), s. 159.

Veri sahibinin itiraz hakkını kullanması için aynı anda iki şart mevcut olmalıdır. Bunlardan ilki, verilerin otomatik düzeneklerle analiz edilmiş olması, diğeryse bu analiz sonucu kişiyle ilgili menfi sonuçların meydana gelmesidir. Örneğin, 11. maddenin gerekçesine göre

“Bir çalışanın performansının, onun tarafından yapılan işlerin, otomatik bir sisteme işlenip analiz edilmesi sonucu çalışanın itirazı bu madde kapsamında değerlendirilecektir.”

Burada dikkat edilmesi gereken bir husus Kanun’da gösterildiği üzere *“işlenen verilerin münhasır otomatik sistemler vasıtasıyla analiz edilmesi”* hususudur. Buna göre eğer bu psikolojik değerlendirme bir yazılım sistemi dışında elle doldurulan bir anket neticesinde yapılmıştırsa, burada otomatik olmayan yöntemlerden söz edilmekte ve itiraz hakkı öngörülmecektir³⁴⁷.

GVKT ile veri sahibine tanınmış bu hak uyarınca veri sahibi onun için profil çıkarma ve yalnızca otomatik işleme faaliyetine müstenit kararlara uymayabilir. Bu kararlar veri sahibi için hukuki sonuçlar doğurabilir, ya da onu ciddi bir biçimde etkiliyor olmalıdır³⁴⁸. Yalnızca söz konusu karar veri sahibi ve veri sorumlusu arasındaki bir sözleşmenin yapılması ya da uygulanması için gerekli olduğunda, karara veri sorumlusunun da tabi olduğu ve veri sahibinin hakları ile özgürlükleri ve yasal menfaatlerinin güvence altına alınması için uygun tedbirlerin belirlendiği Birlik veya üye devlet hukukunda izin verildiğinde veya veri sahibinin açık rızası olduğunda yukardaki hükümler uygulanmaz³⁴⁹.

Veri sahibine kişisel nedenlerle işleme faaliyetine itiraz hakkının verilmesinin en önemli nedeni bireyin hakları ile diğer kişilerin yasal hakları arasında dengenin korunmasıdır. Konuya ilişkin olarak veri sorumlusunun maddi menfaatlerinin ilgili kişinin haklarına ağır basmadığını belirtmek gerekmektedir³⁵⁰.

Veri sahibi itiraz hakkını kullandığında veri sorumlusu işleme faaliyetini devam ettirmesine ancak bu faaliyetin gerekliliğini kanıtlamalıdır³⁵¹.

³⁴⁷ Avcı, a.g.t, s. 85.

³⁴⁸ GVKT, m. 22(3).

³⁴⁹ GVKT, m. 22(2).

³⁵⁰ Dülger, 2019 (a), s. 159.

³⁵¹ GVKT, m. 21(1).

ÜÇÜNCÜ BÖLÜM

3. KİŞİSEL VERİLERİN HUKUKA AYKIRI İŞLENMESİ VE BUNA KARŞI VERİ SAHİBİNİN KORUNMASI

3.1. VERİ İŞLEMENİN HUKUKA UYGUNLUK ŞARTLARI

3.1.1. Genel Olarak

Anayasa'nın 13. maddesi gereğince temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasa'nın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Aynı şekilde Anayasa'nın kişisel verilerin korunması hakkını düzenleyen 20. maddesine göre, kişisel verilerin sadece kanunda öngörülen hallerde veya kişinin açık rızası ile işlenebilir. Bu temel normlar doğrultusunda KVKK'nın ilgili maddeleri (4,5,6) değerlendirildiğinde veri sahibinin kişisel verilerinin işlenmesinin istisnai bir durum olduğu, işlemenin belirli şartlara tabi kılındığı ve belirli hukuka uygunluk şartlarının karşılandığı durumlarda mümkün olacağı görülmektedir. Kişisel verilerin işlenmesine ilişkin hukuka uygunluk şartları kanunda tahdidi bir şekilde sayılmıştır ve kişisel verilerin bunlar dışında herhangi bir sebebe dayanarak işlenmesi hukuka aykırıdır³⁵².

KVKK'da kişisel verilerin işlenmesi için özel hukuka uygunluk şartları (*lex specialis*) düzenlenmiştir. Genel hukuka uygunluk şartlarının (*lex generalis*) tespit edildiği TMK madde 24(2) ve TBK madde 63 ve 64 hükümleri kişisel verilerin işlenmesinde dikkate alınmamaktadır³⁵³. KVKK'nın 5. maddesinde genel veriler, yani özel nitelikli veriler dışındaki verilerin işlenebilmesi için geçerli olacak hukuka uygunluk şartları, 6. maddesinde ise özel verilerin işlenmesine ilişkin şartlar düzenlenmiştir. Söz konusu maddelerde düzenlenen hukuka uygunluk şartları, kanunda sınırlı sayıda (*numerus clausus*) belirlenmiştir ve bu şartların genişletilmesi mümkün değildir. Hukuka uygun işlemenin varlığının kabul edilebilmesi için,

³⁵² Özkan, a.g.e, s. 116, Çabuk, a.g.t, s. 83.

³⁵³ Yücedağ, a.g.m, s. 771.

işlemenin sadece Kanunun 5 ve 6. maddelerinde sıralanan şartlara uygun olması yeterli değildir. İşleme faaliyetinin, hem de Kanunun 4. maddesinde düzenlenen veri işleme ilkelerine de uygun olması gereklidir³⁵⁴. Öncelikle kişisel veriler hukuka ve dürüstlük kuralına uygun olarak işlenmelidir. Bu veri işleme faaliyetinin en temel ilkesidir. Ayrıca hukuka uygunluk denildiğinde yalnızca ülkede yürürlükte olan mevzuata uygunluk değil, genel olarak bütün hukuk kurallarına ve evrensel olan hukuk normlarına uygunluk anlaşılmalıdır³⁵⁵. Dürüstlük kuralına uygunluk denildiğinde ise TMK madde 2 ile düzenlenen dürüstlük kuralına uygunluk anlaşılmalıdır. İlgili maddeye göre her kes, haklarını kullanırken ve borçlarını yerine getirirken dürüstlük kuralına uymak zorundadır ve hakkın açıkça kötüye kullanılması zamanı hak sahibi hukuki korumadan mahrum kalacaktır.

3.1.2. İlgili Kişinin Açık Rızası

KVKK ile rıza kavramı tek başına tanımlanmamış, “*açık rıza*” ifadesi kullanılmıştır. Kanuna göre açık rıza, “....*belirli bir konuya ilişkin bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza*” olarak tanımlanmıştır³⁵⁶. KVKK’nın 5. maddesinde kişisel verilerin bireyin açık rızası olmadan işlenemeyeceği belirtilmiştir.

Açık rıza kanunun lafzından da anlaşılacağı üzere bazı özelliklere sahiptir. Öncelikle, açık rıza, “*belirli bir konuya ilişkin*” olmalıdır. Buna göre, açık rızanın verilmesi zamanı ilgili kişinin hangi tür kişisel verilerinin hangi şekilde işlenmesine rıza verdiğinin açıkça belirtilmesi gerekmektedir. Herhangi belirli, dar bir konu ile alakadar olmayan, genel bir niteliğe sahip rızalar Kurul tarafından “*battaniye rıza*” olarak değerlendirilmektedir³⁵⁷. Bu tip rızalar Kanun’un aradığı “*belli bir konuya ilişkin olma*” şartını sağlayamadığından hukuki geçerliliğe sahip değildir. Bu açıdan örneğin; “*bankacılık faaliyetleri için her türlü kişisel verimin gerekeceği hallerde banka tarafından işlenmesine izin veriyorum*” şeklinde verilen rıza ve bu rızaya dayalı veri işlemleri hukuka aykırı olacaktır. Ancak şunu belirtmek gerekir ki,

³⁵⁴ Tobaz Firdevs Yüzbaşı, Uluslararası İnsan Hakları Hukukunda ve Türk Hukukunda Kişisel Verilerin Korunması, Doktora Tezi, Trabzon Üniversitesi, Lisansüstü Eğitim Enstitüsü, Trabzon, 2021, s. 339-340.

³⁵⁵ Sinem Göçmen Uyarer, Kişisel Verilerin Korunması, 2. Baskı, Ankara, Seçkin Yayıncılık, 2020, s.123

³⁵⁶ KVKK, m. 3(1)(a).

³⁵⁷ Bahri Öztürk, Serkan Seyhan, Elif Altınok Çalışkan, Kişisel Verilerin Korunması Hukuku Teorik ve Pratik Çalışma Kitabı, 2.basım, Ankara, Seçkin Yayıncılık, 2022, s.68.

veri sorumlusunun kişisel veriye ilişkin gerçekleştireceği diğer işlemler ve verilerin aktarımı için ayrıca açıkça rıza alınmasına gerek yoktur³⁵⁸.

Açık rızaya dair bir diğer özellik onun “*bilgilendirmeye dayalı*” olmasıdır. Bunun için ilgili kişinin tam olarak hangi kişisel verilerinin ne şekilde veri işleme faaliyetleri için kullanılacağı konusunda bilgilendirilmesi gerekmektedir. Bilgilendirme şartının Kanun’da yer almasına karşın, ilgili kişinin hangi ölçüde bilgilendirileceğine ilişkin herhangi bir açıklama yer almamıştır. Bilgilendirme sade bir dille yapılmalı ve ilgili kişinin bu dili anlaması sağlanılmalıdır. Ayrıca, kişisel verilerin hangi amaçla işleneceği açık bir şekilde belirtilmelidir. Bununla birlikte, bilgilendirme açık rıza daha alınmadan önce yapılmak zorundadır. Açık rıza alındıktan sonra bilgilendirme yapıldığı takdirde önceden verilen rıza hukuka uygun olmayacaktır. Açık rızanın sözkonusu şartı veri sorumlusunun aydınlatma yükümlülüğü ile alakalıdır. Bu yükümlülüğünü veri sorumlusu aydınlatma metni aracılığıyla yerine getirir³⁵⁹.

Açık rızaya dair son bir şart “*özgür iradeye dayalı*” olmasıdır. Bu şartın gerçekleşmesi için ilgili kişinin veri işlemeye rıza gösterdiği durumlarda özgür iradesinin korkutma, hile ya da hata gibi durumlardan biri ile sakatlanmış olmaması gerekmektedir. Konuya ilişkin bir Kurul kararında da “*hizmetin açık rıza şartına bağlanmış olmasının açık rızayı sakatlayacağı*” ifade edilmiştir³⁶⁰. Karardan yola çıkarak günlük hayatımızda bazı internet sitelerini kullanırken hizmeti kullanmaya devam edebilmemiz için onaylamak zorunda kaldığımız veri işleme beyanları, çerezler vs.’nin açık rızanın önemli şartlarından birinin çiğnenmiş olarak alındığını söyleyebiliriz. Ayrıca açık rıza verecek kişinin ayırt etme gücüne sahip olması da gerekir³⁶¹.

³⁵⁸ Kişisel Verileri Koruma Kurumu, Açık Rıza Alırken Dikkat Edilecek Hususlar, KİŞİSEL VERİLERİ KORUMA KURUMU | KVKK | Açık Rıza Alırken Dikkat Edilecek Hususlar, E.T.: 31.08.2022

³⁵⁹ Kişisel Verileri Koruma Kurumu, Açık Rıza Rehberi, AÇIK RIZA, E.T.: 31.08.2022

³⁶⁰ Kurul Kararı, 09.07.2020, <https://www.kvkk.gov.tr/Icerik/5412/Acik-Rizinin-Hizmet-Sartina-Baglanmasi>, E.T.: 24.04.2022.

³⁶¹ Özgür iradeye dayalılık hususuna ilişkin bir kararda Kurul tarafında WhatsApp uygulamasının güncellediği yeni Hizmet Koşulları ve Gizlilik İlkesine göre verilerinin işlenmesine açık rıza vermeyen kullanıcıların uygulamayı kullanamayacağına ve hesaplarının silineceğine dair bilgilendirme iletildiği tespit edilmiştir. Söz konusu olayda açık rızanın “*özgür iradeyle açıklanması*” unsurunun zedelendiğine karar vermiştir. (Çevrimiçi Kaynak: KİŞİSEL VERİLERİ KORUMA KURUMU | KVKK | WHATSAPP UYGULAMASI HAKKINDA YÜRÜTÜLEN RESEN İNCELEMeye İLİŞKİN KAMUOYU DUYURUSU, E.T.: 25.07.2022

Açık rızanın özgür iradeyle verilmesinin önemini vurgulamak adına WhatsApp LLC hakkında verilmiş olan başka bir Kurul kararını da örnek gösterebiliriz. Özgür iradeyle açık rıza verilmesine ilişkin hususlardan biri veri işleme faaliyetine onay verme ile işleme onay vermeme süreçlerinin aynı ölçekte kolaylığı veya zorluğudur. Söz konusu hususa ilişkin kararlardan biri denetim otoritelerinden biri olan Fransız Veri Koruma Otoritesi (Commission nationale de l'informatique et des libertés - CNIL) tarafından 31.12.2021 tarihinde alınmıştır³⁶². Karara konu olan olayda Google Inc. şirketine ait olan google.fr ve youtube.com gibi internet sitelerinde çerez yönetimine ilişkin olarak kullanıcıların önüne çıkan uyarı bandında “*kabul ediyorum*” seçeneğinin yanında “*kişiselleştir*” seçeneği verilmiş, çerezleri kişiselleştirmek yani veri işleme faaliyetini onaylamamak onaylamanın aksine 5 farklı seviyede işlem yapmayı gerektirdiği için daha zor bir işlem olarak değerlendirilmiştir. Nitekim kurum vermiş olduğu kararda, açık rızanın serbestçe, belli bir amaca ilişkin olarak ve açıkça verilmiş sayılabilmesi için veri işlemeye onay verme süreciyle eş değer kolaylıkta onay vermeme imkanının da veri sahibine sunulması gerektiğini belirtmiştir. Bu bağlamda, rızaların yer aldığı ara yüzde, “*tümünü kabul et*” seçeneği bulunuyorsa, bunun yanında “*tümünü reddet*” seçeneğine de yer verilmesi önerilmektedir³⁶³. Ayrıca rızanın geri alınması ileriye yönelik bir hak olduğundan bu geri alma işlemi geçmişteki işlemler için bir etki doğurmamaktadır³⁶⁴.

KVKK’ da ilgili kişinin rızasını geri alıp alamayacağı hususu, açık bir şekilde düzenlenmemiş olsa da, 11. maddede kişiye, kişisel verilerinin silinmesini, yok edilmesini isteme hakkı tanınmıştır. Keza hem “*Kişisel Sağlık Verilerinin İşlenmesi Yönetmeliği*”³⁶⁵ hem de “*Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi Yönetmeliğinde*”³⁶⁶ kişilere rızayı geri alabilme hakkı tanınmıştır.

KVKK’da rızanın verilmesine ilişkin herhangi bir şekil şartı öngörülmemiştir. Böylece veri işleme faaliyeti için yazılı bir rıza beyanı zorunluluğu bulunmadan açık

³⁶² Kararın orjinal metni için bkz: CNIL, 31.12.2021, 2021-023, Deliberation of the restricted committee No. SAN-2021-023 of 31 December 2021 concerning GOOGLE LLC and GOOGLE IRELAND LIMITED, E.T.: 10.09.2022.

³⁶³ Data Protection Commision (DPC), Guidance note on cookies and other tracking technologies, 2020, s. 9, E.T.: 10.09.2022.

³⁶⁴ Dülger, 2019 (a), s. 116.

³⁶⁵ Kişisel Sağlık Verileri Hakkında Yönetmelik, m. 14.

³⁶⁶ Resmi Gazete, 04.12.2020, Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi Yönetmeliği”, Sayı: 28363, m. 13.

olmak kaydı ile sözlü, örneğin internet aracılığı ile net olmak kaydı ile verilen rıza beyanları geçerli sayılacaktır. Buradan çıkarılacak bir başka sonuç ise, susmanın KVKK kapsamında açık bir rıza olarak kabul edilemeyeceğidir³⁶⁷.

Açık Rızanın alınmamasında meydana gelen ihlallerle ilgili birçok sayıda Kurul Kararları vardır. Örnek olarak, Kurul 08.07.2019 tarihli kararında bir yatırım ve menkul değer şirketi tarafından, ilgili kişinin kendisine ait olan cep telefonu numarasının açık rızası olmadan işlenip, ilgili kişiye reklam ve bilgilendirme amaçlı mesajlar gönderilmesini,³⁶⁸ 31.05.2019 tarihli kararında ise bir anonim şirket tarafından ilgili kişiye açık rızası dışında elektronik ticari ileti gönderilmesini³⁶⁹ KVKK'nın ihlali olarak değerlendirmiştir.

GVKT'ye göre açık rıza,

“....veri sahibinin bir beyan veya açık bir onay eylemiyle kendisine ait kişisel verilerin işlenmesine onay verdiğini gösteren özgür bir şekilde verilmiş spesifik, bilinçli ve açık göstergedir³⁷⁰.

“Açık rıza” kavramı Tüzük'te sözcük olarak açıkça gösterilmese de, KVKK ile karşılaştırıldığında burada rıza kavramı “bilgilendirmeye dayalı bir rıza” olarak tanımlandığı için bu kavramın da alındığı için bu kavramın açık rıza olduğu aşıkardır³⁷¹.

GVKT madde 7/1 uyarınca, açık rızanın varlığında ispat yükümlülüğü veri sorumlusuna aittir. Madde 7/2 uyarınca ise eğer veri sahibi rızasını yazılı bir beyan şeklinde vermişse bu rıza diğer hususlardan açık ayırt edilebilir bir biçimde yapılmalı, anlaşılır, ve açık ve sade bir dil kullanılmalıdır³⁷².

GVKT uyarınca taraflar arasında güç dengesizliğinin mevcut olduğu şartlarda, özellikle veri sorumlusu kamu otoritesi olduğunda veri sahibi tarafınca verilen rıza açıkça geçersiz sayılmaktadır³⁷³. Veri sahibinin rızasının geçerli olması için bu rıza özgür bir şekilde verilmelidir. GVKT, madde 7/4 gereği, rızanın özgür bir iradeyle verildiği değerlendirilirken bu rızanın bir sözleşmenin gereği olup olmaması da incelenmelidir. Verilerin özgür bir şekilde verildiğinin ispatı için veri

³⁶⁷ Yüzbaşı, a.g.t, s. 343.

³⁶⁸ Kurul Kararı, 08.07.2019, <https://www.kvkk.gov.tr/Icerik/5517/2019-204>, E.T.: 24.04.2022.

³⁶⁹ Kurul Kararı, 31.05.2019, <https://www.kvkk.gov.tr/Icerik/5495/2019-162>, E.T.: 24.04.2022.

³⁷⁰ GVKT, m. 4(11).

³⁷¹ Dülger, 2019 (b), s. 22-23.

³⁷² GVKT, m. 7(2): “clearly distinguishable from the other matters, in an intelligible and easily accessible form..

³⁷³ GDPR Recital 43, <https://www.privacy-regulation.eu/en/r43.htm>, E.T.: 14.08.2022.

aktarımının rızadan başka bir yasal dayanağı olmalıdır. Ancak bu rızanın verilmesi veri sahibi için herhangi bir negatif sonuca bağlanmadığında bu rıza özgür iradeyle verilmiş sayılacaktır³⁷⁴.

Aynı şekilde, GVKT'nin 32. maddesinin gerekçesine göre rıza belirli ve tereddüde neden olmayacak açıklıkta olmalıdır³⁷⁵. Aynı gerekçeye göre açık rıza sözlü, yazılı ya da elektronik olarak verilebilir³⁷⁶. Örneğin herhangi bir internet sitesinin ziyareti sırasında kutucuğu işaretleme, ya da sessizlik yani önceden işaretlenmiş kutucuklar veya hareketsizlik rıza veya zımnen kabul olarak değerlendirilmemektedir³⁷⁷. Bunun yanı sıra veri sorumlusunun işlediği her veri için ayrı rızanın alınması gerekmektedir³⁷⁸.

Tüzük ile yapılan tanımdan da anlaşıldığı üzere, rıza “*bilinçli*” olmalıdır. KVKK'da olduğu gibi veri sahibi verilerinin işlenmesi ile ilgili rıza verirken veri işleme faaliyetine ilişkin bilgilendirilmelidir. İlk önce bu bilgilendirme açık ve anlaşılır bir şekilde yapılmalı, işlenecek veriler, işleme amaçları, verilerin aktarılabileceği kişiler, ilgili kişinin sahip olduğu haklar ve s. diğer ilgili konularda tam ve eksiksiz bilgiler içermelidir³⁷⁹.

Bunun beraberinde kişisel verilerin işlenmesi için rıza “*spesifik*”, yani konuya özel olmalıdır. Veri sahibi neye rıza verdiğini bilmelidir³⁸⁰. Dolayısıyla, veri sahibinin verilerinin işlenmesi ile ilgili verdiği genel bir rıza, GVKT'ye göre gerekli koşulları sağlamadığından hukuka uygun sayılmayacaktır³⁸¹.

Şunu da belirtelim ki, öğretide bir takım yazarlar tarafından kanundaki açık rıza kavramının sınırlarının çizilmemesi kanunun yapılma tekniği açısından eleştirilmiştir. Bizim de katıldığımız bir görüşe göre açık rıza kavramı her somut olayda farklı bir şekilde tezahür edeceğinden herhangi kazuistik sıralamaya ve bu kavramın kanunun dar sınırları içerisine alınmasına gerek yoktur³⁸².

³⁷⁴ Dülger, 2019 (a), s. 116.

³⁷⁵ Gerekçeye göre: “*Clear affirmative act establishing a freely given, specific, informed and unambiguous indication*”

³⁷⁶ Handbook, 2018, s. 112 vd.

³⁷⁷ Gerekçede bu kavramlar “*silence*”, “*pre-ticked boxes*” ve “*inactivity*” olarak geçmektedir.

³⁷⁸ Dülger, 2019 (a), s. 115.

³⁷⁹ Article 29 Working Party, Working Document on the processing of personal data relating to health in electronic health records , WP 131, Brüksel, 15 Şubat 2007, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp131_en.pdf, E.T.: 24.04.2022.

³⁸⁰ Develioğlu, a.g.e, s. 52-53.

³⁸¹ Dülger, 2019 (a), s. 115.

