T.C
DOKUZ EYLÜL ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI
AVRUPA BİRLİĞİ HUKUKU PROGRAMI
YÜKSEK LİSANS TEZİ

AVRUPA BİRLİĞİ HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASI VE TÜRK HUKUKU İLE KARŞILAŞTIRILMASI

Mert KANALICI

Danışman
Doç. Dr. Ali Gümrah TOKER

İZMİR – 2022

TEZ ONAY SAYFASI

YEMİN METNİ

Yüksek lisans tezi olarak sunduğum “Avrupa Birliği Hukukunda Kişisel Verilerin Korunması ve Türk Hukuku ile Karşılaştırılması” adlı çalışmanın, tarafımdan akademik kurallara ve etik değerlere uygun olarak yazıldığını ve yararlandığım eserlerin kaynakçada gösterilenlerden oluştuğunu, bunlara atıf yapılarak yararlanılmış olduğunu belirtir ve bunu onurumla doğrularım.

…/…./2022

Mert KANALICI

ÖZET

Yüksek Lisans Tezi

Avrupa Birliği Hukukunda Kişisel Verilerin Korunması ve Türk Hukuku ile Karşılaştırılması

Mert KANALICI

Dokuz Eylül Üniversitesi

Sosyal Bilimler Enstitüsü

Kamu Hukuku Anabilim Dalı

Avrupa Birliği Hukuku Programı

Bir kişiye ait kimliği belirli veya belirlenebilir kılan her türlü bilgi kişisel veridir. Bilişim teknolojilerindeki gelişmeler sonucunda günümüzde kişisel veriler işlenmesi çok büyük boyutlara ulaşmıştır. Bu nedenle kişisel verilerin korunması gereksinimi doğarak kişisel verilerin korunması hakkı ortaya çıkmıştır. Çalışmamızda bu gereksinimler gözetilerek kişisel verilerle ilgili temel kavramlar açıklandıktan sonra kişisel verilerin tarihsel süreçteki korunması ihtiyacı, hukuki niteliği, kişisel verilerin işlenmesinde temel ilkeler ve veri sahibinin hakları irdelenmiş, sonrasında Avrupa Birliği ve uluslararası düzenlemelerde kişisel verilerin korunması hakkı incelenerek Türk Hukukunda yer alan yasal düzenlemeler çerçevesinde mukayese ve farklılıkları tespit edilerek örnek yargı kararları doğrultusunda görüş ve eleştirilere yer verilmiştir.

Çalışmamız üç ana başlıktan oluşmakta olup, Birinci Bölümde; kişisel verilerin korunmasına ilişkin genel açıklamalar, İkinci Bölümde; Uluslararası kaynaklar ve Avrupa Birliği kaynaklarında kişisel verilerin korunması, Üçüncü Bölümde ise; Türk Hukukunda kişisel verilerin korunması hakkı incelenmiştir.

Anahtar Kelimeler: Kişisel Veri, Özel Nitelikte Veri, Kişisel Verilerin Korunması, Veri Güvenliği, Avrupa Birliği Veri Koruma Tüzüğü, 6698 Sayılı Kişisel Verilerin Korunması Kanunu, 95/46/EC sayılı Direktif.

ABSTRACT

Master's Thesis

Protection of Personal Data in European Union Law and Comparison with Turkish Law

Mert KANALICI

Dokuz Eylül University

Graduate School of Social Sciences

Department of Public Law

European Union Law Program

Any information that makes a person's identity specific or identifiable is personal data. As a result of the developments in information technologies, the processing of personal data has reached enormous dimensions today, in this case, the need for the protection of personal data has revealed the right to protect personal data. In our study, after explaining the basic concepts related to personal data by considering these requirements, the need for the protection of personal data in the historical process, its legal nature, the basic principles in the processing of personal data and the rights of the data owner were examined. Comparisons and differences were determined and opinions and criticisms were included in line with sample judicial decisions.

Our study consists of three main titles, in the First Chapter; General explanations on the protection of personal data are in the Second Section; Protection of personal data in international sources and European Union sources, and in the Third Part; The right to the protection of personal data in Turkish Law has been examined and studies have been made.

Keywords: Personal Data, Private Data, Protection of Personal Data, Data Security, European Union Data Protection Regulation, Personal Data Protection Law No. 6698, Directive 95/46/EC.

AVRUPA BİRLİĞİ HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASI VE TÜRK HUKUKU İLE KARŞILAŞTIRILMASI

İÇİNDEKİLER

İKİNCİ BÖLÜM
ULUSLARARASI HUKUKTA VE AVRUPA BİRLİĞİ HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASI

ÜÇÜNCÜ BÖLÜM
TÜRK HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASI

KISALTMALAR

AB	Avrupa Birliği
ABAD	Avrupa Birliği Adalet Divanı
ABD	Amerika Birleşik Devletleri
AİHM	Avrupa İnsan Hakları Mahkemesi
AİHS	Avrupa İnsan Hakları Sözleşmesi
AGİ	Asgari Geçim İndirimi
AYM	Anayasa Mahkemesi
Bkz.	Bakınız
CMK	Ceza Muhakemeleri Kanunu
CNIL	Hürriyetler ve Bilişim Ulusal Komisyonu
Çalışma Grubu	Madde 29 Veri Koruma Çalışma Grubu
E.	Esas
GVKT	Genel Veri Koruma Tüzüğü
İİK	İcra İflas Kanunu
K.	Karar
KVK İmha Yönetmeliği	Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Haline Getirilmesi Hakkında Yönetmelik
KVKK	6698 Sayılı Kişisel Verilerin Korunması Kanunu
KVK Kurulu	Kişisel Verileri Koruma Kurulu
KVK Kurumu	Kişisel Verileri Koruma Kurumu
md.	Madde
NSA	Amerika Ulusal Güvenlik Teşkilatı
OECD	Ekonomik Kalkınma ve İş Birliği Örgütü
R. G	Resmî Gazete
s.	Sayfa
T.	Tarih
T.C	Türkiye Cumhuriyeti
TBK	Türk Borçlar Kanunu
TDK	Türk Dil Kurumu
TMK	Türk Medeni Kanunu
TCK	Türk Ceza Kanunu
TÜİK	Türkiye İstatistik Kurumu

TTK	Türk Ticaret Kanunu
Vb.	Ve Benzeri
VERBİS	Veri Sorumluları Sicili
VSSHY	Veri Sorumluları Sicili Hakkında Yönetmelik
VSBT	Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ
YHGK	Yargıtay Hukuk Genel Kurulu
108 sayılı Sözleşme	Kişisel Verilerin Otomatik İşleme Tabi Tutulmasında Bireylerin Korunmasına Dair Avrupa Konseyi Sözleşmesi

GİRİŞ

Bilgisayarın icadı ve internetin keşfiyle bilişim sistemlerindeki hızlı gelişmeler neticesinde içinde bulunduğumuz çağda veri işlenmesi kaçınılmaz hale gelmiştir. Günümüzde kişisel veriler her an işlenerek ticaret, bankacılık, eğitim, sağlık gibi hayatın her alanında kişilere hizmet sağlanarak bilgi toplanmakta, veriler aracılığıyla kişi davranış biçimleri akıllı sistemler tarafından izlenerek veri tabanlarında kayıt altına alınmaktadır.

Kayıt altına alınan veriler büyük veri uygulamaları ve akıllı sistemler tarafından yapılan algoritmalarla hayatımızı kolaylaştırmakla birlikte; bu verilerin usulüne uygun olarak tutulmaması, veri güvenliğinin sağlanamaması hallerinde kişisel verilerin yetkisiz ve kötü niyetli üçüncü kişilerin eline geçmesi kişisel verilerin korunması ve özel hayatın gizliliği hakkı olmak üzere kişinin bir takım anayasal haklarının tehlike altına alarak özgürlüklerin ihlaline sebep olma risklerini de beraberinde getirmiştir. Bu sebeple, devletler ve uluslararası topluluklar etkili ve yeterli korumanın sağlanarak kişi mahremiyeti gözetilip, verilerin işlenmesi için kişisel verilerin korunması mevzuatı oluşturma çabasına girmişlerdir. Çalışmamızda uluslararası örgütlerin, Avrupa Birliğinin ve Türkiye Cumhuriyeti'nin kişisel verilerin korunması hakkı kapsamında bu çabası incelenerek çeşitli türlerde farklı düzenlemeler açıklanıp mukayese edilerek incelenecektir.

Çalışmamızın birinci bölümünde kişisel verilerin korunması için temel kavramlara, tarihsel süreç içerisinde kişisel verilerin korunması ihtiyacıyla, kişisel verilerin hukuki niteliği, kişisel verilere ilişkin temel ilkeler, veri sahibinin hakları, kişisel verilerin işlenmesinde yer alan aktörler ilişkin kavramlar açıklanarak Avrupa Birliğinde ki mevzuat ve Türk Hukukunda düzenlemelerin karşılaştırmaları yapılarak çeşitli görüş ve eleştirilere yer verilerek yargı kararları da gözetilerek inceleme yapılacaktır.

Çalışmamızın ikinci bölümünde uluslararası kaynaklarda kişisel verilerin korunmasına ilişkin düzenlemelere yer verildikten sonra Avrupa Birliği Hukukunda kişisel verilere ilişkin düzenlemeler incelenerek, Avrupa Birliği Hukukunda kişisel verilerin korunmasına ilişkin ayrıntılı bir çalışma yapılarak Türk Hukuku ile Avrupa Birliğinde ki mevzuatlar kıyas edilerek çeşitli görüş ve eleştirilere yer verilecektir.

Çalışmamızın son bölümü olan üçüncü bölümünde ise Türk Hukukunda kişisel verilerin korunmasına ilişkin olarak başta 6698 Sayılı Kişisel Verileri Korunması Kanunu olmak üzere çeşitli diğer mevzuatlar incelenerek Türk Hukukunda kişisel verilerin korunması, kanunun kapsamı-kapsamının istisnaları, kişisel verilerin

işlenmesinde hukuka uygunluk halleri, Türk hukukunda kişisel verilerin korunması yolları, yargı kararları çeşitli görüş ve eleştirilerin katkısı ile incelenerek ele alınacaktır.

BİRİNCİ BÖLÜM
KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN GENEL AÇIKLAMALAR

I. KİŞİSEL VERİLERLE İLGİLİ TEMEL KAVRAMLAR

A. Kişisel Veri Kavramının Tanımı

Kişisel veri kavramının tanımının yapılması kişinin hak ve özgürlüklerinin korunması açısından önem arz etmesi sebebiyle, içerik ve sınırlarının belirlenmesi hem kişi hak ve özgürlüklerinin korunması hem de bu konuda ortaya çıkacak ihtilaf ve kuralların belirlenmesi açısından bir gerekliliği ortaya koymaktadır. Kişisel veri kavramına ilişkin hem öğretide de hem de uluslararası ve ulusal metinlerde yapılmış birçok tanım mevcuttur.

Kişisel veri kavramı ilk olarak Türkiye'nin 1981 yılında imzaladığı 2016 yılında onayladığı[1] ve taraf olduğu 108 *sayılı "Kişisel Verilerin Otomatik İşlemesi Karşısında Bireylerin Korunması Sözleşmesi"* nin tanımlar başlıklı 2. maddesinde (2.md) "*kişisel veriler kimliği belirli veya belirlenebilir bir gerçek kişi (ilgili kişi) hakkında ki tüm bilgileri ifade eder*." şeklinde tanımlanmıştır[2].

1995 tarihli ve 95/46/EC Sayılı Yönerge gerçek kişilerin kişisel mahremiyet hakları başta olmak üzere temel hak ve özgürlüklerini koruyarak Avrupa Birliği (AB) iç pazarında kişisel verilerin korunmasına ilişkin yeknesak bir düzenleme oluşturmak maksadıyla hazırlanan Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Hakkında ki Avrupa Birliği Konseyi ve Avrupa Parlamentosu Direktifinin *"Tanımlar"* başlıklı 2.md. "*Kişisel Veri*" tanımlanmış veya tanımlanabilir bir gerçek kişi ('veri sahibi') ile ilgili herhangi bir bilgi olarak ifade edilmiştir[3].

Avrupa Birliği tarafından 95/46/EC sayılı Yönergenin yerini almak maksadıyla 14.04.2016 tarihinde kabul edilen ve 25.05.2018 tarihinde yürürlüğe giren Avrupa Veri Koruma Tüzüğünün (GVKT) "*Tanımlar*" başlıklı 4.maddesinde kişisel veri

---

[1] 6669 sayılı Kişisel Verilerin Otomatik İşlemesi Karşısında Bireylerin Korunması Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun, R.G. 18.02.2016 – Sayı. 29628.

[2] 108 sayılı Kişisel Verilerin Otomatik İşlemesi Karşısında Bireylerin Korunması Sözleşmesi, R.G. 17.03.2016 – Sayı.29656.

[3] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML, (17.12.2020).

"*tanımlanmış veya tanımlanabilir bir gerçek kişiye ilişkin her türlü bilgidir."* şeklinde ifade edilmiştir[4].

6698 Sayılı Kişisel Verilerin Korunması Kanununun (KVKK) 3/1.maddesinin (d) bendinde yine kişisel veri "*kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi*" şeklinde tanımlanmıştır [5].

Açıklanan tanımlardan yola çıkıldığında uluslararası ve ulusal mevzuatta kişisel verilerin *"kişilere ilişkin her türlü bilgi"* şeklinde tanımlandığı ve kişisel verilerin tanımında bir görüş birliği olduğu sonucuna varılabilir.

Kişisel veri; belirli veya belirlenebilir bir kimsenin kimliğine, etnik kökenine, fiziksel özelliklerine, sağlık durumuna, genetik verilerine, öğrenim veya istihdam durumuna, ikamet adresine, kredi kartı bilgilerine, banka ve sigorta kayıtlarına, adli arşiv ve genel bilgi toplama kayıtlarına, düşünce ve inançlarına, alışveriş alışkanlıklarına, telefon rehberine, fotoğrafına, parmak izine, e-postalar, sosyal paylaşım sitelerinde ki aktivitelerine, en son gittiği restoran, bar ya da müzeye kadar ilgisi olduğu ve kişiyi tanımlayan her türlü bilgidir[6].

Uluslararası ve ulusal düzenlemeler deki kişisel veri tanımlarından yola çıkarak kişilere ilişkin her türlü bilginin kişisel veri sayılabilmesi için 3 temel unsur bulunmaktadır. Bunlar; *"bilgi"*, *"kimliği belirli veya belirlenebilir bir kişi*" ve *"bilginin kişiye ilişkin olması*" unsurlarıdır.

B. Kişisel Verilerin Unsurları

Bu başlık altında kişisel verilerin üç unsuru "bilgi", "kimliği belirli veya belirlenebilir bir kişi" ve "bilginin kişiye ilişkin olması" kavramları sırası ile incelenecektir.

1. Bilgi

Kişisel verilerin unsurları bakımından bilginin ne anlama geldiğini ifade ederken bilgi ve veri kavramlarına ayrı ayrı değinmekte fayda olduğunu

[4] https://eur-lex.europa.eu/legal, (17.12.2020).
[5] 6698 Sayılı Kişisel Verilerin Korunması Kanunu, R.G. 24.03.2016- Sayı. 29677.
[6] Aydın Akgül, **Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması,** Beta Yayınları, İstanbul, 2014, ss.8-9.; Nilgün Başalp, **Kişisel Verilerin Korunması ve Saklanması**, Yetkin Yayıncılık, Ankara, 2004, s.22.

düşünmekteyiz. Bilgi; Türk Dil Kurumu (TDK) sözlüğünde kişinin veriye yönelttiği anlam olarak tanımlanmıştır[7].

Veri kavramı ise TDK da *"Gözlem ve deneye dayalı araştırmanın sonuçları"* olarak tanımlanırken[8]; öğretide "*bilişim sistemleri üzerinde işlem yapılabildiği, bu işlemlere dayalı sonuçlar üretilebildiği, saklayabildiği, sakladıklarını sonra tekrar okuyup işleyebildiği ve diğer bilişim sistemlerine iletebildiği her türlü bilgi"* [9] ve sonuç çıkarılabilecek olgu, bilgi ve sayılardan oluşan bilgisayar sistemi tarafından işlenen ham materyali tanımlamak için kullanıldığı ifade edilmiştir[10]. Veri, bilgiden daha geniş bir kapsamı ifade etmekte olup, anlamlı bir hale gelebilen veriler bir bilgi oluşturabilir. Bilgi ve veri kavramları aynı anlama gelmese de günümüzde bu kullanım yerleşmiş olduğundan bu çalışma da her iki sözcük birbiri yerine aynı anlamda kullanılacaktır.

GVKT, 95/46/EC sayılı Yönerge ve KVKK da kişisel veri tanımlanırken *"her türlü bilgi"* ifadesi yer almaktadır. Buradaki her türlü bilgi kavramı geniş yorumlanmalıdır. Bu bilgi kişinin siyasi, ailevi, özel, iş hayatına ilişkin olabilir. Bilginin öznel veya nesnelliği; doğru veyahut yanlış olmasının kişisel veri olma hususuna bir etkisi bulunmamaktadır. Kişinin yaşı, kilosu, saç-ten rengi gibi nesnel bilgilerin dışında güzel, çirkin gibi öznel değerlendirmeleri içeren bilgiler de kişisel veridir. Bu bilgilerin doğruluğunun kanıtlanmasının da bir önemi bulunmamaktadır. Örneğin, kişinin doğum yerinin çalıştığı işyerinde herkesçe aynı yer olarak bilindiği ve kişinin asıl doğum yerinin bilinen yerden farklı olduğunu düşünelim. Bu durumda işyerinde çalışan bir kişinin diğer bir kişiye "doğum yeri M ilçesi olan kişi" bilgisinin verilmesi M ilçesinde doğmuş olan başka bir çalışanın olmaması ve bilgiyi alan kişinin bu bilgi sayesinde hakkında yanlış doğum yeri bilinen kişiye ulaşabilmesi halinde kişisel veriden söz edilir[11]. Bu durumda işyerinde kişiyi belirlenebilir kılan yanlış bilgi de kişisel veridir.

Kişisel veri; alfabetik, sayısal, grafiksel, foto grafik, akustik bir biçimde var olabilir. Kâğıt üzerinde tutulan veriler dışında bilgisayar ortamında tutulan bilgiler de kişisel veri olabilir. Örneğin; müşteri hizmetlerini arayan müşterinin ses kaydının alınması, güvenlik kamerası ile görüntülenen kişinin tanınabilir durumda olduğunu

[7] Türk Dil Kurumu Güncel Türkçe Sözcük, https://sozluk.gov.tr/,(17.12.2020).
[8] Türk Dil Kurumu Güncel Türkçe Sözcük, https://sozluk.gov.tr/,(15.04.2021).
[9] Murat Volkan Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku**, 7 Baskı, Seçkin Yayıncılık, Ankara, 2018, ss. 78-79.
[10] Elif Küzeci, **Kişisel Verilerin Korunması**, 4. Baskı, On iki Levha Yayıncılık, İstanbul, 2020, s.11.
[11] Dülger, s.156.

gösteren görüntü kayıtları, velayet davasında ailesine ilişkin çocuğa çizdirilen çizim kişisel veri olarak kabul edilebilmektedir[12].

2. Kimliği Belirli veya Belirlenebilir Kişi

Kişisel verilerin ikinci unsuru, kimliği belirli veya belirlenebilir kişi kavramıdır. Bu sebeple ilk olarak genel anlamda hukukta kişi kavramından bahsedilmesi gerekmektedir.

95/46/EC Sayılı Yönerge de veri sahibi bireyin gerçek kişi olması gerektiği ifade edilmiştir. Tüzel kişilerin 95/46/EC Sayılı Yönerge de kişisel verileri korunmamış fakat üye devletlerin tüzel kişileri de koruma kapsamına alacak yasal düzenlemeler yapmasının önünde bir engel bulunmadığı ifade edilmiştir. Kişilerin belirli veya belirlenebilir olması unsuru GVKT'nin tanımlar başlıklı 4.maddesinde *"tanımlanmış bir gerçek kişi özellikle bir isim, kimlik numarası, konum verileri, çevrimiçi tanımlayıcı ya da söz konusu gerçek kişinin fiziksel, fizyolojik, genetik, ruhsal, ekonomik, kültürel veya toplumsal kimliğine özgü bir ya da daha fazla sayıda faktöre atıfta bulunularak doğrudan veya dolaylı olarak tanımlanabilen bir kişidir*" şeklinde ifade edilmiştir. GVKT de; 95/46/EC Sayılı Yönergeye paralel olarak kişisel verilerin yalnızca gerçek kişilere ait veriler olduğu ifade edilmiştir.

Kişisel verilerin korunması hakkının öznesinin gerçek kişi olmasının sebebi kişisel verilerin korunması ihtiyacının özünde özel hayatın korunması ilkesinin olduğunun düşünülmesidir[13]. Özel hayatın korunması hakkı gerçek kişilere ait bir haktır ve bu sebeple tüzel kişiler bu hakkın süjesi değildirler[14]. Fakat bu noktada tüzel kişiye ait verilerin gerçek kişi ile ilişkilendirilebilir nitelikte olması halinde korunup korunmayacağı hususu akla gelmektedir. Tüzel kişilere ait veri ile gerçek kişiler belirli veya belirlenebilir hale geliyor ise bu verilerin kişisel veri olarak korunması gerekir[15]. Örneğin; bir veri tabanında şirketin ticaret unvanı ve adresi ile birlikte çalışanlarının ismi yazıyor ise kişinin işyeri ve işyeri adresi belirli hale geldiğinden bu veriler kişisel veri olarak kabul edilebilecektir[16].

---

[12] Kişisel Verileri Koruma Kurumu, **Örneklerle Kişisel Verilerin Korunması**, KVKK Yayınları No:29, Ankara, 2019, s.2.
[13] Küzeci, s.78; Dülger, s.81.
[14] Oğuz Şimşek, **Anayasa Hukukunda Kişisel Verilerin Korunması**, Seçkin Yayınları, Ankara, 2008, s.123.
[15] Dülger, s.172.
[16] Armağan Ebru Bozkurt Yüksel, **Bulut Bilişiminde Kişisel Verilerin Korunması**, Yetkin Yayınları, Ankara, 2016, s.89.

Türk Hukukunda 4721 Sayılı Türk Medeni Kanunu (TMK) 28md.[17] gerçek kişinin kişilik hakkının ne zaman başlayacağı ve sona ereceği belirtilmiştir. TMK da doğumla kazanılan ve ölümle sona eren kişilik hakkı 95/46/EC Sayılı Yönerge ve GVKT ile yapılan düzenlemeler ile paraleldir. Doğumla başlayan kişilik hakkı, ölümle birlikte sona ermektedir. Ölmüş kişiye ilişkin veriler kişisel veri sayılmayarak, 95/46/EC Sayılı Yönerge ve GVKT ile koruma altına alınmamıştır. Fakat bu noktada ölmüş kişilerin kişisel verilerinin yakınlarına ilişkin olup olmadığının değerlendirilmesi gerekmektedir. Ölmüş kişinin yakınları ile ilgili veriler yakınları için kişisel veri niteliği kazanabilirler[18]. Örneğin; bir kişinin ölen babası ile olan fotoğrafı o kişinin anıları ile ilgili olduğundan o kişi içinde ölen babasının fotoğrafı kişisel veri sayılarak o bireyin kişisel verilerin korunması hukukundan yararlanmasını gerektirebilecektir[19].

Kişisel verilerin belirlenebilir olmasına ilişkin Avrupa Birliği Adalet Divanı (ABAD)'ın birçok kararı da mevcuttur. ABAD farklı kararlarında çalışma saatlerinin, kişinin kameraya kaydedilen resminin, vergi beyannamelerinin, kişinin paylaşılan bilgiler ışığında kolayca tespit edilmesine yarayacak basın açıklamasında yer alan bilgilerinin kişisel veri niteliği taşıyacağına karar vermiştir [20].

Kişinin kimliğinin belirli veya belirlenebilir olması her somut olayın özelliğine göre farklılık gösteren ve dikkat edilmesi gereken bir husustur.

3. Bilginin Kişiye İlişkin Olması

Kişisel verinin uluslararası veya ulusal mevzuatlar uyarınca korunması için diğer bir unsuru bilginin kişiye ilişkin olduğunun tespitidir. Elde edilen bilgiler ile belirli veya belirlenebilir kişi arasında nedensellik bağının olması, bilginin o kişiye ait olmasının anlaşıldığı durumlarda bu bilgiler kişisel veri olarak kabul edilecektir[21]. Elde edilen bilgiler ile kişi belirlenemiyor ise yani kişi ile bilgi arasında bir illiyet bağı yok ise

---

[17] 4721 Sayılı Türk Medeni Kanunu, R.G. 08.12.2001 – Sayı.24607.
"Madde 28- Kişilik, çocuğun sağ olarak tamamıyla doğduğu anda başlar ve ölümle sona erer. Çocuk hak ehliyetini, sağ doğmak koşuluyla, ana rahmine düştüğü andan başlayarak elde eder."

[18] Murat Uçak, "Kişisel Verilerin Ölümden Sonra Korunması", **İstanbul Medeniyet Üniversitesi Hukuk Fakültesi Dergisi,** Cilt:6, Sayı:10, 2021, ss.113-114.

[19] Dülger, s.173.

[20] 01.10.2015, C-201/14 (Bara), 24.11.2011, C-70/10, (Scarlett Extend) kn.51. Ayrıca bkz. Mesut Serdar Çekin, **Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku**, 3. Baskı, On İki Levha Yayıncılık, İstanbul, 2020, s.46.

[21] Murat Uçak, "Kişisel Verilerin Korunması Hukukunun Genel İlkeleri", **Bilgi Ekonomisi ve Yönetimi Dergisi**, Cilt:13, Sayı:2, 2018, s.121.

bu bilginin toplanması, işlenip, saklanması kişisel verilerin korunması hukuku kapsamında değerlendirilemeyecektir. Örneğin, personel dosyalarında yer alan verilerin orada çalışan kişilere ait olduğu açık olup bilgi ile kişi arasında illiyet bağı bulunduğundan bu verilerin kişisel veri olduğu değerlendirilebilecektir.

Bazı durumlarda bilgi ile kişi arasında bağlantı kurmak zor olabilir. Bu gibi durumlarda somut olayın özelliğine göre eldeki veri ile kişi arasında illiyet bağının olup olmadığı; eldeki veri ile kişinin belirlenebilir olup olmadığına bakılması gerektiği değerlendirilmektedir. Örneğin, nesneye ilişkin kişisel veriler doğrudan kişiyi belirlenebilir kılmamakla birlikte, kişiyi tanımlayabileceğinden o kişiye ilişkin kişisel veri olarak kabul edilebilir. Bir araba servisinde bilgisayar sistemine kaydedilen araç plakası nesneye ilişkin bir veridir. Araç plakası nesneye ilişkin veri olmasına rağmen aracın plaka bilgileri bilgisayara girildiğinde kişilerin ne kadar yolculuk yaptıkları, ne şekilde kaza yaptıkları gibi bilgilere ulaşılması halinde bu veri kişiyi belirlenebilir kıldığından kişisel veri olarak kabul edilebilecektir[22].