³⁸² Uyarer, a.g.e, s. 111.

3.1.2. Veri İşlemenin Kanunda Açıkça Öngörölmüş Olması

Kanunda veri işlemeye dair açık bir hüküm olduğu halde, ilgili kişinin rızasına gerek kalmaksızın kişisel veriler işlene bilmektedir. Burada kanun maddesinin “açıkça” ifadesinden anlaşılan maddenin geniş yorumlanamayacağıdır³⁸³. KVKK’nın gerekçesinde bu düzenlemeye örnek olarak, 2559 s. Polis Vazife ve Salahiyetleri Kanun’un 5. maddesi uyarınca şüpheliden parmak izi alınması ve 5352 sayılı Adli Sicil Kanunu uyarınca Adalet Bakanlığı’nın kişilerin ceza mahkumiyetlerine ilişkin verilerini işlemesi verilmiştir³⁸⁴. Ayrıca yürürlükteki mevzuattan işverene işçiler hakkında özlük dosyası düzenleme yükümlülüğü getiren İş Kanunu’nun 75. maddesi, kredi kartı tahsis edecek olan kuruluşlara, kredi kartı talep eden kişilerin sosyal ve ekonomik durumlarına göre, kredi kartı limiti belirleyebilmeleri için veri işleme yetkisi veren 5464 Sayılı Kredi Kartları Kanunu’nun 9. maddesi, veri işlemeye açıkça izin veren kanuni düzenlemelere örnek olarak verilebilir.

Veri işleme faaliyeti kamu yararı için ya da veri sorumlusuna verilmiş bir yetkinin ifası için yapıldığında bu faaliyet hukuka uygun olacaktır³⁸⁵. Bu hüküm gereği resmi yetkiyi veri sorumlusu kendisi bizzat kullanmasa da, bu yetkiye sahip bir üçüncü kişinin talepleri doğrultusunda hareket edilmesi de hukuka uygundur³⁸⁶.

KVKK maddde 5/2a uyarınca KVKK dışında başka kanunlarda kişisel verilerin işlenmesini serbest kılan açık düzenlemeler olursa, kişisel veriler işlenebilir. İlgili maddeye göre önemli olan, ortada veri işlemeye izin veren bir kanunun bulunmasıdır. Veri sorumlusu böyle bir durumda ilgili kişinin rızasına başvurmadan veri işleyebilecektir. Ancak burada esas olan sadece bir kanunun bulunması değil, bu kanunun ilgili kişinin rızası olmaksızın veri işlemeye açık bir biçimde izin vermesi gerekmektedir.

Aynı şekilde GVKT uyarınca veri işlemenin hukuka uygun sayılması için Birlik hukukunda ya da yerel ülke hukukunda açık ve net, öngörülebilir bir hukuki dayanağın olması gerekir³⁸⁷. Ayrıca GVKT’ye göre AB üyesi devletler kendi iç

³⁸³ Altındere, a.g.e, s.43.

³⁸⁴ “Madde ve Gerekçesi ile KVKK ve Kişisel Verilerin Korunmasına İlişkin Terimler Sözlüğü”, s. 18-19.

³⁸⁵ GVKT, m. 6(1)(e).

³⁸⁶ Develioğlu, a.g.e, s. 64.

³⁸⁷ Dölger, 2019(a), s. 118, GVKT, m. 6(3).

hukuk düzenlemelerine Tüzük'te yer alan işleme faaliyetine ilişkin kuralları uygulamak için daha spesifik hükümler getirebilirler³⁸⁸.

KVKK'da GVKT ile mükayesede bu kavram daha geniş biçimde ifade edilmiştir. Şöyle ki kanun işlemenin hukuka uygunluğu için kamu yararının varlığı gibi bir şart aramamış, bu faaliyetin kanunda açıkça öngörülmesinin yeterli olduğunu belirtmiştir³⁸⁹.

3.1.3. İlgili Kişinin veya Üçüncü Kişinin Üstün Özel Yararı

KVKK maddde 5/2b uyarınca, fiili imkansızlık nedeni ile rızasını açıklayamayacak durumda bulunan veya rızası hukuken geçerli olmayan kişinin yaşamının, beden bütünlüğünün korunması için veri işleme faaliyetinin zorunlu olduğu hallerde kişisel veriler ilgili kişinin rızası olmadan işlenebilir. Burada veri sahibinin ya da başka bir kişinin hayati çıkarlarının korunması adına veri işlemenin meşru görülmesi durumu şarttır ve kişinin rızasını açıklayabilecek durumda olsaydı, veri işlemeye rıza göstereceği varsayılmaktadır. Örneğin, bilinci yerinde olmayan bir kişinin beden bütünlüğünün korunması amacıyla tıbbi müdahale yapılması gereken durumda yakınlarına haber vermek, yetkili sağlık kurumları tarafından tutulan kayıtlar üzerinden hasta geçmişini öğrenerek gerekli müdahaleyi yapmak gibi amaçlarla kişinin adı, soyadı, kimlik numarası, telefon numarası vb. kişisel verilerinin işlenmesi bu madde kapsamında değerlendirilecektir³⁹⁰. Bir başka örnek verecek olursak, uzun zamandır kendisinden haber alınamayan ve hayatından şüphe edilen kişinin, en son bulunduğu yerdeki telefon sinyalinden, konum bilgilerinin işlenmesinde, MOBESE kayıtlarının işlenmesinde ilgili kişinin açık rızasını almaya gerek olmayacaktır³⁹¹.

Aynı şekilde GVKT hükümlerine göre veri sahibinin (bilhassa bu veri sahibi çocuksa) hak ve özgürlükleri veri sorumlusunun yasal menfaatlerine ağır basmadığı takdirde söz konusu menfaatler doğrultusunda gerekli olan işleme faaliyeti hukuka

³⁸⁸ GVKT, m. 6(2).

³⁸⁹ Develioğlu, a.g.e, s. 65.

³⁹⁰ Örneklerle Kişisel Veriler, s. 12.

³⁹¹ Altındere, a.g.e, s.44.

uygun olacaktır³⁹². Veri sahibi çocuk olduğunda çocuğun menfaati daha ağır basacağından bahsi geçen hukuka uygunluk nedeni mevcut olmayacaktır³⁹³.

GVKT'nin, 47. gerekçesine göre meşru bir menfaatin varlığı her somut olaya nazaran dikkatlice incelenmelidir. Burada eğer veri sorumlusunun meşru menfaati aşıkardır, bu menfaat ile veri sahiplerinin hak ve özgürlükleri arasında denge kurulmalıdır³⁹⁴. Veri sahibinin hak ve özgürlükleri veri sorumlusunun menfaatlerine üstün geldiği durumda veri sorumlusu veri sahiplerinin hakları üzerindeki negatif riskleri minimuma indirmelidir. Veri sorumlusu bu amaç doğrultusunda veri işlemeyi hukuka uygun kılmak adına gerekli tedbirler alabilir ve güvenceler sağlayabilir³⁹⁵.

ABAD konuya ilişkin kararlarında verilerin aktarılacağı üçüncü kişilerin menfaatlerinin varlığı ve bu menfaatler doğrultusunda veri işlemenin zorumlu olması gerektiğini, ancak sözkonusu menfaatlerin veri sahibinin hak ve özgürlüklerinden önemli olmadığını vurgulamıştır³⁹⁶. ABAD'a göre veri sahibini bekleyen zarar ve bahsi geçen menfaatler her somut olay bazında ayrı ayrı değerlendirilmelidir³⁹⁷.

Veri sorumlusu verileri “*meşru menfaatler*” gerekçesiyle işlediğinde veri sahibi özel nedenlere dayanarak işleme faaliyetine itiraz etme hakkına sahiptir. Bu durumda eğer veri sorumlusu işlemeye devam edebilmek için inandırıcı bir gerekçe ortaya koyamazsa işleme faaliyetini durdurmalıdır³⁹⁸.

GVKT madde 6(1)(d) uyarınca verilerin veri sahibinin ya da başka bir gerçek kişinin hayati yararları doğrultusunda işlenmesi hukuka uygun olacaktır. Bu hükmün kuralına göre verilerin işlenmesi için yalnızca daha önemli başka bir neden olmadığında bu duruma istinad edilebilir, yani bu hüküm kapsamında veri işleme yetkisi, ikincil niteliği haizdir³⁹⁹.

³⁹² GVKT, m. 6(1)(f).

³⁹³ Lievens Eva, Verdoodt Valerie, “Looking for needles in a haystack: Key issues affecting children's rights in the General Data Protection Regulation”, Computer Law & Security Review, 2018, <http://isiarticles.com/bundles/Article/pre/pdf/114185.pdf>, s. 275, E.T.: 20.04.2022.

³⁹⁴ Article 29 Working Party, “Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC”, 2014, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf, E.T.: 24.04.2022.

³⁹⁵ Article 29 Working Party, “Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC”.

³⁹⁶ Dülger, 2019 (a), s. 119.

³⁹⁷ CJEU, Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v. Rīgas pašvaldības SIA “Rīgas satiksme”, C-13/16, 04.05.2017, <https://curia.europa.eu/juris/document/document.jsf?text=&docid=190322&doclang=EN>, E.T.: 07.09.2022.

³⁹⁸ Dülger, 2019 (a), s. 120, GVKT, m. 21(1).

³⁹⁹ GDPR, Recital 46, <https://www.privacy-regulation.eu/en/recital-46-GDPR.htm>, E.T.: 14.08.2022

3.1.4. Sözleşmenin Kurulması ve İfası İçin Gerekli Olması

GVKT madde 6(1)(b) uyarınca veri sahibinin taraf olduğu sözleşmenin kurulması ve ya uygulanması için veri işleme faaliyetinin gerçekleştirilmesine ihtiyaç duyulduğunda bu işleme hukuka uygun olacaktır. Aynı şekilde KVKK madde 5(1)(c) uyarınca sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması şartıyla sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması halinde veri sahibinin açık rızası aranmaksızın verilerinin işlenmesi mümkündür. Bir sözleşmenin kurulabilmesi için zaten tarafların açık rızaları mevcuttur. Böyle bir durumda tarafların kişisel verilerinin işlenmesi için açık rızalarının alınması, sözleşmenin doğasına aykırı olacaktır⁴⁰⁰.

Bir sözleşmenin kurulması ya da onun ifasıyla doğrudan ilgili olması şartıyla sözleşmenin taraflarına ait kişisel verilerin işlenmesinin zorunlu olması durumunda ilgili kişilerin kişisel verilerinin yalnızca bu amaçla sınırlı olmak üzere ve bu amaca hizmet edecek şekilde işlenmesi mümkündür⁴⁰¹. Örneğin emlakçının, kira sözleşmesi ile ilgili olarak ev sahibi ve kiracı arasında imzalanan sözleşme kapsamında tarafların kimlik numarası, banka hesap numarası, adres, imza ve telefon gibi kişisel verilerini işlemesi, dosyasında muhafaza etmesi sözleşmenin kurulması için gerektiğinden hukuka uygun olacaktır⁴⁰².

Bununla birlikte veri işlemenin hukuka uygun sayılması için sözleşmenin kurulması ya da ifasının varlığı şartı aranmaktadır. Şöyle ki haksız fiil ya da sebepsiz zenginleşmeden doğan borç ilişkilerinde kişisel verilerin işlenmesi hukuka uygunluk kapsamında değerlendirilemeyecektir⁴⁰³.

3.1.5. Veri Sorumlusunun Hukuki Yükümlülüğünü Yerine Getirebilmesi İçin Zorunlu Olması

Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için veri işlenmesinin zorunlu olduğu durumlarda bu amaçla sınırlı olmak kaydıyla ilgili

⁴⁰⁰ Altındere, a.g.e, s. 44.

⁴⁰¹ Koç, a.g.t, s. 109.

⁴⁰² Örneklerle Kişisel Veriler, s. 13.

⁴⁰³ Yosif Umniyahasghar, “Kişisel Verilerin İşlenmesi Şartları ve 6698 sayılı Kişisel Verilerin Korunması Kanununun ruhu olarak Genel İlkeler”, Selçuk Üniversitesi Adalet Meslek Yüksekokulu Dergisi, Cilt 4, Sayı 1, 2021, s. 13.

kişisel verilerin işlenmesi hukuka uygundur⁴⁰⁴. Örneğin; bir işverenin 4857 sayılı İş Kanunu'nun 75. maddesi uyarınca özlük dosyası düzenleme hukuki yükümlülüğü ve 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu'a göre çalışanına ait bazı kişisel verilerini Sosyal Güvenlik Kurumu'na bildirme yükümlülüğü vardır⁴⁰⁵. İşverenin bu yükümlülük kapsamında çalışanın maaşı, banka hesap numarası, evli olup olmadığı, bakmakla yükümlü olduğu kişiler, eşinin çalışıp çalışmadığı, sosyal sigorta numarası gibi verilerini elde etmesi ve işlemesi hukuka aykırılık teşkil etmeyecektir. Ancak veri işleme faaliyeti hukuki yükümlülüğü yerine getirme amacıyla sınırlı olmalı, bu sınır herhangi diğer bir sebeple aşılmamalıdır⁴⁰⁶.

Aynı şekilde GVKT hükümleri uyarınca ister özel alandaki, ister de kamu alanındaki veri sorumluları için geçerli olan⁴⁰⁷ bu hukuka uygunluk sebebi gereği veri sorumlusu tabi olduğu yasal yükümlülüğü yerine getirmek için veri işliyorsa bu işleme hukuka uygundur⁴⁰⁸. Düzenlemede bahsi geçen hukuki yükümlülüğün hem ilgili devletin yerel hukukundan, hem de AB hukukundan kaynaklanabileceği belirtilmiştir⁴⁰⁹.

3.1.6. Kişisel Verilerin İlgili Kişi Tarafından Alenileştirilmiş Olması

Veri sahibinin kendisi tarafından alenileştirilen, bir başka ifadeyle herhangi bir şekilde kamuoyuna açıklanmış olan kişisel verilerin açık rıza istenmeksizin işlenmesi hukuka uygundur. Ancak kişisel verinin aleni kabul edilebilmesi için ait olduğu kişinin bunu gerçekten istemiş olması gerekir. Başka bir ifade ile, alenileştirmenin gerçekleştirilebilmesi için alenileştirme iradesinin varlığı gereklidir. Kişinin kişisel verisinin herkesin görebileceği bir yerde olması alenileşmiş sayılması için yeterli değildir. Bu konuda herhangi bir yasal sınırlamanın öngörülmemiş olmasına rağmen alenileşmiş kişisel verilerin de yalnızca alenileşme amacına uygun olarak işlenmesi gerekmektedir⁴¹⁰. Örneğin bir avukatın kartvizitini verdiği kişi, sadece hukuki konularda danışma gibi bir amaçla kartvizitte yer alan GSM

⁴⁰⁴ KVKK, m. 5(2)(ç).

⁴⁰⁵ Taştan, a.g.e, s. 166.

⁴⁰⁶ Altındere, a.g.e, s. 45.

⁴⁰⁷ Dülger, 2019 (a), s. 117.

⁴⁰⁸ GVKT, m. 6(1)(c).

⁴⁰⁹ GVKT, m. 6(2)

⁴¹⁰ Kişisel Verileri Koruma Kurumu, Kişisel Verilerin Korunması Hukuku Bilgilendirme Rehberi, <https://www.hku.edu.tr/wp-content/uploads/2019/04/kvkk-kitapcik.pdf>, s. 17, E.T.: 31.08.2022.

numarasını kullanabilir. Ancak söz konusu GSM numarasına reklam ve kampanya içerikli SMS gönderilmesi veya arama yapılması avukatın irade beyanına aykırı olacaktır⁴¹¹.

Ayrıca KVKK'nın lafzından da anlaşılacağı üzere⁴¹²; alenileşmiş veriler veri sahibi ilgili kişi tarafından alenileştirilmiş olmalıdır. Başkası tarafından alenileştirilen veriler bu kapsamda sayılmamaktadır⁴¹³.

Bu konuda bir örnek Fransız Kişisel Veri Koruma Otoritesi (CNIL)'nin 08.12.2020 tarihli kararına konu olmuş bir olaydan verilebilir. Karara konu olayda NESTOR isimli yemek şirketi temel olarak çalışanlara öğle yemeği hizmeti vermektedir. Müşteri ağını genişletmek için bu şirket iki farklı şirketle anlaşarak kendisi için LinkedIn üzerinden hedef kitleye yönelik bir veri tabanı oluşturmalarını ve bu veri tabanındaki kişilerin iletişim adreslerinin saptanmasını istemiştir. Bu sürecin sonunda elde edilen mail adreslerine 3 yıl içerisinde firma tarafından toplam 635.000 adet reklam maili gönderilmiştir. Bu mail adresleri kişilerin LinkedIn hesaplarına profesyonel ilişkileri için yükledikleri ve aleni nitelikteki kişisel verilerdir. CNIL kararında, bu şekilde tanıtım maillerinin gönderilmesinin meşru bir sebebe dayanması gerektiği ve bu meşru sebebin de ilgili kişilerin aydınlatılmış onama dayalı açık rızalarının alınması olduğunu belirtmiştir. Halbuki NESTOR mailleri göndermeden önce böyle bir açık rıza almamıştır. Sonuç olarak CNIL firmaya 20.000 Euro para cezası uygulamıştır. Ayrıca firma 3 ay içinde veri işleme faaliyetlerini mevzuata uygun hale getirme yönünde talimatlandırılmış, aksi durumda gün başına 500 Euro para cezası verileceği ve hukuka aykırı elde edilen kişisel verilerin imha edilmesi gerektiği belirtilmiştir⁴¹⁴.

Konuya ilişkin bir Kurul kararında ise ilgili kişi daha önce açık rızası alınmaksızın bir veri sorumlusu sigorta şirketi tarafından sigortacılık faaliyetleri için arandığı gerekçesiyle Kurul'a şikayette bulunmuştur. Sigorta şirketi ise savunmasında, ilgili kişinin bilgilerine herkese açık bir siteden eriştiğini belirtmiştir. Kurul veri sorumlusu tarafından verilerin onların alenileştirilme nedenine uygun olmayan biçimde kullandığı kanaatine gelmiştir. Başka bir deyişle veriler veri sahibinin kendisi tarafından alenileştirilse bile şirket bu verileri kullanım amacı

⁴¹¹ Örneklerle Kişisel Veriler, s. 17.

⁴¹² KVKK, m. 5(2)(d).

⁴¹³ Altındere, a.g.e, s.45.

⁴¹⁴ Kararın orjinal metni için bkz: <https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042848036>

dışında işlediği için şirkete idari yaptırım cezası uygulanmıştır⁴¹⁵. Sonuç olarak, bir kişi, kişisel verilerini kendi iradesiyle alenileştiriyor olsa bile alenileştirme o veriyi korumasız kılmaz, söz konusu veriler alenileştirme amacının dışında kullanıldığında KVKK bakımından korunmaya devam eder⁴¹⁶.

3.1.7. Kişisel Verilerin İşlenmesinin Bir Hakkın Tesisi, Kullanılması veya Korunması İçin Zorunlu Olması

GVKT ile “*veri sorumlusunun kişisel veri işlemedeki meşru menfaati*” adı altında düzenlenmiş olan bir hakkın tesisi, kullanılması veya korunması için zorunlu olması halinde ilgili kişinin kişisel verilerinin işlenmesi aynı şekilde KVKK ile bir hukuka uygunluk sebebidir⁴¹⁷. Örneğin, bir şirketin gelecekte eski çalışanları tarafından kendisine karşı açılacak davalarda ispat için bazı verileri dava zamanaşımı süresince saklaması ya da engelli bir kişinin haklarının korunması amacıyla varisinin veya kayyumun, engellinin mali bilgilerini tutması halinde açık rızaya gerek kalmayacaktır. Ayrıca sözleşme sona erdikten sonra, olası yasal takiplere karşı zamanaşımı süresinin sonuna kadar fatura sözleşme, kefaletname gibi belgelerin söz konusu amaçlar için saklanması bu kapsamda değerlendirilecektir⁴¹⁸.

İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla veri sorumlusu, meşru menfaatleri için zorunlu olan hallerde kişisel veri işleyebileceği durum KVKK kapsamında da hukuka uygunluk sebepleri arasındadır. İlgili kişinin menfaati ile veri sorumlusunun menfaati kıyaslandığında, veri sorumlusunun ilgili kişinin menfaatlerini üstün tutacak şekilde hareket etmesi gerekecektir. Aksi halde bir hukuka uygunluk sebebinden bahsedilemeyecektir.

Bu hükmün kapsamında dikkat edilmesi gereken hususlardan biri de “*hakkın kötüye kullanılması*” yasağıdır. Örneğin; ödenmemiş alacakları temlik alan bir banka tarafından borcluya bir mesaj gönderilerek borcun temlik alındığının, bu nedenle önceki alacaklılara ödeme yapılmaması hususunun hatırlatılması, söz konusu bankanın alacak hakkını koruma amacıyla gerçekleştirildiği bir veri işleme faaliyeti olduğu için açık rıza alınmasına gerek kalmadan, veri işleme bu hüküm kapsamına

⁴¹⁵ Kurul Kararı, 17.11.2019, <https://www.kvkk.gov.tr/Icerik/6623/2019-331>, E.T.: 25.04.2022.

⁴¹⁶ Koç, a.g.t, 111.

⁴¹⁷ GVKT, m. 6(f), KVKK, m. 5(2)(e).

⁴¹⁸ Koç, a.g.t, s. 112;

girecektir. Ancak bankanın aynı içerikteki mesajı ilgili kişiye farklı tarihlerde mükerrer olarak iletmesi durumunda artık hakkın kötüye kullanılması söz konusu olacaktır⁴¹⁹.

Örneğin; bir işletmenin satılması, devralınması gibi bir durumun varlığı halinde, şirketi satın alacak kişinin personelin kişisel verilerinin dahil olduğu birtakım bilgileri incelemesi meşru menfaat kapsamında değerlendirilebilir. Bir işverenin, nükleer santraldeki çalışanların güvenliğini sağlamaya yönelik iş güvenliği mekanizmalarının kurulması amacıyla çalışanların kişisel verilerini işlemesi de yine bu duruma verilebilecek bir başka örnektir⁴²⁰.

3.2. KVKK VE GPDR BAKIMINDAN KİŞİSEL VERİLERİN KORUNMASI

3.2.1. Genel Veri Koruma Tüzüğü Kapsamında Kişisel Verilerin Korunması

3.2.1.1. Denetim Otoriteleri Ve Avrupa Veri Koruma Kurulu

3.2.1.1.1. Denetim Otoritesi

GVKT'nin uygulanmasını kontrol etmek ve Birlik içinde veri korumayı denetlemek ve yeknesak bir biçimde gerçekleştirmek adına GVKT ile bir takım denetleyici ve düzenleyici kurumlar öngörülmüştür. Bu kurumlar veri koruma yetkililerinin bir parçasını oluşturmaktadır.

GVKT'nin Bağımsız Denetim Otoriteleri başlıklı Bölüm'ünde bağımsızlık kısmında, Denetim Otoritesi başlıklı 51. madde hüküm altına alınmaktadır. İlgili madde ve devamındaki maddeleri uyarınca denetim otoriteleri üye devletler içerisinde gerçek kişilerin verilerinin işlenmesine ilişkin hak ve özgürlükleri korumak ve Birlik içinde veri aktarımını kolaylaştırmak için düzenlenmiştir. 51. maddenin birinci fıkrasında, her üye devletin, işleme ile ilgili temel hakları ve özgürlükleri korumak ve kişisel verilerin Birlik içerisinde serbest akışını kolaylaştırmak için, Tüzüğün uygulanmasının gözetiminden (izleme) sorumlu olacak

⁴¹⁹ Kurul Kararı, 31.05.2019, <https://www.kvkk.gov.tr/Icerik/5494/2019-159>, E.T.:31.08.2022

⁴²⁰ Kurum, Örneklerle Kişisel Veriler, s. 17.

bir ya da daha fazla bağımsız kamu otoritesini öngörebileceği düzenlenmektedir. Buna denetim otoritesi denmektedir⁴²¹.

Tüzük uyarınca denetim otoriteleri GVKT hükümlerinin uygulanmasından da mesuldür⁴²². 51. maddenin ikinci fıkrasına göre, her denetim otoritesinden, Birlik içerisinde düzenlemenin uyumlu uygulanmasını desteklemesi beklenmektedir. Bu amacın gerçekleştirilmesi için, denetim otoritelerinin, 7. bölüme uygun olarak, birbirleriyle ve Komisyon ile iş birliği yapmaları öngörülmektedir⁴²³.

Denetim otoritelerinin kişisel verilerin korunmasına ilişkin önemi bazı ABAD kararları ile vurgulanmıştır. Örnek olarak, “*Schrems*” davasında⁴²⁴ mahkemenin geldiği kanaate göre denetim otoritelerinin bağımsızlığının garantisi kişisel verilerin işlenmesi sırasında bireylerin korunmasına ilişkin hükümlere uygunluğun izlenmesinin etkinliğini ve güvenilirliğini sağlamayı amaçlamaktadır. Bu otoriteler veri işleme faaliyetlerinden etkilenen kişi ve kuruluşların korunmasını güçlendirmek amacıyla kurulmuştur⁴²⁵. ABAD’a göre yurt dışına aktarımı uygun görülmüş olsa dahi ulusal denetim otoritesine konuyla ilgili herhangi bir şikayet bulunduğu otorite tarafından bu şikayet özenle incelenmelidir⁴²⁶.

Tüzük uyarınca her denetim otoritesi görevlerini yerine getirirken ve yetkilerini kullanırken tamamen bağımsız hareket etmelidirler⁴²⁷. Her denetim otoritesinin üyesi veya üyeleri görevlerini yerine getirirken ve yetkilerini kullanırken, doğrudan veya dolaylı dış etkilerden bağımsız hareket eder ve hiç kimseden talimat talebinde bulunmaz veya talimat almaz⁴²⁸. Denetim otoritesi üyelerinin ve çalışanlarının onlara teşekkül edecek her türlü dış etkene karşı bağımsızlığını sürdürmesi, verilerin korunmasına ilişkin kararların verilmesi sırasında objektifliğin

⁴²¹ *Supervisory authority; Autorite de controle; Aufsichtsbehörde*, European Commission (EC), “What are Data Protection Authorities (DPAs)?”, What are Data Protection Authorities (DPAs)? | European Commission, E.T.: 10.09.2022.

⁴²² GVKT, m. 51(1)

⁴²³ Turan, a.g.e., s. 213.

⁴²⁴ Benzer davalar için bkz: 1) Google Spain SL ve Google Inc. v. Agencia Espanola de Proteccion de Datos (AEPD) ve Mario Costeja Gonzalez, Grand Chamber of 13.5.2014., ECR (2014) 317, paragraf 32-41.; 2) Digital Rights Ireland Ltd. v. Minister of Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General ve Karntner Landes Regierung, Michael Seitlinger, Christof Tschohl and others, 8.4.2014, ECR (2014) I-238.

⁴²⁵ CJEU, Maximilian Schrems v. Data Protection Commissioner, C-362/14, 06.10.2022, par. 41. <https://curia.europa.eu/juris/liste.jsf?num=C-362/14>, E.T.: 02.05.2022.

⁴²⁶ Dülger, 2019 (a), s. 144-145.

⁴²⁷ GVKT, m. 52(1).

⁴²⁸ Üzeltürk H., Avrupa Birliği Genel Veri Koruma Düzenlemesi, Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, Cilt 15, Sayı 2, 2018, Sayfa: 161-179, s.170.

sağlanması için çok önemlidir⁴²⁹. Örnek olarak, ABAD tarafından “*Avrupa Komisyonu v. Avusturya*” davasında Avusturya Veri Koruma Kurumu’nun Federal İdare’yi sürekli bilgilendirme yükümlülüğü bulunduğu; bu nedenle denetim otoritesinin bağımsızlığının ihlal edildiğine karar verilmiştir⁴³⁰.

Denetim otoriteleri onlara verilen görevleriyle uyuşmayan eylemlerden uzak durmalı, görev süresince vazifelerine uymayan işlerle maddi gelir elde etme maksadı olsun veya olmasın ilgilenmemelidirler⁴³¹. 51. maddenin üçüncü fıkrasında birden çok birden otoritelerinin varlığı halinde işleyişin nasıl olacağı hakkında hükümler yer almaktadır. Buna göre birden fazla denetim otoritesinin oluşturulduğu bir üye devlette, üye devletin Avrup Veri Koruma Kurulu’nda bu otoriteleri temsil etmesi için bir denetim otoritesini ataması gerekmektedir. Ayrıca, söz konusu bu üye devletin, düzenlemenin 63. maddesinde belirtilen uyumluluk mekanizması ile ilgili kurallara diğer otoritelerin uyumunu sağlamak için bir mekanizma oluşturması gerekmektedir⁴³².

Bununla birlikte, üye devletler denetim otoritelerinin vazifelerini etkin bir biçimde gerçekleştirmesi için onları gerekli insan kaynağı, teknik ve mali kaynaklarla, binalar ve altyapıyla temin etmelidir⁴³³. Her denetim otoriteesi kendi personelini seçmeli ve kendi personaline sahip olmalıdır⁴³⁴. Ayrıca, her denetim otoritesinin bağımsızlığı için mali özgürlüğü olmalıdır. Bunun için üye devletler denetim otoritelerine ulusal ya da devlet bütçesinden yıllık bütçeler ayırmalıdır⁴³⁵.

Üye devletler denetim otoritelerin her üyesinin aşağıdaki taraflarca şeffaf bir usul vasıtasıyla tayin edilmesini sağlar:

- Parlamentoları
- Hükümetleri
- Devlet başkanları
- Üye devlet hukuku çerçevesinde atama yetkisi verilen bağımsız bir organ⁴³⁶

⁴²⁹ Dülger, 2019 (a), s. 145.

⁴³⁰ CJEU, *European Commission v. Republic of Austria*, C-614/10, 16.10.2012, Par. 59. <https://fra.europa.eu/en/caselaw-reference/cjeu-c-61410-judgment#deeplink1>, E.T.: 02.05.2022.

⁴³¹ GVKT, m. 52(3).

⁴³² Turan, a.g.e., s.213.

⁴³³ GVKT, m. 52(4).

⁴³⁴ GVKT, m. 52(5).

⁴³⁵ GVKT, m. 52(6).

⁴³⁶ GVKT, m. 53(1).

Denetim otoritelerinin görevleri 57. maddede detaylı olarak düzenlenmiştir. Burada hem koruma, hem de toplumu ve ilgili kurumları bilinçlendirme ile ilgili görevler bulunmaktadır.

GVKT 58. madde uyarınca denetim otoriteleri aşağıdaki soruşturma yetkilerine sahiptir;

- veri sorumluları ve veri sahiplerine tavsiyeler vermek;
- standart sözleşme maddeleri, bağlayıcı kurumsal kurallar veya idare. düzenlemelerini onaylamak;
- veri işleme faaliyetlerini denetlemek ve sonuçlarına bağlı olarak müdahale etmek;
- veri sorumlularının. faaliyetlerini izlemek için gerekli bilgileri talep etmek;
- veri sorumlularını kınamak;
- veri ihlali bildirimlerinin veri sahiplerine gönderilmesini sağlamak;
- verilerin düzeltilmesine, engellenmesine, silinmesine veya yok edilmesine karar vermek;
- veri işleme faaliyetlerine geçici.veya kalıcı bir sınırlama getirmek;
- herhangi bir konuyu mahkemeye taşımak.

Tüzüğe göre denetim otoriteleri düzenlemenin tutarlı bir şekilde yürütülmesi ve uygulanması için birbirlerine gerekli bilgileri ve karşılıklı desteği sağlamalı ve birbirleriyle etkili iş birliğine yönelik tedbirleri uygulamaya koymalıdır⁴³⁷. Denetim otoriteleri, uygun olduğu hallerde, ortak soruşturmalar ve ortak yaptırım tedbirleri dahil olmak üzere diğer üye devletlerin denetim otoriteleri üyeleri veya personelinin müdahil olduğu ortak çalışmalar gerçekleştirir⁴³⁸. Kural olarak, her denetim otoritesi, kendi bölgesinde yetkilerini kullanmayı yetkili olsa da, GVKT “tek durak noktası” mekanizmasını belirlemiştir. GVKT uyarınca çeşitli denetim otoriteleri arasında iş birliği yapılmalıdır ve bu kapsamda uluslararası işleme faaliyetlerinde iş birliği için bir baş denetim otoritesinin oluşturulması düzenlenmiştir⁴³⁹. Bahsettiğimiz mekanizmaya göre bir veri sorumlusu veya veri işleyen birden çok işletmesi varsa ve aynı anda birden çok üye devlette faaliyet gösteriyorsa, aynı şekilde onların faaliyetleri birden çok devletteki veri sahiplerini

⁴³⁷ GVKT, m. 61(1).

⁴³⁸ Üzeltürk, a.g.m., s. 172.

⁴³⁹ GVKT, m. 56(1).

ciddi şekilde etkiliyorsa, ana (veya tek) işletmenin denetim otoritesi sınır ötesi faaliyetleri için baş denetim otoritesi olacaktır⁴⁴⁰. Genel merkezi (yani “*merkezi yönetim yeri*”), Rotterdam, Hollanda’da bulunan, ancak çeşitli AB ülkelerinde kuruluşları bulunan bir şirketin diğer ülkelerdeki kuruluşlarıyla iletişime geçmek ve veri işlemek için aynı yazılımı kullandığı, tüketicilerin kişisel verilerinin pazarlama amacıyla işlenmesine ilişkin tüm araçların ve tüm kararların Rotterdam’daki aynı genel merkez tarafından belirlendiği bir örnekte Rotterdam’daki denetim otoritesi sınır ötesi faaliyetler için baş denetim otoritesi olacaktır⁴⁴¹. Aynı şekilde, GVKT, madde 61(2) uyarınca her denetim otoritesi diğer bir denetim otoritesinin yardım istemini talebi aldıktan sonra gecikmeksizin en geç bir ay içerisinde cevaplamalıdır.

3.2.1.1.2. Avrupa Veri Koruma Kurulu

Avrupa Veri Koruma Kurulu (AVKK), Avrupa Birliği genelinde veri koruma kurallarının tutarlı bir şekilde uygulanmasına katkıda bulunan ve AB’nin veri koruma otoriteleri arasında işbirliğini destekleyen bağımsız bir Avrupa kuruluşudur⁴⁴². Kurul, Genel Veri Koruma Tüzüğü gereğince 25 Mayıs 2018 tarihinde Tüzüğün yürürlüğe girmesi ile birlikte kurulmuştur ve merkezi Belçikanın Brüksel şehrinde yer almaktadır. Kurumun faaliyeti bağımsızlık, şeffaflık, verimlilik ve modernizasyon gibi bir takım temel ilkelere dayanmaktadır⁴⁴³.

Birlik organı olan ve tüzel kişiliği bulunan Avrupa Veri Koruma Kurulu her üye devletin bir denetim otoritesi başkanı ile Avrupa Veri Koruma Denetmeni veya bunların ilgili temsilcilerinden meydana gelir ve bağımsızdır. Komisyon Kurul’un faaliyetleri ve toplantılarına oy hakkı olmaksızın katılma hakkına sahiptir⁴⁴⁴.

Avrupa Veri Koruma Kurulu’na ilişkin hükümler GVKT’nin 68. maddesi ile düzenlenmiştir. Kurul yalnızca GVKT’nin temel kavramlarının yorumlanmasına ilişkin yönergeler yayınlamak için kurulmamıştır. Kurul hem de Birlik dışında veri işlenmesine ilişkin anlaşmazlıklar hakkında bağlayıcı kararlar alarak hükmetmek ve

⁴⁴⁰ Dülger, 2019 (a), s. 147,

⁴⁴¹ Article 29, WP, Guidelines for identifying a controller or processor’s lead supervisory authority, s. 6, <https://ec.europa.eu/newsroom/article29/items/611235/en>, E.T.: 10.09.2022.

⁴⁴² European Commission, What is the European Data Protection Board (EDPB)?, E.T.: 10.09.2021

⁴⁴³ European Data Protection Board, https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_en, E.T. 31.08.2022

⁴⁴⁴ GDPR, Recital 139, <https://www.privacy-regulation.eu/en/recital-139-GDPR.htm>, GDPR, Recital 140, <https://www.privacy-regulation.eu/en/recital-140-GDPR.htm>, E.T.: 10.09.2022

GVKT'nin Birliğe üye ülkeler içerisinde etkin ve yeksenak bir biçimde uygulanmasını sağlamak için kurulmuştur⁴⁴⁵.

Avrupa Veri Koruma Kurul'unun görevleri, GVKT'nin 64. (Kurul'un Görüşü), 65. (İhtilafların Kurul Tarafından Çözülmesi) ve 70. (Kurul'un Görevleri) maddelerinde detaylıca düzenlenmiştir. Bu görevleri “tutarlılık”, “danışma” ve “rehberlik” şeklinde üç ana başlık altında toplayabiliriz.

İlk olarak “tutarlılık” olarak adlandırılan başlık uyarınca, “tek durak noktası” mekanizmasının uyarlanması esnasında denetim otoritelerinden biri itiraz ettiğinde, denetim otoriteleri arasında hangisinin “baş denetim otoritesi” olacağı konusunda görüş birliği mevcut olmadığında, yetkili denetim otoritesi Kurul'un görüşünü talep ettiğinde, ya da bahsi geçen otorite Kurul'un görüşlerine uygun hareket etmediğinde Kurul bağlayıcı kararlar alabilir⁴⁴⁶.

Bunların yanısıra “danışmanlık” işlevini de gerçekleştiren Kurul veri korumaya ilişkin konularda Komisyon'a tavsiyeler verebilir. Ayrıca Kurul Tüzüğü'nün etkili bir biçimde uygulanmasını ve denetim otoriteleri arasında iş birliği ve bilgi ve belge akışı ve ulaşımını sağlamak amacıyla kılavuzlar, tavsiyeler ve örnek uygulamalar yayınlayarak rehberlik işlevini görmektedir⁴⁴⁷.

Kurul her üye devletten bir denetim otoritesi başkanı ve Avrupa Veri Koruma Denetmeni veya temsilcilerinden oluşmaktadır. Kurul başkan tarafından temsil edilir ve başkanlık süresi beş yıldır⁴⁴⁸. Kurul'un görevleri GVKT'nin 70. maddesinde sayılmıştır. İlgili maddeye göre Kurul'un görevleri;

- GVKT'nin doğru bir şekilde uygulanmasını sağlamak;
- Birlik içerisinde veri korumaya ilişkin konularda Komisyon'a tavsiyede bulunmak;
- verilerin kopyalarının halka açık alanlardan silinmesiyle ilgili usullere yönelik kılavuzlar yayınlamak;
- denetim otoritelerinin tutarlılık mekanizması uyarınca sunulan konulara yönelik olarak çıkardığı taslak kararlara ilişkin görüşler bildirmek;

⁴⁴⁵ Role of the EDPB, https://edpb.europa.eu/role-edpb_en, E.T.: 31.08.2022.

⁴⁴⁶ GVKT, m. 65(1-b).

⁴⁴⁷ Dülger, 2019 (a), s. 149, EDPB, Guidelines, Recommendations, Best Practices, https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_en, E.T. 10.09.2022.

⁴⁴⁸ GVKT, 68(2), EDPB, Rules of Procedure, Article 5 (2), s. 7, EUROPEAN DATA PROTECTION BOARD RULES OF PROCEDURE, E.T.: 10.09.2022

- denetim otoriteleri ve mahkemeler tarafından alınan kararlara ilişkin halkın erişebileceği bir elektronik sicil tutmaktır.

Kurul üyelerinin talebi üzerine GVKT'nin uygulanmasıyla ilgili hususları araştırmakta ve düzenlemenin tutarlı bir biçimde uygulanmasını temin etmek için tavsiyeler yayınlamaktadır. Bunun yanı sıra, Kurul ihlallerin tespit edilmesi ve veri ihlali bildiriminin yapılmasına ilişkin uygulamaları yayınlar⁴⁴⁹.

GVKT'nin 70. maddesi gereği, Kurul veri ihlalinin veri sahibinin hak ve özgürlükleri açısından risk oluşturduğu durumları açıklamakla yükümlüdür. Aynı şekilde Kurul verilerin aktarılmasına ilişkin kriterleri ve gereklilikleri tayin eder. Bununla birlikte kendi yayınladığı tüm kılavuz, tavsiye ve en iyi uygulamalara yönelik kararların uygulanmasını da yine Kurul gözetir⁴⁵⁰.

Kurul kararını, aksi kararlaştırılmadıkça, salt çoğunlukla alır. Bütün bu konulara ilişkin Birlik içerisinde, üçüncü ülkelerde ve uluslararası kuruluşlarda gerçek kişilerin korunması ile ilgili hazırladığı kılavuzlar, tavsiyeler ve en iyi uygulamaların pratikte uygulamasına ilişkin bir yıllık rapor hazırlar, bu rapor kamuoyuna açıklanır ve Avrupa Parlamentosu'na, Konsey'e ve Komisyon'a iletilir⁴⁵¹. Bununla birlikte Kurul kararlarından ABAD'a şikayet etmek mümkündür⁴⁵².

3.2.1.2. Kişisel Verilerin Korunma Yolları

GVKT'nin madde 77 ve devamı maddelerde ilgili kişinin veri işleme faaliyeti esnasında sahip olduğu haklara zarar geldiği zaman başvurabileceği yollar, zararların tazmini ve ihlalinin engellenmesi için idari, hukuki ve cezai yaptırım yolları düzenlenmiştir.

⁴⁴⁹ GVKT, m. 70(d),(f).

⁴⁵⁰ GVKT, m. 70(l).

⁴⁵¹ EDPB, Rules of Procedure, Article 35, Daha detaylı olarak bkz. GVKT m. 71-73.

⁴⁵² GDPR, Recital 143, <https://www.privacy-regulation.eu/en/recital-143-GDPR.htm>, Treaty on the Functioning of the European Union (TFEU) m. 263, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT>, E.T.: 10.09.2022.

3.2.1.2.1. İdari Başvuru Yolları

GVKT ile idari başvuru yolları olarak denetim otoritelerine şikayette bulunma ve idari para cezası konuları ele alınabilir. GVKT madde 77, 78 ve 79’da yer alan: bir denetim otoritesine şikayette bulunma hakkı, bir denetim otoritesine karşı etkili bir kanun yoluna başvuru hakkı, bir kontrolör ve işleyiciye karşı etkili bir kanun yoluna başvurma hakkı gibi önemli haklar bu kapsama dahildir.

GVKT uyarınca, her bir veri sahibi kendisine ait kişisel verilerin işlenmesi sırasında haklarının ihlal edildiğini düşündürecek haller ortaya çıkarsa, yerleşim yerinde, iş yerinin bulunduğu yerde veya ihlalin meydana geldiği yerde bulunan denetim otoritelerinden birine şikayette bulunma hakkına sahiptir⁴⁵³.

Şikayet başvurusunu almış denetim otoritesi şikayetin seyri ve sonucu ile ilgili veri sahibini bilgilendirmelidir⁴⁵⁴. Kişisel verilerinin ihlal edildiği ile ilgili şikayette bulunmuş veri sahibinin, şikayetin bildirdiği denetim otoritesi, şikayete ilişkin GVKT hükümleriyle getirilen çözüm yollarını ve yaptırımları uygulamalı, bu esnada somut olayın tüm özelliklerini bir arada değerlendirmekle karar vermelidir⁴⁵⁵. Uygulanabilecek çözüm yolları ile yaptırımların etkili, orantılı ve caydırıcı nitelikte olması, ayrıca Birlik içerisinde oluşabilecek aynı ya da benzer nitelikteki ihlallerle aynı değerde yaklaşımlar geliştirilerek uygulamada tutarlılığın sağlanması denetim otoritelerinin sorumluluğundadır⁴⁵⁶.

Denetim otoritelerinin yetkilerinin sınırlamak için GVKT’nin 78. maddesinde bu kurumların kararlarına karşı başvuru yolları belirlenmiştir. Buna göre her gerçek veya tüzel kişi denetim otoritesinin yasal bağlayıcılığı olan bir kararına karşı kanun yoluna başvurabilir. Böyle bir başvurunun yapılması veri sahibinin diğer adli ve idari yaptırım yollarına başvurma hakkına engel olmayacaktır. Denetim otoritelerinin yetkili oldukları alanlarda onlara yapılmış herhangi bir şikayet başvurusunu üç ay içerisinde araştırmaya başlamadığı ya da şikayetin seyri veya sonucu hakkında veri

⁴⁵³ GVKT, m. 77(1).