Avrupa birliği bünyesinde 95/46/EC Sayılı Yönergenin 29md. uyarınca 29.Madde Veri Koruma Grubu (Çalışma Grubu) kurulmuştur. Bu kurul bağımsız bir danışma organı olarak görev yapmakta olup, bugüne kadar kişisel verilerin korunması konusunda çeşitli çalışmalar ve raporlar hazırlamış, teori ve uygulamaya ışık tutmuştur[23]. Çalışma Grubu bilginin kişiye ait olmasına ilişkin "*bir bilgi kişinin kimliğine, karakterine veya davranışlarına gönderme yapıyorsa ya da bu bilgi kişinin nasıl muamele göreceği ya da değerlendirileceğini belirlemede kullanılıyorsa kişiye ilişkindir."*[24] şeklinde tespitte bulunmuştur. Çalışma Grubu bu tespitini, müşteriye daha iyi ve çabuk hizmet vermek isteyen ve bu sebeple müşteriye en yakın taksiyi müşterinin adresine yönlendiren sistemde, sistemin amacının taksi de ki sürücü ile ilgili olmamakla birlikte; taksi sürücülerinin hız limitlerine uyup uymadığı, güzergahlarının bilgisinin bulunması halinde, bu bilgilerin taksicinin davranışlarına gönderme yapması sebebi ile kişisel veri olarak kabul edilebileceğini örnek göstererek açıklamıştır[25].

---

[22] Dülger, ss.168-170.

[23] 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.121.; Küzeci, s.177.

[24]https://ec.europa.eu/justice/article-29/documentation/opinion recommendation/files/2005/wp105_en.pdf , (19.01.2020), s.8.

[25]https://www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf, (19.01.2020), s.11.

C. Hassas (Özel Nitelikli) Kişisel Veriler

Hassas veya özel nitelikli kişisel veriler; uluslararası veya ulusal mevzuatta kişisel verilerden ayrı bir başlık altında düzenlenmiştir. Bu tip veriler genel anlamda kişisel verilerden niteliği ve önemi itibari ile daha fazla korunmasına ihtiyaç duyulan verilerdir. Bazı verilerin hassas veriler olarak adlandırılıp, özel düzenlemelerle korunmasının sebebi bu verilerin kişinin temel hak ve özgürlükleriyle ilgili olmasından kaynaklanmaktadır. Söz konusu hassas verilerin kötüye kullanılması halinde ilgili kişinin bu durumdan ciddi anlamda zarar görme ihtimali mevcuttur[26]. Örneğin, kişilerin etnik ırkı ve dini kökeni hassas kişisel verilerdir. Kişinin etnik ırkı veya dini kökeni hakkında kaydedilen kişisel verilerin kötüye kullanılması halinde; kişi toplum içerisinde ayrımcılığa maruz kalabilecektir. Hassas verilere ilişkin İngiltere de Naomi Campbell ile The Mirror gazetesi arasında görülmüş davada, Mahkeme, siyahi manken Campbell'ın tedavi için gittiği merkezin önünde çekilen fotoğraflarının mozaiklenmesine rağmen ten rengi nedeni ile kolayca tanınıyor olması açısından Campbell'ın etnik kökenine ilişkin bilgiler içermesi sebebi ile fotoğrafın hassas nitelikli kişisel veri olduğunu tespit etmiştir[27].

Konuya ilişkin uluslararası ve ulusal düzenlemelere değinmek gerekirse; 108 Sayılı Sözleşmenin 6.md kişiye ilişkin ırksal köken, siyasi düşünce, dini ve diğer inançları, sağlık ve cinsel hayat, ceza mahkumiyetine ilişkin bilgilerin özel nitelikli kişisel veri olduğu ve otomatik işleme tabi tutulamayacağı belirtilmiştir. 108 sayılı Sözleşme de hassas bilgiler belirtilerek bu verilerin otomatik olarak işlenemeyeceği özel olarak düzenlenmiştir.

95/46/EC sayılı Yönergenin 8.maddesi, 108 sayılı Sözleşmeye paralel olarak; üye devletlerin kişilerin sağlık durumu, cinsel tercihi, sendika üyeliği, dini ve felsefi inancı, siyasi görüşleri, ırk ve etnik kökeni hassas nitelikli kişisel veri olarak sayılmıştır.

GVKT'nin 9.maddesi kişiye ilişkin yine etnik köken, siyasi görüş, felsefi ve dini inanç, sağlık, cinsel tercihleri hassas nitelikli kişisel veri olarak tanımlanmış, burada 95/46/EC sayılı Direktif ve 108 Sayılı Sözleşmeden farklı olarak genetik ve biyometrik veriler de hassas nitelikte kişisel veriler olarak kabul edilmiştir.

---

[26] Metin Bulut, "Özel Bir Hukuksal Koruma ve Veri Kategorisi Alanı: Hassas Kişisel Veriler", **Ankara Barosu Dergisi,** Cilt:78, Sayı:3, 2020, s.123.

[27]https://www.theguardian.com/media/2002/mar/27/pressandpublishing.privacy, (18.04.2021).

Görüleceği üzere uluslararası mevzuatlar da genel olarak hassas (özel) nitelikli kişisel veriler sınırlı olarak sayılarak; hassas-hassas olmayan kişisel veri ayrımı yapılmıştır. Fakat bu durum tüm ülkeler tarafından kabul edilen bir ayrım değildir. Örneğin; Federal Almanya Anayasa Mahkemesi 1983 yılında verdiği nüfus sayımı konulu bir kararında kişisel verilerin tamamının önemli olduğunu, "önemli "veya "az önemli" ayrımının yapılamayacağını belirtmiştir[28].

Türk Hukukunda ise; KVKK da özel nitelikli veriler sınırlı olarak sayılmıştır. Kişilerin; ırkı, siyasi düşüncesi, felsefi inancı, dini mezhebi diğer inançları, kılık kıyafeti, dernek-vakıf- sendika üyelikleri, sağlığı, cinsel hayatı, ceza mahkumiyeti ve güvenlik tedbirleri ile ilgili verileri özel nitelikli kişisel veriler olarak ifade edilmiştir.

Hassas nitelikli kişisel veriler artan internet kullanımı sebebi ile son yıllarda daha da önemli bir hale gelmiştir. Bu kapsamda artan internet kullanımı sebebi ile *"tıklama akışlı veriler"*in özel nitelikli kişisel veri olup olmadığını değerlendirmek gerekmektedir. Tıklama akışlı veriler, bir bilgisayar kullanıcısının internette gezinirken veya başka bir yazılım uygulamasını kullanırken tıkladığı ekran bölümlerinin kaydedilmesidir[29]. Tıklama akışlı veriler sayesinde internet sitesini ziyaret eden kişilerin internet profili oluşturulabilmektedir. Tıklama akışlı verilerin de hassas nitelikli kişisel veri olarak kabul edildiği görülmektedir. Örneğin, ABAD bir kararında, kişinin ziyaret ettiği web sitesi aracılığıyla meydana gelen profilinde özel bilgiler bulunuyor ise kişisel verilerin geniş yorumlanması gerektiğinden bahsederek tıklama akışlı verilerin hassas (özel) nitelikte kişisel veriler olabileceğini ifade etmiştir[30].

Kural olarak hassas (özel) kişisel verilerin işlenmesi yasak olmakla birlikte; bu durumun istisnaları ulusal ve uluslararası mevzuatta yer almaktadır. GVKT'nin 9.maddesinde özel nitelikli kişisel verilerin kaydedilmesine ilişkin istisnalara yer verilmiştir.

II. KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ

A. Tarihsel Süreç İçerisinde Kişisel Verilerin Korunması İhtiyacı

İnsanlık tarihi boyunca kişisel veri kavramı bilinme isteği duyulan ve kişi ile kurumlar tarafından merak edilen, önem atfedilen bir kavram olmuştur. Öncelikle

[28] Küzeci, s.281.
[29] https://tr.wikipedia.org/ (25.04.2021).
[30] Case C-101/01, Bodil Lindqvist (ECJ) 2003, par. 49-51 ayrıca bkz. Küzeci, ss.280-281.

bunun sebebi insanda var olan merak duygusu ve bilme isteğidir. Bilgi teknolojilerinin kullanımının artması, teknolojinin ilerlemesi sebebi ile kişisel verilerin bilinme sebepleri siyasi, sosyolojik, ekonomik pek çok farklı sebepten kaynaklanmıştır.

Teknolojinin gelişmesi, özellikle de bilgisayarların ortaya çıkması ile kişisel veriler kolayca saklanıp, elde edilebilen, işlenen veriler haline gelmiştir. Dolayısıyla 1960'lardan itibaren özellikle devlet kurumları tarafından kişisel verileri otomatik olarak işleyen bilgi bankaları oluşturulmaya başlanmıştır. Bu husus aynı zamanda kişinin mahremiyetinin korunması ve devletin birey üzerinde bilgi hakimiyetini sınırlandırması yönünde taleplere sebebiyet vermiştir. Çünkü birey teknolojik gelişmeler sebebi ile gözetlendiğini ve kayıt altında alındığını düşünmeye başlamıştır. Verilerin korunmasına ilişkin ilk yasal düzenleme 1970 yılında Almanya'nın Hessen Eyaletinde yapılmıştır. Hessen Eyaletinde Kişisel Verilerin Korunması Kanunun kabul edilmesine neden olan önemli olay *"Hessen Planı"* programı içerisinde merkezi veri bankasının kurulma tasarısıdır[31]. İlgili kanun ile elektronik işlenen kişisel verilerin yetkisiz üçüncü kişilere karşı korunması, veri işleyen kişilerin sır saklama yükümlülükleri ve ilgili kişinin yanlış veriyi düzeltilmesinin talep etme hakkı düzenlenmiştir[32].

Almanya federal düzeyde ilk düzenlemeyi 1977 tarihinde Federal Koruma Kanunu, Fransa 1978 tarihli Veri İşleme ve Hürriyet Kanunu, Avusturya 1978 tarihinde Federal Kişisel Verilerin Korunması Kanunu, İsviçre 1992 tarihinde Federal Veri Koruma Kanunu, İngiltere ise 1998 tarihinde Veri Koruma Kanunu ile düzenlemiştir[33].

Türk Hukukunda ise kişisel verilerin korunmasına dair yasal düzenlemelerin uzun bir geçmiş tarihi olmamakla birlikte; 5982 sayılı Türkiye Cumhuriyeti Anayasasının Bazı Maddelerinde Değişiklik Yapılması Hakkında Kanunun 2.md çerçevesinde Anayasanın 20.md eklenen üçüncü fıkra ile *"Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir"* ibaresi ile kişisel verilerin korunması bir temel hak olmuştur. 5237 sayılı Türk Ceza Kanunun (TCK) 135 md.[34] kişisel verilerin hukuka aykırı şekilde kaydedilmesi, elde edilmesi, kanunlarda belirtilen süreler geçmesine rağmen yok edilmemesi hallerinde cezai yaptırımlar öngörülmüştür. 07.04.2016 tarihinde ise 6698 sayılı KVKK yasalaştırılmıştır.

Uluslararası ve ulusal mevzuatlarda bu düzenlemelerin yapılmasının sebebi bireyin; toplum içerisinde temel hak ve özgürlükleri rahatça kullanabilmesi, kendini

[31] Küzeci, s.118.
[32] Çekin, s.5.
[33] Çekin, s.6.
[34] 5237 Sayılı Türk Ceza Kanunu, R.G.12.10.2004- Sayı. 25611.

ifade edebilmesi, devlet veya diğer üçüncü kişiler tarafından gözetim ve denetim altında tutulmaması gerekliliğinden kaynaklandığını kanaatindeyiz. Kişisel verilerin korunması ile bireyin özerkliği ve özgür düşünen demokratik bir toplum meydana gelebilecektir. Bu sebeple de zaman içerisinde kişisel veri kavramı düzenlenmesi ve korunması gereken bir hak ve kavram haline gelmiştir.

B. Kişisel Verilerin Hukuki Niteliği

Kişisel verilerin korunması hakkı, kişinin tüm verileri üzerindeki hakimiyetini ifade eder. Kişisel veri kavramının tanımının geniş olması sebebi ile kişisel verilerin korunması hukuku birçok hak ile yakın temas içerisindedir. İnsan onuru, özel hayatın gizliliği, düşünce açıklama özgürlüğü, haberleşme özgürlüğü ve bunun gibi birçok hak kişisel veriler ile iç içe geçmiştir. Bu sebeple kişisel verilerde korunan hak ve amaçlanan çıkarımın ne olduğu konusunda farklı yaklaşımlar bulunmakla birlikte bu konuda iki temel ayrım bulunmaktadır. Bu yaklaşımlardan birincisi kişisel verilerin korunmasının ekonomik bir hak olduğu, ikincisi ise kişisel veri kavramının insan hakları kapsamında değerlendirilmesi görüşüdür[35].

1. Ekonomik Hak Yaklaşımı

Kişisel verilerin korunması hakkını ekonomik hak olarak ele alan yaklaşımlar verinin ekonomik değerine odaklanarak bu hakkı insan hakları bağlamından uzaklaştırmaktadır[36]. Ağırlıklı olarak Amerika Birleşik Devletinde (ABD) savunulan bu yaklaşımlar kişisel verilerin mülkiyet hakkı veya fikri mülkiyet hakkı olduğu görüşüne dayanmaktadır.

a. Mülkiyet Hakkı Görüşü

ABD'de kişisel verilerin korunması anayasal bir hak değildir. Geniş, kapsamlı bir korumanın ekonomiyi olumsuz etkileyeceği görüşünden yola çıkarak kişisel verilerin korunmasına ekonomik değer temelli yaklaşımlar geliştirilmiştir. Bu temel yaklaşımlardan birisi mülkiyet hakkı teorisidir.

---

[35] Sami Sinan Akkurt, "Kişisel Veri Kavramının Hukukî Niteliğine İlişkin Yaklaşımlara Mukayeseli Bir Bakış", **Kişisel Verileri Koruma Dergisi**, Cilt:2, Sayı:1, 2020, ss.21-22.
[36] Sinem Göçmen Uyarer, **Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması**, 2. baskı, Seçkin Yayıncılık, Ankara, 2019, s.23.

Türk hukukunda mülkiyet hakkı bilindiği üzere, kişiye sahip olduğu eşya üzerinde kullanma, yararlanma, tasarruf etmek üzere yetki sağlayan ayni bir haktır[37]. Mülkiyet hakkında bir malın sahibi dilerse bu hakkını başkasına satıp, kiralayabilir. Fakat bir hak mülkiyet hakkına göre devredildikten sonra yeni sahibi o hakkı dilediği gibi kullanarak yine başkasına satabilecektir. Bu sebeple kişinin hakkını devretmesi sonucunda istenmeyen sonuçlar ortaya çıkabilecektir. Devretme özgürlüğü araba, ev gibi menkul ve gayrimenkullerde iyi bir şekilde işlerken aynı şeylerin kişisel veriler için söz konusu olacağını söylemek zordur[38]. Kişisel verilerin niteliği gereği mülkiyet hakkına konu olamayacağı, bu hakka ilişkin tüm sorumluluk ve yetkinin bireylerde olmasının bireyler için geri dönülmez şekilde maddi-manevi zararlara yol açacağı düşüncesi ile eleştirilmektedir[39].

Mülkiyet hakkı teorisinin güçlü yanı, bilgilerin kişi aleyhine kullanılması halinde kişinin doğrudan dava açma veyahut zararın tazminini talep etme hakkı doğurmasıdır. Çünkü mülkiyet hakkı kişiye geniş bir ayni hak verecektir[40].

Kanaatimizce, mülkiyet hakkı teorisine ilişkin eleştirilere katılıyoruz. Kişisel verilerin devredilmesi halinde devreden kişinin bu veriler hakkında söz sahibi olamayacaktır. Bu durumunda kişide mutlak bir zarara yol açacağı aşikârdır. Tüm bunların yanında günümüz de kişilerin kurumlar ile yaptığı alışverişte çoğunlukla güçsüz konumda olup, kişisel verilere ilişkin pazarlığı eşit koşullarda yapamayacağını da düşünmekteyiz. Örneğin; birey, bir devlet kurumunda çalışmak için işe başvurduğunda verilerinden gönüllü olarak vazgeçmek durumunda kalabilecektir. Bu durum bireylerin kişisel verilerinden gönüllü olarak vazgeçmesine kadar giden bir sürece yol açabilecek olup, bu sebeple kişisel verilerin mülkiyet hakkı üzerinden temellendirilmesi oldukça güçtür.

b. Fikri Mülkiyet Hakkı Görüşü

Fikri mülkiyet görüşünün ortaya çıkmasının sebeplerinden biri, fikri mülkiyet hakkının özünde de kişisel verilerdeki gibi bireye ait bir veri olmasıdır. Bir düşünce, fikir, kitap, resim gibi eserler üreten kişi eseri üzerinde manevi haklara sahipse, veri

---

[37] Lale Sirmen, **Eşya Hukuku,** 5. Baskı, Yetkin Yayınları, Ankara, 2018, s.241; Bilge Öztan, **Medeni Hukukun Temel Kavramları**, 30. Baskı, Turhan Kitabevi Yayınları, Ankara,2009, s.664.
[38] Küzeci, s.70.
[39] Dülger, s.79.
[40] Betül Özlük, "Mülkiyet ve Zilyetlik Üzerine Düşünceler", **Selçuk Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:27, Sayı:1, 2019, ss.142-143.

sahibinin de kişisel verileri üzerinde manevi hakları olduğu düşünülmektedir. Bu görüş, kişisel veriler ile telif hakkı arasında bağlantı kurarak kişisel verileri fikri mülkiyet hakkı gibi düşünmektedir[41]. Nasıl ki telif hakkı sahibi eseri üzerinde değişiklik yapılmasını yasaklama yetkisi var ise; kişisel verilerin de aynı şekilde sahibi olduğu kişiye aynı hakları vereceği düşünülmektedir.

Fikri mülkiyet hakkı görüşüne getirilen eleştirilerden biri kişisel verilerle fikri mülkiyet hakkı arasında benzerlik olmadığı yönündedir[42]. Fikri mülkiyette kişi sarf ettiği çaba sonucunda bir ürün, düşünce, kitap, resim üretmekte iken, kişisel verilerde böyle bir çaba söz konusu olmayıp kişisel veriler kişinin yalnızca insan olması sebebi ile kendiliğinden ortaya çıkan, bir çaba gerektirmeksizin oluşan verilerdir. Bir diğer eleştiri ise fikri mülkiyet hakkı ile kişisel verilerin amacına yönelik eleştiridir. Fikri mülkiyet hakkında bireyin bir eser meydana getirmesi teşvik edilerek bir buluşun ortaya çıkması amaçlanırken, kişisel verilerin korunması hukuku kişinin rızası dışında kişisel verilerinin depolanıp, saklanmaması, kullanılmaması üzerine veri dolaşımına ait konuları içermektedir [43].

Kanaatimizce, fikri mülkiyet hakkı ile kişisel verilerin birbirine benzetilmesi uygun değildir. Her iki hakta bireyin kendi özüne ağırlıklı olarak manevi yönüne hitap etmesine rağmen kişisel veriler kendiliğinden oluşan kişinin insan olması sebebi ile meydana gelen veriler iken fikri mülkiyet hakkı kişinin çalışması ve yoğun çabası sonucunda ortaya çıkan bir eserdir. Ayrıca amaç konusunda da fikri mülkiyet hakkının geliştirilmesi için devlet ve kurumlar tarafından çeşitli teşvikler mevcut iken, kişisel verilerin meydana gelmesi için devlet veya kurumların bir teşviki bulunmamaktadır.

2. İnsan Hakkı Yaklaşımı

İnsan hakları, kişinin insan olmasından kaynaklanan bireylerin doğuştan sahip olduğu dokunulmaz, devredilemez haklardır. İnsan hakları uluslararası, ulusal tüm metinlerde yer alan önemli bir konudur. İnsan haklarını üç alt kategori de belirtmek mümkündür[44]. Birinci kuşak haklar, kişi özgürlükleri ve siyasal haklar; ikinci kuşak haklar sosyal, ekonomik hak ve özgürlükler; üçüncü kuşak haklar ise dayanışma

---

[41] Küzeci, s.79.
[42] Akgül, ss.66-67; Hüseyin Can Aksoy, **Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması,** Çakmak Yayınları, Ankara, 2010, s.42.
[43] Çiğdem Ayözger Öngün, **Kişisel Verilerin Korunması Hukuku**, 2. Baskı, Beta Yayıncılık, İstanbul, 2019, ss.17-18.
[44] Aydın Turhan, "İnsan Hakkı Kuşakları Arasındaki Tamamlayıcılık İlişkisi", **İnönü Üniversitesi Hukuk Fakültesi Dergisi,** Cilt:4, Sayı:2, 2013, ss.359-360.

haklarıdır. Kişi özgürlükleri negatif statü hakları olarak da ifade edilmektedir. Negatif statü hakları kişiyi, devlete ve topluma karşı koruyan haklardır. Kişisel verilerin korunması da negatif statü haklarından birisidir [45].

Avrupa ülkelerinde baskın görüş, kişisel verilerin temel insan haklarından olduğu yönündedir[46]. Birleşmiş Milletler Evrensel İnsan Hakları Beyannamesi 17.md, Birleşmiş Milletler Bireysel ve Siyasal Haklar Şartı 12.md, Avrupa İnsan Hakları Sözleşmesi 8.md gibi birçok önemli metinde özel yaşamın gizliliği temel bir insan hakkı olarak kabul edilmiş ve ilk başlarda kişisel verilerin korunması özel hayatın gizliliği hakkının bir alt başlığı olarak düşünülmüştür. Nitekim şu anda ulusal mevzuatımızda kişisel verilerin korunması hakkında Anayasamızın "*Özel Hayatın Gizliliği*" başlıklı 20.md içerisinde bahsedilmektedir.

Tarihsel süreçte kişisel verilerin korunması hakkının, özel hayatın gizliliği hakkından ayrı bir hak olarak değerlendirilerek farklı bir açıdan konuya bakmamızı sağlayan Almanya Anayasa Mahkemesi'nin 15 Aralık 1983 tarihli *"Nüfus Sayımı"* kararıdır. Kararın konusu Almanya Parlamentosu tarafından kabul edilen 1982 tarihli nüfus sayım yasası oluşturmaktadır. Belirtilen yasa uyarınca 1983 yılında memurlar nüfus sayımı yaparken yurttaşların kapsamlı bilgilerinin edinme imkânı elde etmekteydi. Sayım sırasında sorulacak sorular ile kişilerin isim, adres, gelir kaynakları, eğitim durumu gibi verileri açığa çıkarması ve bu verilerin gizli tutulacağı hüküm altına alınmasına rağmen nüfus sayım amacı dışında verilerin kullanılması riskinin yüksek olması eleştirilere yol açmıştır[47]. Kişisel verilerin korunması hususunda kaygılar ortaya çıkmıştır. Almanya Anayasa Mahkemesi Nüfus Sayım yasasını ilk olarak geçici olarak durdurmuş sonrasında bazı hükümleri insan haysiyetinin dokunulmazlığı ve kişiliğini geliştirme hakkına aykırılık oluşturduğuna karar vererek hükümleri iptal etmiştir. Almanya Anayasa Mahkemesince verilen bu karar sonuçları itibariyle önemli bir karardır. Bu karar ile *"bilgilerin geleceğini belirleme hakkı"* türemiştir[48]. Mahkemeye göre anayasal düzenin içerisinde toplumun üyesi olarak kişinin onuru bulunur. Kişi hakkında edinilen bilgilerin neler olduğunu, bu bilgilerin kimin elinde olduğunu bilmeyen bireyin kendi kararlarını verme özgürlüğü önemli ölçüde zarar görür. Sürekli izlenen, yaptıkları kaydedilen bir bireyin kendini serbeste geliştirebilmesi mümkün değildir. Bu kişinin kararları kendisinin verememesi

[45] Doğan Kılınç, "Anayasal Bir Hak Olarak Kişisel Verilerin Korunması", **Ankara Üniversitesi Hukuk Fakültesi Dergisi,** Cilt:61, Sayı:3, 2012, s.1099.
[46] Küzeci, s.74.; Öngün, s.15.
[47] BVerfGE, 65, 1- Volkszahlung, 15 Aralık 1983 ayrıca bkz. Dülger, s.84.
[48] Küzeci, s.76.

ve kendini baskı altında hissetmesi oldukça beklenebilir bir durumdur. Kişisel verilerin hukuka aykırı olarak sürekli kaydedilmesi, işlenmesi, paylaşılması bireye kişisel verilerinin korunması hakkını vererek bireyi özneden nesneye dönüşmesini engelleyecektir[49]. Özetlemek gerekirse; Mahkeme kararında bilgilerin geleceğini belirleme hakkı ile bireye; verilerinin kullanılması hakkında karar verme hakkı tanıdığını belirtmiştir. Alman Anayasa Mahkemesi kararı ile kişisel verilerin korunması hakkı, özel hayatın gizliliği hakkından tamamen ayrı düşünülmese de kişilik hakkının özel bir görünümü olarak ifade edilmiştir[50].

Kişisel verilerin korunması hakkı her ne kadar ilk başta özel hayatın gizliliği hakkı içerisinde değerlendirilmişse de; gelişen teknoloji, kişisel verilerin kullanılması ve korunması ihtiyacını arttırmış özel hayatın gizliliği hakkı kişisel verilerin korunmasında yetersiz kalmıştır. Bu da kişisel veriler üzerinde daha geniş kapsamlı bir korumayı gerektirmiştir. Bununla birlikte kişisel veriler özel hayatın gizliliği kapsamında korunsa da kişinin özel hayatına ilişkin her bilgi kişisel veri değildir. Her kişisel veri de gizli bilgi değildir. Örneğin: kişinin adı kişisel veri kapsamındayken, kişinin özel hayatına ilişkin gizli bir bilgi değildir. Bu sebeple, her ne kadar başlangıçta kişisel verilerin korunması, özel hayatın korunması hakkı kapsamında düşünülmüşse de her iki hak birbirinden farklıdır[51].

Kişisel verilerin korunması hakkı özel yaşamın gizliliği hakkının özelliklerini taşımak ile birlikte kendine özgü gereklilikleri sebebi ile bağımsız bir temel hak olarak algılanmaya başlanmıştır. Nitekim günümüzde kişisel verilerin korunması hakkı, GVKT, AB 2000 Tarihli Temel Haklar Şartı, Lizbon Sözleşmesi ve 108 sayılı Kişisel Verilerin Otomatik İşlemesi Karşısında Bireylerin Korunması Sözleşmesinde bireyler için temel bir hak olarak öngörülmektedir.

C. Kişisel Verilerin İşlenmesi

Kişisel verilerin işlenmesi kavramı, kişisel verilerin; işlenmesi, toplanması, değiştirilmesi, depolanması, silinmesi gibi birçok işlemi kapsayıcı nitelikte geniş bir kavramdır.

---

[49] Şimşek, s.112.
[50] Yaşar SalihPaşaoğlu ve Burcu Değirmencioğlu, “Unutulma Hakkının Bir İnsan Hakkına Dönüşme Yolculuğu”, **Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:24, Sayı:2, 2020, ss:369-371.
[51] Uyarer, s.31.

95/46/EC Sayılı Yönergenin 2/b. maddesine göre kişisel verilerin işlenmesi " *silme veya tahrip etme, engelleme, birleştirme veya sıralama, sağlama veya dağıtma, iletmeyle açıklama, toplama, kaydetme, organizasyon, depolama, adaptasyon ve değiştirme, kurtarma, danışma gibi otomatik veya otomatik olmayan araçlarla kişisel veriler üzerinden yapılan herhangi bir faaliyet veya faaliyet dizisini kastedecektir*." şeklinde ifade edilmiştir.

GVKT'nin 4.maddesinde ise kişisel verilerin işlenmesi kavramı kişisel verileri; elde etme, kaydetme, düzenleme, yapılandırma, depolama, uyarlama, değiştirme, erişme, başvurma, kullanma, yayınlama, yayma, sıralama, sınırlama, silme, imha etme gibi filler olarak sayılmıştır.

Türk Hukukunda ise KVKK 3/e md. ise kişisel verilerin işlenmesi kavramı *"Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem* olarak" ifade edilmiştir.

Tüm bu düzenlemelerden kişisel verilerin işlenmesi genel bir ifade ile "*kişisel verilerin ilk defa elde edilmesinden başlayarak veriler üzerinde gerçekleştirilen tüm işlemleri "ifade ettiği anlaşılmaktadır*[52].

Avrupa birliğindeki kişisel verilerin işlenmesi hakkında düzenlemeler daha ayrıntılı olmakla birlikte, özünde Türk hukukundaki düzenlemeler ile Avrupa Birliği nezdinde yapılan düzenlemeler birbiri ile paraleldir.

GVKT ve KVKK da kişisel verilerin kısmen veya tamamen otomatik olan yollar ile gerçekleştirilmesi kişisel verilerin işlenmesi anlamına gelmektedir. Otomatik olan yollarla işlenen kişisel verilerde veri tamamen sistem aracılığıyla elde edilerek analiz edilip işlenmekteyken, kısmen otomatik işlenen kişisel verilerde kişisel veriler insan müdahalesi ile işlenmektedir. Otomatik olarak işlenmemekle birlikte, bir veri kayıt sisteminin parçası olmak kaydıyla manuel gerçekleştirilen kayıtlar da kişisel verilerin işlenmesidir[53]. Kısaca kişisel verilerin otomatik veya herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenmesi arasında bir fark

---

[52] Kişisel Verilerin Koruma Kurumu, **100 soruda Kişisel Verilerin Korunması Kanunu**, KVKK Yayınları No:3, Ankara, 2019, s.39.

[53] Hüseyin Murat Develioğlu, **6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku**, On İki Levha Yayıncılık, İstanbul, 2017, ss.97-98.

bulunmamakta olup, iki durumda kişisel verilerin işlenmesidir. Örneğin, bir okul kütüphanesinde kitap alan öğrencinin kayıtlarının elle tutulması, otomatik vasıtalar kullanılmasa da bir veri kayıt sisteminin parçası olduğunda kişisel veri işleme olarak kabul edilecektir.

1. Kişisel Verilerin İşlenmesinde Yer Alan Aktörler

Veri işlenmesi faaliyetinde rol oynayan iki önemli aktör bulunmaktadır. Bu aktörler veri işleyen ve veri sorumlusudur. Bu başlık altında her iki aktörlere ilişkin açıklamalar yapılacaktır.

a. Veri Sorumlusu

Veri sorumlusu, kişisel verilerin korunması hukukunda önemli bir aktördür. Veri sorumluları kişisel verilerin işlenme amaç ve vasıtalarını belirleyen veri kayıt sisteminin kurulması ve yönetilmesinden sorumlu olan kişilerdir. Uluslararası mevzuata baktığımızda:

GVKT'nin 4/7. maddesinde veri sorumlusunun; tek başına veya başkaları ile birlikte kişisel verilerin hangi amaçlarla ve nasıl bir yöntem izlenerek işleneceğini belirleyen gerçek, tüzel kişi veya kamu idaresi olabileceği ifade edilmiştir.

KVKK 3.maddesinin (ı) fıkrasında ise veri sorumlusu; kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiler olabileceği ifade edilmiştir.

GVKT ile KVKK büyük oranda birbiri ile paralel olmakla birlikte aralarında birkaç fark bulunmaktadır. GVKT de kamu kurumlarının veri sorumlusu olabileceği belirtilmişken, KVKK da bu konuya ilişkin açık bir düzenleme bulunmamaktadır. GVKT ile KVKK arasındaki bir diğer fark birden fazla veri sorumlusunun bulunduğu durumlardır. Uygulamada, aynı veri işleme fiilinde birden fazla veri sorumlusu bulunabilmektedir. GVKT de ortak veri sorumluluğuna ilişkin hüküm bulunmakta iken KVKK da buna ilişkin bir hüküm bulunmamaktadır[54].

Tanımlardan anlaşılacağı üzere gerçek kişiler, şirket, dernek, vakıf gibi tüzel kişiler veri sorumlusu olabilmektedir. Veri sorumlusunun tanımı uluslararası ve ulusal mevzuatta açık olmakla birlikte, somut olay içerisinde veri sorumlusunun tespiti her zaman kolay olmayabilir. Bu nedenle veri sorumlusunun belirlenmesi için; kişisel

[54] Küzeci, s.365.

verilerin işlenmesi ve işlenmesi yöntemi, işlenecek veri türleri, işlenen kişisel verilerin nerede hangi amaçlarla kullanılacağı, hangi bireylerin kişisel verilerinin toplanacağı, işlenen verilerin başka kişi veya kurumlarla paylaşılıp paylaşılmayacağı, paylaşılacaksa kiminle paylaşılacağı, verilerin ne kadar süreyle muhafaza edileceği gibi ölçütlere dikkat edilmelidir[55]. Veri sorumlusunun kim olduğuna ilişkin örnekler vermek gerekirse:

- Personelin maaşını ödemek için kimlik, iletişim, banka hesap bilgilerini işleyen bir şirket ya da özel kişi hangi kişinin hangi verilerin nasıl işleneceğine kendisi karar vermektedir. Kişisel verilerin neden ve nasıl işlendiğine dair karar veren şirket veya gerçek kişi burada veri sorumlusudur[56].
- Bankacılık sektöründe farklı bankaların bilgi aktardığı bilgi havuzları bakımından ilgili bilgiyi aktaran ve kullanan bankalar ayrı ayrı veri sorumlusudur [57].
- Müşterilerinin iletişim bilgilerini liste halinde tutan firma bu bilgileri bir bulut veri tabanında bulunan kendi kontrolündeki hesaba aktardığında, hala veri sorumlusu kalmaya devam eder. Bulut veri tabanının sahibi firma ise kişisel verilerin işlenmesi amaç ve vasıtalarını belirlemediğinden veri sorumlusu değildir. Ancak bulut veri tabanı sahibi listedeki bilgileri kullanarak bu kişilere reklam mesajları yollar ise, veri sorumlusu olacaktır[58].

b. Veri İşleyen

Veri sorumlusunun kişisel verileri bizzat işlemesi gerekmemektedir. Veri sorumlularının talimatları doğrultusunda kişisel veriler veri işleyen tarafından işlenebilir.

GVKT'nin 4/7. maddesinde veri işleyen; veri sorumlusu adına işleme yapan gerçek veya tüzel kişi, kamu idaresi veya kurumu olabileceği belirtilmiştir.

KVKK 3.maddesinin (ı) fıkrasında veri işleyen; veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi, kamu kurumlarının olabileceği belirtilmiştir.

Tanımlardan anlaşılacağı üzere veri sorumlusu kişisel verilerin işlenmesine ilişkin her türlü karar verme yetki ve sorumluluğuna sahip iken, veri işleyen veri

[55] https://www.kvkk.gov.tr/Icerik/4195/Veri-Sorumlusu-ve-Veri-Isleyen, (14.05.2021).
[56] Kişisel Verilerin Koruma Kurumu, **Örneklerle Kişisel Verilerin Korunması**, KVKK Yayınları No:29, Ankara, 2019, ss.60-61.
[57] Dülger, ss.190-194.
[58] Develioğlu, s.42.

sorumlusunun verdiği talimatlar doğrultusunda hareket eden ondan bağımsız ve ayrı bir gerçek veya tüzel kişidir. Veri işleyen ile veri sorumlusu arasında hukuki bir ilişki söz konusudur. Veri sorumlusunun tüzel kişi olması durumunda verdiği talimatlar doğrultusunda onun adına faaliyet gösteren söz konusu tüzel kişi organizasyonundan ayrı gerçek kişi veya tüzel kişi veri işleyen olabilir[59]. Örneğin, bir özel şirketin, topladığı kişisel verilerin saklanması için bir bulut hizmeti sağlayıcısı ile sözleşme yapması durumunda, bulut hizmeti sağlayıcısı veri işleyen durumundadır. Çünkü taraflar arasındaki sözleşme gereği bulut hizmeti sağlayıcısının verileri kendi amaçları için kullanması mümkün değildir[60]. Ayrıca, bulut hizmeti sağlayıcısının kendisi de veri toplamamaktadır. Bulut hizmet sağlayıcısının faaliyeti özel şirketle aralarında yapılan anlaşma uyarınca onun talimatlarına uygun olarak verileri saklamasıdır[61].

Veri sorumlusu ile veri işleyenin ayırt edilmesi hususu önemli bir konu olup, bu konuda Türk Hukukunda Kişisel Verilerin Korunması Kurulunun (KVK Kurulu) 7 Mayıs 2020 tarihli Yurt Dışına Kişisel Veri Aktarımında Hazırlanacak Taahhütnamelerde Dikkat Edilmesi Gereken Hususlara İlişkin Duyurusunda :

> *Veri işleyenin faaliyetleri, veri işlemenin daha çok teknik kısımları ile ilgilidir. Kişisel verilerin işlenmesine ilişkin kararların alınması yetkisi ise veri sorumlusuna aittir. Veri işleyen, veri sorumlusu adına kişisel verileri işlemekte olup, veri sorumlusunun belirlemiş olduğu temel amaç ve araçlar kapsamında ve veri sorumlusunun verdiği yetki doğrultusunda veri işleme faaliyetini gerçekleştirmektedir. Diğer bir deyişle veri işleyen, veri sorumlusunun çıkarlarını gözeten, kendisine verilen belirli görevleri aldığı talimatlar doğrultusunda yerine getirmekle yükümlü olan taraftır.* ifadelerine yer verilmiştir[62].

Veri işleyen belirleme noktasında en önemli kriterlerden biri, bir veri sorumlusu adına hareket etmek, veri işleyenin verinin işlenmesine doğrudan bir menfaatinin bulunmamasıdır. Veri işleyen, veri sorumlusu adına hareket etmelidir. Örneğin, bir şirket çalışanları için kimlik kartı hazırlatmaktadır. Bu iş için ayrıca hizmet alınan firma şirket çalışanlarının çeşitli bilgilerini işler. Bu işlemlerin tamamı veri sorumlusu işveren adına gerçekleştirildiğinden hizmet veren firma veri işleyendir[63].

---

[59] Turan Gamze Başara, **"Kişisel Veri İşleme Sözleşmesi"**, Uyuşmazlık Mahkemesi Dergisi, Sayı:16, 2020, ss.64-67.

[60] Cengiz Paşaoğlu ve Emel Cevheroğlu, "Bulut Bilişim Sistemleri Kapsamında Kişisel Verilerin Şifreleme Yöntemleri ile Korunması", **Bilişim Teknolojileri Dergisi**, Cilt:13, Sayı:2, 2020, s:191.

[61] Kişisel Verilerin Koruma Kurumu, **Örneklerle Kişisel Verilerin Korunması**, KVKK Yayınları No:29, Ankara, 2019, ss.60-61.

[62]https://www.kvkk.gov.tr/Icerik/6741/YURT-DISINA-KISISEL-VERI-AKTARIMINDA-HAZIRLANACAK-TAAHHUTNAMELERDE-DIKKAT-EDILMESI-GEREKEN-HUSUSLARA-ILISKINDUYURU,(27.12.2020)

[63] Dülger, s.209.

Kişisel Verileri Koruma Kurumu (KVK Kurumu) "Veri Sorumlusu ve Veri İşleyen Rehberi" içeriğinde veri sorumlusunun bazı yetkilerini veri işleyene devredebileceğinden bahsetmiştir. Bu yetkiler, kişisel verilerin toplanması için hangi bilgi teknolojileri sistemlerinin veya diğer metotların kullanılacağı, kişisel verilerin hangi yöntemle saklanacağı, kişisel verilerin korunması için alınacak güvenlik önlemlerinin detayları, kişisel verilerin aktarımının hangi yöntemle yapılacağı, kişisel verilerin saklanmasına ilişkin sürelerin doğru uygulanabilmesi için kullanılacak metot, kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesi yöntemleridir [64].Buradaki sayımlar örnekleme niteliğinde olup, bunlar çoğaltabilecektir.

Veri sorumlusunun bazı yetkilerini veri işleyene devretmesi halinde bu konuda doğan hukuki sorumluluğun kimin üzerinde olduğu da önemli bir problemdir. Veri işleme faaliyetlerinde temel sorumluluk veri sorumlusuna aittir. Veri işleyen sorumlu olsa dahi bu durum veri sorumlusunun sorumluluğunu ortadan kaldırmamaktadır[65]. Nitekim KVKK'nın 12.md veri sorumlusunun kişisel verilerin korunması amacıyla her türlü teknik ve idari tedbirleri almak zorunda olduğu ve bu hususta veri işleyen ile birlikte müştereken sorumlu olduğu ifade edilmiştir.

III. KİŞİSEL VERİLERİN İŞLENMESİNE İLİŞKİN TEMEL İLKELER

Kişisel verilerin korunması için, veriler işlenirken uyulması gereken birtakım ilkeler uluslararası ve ulusal mevzuatta belirlenmiştir. Kişisel verilerin işlenmesine ilişkin temel ilkeler, tüm kişisel veri işleme faaliyetlerinin özünde bulunması gereken veri işleme faaliyetlerinin tüm aşamalarında gözetilmesi gereken ilkelerdir[66]. Bu ilkelerden her biri, kişisel verilerin korunması hukukunda eşit öneme sahip birbirleri ile bağlantılı ilkelerdir.

GVKT 5. maddesinde bu ilkeler*; "hukuka uygunluk", "hakkaniyet ve şeffaflık", "amaca uygunluk", "veri ekonomisi", "doğruluk", "saklama süresinin kısıtlanması" , "bütünlük ve gizlilik", " hesap verilebilirlik"* olarak ifade edilmiştir[67].

KVKK 4.maddesinde ise temel ilkeler; *"hukuka ve dürüstlük kurallarına uygun olma", "doğru ve gerektiğinde güncel olma", "belirli, açık ve meşru amaçlar için*

[64] https://www.kvkk.gov.tr/Icerik/4195/Veri-Sorumlusu-ve-Veri-Isleyen, (27.12.2020)
[65] Küzeci, ss.366-367.
[66] Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin Korunması Kanuna İlişkin Uygulama Rehberi,** KVKK Yayınları No:1**,** Ankara, 2019, s.63.
[67] Bora Gemicioğlu ve Zeynephan Gemicioğlu, **Kişisel Verilerin Korunması Mevzuatı Uluslararası Düzenlemeler ve İçtihatları**, 2.baskı, On iki Levha Yayıncılık, İstanbul, 2019, s.457.

işlenme", "işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma", "ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme" şeklinde ifade edilmiştir.

KVKK ile GVKT arasında farklılıklar bulunsa da genel hatlarıyla birbirine benzer ilkeler kişisel verilerin işlenmesi için belirlenmiştir[68]. Aşağıda öğretide ve mevzuatta genel olarak benimsenen kişisel verilerin korunması hakkına özgü ilkeler ayrıntılı olarak incelenecektir.

A. Hukuka ve Dürüstlük Kurallarına Uygun İşleme

Uluslararası ve ulusal düzenlemelerde kişisel verilerin hukuka ve dürüstlük kurallarına uygun işlenmesi gerektiği ifade edilmektedir. Veri işlemenin hukuka ve dürüstlük kurallarına uygun olması ilkesi veri işleme faaliyetinin temel ilkelerinden biridir.

95/46/EC Sayılı Yönergenin *"Veri Kalitesine İlişkin Prensipler"* başlıklı 6/1. maddesi, 108 Sayılı Sözleşmesinin "*Verilerin Niteliği"* başlıklı 5(a). maddesi, GVKT'nin "*Kişisel Verilerin İşlenmesine Dair İlkeler* " başlıklı 5.maddesi, KVKK "*Genel İlkeler"* başlıklı 4/2(a).maddesi; kişisel verilerin işlenmesi sırasında bu prensibin uygulanması gerektiği ifade edilmiş ve bu ilke kişisel verilerin korunması hukukunun birincil ilkesi olarak değerlendirilmiştir[69]. Bu ilkenin bir başka önemi diğer ilkeleri kapsayıcı genel bir kural niteliğinde olarak, diğer ilkelerin kişisel verilerin işlenmesi ilkelerine uygun olmasından bahsedebilmek için verilerin mutlak surette hukuk ve dürüstlük kurallarına uygun işlenmesi gerekmesidir [70].

Bu ilkeyi değerlendirirken ilkenin iki parçasını ayrı ayrı değerlendirmek gerekmektedir. Bunlardan ilki kişisel verilerin hukuka uygun diğerinin ise kişisel verilerin dürüstlük kurallarına uygun olarak işlenmesi ilkesidir.

Hukuka uygun olma ilkesinden anlaşılması gereken, kişisel verilerin işlenmesinde yasalara, diğer genel hukuk kuralları ve evrensel hukuk ilkelerine uygunluktur. Kişisel verilerin korunması hukuku açısından hukuka uygun bir veri

---

[68]Yosif Umniyahasghar, "Kişisel Verilerin İşlenmesi Şartları Ve 6698 Sayılı Kişisel Verilerin Korunması Kanunun Ruhu Olarak Genel İlkeler", **Selçuk Üniversitesi Adalet Meslek Yüksekokulu Dergisi,** Cilt:4, Sayı:1, 2021, s.20.

[69] İbrahim Korkmaz, **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, Seçkin Yayınları, Ankara, 2017, s.113; Küzeci, s.228.; Uyarer, s.123.

[70] Kişisel Verileri Koruma Kurumu, **KVKK Yayınları, Kişisel Verilerin Korunması Kanunu Hakkında Sıkça Sorulan Sorula**r, Ankara,2019, s.42.

işleme faaliyetinin olabilmesi için işlemin genel hukuk normlarına uygun olmasının yanında kanun ve diğer hukuki düzenlemelere de uygun olması gerekmektedir.

İkinci olarak, kişisel verilerin işlenmesine ilişkin her türlü eylemde dürüstlük kurallarına uyulmalıdır. Dürüstlük kuralı genel bir kavram olup, dürüstlük kuralından TMK 2.maddesinde belirtildiği üzere; tüm bireylerin hukuk düzeninden doğan haklarının kullanıp-yükümlülüklerini yerine getirirken bu eylem ya da işlemleri dürüstlük kuralına uygun olarak yapacakları ve aksi yönde bir davranışın hakkın kötüye kullanılması anlamına gelerek hukuk düzeni tarafından korunmayacağının anlaşılmasıdır. Dürüst davranma ilkesi hak sahibinin hakkını kullanırken veya bir borçlunun borcunu ifa ederken dürüst, makul, fiilinin neticesini bilen, orta zekalı her insanın benzer hadiselerde takip edecek olduğu yolda hareket etmesi anlamına gelmektedir[71].

Kişisel veriler açısından dürüstlük kuralına uygunluk, her kişisel veri işleme faaliyetinde objektif olarak makul bir kimseden beklenecek davranışlar dikkate alınarak objektif özen yükümlülüğüne uygun hareket edilmesidir. Dürüstlük kurallarına uygun olma ilkesi doğrultusunda veri sorumlusu veri işlerken ilgili kişinin çıkarlarını ve makul beklentilerini dikkate almalıdır. Veri sorumlusuna kanun veya diğer yasal mevzuatlarda kişisel verilerin işlenmesi için bir hak veya yükümlülük verilse dahi veri sorumlusu bu veriler için dilediği gibi hareket etmemeli, dürüstlük kuralına aykırı şekilde kişilerin ön göremeyeceği işlemlerde bulunmamalıdır[72].

Kişisel verilerin dürüstlük kuralına uygun olarak işlenmesinden söz edilebilmesi için GVKT de ayrıca veri işleme faaliyetinin şeffaf olması gerektiği ifade edilmiştir[73]. Kişisel verilerin işlenmesi işleminin şeffaf olması, ilgili kişinin kişisel verilerin kim tarafından ve hangi amaçla işlendiğini her halükârda öğrenebilmesinin sağlanmasını ifade etmektedir[74]. KVK Kurulu önüne gelen bir olayda ilgili kişi, ulaşım hizmeti sağlayan Bitaksi uygulaması hakkında yaptığı yolculukların şoförler tarafından puanlandığını öğrenerek, kendi yolculuklarına ait bu puanlara kendisi tarafından ulaşılamaması ve puanlama yapılacağı hususunda veri sorumlusunun aydınlatma metninde herhangi bir bilginin yer almaması sebebiyle KVK Kuruluna başvurmuştur. KVK Kurulu yaptığı incelemede başvuruyu genel ilkeler ve şeffaflık açısından değerlendirerek, müşterilerin/yolcuların yaptığı seyahatlerin şoförler

[71] YHGK,13.07.2011, E.2011/4-410, K.2011/511.; Ahmet Kılıçoğlu, **Borçlar Kanunu**, 12.baskı, Turhan Kitabevi, Ankara, 2011, ss. 115-118.
[72] Dülger, s.266.
[73] Şehriban İpek Aşıkoğlu, "Veri Sorumlularının Aydınlatma Yükümlülüğü Avrupa Birliği ve Türk Hukukunda", **Kişisel Veri Koruma Dergisi,** Cilt:1, Sayı:2, 2019, s.43.
[74] Develioğlu, ss.97-98.

tarafından puanlanmasına ve bu puanların ortalamasının alınmasına dayanan veri işleme faaliyetinin, KVKK 5/2.maddesi (c) fıkrası şartı kapsamında sözleşmenin ifasına ilişkin ana kurucu öğe olmadığı veya sözleşmenin ifasıyla doğrudan doğruya bir ilişkisinin var olmadığını tespit etmiştir. Bu sebeple de KVK Kurulu veri sorumlusunun şeffaflık ilkesine ve ilgili kişiyi aydınlatma yükümlülüğüne aykırı davrandığına hükmetmiştir[75]. Kararda da bahsedildiği üzere dürüstlük kuralına uygun bir veri işleme faaliyetinden bahsedilebilmesi için veri sorumlusunun, aydınlatma yükümlülüğü kapsamında kişisel verilerin hangi amaçlarla işlediğini bu verilerin hangi amaçlarla kimlere aktarılabileceği, kişisel verilerin işlenmesinin sonuçları kapsamında ilgili kişiye bilgi vermesi gerekmektedir.

Veri sorumlusunun hukuka uygun olarak işlediği verileri amacı sona ermesine rağmen silmemesi, yok etmemesi de dürüstlük kurallarına aykırı bir veri işleme faaliyeti olacaktır. Veri sorumlusunun yasal düzenlemelere dayandırmadığı meşru bir amaç ve gerekçesi olmaksızın gerçekleştirdiği her türlü faaliyet dürüstlük kurallarına aykırılık teşkil edecektir. Dürüstlük kuralı gereğince, veri işleme konusunda izin ya da emir veren hukuk kurallarına dayanarak gerçekleştirilen veri işleme fiillerinde, mümkün olan en az miktarda veri işlenmesi gerekmektedir. Haklı bir gerekçe olmaksızın ilgili kişinin özel hayatının gizliliğini, onurunu ihlal edecek şekilde fazla veri işlenmesi şüphesiz bu ilkeye aykırılık teşkil edecektir. Örneğin, veri sorumlusu tarafından işlenmesi gerekmeyen işlenme amacı makul olmayan verinin, ilgili kişiden talep edilerek bu verinin işlenmesi dürüstlük kurallarına aykırılık teşkil edecektir[76].

B. Belirli, Açık ve Meşru Amaçlara Yönelik İşleme

Bu ilke kapsamında kişisel verilerin işlenmesi; verilerin işlenme amacının belirli olmasını ve meşru amaçlarla işlenmesi gerektiğini ifade etmektedir. Amacın meşru olması, amacın yasal dayanağı olduğunu ifade etmekle birlikte dürüstlük ilkesi kapsamında amacın evrensel hukuk ilkeleri ve diğer yasal düzenlemelerle uyum içerisinde olması gerektiği anlamına da gelmektedir. Meşru amaca yönelik işlenen verilerde, veri sorumlusunun yaptığı iş, sunduğu hizmetle bağlantılı ve bunlar için gerekli verilerin işlenmesidir[77]. Örneğin; bir e-ticaret sitesinin, alışveriş yapan kişinin ad, soyadı ve kargo gönderimi için adres bilgilerini işlemesi meşru amaç

[75]https://www.kvkk.gov.tr/Icerik/6717/2020-65,(28.12.2020).
[76] Kişisel Verileri Koruma Kurumu, KVKK Yayınları, **Kişisel Verilerin Korunması Kanunu Hakkında Sıkça Sorulan Sorular**, Ankara, 2019, s.43.
[77] Dülger, s.277.

kapsamındayken, anne kızlık soyadı veya kan grubu bilgisini işlemesi meşru amaç kapsamında değerlendirilemeyecektir. Başka bir örnek verilirse; üniversite de yapılacak bir sempozyuma katılmak için üniversiteye e-posta adresini bildiren kişiye üniversite tarafından e-posta yoluyla reklam içerikli mesajlar gönderilmesi, amaçla sınırlı olma ilkesine aykırılık oluşturacaktır[78].

Kişisel veriler; bireylerin açık rızası alınarak işlenebileceği gibi kanunda belirtilmesi halinde açık rıza aranmaksızın da işlenebilir. Kişisel verilerin bireylerin açık rızası ile işlenmesi halinde bu açık rızanın hukuka uygun olabilmesi için ilgili kişilerin verilerin işlenme amaçları konusunda doğru ve şeffaf şekilde bilgilendirilmesi gerekmektedir. Tam da bu nokta da bireylere açıklanan kişisel verilerin işleme amaçlarının belirli ve açık olması gerekmektedir. Kişisel verilerin hangi amaçlarla, hangi sınırlarla, hangi süreyle işleneceği bireylere açık şekilde ifade edilmelidir[79].