⁴⁵⁴ GVKT, m. 77(2).

⁴⁵⁵ Daha detaylı bkz. GDPR, Recital 141, <https://www.privacy-regulation.eu/en/recital-141-GDPR.htm>, E.T.: 10.09.2022.

⁴⁵⁶ Bulut Çimen İpek, “Avrupa Birliği Genel Veri Koruma Tüzüğü Kapsamında Getirilen Yeni Teknik ve Yaptırım Mekanizmaları”, Anadolu Üniversitesi Sosyal Bilimler Dergisi, Cilt 20, Sayı 2, 2020, s.135.

sahibini bilgilendirmediği durumlarda her veri sahibi diğer kanun yollarına başvurabilir⁴⁵⁷.

Veri sahiplerince denetim otoritesine karşı açılacak davalar ilgili denetim otoritesinin bulunduğu üye devletin yerel mahkemelerinde açılır⁴⁵⁸.

GVKT uyarınca veri sahibi hukuka aykırı bir işleme faaliyeti sonucu haklarının ihlal edildiğini değerlendirdiği durumda denetim otoritesine şikayette bulunma hakkının yanı sıra, mevcut idari veya adli olmayan çözüm yollarına engel olmadan, etkili bir kanun yoluna başvurma hakkına da sahiptir⁴⁵⁹. Bu kapsamda veri sahibince veri sorumlusu ya da veri işleyene karşı açılacak davalar, kişisel veri ihlalini gerçekleştiren işletmenin bulunduğu üye devletin mahkemelerinde veya veri sorumlusunun veya veri işleyenin üye devletlerden birinin kamu yetkilerinin kullanımına ilişkin hareket eden bir kamu kuruluşu olması durumunda veri sahibinin mutlak meskeninin bulunduğu üye devletin mahkemelerinde açılabilir⁴⁶⁰.

Veri sahibinin Avrupa Birliği içerisinde faaliyet gösteren herhangi bir organın, kişisel verilerin işlenmesinde hukuka aykırı davranması nedeniyle ABAD'a başvurusunun mümkünlüğünün beraberinde, veri sahibi, veri sorumlusu, veri işleyen veya denetim otoritesinin kendilerini ilgilendiren Avrupa Veri Koruma Kurulu'nun bir kararını iptal etmek amacıyla da ABAD'a başvurabilirler. Veri sahibinin kişisel verilerinin korunması hakkının ihlali gerekçesiyle yapacağı başvuru, ABAD'ın ilk derece mahkemesi olan Avrupa Birliği Genel Mahkemesi'ne yapılacaktır⁴⁶¹.

Kural olarak, şikayet yollarına ancak kişisel verilerin korunması hakkı ihlal edilmiş veri sahibi kendisi bizzat başvurabilirse de, GVKT ile şikayet başvurusunda bulunacak veri sahibinin temsil edilebilmesi de düzenlenmiştir. İlgili maddeye göre veri sahibi, bir üye devlet hukukunca kurulmuş bulunan ve veri sahiplerinin kişisel verilerinin korunmasına ilişkin hakları ve özgürlüklerinin korunması alanında aktif olan ve kar amacı gütmeyen bir kuruluşa kendi adına şikayet yapması için yetki verebilir. Yetki verilmiş organ idari başvuru yolları bakımından veri sahibine tanınmış hakları tazminat alma hakkı da dahil olmak üzere kullanma yetkisine sahip olur⁴⁶².

⁴⁵⁷ GVKT, m. 78(2).

⁴⁵⁸ GVKT, m. 78(3).

⁴⁵⁹ GVKT, m. 79(1).

⁴⁶⁰ GVKT, m. 79(2).

⁴⁶¹ Dülger, 2019 (a), s. 163.

⁴⁶² GVKT, m. 80(1).

3.2.1.2.2. İdari Para Cezası

GVKT'nin 83. maddesi uyarınca, denetim otoriteleri veri ihlali tespit ettikleri durumlarda etkili, ölçülü ve caydırıcı nitelikte idari para cezası kesebilirler. Para cezasının miktarı somut olayın özelliklerine göre değişmekte olup, denetim makamlarınca veri işleme faaliyetinin idari para cezası gerektirip gerektirmediği, verilecek para cezasının miktarına ilgili işleme faaliyetinin mahiyeti, kapsamı veya amacına dikkat edilmekle ihlalin ciddiyeti ve süresinin yanı sıra etkilenen veri sahiplerinin sayısı ve yaşadıkları zarar düzeyi dikkate alınarak belirlenmektedir⁴⁶³.

Denetim otoriteleri tarafından veri ihlaline ilişkin para cezasının miktarının belirlenmesinde ihlalin kasıtlı veya ihmalkarlık kaynaklı olup olmaması, veri sahiplerinin yaşadığı zararın azaltılması için veri sorumlusu veya veri işleyen tarafından gerçekleştirilen herhangi bir işlemin olup olmadığı, veri sorumlusu veya veri işleyenin sorumluluk derecesi veya geçmişte konuyla ilgili ihlallerinin varlığı, ihlalin onarılması ve olumsuz sonuçlarının azaltılması amacı ile denetim otoritesi ile gerçekleştirilen işbirliğinin ne düzeyde olduğu gibi hususlar göz önünde bulundurulmaktadır⁴⁶⁴.

GVKT ile getirilmiş aşağıdaki durumlarda denetim otoriteleri tarafından 20.000.000 Euro'ya kadar idari para cezaları uygulanmaktadır:

- veri işleminin temel ilkeleri ve ya rızanın koşulları ihlal edildiğinde;
- veri sahiplerinin hakları ihlal edildiğinde;
- GVKT ile belirlenmiş yurt dışına veri aktarımına ilişkin kurallara uyulmadığında;

Yalnızca veri sorumlusu veya işleyenin konuya ilişkin bir teşebbüsünün varlığında olduğunda, denetim otoriteleri bir önceki mali yılın yıllık dünya çapındaki cirosunun %4'üne kadar idari para cezası kesebilir⁴⁶⁵. Burada hangi meblağ yüksektirse o geçerli olacaktır. Diğer ihlaller için ise denetim otoritesi 10.000.000 euro'ya kadar, ya da veri sorumlusu veya işleyenin bir teşebbüs olduğunda ise bir önceki mali yılın yıllık dünya çapındaki cirosunun %2'sine kadar idari para cezası (hangi meblağ yüksek ise o geçerlidir) kesebilmektedir⁴⁶⁶.

⁴⁶³ GVKT, m. 83(2).

⁴⁶⁴ GVKT, m. 83(2).

⁴⁶⁵ GVKT, m. 83(5).

⁴⁶⁶ GVKT, m. 83(4).

Denetim otoriteleri idari para cezası kesmek yerine “*düzeltilici*” yetkilerini de kullanabilir⁴⁶⁷. Örnek olarak, ihtarda bulunma, kınama gibi tedbirler alabilir, aynı şekilde bir veri işleme yasağı verebilir ya da veri işleme faaliyeti için geçici veya net bir sınırlama getirebilir⁴⁶⁸.

Konuya ilişkin önemli bir husus, üye devletlerin GVKT ile belirlenmiş ihlallere karşı kendi iç hukukunda cezalar koyabilecek olmasıdır⁴⁶⁹. Bu noktada dikkat edilmesi gereken tek mesele yerel hukuklarda getirilen düzenlemelerle birlikte ihlalden sorumlu olan kişinin iki kere yargılanmaması, dolayısıyla “*non bis in idem*” prensibinin ihlal edilmemesidir⁴⁷⁰. Örnek olarak; Almanya Federal Veri Koruma Yasası’na göre bazı veri koruma kurallarının kasıtlı ihlali suç teşkil etmektedir⁴⁷¹.

3.2.1.2.3. Hukuki Yaptırımlar

GVKT ile belirlenen ihlallerden dolayı maddi ya da manevi zarar gören bir kişinin veri sorumlusundan ya da veri işleyenden maruz kaldığı zarardan dolayı tazminat talep etme hakkı vardır⁴⁷².

Veri işleme faaliyetine dahil olmuş herhangi bir veri sorumlusu Tüzüğün ihlaline neden olan faaliyetinden dolayı oluşan zarardan mesuldür⁴⁷³. Bir veri işleyen ise veri sorumlusunun talimatlarına ya da Tüzük ile belirlenmiş yükümlülüklerine aykırı bir biçimde davrandığı takdirde oluşan zarardan sorumlu olacaktır⁴⁷⁴.

Bununla birlikte Tüzük’te birden çok veri sorumlusu veya işleyen aynı veri işleme faaliyeti sırasında onların hareketlerinden dolayı veri sahibi zarara uğradığı takdirde veri sahibinin zararının tazmini için her birinin sorumlu olacağı düzenlenmiştir⁴⁷⁵. Ancak, böyle bir durumda, veri sorumlularından biri zararı tam tazmin ederse, işleme faaliyetine dahil olan ve diğer veri sorumluları ve veri işleyenlerden zarardan sorumlu oldukları kadarını geri alabilir⁴⁷⁶. GVKT’ye bu

⁴⁶⁷ GVKT, m. 58.

⁴⁶⁸ Dülger, 2019 (a), s. 166, GVKT, m. 58(2)

⁴⁶⁹ GVKT, m. 84(1).

⁴⁷⁰ GVKT, Gerekçe 149.

⁴⁷¹ Federal Data Protection Act, Section 42, Penal provision, https://www.gesetze-im-internet.de/englisch_bdsge/englisch_bdsge.html#p0338, E.T.: 03.05.2022.

⁴⁷² GVKT, m. 82(1).

⁴⁷³ GVKT, m. 82(1).

⁴⁷⁴ GVKT, m. 82(2).

⁴⁷⁵ GVKT, m. 82(4).

⁴⁷⁶ GVKT, m. 82(5).

hükmün getirilmesinin temel amacı veri sahibinin zararının “*tam ve eksiksiz*” olarak giderilmesini sağlamaktır⁴⁷⁷.

Ancak düzenlemede zarara neden olmuş olaylardan hiçbir şekilde sorumlu olmadıklarının kanıtlamaları durumunda veri sorumlusu veya işleyenlerin tazminat sorumluluğundan muaf olacakları belirtilmiştir⁴⁷⁸.

3.2.2. Kişisel Verilerin Korunması Kanunu Kapsamında Kişisel Verilerin Korunması

Kişisel Verilerin Korunması Kanunu ile veri sahiplerine verilerin korunması için hak arama yolları düzenlenmiştir. Bahsedilen düzenleme hem de Kişisel Verilerin Korunma Kanunu’nun uygulanmasına yönelik taleplerin giderilmesi amacı taşımaktadır. İlgili düzenlemelere göre veri sahipleri verilerin korunmasıyla ilgili konularda Kurul’a veya doğrudan mahkemeye başvurabilirler.

3.2.2.1. Veri Sorumlusuna Başvuru

KVKK madde 13 ile veri sahibinin veri sorumlusuna başvuru yapma yolunu düzenlenmiştir. Söz konusu hükme göre, ilgili kişi, Kanun’un uygulanmasıyla ilgili taleplerini yazılı bir şekilde ya da Kurul’un belirleyeceği başka yöntemlerle veri sorumlusuna iletir.

KVKK hükümlerine bakıldığında veri sahibinin veri sorumlusuna başvuru yapma şekline dair iki temel yolun belirlenmiş olduğu gözlemlenmektedir. Bunlardan ilki genel hükümlere göre ıslak imza içeren belge ile yapılan yazılı başvurudur. Veri sahibinin başvuru yapabilme imkanına dair diğer şekil ise güvenli elektronik imza ile imzalanan belgelerdir. Yazılı başvuru dışında, diğer başvuru usullerinin belirlenmesi için Kişisel Verileri Koruma Kurulu’u yetkilendirilmiştir⁴⁷⁹.

Veri sorumlusuna yapılabilecek başvuruyla ilgili diğer usul ve yöntemler Kişisel Verileri Koruma Kurulu tarafından yayınlanmış Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ’de belirtilmiştir⁴⁸⁰. Tebliğ’in “*başvuru usulü*” adlı

⁴⁷⁷ Dülger, 2019 (a), s. 164.

⁴⁷⁸ GVKT, m. 82(3).

⁴⁷⁹ KVKK, m. 13(1).

⁴⁸⁰ Resmi Gazete, 10.03.2018, Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ”, Sayı : 30356.

5. maddesinin 1. fıkrasına göre veri sahibi kendi taleplerini, yazılı olarak veya kayıtlı elektronik posta (KEP) adresi, güvenli elektronik imza, mobil imza ile ya da, kendisi tarafından veri sorumlusuna daha önceden bildirilmiş ve veri sorumlusunun sisteminde mevcut olan elektronik posta adresini kullanarak veya başvuru amacına yönelik geliştirilmiş bir yazılım ya da uygulama aracılığıyla veri sorumlusuna iletir. Uygulamada veri sorumlularının internet sitelerinde, ilgili kişilerin kendilerine başvuru yapılmasına yönelik formlar bulundurdıkları sıklıkla görülmektedir⁴⁸¹.

Tebliğ'in 5. maddesinin 2. fıkrasına göre ise başvuruda bulunması zorunlu olan bilgiler ilgili kişinin adı, soyadı, başvuru yazılı ise imzası, T.C vatandaşları için T.C kimlik numarası, yabancılar içinse ilgili kişinin uyruğu, pasaport numarası veya varsa kimlik numarası, tebligata esas yerleşim yeri veya işyeri adresi, varsa bildirimde esas elektronik posta adresi, telefon veya faks numarası ve talep konusudur. Konuya ilişkin bilgi ve belgeler başvuruya eklenerek başvuru tamamlanır. Bu başvurular türkçe olarak yapılmalıdır⁴⁸². Bununla beraber, yapılabilecek ihbar ve şikayetler *"Dilekçe Hakkının Kullanılmasına Dair Kanun"*un 6. maddesinde belirtilen şartlara uygun olmalıdır⁴⁸³.

Veri sorumlusu, ilgili kişi tarafından yapılan başvuruları etkin, hukuka ve dürüstlük kuralına uygun şekilde sonuçlandırmak için gereken her türlü teknik ve idari tedbirleri almakla yükümlü kılınmıştır ve o kendisine yapılan bu doğrultudaki tüm başvuruları kabuleder veya gerekçesini açıklayarak reddeder. Red kararının gerekçeli olması zorunluluğunun konulmasıyla birlikte veri sorumlusuna yapılan başvuruların keyfi olarak reddinin önüne geçilebileceği düşünülmektedir⁴⁸⁴.

Kural olarak veri sorumlusu başvuruya cevabı ilgili kişiye yazılı bir şekilde veya elektronik ortamda bildirir ve başvuruda yer alan talepleri talebin niteliğine uygun olarak en kısa sürede ve en geç otuz iş günü içinde ücretsiz olarak sonuçlandırır. Talebin gerçekleştirilmesi ayrıca bir maliyet gerektirirse veri sorumlusu ilgili kişiden ücret talep edebilir⁴⁸⁵. Tebliğ'in 7. maddesi uyarınca, ilgili kişinin başvurusuna yazılı bir şekilde cevap verilecekse, on sayfaya kadar ücret alınmaz. On sayfanın üzerindeki cevaplar içinse sayfa başına 1 (bir) Türk Lirası işlem ücreti veri sorumlularınca talep edilebilir. Cevap CD, harici bellek gibi bir

⁴⁸¹ Çabuk, a.g.t, s. 119.

⁴⁸² Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ, m. 4.

⁴⁸³ Resmi Gazete, 10.11.1984, 3071 Sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun, Sayı 18571.

⁴⁸⁴ Çabuk, a.g.t, s. 119.

⁴⁸⁵ KVKK, m. 13(2).

kayıt ortamında verildiği halde ise, talep edilebilecek ücret kayıt ortamının maliyetini geçmemelidir. Başvuru veri sorumlusunun hatalarından kaynaklandığı takdirde alınan ücret veri sahibine iade edilmelidir⁴⁸⁶.

3.2.2.2. Kurula Şikayet

KVKK 14. maddeye göre veri sahibinin başvurusunun reddedilmesi, verilen cevabın yetersiz bulunması veya başvuruya süresinde cevap verilmemesi durumlarında veri sahibi cevabı öğrendiği tarihten itibaren otuz, ancak her bir halde başvuru tarihinden itibaren altmış gün içinde Kurul'a şikayette bulunabilir. Öncelikle, veri sahibinin başvurabileceği veri koruma makamları için kanunla aşamalı bir mekanizma belirlenmiştir. Veri sahibi veri sorumlusuna başvuru yolunu tüketmeden şikayet yoluna başvuramaz. Buna ek olarak, kişilik hakları ihlal edilen kişiler genel hükümlere göre tazminat haklarının saklı olmalarından dolayı, veri sahiplerinin, yargı organlarına başvurabilmesi için veri sorumlusuna başvuruda bulunması zorunluluğu olmayıp, bu zorunluluk yalnızca Kurul'a şikayette bulunabilmenin ön şartı olarak görülmektedir.

Kurula yapılan şikayete ilişkin olarak Kurul tarafından yapılacak olan incelemenin usul ve esasları, KVKK madde 15 kapsamında belirlenmiştir. İlgili maddeye göre Kurul, şikayet üzerine veya ihlal iddiasını öğrenmesi halinde kanunen, görev alanına giren konularda gerekli incelemeyi yapar. Bu sırada, inceleme kapsamında veri sorumlularından bir takım bilgi ve belgeleri isteyebilir ve böyle bir durumda veri sorumluları, devlet sırrı niteliğindeki bilgi ve belgeler hariç,, Kurul'un istemiş olduğu bilgi ve belgeleri on beş gün içinde Kurul'a göndermeli ve eğer gerekiyorsa yerinde inceleme yapılmasına imkan sağlamalıdır⁴⁸⁷. Kurul, şikayet üzerine olan talepleri inceleyerek ilgililere cevap verir ve eğer şikayetin verilme tarihinden itibaren altmış gün içerisinde ona cevap verilmezse talep reddedilmiş sayılır⁴⁸⁸. Şikayetle ilgi veya re'sen yapılan incelemenin sonucunda, ihlalin varlığının anlaşılması halinde Kurul, tespit ettiği hukuka aykırılıkların veri sorumlusu tarafından giderilmesine karar vererek, kararı ilgililere tebliğ eder. Bu karar, veri

⁴⁸⁶ KVKK, m. 13(3), Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ, m. 6.

⁴⁸⁷ Cemal Başar, Kişisel Verilerin Korunması Bakımından Kişisel Verileri Koruma Kurul'na Yapılan Şikayet Başvurusu, Fasikül Hukuk Dergisi, Cilt 12, Sayı 125, 2020, s. 27-28.

⁴⁸⁸ KVKK, 15(4).

sorumlusu tarafından, kendisine tebliğden itibaren gecikmeksizin ve en geç otuz gün içinde yerine getirilmelidir⁴⁸⁹.

KVKK madde 18 uyarınca, Kurul kararının veri sorumlusu tarafından yerine getirilmemesi durumunda, veri sorumlusu hakkında 25.000 TL'den 1.000.000 TL'ye kadar idari para cezasına hükmedilir.

İnceleme sonucunda, ihlalin yaygın olması tespit edilirse, Kurul, bu konuda emsal niteliğinde bir ilke kararı alır ve bu kararı yayımlar. Kurul ilke kararı almadan önce eğer ihtiyaç duyarsa ilgili kurum ve kuruluşların görüşlerini alabilir. Buna ek olarak, telafisi güç veya imkansız zararların doğması ve açıkça hukuka aykırılığın varlığı durumunda, Kurul, kişisel verilerin işlenmesinin veya yurt dışına veri aktarımının durdurulmasına karar verebilir⁴⁹⁰. Kişisel Verilerin Korunması Kanunu'na İlişkin Uygulama Rehberi'nde, Kurul'un bu yetkisinin yargı organlarındaki ihtiyati tedbir kurumuna benzediği ve bu şekilde olası hak ihlalleri ile zararların hızlıca önüne geçilebilmesinin mümkün olacağı belirtilmiştir⁴⁹¹.

3.2.2.3. İdari Yaptırımlar

KVKK'nın "*Kabahatler*" başlıklı 18. maddesi uyarınca KVKK madde 10 kapsamında öngörülen aydınlatma yükümlülüğünü yerine getirmeyen veri sorumluları hakkında, 5.000 TL'den 100.000 TL'ye kadar, madde 12 kapsamında öngörülen veri güvenliğine ilişkin yükümlülüklerini yerine getirmeyen veri sorumluları hakkında 15.000 TL'den 1.000.000 TL'ye kadar, madde 15 kapsamında öngörülen Kurul kararlarını yerine getirmeyen veri sorumluları hakkında, 25.000 TL'den 1.000.000 TL'ye kadar, madde 16 kapsamında öngörülen Veri Sorumluları Sicili'ne kayıt ve bildirim yükümlülüğüne aykırı hareket eden veri sorumluları hakkında, 20.000 TL'den 1.000.000 TL'ye kadar Kurul tarafından idari para cezasına hükmedilmesi öngörülmüştür.

Yukarıda tespit edilmiş idari para cezaları veri sorumlusu olan gerçek kişiler ile özel hukuk tüzel kişileri bakımından uygulanır. Bu idari para cezalarına karşı idari yargı yolu açıktır. Ancak maddenin 3. fıkrasına göre, aynı maddede sayılan

⁴⁸⁹ KVKK, m. 15(5).

⁴⁹⁰ KVKK m. 15.

⁴⁹¹ Kişisel Verilerin Korunma Kurumu, Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi, Ankara, 2019, s. 108, <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/41784a70-2bac-4e4a-830f-35c628468646.PDF>, E.T.: 04.05.2022.

eylemler kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları tarafınca yapıldığı durumda Kurul'un bildirimi üzerine, ilgili kamu kurum ve kuruluşunda görev yapan memurlar ve diğer kamu görevlileri ile kamu kurumu niteliğindeki meslek kuruluşlarında görev yapanlar hakkında disiplin hükümleri gereği göre işlem yapılır ve sonuç Kurul'a bildirilir.

3.3. TÜRK MEDENİ KANUNU IŞIĞINDA KİŞİSEL VERİLERİN KORUNMASI

3.3.1. Genel Olarak

Kişisel veriler “*çağdaş ekonominin hammaddesi*” olarak ifade edilmektedir. Buna bağlı olarak verilerin önemini anlayan birçok şirkette büyük miktarlarda veri toplanmış, veri bankaları oluşturulmuştur. Söz konusu veri bankaları gelir elde etme fonksiyonu yerine getirmektedir⁴⁹². Günümüzde hayatımızın her alanında veri işleme faaliyeti büyümektedir ve bunun sonucunda kişiler kendilerine ait verilerin nerede veya hangi ölçüde işlendiğini, ya da kimlere aktarıldığını ve kimlerin bu verilere eriştiğini bilemez hale gelmiştir. Kişisel verilerin işlenmesi hususunun ve buna ilişkin diğer konuların bu kadar gündemde olması konuya ilişkin kanuni düzenlemelere olan ihtiyacı beraberinde getirmiştir. Bu bakımdan kişisel verilerin etkin bir şekilde korunmasında yalnızca KVKK ile yetinilmemiş, Anayasa Hukuku, İdare Hukuku, Ceza Hukuku, Medeni Hukuk, Borçlar Hukuku ve İş Hukuku gibi birçok hukuk alanındaki mevcut hukuki düzenlemeler ile kişisel veriler kümülatif bir hukuki koruma kapsamına alınmıştır.

Her şeyden önce kişisel verilerin korunması hakkı anayasal bir haktır. Daha önce de belirtildiği üzere⁴⁹³ 2010 yılında 5982 sayılı kanunla Anayasa'da yapılan değişiklikle birlikte kişisel verilerin korunması özel hayatın gizliliği ve korunmasıyla doğrudan ilişkili ve bu hakkın parçası olarak Anayasal hukuki koruma rejimine dahil edilmiştir⁴⁹⁴. Bundan dolayı kişinin kişisel verilerine karşı saldırıların TMK madde 24 ve 25 hükümlerine dayanarak dava yoluyla korunması mümkündür⁴⁹⁵.

⁴⁹² Aksoy, a.g.e, s. 77-78

⁴⁹³ 1.1.2-ci paragraf, “*Ulusal Düzenlemeler*”, s. 25-27.

⁴⁹⁴ Zeybek Ünsal Çağrı, “Google’ın Yeni Gizlilik Politikası Google Inc. Tarafından 1 Mart 2012 Tarihinde Yayınlanan Politikasının Kişisel Verilerin Korunması ile Uyumluluğu ve Avrupa Birliğinin

KVKK madde 11/1/ğ uyarınca kişi uğradığı zararın tazminini talep edebilir. Aynı şekilde KVKK m. 14/3'e göre *“Kişilik hakları ihlal edilenler, genel hükümlere göre tazminat hakkına sahiptir.”* Burada bahsedilen *“genel hükümler”* TMK ve TBK ile kişilik hakkına ilişkin mevcut düzenlenmelerdir⁴⁹⁶.

Bu bağlamda TMK madde 23 kişiliği hukuki işlemlerle, yani ilgili kişinin rızasıyla gerçekleştirilen saldırılara karşı korurken, TMK madde 24 ise kişiliği hukuka aykırı fiillerle, dolayısıyla kişinin rızası dışında gerçekleştirilen saldırılara karşı korumaktadır⁴⁹⁷. Yine aynı şekilde, TMK madde 25 ile kişilik hakkına karşı hukuka aykırı fiillerin mevcut olması durumunda başvurulabilecek hukuki yollar hüküm altına alınmıştır⁴⁹⁸.

TMK madde 23'e göre; *“Kimse, hak ve fiil ehliyetlerinden kısmen de olsa vazgeçemez. Kimse özgürlüklerinden vazgeçemez veya onları hukuka ya da ahlaka aykırı olarak sınırlayamaz.”* TMK madde 23 ile ilgili kişinin rızası kapsamında onun hakkında işlem yapılmasına izin verse de kişiliği koruyan bir hüküm getirilmiştir⁴⁹⁹. Bu hükmün belirlenme nedeni zayıf tarafın haklarının sınırlandırılmasını engellemektir. Hak-fiil ehliyetini ve özgürlüklerini sınırlandıran sözleşmeler geçerli olsa da, bu sözleşmeler TBK madde 27 ile belirlenmiş koşullara aykırı olmamalıdır. Örnek olarak, kişinin özel hayatına dair bilgilerin paylaşımına dair bir sözleşme kurulabilir. Ancak bu sözleşme bahsi geçen koşullara uygun olmalıdır⁵⁰⁰.

Bir sözleşmenin içeriği TBK madde 26 gereğince, taraflarca kanunla öngörülen sınırlar dahilinde belirlenebilir. Bu maddeden anlaşılabileceği gibi bir sözleşmenin içeriğini kişisel veriler oluşturabilir. İlgili maddede öngörülmüş sözleşme özgürlüğünün sınırlarını TMK madde 23 ve TBK madde 27 oluşturmaktadır. TMK madde 23 ile kişilik hakkının korunması adına sözleşme özgürlüğü kısıtlanırken⁵⁰¹, TBK madde 27 ile kanunun emredici hükümlerine, ahlaka, kamu düzenine, kişilik

95/46/EC Sayılı Veri Koruma Direktifi Açısından Değerlendirilmesi”, Hacettepe Üniversitesi Hukuk Fakültesi Dergisi, Cilt 3, Sayı 1, s.102.

⁴⁹⁵ Sefer Oğuz, “Kişisel Verilerin Korunması Hukukunun Genel İlkeleri”, Bilgi ve Ekonomi Yönetimi Dergisi, Cilt 13, Sayı 2, 2018, s.123.

⁴⁹⁶ Gürpınar, a.g.m., s. 689.

⁴⁹⁷ Mustafa Dural, Tufan Öğüz, Türk Özel Hukuku, Kişiler Hukuku, 20. Baskı, İstanbul, Filiz Kitabevi, 2019, s. 148; Helvacı, 2021, s. 139.

⁴⁹⁸ Özkan, a.g.e, s. 217.

⁴⁹⁹ Özkan, a.g.e, s. 217.

⁵⁰⁰ Ahmet M. Kılıçoğlu, Borçlar Hukuku Genel Hükümler, Genişletilmiş 23. Bası, Ankara, Turhan Kitabevi, 2019, s. 142.

⁵⁰¹ Serozan, 2017, s. 457.

haklarına aykırı veya konusu imkansız olan sözleşmeler kesin olarak hükümsüz sayılmıştır. Görüldüğü üzere “*kişilik hakkına aykırı sözleşmelerin*” hükümsüz kanunda olacağı açıkça tespit edilmiştir⁵⁰².

Hakları saldırıya uğramış bir kişi TMK madde 24/1’e göre hakimden mevzubahis saldırılara karşı korunmasını isteme hakkına sahiptir. Burada esas olan öncelikle kişilik hakkına hakikaten bir saldırının vuku bulup bulmaması ve ayrıca bu saldırının hukuka aykırı olup olmamasıdır⁵⁰³. Dolayısıyla, kişisel verilerin korunması hakkının ihlaline ilişkin başvuru yapılması durumunda ilk olarak hakim “*kimliği belirli veya belirlenebilir gerçek kişiye ilişkin bir bilgi*” yani kişisel veri olup olmadığı tespitini yapacak, sonra ise söz konusu kişisel veriye karşı hukuka aykırı saldırının mevcutluğunu değerlendirecektir⁵⁰⁴. TMK uyarınca kişilik hakkı zedelenen kişinin rızası, daha üstün nitelikte özel veya kamusal yarar ya da kanunun verdiği yetkinin kullanılması nedenlerinden biriyle haklı kılınmadıkça, kişilik haklarına yapılan her saldırı hukuka aykırı sayılmıştır⁵⁰⁵.

Kanunun lafzından anlaşıldığı üzere kişilik haklarına dolayısıyla kişisel verilerin korunması hakkına ilişkin saldırılar hukuka aykırıdır. Yalnızca hukuka uygunluk sebeplerinin bulunması halinde kişilik haklarına ilişkin müdahaleler hukuka aykırı sayılmayacaktır⁵⁰⁶. Kişisel verilerle ilişkin konularda hukuka uygunluk şartlarının sağlanması halinde veri işleme hukuka uygun olacaktır. Örneğin, verilerin işlenmesi için ilgili kişinin rızasının alınması durumunda rıza hukuka ve ahlaka uygun olarak alınmışsa hukuka uygun olacaktır⁵⁰⁷. Hukuka aykırı rızanın yalnızca tazminat indiriminde gözönünde bulundurulması mümkündür⁵⁰⁸.

Veri işlemenin hukuka uygunluk nedenleri önceki bölümlerde anlatıldığı üzere KVKK 5 ve 6. maddelerde düzenlenmiştir. veri işleme faaliyeti bu nedenlere uygun yapıldığı sürece TMK madde 25 ile düzenlenen davalar açılması gerekmemektedir⁵⁰⁹. TMK hükümlerine göre hukuka uygunluk nedenleri “*kişilik*

⁵⁰² Kılıçoğlu, 2019 (a), s. 141.

⁵⁰³ Dural/Öğüz, s. 148.

⁵⁰⁴ Özkan, a.g.e, s. 220.

⁵⁰⁵ TMK, m. 24/2.

⁵⁰⁶ Erhan Günay, Kişilik Haklarına Saldırıdan Kaynaklanan Tazminat Davaları, Güncellenmiş 2. Baskı, Ankara, Seçkin Yayınevi, 2017, s. 86.

⁵⁰⁷ Özkan, a.g.e, s. 221.

⁵⁰⁸ Helvacı, 2021, s. 103-104.

⁵⁰⁹ Özkan, a.g.e, s. 222.

hakkı zedelenen kimsenin rızası”, “daha üstün nitelikte özel yarar”, “kamusal yarar” ve “kanunun verdiği yetkinin kullanılması” olarak belirlenmiştir⁵¹⁰.

KVKK TMK’ya göre özel nitelikli (*lex specialis*) olduğundan veri işleme konusunda hukuka uygunluk nedenleri ilk olarak KVKK hükümlerince aranacaktır. Ancak bundan sonra TMK hükümlerine bakılacak ve bu hükümler niteliğine uygun düştüğü ölçüde uygulanacaktır⁵¹¹.

3.3.2. Kişisel Verilerin Hukuka Aykırı Olarak İşlenmesi Halinde Açılabilir Davalar

3.3.2.1. Önleme Davası

Kişisel verilerin korunması hakkına yönelik saldırılara karşı açılabilir davalardan biri önleme davasıdır. Bu dava TMK madde 25’te kişilik haklarını koruyucu davalar içerisinde yer almaktadır. Bu dava türü öncelikle saldırının önlenmesini amaçlamaktadır⁵¹². Önleme davası bir takım eylem ve belirtiler olduğu halde ve yakın bir gelecekte kişilik hakkına karşı “*ciddi ve yakın bir saldırı tehlikesi*”nin bulunduğu durumlarda tehlike henüz mevcut olmasa bile açılabilir⁵¹³. Haklara yönelik herhangi bir saldırı tehlikesinin bulunması davanın açılabilmesi için yeterli değildir, davanın açılabilmesi için saldırının gerçekleşeceği yönünde ciddi bir tehdit mevcut olmalıdır⁵¹⁴. Önleme davası sonucu verilen karar geleceğe etkili olarak hüküm doğurur⁵¹⁵.

Saldırı tehlikesinin önlenmesi amacıyla dava açabilmek için, saldırı tehlikesi yaratan kişinin kusurlu olması değil, davalının fiilinin hukuka aykırı nitelikte olması gerekmektedir⁵¹⁶. İlaveten, dava açma hakkı devredilemez ve miras yoluyla intikal

⁵¹⁰ TMK, 24/2.

⁵¹¹ Taştan, a.g.e, s. 150.

⁵¹² Ahmet Kılıçoğlu, Medeni Hukuk, 3.basım, Ankara, Seçkin Yayıncılık, 2019, s.326.

⁵¹³ Dural/Öğüz, a.g.e, s. 153, Serozan, 2017, s. 476, Hüseyin Hatemi, Kişiler Hukuku, 9. Baskı, İstanbul On İki Levha Yayıncılık, 2017, s. 75.

⁵¹⁴ Çabuk, a.g.t, s. 125.

⁵¹⁵ Jale Akipek/ Turgut Akıntürk/ Derya Ateş, Türk Medeni Hukuku Başlangıç Hükümleri Kişiler Hukuku, 15.basım, İstanbul, Beta Basım, 2019, s.399.

⁵¹⁶ Dural/Öğüz, a.g.e, s. 154.

edemez⁵¹⁷. Bu dava kapsamında hakimden davalının saldırı teşkil eden davranışlarından kaçınmaya mahkum edilmesi talep edilir⁵¹⁸.

Dava sonucunda verilen karar, geleceğe yönelik olup, kişisel verilerin korunması hakkına ilişkin gerçekleşmesi muhtemel olan bir saldırının engellenmesine yönelik olmalıdır⁵¹⁹. Önleme davası konuya ilişkin açılacak diğer davalardan farklı olarak, saldırı sonuçlarını değil, saldırı fiilini esas alan bir davadır⁵²⁰. Bu dava türünün kişisel verilerin korunması alanında önleyici bir koruma türü olmasının yanı sıra veri koruma alanında sınırlı bir uygulama alanı bulacağı söylenebilir⁵²¹.

3.3.2.2. Durdurma Davası

Kişisel verilerin korunması konusunda açılacak bir diğer dava durdurma davasıdır. TMK madde 25'e göre; "*Davacı, hakimden... sürmekte olan saldırıya son vermesini*" isteyebilecektir. Bu dava ilgili kişinin haklarına yönelik herhangi saldırının bulunması durumunda ilgili kişi tarafından saldırıya son verilmesi ya da saldırının tekrar edilmesine karşı tedbir almak amacıyla açılır⁵²². Önleme davasında olduğu gibi bu davada da davacının mahkeme yoluna başvurması için davalının kusurlu olması şartı aranmamaktadır. Burada önemli olan hukuka aykırı ve halen devam eden bir saldırının mevcut olmasıdır. Örneğin, dağıtımdaki bir kitapta kişisel verilerin hukuka aykırı olarak işlenmesi durumunda durdurma davasının açılması mümkün olacaktır⁵²³. Durdurma davasında hukuka aykırılığın durdurulması mümkün olmalı ve durdurma için bir hukuki yararın bulanması gereklidir⁵²⁴. Saldırının sona erdiği fakat etkilerinin devam ettiği durumda durdurma değil, tespit davası açılacaktır⁵²⁵.

⁵¹⁷ Onur Baskın, Kişilik Hakkı Kapsamında Kişisel Verilerin Korunması, 1.basım., Ankara, Seçkin Yayıncılık, 2021, s.127.

⁵¹⁸ Çabuk, a.g.t, s. 125.

⁵¹⁹ Çabuk, a.g.t, s. 125.

⁵²⁰ Develioğlu, a.g.e, s. 132.

⁵²¹ Baskın, a.g.e, s. 217, Küzeci, a.g.e, s. 315.

⁵²² Dural/Ögüz, a.g.e, s. 152; Akipek/Akıntürk/Ateş, 2019, a.g.e, s. 397; Kılıçoğlu, 2019 (b), a.g.e., s.336.

⁵²³ Helvacı, 2001 (b), s. 130.

⁵²⁴ Hayrunnisa Özdemir, Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması, 1.basım, Ankara, Seçkin Yayıncılık, 2009, s.193-195, Kılıçoğlu, 2019 (b), s. 340-343.

⁵²⁵ Dural/Ögüz, a.g.e, s. 152

Kişisel veriler hukuka, ahlaka ve dürüstlük kuralına uygun olmayan bir biçimde işlendiği durumlarda hukuka aykırı bir saldırının mevcudluğu esasıyla durdurma davası açılabilir. Yalnızca kişisel verilerin işlenmesi değil, verilerin elde edilmesi de hukuka aykırı olabilir. Örnek olarak, kişinin onayı olmadığı halde telefonuna reklam amaçlı bilgilendirme mesajları gönderilmesi ya da bu konudaki rızasını geri alan kişiye hala mesaj gelmeye devam etmesi halinde durdurma davası açılabilir. Bu dava kapsamında, kişisel verilerin yok edilmesi ya da internette yer alan bilgilerin/gönderilerin silinmesi mümkündür⁵²⁶.

Durdurma davası sonucunda, hakim kişilik hakkına yönelen hukuka aykırılık şartları varsa hukuka aykırı veri işlemenin durdurulmasına karar verecektir. Ayrıca bu dava sonunda verilen karar, İcra İflas Kanunu madde 30 ve madde 343 hükümleri gereği icrai bir niteliğe sahip olacaktır⁵²⁷.

3.3.2.3. Tespit Davası

Hukuk Muhakemeleri Kanunu'nun 106. maddesi uyarınca tespit davası mahkemeden, bir hakkın veya hukuki ilişkinin varlığının ya da yokluğunun yahut bir belgenin sahte olup olmadığının belirlenmesinin talep edildiği dava türüdür⁵²⁸. Tespit davasının amacı hakların ihlaline yönelik hukuka aykırı bir saldırının varlığı durumunda bu saldırının mahkeme kararıyla tespit ettirilmesidir. Bu tür davaların konusu maddi olaylar değil, hukuki ilişkilerdir⁵²⁹. Tespit davası önleme ve durdurma davalarını tamamlayan bir dava türüdür⁵³⁰. Bu davanın sonucunda verilen tespit kararı sadece dava konusu durumu ortaya koyar ve daha sonra çıkacak uyuşmazlıklarla ilgili olarak kesin delil niteliğinde olur⁵³¹. Tespit davasının açılabilmesi için davalının kusuru aranmaz ve aynı şekilde bir zararın meydana gelmesi beklenmez⁵³². TMK m. 25/1 uyarınca;

⁵²⁶ Serozan, 2017, s. 476.

⁵²⁷ Kılıçoğlu, 2019 (b), s. 336, Baskın, a.g.e, s. 130.

⁵²⁸ Resmi Gazete, 12.01.2011, Hukuk Muhakemeleri Kanunu, Sayı 27836.

⁵²⁹ Kılıçoğlu, 2019 (b), s. 315-316.

⁵³⁰ Helvacı, 2021, s.162.

⁵³¹ Kemal Öguzman, Nami Barlas, Medeni Hukuk, 25.bs, İstanbul, On İki Levha Yayıncılık, 2019, s.332.

⁵³² Bilge Öztan, Şahsın Hukuku, 1. Basım, Ankara, Turhan Kitabevi, 1987, s. 135, Dural/Ögüz, a.g.e, s. 154.

Davacı, hakimden saldırı tehlikesinin önlenmesini, sürmekte olan saldırıya son verilmesini, sona ermiş olsa bile devam eden saldırının hukuka aykırılığının tespiti isteyebilir.”

Dava sonucunda verilecek karar hukuka aykırılığın tespitine yönelik olacaktır. Dolayısıyla, kişisel verilerin korunması hakkına saldırı hallerinde, diğer davaların açılmadığı durumlarda tespit davasına başvurulabilir. Zira durdurma davası veya maddi ve manevi tazminat davalarında önce hukuka aykırı durumun tespiti yapılır, ardından mevcut saldırının durdurulmasına ya da davacıya tazminat ödenmesine karar verilir⁵³³. Örnek olarak, kişisel verilerin hukuka aykırı olarak işlendiği durumda, veri sahibi, hukuka aykırı işlemenin durdurulmasını talep eder. Bu dava, hukuka aykırı işlemenin durdurulması talebine yöneldiğinden durdurma kararı, hukuka aykırılığın tespiti kararını içereceğinden ayrıca bir tespit davası açılması gerekmecektir⁵³⁴.

İlgili kişi genel hükümlere dayanarak tespit davası açmadan doğrudan KVKK hükümlerine de başvurabilir. Şöyle ki KVKK'nın 11. maddesinin a, b, c ve ç bentleri uyarınca veri sorumlusuna başvuru yapan ilgili kişiye; kendisine ilişkin kişisel verilerin işlenip işlenmediğini öğrenme, eğer işlenmişse buna ilişkin bilgi talep etme, işlenmenin amacını ve verilerin amacına uygun kullanıp kullanılmadığını öğrenme, yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme imkanı tanınmıştır. KVKK'da düzenlenen bu hüküm ile ilgili kişi tespit davası açmak yerine, bu düzenlemede sayılan haklarını kullanarak kişisel verilerin korunmasına ilişkin tespit yapabilme imkanına sahiptir⁵³⁵. Bu durum kişilerin kişisel verilerine ilişkin hukuka aykırılığı tespit talebini daha pratik bir hale getirmektedir. Dolayısıyla KVKK'da düzenlenen bu yol, genel tespit davası ile kıyasta daha sık tercih edilmektedir⁵³⁶.

3.3.2.4. Sebepsiz Zenginleşme Davası

TBK madde 77 uyarınca, haklı bir sebep olmaksızın, bir başkasının malvarlığından veya emeğinden zenginleşen kişi, bu zenginleşmeyi geri vermekle

⁵³³ Çabuk a.g.t, s. 127.

⁵³⁴ Özdemir, a.g.e, s. 188.

⁵³⁵ Özdemir, a.g.e, s.188 - 955, Taştan, a.g.e, 196.

⁵³⁶ Özdemir, a.g.e, s. 188 - 955, Taştan, a.g.e, 196.

yükümlüdür. Dolayısıyla; failin elde ettiği kazancın sebepsiz zenginleşme hükümlerine göre zarar görmüş kişiye iadesi kanunla mümkün kılınmıştır⁵³⁷. Söz konusu davanın açılabilmesi için ilk önce, kişilik hakkına yönelik saldırıda bulunan kişinin malvarlığında meydana gelen bir artış, yani zenginleşme ve saldırıya uğrayan kişinin, bu saldırı sebebiyle malvarlığında bir azalma (fakirleşme) oluşmalıdır⁵³⁸.

Bu dava türünde saldırıyı gerçekleştiren kişinin zenginleşmesi ile saldırıya uğrayan kişinin fakirleşmesi arasında uygun illiyet bağı bulunmalıdır⁵³⁹. Ayrıca saldırıdan dolayı zenginleşmiş kişinin kusurunun bulunması gerekmemektedir⁵⁴⁰.