KVK Kurumu tarafından, kişisel veri işleme amaçlarının açıklandığı hukuki işlem ve metinlerde belirlilik ve açıklık ilkesine uygun olarak teknik-hukuk terminoloji kullanılmasından kaçınılması gerektiği ifade edilmiştir[80].

Kişisel verileri işlenen ilgili kişi, veri işleyen kişilerden veyahut kurumlardan hangi amaç için verilerinin toplandığını ve söz konusu amaç için işlenip işlenmediğini öğrenebilme imkanına sahiptir. Amacın meşru olması işlenen kişisel verilerin yasal dayanağı olduğu anlamına gelmektedir.

C. Doğru ve Gerektiğinde Güncel Olma

Bu ilke işlenen kişisel verilerin doğru olarak işlenmesi ve değişen şartlara ve durumlara göre talep edilmesi halinde güncellenmesi ilkesidir. Birçok uluslararası belgede ve iç mevzuatımızda bu ilkeye yer verilmiştir. Kişisel verilerin doğru olarak tutulması ilgili kişinin hakları ile veri sorumlusunun çıkarları ile ilişkilidir[81]. Kişisel verilerin doğru tutulmaması bireyin temel hak ve özgürlüklerini, ekonomik çıkarlarını zedeleyici sonuçlar doğurabilir[82]. Yanlış veriler yanlış sonuçlara yol açabilecektir.

---

[78] Kişisel Verileri Koruma Kurumu, **Örneklerle Kişisel Verilerin Korunması**, KVKK Yayınları No:29, Ankara, 2019, ss.7-8.
[79] Yıldırım Keser, "Tüketicinin Kişisel Verisinin İşlenmesinde Açık Rıza", **Selçuk Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:28, Sayı:3, 2020, ss.1193-1196.; Uyarer, s.126.
[80]https://www.kvkk.gov.tr/Icerik/4189/Kisisel-Verilerin-Islenmesine-Iliskin-Temel-Ilkeler, (21.12.2020), s.8.
[81] Küzeci, s.243.
[82] Miray Özer Deniz, "İşçilerin Özel Nitelikli Kişisel Verilerinin Korunması ve Bundan Doğan Sorumluluk", **Türkiye Adalet Akademisi Dergisi**, Sayı:45, 2021, s.361.

Kişisel verilerin aynı zamanda güncel olarak da tutulması gerekmektedir. Doğru olarak tutulan veriler zamanla değişebilir bu nedenle güncel olmayan verilerin güncel olan veriler ile değiştirilmesi gerekmektedir[83]. Aksi halde, verilerin doğru ve güncel olmaması halinde bu durum ilgili kişiler ve veri sorumluları için farklı ve ağır sonuçlara yol açabilecektir. Örneğin: Asgari Geçim İndirimi (AGİ) hesaplanırken çocuk sayısı ve eşin çalışma durumuna bakılmaktadır. Bu sebeple eşin çalışma durumu ile çocuk sayısının güncel olarak tutularak AGİ'nin doğru hesaplanması kişinin maddi çıkarları açısından önemlidir[84]. Bu bilgi yanlış olarak işlenmiş ise kişinin eksik ücret alma durumu söz konusu olabilecektir. Bireyin sağlık verisi gibi hassas verilerinde bu verilerin doğru ve güncel tutulması oldukça önemlidir[85].

Bu ilke, ilgili kişilerin erişim hakkı ve KVKK'nın 11.maddesinde düzenlenen ilgili kişilerin yanlış bilgilerin düzeltilmesini talep edebilmesi hakkı ile yakından ilişkilidir[86]. Bilgilere erişilememesi halinde kişisel verilerin doğruluğunun tespit edilmesi mümkün değildir. Verileri düzeltilmesini talep etme hakkı, hem yanlış ve hatalı tutulan verilerin hem de güncel ve değişen verilerin güncel olanı ile değiştirilmesi hakkında talepte bulunma yetkisini içerir.

Kişisel verilerin doğru ve güncel olarak tutulması veri sorumlusuna ait bir yükümlülüktür, devredilemez. Veri sorumlusunun böyle bir yükümlülüğü olmasına rağmen, ilgili kişi tarafından verilen her bilginin doğruluğunu ve kişisel verilerin güncelliğinin saptanması da kendisinden beklenemez. Bu sebeple ilgili kişinin, kişisel verilerin de bir değişiklik olduğunda bu durumu veri sorumlusunu bildirmesinin daha doğru olduğu düşünülmektedir[87]. Veri sorumlusunun işlediği verilerin güncel ve doğru olmasını sağlama yükümlülüğü olduğundan olumsuz sonuçlarla karşılaşılmaması için belirli aralıklarla veri sorumlusunun ilgili kişilerin verilerinin güncel olup olmadığını ilişkin bilgilendirme yaparak talepte bulunulmasına ilişkin bir mekanizma kurulması hususu öğretide önerilmektedir[88]. Kanaatimizce de veri sorumlularının olumsuz sonuçlarla karşılaşmaması ve ilgili kişinin haklarının ihlal edilmemesi adına belirli aralıklarla verilerin güncel olup olmadığının tespiti hususu son derece önemli olup, bu

[83] Turan Atlı, "Kişisel Verilerin Önleyici, Koruyucu ve İstihbari Faaliyetler Amacıyla İşlenmesi", **Necmettin Erbakan Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:2, Sayı:1, 2019, s.10.
[84] Kişisel Verileri Koruma Kurumu, **Örneklerle Kişisel Verilerin Korunması**, KVKK Yayınları No:29, Ankara, 2019, s.6.
[85] Uyarer, s.125.
[86] Çekin, s.81.
[87] Küzeci, s.244.; Dülger, s.298.
[88] Dülger, s.298.; Korkmaz, s.143.

konuda gerekirse bilişim sistemlerinden yararlanarak veri sorumluları tarafından bir mekanizma kurulması doğru olacaktır.

D. İşlendikleri Amaçla Bağlantılı, Sınırlı ve Ölçülü Olma

Bu ilke kişisel verilerin, veri sorumlusu tarafından işlenme amacı ile bağlantılı, sınırlı ve ölçülü olarak işlenmesini ifade etmektedir. İşlenme amacı ile bağlantısı olmayan kişisel veriler işlenmemeli, amaca ulaşmak için gerekli olan en az miktarda veri işlenerek nihai sonuca ulaşılmalıdır.

95/46/EC Sayılı Yönergenin 6/1. maddesi (c) bendinde kişisel verilerin toplandığı amaçlara ilişkin olarak yeterli, ilgili ve bu amacı aşmayacak şekilde işlenmesi gerektiği ifade edilmiştir.

108 sayılı Sözleşmesinin 5. Maddesinin (c) bendinde otomatik işleme konu olan kişisel verilerin kaydedilme amaçlarına uygun şekilde asgari oranda işlenmesi gerektiği ifade edilmiştir[89].

KVKK'nın 4.maddesinin (ç) bendinde kişisel verilerin işlenirken" *İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olm*a" gerekliliklerinin yerine getirilmesinin zorunlu olduğu ifade edilmiştir.

Bu ilke çeşitli metinlerde ve kaynaklarda *"veri asgarileştirme", "yeterlilik ilkesi", "veri ekonomisi", " veri minimizasyonu", "orantılılık"* ilkesi şeklinde de ifade edilmiştir[90].

Bu ilke gereği veri sorumlusu, belirtilen amaca başka bir araç aracılığıyla ulaşıyor ve bu araç temel hak ve özgürlüklere daha az müdahale ediyor veyahut hiç müdahale etmiyorsa, temel hak ve özgürlüklere an az müdahale eden aracın kullanılması gerekmektedir[91]. Örneğin, spor salonuna girişte uygulanan "*el ve parmak izi taraması"* sistemine üyelerin açık rızası olsa bile, üyelerin parmak izi verilerinin işlenmesi ölçülülük ilkesi ve minimum düzeyde veri talep edilmesi ilkelerine aykırılık teşkil edecektir[92]. Başka bir örnekte KVK Kurulu, ilgili kişinin din ve kan grubu gibi özel nitelikli kişisel verilerini de içeren arkalı-önlü kimlik görüntüsünün talep edilmesinin, KVKK'nın *"Genel İlkeler*" başlıklı 4.md düzenlenen *"işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma*" ilkesine uygun olmadığına karar vermiştir[93].

---

[89] Gemicioğlu, s.410.
[90] Küzeci, s.237; Öngün, s.84.
[91] Çekin, s.81.
[92] Kişisel Verileri Koruma Kurulunun 27.02.2020 tarihli 2020/167 sayılı Kararı, https://www.kvkk.gov.tr/Icerik/6738/2020-167, (05.01.2022).
[93] Kişisel Verileri Koruma Kurulunun 27.02.2020 tarihli 2019/294 sayılı Kararı, https://www.kvkk.gov.tr/Icerik/6556/2019-294, (05.01.2022)

İşlendiği amaçla sınırlı olarak veri elde edilmesi ilkesi teknolojik ürünler açısından da söz konusudur. Almanya görülmüş olan bir davada, mağaza içinde bulunan kameraların mağazanın dışını da görüş alanına almasını Mahkeme amacı aşan oranda veri toplanması olarak nitelemiştir[94].

Veri sorumlusunun amacından fazla kişisel veriyi işlemesi halinde bu ilke ihlal edilmiş olacaktır. "*Nasılsa lazım olur"*, *"belki ihtiyacımız olur"* mantığıyla gerekenden fazla kişisel veri işlenmemelidir[95].

E. Verilerin Amaç İçin Gerekli Süre Kadar Muhafaza Edilmesi

Bu ilke gereği kişisel veriler, ilgili mevzuatlarda öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmelidir. Kişisel verilerin işlenmesi faaliyeti belirli bir amacın gerçekleştirilmesi için yapılır. Belirli bir amacın ortadan kalkması veyahut gerçekleşmesi halinde veri sorumlusu tarafından kişisel verilerin elde tutulmasının bir anlamı, gerekçesi bulunmamaktadır. Bu sebeple kişisel verilerin, ilgili mevzuatta öngörülen süreler veya işlendikleri amaç için gerekli süre kadar elde tutulması gerekmektedir.

Kişisel verilerin gerekenden daha fazla süre elde tutulması verilerin bilişim teknolojisinde gerçekleşen hızlı gelişmeler sonucunda siber saldırılar ve sızıntılar yolu ile çalınarak hukuka aykırı şekilde elde edilmesine de sebep olabilecektir. Bu durum bireyin özel yaşamının gizliliği ve maddi-manevi bütünlüğüne zarar verecektir. Kişisel verilerin mümkün olduğu en az süre tutularak gerekli olmayan kişisel verilerin mümkün olduğu en kısa sürede silinmesi, yok edilmesi, anonim hale getirilmesi gerekmektedir[96]. Örneğin; bir telekom şirketine yapılan şikâyete ilişkin çağrı merkezine bırakılan ses kaydı şikâyet sonlandıktan sonra silinmelidir[97].

GVKT'nin 5(1). maddesinin (e) bendinde kişisel verilerin işlenme amaçlarının gerektirdiğinden daha uzun süre saklanmaması gerektiği ifade edilmiştir. KVKK da kişisel verilerin *"ilgili mevzuatta öngörülen veya işledikleri amaç için gerekli olan süre kadar muhafaza edilmesi ilkesine*" yer verilmiştir.

Türk Hukukunda ulusal mevzuattaki kanunlarda, kişisel verilerin ne kadar süre ile muhafaza edileceğine ilişkin bir hüküm varsa hükümde belirtilen sürelere

---

[94] Küzeci, ss.238-239.
[95] Dülger, s.286.
[96] Rıza Saka ve diğerleri, **Avrupa Birliği Hukuku, İdare Hukuku, Ceza Hukuku Açısından Kişisel Verilerin İmhası,** Seçkin Yayıncılık, Ankara, 2020, ss. 74-77.; Öngün, s.144.
[97] Develioğlu, s.49.

uyulmalıdır. 216 sayılı Vergi Usul Kanunu[98], 5510 Sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanununda[99], 1136 Sayılı Avukatlık Kanunu[100] gibi birçok mevzuatta kişisel verilerin muhafaza edilmesi gereken sürelere yer verilmiştir. Örneğin, 1136 Sayılı Avukatlık Kanunu 39.md uyarınca avukatlar kendisine teslim olunmuş evrakı vekalet ilişkisinin sona ermesinden itibaren en az 3 yıl saklamakla yükümlüdür. İlgili kanunlarda kişisel verilerin saklama süresi belirtilmişse o sürelere uyularak kişisel veriler o sürenin sonunda kadar saklanması gerekmektedir. Türk Hukukunda kişisel verilerin muhafaza edilmesine ilişkin kanunda bir süre belirtilmemişse veri sorumlusu, verinin işleme amacı ve ilgili kişinin niteliğini değerlendirerek kişisel verilerin saklanması için gerekli süreyi belirleyecek ve KVKK'nın 16.md gereğince kayıtta kişisel verileri işleme amacı ile işleyecekleri azami süreleri veri sorumluları siciline bildirecektir. Veri sorumlusunun bu süre bittikten sonra veriyi muhafaza etmek gibi bir takdir yetkisi bulunmamaktadır[101].

Kişisel verilerin işlenmesinde hedeflenen amacın ortadan kalkması, amaca ulaşmak için kişisel verilerin işlenmesinin gereksiz olduğunun anlaşılması veya yapılan işleme fiili sonucunda amaca ulaşılması halinde kişisel veriler elde tutulmayarak imha edilmelidir[102]. Bu durumda amaç ile kişisel veri arasında illiyet bağı kopmuş olup kişisel verilerin muhafazasına son verilmesi gerekmektedir. Avrupa İnsan Hakları Mahkemesi'nin (AİHM) bu konuya ilişkin kararları bulunmaktadır. AİHM bir kararında, herhangi bir kişinin parmak izi ya da DNA örneklerinin belirsiz süre saklanmasına izin veren uygulamayı sözleşmenin 8.maddesine aykırı bulmuştur[103].

IV.VERİ SAHİBİNİN (İLGİLİ KİŞİNİN) HAKLARI

Kişisel verilerin korunması sağlamak için uluslararası ve ulusal mevzuatlarda veri sahiplerine birtakım haklar verilmiştir.

GVKT de veri sahibinin hakları 12.madde ile 22.madde arasında sayılmıştır. GVKT'ye göre veri sahibinin; şeffaf bilgilendirilme, erişim, düzeltme, sildirme (unutma), veri faaliyetini kısıtlama, veri taşınması, itiraz hakları bulunmaktadır.

---

98 216 sayılı Vergi Usul Kanunu, R.G. 10.01.1961 – Sayı.10703-10705.
99 5510 Sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu, R.G. 31.05.2006-Sayı.26200.
100 1136 Sayılı Avukatlık Kanunu, R.G. 19.03.1969- Sayı.13168.
101 Uyarer, s.129.
102 Saka ve diğerleri, s.68.
103 S. Ve Marper, Birleşik Krallık'a karşı, b.n. 30562/04, 30566/04, K.T 4.Aralık 2008., Ayrıca bkz. Küzeci, s.246.

KVKK'nın 11.maddesinde veri sahiplerinin, veri sorumlularına ilişkin kullanabilecekleri haklar sayılmıştır. KVKK'nın 11.maddesine göre veri sahiplerinin: "*kişisel verinin işlenip işlenmediğini öğrenme", "kişisel verileri işlenmişse buna ilişkin bilgi talep etme", "kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme", "yurt içinde veya yurt dışında kişisel verilerinin aktarıldığı üçüncü kişileri bilme", "kişisel verilerinin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme", "kişisel verilerinin silinmesini veya yok edilmesini isteme"," kişisel verilerinin aktarıldığı üçüncü kişilere bildirilmesini isteme",* "*itiraz etme",* "*kişisel verilerinin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme"* hakları bulunmaktadır.

GVKT ve KVKK da veri sahibinin bu haklarını veri sorumlusuna karşı ileri sürebileceğini ve bu hakların veri işleme faaliyetinin her aşamasında kullanabileceğini belirtmek gerekir[104]. KVKK da kişisel verilerin korunmasına ilişkin yer alan haklar GVKT de yer almakta iken, GVKT de kişisel verilerin korunmasına ilişkin yer alan bazı haklar KVKK da yer almamaktadır.

A. Bilgilendirme Hakkı

Kişisel veri sahibinin kendisi hakkında işlenen verilere ilişkin bilgi alarak veri işleme sürecini takip etme hakkı bulunmaktadır. Bu durum, daha önce bahsettiğimiz verilerin geleceğini belirleme hakkının bir yansımasıdır[105]. Bireyin kişisel verilerin işlenmesi hakkında bilgilendirilmesi iki açıdan önemlidir. Birincisi, bu hak sayesinde birey kişisel verilerinin işlenmesi hakkında bilgi sahibi olmakta, ikincil olarak ise kamusal organların elinde bulundurduğu kişisel veriler gözetilerek idarenin şeffaflığı bu hak sayesinde sağlanmaktadır[106]. Kişinin bilgilendirilmesinin dürüstlük kuralı ile yakından ilişkili olduğunu da belirtmek gerekir[107].

GVKT, veri sahibine haklarının içeriği, kapsamı ve kullanma yöntemine ilişkin şeffaf bir şekilde bilgilendirme yapılması gerektiğini ifade etmiştir. GVKT'nin 13.maddesi veri sahibine verilecek bilgiler arasında; veri sorumlusunun veya temsilcisinin kimlik ve irtibat bilgileri, veri koruma görevlisinin irtibat bilgileri, kişisel verilerin planlanan işlenme amaçlarının yanı sıra işleme faaliyetinin yasal dayanağı,

---

[104] Dülger, ss.471-472.
[105] Uyarer, s.145.
[106] Fatma Ebru Gündüz ve İsmail Yazıcıoğlu, "Bilgi Edinme Hakkı Çerçevesinde Kişisel Verilerin Korunması"**, Anayasa Yargısı Dergisi**, Cilt:38, Sayı:1, 2021, s.174.
[107] Küzeci, ss.248.

ilgili kişisel verilerin aktarıldığı kişi veya kişi kategorileri, işlemenin meşru menfaatlere dayanarak gerçekleştirilmesi halinde meşru menfaatlerin neler olduğu, veri sorumlusunun kişisel verileri bir üçüncü ülkeye veya uluslararası kuruluşlara aktarma niyeti olduğu durumlarda alınan tedbirlerin neler olduğu, kişisel verilerin ne kadar süre saklanacağı veya bu bilgiyi sağlamak mümkün değilse ilgili sürenin belirlenmesinde kullanılacak kriterler, kişisel verilere erişme, kişisel verilerin düzeltilmesini veya silinmesini, işlemeye itiraz edilmesini, denetim makamlarına şikayette bulunma hakkı bulunmaktadır.

GVKT'ye paralel olarak KVKK'nın 10.maddesinde veri sahiplerine bilgi verilmesi veri sorumluları için bir yükümlülük olarak düzenlemiştir. Bu yükümlülüğün yerine getirilmemesi kişisel verilerin işlenmesini hukuka aykırı kılacaktır. Kanunda veri sorumlusunun yükümlülüğü olarak belirlenen bu durum GVKT de ilgili kişinin hakkı olarak tanımlanmıştır. Bu farklılık içerik olarak herhangi bir fark yaratmamakta olup, düzenlemelerin sistematiğine ilişkindir[108].

KVKK'nın 10.maddesine göre veri sorumlusu veyahut yetkilendirdiği kişi; veri sorumlusunun kimliği, kişisel verilerin hangi amaçla işleneceği, işlenen verilerin kimlere ve hangi amaçla aktarılabileceği, kişisel verilerin toplanma yöntemi ve hukuki sebebi konularında ilgili kişilere bilgi vermelidir.

Veri sahibi, kişisel verilerin işlenmesi konusunda KVKK'dan kaynaklanan haklarını 10 Mart 2018 tarihinde yayınlanan *"Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ"* hükümleri gereğince veri sorumlusu ve ilgili kurumlara karşı yazılı, e-posta, güvenli elektronik imza, mobil imza aracılığıyla kullanabilir[109]. Yapılan başvuru üzerine GVKT ve KVKK da bilgilendirme hakkı veri sorumlusu tarafından yerine getirilirken, kişisel verilerin işlenmesinin aşamaları ile ilgili veri sahibine oldukça sade, anlaşılır, uzun olmayacak şekilde açıklama yapılmalıdır. Yapılan açıklamalarda çok fazla hukuksal ve teknik açıklamalara yer verilmeyerek muğlak ifadeler kullanılmamalıdır. Bilgi verilmesi hakkında bir şekil şartı mevcut değildir. GVKT bilgilendirmenin sözlü olarak sağlanabileceğini ifade etmiş, KVKK da ise bu konuya ilişkin açık bir şekilde yer verilmemekle birlikte "*Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ"* ile bilgilendirmenin sözlü olarak yapılabileceği ifade edilmiştir. Bilgilendirme konusunda şekil şartı olmamakla birlikte; gereken bilgilerin

[108] Dülger, s.473.
[109] https://www.resmigazete.gov.tr/eskiler/2018/03/20180310-5.htm,(20.04.2021).

verildiği konusundaki ispat yükünün veri sorumlusu ve veri işleyende olduğunu belirtmek gerekir[110].

Bilgilendirmenin hangi dilde olacağına ilişkin KVKK ve GVKT de açık bir düzenleme bulunmamaktadır. Veri sahibi açısından bilgilendirmenin anlaşılabilmesi için bilgilendirmenin veri sahibinin veya üye devletin dilinde yapılması gerekmektedir. Veri sahibi başka bir yabancı dili anlayacak kadar bilmesi ve kendisine o dilde bilgilendirme yapılmasını kabul etmesi halinde başka bir dil kullanılması da mümkündür[111].

B. Veri Sahibinin Erişim Hakkı

Bireyin, kişisel verilerini korunması hakkına ulaşabilmesi ve kişilerin verileri üzerinde hakimiyet kurarak verilerinin geleceğini belirleyebilmesi için her zaman verilerine erişebilir olması gerekmektedir. Günümüz toplumunda, sosyal hayatın getirdiği bazı gelişmeler neticesinde verilerimiz hukuka uygun şekilde tutuluyor dahi olsa üçüncü kişilerin elinde bulunmaktadır. Bireylerin, üçüncü kişiler elinde bulunan bu verilerin nerede, nasıl, hangi amaçlarla tutulup kullanıldığını ve kimlerle paylaşıldığını öğrenmeye hakkı bulunmaktadır. Bu nedenle uluslararası ve ulusal mevzuatlarda bireylere kişisel verilerine erişme hakkı tanınmıştır. GVKT de kişisel verilere erişme hakkı geniş kapsamlı olarak düzenlenmiştir. KVKK da ise açık olarak erişim hakkı kavramından söz edilmemiş fakat, erişim hakkı kapsamında istenebilecek bilgiler sayılmıştır.

GVKT'nin 15.maddesinde *"Erişim Hakkı"* başlığı altında veri sahibinin kendisi ile ilgili kişisel verilerin işlenip işlenmediğini teyit etme ve işleme faaliyeti olması halinde:

"a) Kişisel verilere erişim ile ilgili işleme amaçları;

b) İlgili kişisel veri kategorileri;

c) Üçüncü ülkeler veya uluslararası kuruluşlardaki alıcılar başta olmak üzere kişisel verilerin açıklandığı veya açıklanacağı alıcılar veya alıcı kategorileri;

d) Mümkün olması halinde kişisel verilerin saklanması açısından öngörülen süre veya bunun mümkün olmaması halinde bu sürenin belirlenmesi amacı ile kullanılan kriterlere;

---

[110] Develioğlu, s.86.
[111] Dülger, s.480.

e) Veri sahibine ilişkin kişisel verilerin düzeltilmesi veya silinmesini söz konusu verilerin işlenmesinin kısıtlanmasını talep etme ve söz konusu işleme faaliyetine itiraz etme hakkının varlığı;

f) Bir denetim makamına şikâyette bulunma hakkı;

g) Kişisel verilerin veri sahibinden elde edilmemesi halinde, bu verilerin kaynaklarına ilişkin mevcut bilgiler; profil çıkarma da dahil olmak üzere otomatik karar vermenin varlığı ve en azından bu hallerde yürütülen mantığa ilişkin anlamlı bilgilerin yanı sıra söz konusu işleme faaliyetinin veri sahibi açısından önemi ve öngörülen sonuçları;"

Hakkında erişim hakkını kullanabilecektir.

KVKK da kişisel verilere erişim hakkı kapsamında talep edilebilecek bilgiler 11.madde de sayılmış olup, ilgili maddeye göre veri sahibinin;

"a) *Kişisel veri işlenip işlenmediğini öğrenme,*

b) Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,

c) Kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,

d) Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,

e) Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme, kişisel verilerin silinmesini veya yok edilmesini isteme,

f) Kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,

g) İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,

h) *Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme,"* haklarının olduğu açıkça ifade edilmiştir.

Yukarıda sayılan uluslararası ve ulusal mevzuattan kaynaklanan erişim hakları bireyler tarafından kullanırken başkalarının hak ve özgürlüklerini olumsuz şekilde etkilemeden bu hakların kullanılması gerekmektedir. Bu haklar doğrultusunda veri sorumlusu, veri sahibine bilgi verirken veri sahibi tarafından anlaşılmayacak kodlanmış, düzenlenmiş bilgileri veri sahibine bu yöntem ve dili açıklayarak yapmalıdır[112].

Bu hak kapsamında veri sahibinin talebi üzerine veri sorumlusu veri sahibine kişisel verilerin kopyasını da temin etmelidir. Veri sahibi birden fazla kopya isterse

[112] Dülger, s.480.

masraflar göz önüne alınarak kendisinden makul bir masraf veri sorumlusu tarafından talep edilebilir[113].

C. Unutulma Hakkı

Unutulma hakkı, bireyin dijital hafızada yer alan fotoğraf, kimlik bilgisi, adres ve bunun gibi diğer kişisel verilerinin kendi talebi üzerine bir daha getirilemeyecek şekilde ortadan kaldırılmasıdır[114]. Bu hak ile veri sahibi, kişisel verilerinin 3.kişilerce görülüp, izlenilmemesini hedeflemektedir[115].

Unutulma hakkı, kişisel verilerin korunması hakkında son zamanlarda ilgi duyulan güncel bir haktır. İnternetin hayatımızı etkisi altına alması, birçoğumuzun sosyal platformlar üzerinden iletişim kurması ve bunun gibi birçok sebeple kurum ve kuruluşlar bireyler hakkında oldukça fazla kişisel veri işlemiş, arşivlemişlerdir. Birçoğumuzun günlük hayatında tecrübe ettiği üzere bireyin kendisi tarafından bile geçmişte yaşanmış bir olaya ilişkin anı sosyal medya mecralarında zaman zaman bireye hatırlatılmaktadır. Facebook veya benzeri paylaşım sitelerinde kişisel veriler sürekli olarak tutulmaktadır. Hatta kullanıcıların sildiği mesaj, fotoğraf ve videoların kayıt altında tutulmaya devam ettiği düşünülmektedir[116]. İşte bu sebeplerle bireylerin verileri üzerinde kontrol hakkı sahibi olması düşüncesine dayanarak unutulma hakkı ortaya çıkmıştır.