Zenginleşmenin hukuken geçerli bir haklı sebebe dayalı olmaması durumu sebepsiz zenginleşme davasının açılabilmesi için aranan diğer şarttır⁵⁴¹. “*Geçerli bir haklı sebebin olmaması*” ifadesinden hukuki sebebin mevcut olmaması veya irade beyanlarının birbirine uygun bulunmaması ya da onay, izin, ehliyet, vb. geçerlilik ve etkinlik unsurlarından birinin mevcut olmaması sebebiyle zenginleşmeye esas teşkil eden hukuki işlemin kurulamaması, eksik kurulması ya da geçersiz kurulması sonucunu doğuran sebepler anlaşılmalıdır⁵⁴². Bu durumda zenginleşmeye esas teşkil eden hukuki işlem geçersiz olacağından dava sonucunda sonra taraflar aldıklarını iade ile yükümlü olacaktır⁵⁴³.

Kişisel verilerin hukuka aykırı işlenmesinden veri sorumlusunun zenginleşmesine ve veri sahibinin aynı oranda fakirleşmesine pek rastlamak mümkün değildir. Örneğin; hastanenin kişisel sağlık verilerini sigorta şirketlerine satarak zenginleştiği, hastanın ise aynı oranda fakirleştiğini söylemek mümkün olamayacaktır⁵⁴⁴.

⁵³⁷ Serozan, 1997, s. 98, Kılıçoğlu, 2019 (b), s. 347.

⁵³⁸ Doktrinde sebepsiz zenginleşme sorumluluğunun oluşması için fakirleşmenin aranması gerekmediği savunulmaktadır. Fikret Eren, Borçlar Hukuku Genel Hükümler 20. Baskı, Ankara Yetkin Yayınları, 2016, s. 890.

⁵³⁹ Kılıçoğlu, 2019 (b), s. 348, Özdemir, a.g.e, s. 199.

⁵⁴⁰ Kılıçoğlu, 2019 (b), s. 348, Özdemir, a.g.e. s. 200;

⁵⁴¹ Kılıçoğlu, 2019 (b), s. 348

⁵⁴² Eren, a.g.e, s. 900.

⁵⁴³ Eren, a.g.e, s. 900, Özdemir, a.g.e. s. 204;

⁵⁴⁴ İrem Gürbüz Erel, Sağlık Hukukunda Kişisel Verilerin Korunması, Yüksek Lisans Tezi, Kocaeli Üniversitesi, Sosyal Bilimler Enstitüsü, Kocaeli, 2021, s. 160.

3.3.2.5. Vekaletsiz İş Görme Davası

TMK madde 25/3 hükümlerince ilgili kişi, kişilik hakkına yönelik hukuka aykırı bir saldırı dolayısıyla elde edilmiş kazancın vekaletsiz iş görme hükümlerine göre kendisine verilmesini talep edebilir. Ancak iş gören işi iş sahibinin menfaatine iş yapmamış olduğu için burada gerçek olmayan vekaletsiz iş görme hükmü (TBK madde 530) söz konusu olacaktır⁵⁴⁵. TBK madde 530 uyarınca; *“İşsahibi, kendi menfaatine yapılmamış olsa bile, işgörmeden doğan faydaları edinme hakkına sahiptir”*. Buna göre iş sahibi işgörenin, yetkisiz olarak kendi menfaatine veya üçüncü bir kimsenin menfaatine yaptığı, bir başka deyişle iş sahibinin menfaatine yapmadığı işlerden elde ettiği kazancın verilmesini isteyebilir⁵⁴⁶.

Bu dava türünün açılabilmesi için iki şart aranmaktadır. İlk şart, başkasına ait bir işin görülmesi gerekmesi, yani işin vekaletsiz bir şekilde adına iş görülen kişiye ait ve yalnızca, o kişi tarafından görülebilecek bir iş olmasıdır. Diğer bir şart ise, başkasına ait bir işin görülmesi sonucunda maddi bir kazancın elde edilmiş olmasıdır⁵⁴⁷. Ancak burada bahsi geçen hakları ihlal edilmiş kişinin elde etmek istemediği veya elde edemeyeceği kazançtır⁵⁴⁸. Örnek olarak, ilgili kişinin unutulma hakkına dayanarak hatırlanmasını istemediği, geçmişte yaşanmış bir olayın tiyatro oyunu ya da sinema filmi haline dönüştürülmesi halinde söz konusu tiyatro oyunundan/sinema filminden elde edilen kazancın vekaletsiz iş görme hükümlerine dayanarak talep edilebilmesi mümkündür⁵⁴⁹.

3.3.2.6. Maddi Tazminat Davası

KVKK madde 14(3)’e göre, kişilik hakkı ihlal edilenlerin, TBK madde 49 vd. hükümleri uyarınca tazminat hakkı vardır. Kişi kendi kişilik haklarına yönelik olarak bir saldırı olduğunda ve bu saldırı sonucu maddi zarara uğradığında söz konusu

⁵⁴⁵ Gülşah Sinem Aydın, Kişilik Hakkı İhlalinden Doğan Vekâletsiz İş Görme, İstanbul, On İki Levha Yayıncılık, 2017, s. 12, Ece Baş Süzel, Gerçek Olmayan Vekaletsiz İş Görme ve Menfaat Devri Yaptırımı, İstanbul, On İki Levha Yayıncılık, 2015, s. 278 vd, Gülşah Sinem Aydın, “Kişilik Hakkı İhlalinden Doğan Vekaletsiz İşgörmeye Kusurun Bir Şart Olarak Aranıp Aranmayacağı Sorunu”, MÜHF, HAD, Cilt 23, Sayı 1, 2017, s. 268, Kılıçoğlu, 2019 (b), s. 349.

⁵⁴⁶ Süzel, a.g.e, s. 7, Kılıçoğlu, 2019 (b), s. 354.

⁵⁴⁷ Çabuk, a.g.t, s. 129-130.

⁵⁴⁸ Dural/Ögüz, a.g.e, s. 156; Özdemir, a.g.e, s. 202.

⁵⁴⁹ Aydın, a.g.e, s. 95.

zararın tazminine yönelik maddi tazminat davası açabilir⁵⁵⁰. Bu davanın amacı hukuka aykırı saldırının sonucunda zarara uğramış kişinin maddi zararının telafisidir⁵⁵¹.

Maddi tazminat davasının açılabilmesi için TBK madde 49 uyarınca, için, hukuka aykırı olan fiil, kusur ve saldırıyla zarar arasında uygun illiyet bağı olmalıdır⁵⁵². Kişisel verilerin korunması hakkının ihlali durumunda açılacak diğer davalardan farklı olarak maddi tazminat davasının açılabilmesi için hakkı ihlal etmiş kişinin kusuru olmalıdır.

Kişisel verilerin korunması ile ilgili ekonomik bilgilerin, bankalar veya kredi kuruluşları tarafınca yalnız işlendiği durumlarda maddi bir zarar söz konusu olabilir⁵⁵³. Örneğin, sözleşme ilişkisi kapsamında banka tarafından kişinin kredibilitesinin “çok kötü” kodu ile hukuka aykırı biçimde, yanlış işlenirse, kişi kredi çekmek amacıyla başvuracağı bankalardan olumsuz cevap alacak, ve eğer bu kişi tacirse ekonomik anlamda büyük zarara uğrayabilecektir. Böyle bir durumda kişi, kendi kişisel verilerinin hukuka aykırı bir şekilde işlendiği için oluşmuş maddi zararını, bankadan maddi tazminat davası ile talep edebilecektir⁵⁵⁴.

Saldırının sonucunda veri sahibi zarara uğrayabileceği gibi elde edebileceği kardan da yoksun kalabilir. Örneğin ünlü bir sanatçının doktorunun kendi internet sitesinde hastası olan bu sanatçının HIV virüsü taşıdığına ilişkin açıklamada bulunması sonucu sanatçının mevcut anlaşmalarının (konser, reklam, sponsorluk vb.) iptal edilmesi ve yeni anlaşmalar yapamaması onu bu faaliyetlerden elde edebileceği kardan yoksun bırakacaktır⁵⁵⁵.

Bunların dışında TBK madde 50’de tesbit edildiği üzere, maddi tazminat davasında davacı maruz kaldığı zararı ispat etmekle yükümlüdür⁵⁵⁶. Dolayısıyla maddi tazminat davası açan ve kişisel verilerinin hukuka aykırı işleme tabi tutulduğunu iddia eden veri sahibi bunu ispatlamakla yükümlüdür⁵⁵⁷. Davacı zararını tam olarak ispat edemedikçe, hakim, olayların olağan akışı ve zarara maruz kalan kişinin bu zarara karşın aldığı tedbirleri göz önünde bulundurarak, zarar miktarını

⁵⁵⁰ Dural/Ögüz, a.g.e, s. 157, Helvacı, 2021, s. 124.

⁵⁵¹ Helvacı, 2021, s. 124, Helvacı, 2001, s. 177.

⁵⁵² Helvacı, 2021, s. 124-125, Kılıçoğlu, 2019 (b), s. 371.

⁵⁵³ Taştan, a.g.e, s. 175.

⁵⁵⁴ Çabuk, a.g.t, s. 132.

⁵⁵⁵ Özdemir, a.g.e, s. 209.

⁵⁵⁶ Kılıçoğlu, 2019 (b), s. 363-365.

⁵⁵⁷ Özdemir, a.g.e, s. 209, Taştan, a.g.e, s. 182, Kılıçoğlu, 2019 (b), s. 366.

hakkaniyetle belirler⁵⁵⁸. Doktoru tarafından bilgileri yayımlanmış sanatçının örneğinde, hukuka aykırı saldırı sonucunda kişinin maddi olarak bir kazanç kaybı yaşaması, olayların mümkün akışı ve hayat tecrübesi göz önünde bulundurularak değerlendirilecektir⁵⁵⁹.

TBK madde 52 uyarınca hak sahibinin rızası tazminatın indirilmesi veya tamamen kaldırılması sebeplerinden biri olarak gösterilmiştir. Dolayısıyla; zarara uğramış kişinin zararı oluşturmuş saldırıya rıza göstermişirse ve bu rıza zararın doğmasında veya artmasında etkili olmuşursa, hakim, tazminatın indirilmesine ya da tamamen kaldırılmasına karar verebilir⁵⁶⁰. Bilindiği gibi, ilgili kişinin rızası, kişisel verilerin korunması alanında bir hukuka uygunluk sebebidir. Bu bağlamda kişinin verilerinin işlenmesine ilişkin rıza göstermesi tazminatın belirlenmesinde önem arz edecektir⁵⁶¹. Veri sahibinin rızasının neden olduğu zarar veri işleme faaliyeti sırasında verilmiş rızanın hukuka uygunluğu bağlamında değerlendirilmelidir. Örneğin; veri sahibinin işlenmesi için izin verdiği amaç dışında verilerinin işlenmesi ya da izin verdiği ölçüden fazla verinin işlenmesi durumunda veri sahibi maddi zarara maruz kalırsa hakim rıza kavramına dayanarak maddi tazminle ilgili hükümleri uygulama dışında bırakmamalıdır.

3.3.2.7 Manevi Tazminat Davası

TMK madde 25/3'ten yola çıkarak TBK madde 58'deki kişilik hakkının zedelenmesine ilişkin düzenlemelere göre, kişilik hakları hukuka aykırı bir şekilde saldırıya uğrayan kişi bundan dolayı oluşmuş manevi zararını, diğer bir deyimle acı, elem ve ızdırabını gidermek için manevi tazminat davası açabilir⁵⁶².

Manevi tazminat davasının açılması ile ilgili şartlar maddi tazminat davasının şartları ile benzetilmektedir. Şöyle ki, kişinin manevi tazminat davası açabilmesi için kişilik haklarına yönelik bir saldırının mevcudluğu ve bu saldırı sonucunda bir manevi zararın ortaya çıkmış olması gereklidir. Ayrıca, sözkonusu zararın saldırganın bir kusuru sonucu ya da kusursuz sorumluluktan dolayı oluşmalı ve

⁵⁵⁸ Çabuk, a.g.t, s. 132.

⁵⁵⁹ Özdemir, a.g.e, s. 209.

⁵⁶⁰ Çabuk, a.g.t, s. 133.

⁵⁶¹ Gürbüz, s. 162.

⁵⁶² Dural/Ögüz, a.g.e, s. 158, Helvacı, 2001, s. 177.

saldırı ile manevi zarar arasında illiyet bağı bulunmalıdır⁵⁶³. Konuya ilişkin Danıştay kararında, Devlet hastahanesinde HIV testi pozitif çıkan hastanın doğrulama testi için bir üst basamak sağlık kuruluşuna sevki gerekliken, laboratuvar teksiye tarafından sonucunu doğrulama aşaması yapılmadan hastanın yakınlarına pozitif sonucun açıklanması üzerine hasta yakınının intihar etmek suretiyle yaşamını yitirmesi, hastalığın ağırlığı ve olayın oluşumu göz önünde bulundurularak davacı yakının idarenin ağır hizmet kusurunun neden ve etkisiyle intihar ederek yaşamını yitirmesi sonucunda doğan zarar ile uygun nedensellik bağı bulunduğu karar verilmiştir⁵⁶⁴.

Maddi tazminatla manevi tazminat arasındaki temel fark zararın ispatına ilişkindir. Her iki dava türünde davacı taraf zararı ispat etmekle yükümlü olsa da, manevi zararı daha çok kişinin zarardan dolayı yaşadığı duygu değişimleri, üzüntülerle, kederle bağlantılı olduğundan her somut olay ayrıca incelenmeli ve manevi zararın mevcut olup olmaması araştırılmalıdır⁵⁶⁵. Konuya ilişkin Yargıtay kararında, davacının kişisel verilerine hukuka aykırı biçimde erişilmesinin ne gibi manevi zarara neden olmasının ispatlanamadığı ve TBK 58. maddenin şartlarının oluşmadığı gerekçesiyle verilen ret kararının doğru olmadığı, e-devlet şifresiyle davacının kişisel verilerine erişildiği, dolayısıyla manevi zararın oluştuğu belirtilmiştir⁵⁶⁶. İlgili başka bir Danıştay kararında ise yanlış olarak konulan HIV tanısı sonucunun basına sızdırılması sonucu hastanın işsiz kalması ve bunun sonucunda uğradığı maddi zararın ve elem, üzüntü, sarsıntı nedeniyle uğradığı manevi zararın tazminine karar verilmiştir⁵⁶⁷.

Manevi tazminat davasının amacı kişilik hakları saldırıya maruz kalmış kişinin uğradığı zararın parasal bakımdan karşılanması değildir. Burada amaç kişinin yaşadığı üzüntü, acı ve ruhsal sorunların giderilmesidir⁵⁶⁸. Bu nedenle de tazminat miktarı saldırıya uğrayan kişinin sebepsiz zenginleşmesine neden olmamalıdır⁵⁶⁹.

Davanın sonucunda hakim ile de hakkı ihlal etmiş kişinin zarar görmüş kişiye para ödeyecek olmasına karar vermesi gerekmemektedir. Zira TBK madde 58

⁵⁶³ Eren, a.g.e., s. 812.

⁵⁶⁴ Danıştay, 10. Daire, E. 2005,8407, K. 2007,6526, T. 28.12.2005, Künyeli kararı.

⁵⁶⁵ Yargıtay, 4. Hukuk Dairesi, 2000/1501 E, 2000/1501K, 15.01.2001 T, Kazancı Bilgi ve İhtihat Bankası, E.T.: 10.09.2022.

⁵⁶⁶ Öztürk/Seyhan/Çalışkan, a.g.e, s. 242.

⁵⁶⁷ Danıştay, 10. Daire, E. 1994/5314, K.1996/294, T. 31.01.1996, Künyeli kararı.

⁵⁶⁸ Çiğdem Öngün Ayözger, Kişisel Verilerin Korunması Hukuku, 2. Bası, İstanbul, Legal Kitabevi, 2019, s. 281.

⁵⁶⁹ Dural/Ögüz, a.g.e, s. 160.

uyarınca, hakim, tazminatın ödenmesi yerine, zararın başka bir şekilde giderilmesine karar verebilir veya bunu da tazminata ekleyebilir⁵⁷⁰. Ayrıca hakimın re'sen saldırıyı kınayan bir karar vermesi ve bu kararın yayımlanmasına hükmedebilmesi mümkündür. Örnek olarak, kişisel verilere ilişkin basın ve yayın yoluyla gerçekleştirilen saldırıya ilişkin kararın yayımlanması⁵⁷¹, zararın tazmini açısından oldukça önemli olacaktır. Başka bir örnekte, kişinin yazışmalarının, ya da telefon kayıtlarının telefon operatörü tarafından kişinin kendi rızası olmaksızın başka kişilerle paylaşılması sonucu kişi özel hayatına ilişkin kişilik haklarının ihlali gerekçesiyle manevi tazminat davası açabilir.

⁵⁷⁰ Kılıçoğlu, 2019 (b), s. 417.

⁵⁷¹ Resmi Gazete, 26.06.2004, 5187 Sayılı Basın Kanunu, Sayı 25504.

SONUÇ

Günümüzde teknoloji dünyasında yaşanan gelişmelerin etkisiyle hayatımızın neredeyse her alanında veri kavramı karşımıza çıkmaktadır. Üretilen veri miktarındaki hızlı artışa bağlı olarak veri işleme faaliyetleri de artmıştır. Bu faaliyetler ise belirli kurallar dahilinde gerçekleştirilmelidir. Aksi halde; hukuka aykırı bir veri işleme faaliyeti veri sahibinin maddi, manevi zarara uğramasına sebep olabilmektedir. Bu nedenle kişisel verilerin korunmasına ilişkin hukuki düzenlemelerin yapılması gerekmektedir. AB’de veri koruma hukukuna dair ilk kapsamlı düzenleme olan veri koruma Direktif’i esas alınarak 2016 senesinde Türkiye’de bu alanda ilk özel düzenleme olan 6698 sayılı KVKK kabul edilmiştir. Bunun hemen ardından; aynı yılda GVKT kabul edilmiş, 2018 senesinde yürürlüğe girmiştir. Direktif’e göre uygulama alanı daha geniş olan bu düzenlemenin halefinden bir diğer farkı; üye devletler tarafından ulusal hukuka aktarılmasına ihtiyaç duyulmaksızın uygulanabilmesiydi. Çalışmamız kapsamında; bu iki temel düzenlemede yer alan kavramlar, sükeler, ilkeler, haklar, yükümlölükler, kişisel verilerin işlenmesi ve korunmasına ilişkin başvurulabilecek yollar ve kavram haritası karşılaştırılmalı şekilde açıklanmaya çalışılmıştır.

Birinci bölümde ilk olarak kişisel veri kavramının tanımı ve unsurları incelenmiştir. Kavramın kendisi, her iki düzenlemeye göre kimliği belirlenebilir, gerçek kişiye ait olan “*her türlü bilgi*”yi ifade etmektedir. Kişisel verilerin türleri ise iki düzenleme açısından farklılığın mevcut olduğu alanlardan biridir. Şöyle ki, her iki düzenlemede de özel nitelikli veri kavramına yer verilmiş, ancak GVKT ile bu verilerin işleme şartları daha geniş tutulmuştur. Aynı şekilde, Tüzük’te kişinin cinsel yönelime ilişkin veriler tahdidi olarak sayılmış, KVKK’da ise bu konuya ilişkin ayrıca bir koruma tespit edilmemiştir. Buna ek olarak; kişinin kılık kıyafetine ilişkin verileri KVKK ile özel nitelikli kişisel veri sayılırken, GVKT’de böyle bir husus düzenlenmemiştir. İlk bölüm kapsamında yer verilen diğer bir husus ise kişisel verilerin hukuki niteliğine ilişkin görüşlerdir. Buradan çıkarılacak ilk sonuç; mülkiyet hakkı ve fikri hak görüşlerinin kişisel verilerin kendisine has özellikleriyle başdaşmamasıdır. Ancak kişilik hakkı görüşü de kişisel verilerin korunmasında tek başına yetersiz kalmaktadır. Kanaatimizce; kişisel veriler hayatımızdaki önemi ve kendi özellikleri esas alınarak ayrı bir hak alanı olarak korunmalıdır.

İkinci bölümün ilk kısmında veri işleme faaliyetine ilişkin temel kavramlara yer verilmiştir. Veri sahibi ve veri sorumlusuna ilişkin tanımlar iki düzenlemeye benzer şekildedir. Her iki düzenlemeye göre; yalnızca gerçek kişiler veri sahibi sayılırken, hem gerçek, hem de tüzel kişiler veri sorumlusu veya veri işleyen olabilmektedirler. Burada farklılık GVKT’de ortak veri sorumluları kavramına da yer verilmiş olmasıdır. Kişisel verilerin işlenmesine ilişkin genel ilkeler çalışma kapsamında karşılaştırılan bir diğer husustur. İşleme faaliyetine ilişkin genel ilkeler iki düzenlemeye de çoğunlukla benzer şekilde düzenlenmiştir. Ancak bütünlük ve gizlilik, ve hesap verebilirlik ilkesi yalnızca GVKT’de düzenlenmiş, KVKK’da bu ilkelere yer verilmemiştir. Veri aktarımı hususu ise her iki düzenlemeye göre; belirli şartlara tabi tutulmuştur. Burada esas fark; Tüzüğün uluslararası niteliğine bağlı olarak veri aktarımı konusunda kapsamının KVKK’ya kıyasta daha geniş olmasıdır. Aynı şekilde GVKT’de veri sorumlularına KVKK’da birebir karşılığı olmayan ve orada tespit edilenlere ek olarak; temsilci atama, iş bölümü anlaşması yapma, ispat, veri güvenliğini sağlama yükümlülükleri belirlenmiştir. Veri sahiplerinin hakları da Tüzük kapsamında genişlendirilmiştir. KVKK’dan farklı olarak; GVKT’de veri sahiplerine unutulma, işlemin sınırlandırılması, veri taşınabilirliği hakları tanınmıştır.