Unutulma hakkının doğuşunda İsviçre Federal Mahkemesinin vermiş olduğu kararın etkisi büyüktür. İsviçre Federal Mahkemesi, bireyin 10 yıl önce işlemiş olduğu bir suçtan dolayı cezasını çektiğini, hatta bireyin adli sicil kaydından dahi suçun silindiğini belirterek söz konusu suçla ilgili yazı yazılarak bireyin ifşa edilmesinin doğru olmadığına karar vermiştir[117].

---

[113] Develioğlu, s.88.
[114] Seray Nalbantoğlu, "Bir Temel Hak Olarak Unutulma Hakkı", **Türkiye Adalet Akademisi Dergisi,** Sayı:35, 2018, s.589.; Hasan Elmalıca, "Bilişim Çağının Ortaya Çıkardığı Temel Bir İnsan Hakkı Olarak Unutulma Hakkı", **Ankara Üniversitesi Hukuk Fakültesi Dergisi,** Cilt:65, Sayı:4, 2016, s.1611.
[115] Bekir Gürses, **AB ve Türk Hukukunda Kişisel Verilerin Korunması Mevzuat Uyumuna Yönelik Bir Değerlendirme,** (Yayınlanmamış Yüksek Lisans Tezi), Marmara Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2019, ss.62-63.
[116] https://www.dijitalguvenlik.org/arama-motorlari/iste-facebook-ve-googlein-size-dair-sahip-oldugu-tum-veriler/,(20.04.2021)
[117] Uyarer, ss.35-36.

ABAD'ın 13 Mayıs 2014 tarihli Google-İspanya kararı ise unutulma hakkı konusunda verilmiş en önemli kararlardan biridir[118]. Karara konu olayda İspanya vatandaşı Costeja Gonzalez, adının Google arama motoruna yazıldığında geçmişte sonuçlanmış artık geçerliliği bulunmayan sosyal güvenlik borçlarının tahsiline ilişkin haciz davaları ile bağlantılı bir gayrimenkul açık artırma ilanın yer aldığı bu ilanın Google arama motorunda yer almasını istemediğini, bu durum sebebi ile zarar gördüğünü beyan ederek buna ilişkin sayfaların kaldırılmasını ve düzenlenmesini İspanya da günlük tirajı yüksek bir gazete ve Google İspanya'dan talep etmiştir. İspanya Veri Koruma Kurumu, Google ile ilgili şikâyeti haklı bularak kabul etmiştir. Google şirketi de bunun üzerine davayı İspanya Yüksek Mahkemesine taşımıştır. Yüksek Mahkeme 95/46/EC sayılı Yönergenin yürürlüğe girmesinden sonra yaşanan teknolojik gelişmelerin değerlendirilerek bazı soruların sorulması açısından konuyu ABAD'a göndererek dosyayı bekletici mesele yapmıştır. ABAD yaptığı inceleme sonucunda veri sahibi ilgili kişinin bilginin kamuya sunulmamasını talep hakkı bulunduğunu ve bu hakkın Google şirketinin ekonomik faaliyeti ile kamunun bu habere ulaşma menfaatinden daha üstün olduğuna karar vermiştir. ABAD, 95/46/EC sayılı Yönergenin 12. maddesine de atıf yaparak kişinin kişisel verilerinin geçersiz veya ilgisiz hale gelmesinden sonra amacını aşması halinde silinmesi gerektiğine hükmetmiştir[119].

Türk hukukunda ise unutulma hakkı Anayasa Mahkemesinin (AYM) 3 Mart 2016 tarihli *"N.B.B. Başvurusu"* ile ele alınmıştır[120]. Başvuru bireyin, bir gazetenin internet arşivinde ulaşılabilir durumda olan haber ve içeriğin yayından kaldırılmasına ilişkin talebin yetkili makamlarca reddedilmesine ilişkin bir başvurudur. Ulusal nitelikteki gazetenin internet arşivinde başvurucunun uyuşturucu kullanması sonucunda adli para cezası almasına ilişkin 1998 ve 1999 yıllarına ait üç haber bulunmaktadır. Başvurucu bu haberlerin kendisinin şeref ve haysiyetini zedelediğini, topluma mal olmuş bir kişi olarak bu durumun iş ve sosyal hayatını olumsuz etkilediğini beyan ederek gazeteye ihtar göndermiş ve talebinin reddedilmesi üzerine olay AYM önüne gelmiştir. AYM kararında, internet ortamının sağladığı ulaşılabilirlik, yaygınlık düşünülerek haberin internet ortamında uzun süre kalmasının kişinin şeref ve itibarını zedeleyebileceğini ifade etmiştir. Unutulma hakkı Anayasada açıkça

[118]https://eur-lex.europa.eu/legal content/EN/TXT/?uri=CELEX%3A62012CJ0131,(20.04.2021).
[119] Ayşenur Ocak, "Hakları Dengelemek: Unutulma Hakkı İfade Özgürlüğüne Karşı", **Türkiye Adalet Akademisi Dergisi,** Sayı:33, 2018, ss.515-516.
[120] AYM, N.B.B. Başvurusu, Başvuru No: 2013/5653, 3.3.2016 (24.08.2016 tarih ve 29811 sayılı RG).

düzenlenmemiş olsa da Anayasanın *"Devletin Temel Amaç ve Görevleri*" başlıklı 5.maddesinde belirtilen *"insanın maddi manevi varlığının gelişmesi için gerekli şartları hazırlamaya çalışmak"* ifadesi ile devlete bireyin geçmişte yaşadıklarının başkası tarafından öğrenilmesini engelleyerek yeni bir sayfa açma olanağı verme konusunda pozitif bir yükümlülük yüklemiştir. AYM bu kararı ile devletin amaç ve görevleri dikkate alarak, kişinin şeref ve itibarı, maddi-manevi varlığı, özel hayatının gizliliği haklarının doğal bir sonucu olarak unutulma hakkı kanunda belirtilmese bile bu hakkı açıkça tanımıştır[121].

Unutulma hakkının ihlal edilmesi, kişilik haklarına saldırı sayılarak tazminat taleplerine de konu olmuştur. Yargıtay incelemesine konu olan bir olayda, cinsel saldırıya ilişkin Mahkemeye de konu olan bir olay mağdur ve sanığın isimleri gizlenmeden bir kitapta yer almıştır. Davacı rızası dışında kitapta yer alan isminin kişisel veri olduğunu belirterek manevi tazminat talebinde bulunmuştur. Yargıtay, davacı isminin kitapta yer almasının kişinin özel hayatı ve unutulma hakkını ihlal ettiğini belirterek ihlali yapanlar hakkında manevi tazminata hükmetmiştir[122].

Unutulma hakkı, GVKT'nin 17.maddesinde detaylı şekilde ifade edilmiştir. Veri sahibinin unutulma hakkını kullanması halinde kişisel verilerin gecikmeden silinmesinin veri sorumlusu tarafından bir yükümlülük teşkil edeceği açıkça ifade edilmiştir. Bunun yanında; kişisel verilerin toplanma ve işlenmelerine artık ihtiyaç duyulmaması, işlemenin rızaya dayanması halinde ilgili kişinin rızasını geri çekmesi, uygun olarak işlemeye itiraz edilmesi, kişisel verilerin hukuka aykırı olarak işlenmesi durumunda talep üzerine kişisel verilerin silinmesi gerektiği ifade edilmiştir.

Kanaatimizce Türk hukukunda unutulma hakkı şu anda da açıkça düzenlenmemişse de, KVKK'nın 11.maddesinde herkesin veri sorumlusuna başvurarak ilgili kişisel verilerini 7.madde de öngörülen şartlar çerçevesinde silinmesi ve yok edilmesini isteme hakkı olduğu gözetilerek bu hakkın kullanılabileceğini söylemek mümkündür.

---

[121] Muhammed Emin Karakaş, "Dijital Geçmişin İnternet Erişiminden Kaldırılması "Unutulma Hakkı" ve Türk Hukukunda Görünümü", **Necmettin Erbakan Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:3, Sayı:2, 2020, ss.281-282.

[122] YHGK, 17.06.2015, E. 2014/4-56, K. 2015/1679 Ayrıca Bkz. Ceren Küpeli, "Şiddet Mağduru Kadınların Unutulma Hakkı", **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, Cilt:22, Sayı:1, 2016, ss.234-235.

D. İşleme Faaliyetini Kısıtlama Hakkı

GVKT ile bireylere işleme faaliyetinin sınırlandırılması hakkı tanınmıştır. İşleme faaliyetinin kısıtlanması, saklanan kişisel verilerin gelecekte işlenmelerinin sınırlanması amacıyla işaretlenmesini ifade eder. Bu hakkın kullanılması halinde işaretlenen kişisel veriler bir süre işlenemeyecek, durumu belli olduktan sonra ona göre hareket edilecektir[123].

Bu hakkın kullanılması ile kısıtlama konusu işaretlenen veriler veri sorumlusu tarafından depolanır fakat veri sahibinin rızası veya hukuki bir sebep olmaksızın kullanılmaz. Veri sahibinin işleme faaliyetinin kısıtlanmasını talep etme hakkı GVKT'nin 18.maddesinde düzenlenmiş olup, KVKK da bu konuda bir düzenleme bulunmamaktadır. KVKK da bulunan genel düzenlemeler neticesinde işleme faaliyetini kısıtlama hakkının ayrıca düzenlenmesi gerekmeyen doğal bir hak olduğu düşünülmektedir[124].

Çalışanın işverenine işi giriş saatinin yanlış kaydedilmesini bildirerek işlemenin kısıtlanarak sosyal güvenlik kurumuna iletilmemesini talep etmesi, işveren bu durumu açığa kavuşturup teyit edene kadar bu bilgiyi işaretleyerek kuruma bildirmemesi bu hakkın örneğidir[125].

E. İtiraz Hakkı

Veri sahibi kişisel verilerine erişim, verileri düzeltme gibi haklarının yanında kendi özel durumu ile ilgili gerekçelerle kişisel verilerin işlenmesine itiraz edebilir.

GVKT'nin 21.maddesinde *"itiraz etme hakkı"* başlıklı özel bir düzenleme bulunmaktadır. Bu maddeye göre veri sorumlusu; veri sahibine, veri işlemesindeki çıkar hak ve özgürlüklerine ilişkin ikna edici meşru gerekçeler göstermez veya veriyi işlemenin yasal bir dayanağı bulunmaz ise veri sahibinin kişisel verilerini işleyemeyecektir.

GVKT'ye göre veri sahibinin doğrudan pazarlamaya ilişkin yaptığı itirazlar mutlak olup, her zaman ileri sürülebilir. Mutlak olmasından anlaşılması gereken veri sorumlusunun herhangi bir istisna olmaksızın itiraz konusu işleme faaliyetine son vermesi gerektiğidir. Örneğin; kişinin evine bir klima aldığını ve yaptığı bu alışveriş

[123] Develioğlu, s.93.
[124] Dülger, s.505.
[125] Develioğlu, s.94.

sonrasında klima firmasından sıklıkla e-posta, SMS alarak, adresine broşürler gönderilmesi doğrudan pazarlamaya ilişkin itiraz hakkını gündeme getirebilecektir[126]. İşlenen veriler kamu görevinin yerine getirilmesi, veri sorumlusunun yasal yükümlülüklerini yerine getirmesi, veri sahibinin hak ve özgürlüklerinin ile meşru menfaatlerinin korumaya uygun tedbirleri öngörmüşse itiraz hakkı mutlak değildir.

Türk hukukunda ise KVKK'nın 11.maddesinde ilgili kişinin işlenen kişisel verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi durumunda kişinin kendi aleyhine çıkacak sonuca itiraz etme hakkı olduğu ifade edilmiştir. İlgili kişinin bu hakkı kullanabilmesi için kişisel verilerinin sadece yapay zekâ gibi otomatik vasıtalar yolu ile analiz edilmiş olması ve bu analizin ilgilinin aleyhine sonuç doğurması gerekmektedir. Örneğin; kişilerin birçok aygıt üzerinden reklam faaliyetlerinin yapılması için takip edilmesi kişinin beklentileri, istek, zafiyetleri üzerinden istifade edilerek ciddi olumsuz sonuçlara neden olabilecektir. Maddi durumu kötü olan bir kişinin sürekli yüksek faizli kredi reklamları görmesi bu duruma örnektir. İlgili kişi bu durumun gerçek bir kişi tarafından değerlendirilmesini talep edebilir[127]. KVKK gerekçesinde; bir çalışan performansının, onun tarafından yapılan işlerin, otomatik bir sisteme işlenip analiz edilerek, analiz sonucuna göre değerlendirilmesine, çalışanın itiraz edebilmesinin de bu kapsamda olduğunu belirtilmiştir[128].

F. Düzeltme Hakkı

Düzeltme hakkı hem GVKT de hem de KVKK da düzenlenmiş önemli haklardan biridir. Kişisel verilerin işlenirken uyulması gereken kurallardan biri *"doğru ve gerektiğinde güncel olma"* ilkesidir. Kişisel verilerin doğru ve güncel olarak saklanması hem veri sahibi hem de veri sorumlusu için oldukça önemli olup, ilgili kişi bu ilke kapsamında kişisel verilerinin eksik, yanlış işlenmesi halinde bunun düzeltilmesini talep etme hakkına sahiptir. Örneğin:

- Kişinin boşanması ve soyadının değişmesi durumunda soyadı değişikliğini hizmet aldığı bankalara bildirmesi yararlı olacaktır. İlgili kişi bu bildirimi yapmış olmasına rağmen yeni kredi kartı talebinde eski soyadının yazılı olduğu bir kredi kartının kendisine ulaşması halinde veri sorumlusuna başvurarak bu durumun düzeltilmesini talep edebilecektir.[129].

[126] Dülger, s.488.
[127] Çekin, s.171.
[128] KVKK 11 madde gerekçesi.
[129] Öngün, s.209.

- Kişinin adres bilgisinin veri sistemine yanlış kaydedilmesi sebebiyle kendisine yapılan tebligatları zamanında alamaması ve bu sebeple hukuki yollara başvuramaması durumunda ilgili kişi maddi ve manevi zarar görebilecektir[130].

G. Veri Taşınabilirliği Hakkı

Veri taşınabilirliği hakkı GVKT'nin 20.maddesinde düzenlenmiş, KVKK da düzenlenmemiştir. Bu hak doğrultusunda ilgili kişi kendisi hakkında veri sorumlusunun işlemekte olduğu kişisel verileri yapılandırılmış, yaygın olarak kullanılan ve bir makine tarafından okunacak formatta alabilecektir. İsterse ilgili kişi, bu kişisel verileri başka bir veri sorumlusuna iletilmesini isteme hakkı da bulunmaktadır[131]. Bu hakkın kesin kullanılabilmesi için aşağıdaki şartlara ihtiyaç vardır:

a) Veri taşınabilirliğine konu kişisel veriler ilgili kişi tarafından sağlanmış olmalıdır.
b) Veri sorumlusunun bu veriler üzerinde gerçekleştirdiği işleme faaliyetleri ilgili kişinin açık rızası veya ilgili kişinin taraf olduğu bir sözleşmenin uygulanması veya bir sözleşme yapılmadan önce ilgili kişinin talebi ile adımlar atılması için işleme faaliyetinin gerekli olması hallerinden birine dayanmalıdır.
c) İşleme faaliyeti otomatik yollarla gerçekleştirilmelidir[132].

Bir e-posta kutusu sağlayıcısı aracılığıyla e-posta hesabı açan kişi, bu hesaba gelen e-postaların kendisine verilmesini isteyerek başka bir e-posta sağlayıcısına geçebilmelidir[133].

H. Zararın Giderilmesini İsteme Hakkı

Kişisel verileri; hukuka aykırı şekilde, izinsiz, yanlış veya geçersiz şekilde işlenen ilgili kişiler kişisel verileri işleyen görevli gerçek ve tüzel kişilerden zararın tazminini talep edebilirler.

---

[130] Kişisel Verilerin Koruma Kurumu, **100 soruda Kişisel Verilerin Korunması Kanunu**, KVKK Yayınları No:3, Ankara, 2019, s.36.
[131] Berrak Yılmaz, **Türk Anayasa Mahkemesi ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması**, (Yayınlanmamış Doktora Tezi), Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü, Ankara, 2019, ss.189-190.
[132] Dülger, s.484.
[133] Develioğlu, ss.95-96.

GVKT'nin 82. Maddesinde *"Bu Tüzük'e ilişkin bir ihlal sonucu maddi veya manevi zarar gören herhangi bir kişi, yaşanan zarara ilişkin olarak kontrolör veya işleyiciden tazminat alma hakkına sahiptir."* hükmüne yer verilmiştir.

KVKK'nın 12/ğ. maddesinde ilgili *kişinin "kişisel verilerin kanuna aykırı şekilde işlenmesi sebebi ile zarar uğraması halinde zararların giderilmesini talep etme"* hakkı düzenlenmiştir.

Bu konuya ilişkin detaylı açıklamaları, kişisel verilerin korunması hukukunda Türkiye Mevzuatı başlıklı çalışmamın üçüncü bölümde açıklayacağım[134].

[134]Detaylı bilgi için bkz. 3. Bölüm Türk Hukukunda Kişisel Verilerin Korunması III.Kişisel Verilerin Korunması Yolları, C. Genel Düzenlemelerde Yer Alan İmkanlar Yoluyla Koruma.

İKİNCİ BÖLÜM
ULUSLARARASI HUKUKTA VE AVRUPA BİRLİĞİ HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASI

I. ULUSLARARASI KAYNAKLARDA KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN DÜZENLEMELER

A. OECD (Ekonomik Kalkınma ve İşbirliği Örgütü)

OECD'nin temel kuruluş amacı kendisine üye olan tüm devletlerin demokrasi, insan hakları, vatandaş haklarını gözeterek ekonomik kalkınmayı sağlayarak üye devletlerin ekonomisini geliştirmektir[135]. OECD kişisel verileri korumayı ulusal ve uluslararası alanda değerli bir meta olarak görmesi sebebi ile kişisel verilerin korunmasının ekonomik açıdan önemini de ortaya koyarak 23.09.1980 tarihinde kişisel verilerin korunmasına ilişkin "Özel Yaşamın Gizliliği ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeler" başlıklı bir metin yayınlamıştır[136]. Bu metin ile OECD kişisel verilerin korunmasına ilişkin olarak uluslararası alanda adım atan ilk kuruluş olmuştur[137].Bu belge ile verilerin korunması ve sınır ötesi taşınmasına ilişkin bir takım temel ilkeler belirtilmiştir. Belirtmek gerekirse[138]:

a) Veri Toplanmasını Sınırlama İlkesi: Kişisel verilerin toplanmasında sınırlamalar olmalıdır. Bu tür veriler hukuka uygun olarak adil yollar ile veri sahibinin bilgisi ve rızası ile toplanmalıdır (7.md).

b) Veri Kalitesi İlkesi: Kişisel veriler amacına uygun olmalı, bu amaç için gerekli ölçüde eksiksiz ve güncel olmalıdır (8.md).

c) Amaca Özgülük İlkesi: Kişisel verilerin toplanma amacının verilerin toplanması anında belirli olması gerekmektedir Verilerin kullanımı bu amaçlar ile çelişkili olmamalıdır (9.md).

d) Kullanımının Sınırlı Olması İlkesi: Kişisel veriler veri sahibinin rızası olmadan veya kanunun verdiği yetki olmadan paylaşılmamalı ve açıklanmamalıdır (10.md).

---

[135] Dülger, s. 86.

[136]https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm ,(30.12.2021); Sadık Akif, **Uluslararası Hukukta Kişisel Verilerin Korunması**, (Yayınlanmamış Yüksek Lisans Tezi), Anadolu Üniversitesi Sosyal Bilimler Enstitüsü, Eskişehir, 2020, s.23.

[137] Dülger, ss. 86-87.

[138] Gemicioğlu, ss.384-385.

e) Güvenlik Önlemleri İlkesi: Kişisel veriler kaybolma, yetkisiz erişim, tahrip edilme, kullanma, değiştirilme, ifşa edilme gibi risklere karşı makul güvenlik önlemleri ile korunmalıdır (11.md).

f) Açıklık İlkesi: Kişisel veriler ile ilgili gelişmeler, uygulama ve politikaları hakkında genel bir şeffaflık politikası olmalıdır (12.md).

g) Bireyin Katılımı İlkesi: Bireyin; veri sorumlusunun kendisine ilişkin verilere sahip olup olmadığı hakkında veri sorumlusundan bilgi edinme, kendisi ile ilgili verilerin fahiş olmayan bir fiyat ile makul süre içerisinde rahatça anlayabileceği formatta kendisine iletilmesi,bu taleplerinin reddedilmesi halinde bunun sebeplerinin kendisine açıklanması ve buna itiraz edebilme, kendisi ile ilgili verilere itiraz etmesi halinde itirazı başarılı olursa verileri sildirtme, düzelttirme, tamamlatma, değiştirtme hakkına sahiptir (13.md).

h) Hesap Verilebilir İlkesi: Veri sorumlusu yukarıda belirtilen ilkelerin hayata geçirilmesi bakımından hesap verebilir durumda olmalıdır (14.md).

Bu ilkeleri içerir metin tavsiye niteliğinde bir metin olup, devletler arasından hukuki bir bağlayıcılığı yoktur. OECD üyesi devletler bu ilkeleri iç hukuklarının bir parçası haline getirip getirmemek konusunda serbest olup, takdir hakkı üye devletlerdedir[139].

OECD, 2013 yılında bu ilkeleri güncellemiş, temel ilkeleri koruyarak kişisel verilerin ihlalinde bildirim yükümlülüğü, rıza kavramı, veri sorumlularının kişisel verilerin sınırlar arası veri akışı bağlamında sorumlu tutulmasına ilişkin çalışmalar düzenlemiştir[140].

OECD'nin kabul ettiği Rehber İlkeler Avrupa Birliği Direktiflerine ve 6698 Sayılı Kişisel Verilerin Korunması Kanununa temel teşkil etmesi sebebi ile de oldukça önemlidir.

B. BİRLEŞMİŞ MİLLETLER

II. Dünya Savaşından sonra galip çıkan devletler savaşın yıkıcı etkilerinin giderilmesi, uluslararası barışın ve güvenliğin sağlanması, savaşın tekrarlanmaması

[139] Berna Akçalı Gür, "Uluslararası Hukuk ve AB Hukuku Boyutuyla Kişisel Verilerin Yurt Dışına Aktarılması", **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, Cilt:25, Sayı:2, Prof. Dr. Ferit Hakan Baykal Armağanı, 2019, s.852; Küzeci, s.130.
[140] Uyarer, s.46.

amacıyla 24 Ekim 1945 tarihinde 51 devlet Birleşmiş Milletler örgütünü kurmuştur[141]. Örgütün amaçlarından biri insan hakları ve temel özgürlüklere saygı gösterilerek bu hakların desteklenmesidir[142].

Kişisel verilerin korunması, Birleşmiş Milletlerce de öncelikli olarak özel yaşamın gizliliği kapsamında değerlendirilmiş[143] ve İnsan Hakları Evrensel Beyannamesinin 12.maddesinde *"Kimsenin özel yaşamına, ailesine, konutuna ya da haberleşmesine keyfi olarak karışılamaz, şeref ve adına saldırılamaz"* hükmüne yer verilmiştir. Bu hükümle bağlantılı olarak OECD'nin tavsiye niteliğinde ki ilkelerine benzer şekilde 14 Aralık 1990 tarihinde 45/95 sayılı Bilgisayarla İşlenen Kişisel Veri Dosyalarına İlişkin Rehber İlkeler adıyla bir kılavuz yayınlanmıştır[144]. Bu metinde: yasallık ve dürüstlük, doğruluk ilkesi, amacın belirliliği ilkesi, ilgili kişinin erişim ilkesi, ayrımcılık yapmama ilkesi, istisna koyma yetkisi, güvenlik ilkesi, denetleme ve yaptırımlar, sınır ötesi veri akışı ilkelerine yer verilmiştir. Bu belge OECD tavsiye ilkeleri gibi bağlayıcı nitelikte olmayıp, tavsiye niteliğindedir. Birleşmiş Milletlerde bu ilkelerin uygulanması için bir denetim mekanizması öngörülmüş olup bu durum kişisel verilerin denetlenmesine ilişkin mekanizmalar kurulmasına öncülük etmiştir[145] .

C.AVRUPA KONSEYİ

Kişisel verilerin korunması hakkında çalışmalar yürüten bir diğer önemli uluslararası kuruluşlardan biri Avrupa Konseyidir. II. Dünya Savaşının sonlanması ile savaşın yıkıcı etkilerini ortadan kaldırmak, barışın sağlanması ve bir daha savaşın yaşanmasını önlemek için 5 Mayıs 1949 tarihinde 10 Avrupa ülkesi devlet tarafından kurulmuştur. Konseyin Avrupa çapında insan hakları, demokrasi ve hukuk devleti kavramlarını korumak ve geliştirmek önemli hedefleri arasındadır.

Avrupa Birliği Konseyi Statüsünün 3.maddesinde "*Avrupa Konseyinin her üyesi, hukukun üstünlüğü ilkesiyle yargı yetkisi içindeki herkesin insan hakları ve temel özgürlüklerden yararlanması ilkesini kabul eder ve 1. Bölümde belirlenen*

---

[141] Bilal Altıner, "Birleşmiş Milletler: Amacı, Gelişimi, Etkinliği, Uluslararası Güvenliğe Katkısı ve Geleceği", **Avrasya Sosyal ve Ekonomi Araştırmaları Dergisi,** Cilt: 1, Sayı:1, 2014 ss. 1-2.

[142]Tacettin **Çalık,**"Birleşmiş Milletler Organlarının İnsan Hakları İle İlişkisi", **İnönü Üniversitesi Hukuk Fakültesi Dergisi**, Özel Sayı, Cilt:2, 2015, s.1094.

[143] Yeşim Çelik, "Özel Hayatın Gizliliğinin Yansıması Olarak Kişisel Verilerin Korunması Ve Bu Bağlamda Unutulma Hakkı, **Türkiye Adalet Akademisi Derneği**, Sayı:32, 2017, ss.397-398.

[144] https://www.refworld.org/pdfid/3ddcafaac.pdf. ,(20.12.2021).

[145] Uyarer, ss.45-46.

Konsey amacının gerçekleşmesinde içten ve etkin bir biçimde iş birliği yapmayı üstlenir." hükmüne yer verilmiştir.

Avrupa Konseyinin yukarıda belirttiğim gibi temel faaliyetleri arasında insan hakları ve temel hak ve özgürlükler bulunduğundan 4 Kasım 1950 tarihinde bu temel hak ve özgürlüklerin korunması ve geliştirilmesi için Avrupa İnsan Hakları Sözleşmesi (AİHS) kabul edilmiştir. AİHS temel hakların korunması ve geliştirilmesi için son derece önemli bir uluslararası belgedir. Kişisel verilerin korunması hukuku açısından da AİHS sözleşmesi son derece önemlidir. AİHS kişisel verileri özel yaşama saygı hakkının özel bir şekli olarak korunmuştur[146].

Elektronik veri işletim sistemlerindeki hızlı gelişmeler ve kişisel verilerin geniş bir şekilde depolanması sonucunda AİHS kişisel verilerin korunması için yeterli olmamış bunun üzerine Avrupa Konseyi kişilerin verilerin korunması için çalışmalar başlatmış ve bu çalışmalar sonucunda 1981 yılında 108 sayılı Sözleşme kabul edilmiştir[147].

1. 108 no.lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi

1981 tarihli ve 108 sayılı Avrupa Konseyi Sözleşmesi, kişisel verilerin korunması hukuku açısından çok önemli bir yere sahip olan verilerin korunması hakkında temel ilkeleri ortaya koyan kişisel verilerin korunması hakkında bağlayıcılığı bulunan ilk uluslararası sözleşmedir[148]. Sözleşme, sözleşmeye taraf olan ülkeler için kişisel verilerin korunması hakkında bir çerçeve sunmaktadır.

Bu sözleşmenin ortaya çıkmasında Avrupa İnsan Hakları Sözleşmesinde kişisel verilerin korunması hakkına açıkça yer verilmemesi yatmaktadır. AİHS kişisel verilerin korunmasını bağımsız bir hak olarak düzenlememiştir. AİHS'de kişisel veriler özel yaşama saygı hakkının bir görünümü olarak korunmuştur. Fakat teknolojinin hızla ilerlemesi ve gereksinimlerin artması, bilgisayar kullanımın daha da yaygınlaşması, veri sistemlerinin artması sebebi ile kişisel verilerin korunması hukukunda bazı özel düzenlemelere yer verilmesi gerektiği düşünülmüştür. Bu

---

[146] 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, ss.88-89.

[147] Korkmaz, s.143

[148] Mehmet Altundiş, "Tıbbi Kişisel Verilerin Tutulması ve Korunması Yükümlülüğü ve İdarenin Bu Yükümlülüğünü Yerine Getirmemesinden Doğan Sorumluluğu", **Türkiye Adalet Akademisi Derneği,** Sayı:28, 2016, s.316.

sebeple de 108 sayılı Sözleşmesi ile bu alanda olan boşluğun doldurulması amaçlanmıştır[149].

Sözleşme 1981 tarihinde hazırlanmasına rağmen 01.10.1985 tarihinde yürürlüğe girmiştir. Türkiye 28.01.1981 tarihinde sözleşmeyi imzalamasına rağmen, 17.03.2016 tarihinde onay kanunu çıkararak uygulamasını başlatmıştır[150]. Onay kanunu tasarısının gerekçe kısmında bilgi teknolojilerinde yaşanan hızlı gelişmelerin konuyu hassas bir boyuta taşıdığı ve bu sebeple konunun önemlilik teşkil ettiği belirtilerek sözleşmenin iç hukuka dahil edilmesinin uygun olacağı ifade edilmiştir[151].

Sözleşmenin 1.maddesinde sözleşmenin amacının, sözleşmeye taraf devlette uyruğu veya ikamet yeri ne olursa olsun her gerçek kişinin temel hak ve özgürlüklerini ve özellikle kendisiyle ilgili kişisel verilerin otomatik işleme tabi tutulması karşısında özel hayata saygı hakkını güvence altına almak olduğu ifade edilmiştir.

Sözleşmenin 2.maddesinde kişisel verilerle ilgili temel kavram ve ilkeler açıklanmış, sözleşmenin 3.maddesinde ise bu sözleşmenin hem kamu hem de özel sektörde uygulanabileceği ifade edilerek anlaşmaya taraf devletlerin eğer isterlerse bu sözleşmeyi gerçek ve tüzel kişilere uygulayabileceği belirtilmiştir. Yine aynı madde de otomatik yollarla işlenen veriler için güvence öngörülmüştür. Sözleşmeye göre otomatik işlemeden söz edebilmek için sürecin tamamen otomatik olması gerekmemekte, kısmen otomatik olarak işlenen verilerin de sözleşme kapsamında olduğu düşünülmektedir[152].

Sözleşmenin 4.maddesinde sözleşmeye taraf olan devletlerin verilerin korunması için gerekli önlemleri alması ve bu önlemlerin sözleşmenin yürürlüğe girdiği tarihten itibaren alınması gerektiği ifade edilmiştir. Sözleşmenin 5.maddesinde kişisel verilerin işlenmesinde uyulması gereken kurallara yer verilmiş, bu maddeye göre kişisel veriler hukuka uygun şekilde toplanmalı ve bu toplanan veriler yine bu amaçlar şeklinde işlenmeli, veriler doğru ve güncel olarak tutulmalıdır.

Sözleşmenin 6.maddesinde özel veri kategorisi başlığı ile düzenlenmiş, bu düzenlemeye göre hassas veriler gerekli önlemler alınmadıkça otomatik yollar ile işlenemeyecektir. Madde de hassas veriler; kişinin ırksal kökeni, siyasi düşüncesi, inançlarını ortaya koyan, sağlık ve cinsel hayatla ilgili, ceza mahkumiyetini içerir bilgiler olarak nitelendirilmiştir. Hassas nitelikli kişisel verilerin çalışmamızın ilk

[149] Küzeci, s.145.
[150] 108 sayılı Kişisel Verilerin Otomatik İşlemesi Karşısında Bireylerin Korunması Sözleşmesi, R.G 17.03.2016 – Sayı.29656.
[151] Dülger, s.91.
[152] Küzeci, s.145.

bölümünde ifade ettiğimiz gibi diğer kişisel verilerden daha özenli şekilde korunmasının sebebi hukuka aykırı olarak işlenmeleri halinde kişileri zarara uğratma olasılığının oldukça yüksek olmasıdır.

Sözleşmenin 7.maddesinde otomatik veri dosyalarında saklanan kişisel verilerin izinsiz veya kaza sonucu olarak imhası, kaybolması, dağıtılması, değiştirilmesine karşı güvenlik önlemlerinin alınması gerektiği ifade edilmiştir.

Sözleşmenin 8.maddesinde kişisel veri sahibine tanınan haklar düzenlenerek, kişilerin bu hak kapsamında verilerinin işlenip işlenmediğini öğrenme, veri sorumlusu hakkında bilgi alma, verileri düzeltme veya sildirme ve bu hakların kullandırılmadığı takdirde itiraz hakkına sahip olduğu vurgulanmıştır.

Sözleşmenin 12.maddesi kişisel verilerin sınır ötesi transferine ilişkindir. Sözleşmeye taraf devletlerden hiçbiri özel yaşamın korunması amacıyla kişisel verilerin sınırı aşan veri aktarımını yasaklayamaz. Sözleşmeye taraf ülke, mevzuatında kişisel veriler ile ilgili özel hükümler bulunması halinde verilerin ülke dışına aktarımını sınırlandırabilir. Ancak bu sınırlandırmanın söz konusu olabilmesi için, verilerin aktarılacağı diğer ülkede verisi aktarılan ülke ile aynı seviyede bir korumanın sağlanmıyor olması gerekmektedir. Kısaca, sözleşmeye taraf ülkelerden biri verilerin aktarılacağı ülke mevzuatında kendine eşit seviyede bir koruma var ise verilerin aktarımını sınırlayıp, engelleyemeyecektir.

Sözleşmenin 18.maddesinde sözleşmede yer alan hükümlerin ve bu hükümlerin uygulanmasını geliştirmeye yönelik danışma komitesi kurulmuştur. Komite de sözleşmeye taraf devletlerin temsilcilerinin yanında belirli koşullar çerçevesinde Avrupa Konseyi üyesi olmayan devletlerin gözlemcilerinin de bu Komite de temsil edilebileceği ifade edilmiştir. Bu komitenin görevleri arasında kişisel verilerin korunması ilişkin raporlar hazırlamak ve rehber ilkeleri geliştirmek olduğu da ifade edilmiştir[153]. Komite ayrıca yine sözleşmenin 19.maddesi uyarınca da taraflardan birinin talebi üzerine, sözleşmenin uygulanması ile ilgili tüm sorular hakkında görüş bildirebilir.

Sözleşmenin 22.maddesinde, bu sözleşmenin Avrupa Konseyi üyesi devletlerinin imzasına açık olduğu, Sözleşmenin 23.maddesinde ise belirli şartlar altında Avrupa Konseyine üye olmayan herhangi bir devletin sözleşmeye katılmaya davet edilebileceği ifade edilmiştir. Sözleşmenin 25.maddesinde ise sözleşmenin hükümlerine hiçbir şekilde çekince koyulamayacağı ifade edilmiştir.

[153] Küzeci, s.148.

Yukarıda incelenen sözleşme maddeleri ışığında 108 sayılı Kişisel Verilerin Otomatik Olarak İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşmenin birçok hukuki metine kaynaklık etmiş olduğunu ve yol gösterdiğini belirtmek gerekmektedir. Sözleşmenin önemli özelliklerinden birisi de bu sözleşmenin sadece konsey üye devletlerinin değil konsey üye devletleri dışında devletlerinde imzasına açık olmasıdır[154].

108 sayılı Sözleşmenin, 1981 yılından bugüne gerçekleşen teknolojide ki gelişmeler gözetilerek güncellenerek yenilenmesi gerekmiştir. Bunun üzerine çalışmalar başlatılarak yapılan çalışmalar sonucunda 03.12.2014 tarihinde Avrupa Konseyi Veri Koruma Geçici Komitesi yenilenmiş hükümleri içeren Sözleşme 108+ protokol taslağını kabul etmiş, Avrupa Konseyi Bakanlar Komitesi ise 18.05.2018 tarihinde metni kabul etmiştir. Sözleşme 108+ ile bilişim teknolojilerindeki gelişmeler dikkate alınarak daha güçlü bir veri koruma mekanizması öngörülmüş, GVKT de olduğu gibi güvenlik yükümlülükleri güçlendirilmiş, şeffaflık prensibine atıf yapılarak biyometrik veriler özel nitelikli kişisel veriler kapsamına dahil edilmiştir[155].

108 sayılı Sözleşmenin modernize edilmiş Sözleşme 108+ metni Türkiye tarafından henüz imzalanmamıştır. Türkiye açısından sözleşme 108+ hüküm doğurması için imzalanarak onaylanması gerekmekte olup, en kısa sürede metnin onaylanarak iç hukukumuza dahil edilmesinin kişisel verilerin korunması hukukumuz açısından önemli olacağını düşünmekteyiz[156].

2. Avrupa İnsan Hakları Sözleşmesi

Avrupa Konseyi başlığı altında incelenecek en önemli düzenlemelerden biri de Avrupa İnsan Hakları Sözleşmesidir.

AİHS, II. Dünya Savaşı sırasında tüm dünyanın göz önünde işlenen insanlık suçları sonucunda bireyin devlete karşı ezilmemesi ve daha fazla korunması amacıyla; insan hakları, demokrasi ve hukukun üstünlüğü kavramlarını temel alarak Avrupa Konseyi tarafından 04 Kasım 1950'de Roma'da imzalanarak 3 Eylül 1953 de yürürlüğe girmiştir. Türkiye AİHS'i 18 Mayıs 1954'te onaylamış[157] olmasına rağmen Avrupa İnsan Hakları Mahkemesinin yargı yetkisini 28 Ocak 1990 tarihinde kabul

[154] Uyarer, s.48; Mehmet Bedii Kaya, "Kişisel Verilerin Korunmasında Yeni Paradigma: Hesap Verebilirlik İlkesi", **İstanbul Üniversitesi Hukuk Mecmuası**, Cilt:78, Sayı:4, 2020, s.1869.
[155] Uyarer, s.51.
[156] Dülger, s.92.
[157] 10.03.1954 tarihli ve 6366 Sayılı Onay Kanunu, R.G 19.03.1954- Sayı.8662.

etmiştir. AİHS deki temel hak ve hürriyetlerin korunup korunmadığını denetleyen yargı organı AİHM'dir.

AİHS kaleme alındığı dönemde kişisel verilerin korunması hususu bugünkü kadar gündemde olan ve ihtiyaç gerektirecek bir mesele olarak görülmediğinden bu sözleşmede kişisel verilerin korunmasına ilişkin ayrıca bir madde bulunmamaktadır. Fakat zamanla gelişen bilişim sektörü ve teknoloji sebebi ile kişisel verilerin korunmasının bir insan hakkı haline gelerek, müdahalesi bireylerin özel yaşamına olumsuz yönde etki etmiş ve AİHM de kişisel verilerin korunması hususunu AİHS 8.maddesi kapsamında değerlendirmeye başlamıştır[158].

AİHS'nin Özel ve Aile Yaşamına Saygı Hakkı" başlıklı 8.maddesinde: *"Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir. Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir."* hükmüne yer verilmiştir. Avrupa İnsan Hakları Mahkemesi sözleşmeyi geniş yorumlayarak kişisel verilerin korunmasına dair temel ilkeleri de koruma altına almıştır.

AİHS'nin 8.maddesinde kişinin özel hayatı, aile hayatı, ev yaşamı ve yazışmalarının koruma altına alındığı ifade edilmiştir. Burada bu hüküm ile devlete hem pozitif hem de negatif yükümlülük yüklenmiştir. Bu hükümde devletin pozitif yükümlülüğü kişinin sayılan bu dört hakkının korunması için gerekli güvenlik önlemlerini alması negatif yükümlülüğü ise devletin kişinin özel hayatı, aile hayatı, ev yaşamı ve yazışmalarına müdahale etmemesidir[159]. Aynı hükümde bu hakların kullanılmasına müdahalenin ancak ve ancak belirli sebeplerle olabileceği teker teker sayılarak ve bu müdahalenin ulusal mevzuatta belirlenen yasalar ile yapılabileceği ifade edilmiştir.

AİHM, kişisel verilerin korunması hakkında önüne gelen başvurularda üç aşamalı bir inceleme yapmaktadır. AİHM önüne gelen başvuruda;

1. Başvuru konusu olayın AİHS 8.maddesinde yer alan özel yaşam, aile yaşamı, ev yaşamı ve kişinin yazışmaları ile ilgili olup olmadığını incelemekte;

---

[158] Eren Solmaz. "Avrupa İnsan Hakları Mahkemesi Kararlarının "Kişisel Verilerin Korunmasına Katkısı", **İstanbul Üniversitesi Hukuk Mecmuası**, İdare Hukuku ve İlimleri Dergisi, Cilt:18, Sayı:1, 2018, ss.63-67.

[159] Uyarer, s.53.

2. Başvuru konusu olayın AİHS 8.maddesi kapsamında olduğuna kanaat getirilirse, yapılan işlem veyahut müdahalenin bu hükme aykırı olup olmadığını değerlendirmekte;
3. Son aşama olarak da yapılan başvuru konusu işlemin AİHS 8.maddesine aykırı olduğu ve bu hakka müdahale edildiğinin tespit edilmesi halinde bu müdahalenin AİHS 8/2.maddesi gereğince müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olup olmadığını meşruluğunu incelemektedir[160].

AİHM öncelikle önüne gelen somut olayda olayın koşullarına göre bir değerlendirme yapacak ve başvuru konusunun özel, aile ve kişinin sözleşmede belirtilen yaşam alanlarına ilişkin olup olmadığını inceleyecektir. Eğer başvuru konusu olayda özel yaşama saygı hakkına bir müdahale olduğu saptanır ise bu müdahalenin meşru olup olmadığı gözetilecektir. Sözleşmede meşru amaçlar; ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, dirlik ve düzenin korunması, suç işlenmesinin önlenmesi, sağlık, ahlak ve başka kişilerinin haklarının korunması olarak ifade edilmiştir. Sözleşme de ayrıca bu hakka yapılacak müdahalenin yasal temelinin bulunması gerektiği de ifade edilmiştir. AİHM, özel ve aile yaşamına müdahaleyi incelerken aynı zamanda müdahalenin demokratik bir toplumda gerekli olup olmadığına da sorgulamaktadır. AİHM içtihatlarında, sözleşmede belirtilen özel ve aile hayatının korunması hakkı ile sözleşmede belirtilen meşru sebeplere dayanarak belirli makamlarca yapılacak müdahale arasında makul bir dengenin olması gerektiği de gözetilmektedir. AİHS 8.maddesi kapsamında AİHM tarafından verilen bazı önemli kararları inceleyelim:

AİHM; Türkiye'ye karşı Mustafa Sezgin Tanrıkulu kararında, başvurucu kendisi ile beraber Türkiye'de bulunan herkesin, 2005 yılında verilen bir ulusal mahkeme kararına dayanarak bir buçuk ay boyunca iletişiminin denetlendiğini bu durumun ulusal mevzuata ve AİHS 8.maddesine aykırı olduğunu iddia etmiş ve AİHM'e başvurmuştur. AİHM konuyu değerlendirerek başvurucunun 8.madde kapsamında hakkının ihlal edildiğine hükmetmiştir[161].

[160] Küzeci, s.156.
[161] https://hudoc.echr.coe.int/tur#%20 (14.05.2021) Ayrıca bkz. Uyarer, s.55.

AİHM “L.H – Litvanya” kararında, başvurucu kendisine ait kişisel sağlık verilerinin rızası aranmaksızın devlet tarafından toplanmasının özel hayatına haksız bir müdahale olduğunu ve sözleşmenin 8.maddesi uyarınca hakkının ihlal edildiğini iddia etmiştir. Mahkeme yaptığı incelemede, Litvanya yasalarının bu konuda yeterli netlik ve açıklığa sahip olmadığını, Litvanya hukukunda başvuru konusu devlet kurumları tarafından toplanan verilere ilişkin hiçbir sınırlama getirilmediğini bu durumun başvurucunun sağlık verilerinin 7 yıldan bu yana toplanmasına sebep olduğunu belirterek 8.maddenin ihlal edildiğine hükmetmiştir. Mahkeme bu kararında sağlık verileri hakkında gereken hassasiyeti vurgulayarak bu tür verilerin işlenmesi açısından veri sorumlusunun yasa ile bir sınırlama ve değerlendirilmeye tabi tutulması gerektiğini ifade etmiştir[162].

Mahkemenin kişisel verilerin korunmasına ilişkin ilk kararı “ Klass ve Diğerleri-Almanya” kararıdır. Bu kararda Mahkeme gizli telefon dinlemelerini özel yaşam kapsamında değerlendirerek sözleşmenin 8.maddesinin ihlal edildiğini, sözleşmenin 8/2.maddesi uyarınca meşru hallerin dar yorumlanması gerektiğini sözleşmeye taraf devletlerin bireyler üzerinde sınırsız şekilde gözetim yapamayacağını ifade etmiştir[163].

Mahkeme “Gaskin- Birleşik Krallık” kararında, başvurucu evlatlık kayıtlarının kendisine açıklanmaması nedeniyle Mahkemeye başvurmuştur. AİHM kamu belgelerinin gizliliğinin 3.kişilerin korunması için gerekli olmakla beraber özel hayatına ilişkin kayıtlara ulaşmak isteyen bireyin menfaatlerinin diğer menfaatlerden üstün olduğunu belirterek sözleşmenin 8.maddesinin devletin pozitif yükümlülüğünün ihlal edildiğine hükmetmiştir[164].

“Segerstedt- Wiberg ve Diğerleri-İsveç” davasında, başvuranlar İsveç Polisi tarafından suçun önlenmesi ve ulusal güvenliğin korunması gerekçeleri ile kendileri hakkında tutulan dosyalara erişim hakkı verilmemesinden dolayı şikayetçi olmuşlardır. Mahkeme kararında, bu kayıtların erişime açılmamasının ulusal güvenlik ve terörle mücadele açısından meşru olduğunu ve sözleşmenin 8.maddesinin ihlal edilmediğini belirtmiştir[165].

Mahkeme “Kruslin- Fransa “başvurusunda, bir cinayet soruşturması sebebi ile yapılan telefon dinlemelerinin, telefon dinleme kararının makul bir netlikle

[162] https://www.echr.coe.int/Documents/FS_Data_TUR.pdf (14.05.2021) Ayrıca bkz Uyarer, ss.55-56.
[163]https://hudoc.echr.coe.int/tur (14.05.2021) Ayrıca bkz Korkmaz, s.154.
[164] https://hudoc.echr.coe.int/tur (14.05.2021)
[165]https://hudoc.echr. coe.int/tur (14.05.2021) , Ayrıca bkz Korkmaz, s.158.

belirlenmemesi ve bu durumun vatandaşların haklarının korunmasında yetersiz kaldığı ifade edilerek sözleşmenin 8.maddesinin ihlal edildiğine hükmetmiştir[166].

Mahkeme " Peck v.- Birleşik Krallık" davasında, başvurucunun sokakta bileğini kestiği görüntüler kameraya kaydedilmiş ve görüntüler medyaya verilmiştir. Başvurucu konuya ilişkin Mahkemeye başvurmuş, Mahkeme kararında başvurucunun rızası alınmaksızın bu görüntülerin yayınlanmasının özel hayata orantısız bir müdahale olarak nitelendirmiştir[167].

Yukarıda örnek verilen kararlar gözetildiğinde AİHM'sinin; bireylerin kişisel verilerinin resmi makamlarca toplanarak arşivlenmesi, telefon görüşmelerinin izlenmesi, toplanan verilerin amacı dışında kullanılması, sağlık verilerinin gizliliği, çalışanların bilgisayar kullanımının izlenmesi, emniyet güçleri tarafından parmak izi ve fotoğrafların alınması, kişisel verilerin gerektiğinden uzun süre tutulması, gibi konuları sözleşmenin 8.maddesi kapsamında değerlendirilmiştir[168].

D. AVRUPA BİRLİĞİ

1. 95/46/EC Sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Yönergesi

a. Yönergenin Amacı

Avrupa Birliğinde kişisel verilerin korunmasına ilişkin en önemli metinlerden biri 24 Ekim 1995 tarihinde kabul edilen ve 24 Ekim 1998 tarihinde yürürlüğe konan "95/46/EC Sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Yönergesi"dir[169].

Yönerge kabul edilmeden önce Avrupa ülkelerinde kişisel verilerin korunmasına ilişkin ayrı ayrı hukuki düzenlemeler bulunmaktaydı. Fakat teknolojinin gelişmesi, bilgi paylaşımının uluslararası seviyede önemli ölçüde artması ve 1 Kasım 1993 tarihinde yürürlüğe giren Maastricht Anlaşması ile Avrupa Birliği sınırları

[166]https://hudoc.echr.coe.int/eng, Ayrıca bkz Korkmaz, s.160.
[167] https://hudoc.echr.coe.int/eng (14.05.2021), Ayrıca bkz Dülger, s.129.
[168] Küzeci, s.159.
[169] Avrupa Birliği 95/46/EC Numaralı Kişisel Verilerin İşlenmesi Sırasında Gerçek Kişilerin Korunması ve Serbest Veri Trafiği Yönergesi, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995 L0046&from=EN, (15.12.2021).

içerisinde mal ve sermayenin serbestçe dolaşması tek iç pazarın kurulabilmesi için kişisel verilerin korunmasına ilişkin yeknesak bir düzenleme yapılmasını gerekli kılmıştır[170]. Örneğin, Almanya, Fransa, İskandinav ülkeleri kişisel verilerin korunması kavramını insan hakları kapsamında değerlendirirken, Yunanistan da kişisel verilerin korunmasına ilişkin o dönemlerde yasa dahi bulunmamaktaydı[171]. Bu sebeple, öncelikli olarak üye ülkelerin veri koruma mevzuatlarının birbiri ile uyumunu sağlayarak kişisel verilerin tüm üye ülkelerde belirlenen asgari seviye de korunmasını sağlamaktır[172].

Yönergenin 1.maddesinde "*Bu Direktife uygun olarak, Üye Devletler, kişisel verilerin işlenmesine dair başta kişisel mahremiyet hakkı olmak üzere gerçek kişilerin temel haklarını ve özgürlüklerini koruyacaktır"* hükmüne yer verilmiştir. Bu hükümden anlaşılacağı üzere bu yönergenin asıl amaçlarından bir diğeri ise gerçek kişilerin temel hak ve hürriyetlerinin korunmasıdır. Kişisel verilerin korunması hakkı bu metinde temel bir insan hakkı olarak sayılmıştır.

Yönergeler, Avrupa Birliği üyesi ülkelere doğrudan uygulanmaz. Yönerge de yer alan kuralların ulusal hukuka aktarılması gerekmektedir. Buradaki düzenleme yönerge olması sebebi ile Avrupa Birliği üyesi ülkeler yönerge kapsamında iç hukukta gerekli düzenlemeleri yapmakla yükümlüdürler. Yapılacak düzenlemelerin yönergenin asgari standartlarını içermesi gerekmektedir[173].

b. Yönergedeki Temel Kavramlar

Yönerge de kişisel verilerin korunması hukukuna ilişkin kavramlara da yer verilmiştir. Kısaca değinmek gerekirse,

a) Kişisel veri: fiziksel, fizyolojik, zihinsel, ekonomik, kültürel veya sosyal kimliğine özel bir veya daha fazla faktöre veya bir kimlik numarasına atıf başta olmak üzere

[170]Nilgün Başalp, " Avrupa Birliği Veri Koruması Genel Regülasyonunun Temel Yenilikleri**", Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, Cilt 21, Sayı 1, 2015, ss.85-87.

[171] Küzeci, s.184.

[172]Çağrı Uysal Zeybek, "Google'ın Yeni Gizlilik Politikası Google Inc. Tarafından 1 Mart 2012 Tarihinde Yayımlanan Politikasının Kişisel Verilerin Korunması İlkeleri İle Uyumluluğu Ve Avrupa Birliği'nin 95/46/EC Sayılı Veri Koruma Direktifi Açısından Değerlendirilmesi", **Hacettepe Hukuk Fakültesi Dergisi,** Cilt:3, Sayı:1, 2013, s.106.