Çalışmamızın sonuncu bölümünde kişisel verilerin hukuka aykırı işlenmesinden veri sahibinin korunması incelenmiştir. İlk olarak veri işleme faaliyetinin hukuka uygun olma şartları AB ve Türk özel hukuku açısından karşılaştırılmıştır. Burada dikkat edilmesi gereken ilk husus çocukların rızasının alınması konusunda iki düzenleme arasındaki farklılıktır. Şöyle ki, GVKT’nin 8. maddesi uyarınca işleme faaliyetlerinin hukuka uygunluğu için veri sahibinin rızasına gerektiği durumlarda rızanın geçerli olabilmesi için çocuk en az 16 yaşında olmalıdır. Çocuk 16 yaşından küçük olduğunda ise veri işleme faaliyeti, yalnızca rızanın çocuğun üzerinde velayet hakkı bulunan kişi tarafından verildiği, ya da onaylandığı durumlarda ve ölçüde hukuka uygun olacaktır. Bahsi geçen husus KVKK ile düzenlenmemiştir. Diğer bir önemli farklılık veri koruma hakkının ihlal edilmesi durumunda veri sahibince yapılabilecek başvuruya ilişkindir. KVKK hükümlerine göre veri sahibinin Kurul’a şikayette bulunabilmesi için aşamalı bir mekanizma belirlenmiştir. Veri sahibi veri sorumlusuna başvuru yolunu tüketmeden Kurul’a şikayet yoluna başvuramaz. Ancak Tüzük’te veri sahiplerinin denetim

otoriteleri ya da Avrupa Veri Koruma Kurul’una baş vurabilmeleri için böyle bir şart aranmamıştır.

Kişisel verilerin korunması kapsamında günümüzde en önemli mesele, insanlar arasındaki bilincin artırılması, doğru bilinen yanlışların düzeltilmesidir. GVKT’nin kabulünden bir sene sonra AB vatandaşlarına yapılan ankette; 2015’deki sonuçlar göre %20 puanlık bir artışla, katılımcıların %67’si GVKT’yi duyduğunu, %36’sı ise düzenlemenin neleri kapsadığını, %57’si ise ülkelerinde veri koruma haklarını korumaktan sorumlu bir denetim otoritesinin varlığından haberdar olduklarını bildiklerini belirtmiştir⁵⁷². Bu bağlamda, en fazla veri ihlali yaklaşık 125 milyon vaka ile 2020’nin dördüncü çeyreğinde tespit edilirken, 2022’nin ikinci çeyreğinde, bu rakam bir önceki çeyreğe göre %56 düşerek 52 milyona ulaşmıştır⁵⁷³. Rakamlardan da görüldüğü üzere; düzenlemenin kabulünden sonra özellikle veri sahiplerinin veri koruma alanına ilişkin bilinci gözle görülür derecede artmıştır. KVKK’nın ulusal bir düzenleme veya Türk veri koruma hukukundaki ilk ulusal düzenleme olmasından dolayı GVKT ile tespit edilen hususların bazılarının burada tespit edilmemesi normal olarak değerlendirilebilir. Kişisel Verileri Koruma Kurumu tarafından Kanun’da tespit edilmeyen hususlara ilişkin yönetmelikler, rehberler, klavuzlar, tavsiyeler ve s. yayımlanmaktadır. Ancak herhangi bir hukuka aykırı olayın yaşanması durumunda mahkemelerce bakılacak ilk düzenlemenin KVKK olduğunu varsayarak; Kanun’un gelişim ve uluslararası düzenlemeler dikkate alınarak daim güncel tutulması önem arz etmektedir.

⁵⁷² EDPB, 1 year GDPR – taking stock, https://edpb.europa.eu/news/news/2019/1-year-gdpr-taking-stock_en, E.T.: 11.09.2022.

⁵⁷³ Statista Research Department, “Global number of quarterly data breaches 2021-2022”, 2022, Data breaches worldwide quarterly 2022 | Statista, E.T.: 11.09.2022.

KAYNAKÇA

1. Kitaplar:

Akipek Jale / Akıntürk Turgut / Ateş Derya (2019), Türk Medeni Hukuku Başlangıç Hükümleri Kişiler Hukuku, 15.basım, İstanbul, Beta Basım.

Aksoy Hüseyin Can (2010), Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması, Ankara, Çakmak Yayınevi.

Akgül Aydın (2014), “Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması”, 2. Basım, İstanbul, Beta Basım Yayım.

Akipek Jale/ AkıntürkTurgut/Ateş Derya (2019), Eşya Hukuku, 15.Basım, İstanbul, Beta Basım Yayım.

Altındere Murat (2020), Kişisel Verilerin Korunması Hukuku ve Uygulaması, 1. Basım, İstanbul, Adalet Yayınevi.

Aydın Gülşah Sinem (2017), Kişilik Hakkı İhlalinden Doğan Vekâletsiz İş Görme, İstanbul, On İki Levha Yayıncılık.

Aydın Sedat Erdem (2015), AİHM İçtihatları Bağlamında Kişisel Verilerin Kaydedilmesi Suçu, 1. Baskı, İstanbul, On İki Levha Yayıncılık.

Ayözger Çiğdem Öngün (2019), Kişisel Verilerin Korunması Hukuku, 2. Bası, İstanbul, Legal Kitabevi.

Baskın Onur (2021), Kişilik Hakkı Kapsamında Kişisel Verilerin Korunması, 1.basım., Ankara, Seçkin Yayıncılık.

Başalp Nilgün (2004), Kişisel Verilerin Korunması ve Saklanması, 1. Baskı, Ankara, Yetkin Yayınları.

Baysal Mustafa (2022), Kişisel Verilerin Korunması Kanunu El Kitabı, 5. Baskı, Ankara, Seçkin Yayınları.

Çekin Mesut Serdar (2019), Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku, 2. Baskı, İstanbul, On İki Levha Yayıncılık.

Çelikel Serdar (2021), Kişisel Verilerin Korunması Hukuku Kapsamında Veri Sorumlusu ve Veri Sorumlusunun Yükümlülükleri, 1. Baskı, Ankara, Seçkin Yayınları.

Develioğlu Murat (2017), 6698 Sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku, İstanbul, On İki Levha Yayıncılık.

- Dural Mustafa, Ögüz Tufan (2019), Türk Özel Hukuku, Kişiler Hukuku, 20. Baskı, İstanbul, Filiz Kitabevi.
- Dülger Murat Volkan (2019), Kişisel Verilerin Korunması Hukuku, 2. Baskı, İstanbul, Hukuk Akademisi yayınevi.
- Eren Fikret (2016), Borçlar Hukuku Genel Hükümler, 20. Baskı, Ankara, Yetkin Yayınları.
- Erhan Günay (2017), Kişilik Haklarına Saldırıdan Kaynaklanan Tazminat Davaları, Güncellenmiş 2. Baskı, Ankara, Seçkin Yayınları.
- Gürses Bekir (2022), AB ve Türk Hukukunda Kişisel Verilerin Korunması-Mevzuat Uyumuna Yönelik Bir Değerlendirme, 1. Baskı, İstanbul, Platon Hukuk.
- Hatemi Hüseyin (2017), Kişiler Hukuku, 9. Baskı, İstanbul, On İki Levha Yayıncılık.
- Helvacı Serap (2021), Gerçek Kişiler, 9. baskı, İstanbul, Legal Kitabevi.
- Helvacı Serap (2001), Türk ve İsviçre Hukuklarında Kişilik Hakkını Koruyucu Davalar, İstanbul, Beta Basım Yayın Dağıtım.
- Hizarcı Emine (2020), 6698 Sayılı Kişisel Verilerin Korunması Kanununun AB Veri Koruma Hukuku Işığında Değerlendirilmesi, İstanbul, Yetkin Yayınları.
- Kaya Cemil (2005), İdare Hukukunda Bilgi Edinme Hakkı, Ankara, Seçkin Yayıncılık.
- Kaya Mine (2015), Elektronik Ortamda (Elektronik haberleşme – İnternet – Sosyal Medya) Kişilik Hakkının Korunması, 1. Baskı, Ankara, Seçkin Yayınları.
- Kılıçoğlu Ahmet M. (2019), Borçlar Hukuku Genel Hükümler, Genişletilmiş 23. Bası, Ankara, Turhan Kitabevi.
- Kılıçoğlu Ahmet M. (2019), Medeni Hukuk, 3.basım, Ankara, Seçkin Yayıncılık.
- Kılıçoğlu Ahmet (2013), Sınai Haklarla Karşılaştırmalı Fikri Haklar, Genişletilmiş-Gözden Geçirilmiş 2. Bası, Ankara, Turhan Kitabevi.
- Kılıçoğlu Ahmet M (2016), Şeref, Haysiyet ve Özel Yaşama Basın Yoluyla Saldırılarından Hukuksal Sorumluluk, Yeniden Gözden Geçirilmiş, Güncelleştirilmiş 5. Bası, Ankara, Turhan Kitabevi.
- Küzeci Elif (2019), Kişisel verilerin Korunması, Yenilenmiş ve Gözden Geçirilmiş 3. Baskı, Ankara, On İki Levha Yayıncılık.
- Oğuzman Kemal, Barlas Nami (2019), Medeni Hukuk, 25.basım, İstanbul, On İki Levha Yayıncılık.

- Osman Gökhan/Topuz Murat (2019), Eşya Hukuku, C. IV/1, Genişletilmiş 3. Baskı, Ankara, Seçkin Yayıncılık.
- Özcan Göknıl (2020), Bankacılık İş ve İşlemlerinde Kişisel Verilerin Korunması, İstanbul, On İki Levha Yayınları.
- Özdemir Hayrünnisa (2009), Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması, Ankara, Seçkin Yayıncılık.
- Özel Sibel (2004), Uluslararası Alanda Medya ve İnternette Kişilik Hakkının Korunması, 1. Baskı, Ankara, Seçkin Yayıncılık.
- Özkan Oğulcan (2020), Kişisel Verilerin Korunması, 1. Baskı, Ankara, Yetkin Yayınları.
- Öztan Bilge (1987), Şahsın Hukuku, 1. Basım, Ankara, Turhan Kitabevi.
- Öztürk Bahri, Seyhan Serkan, Çalışkan Altınok Elif (2022), Kişisel Verilerin Korunması Hukuku Teorik ve Pratik Çalışma Kitabı, 2.basım, Ankara, Seçkin Yayıncılık.
- Serozan Rona (2014), Eşya Hukuku I, Genişletilmiş 3. Bası, İstanbul, Filiz Kitabevi.
- Serozan Rona (2017), Medeni Hukuk-Genel Bölüm/Kişiler Hukuku, 7. Bası, İstanbul, Filiz Kitabevi.
- Sirmen A. Lale (2018), Eşya Hukuku, 6. Baskı, Ankara, Legal Kitabevi.
- Süzel Ece Baş (2015), Gerçek Olmayan Vekâletsiz İş Görme ve Menfaat Devri Yaptırımı, İstanbul, On İki Levha Yayıncılık.
- Şimşek Oğuz (2008), Anayasa Hukukunda Kişisel Verilerin Korunması, İstanbul, Beta Basım Yayım.
- Taştan Furkan Güven (2017), Türk Sözleşme Hukukunda Kişisel Verilerin Korunması, İstanbul, On iki Levha Yayınevi.
- Turan Metin (2019), Karşılaştırmalı Hukukta Kişisel Verilerin Korunması, 2. Baskı, Ankara, Seçkin Yayınevi.
- Uyarer Sinem Göçmen (2020), Kişisel Verilerin Korunması, 2. Baskı, Ankara, Seçkin Yayıncılık.
- Yavuz Nihat (2018), Borçlar Hukuku El Kitabı, Ankara, Adalet Yayınevi.

2. Makaleler, Raporlar ve Diğer Basılı Yayınlar

- Akkurt Sinan Sami (2020), “Kişisel Veri Kavramının Hukuki Niteliğine İlişkin Yaklaşımlara Mukayeseli Bir Bakış”, *Kişisel Verileri Koruma Dergisi*, 2(1), 20-32.
- Albretch, J. (2015) “How the GDPR Will Change the World” *European Data Protection Law Review*, 2(3), 287-289
- Aşıkoğlu Ş. İ. (2019) “Veri Sorumlularının Aydınlatma Yükümlülüğü - Avrupa Birliği ve Türk Hukukunda”, *Kişisel Verileri Koruma Dergisi*, 1(2), 41-65.
- Atasoy Kemal, (2016), “Kişilik Hakkı Kapsamında Sosyal Medyada Kişisel Verilerin Korunması ve Veri Sahibinin Rızası”, *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, 22(3), 269-301.
- Avcı Yasemin (2019), *Kişisel Verilerin Korunması, Yüksek Lisans Tezi*, Selçuk Üniversitesi, Sosyal Bilimler Enstitüsü, Konya.
- Aydın Gülşah Sinem (2017), “Kişilik Hakkı İhlalinden Doğan Vekaletsiz İşgörmeye Kusurun Bir Şart Olarak Aranıp Aranmayacağı Sorunu”, *MÜHF, HAD*, 23(1), s. 265-302.
- Aydın Muhammet (2020), *Kişisel verilerin Korunması Bağlamında idarenin Sorumluluğu ve Yargısal Denetimi*, Yüksek Lisans Tezi, Ufuk Üniversitesi, Sosyal Bilimler Enstitüsü, Ankara.
- Aysal Necdet (2011), “Tanzimat'tan Cumhuriyet'e Giyim ve Kuşamda Çağdaşlaşma Hareketleri”, *Çağdaş Türkiye Tarihi Araştırmaları Dergisi*, 10(22), 3-32.
- Başalp Nilgün (2015), “Avrupa Birliği Veri Koruması Genel Regülasyonu’nun Temel Yenilikleri”, *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, 21 (1), s. 77-105.
- Başar Cemal (2020), “Kişisel Verilerin Korunması Bakımından Kişisel Verileri Koruma Kurul’na Yapılan Şikayet Başvurusu”, *Fasikül Hukuk Dergisi*, 12(125), s. 16-33.
- Bibas Steven A.,(1994) “A Contractual Approach to Data Privacy”, *Harvard Journal of Law & Public Policy*, 17(2), s. 591-611.
- Bilir Faruk (2021), “Kişisel Verilerin Korunması Kişinin Kendisinin Korunmasıdır”, *TRT Akademi* , 6 (11), s. 172-181.
- Boran Güneysu Nilüfer, Memiş Burak (2019), “Kişisel Verilerin Korunması Kanunu Kapsamında Avukatın Yükümlülük ve Sorumlulukları”, *Anadolu Üniversitesi Hukuk Fakültesi Dergisi*, 5(2), s. 313-337.

- Bulut Çimen İpek, (2020), “Avrupa Birliği Genel Veri Koruma Tüzüğü Kapsamında Getirilen Yeni Teknik ve Yaptırım Mekanizmaları”, Anadolu Üniversitesi Sosyal Bilimler Dergisi, 20(2), s. 127-142.
- Çabuk Ezgi, 2020, Avrupa Birliği düzenlemeleri ışığında Türk hukukunda kişisel verilerin korunması, Yüksek Lisans Tezi, Bahçeşehir Üniversitesi, Sosyal Bilimler Enstitüsü, İstanbul.
- Doğan Buse (2019), Kişisel Verilerin İşlenme Şartları Bağlamında Açık Rıza, Yüksek Lisans Tezi, İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü, İstanbul.
- Dülger Murat Volkan, (2018), “İnsan Hakları ve Temel Hak ve Özgürlükler Bağlamında Kişisel Verilerin Korunması”, İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi, 5(1), s. 71-143.
- Dülger Murat Volkan (2019), “Avrupa Birliği Veri Koruma Tüzüğü Bağlamında Kişisel Verilerin Korunması”, Yaşar Hukuk Dergisi, 1(2), s. 71-174.
- Erel Gürbüz İrem (2021), Sağlık Hukukunda Kişisel Verilerin Korunması, Yüksek Lisans Tezi, Kocaeli Üniversitesi, Sosyal Bilimler Enstitüsü, Kocaeli.
- Ergün Ömer (2017), “Kişilik Kavramı ve Çeşitleri”, Dicle Üniversitesi Adalet Meslek Yüksekokulu Dicle Adalet Dergisi, 1(1), 1-14.
- Gonzalez Gloria Fuster (2014), “The Emergence of Personal Data Protection as a Fundamental Right of the EU”, The Cambridge Law Journal, 74(02), s. 74-375.
- Güner Tülay Selin (2021), Kişisel Verilerin İşlenmesine Yönelik Olarak Açık Rıza Verilmesi ve Açık Rıza Beyanında Bulunma Ehliyeti, Yüksek Lisans Tezi, Eskişehir Üniversitesi, Sosyal Bilimler Enstitüsü, Eskişehir.
- Gürpınar Damla (2017), “Kişisel Verilerin Korunamamasından Kaynaklanan Hukuki Sorumluluk”, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, 19(2), s. 679-694.
- Habip Oğuz, (2014), “Elektronik Ortamda Kişisel verilerin Korunması, Bazı Ülke Uygulamaları ve Ülkemizdeki Durum”, Uyuşmazlık Mahkemesi Dergisi, 0(3), s. 1-38
- Helvacı Serap, Aydın Gülşah Sinem, (2017), ”Kişilik Hakkı İhlalinden Doğan Vekaletsiz İşgörmeye Kusurun Bir Şart Olarak Aranıp Aranmayacağı Sorunu”, MUHF, HAD, 23(1), s. 266-301.
- İmançlı Canan (2019), Kişisel Sağlık Verilerinin Korunamamasından Doğan Özel Hukuk Sorumluluğu, Yüksek Lisans Tezi, İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü, İstanbul.

- Islam Toriqul, Karim Mohammad Ershadul (2019) “A brief historical account of global data privacy regulations and the lessons for Malaysiya”, Journal of History Department, University of Malaya, 28(2), s. 169-186.
- Jagner Edward J (2003), “Privacy Property, Information Costs and the Anticommons”, Hastings Law Journal, 54(4), 899-929.
- Kanf Jerry (2004), “Information Privacy in Cyberspace Transactions”, Standorf Law Review, 50, s. 1193- 1294?
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=631723, E.T.: 10.09.2022.
- Kaşak Fahri Erdem (2020), “Tüzel Kişilik Kavramı ve Tüzel Kişilik Perdesinin Kaldırılması”, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, 26(2), 1242-1263.
- Kaya Cemil (2011), “Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi”, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, 69(1-2), 317-324.
- Kılınç Doğan (2012), “Anayasal Bir Hak Olarak Kişisel Verilerin Korunması”, Ankara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, 61(3), 1089 – 1172.
- Koç Elif Gizem (2020), Kişisel Verilerin korunmasında Veri Soeumlusunun Medeni Hukuktan doğan Sorumluluğu, Yüksek Lisans Tezi, Marmara Üniversitesi, Sosyal Bilimler Enstitüsü, İstanbul.
- Kurt Leyla Müjde (2011), “Ceninin Mal Varlığı Hakları”, İnönü Üniversitesi Hukuk Fakültesi Dergisi, 2(1), 196-203.
- Memiş Tekin (2017), “Veri Sorumlusu ve Veri İşleyen Arasındaki İlişkiler ve Sorumluluk Düzeni”, Beykent Üniversitesi Hukuk Fakültesi Dergisi, 3(6), s. 9-23.
- Leej Riccardi (1983) “The German Federal Data Protection Act of 1977: Protecting the Right to Privacy?”, Boston College International and Comparative Law Review, 1983, 6(1), s. 243-271.
- Ovalıoğlu Senem (2021), Avrupa Birliği hukukunda Kişisel Verilerin Korunması, Yüksek Lisans Tezi, Dokuz Eylül Üniversitesi, Sosyal Bilimler Enstitüsü, İzmir.
- Özel Kadir Can, (2020) “Ana Hatlarıyla Kişisel Verilerin Korunmasının Tarihsel Süreci ile Amacı ve Kişisel Verilerin Korunması Hakkı”, İstanbul Barosu Dergisi, 94(2), s. 241-256.
- Prins J.E.J (2004), “The Propertization of Personal Data and Identities”, Electronic Journal of Comparative Law, 8(3).

- Resmi Gazete, 04.12.2020, Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi Yönetmeliği”, Sayı 28363.
- Resmi Gazete, 21.06.2019, Kişisel Sağlık Verileri Hakkında Yönetmelik, Sayı 30808.
- Resmi Gazete, 10.03.2018, Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ”, Sayı 30356.
- Resmi Gazete, 10.03.2018, Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ, Sayı: 30356.
- Resmi Gazete, 27.10.2017, Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik, Sayı 30224
- Resmi Gazete, 30.12.2017, Veri Sorumluları Sicili Hakkında Yönetmelik, Sayı 30286.
- Resmi Gazete, 12.01.2011, Hukuk Muhakemeleri Kanunu, Sayı 27836.
- Resmi Gazete, 26.06.2004, 5187 Sayılı Basın Kanunu, Sayı 25504.
- Resmi Gazete, 10.11.1984, 3071 Sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun, Sayı 18571
- Salihpaşaoğlu Yaşar, (2013), “Özel Hayatın Kapsamı: Avrupa İnsan Hakları Mahkemesi İçtihatları Kapsamında Bir Değerlendirme”, Gazi Üniversitesi Hukuk Fakültesi Dergisi, 17(3), s. 227-266
- Saygı Samet (2020),”6698 Sayılı Kanun’un Sistematiğinde Yargısal Başvuru Yolları”, Kişisel Verileri Koruma Dergisi, 2(2), s. 30-61.
- Schwartz Paul (1989), “The Computer in German and American Constitutional Law:
- Sefer Oğuz (2018), “Kişisel Verilerin Korunması Hukukunun Genel İlkeleri”, Bilgi ve Ekonomi Yönetimi Dergisi, 13 (2), s. 121-138.
- Selek Ozan (2019), “Genel Veri Koruma Tüzüğü Işığında Kişisel Verilerin İşlenmesinde Rıza Açıklaması”, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, 21(2), s. 911-951.
- Serozan Rona (1997), “Kişilik hakkının korunmasıyla ilgili bazı düşünceler”, İstanbul Üniversitesi Mukayeseli Hukuk Araştırmaları Dergisi, 11(14), s. 93-112.
- Soysal Tamer (2019), “Unutulma hakkının Avrupa Birliği’nin Genel Veri Koruma Tüzüğü Çerçevesinde İncelenmesi”, 0(13), s. 339-422.