[173] Ahmet M. Güneş, "Avrupa Birliği Yönergelerinin Doğrudan Etkisi", **Ankara Üniversitesi Hukuk Fakültesi Dergisi,** Cilt 58, Sayı 2, 2009, ss.287-290.

doğrudan veya dolaylı olarak tespit edilebilen bir tespit edilebilir kişiye ilişkin herhangi bir bilgiyi kastetmektedir.

b) Kişisel verilerin işlenmesi: Kişisel verilerin silme veya tahrip etme, engelleme, birleştirme veya sıralama, sağlama ya da dağıtma, iletmeyle açıklama, toplama, kaydetme, organizasyon, depolama, adaptasyon veya değiştirme, kurtarma, danışma gibi otomatik ya da otomatik olmayan araçlarla kişisel veriler üzerinde yapılan herhangi bir faaliyet veya faaliyet dizisidir.

c) Kişisel veri dosyalama sistemi: Merkezi olsun veya olmasın bir işlevsel veya coğrafi tabana dağıtılmış özel kriterlere göre erişilebilir olan herhangi bir yapılandırılmış kişisel veri dizisini kast edecektir.

d) Denetleyici: Kişisel verilerin işlenme araçlarını ve amaçlarını tek başına ya da diğerleriyle ortaklaşa belirleyen gerçek veya tüzel kişiyi, kamu makamını, devlet dairesi veya başka bir kuruluştur.

e) İşleyici: Denetleyici adına kişisel verileri işleyen bir gerçek veya tüzel kişiyi, kamu makamını, devlet dairesini veya diğer bir kuruluşu ifade etmektedir.

f)Üçüncü şahıs: Veri işlemek için yetkilendirilen işleyici veya denetleyicinin doğrudan yetkisi altındaki kişiler ve işleyici, denetleyici, veri öznesi dışındaki herhangi bir gerçek veya tüzel kişi, kamu makamını, devlet dairesini veya başka bir kuruluşu olarak ifade edilmiştir.

g) Alıcı: İster bir üçüncü şahıs olsun ya da olmasın, verilerin açıklandığı bir gerçek veya tüzel kişiyi, kamu makamını, devlet dairesini veya başka bir kuruluşu ifade edecek olup, özel bir soruşturma çerçevesinde verileri alan makamlar alıcı olarak kabul edilmeyecektir.

h) Veri öznesinin rızası: Kendisine dair kişisel verilerin işlenmesi için veri öznesinin kabulüne işaret eden, özgürce ve bilgilendirilme yapıldıktan sonra alınan rızayı ifade edecektir.

Yönergenin 2.maddesinde temel kavram ve tanımlar ifade edilmiştir.

c. Yönergenin Kapsamı ve Uygulama Alanı

Yönerge kişisel verilerin korunması için güçlü bir koruma öngörmekle birlikte aynı zamanda Avrupa Birliğine üye ülkelerin kişisel verilerin işlenmesini düzenleyecek kanunları yürürlüğe koymasını kapsayacak düzenlemelerde öngörmektedir. Yönergenin kapsamı 3.maddesinde ifade edilmiştir. 3.madde de:

"Bu Direktif, bir dosyalama sisteminin parçasını oluşturması istenen veya bir dosyalama sisteminin parçasını oluşturan kişisel verilerin otomatik araçlar dışında işlenmesine ve kısmen veya tamamen otomatik araçlarla kişisel verilerin işlenmesine uygulanacaktır. Bu Direktif, kişisel verilerin işlenmesine uygulanmayacaktır" hükmüne yer verilmiştir.

Buna göre kişisel verilerin kısmen veya tamamen otomatik araçlarla işlenmesi veyahut kişisel verilerin elle işlenmesi ve yönerge de belirtildiği üzere dosyalama sisteminin bulunması halinde Yönerge hükümleri uygulanacaktır. Yönergenin uygulama alanı veri işleyen kişiye ve işleme amacı ile ilgili olarak bazı konularda sınırlandırılmıştır. Kamu güvenliği, savunma, devlet güvenliği, ceza hukuku alanında devlet işlemlerinde Yönerge hükümleri uygulanmayacaktır. Yine bir gerçek kişinin ailesi ve ailevi faaliyetleri ile ilgili olarak veri işlemesi halinde de Yönerge hükümleri uygulanmayacaktır[174].

ABAD'ın, Yönergenin uygulama alanına ilişkin kararları bulunmaktadır. ABAD'ın "Lindqvist" kararı bu kararlardan biridir. Karara konu olayda, İsveçli bir kadın olan Lindqvist kilise de gönüllü çalışmaları ile ilgili bir internet sayfası hazırlamıştır. Bu internet sitesinde kilise de beraber çalıştığı arkadaşlarına ilişkin adres, telefon numarası, hobi, sağlık durumlarını içerir kişisel verilere yer vermiştir. Lindqvist bu bilgileri yayınlarken ilgili kişilerden bu konuda rızasını almamıştır. İlgili kişilerden birinin uyarısı üzerine de bilgileri internet sitesinden kaldırmıştır. Buna rağmen İsveç Veri Koruma Yetkilileri Lindqvist hakkında soruşturma başlatarak otomatik olarak kişisel verilerin işlenmesi ve ilgili kişilerin izni alınmaksızın bu bilgilerin transfer edilmesi sebebi ile tazminat ödemesine karar verilmiştir. Bu kararı Lindqvist temyiz etmiş, Gota Temyiz Mahkemesi de Yönergenin doğru yorumlamak için durumu ABAD'a sormuştur. ABAD bilgilerin internet sitesinde yayınlanmasını başlı başına veri aktarımı anlamına gelmediğini fakat internet üzerinde yayınlanan veriler bu sayfaları aramayan kişilere gönderiliyor veya internet sunucu altyapısı AB üyesi olmayan bir ülkede bulunuyor ise bu durumun geçerli olmadığını bunun bir veri transferi haline geleceğini ifade etmiştir. Ayrıca ABAD bu kararında, kâr amacı gütmeyen kuruluşlara da Yönergenin uygulanacağına karar vermiştir[175].

---

[174] Nurullah Tekin, "Kişisel Verilerin Korunması İle İlgili Türkiye'deki Kanun Tasarısının Avrupa Birliği Veri Koruma Direktifi Işığında Değerlendirilmesi", **Uyuşmazlık Mahkemesi Dergisi**, Sayı: 4, 2014, ss.226-227.

[175] https://curia.europa.eu/juris/liste.jsf?num=C-101/01 (20.12.2021), Ayrıca bkz. Küzeci, ss.190- 191.

Yönergenin etki alanı AB ülkeleri ile sınırlı kalmamıştır. AB üyesi olmayan pek çok devlette hukuksal düzenlemelerinde Yönergeden etkilenmiştir. Nitekim Yönerge 6698 sayılı KVKK'ya da büyük ölçüde örnek olduğu ifade edilmektedir[176].

d. Kişisel Verilerin İşlenmesine İlişkin Yönergedeki Temel İlkeler ve İlgili Kişinin Hakları

Yönerge de kişisel verilerin korunması ve işlenmesine ilişkin temel ilkelere de yer verilmiştir (6.md). Belirtilen temel ilkeler aşağıdaki gibidir:

a) Kişisel veriler adil ve yasal olarak işlenmelidir.

b) Kişisel veriler belirli, açık ve meşru amaçlar için toplanmış ve bu amaçlarla uyumsuz biçimde başkaca işlenmemesi gerekmektedir.

c) Kişisel veriler toplandığı ve ayrıca işlendiği amaçlara ilişkin olarak yeterli ve orantılı olmalıdır.

d) Kişisel veriler doğru şekilde ve güncel olarak tutulur. Kişisel verilerin toplanma ve sonrasındaki işlenme, silinme veya düzeltilme amaçlarını göz önünde tutarak verilerin yanlış veya eksik olmamasını sağlayacak tüm makul önlemler alınmalıdır.

e) Kişisel verilerin toplandığı esnada veya sonrasında işlendiği amaçlar için gerekenden daha uzun olmayan süre boyunca, veri öznelerinin tespitine izin veren biçimde tutulabilir. Üye Devletler, tarihsel, istatistiksel veya bilimsel kullanım amacıyla daha uzun süreli depolanan kişisel veriler için uygun koruma önlemleri almalıdır.

Yönerge ile kişisel verilerin hangi şartlarda hangi ilkeler doğrultusunda işlenebileceği, işlenen verilerin hangi amaçlar ile sınırlı olarak kullanılabileceği ifade edilmiştir. Ayrıca Yönergenin 8.maddesinde hassas verilerin istisnai durumlarda işlenebileceği ve veri ilgilisinin bilgilendirilmesi gerekeceği de ifade edilmiştir.

Yönerge de yine kişisel verilerin korunması hususunda ilgili kişinin haklarına çeşitli maddelerde yer verilmiştir. İlgili kişinin kişisel verilere ilişkin bilgi edinme (12.md), itiraz (14.md), yargı yollarına başvurma (22.md), otomatik bireysel kararlara tabi olmama (15.md) gibi haklarına yer verilmiştir.

Yönerge kişisel verilerin işlenmesinde şeffaflık ilkesine de yer verilmiştir. Şeffaflık ilkesinin sağlanabilmesi için ilgili kişinin bilgilendirilmesi ve kendisi hakkında tutulan bilgilere erişebilmesi gerekmektedir[177]. Yönergede bu hususlara ilişkin bilgi verilmesi

[176] Dülger, s.96.

[177] Nafiye Yücedağ. "Kişisel verilerin korunması kanunu kapsamında genel ilkeler", **Kişisel Verileri Koruma Dergisi,** Cilt:1, Sayı: 1, 2019, s.49.

yükümlülüğü getirilmiştir. Yönergeye göre ilgili kişiye talep ettiği bilgi aşırı gecikme olmaksızın mutlak surette verilmesi gerekmektedir.

Yönergenin 29.maddesinde, kişisel verilerin korunması alanında danışma organı niteliğinde bağımsız bir organ kurulması öngörülmüştür. Çalışma grubu olarak anılacak olan bu otoritenin çalışma prensiplerine de yine Yönergenin 30.maddesinde yer verilmiştir. Çalışma grubu, Yönergenin iç hukuka aktarılması için çalışmalar yaparak ve bu çalışmaları denetleyerek görüşlerini bildirir raporlar hazırlamaktadırlar. Çalışma grubunun görüşleri bağlayıcı değildir[178].

e. Kişisel Verilerin Üçüncü Ülkelere Aktarımı

Yönergenin 25.maddesinde kişisel verilerin üçüncü ülkelere aktarılması konusu düzenlenmiştir. 25.maddeye göre göre kural olarak Avrupa Birliği üyesi ülkeler haricinde bulunan üçüncü ülkelere yapılacak kişisel verilerin aktarımı, ancak ve ancak o ülkede yeterli seviyede bir koruma olması ile mümkündür. Aksi halde, bu ülkelere veri aktarımı yasaktır[179]. Bu sebeple Yönergedeki bu madde Avrupa Birliği dışında bulunan üçüncü ülkelerin tüm veri işleme işlemlerini Avrupa Birliği ile uyumlu hale getirmeye zorlamaktadır[180]. Yönerge de "yeterli seviyede koruma" ile bahsedilen korumanın tam olarak ne olduğu açıklanmamıştır. Yeterli seviyede koruma kavramının yorumlanması üye ülkelere ve Avrupa Komisyonuna bırakılmıştır. Yapılan inceleme sonucunda yeterli düzeyde korumanın sağlanmadığı fark edilirse Komisyon ve üye devletlerin birbirlerini durumdan haberdar etme yükümlülükleri bulunmaktadır.

Yönergeye göre, eğer verilerin aktarılacağı ülkede yeterli düzeyde koruma yoksa aktarımın yapılabilmesi istisnai bir durumdur. Bu istisnalar Yönergenin 26.maddesinde düzenlenmiştir. İstisnaları kısaca açıklamak gerekirse[181];

---

178 Sena Kontoğlu, "Madde 29 Veri Koruma Çalışma Grubu Avrupa Adalet Divanı'nın 13 Mayıs 2014 Tarihli Google Unutulma Hakkı Kararının Uygulanması Hakkında Yönerge Avrupa Adalet Divanı'nın "Google İspanya Ve Google Inc Karşı Agencıa Espanola Deproteccıo De Datos Aepd Ve Marıo Costejagonzalez Tarafından Açılan" Davada Verilen C-131/12 Kararının Uygulanması Hakkında Yönerge", **Küresel Veri Çeviri Hukuk Dergisi**, Cilt:6, Sayı:21, 2016, ss.1-2.

179 Örnek Büken ve Zeybek Ünsal, "Kişisel Verilerin Korunması Kanununun Biyomedikal Alana Yansımaları Açısından Değerlendirilmesi", **Hacettepe Hukuk Fakültesi Dergisi**, Cilt:7, Sayı:2, 2017, ss:48-49.

180 Esin Gürsel ve Fatih Düğmeci, "Yapısal Anlamda Türkiye Kişisel Verileri Koruma Kurumu'na İlişkin Bir Değerlendirme", **R&S Research Studies Anatolia Journal**, Cilt:1, Sayı:2, 2018, s.321.

181 Küzeci, ss.195-198.

a) İlgili kişinin aktarım için açık rızasının bulunması: Burada yalnızca rızanın olması yeterli olmayıp, rızanın açık ve özgürce ilgili kişi bilgilendirilerek alınması gerekmektedir.

b) Aktarımın sözleşmenin ifası veya sözleşme öncesi bir ilişkinin yürütülmesi için gerekli olması: Burada ölçüt kısaca gerekliliktir. Örneğin, otel rezervasyonu yaptırırken kişisel bilgilerin seyahat acentesine aktarılması bu kapsamda değerlendirilebilir.

c) Aktarımın ilgili kişinin çıkarlarını koruması, veri sorumlusu veya üçüncü bir kişi arasında yapılan bir sözleşmenin sonuçlandırılması ve uygulanması için gerekli olmasıdır.

d) Aktarımın önemli bir kamusal çıkarı koruması, hukuksal taleplerin sağlanması için gerekli veya yasal zorunluluğu olması: Burada kamusal çıkardan bahsedilmektedir. Bu istisnanın dar yorumlanması gerekmektedir. Aksi durum istisnanın keyfi bir uygulamaya dönüşmesine sebep olabilecektir.

e) Aktarımın ilgili kişinin yaşamsal çıkarlarının korunması için gerekli olması: Burada ilgili kişinin sağlığına ilişkin acil bir durumda tıbbi bir yardım alması için veri aktarılmasını öngörmektedir.

f) Aktarımın herkese açık olan kamu kayıtlarından yapılması ve yasanın aradığı şartları taşıması: Bu istisnanın sebebi kayıtların herkese açık olmasından ve meşru çıkarı olan herkesin bu bilgiye ulaşma hakkı bulunuyor ise üçüncü ülkelerde bulunan kişilerin de bu bilgilere ulaşmasında sakınca görülmemesidir.

Yukarıda belirtilen istisnaların hepsi dar yorumlanmalıdır. İstisnalar, kural haline gelmemelidir.

Bu istisnaların dışında Yönergeye göre verilerin korunması hususunun bir sözleşmeyle garanti edilmesi durumunda üye ülkeler belirli kategoriye ilişkin verilerin transferine izin verebilecektir. Bu uygulamaya örnek olarak, FIAT'ın Fransa da bulunan alt şirketi, bazı verilerin İtalya'da bulunan merkezlerine transferi için Fransız Veri Koruma Otoritesinden izin istemiş fakat bu talep İtalya da yeterli seviyede koruma olmaması sebebi ile Fransız yetkili makamınca reddedilmiştir. Bunun üzerine FIAT ile Fransız alt şirketi arasında veri koruma ilkelerini içeren bir sözleşme imzalanınca gerekli izin alınmıştır[182].

[182] Murat Uygun, **Avrupa Birliğinin 95/46 Sayılı Veri Koruma Yönergesi Işığında Kişisel Verilerin Korunması,** (Yayınlanmamış Yüksek Lisans Tezi), Gazi Üniversitesi, Sosyal Bilimler Enstitüsü, Ankara, 2010, ss.83-84.

Veri Koruma Yönergesinde "yeterli düzeyde" koruma sağlamayan ülkelere veri aktarılamaması ABD ile AB arasında sorunlara neden olmuştur. İki ülkenin kişisel verilere bakış açısı farklıdır. Çalışmanın ilk bölümünde bahsettiğimiz üzere ABD temel olarak kişisel verilerin korunmasına ekonomik bir hak olarak bakarken AB kişisel verilerin korunmasına temel bir hak olarak algılamaktadır. Bu sebeple ABD mevzuatı, AB mevzuatında bahsedilen "yeterli düzeyde" koruma kriterini karşılamamaktadır. Fakat iki tarafın dünya ticaretinde etkin rolleri göz önüne alındığında taraflar arasında veri akışının durması halinde bu durumun bazı ekonomik problemlere yol açacağı açıktır. Bu sebeple bu problemlerin bertaraf edilmesi için 2000 yılında ABD ile AB aralarında bağışıklık sözleşmesi imzalamışlardır. Fakat bu anlaşma 2015 yılında ABAD sözleşmenin yeterli güvenceleri taşımaması sebebiyle geçersiz olduğuna karar vererek sözleşmeyi yürürlükten kaldırmıştır. Bunun üzerine Avrupa Komisyonu 2016 yılında ABD merkezli bir şirketin veri transferi için yeterli koruma sağladığını ifade ederek bu duruma onay vermiştir. Konuya ilişkin tartışmalar halen devam etmektedir[183].

2. Avrupa Birliği Temel Haklar Şartı

Avrupa Birliği üye ülkeleri birçok temel hakkı bu metinde toplayarak, temel hakların korunması için 07.12.2000 tarihinde Nice şehrinde bu metne imza atmış, metin 01.12.2009 tarihli Lizbon Antlaşmasının kabul edilmesi ile bağlayıcılık kazanmıştır. Avrupa Birliği Temel Haklar şartı temel hak ve özgürlüklerin bilim ve teknolojideki gelişmeler ışığında korunması hedeflenerek imzalanmıştır[184].

Avrupa Birliği Temel Haklar Şartı temelde saygınlık, özgürlükler, eşitlik, dayanışma, yurttaş hakları, adalet kavramları kapsamında altı bölüm halinde düzenlenmiştir. Temel Haklar Şartında kişisel verilerin korunması özel hayatın gizliliği hakkından bağımsız bir hak olarak 8.maddede ayrıca düzenlenmiştir. Avrupa Birliği Temel Haklar Şartı 8.maddesi şu şekildedir:

> *Herkes, kendisini ilgilendiren kişisel verilerin korunması hakkına sahiptir. Bu veriler, adil bir şekilde, belirli amaçlar için ve ilgili kişinin rızasına veya yasa ile öngörülmüş diğer meşru bir temele dayanarak tutulur. Herkes, kendisi hakkında toplanmış verilere erişme ve bunları düzelttirme hakkına sahiptir. Bu kurallara uyulması, bağımsız bir makam tarafından denetlenir.*[185]

---

[183] ABAD, C-362/14 Maximillian Schrems v Data Protection Commissioner, 6 Ekim 2015, ayrıca bkz Küzeci s.204.

[184] Yüksel Metin, "Avrupa Birliği Temel Haklar Şartı", **Ankara Üniversitesi Siyasi Bilimler Fakültesi Dergisi,** Cilt:57, Sayı:4, 2002, ss.46-47.

[185] https://www.avrupa.info.tr/tr/avrupa-birligi-temel-haklar-bildirgesi-708,(10.11.2020).

Avrupa Birliği Temel Haklar Şartında kişisel verilerin korunması hakkının özel hayatın gizliliği ilkesinden ayrı olarak koruma altına alınması oldukça önemli olup, bu durumu kişisel verilerin korunması hakkının bağımsız bir hak olarak kabul edildiğinin önemli bir işaretidir[186].

Avrupa Birliği Temel Haklar Şartı, üye ülkeler için bağlayıcılığı olan ve bağımsız makamlarca ilgili maddelere uyulup uyulmadığının denetlenmesini de öngörmektedir[187].

3. 97/66 sayılı Telekomünikasyon Alanında Kişisel Verilerin İşlenmesi ve Mahremiyetin Korunması Direktifi ve 2002/58/EC Sayılı Elektronik Haberleşme Sektöründe Özel Alanın Korunması ve Kişisel Bilgilerin İşlenmesi Yönergesi

1997 tarihli 97/66 sayılı Avrupa Konseyi ve Avrupa Parlamentosu Direktifi, 95/46/EC sayılı Yönergenin telekomünikasyon sektörünün kendine özgü niteliklerini tamamlaması ve bu konuda ortaya çıkan boşluğu tamamlamak üzere yürürlüğe konmuştur. Fakat bu direktifin iç pazara, gelişen teknolojiye adapte edilememesi, 11 Eylül saldırısının yarattığı ortam ve Avrupa Birliği üye ülkelerinin yarattığı baskı sonucunda 97/66 sayılı Telekomünikasyon Alanında Kişisel Verilerin İşlenmesi ve Mahremiyetin Korunması Direktifi yerini 2002/58/EC Sayılı Elektronik Haberleşme Sektöründe Özel Alanın Korunması ve Kişisel Bilgilerin İşlenmesi Yönergesine bırakmıştır[188]. 2002/58/EC Sayılı Yönergenin yürürlüğe girmesi ile 97/66 Sayılı Direktif yürürlükten kalkmıştır.

Avrupa birliği Komisyonu 2002/58/EC Sayılı Yönergeyi hazırlarken, iletişim araçlarının gelişmişliğini göz önünde bulundurarak geleceğe yönelik tarafsız bir düzenleme yapmak istemiştir[189]. 2002/58/EC Sayılı Yönerge, 95/46/EC sayılı Yönergenin elektronik haberleşme sektörü için ayrılmış spesifik bir versiyonudur. Nitekim Elektronik İletişim Yönergesinde özel olarak düzenlenmeyen konularda 95/46/EC Sayılı Yönergenin uygulanacağı ifade edilmiştir. Bu noktada 29.madde de

---

[186] Küzeci, s.182.
[187] Füsun Ayşe Arsava. "AB Temel Haklar Şartının AB Hukuku ile İlişkisi", **Uyuşmazlık Mahkemesi Dergisi,** Sayı:7, 2016, ss.155-159.
[188] Uyarer, s.61.; Zeynep Ceren Nurata, "Hukuksal, Örgütsel ve Etik Bir Sorun Olarak İşyerinde Elektronik Gözetim", **Gazi İşletme ve İktisat Dergisi**, Cilt:7, Sayı:3, 2021, s.217.
[189] Uygun, s.85.

belirtilen Çalışma Grubunun yorumu yol gösterici olup 95/46/EC Sayılı Yönerge, Elektronik İletişim Yönergesinin kapsamadığı alanlarda uygulanabilecektir[190].

2002/58/EC sayılı direktifin amacı *"Üye ülkelerin elektronik haberleşme sektöründe kişisel bilgilerin işlenmesine ilişkin olarak temel hak ve özgürlüklerin, özellikle de gizlilik hakkının eşit ölçüde korunmasını ve Birlik içinde bu tür veriler ile elektronik haberleşme ekipmanı ve hizmetlerinin serbest bir şekilde dolaşmasını sağlamasını gerektiren hükümleri uyumlaştırmaktır."* şeklinde ifade edilmiştir[191]. Direktifin amacı incelendiğinde, üye devletlere, elektronik haberleşme sektöründe işlenen kişisel verilere ilişkin kullanıcıların temel hak ve özgürlüklerinin, özel yaşamın gizliliği hakkının korunmasının sağlanması ile elektronik haberleşme ekipman ve servislerinin topluluk sınırları içinde serbest dolaşımının amaçlandığı görülmektedir[192].

2002/58/EC sayılı Yönerge, halka açık iletişim vasıtaları ile verilen elektronik iletişim hizmetleri hakkında uygulanacaktır (3.md). Özel ağlar Yönergenin uygulama alanı dışındadır. Halka açık elektronik iletişim hizmeti verenler, bu hizmetlerin güvenliğini sağlamak üzere uygun teknik ve kurumsal tedbirleri almakla yükümlüdürler (4.md). Hizmet sağlayıcısı hizmetin güvenliğini sağlamak için gerekli önlemleri alarak sistemde bir güvenlik açığı bulunması halinde bu durum hakkında abonelerini bilgilendirmelidir[193].

Yönergenin 5.maddesine göre üye ülkeler iletişimin gizliliğinin sağlanması için bu konuda bir yasa çıkarmalı ve kullanıcının rızası veya kanunda verilen açık bir yetki olmaksızın haberleşmenin dinlenmesi, kaydedilmesi, başka bir şekilde müdahale edilmesi, izlenmesi yasaklanmalıdır. Ulusal güvenlik, suçun önlenmesi, kamu güvenliği ve bazı gerekçeler ile bu duruma istisna getirilebilir (15.md).

2002/58/EC sayılı Yönerge de "cookie" adı verilen internete bağlanan bir kullanıcının ziyaret ettiği internet sayfalarının sunucuları tarafından işlenerek kullanıcının alışkanlıklarına göre bir web sayfası oluşturulmasına ilişkin düzenleme de bulunmaktadır (6.md). Yönergeye göre "cookie" adı verilen küçük veri topluluklarının hukuka uygun olması için kullanıcının cookielerinin kullanım amaçları

[190] Küzeci, s.213.
[191] Öngün, s.84.
[192] Hüseyin Aksoy ve Mesut Halıcıoğlu, "E-Gizlilik Tüzüğü Çalışmaları Işığında Türk Hukukunda Elektronik Haberleşmenin Gizliliğinin Korunması", **Kişisel Verileri Koruma Dergisi,** Cilt:2, Sayı:2/1,2020, ss:2-3.
[193] Küzeci, s.214.

için aydınlatılması ve cookilerin yerleştirilmesini engelleme hakkının kullanıcıya sağlanması gerekmektedir[194].

Yönergede istenmeyen iletilere (spamlara) ilişkin de düzenlemeler yapılmıştır. Yönergeye göre abonelere yönelik pazarlama mesajlarının iletilmesi için ilgili kişinin rızası alınmalıdır (13.md). Abonelere ait kişisel veriler, reklam ve pazarlama alanında kullanılacaksa ilgili kişiden mutlaka izin alınmalıdır. Burada abonelere ait verilerin reklam amacıyla kullanılması engellenmek istenmiştir[195].

2002/58/EC sayılı Yönerge, 25.05.2018 tarihli Avrupa Birliği Genel Veri Koruma Tüzüğünün yürürlüğe girmesi ile mülga edilmiştir.

4. 2006/24/AT Sayılı İletişim Trafik Verilerinin Saklanması Yönergesi

Veri gizliliği konusunda 2002/58/EC sayılı Yönergede yer alan eksiklikleri gidermek ve 2005 yılının temmuz ayında İngiltere'de yaşanan terör saldırısı sonucunda bu tür olayların yaşanmadan daha etkin bir şekilde takip edilerek önlenmesi için 2006/24/AT Sayılı İletişim Trafik Verilerinin Saklanması Yönergesi 15 Mart 2006 tarihinde kabul edilerek yürürlüğe girmiştir[196].

Yönergenin çıkarılmasındaki amaç terörizmle ile mücadele ederken trafik verilerine ulaşma da üye devletler arasındaki farklılıkların giderilmesidir. Yönergenin uygulama alanı iletişim trafik verileri ve bulunulan yer bilgileridir. Örneğin, sabit veya mobil telefon görüşmeleri, kısa mesaj gönderimi, internet bağlantısı gibi hizmetleri kullanan kişinin adı, soyadı, IP veya e-posta adresi, iletişimin gerçekleştiği saat ve iletişim süresine ilişkin bilgiler yönerge kapsamındadır. Konuşmanın veya iletişimin içeriği Yönerge kapsamında değildir[197].