- Tapan Mehmet Nuri (1998) “Avrupa Birliđi (AB) Hukukunun Kaynakları ve Ulusal Hukuka Etkileri: Avrupa Adalet Divanı”, Türkiye Barolar Birliđi Dergisi, Sayı: 3. 971-1020.
- Tolun Yüksel (2020), Kişisel Verilerin KVKK ve GVKT Kapsamında Korunması, Yüksek Lisans Tezi, Kırıkkale Üniversitesi, Sosyal Bilimler Enstitüsü, Kırıkkale.
- Tortop Nuri (2000) “Çağımızın Önemli Sorunu: Kişisel Bilgilerin Güvenliđi Sorunu”, Amme İdaresi Dergisi, 33(3), 1-14.
- Towards an American Right of Informational Self-Determination”, The American Journal of Comparative Law, 37(4), s. 675-701.
- Uçak Murat (2021), “Kişisel Verilerin Hukuka Uygun İşlenmesinde Çocuğın Rızası”, Kişisel Verilerin Koruma Dergisi, 3(1), s. 41-60.
- Uzun Fatih Burak, (2016), “Gerçek Kişilerin Hak Ehliyeti ve Hak Ehliyetine Uygulanacak Hukukun Tespiti”, Hacettepe Hukuk Fakültesi Dergisi, 6(2), s.11-48.
- Üzeltürk H. (2018), “Avrupa Birliđi Genel Veri Koruma Düzenlemesi”, Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, 15(2), 161-179
- Yosif Umniyahashgar (2021), “Kişisel Verilerin İşlenmesi Şartları ve 6698 sayılı Kişisel Verilerin Korunması Kanununun ruhu olarak Genel İlkeler”, Selçuk Üniversitesi Adalet Meslek Yüksekokulu Dergisi, 4(1), s. 1-22.
- Yücedağ Nafiye (2017), “Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu’nun Uygulama Alanı Ve Genel Hukuka Uygunluk Sebepleri”, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, 72(2), s. 765-790.
- Yüksel Mehmet, (2003), “Mahremiyet hakkı ve Sosyo – Tarihsel Gelişimi”, 58(01), https://doi.org/10.1501/SBFder_0000001619, E.T.: 23.07.2022
- Yüzbaşı Tobaz Firdevs, 2021, Uluslararası İnsan Hakları Hukukunda ve Türk Hukukunda Kişisel Verilerin Korunması, Doktora Tezi, Trabzon Üniversitesi, Lisansüstü Eğitim Enstitüsü, Trabzon.
- Zeybek Ünsal Çağrı, “Google’ın Yeni Gizlilik Politikası Google Inc. Tarafından 1 Mart 2012 Tarihinde Yayınlanan Politikasının Kişisel Verilerin Korunması ile Uyumluluđu ve Avrupa Birliđinin 95/46/EC Sayılı Veri Koruma Direktifi Açısından Değerlendirilmesi”, Hacettepe Üniversitesi Hukuk Fakültesi Dergisi, 3(1), 99-124

3. Elektronik Kaynaklar

A Guide for Policy Engagement on Data Protection, Part 3 – “Data Protection Principles”, Data Protection Principles, E.T.: 04.09.2022.

Anayasa Mahkemesi, Basın Duyurusu, 29.07.2021, Başkasına Ait Bilgilerin Sosyal Medya Hesabında Paylaşılması Nedeniyle Kişisel Verilerin Korunmasını İsteme Hakkının İhlal Edilmesi | Anayasa Mahkemesi, E.T.: 11.09.2022

Article 29 Working Party (2018), https://edpb.europa.eu/about-edpb/more-about-edpb/article-29-working-party_en, E.T.: 11.07.2022

Article 29, Working Party (2017), Guidelines for identifying a controller or processor’s lead supervisory authority, <https://ec.europa.eu/newsroom/article29/items/611235/en>, E.T.: 10.09.2022

Article 29 Working Party (2016), “Guidelines on the right to data portability”, https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf, E.T.: 29.04.2022.

Article 29 Working Party (2010), Opinion 1/2010 on the concepts of “controller” and “processor”, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf, E.T.: 16.04.2022

Article 29 Working Party, (2014), “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.: 24.04.2022.

Article 29 Working Party (2007), Working Document on the processing of personal data relating to health in electronic health records, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp131_en.pdf, E.T.: 24.04.2022.

Bart van der Sloot , Data Protection and Privacy: (In)visibilities and Infrastructures, “Legal fundamentalism: is data protection really a fundamental right?”, https://link.springer.com/chapter/10.1007/978-3-319-50796-5_1, E.T.: 25.07.2022.

Cambridge Dictionary, <https://dictionary.cambridge.org/dictionary/english/personal>, E.T.: 11.09.2022

“Code of Justinian (Codex Justinianus)”, <http://thelatinlibrary.com/law/institutes.html>, E.T.: 28.01.2022.

Council of Europe, “Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 1981, Details of Treaty No.108, E.T.: 10.09.2022

Data Protection Commission (DPC) (2019), “Quick Guide to the Principles of Data Protection”, Quick Guide to the Principles of Data Protection, E.T.: 04.09.2022.

Data Protection Commission (DPC) (2020), Guidance note on cookies and other tracking technologies, E.T.: 10.09.2022.

Data Protection WP (2007), 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.: 31.10.2021

Data Protection WP (2005), 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.: 04.12.2021.

Datastreams (2017), “Explicit vs. unambiguous consent: what’s the difference?” <https://www.datastreams.io/explicit-vs-unambiguous-consent-whats-the-difference/>, E.T.: 20.04.2022

EDPB (2019), Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - Version for public consultation, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) Version 2.1 12 November 2019 E.T.: 25.04.2022

EDPB (2020), Guidelines 05/20 Consent under Regulation 2016/679, Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1, E.T.: 05.09.2022.

EDPB, Guidelines, Recommendations, Best Practices, https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_en, E.T. 10.09.2022.

EDPB, Rules of Procedure (2018), EUROPEAN DATA PROTECTION BOARD RULES OF PROCEDURE, E.T.: 10.09.2022

EDPB, Role of the EDPB, https://edpb.europa.eu/role-edpb_en, E.T.: 31.08.2022.

EDPB, https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_en, E.T. 31.08.2022.

EDPB (2019), 1 year GDPR – taking stock, https://edpb.europa.eu/news/news/2019/1-year-gdpr-taking-stock_en, E.T.: 11.09.2022.

European Commission, “Adequacy decisions”, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en, E.T.: 21.04.2022

European Commission (2012), Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses, https://ec.europa.eu/commission/presscorner/detail/en/IP_12_46, E.T.: 14.04.2022

European Commission, “What are Data Protection Authorities (DPAs)?”, What are Data Protection Authorities (DPAs)? | European Commission, E.T.: 10.09.2022

European Commission, “Adequacy decisions”, Adequacy decisions | European Commission, E.T.: 11.09.2022.

European Commission (2012), “Viviane Reding Vice-President of the European Commission, EU Justice Commissioner The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age Innovation Conference Digital, Life, Design”, https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_12_26, E.T.: 10.09.2022.

European Commission, What is the European Data Protection Board (EDPB)?, E.T.: 10.09.2021

European Convention on Human Rights (1953), <https://www.echr.coe.int/Pages/home.aspx?p=basictexts&c>, E.T.: 16.04.2022

European Court of Human Rights (2021), “Factsheet – Religious symbols and clothing”, https://www.echr.coe.int/documents/fs_religious_symbols_eng.pdf, E.T.: 03.09.2022.

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.: 11.09.2022

European Union, 2022, “Sources and Scope of European Union Law”, https://www.europarl.europa.eu/ftu/pdf/en/FTU_1.2.1.pdf, E.T.: 03.09.2022.

European Union, “Types of legislation”, https://european-union.europa.eu/institutions-law-budget/law/types-legislation_en, E.T.: 03.09.2022.

Federal Data Protection Act, https://www.gesetze-im-internet.de/englisch_bdsch/englisch_bdsch.html#p0338, E.T.: 03.05.2022.

GDPR, Recital 38, <https://www.privacy-regulation.eu/en/recital-38-GDPR.htm>, E.T.: 04.09.2022

GDPR Recital 43, <https://www.privacy-regulation.eu/en/r43.htm>, E.T.: 14.08.2022.

GDPR, Recital 46, <https://www.privacy-regulation.eu/en/recital-46-GDPR.htm>, E.T.: 14.08.2022

GDPR, Recital 58, <https://www.privacy-regulation.eu/en/recital-58-GDPR.htm>, E.T.: 04.09.2022.

GDPR, Recital 68, <https://www.privacy-regulation.eu/en/recital-68-GDPR.htm>, E.T.: 11.09.2022.

GDPR, Recital 85, <https://www.privacy-regulation.eu/en/recital-85-GDPR.htm>, E.T.: 01.09.2022.

GDPR, Recital 139, <https://www.privacy-regulation.eu/en/recital-139-GDPR.htm>, E.T.: 10.09.2022

GDPR, Recital 140, <https://www.privacy-regulation.eu/en/recital-140-GDPR.htm>, E.T.: 10.09.2022

GDPR, Recital 141, <https://www.privacy-regulation.eu/en/recital-141-GDPR.htm>, E.T.: 10.09.2022.

GDPR, Recital 143, <https://www.privacy-regulation.eu/en/recital-143-GDPR.htm>, E.T.: 10.09.2022.

Gernot Fritz, Nadja Paulus, “CJEU rules on joint controllership – what does this mean for companies?”, Freshfields Bruckhaus Deringer LLP, <https://technologyquotient.freshfields.com/post/102f0aw/cjeu-rules-on-joint-controllership-what-does-this-mean-for-companies>, E.T.: 25.04.2022.

Handbook on European Data Protection (2018), https://www.echr.coe.int/documents/handbook_data_protection_eng.pdf, E.T.: 16.04.2022.

History of data privacy (2021), <https://www.accountablehq.com/post/history-of-data-privacy-laws>, E.T.: 30.01.2022.

Information Commissioner's Office, What does it mean if you are joint controllers?”, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-GDPR/controllers-and-processors/what-does-it-mean-if-you-are-joint-controllers/>, E.T.: 25.04.2022.

Information Commissioner’s Office, Children and GDPR, What are the rules about an ISS and consent? | ICO, E.T.: 04.09.2022.

Jenna Kersten, “What is GDPR Personal Data and Who is a GDPR Data Subject?”, What is GDPR Personal Data and Who is a GDPR Data Subject? | GDPR Compliance, E.T.: 16.04.2022

Kişisel Verileri Koruma Kurumu, 100 Soruda Kişisel Verilerin Korunması Kanunu, Ankara, KVKK Yayınları, 2018, 100 Soruda Kişisel Verilerin Korunması Kanunu, E.T.: 17.04.2022.

Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu, 2016, https://www.tbmm.gov.tr/develop/owa/tasari_teklif_sd.onerge_bilgileri?kanunlar_sira_no=193635, E.T.: 23.04.2022.

Kişisel Verileri Koruma Kurumu, Açık Rıza Alırken Dikkat Edilecek Hususlar, KİŞİSEL VERİLERİ KORUMA KURUMU | KVKK | Açık Rıza Alırken Dikkat Edilecek Hususlar, E.T.: 31.08.2022

Kişisel Verileri Koruma Kurumu, Açık Rıza Rehberi, AÇIK RIZA, E.T.: 31.08.2022

Kişisel Verileri Koruma Kurumu (2018), Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi, AYDINLATMA YÜKÜMLÜLÜĞÜNÜN YERİNE GETİRİLMESİ REHBERİ, Ankara, KVKK Yayınları, E.T.: 27.04.2022

Kişisel Verileri Koruma Kurumu (2019), Kişisel Veri İşleme Envanteri Hazırlama Rehberi, Ankara, KİŞİSEL VERİ İŞLEME ENVANTERİ HAZIRLAMA REHBERİ, E.T.: 28.04.2022

Kişisel Verileri Koruma Kurumu (2020), 6698 sayılı Kişisel Verilerin Korunması Kanunu Hakkında Doğru Bilinen Yanlışlar, Yayın: 31, Ankara. 6698 SAYILI KİŞİSEL VERİLERİN KORUNMASI KANUNU HAKKINDA DOĞRU BİLİNE YANLIŞLAR, E.T.: 18.04.2022

Kişisel Verileri Koruma Kurumu, Kamoyu Duyurusu, KİŞİSEL VERİLERİ KORUMA KURUMU | KVKK | WHATSAPP UYGULAMASI HAKKINDA YÜRÜTÜLEN RESEN İNCELEMeye İLİŞKİN KAMUOYU DUYURUSU, E.T.: 25.07.2022

Kişisel Verileri Koruma Kurumu (2018), Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler), Yayınları, Ankara, https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf, E.T.: 28.04.2022.

Kişisel Verileri Koruma Kurumu (2019), Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi, Ankara, <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/41784a70-2bac-4e4a-830f-35c628468646.PDF>, E.T.: 04.05.2022

Kişisel Verileri Koruma Kurumu, Kişisel Verilerin Korunması Hukuku Bilgilendirme Rehberi, <https://www.hku.edu.tr/wp-content/uploads/2019/04/kvkk-kitapcik.pdf>, E.T.: 31.08.2022.

Kişisel Verileri Koruma Kurumu (2017), Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi, Ankara, KİŞİSEL VERİLERİN SİLİNMESİ, YOK EDİLMESİ veya ANONİM HALE GETİRİLMESİ REHBERİ, E.T.: 18.04.2022.

Kişisel Verileri Koruma Kurumu (2019), “Madde ve Gerekçesi ile KVKK ve Kişisel Verilerin Korunmasına İlişkin Terimler Sözlüğü”, Ankara, Madde ve

Gerekçesi ile Kişisel Verilerin Korunması Kanunu (Bilgi Notu) ve Kişisel Verilerin Korunmasına İlişkin Terimler Sözlüğü, E.T.: 31.08.2022

Kişisel Verileri Koruma Kurumu (2019), Örneklerle Kişisel Verilerin Korunması, Ankara, ÖRNEKLERLE KİŞİSEL VERİLERİN KORUNMASI, E.T.: 09.11.2021.

Kişisel Verileri Koruma Kurumu, “Yurtdışına Veri Aktarımında Veri Sorumlularınca Hazırlanacak Taahhütnamede Yer Alacak Asgari Unsurlar”, <https://www.kvkk.gov.tr/Icerik/4236/Yurtdisina-Veri-Aktariminda-Veri-Sorumlularinca-Hazirlanacak-Taahhutnamede-Yer-Alacak-Asgari-Unsurlar>, E.T.: 23.04.2022

Kişisel Verileri Koruma Kurumu, Yurtdışına Aktarım, <https://www.kvkk.gov.tr/Icerik/2053/Yurtdisina-Aktarim>, E.T.: 23.04.2022.

Lievens Eva (2018), Verdoodt Valerie, “Looking for needles in a haystack: Key issues affecting children's rights in the General Data Protection Regulation”, Computer Law & Security Review, <http://isiarticles.com/bundles/Article/pre/pdf/114185.pdf>, E.T.: 20.04.2022.

Mário Fernandes, Alberto Rodrigues da Silva, António Gonçalves, “Specification of Personal Data Protection Requirements: Analysis of Legal Requirements based on the GDPR Regulation” (2019), <https://www.scitepress.org/Papers/2018/68106/68106.pdf>, E.T.: 16.04.2022

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”), 2013, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, E.T. 11.09.2022

P. M. Schwartz, “Information Privacy in the Cloud”, University of Pennsylvania Law Review, Cilt 161, s. 1623-1662, https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1024&context=penn_law_review, E.T.: 31.07.2022.

Supereeth Shastri, Wasserman Melissa, Chidambaram Vijay, “The seven sins of personal-data processing systems under GDPR”, <https://www.usenix.org/system/files/hotcloud19-paper-shastri.pdf>, E.T.: 16.04.2022

SSRN Electronic Journal, “GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy?”, 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3212210, E.T.: 18.04.2022

Statista Research Department, “Global number of quarterly data breaches 2021-2022”, 2022, Data breaches worldwide quarterly 2022 | Statista, E.T.: 11.09.2022.

The Evolution Of Data Storage,
<https://www.securedatarecovery.com/infographics/the-evolution-of-data-storage>, E.T.: 31.07.2022.

Treaty on the Functioning of the European Union (TFEU), 2012, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT>, E.T.: 10.09.2022.

Torre Lydia F de la (2018)“What is ‘personal data’ under EU data protection law?”, <https://medium.com/golden-data/what-is-personal-data-under-eu-data-protection-law-a9983fb2e483>, E.T.: 16.04.2022.

Torre, Lydia F de la (2019), “The right to restrict processing under EU data protection law”, <https://medium.com/golden-data/what-is-the-right-to-restrict-processing-under-eu-data-b6627db1319f>, E.T.: 16.04.2022.

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

Türkiye Yılı İlerleme Raporları, (2013, 2014, 2015) https://www.ab.gov.tr/ilerleme-raporlari_46224.html, E.T.: 24.07.2022

4. Bölgesel ve Uluslararası Mahkeme Kararları

Anayasa Mahkemesi Kararı, 28.09.2017,
<https://normkararlarbilgibankasi.anayasa.gov.tr/Dosyalar/Kararlar/KararPDF/2017-143-nrm.pdf>, E.T.: 28.04.2022.

Anayasa Mahkemesi Kararı , 09.04.2014,
<https://normkararlarbilgibankasi.anayasa.gov.tr/Dosyalar/Kararlar/KararPDF/2014-74-nrm.pdf>, E.T.: 11.09.2022.

Bundesverfassungsgericht, No. 1 BvR 209/83, 15.12.1983,
Bundesverfassungsgericht - Decisions - Decision on the constitutionality of the 1983 Census Act , E.T: 20.01.2022.

CJEU, *Directive 95/46 / EC - Scope - Publication of personal data on the Internet - Place of publication - Concept of transfer of personal data to third countries - Freedom of expression - Compatibility with directive 95 / 46 stronger protection of personal data by the legislation of a Member State*”, C-101/01, 06.11.2003, 62001CJ0101 - EN - EUR-Lex, E.T.: 10.09.2022

CJEU, European Commission v. Republic of Austria, C-614/10, 16.10.2012,
<https://fra.europa.eu/en/caselaw-reference/cjeu-c-61410-judgment#deeplink1>,
E.T.: 02.05.2022.

CJEU, Maximilian Schrems v. Data Protection Commissioner, C-362/14,
06.10.2022, <https://curia.europa.eu/juris/liste.jsf?num=C-362/14>, E.T.:
02.05.2022.

CJEU, Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v. Rīgas
pašvaldības SIA ‘Rīgas satiksme’, C-13/16, 04.05.2017,
[https://curia.europa.eu/juris/document/document.jsf?text=&docid=190322&do](https://curia.europa.eu/juris/document/document.jsf?text=&docid=190322&doclang=EN)
[clang=EN](https://curia.europa.eu/juris/document/document.jsf?text=&docid=190322&doclang=EN), E.T.: 07.09.2022.

CNIL, 2021-023, 31.12.2021, , Deliberation of the restricted committee No. SAN-
2021-023 of 31 December 2021 concerning GOOGLE LLC and GOOGLE
IRELAND LIMITED, E.T.: 25.07.2022.

CNIL, 2020-018, 08.12.2020,
<https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042848036>, E.T.:
25.07.2022.

Decision of the EEA Joint Committee, No 154/2018, 06.07.2018, <https://eur-lex.europa.eu/legal-content/GA/ALL/?uri=CELEX:22018D1022>, E.T.:
21.04.2022

EctHR, “Ciubotaru v. Moldova”, No. 27138/04, 27.04.2010,
[https://hudoc.echr.coe.int/fre#{%22itemid%22:\[%22001-98445%22\]}](https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-98445%22]}), E.T.
29.04.2022.

EctHR, “Peruzzo and Martens v. Germany” No. 7841/08 and 57900/12, 04.06.2013,
[https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-121998%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-121998%22]}), E.T.
04.09.2022

EctHR, “P.N. v. Germany”, No. 74440/17 , 16.11.2020,
[https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-202758%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-202758%22]}), E.T.:
04.09.2022.

Danıştay, 10. Daire, E. 2005,8407, K. 2007,6526, T. 28.12.2005, Künyeli kararı.

Danıştay, 10. Daire, E. 1994/5314, K.1996/294, T. 31.01.1996, Künyeli kararı.

Kurul Kararı, 10.03.2022, <https://www.kvkk.gov.tr/Icerik/7296/2022-224>, E.T.:
05.09.2022

Kurul Kararı, 09.06.2021, <https://www.kvkk.gov.tr/Icerik/6986/2021-571>, E.T.:
28.04.2022.

Kurul Kararı, 04.11.2021, <https://www.kvkk.gov.tr/Icerik/7267/2021-1127>, E.T.:
06.08.2022

Kurul Kararı, 09.07.2020, <https://www.kvkk.gov.tr/Icerik/5412/Acik-Rizinin-Hizmet-Sartina-Baglanmasi>, E.T.: 24.04.2022.

Kurul Kararı, 01.12.2020, <https://kvkk.gov.tr/Icerik/6872/2020-915>, E.T.: 12.07.2022.

Kurul Kararı, 24.01.2019, <https://www.kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirimi>, E.T.: 28.04.2022.

Kurul Kararı, 25.03.2019, <https://www.kvkk.gov.tr/Icerik/5434/2019-78>, E.T.: 21.04.2022.

Kurul Kararı, 31.05.2019, <https://www.kvkk.gov.tr/Icerik/5495/2019-162>, E.T.: 24.04.2022.

Kurul Kararı, 31.05.2019, <https://www.kvkk.gov.tr/Icerik/5494/2019-159>, E.T.: 31.08.2022

Kurul Kararı, 08.07.2019, <https://www.kvkk.gov.tr/Icerik/5517/2019-204>, E.T.: 24.04.2022.

Kurul Kararı, 18.09.2019, <https://www.kvkk.gov.tr/Icerik/5545/2019-277>, E.T.: 22.04.2022.

Kurul Kararı, 18.09.2019, <https://kvkk.gov.tr/Icerik/6710/2019-273>, E.T.: 29.04.2022

Kurul Kararı, 01.10.2019, <https://www.kvkk.gov.tr/Icerik/6556/2019-294>, E.T.: 22.04.2022.

Kurul Kararı, 30.10.2019, <https://www.kvkk.gov.tr/Icerik/6876/2019-316>, E.T.: 12.07.2022.

Kurul Kararı, 17.11.2019, <https://www.kvkk.gov.tr/Icerik/6623/2019-331>, E.T.: 25.04.2022.

Kurul Kararı, 26.12.2019, <https://www.kvkk.gov.tr/Icerik/6668/2019-389>, E.T.: 21.04.2022.

Kurul Kararı, 02.04.2018, <https://kvkk.gov.tr/Icerik/4233/2018-32>, E.T.: 28.04.2022.

Kurul Kararı, 05.12.2018, <https://www.kvkk.gov.tr/Icerik/5424/2018-142>, E.T.:23.04.2022.

Yargıtay, 4. Hukuk Dairesi, 2000/1501 E, 2000/1501K, 15.01.2001 T, Kazancı Bilgi ve İtihat Bankası, E.T.: 10.09.2022.