Verilerin saklanmasında amaç, ciddi suçların araştırılarak kovuşturulmasıdır (1.md). Ciddi suç kavramına Yönergede yer verilmesine rağmen, ciddi suç tanımının ne olduğu ve ölçütlerine Yönerge de yer verilmemiştir. Bu sebeple herhangi bir suç işleme tehlikesi olmaksızın kişisel verilerin kayıt altında tutulması özel haberleşmenin gizliliği hakkı ve masumiyet karinesi gibi kavramlara aykırı olduğundan Yönerge

---

[194] Korkmaz, s.202; Ayça Atabey ve diğerleri, E-Gizlilik Tüzük Taslağının Son Versiyonu Üzerine Düşünceler, **Kişisel Verileri Koruma Dergisi**, Cilt:1, Sayı:2, 2019, ss. 67-73.
[195] Hayrunnisa Özdemir**, Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması,** 1. Baskı, Seçkin Yayıncılık, Ankara, 2009, s.69.
[196] Öngün, s.85.
[197] Korkmaz, s.204.

oldukça eleştirilmiştir[198]. Nitekim 29. Madde Çalışma Grubu da verilerin yalnızca belirli amaçlar için saklanması gerektiğini ifade etmek durumunda kalmıştır[199].

Avrupa Adalet Divanı, 08.04.2014 tarihinde verdiği karar ile Veri Saklama Direktifinin temel insan hakları, özel hayatın gizliliği, kişisel verilerin korunması hukukunu ağır şekilde ihlal ettiğine karar vererek Veri Saklama Direktifini geçersiz kılmış[200], ayrıca Yönergenin kötüye kullanıma müsait olduğunu ve kötüye kullanım durumunda yeterli güvenceleri sağlamaması ve Yönerge de bulunan düzenlemelerin orantılılık ilkesine de aykırı olduğunu tespit etmiştir[201].

5. Avrupa Birliği Vatandaş Hakkı Direktifi- 2009/136/EC

Avrupa Birliği Vatandaş Hakkı Direktifi 2002/58/EC Sayılı Yönergeyi tadil eden bir düzenlemedir. Vatandaş Hakkı Direktifinde veri güvenliği ve veri gizliliği konusunda bir takım ek düzenlemeler yapılmıştır.

Vatandaş Hakkı Direktifinde veri güvenliği konusunda kullanıcıların haklarının korunması için telekomünikasyon hizmet sağlayıcıların bu konuda gerekli tedbirleri alması gerektiği ifade edilmiştir[202]. Örneğin; cookies adı verilen bilgisayar çerezleri ile veri toplanabilmesi için kişinin 202/58/EC Sayılı Yönergeye göre bilgilendirilmesi ve bu işlemi reddetme hakkının kişiye verilmesi gerekmektedir. Vatandaşlık Hakkı Direktifinde ise kişi cookies adlı çerezler hakkında bilgilendirildikten sonra bu işlemi onaylaması gerekmektedir. Bu metin üzerinde çalışma yürüten 29.Madde Çalışma Grubu kişilerin kabul iradesinin açıkça ortaya koyması gerektiğini ifade etmiştir[203]. Vatandaşlık Hakkı Direktifi bu yönleri ile 2002/58/EC Sayılı Yönerge de yer alan hükümlerden tüketicilerin korunması maksadı ile hazırlanmıştır[204].

[198] Küzeci, s.216; Korkmaz, s.204.
[199] Korkmaz, s.204.
[200] Öngün, s.86.
[201] Küzeci, ss.220-221.
[202] Öngün, s.87.
[203] Uyarer, s.63.
[204] Öngün, s.87.

6. 2016/679 Avrupa Birliği Genel Veri Koruma Tüzüğü (GVKT)

a. Tüzüğe İlişkin Genel Bilgiler

95/46/EC sayılı Yönergenin yürürlüğe girmesinin ardından teknoloji alanında gelişmeler, küreselleşme, internetin büyük kitleler tarafından kullanılmaya başlanması özellikle Google, Facebook gibi bulut bilişim sistemlerinin bireylerin kişisel verilerini işlemesi sonucunda kişisel verilerin işlenmesinde bazı açıklar ortaya çıkmıştır. 95/46/EC sayılı Yönerge veri koruma hukukunun ihtiyacını karşılamayacak duruma gelmiştir. Bu sebeplerle gelişen teknolojiyle uyumlu, çağımızı yakalayacak yeni bir düzenlemeye ihtiyaç duyulmuştur[205].

Yeni bir düzenleme yapılması gerektiğini, böyle bir ihtiyaç olduğunu ABAD kararları da ortaya koymaktaydı. Amerika Ulusal Güvenlik Teşkilatı (NSA) eski analisti Edward Snowden; Google ve Facebook gibi birçok şirketin kullanıcı bilgilerinin NSA'nın dinleme ve gözleme faaliyetlerine konu olduğunu ifade etmiştir[206]. Bunun üzerine Avusturalyalı Max Schrems, Facebook'un Avrupa Birliği vatandaşlarının kişisel verilerini toplanması ve bu verilerin ABD'de bulunan sunuculara aktarılmasını yargı konusu yapmıştır. ABAD önüne gelen bu olayda; kişisel verilerin ABD'de bulunan sunuculara aktarılmasının ABD de bulunan veri koruma hukuk kuralları sebebi ile tehlikeli olabileceğinden bahisle ABD ile AB arasında imzalanan veri transferi anlaşmasını geçersiz kılmıştır[207].

ABAD yine 08.04.2014 tarihinde verdiği karar ile 2006/24/EC sayılı Yönergenin temel insan hakları, özel hayatın gizliliği, kişisel verilerin korunması hukukunu ağır şekilde ihlal ettiğine karar vererek 2006/24/EC sayılı Yönergeyi geçersiz kılmış, ayrıca Yönergenin kötüye kullanıma müsait olduğunu ve kötüye kullanım durumunda yeterli güvenceleri sağlamaması ve Yönerge de bulunan düzenlemelerin orantılılık ilkesine de aykırı olduğunu tespit etmiştir[208].

---

[205] İpek Çimen Bulut, "Avrupa Birliği Genel Veri Koruma Tüzüğü Kapsamında Getirilen Yeni Teknik ve Yaptırım Mekanizmaları", **Anadolu Üniversitesi Sosyal Bilimler Dergisi,** Cilt:20, Sayı:2, 2020, ss.127-129.

[206]Serkan Bulut, "Söylemin Kapatılma ve Açımlama Savaşımında Edward Snowden", **Üsküdar Üniversitesi Etkileşim Dergisi**, Sayı:3, Yıl:2, 2019, ss.131-134.

[207]https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf(01.01.2022); https://tr.sputniknews.com/20200716/abd-ile-ab-arasindaki-veri-transferi-anlasmasi-avrupa-adalet-divanina-takildi-kisisel-veriler-1042468896.html (03.01.2021).

[208] https://curia.europa.eu/juris (01.04.2021).

Bu sebeplerle kişisel verilerin korunması hukukunda mevcut düzenlemelerin yetersiz kaldığı kabul edilerek Avrupa Birliği üye ülkelerinin tümü için geçerli ve bağlayıcı olacak yeni bir düzenleme yapılması ihtiyacı doğmuştur. Bunun sonucunda da 173 paragraflık giriş bölümü ve 99 maddeden oluşan GVKT, 27 Nisan 2016 tarihinde kabul edilmiş ve 24 Mayıs 2016 tarihinde Avrupa Birliği tarafından onaylanmıştır. Tüzük için iki yıllık bir geçiş süresi belirlenmiş bu sebeple Tüzük 25 Mayıs 2018 tarihinde yürürlüğe girmiştir.

Çalışmamızın bu kısmında GVKT hakkında genel bilgilere yer vermekle birlikte, GVKT ile Avrupa Birliği mevzuatında getirilen temel değişiklikler ve yenilikleri incelenecektir.

b. GVKT'nin Öngördüğü Temel Değişiklik ve Yenilikler

(1) Kapsam ve Uygulama Alanı

GVKT uygulama alanı ve kapsamı bakımından yalnızca AB üye ülke devletleri için değil, Avrupa Birliği üye devletleri ile ekonomik bağlarını sürdürmek isteyen diğer dünya devletleri açısından da küresel bir öneme sahiptir. GVKT bu başlık altında incelenecek düzenlemelerinde görüleceği üzere GVKT dünya çapında uygulanabilir niteliktedir[209].

GVKT'nin uygulama alanını ve kapsamını düzenleyen 3.maddesinde üç tipik durumda GVKT'nin kapsam alanı ifade edilmiştir. Bu durumlardan birincisi Avrupa Birliği sınırları içerisinde gerçekleştirilen veri işleme faaliyeti; ikincisi Avrupa Birliği sınırları içerisinde verilerin işlenip işlenmediğine bakılmaksızın Avrupa Birliği sınırlarında bulunan kişilere mal ve hizmet sunulması bir diğer üçüncü durum ise Avrupa Birliği sınırları içerisinde bulunan kişilerin davranışlarının gözlenmesi halidir. Ayrıntılı şekilde incelenirse:

GVKT'nin 3/1.maddesinde yer alan düzenlemeye göre veri sorumlusunun veya veriyi başka birisi adına işleyen gerçek ve tüzel kişinin Avrupa Birliği sınırları içerisinde faaliyetlerini gerçekleştirilmesi halinde GVKT uygulama alanı bulacaktır. Verisi işlenen gerçek veya tüzel kişinin Avrupa Birliği sınırları içerisinde olması

[209] Ufuk Dal, "Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Ülke Dışı Uygulama Yetkisi ve Bu Yetkinin Uluslararası Hukukta Meşruiyeti", **Kişisel Verileri Koruma Dergisi**, Cilt:1, Sayı:1,21, 2019, ss.24-29.

GVKT'nin uygulanması için yeterlidir[210]. Verisi işlenen kişilerin Avrupa Birliği vatandaşı olması gerekmemektedir. Tüzel kişiler için burada önemli olan husus şirket merkezinin nerede olduğu değil, nerede faaliyet gösterdiğidir. Örneğin; Avrupa Birliği üyesi olmayan ülkemizde Türk kanunlarına göre kurulan bir tüzel kişi, Fransa ile olan ekonomik ilişkilerinde Fransa ile yaptığı ekonomik temas kapsamında işlediği kişisel veriler açısından GVKT uygulama alanı bulacaktır.

GVKT'nin uygulanması açısından Avrupa Birliği'nde bulunan kişilere mal ve hizmet sunma iradesi de oldukça önemlidir. İşletme faaliyetlerinin Avrupa Birliği'nde bulunan veri sahiplerine mal ve hizmet sunulmasını kapsaması halinde GVKT veri sorumluları için uygulama alanı bulacaktır. Bu sebeple GVKT'nin uygulanması açısından ürün ve hizmet sunma iradesinin tespiti son derece önemlidir. Veri sorumlusu açık bir irade beyanı ile Avrupa Birliğinde ikamet eden gerçek kişiler ile ticari bir ilişki içine girmek istediğini ifade etmelidir[211]. Veri sorumlusunun web sayfasında İngilizce gibi Avrupa Birliği dışında da dünyada kullanılan bir dilin kullanılması veyahut web sayfasında e-posta adresine yer vermesi veri sorumlusunun açık iradesini göstermez. Fakat veri sorumlusunun web sayfasında Avrupa Birliğinde yaygın bir dilin kullanılması ve farklı para birimlerinde ödeme imkânı sunması açık iradenin varlığı anlamına gelecektir. Buradan Avrupa Birliği dışında kurulan fakat Avrupa da faaliyet gösteren Amazon, Google, Facebook gibi bulut tabanlı hizmet sunucularının GVKT hükümlerine tabi olacağını göstermektedir[212].

GVKT 3/2(b). maddesinde belirtilen gözleme faaliyeti kişilerin internet üzerinde yaptıkları faaliyetlerinin izlenmesi ve takip edilmesidir. Bu durum cookies (çerez) kullanımını ifade etmektedir. Çerezler yolu ile kişilerin internet üzerinde ki hareketleri, alışveriş alışkanlıkları, zevkleri, harita uygulamaları, sağlık ve diyet alışkanlıkları gibi konularda bilgi edinilmektedir. Bu sebeple, kişilerin haklarının korunması ve kişisel verilerin güvenilir şekilde işlenmesi için çerez kullanımı vasıtası ile Avrupa Birliği sınırları içerisinde işlenen veriler GVKT'nin uygulama alanına ve kapsamına girmektedir[213].

---

[210] Cansu Akgün Tekgül, "Brüksel 1Bis Tüzüğü İle Avrupa Birliği Genel Veri Koruma Tüzüğü Çerçevesinde Kişisel Verilerin İhlaline İlişkin Özel Hukuk Uyuşmazlıklarında Milletlerarası Yetki Kuralları", **Hacettepe Hukuk Fakültesi Dergisi**, Cilt:9, Sayı:1, 2019, ss.260-261.; Dülger, ss.103- 104.

[211] Çekin, s.40.

[212] Murat Volkan Dülger, "Avrupa Birliği Genel Veri Koruma Tüzüğü Bağlamında Kişisel Verilerin Korunması", **Yaşar Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:1, Sayı:2,71, 2019, (GVKTKV), ss.98.

[213] Çekin, s.42.

(2) Rıza

(i) Genel Olarak

95/46/EC Sayılı Yönergede rızanın kişisel verilerin işlenmesinde hukuka uygunluk sebebi olarak kabul edilmesi için niteliği bakımından açık bir kriter belirlenmemiş rızanın geçerliliği her ülkenin kendi iç mevzuatında ki düzenlemelere bırakılmıştır. Örneğin, Fransa da rızanın açık şekilde verilmesi ön görülürken, Belçika da internet tarayıcısının otomatik ayarlarını değiştirmemek rıza olarak kabul ediliyordu. GVKT ile AB üyesi ülkelerde geçerli bir rızanın nasıl olması gerektiği açık bir şekilde ifade edilmiştir[214].

GVKT'nin 4. Maddesi 11. fıkrasında rıza *"veri sahibinin bir beyan yoluyla ya da açık bir onay eylemiyle kendisine ait kişisel verilerin işlenmesine onay verdiğini gösteren özgür bir şekilde verilmiş spesifik, bilinçli ve açık gösterge"* şeklinde tanımlanmıştır.

GVKT uyarınca kişi rızasını açıkça aktif bir tavır ile hiçbir baskı ve etki altında kalmaksızın özgürce vermelidir. Örneğin, kişinin aktif eylemini içermeyen internet ortamında onay vermeye ilişkin kutucuğun kişi tıklamaksızın işaretli olduğu durumlarda rıza geçerli olmayacaktır[215]. GVKT kişinin hareketsiz, sessiz kalması sonucunda açık bir rızadan bahsedilemeyeceğini kişinin özgürce karar veremediğini ifade etmiştir.

GVKT'ye göre rızanın hangi faaliyete ilişkin verildiğinin açık ve anlaşılabilir olması genel bir onay şeklinde olmaması gerekmektedir. Herkesin anlamayacağı bir hukuki metin aracılığıyla alınan rıza geçerli değildir, rıza metninde herkes tarafından anlaşılır açık ve sade bir dil kullanılır. Veri işleme faaliyeti birden fazla amaç için yapılıyorsa her bir veri işleme faaliyeti için kişiden ayrıca rıza alınmalıdır. Kişi verdiği rızayı her zaman geri alabilme hakkına sahip olduğu gibi rızanın geri alınması da rızanın verilmesi kadar kolay olmalıdır. Rızanın ilgili kişi tarafından geri alınması halinde, rızanın geri alınana kadar gerçekleştirilen veri işleme faaliyetlerinin hukuka uygun olduğunun kabulü gerekmektedir (7.md).

GVKT'ye göre rızanın veri işleme faaliyetinden önce alınması gerekmektedir. Sonradan ilgili kişiden icazet şeklinde alınan rızalar geçerli değildir.

---

[214] Develioğlu, s.52.; Serdar Çelikel, "Kişisel Verilerin İşlenmesinde, Açık Rıza Hukuka Uygunluk Nedeninin, 95/46 Sayılı Direktif ve GDPR ile Karşılaştırmalı Olarak İncelenmesi**", Uyuşmazlık Mahkemesi Dergisi,** Sayı:17, 2021, ss.168-169.
[215] Çekin, s.90.

GVKT'nin yürürlük tarihi 25 Mayıs 2018 tarihinden önce kişisel verilerin işlenmesine ilişkin alınan rızalar, GVKT'ye uygun olması halinde geçerliliği devam edecektir. Veri sorumlularının GVKT yürürlüğe girmeden önce aldığı rızaların tamamı geçersiz olmayıp, GVKT yürürlüğe girdikten sonra alacakları rızanın GVKT'ye uygun olması gerekmektedir[216].

(ii) Çocuklara Ait Kişisel Verilerin İşlenmesinde Rıza

95/46/EC sayılı Yönergede çocukların kişisel verilerinin işlenmesine ilişkin bir düzenleme bulunmamaktaydı. Bu sebeple 95/46/EC Sayılı Yönerge bu konuda eleştirilmiş[217] ve GVKT de bu hususta çocukların kişisel verilerinin işlenebilmesi için açık rıza gerektiğine dair bir hüküm getirilmiştir. GVKT'nin 8.maddesine göre 16 yaşından küçük çocukların doğrudan bilgi toplum hizmetlerine erişimi esnasında toplanan verileri için rıza, çocuğun veli ya da vasisi tarafından verilerek onaylanmalıdır[218]. Veri sorumlusu ebeveyn tarafından verilen onay veya rızanın yetkili ebeveyn tarafından verildiğini "makul bir çaba" ile denetlemelidir.

Türk Hukukunda, çocukların kişisel verilerinin işlenmesine ilişkin özel bir düzenleme bulunmamaktadır. Çocukların kişiliklerinin henüz oturmaması, korunmaya ihtiyaçları olması sebebiyle bu konuya ilişkin özel bir hukuki düzenlemenin Türk Hukukunda yapılması gerektiği kanaatindeyiz.

(3) Unutulma Hakkı ve Veri Taşınabilirliği Hakkı

Unutulma hakkı ve veri taşınabilirliği hakkı GVKT ile ortaya konan, veri sahibine tanınan haklarındandır. Unutulma hakkı ve veri taşınabilirliği hakkına ilişkin detaylı bilgi ve açıklamayı çalışmamın veri sahibinin (ilgili kişinin) hakları kısmında yer verdiğimden burada tekrara düşmemek için bu haklardan ayrıca bahsetmeyeceğim. Unutulma hakkı GVKT'nin 17.maddesinde, veri taşınabilirliği hakkı GVKT'nin 20.maddesinde düzenlenmiş olup, konunun detayları için çalışmamın 1. bölümü incelenebilecektir[219].

---

[216] Dülger, s.230.
[217] Çekin, s.99.
[218] Murat Uçak ve Serdar Çelikel, "Kişisel Verilerin İşlenmesinde, Açık Rıza Hukuka Uygunluk Nedeninin, 95/46 Sayılı Direktif ve GDPR ile Karşılaştırmalı Olarak İncelenmesi", **Kişisel Verileri Koruma Dergisi,** Cilt:3, Sayı:1, 2021, s.54.
[219] 1. Bölüm Kişisel Verilerin Korunmasına İlişkin Genel Açıklamalar, IV. Veri Sahibinin Hakları, C. Unutulma Hakkı- G.Veri Taşınabilirliği Hakkı

(4) Veri Koruma Etki Değerlendirilmesi

Veri koruma etki analizi veri sorumlusuna GVKT ile yüklenen sorumluluklardan birisidir. Yeni teknolojilerin kullanımı sırasında veri işleme türünün şekli, kapsamı, amacı kişi hürriyeti ve hakları açısından ciddi bir tehlikeye yol açabilecek ise bu teknolojiyi kullanan veri sorumlusunun etki analizi yaptırması gerekmektedir. GVKT de veri sorumlularına kişisel veriler işlenirken oluşabilecek tehlikeleri öngörme ve bunları önlemeye ilişkin bir nevi "erken uyarı mekanizması" teşkil eden bu analiz sistemi öngörülmüştür[220]. Bu analiz özellikle profilleme, özel nitelikli kişisel verilerle suçlara ilişkin kişisel verilerin işlenmesinde kullanılacaktır[221]. GVKT'nin 35/3.maddesi hangi durumlarda veri koruma etki analizi yapılması gerektiği ifade edilmiştir. Maddeye göre;

"(a) gerçek kişilerle ilgili kişisel özellikler hususunda profil çıkarma da dahil olmak üzere otomatik işlemeye dayalı olan ve gerçek kişi ile ilgili hukuki sonuçlar doğuran veya gerçek kişiyi kayda değer şekilde etkileyen kararların dayandığı sistematik ve kapsamlı bir değerlendirme;

(b) 9(1) maddesinde atıfta bulunulan özel kategorilerdeki verilerin veya 10. maddede atıfta bulunulan mahkûmiyet kararları ve ceza gerektiren suçlara ilişkin kişisel verilerin büyük çaplı olarak işlenmesi veya

(c) kamunun erişebileceği bir alanın büyük çaplı olarak sistematik bir şekilde izlenmesi halinde" Veri koruma etki analizi yapılmalıdır.

Veri koruma etki analizinde asgari olarak hangi şartların değerlendirilmesi gerektiği GVKT'nin 35/7.maddesinde sayılmıştır. Maddeye göre;

"(a) Uygun olduğu hallerde, kontrolör tarafından gözetilen meşru menfaat de dahil olmak üzere öngörülen işleme faaliyetleri ve işleme amaçlarına ilişkin sistematik bir açıklama;

(b) İşleme faaliyetlerinin amaçlarla ilişkili olarak gerekliliği ve orantılılığına yönelik bir değerlendirme;

(c) 1. paragrafta atıfta bulunulduğu üzere veri sahiplerinin hakları ve özgürlüklerine yönelik risklere ilişkin bir değerlendirme,

---

[220] Çekin, s.210.

[221] Hidayet Takçı ve Pelin Canbay, "Kişisel Verilerin Korunmasında Öznitelik Tabanlı Gizlilik Etki Değerlendirmesi Yöntemi", **Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi,** Cilt:32, Sayı:4, 2017, ss:1301-1302.

(d) Veri sahipleri ve ilgili diğer kişilerin hakları ve meşru menfaatleri dikkate alınarak, kişisel verilerin korunmasının sağlanması ve bu Tüzüğe uygun hareket edildiğinin gösterilmesiyle ilgili güvenceler, güvenlik tedbirleri ve mekanizmalar da dahil olmak üzere risklerin ele alınması hususunda öngörülen tedbirler." Veri koruma etki analizinde değerlendirilmelidir.

Risk grubu ne kadar yüksek ise analiz de o kadar ayrıntılı olmalıdır. Veri koruma etki analizine ilişkin raporda kişilerin hak ve özgürlüklerine dair risk analizine de mutlaka yer verilmelidir[222].

Veri sorumlusu, veri koruma etki analizi sonucunda veri işleme faaliyetine ilişkin gerekli tedbirleri almaz ise, işlemenin yüksek riskli olduğu kanaatine varırsa GVKT'nin 36.maddesi uyarınca denetim makamının ön görüşüne başvurmalıdır.

(5) Veri Koruma Görevlisi

GVKT ile öngörülen yeni kurumlardan biri de veri koruma görevlisidir. GVKT de yapılan bu yeni düzenlemeyle kurumların GVKT'ye uyum sağlamaları, kişisel verilerin korunması hakkında öneriler üretilmesi, hesap verilebilirlik ve diğer GVKT de belirtilen ilkelere etkinlik kazandırmak amaçlanmıştır[223].

Veri koruma görevlileri; işleme faaliyetinin kendi yargı yetkisi çerçevesinde hareket eden mahkemeler haricindeki bir kamu kuruluşu veya organı tarafından gerçekleştirilmesi, işleyicinin temel faaliyetlerinin yapıları- kapsamları veya amaçları gereği veri sahiplerinin düzenli ve sistematik bir şekilde büyük çaplı olarak izlenmesini gerektiren işleme faaliyetlerinden meydana gelmesi, işleyicinin temel faaliyetlerinin özel kategorilerdeki verilerin ve mahkumiyet kararları ceza gerektiren suçlara ilişkin kişisel verilerin büyük çaplı olarak işlenmesinden meydana gelmesi hallerin de veri sorumlusu ve işleyenler tarafından atanırlar(37.md). Bunun dışında kurumlarca isteğe bağlı olarak da veri koruma görevlileri atanabilir. GVKT'nin 37.maddesinde belirtilen esas faaliyet kavramı veri sorumlusunun amacına ulaşmak için gerekli bütün önemli işleme faaliyetleri olarak tanımlanmaktadır. Örneğin; hastanelerin esas faaliyet nedeni hastaların tedavisidir. Hasta bilgilerinin işlenmesi hastanın tedavi edilmesi için kaçınılmazdır. Bu sebeple de buradan hastanelerin esas faaliyetinin kişisel verilerin işlenmesi olduğunu söylemek mümkündür. GVKT'nin 37/2.maddesinde belirtilen ilgili

[222] Çekin, s.214.
[223] Metin Turan, **Karşılaştırılmalı Hukukta Kişisel Verilerin Korunması**, 4 Baskı, Seçkin Yayıncılık, 2021, s.208.

kişinin düzenli ve sistematik izlenerek verilerinin işlenmesinden ise, çevrimiçi ve çevrimdışı bütün izleme ve profil çıkarma faaliyetleri anlaşılmalıdır. Örneğin, mobil uygulamalar ile kişilerin takip edilmesi, kişinin yaptığı alışverişin yer-miktar-zaman-içeriğine ilişkin bilgilerin toplanmasıdır[224].

GVKT'ye göre şirket toplulukları her bir işletme tarafından kolayca erişilebilir olması koşulu ile tek bir veri koruma görevlisi atayabilecektir. Atanan veri koruma görevlisi, veri sorumlusundan talimat almaz. Veri sorumlusu görevinin ifa etmesi sebebi ile veri koruma görevlisini cezalandıramaz. Veri sorumlusu, veri koruma görevlisi görevini yerine getirirken gerekli tüm belge ve bilgileri veri koruma görevlisine vermekle yükümlüdür. Şirket bünyesinde bulunan herkes veri koruma görevlisinden veri güvenliği konusunda bilgi alabilir. Veri koruma görevlisi şirket içinden veya dışından bir kişi olabilir fakat veri koruma görevlisinin her hâlükârda veri korunması alanında yeterli bilgi ve beceriye sahip olması gerekmektedir[225].

Veri koruma görevlisi, veri koruma hükümleri hakkında ilgili kişi ve kurumları bilgilendirerek danışmanlık yapmalı, işleme faaliyeti ile kişisel verilerin korunması hakkında politikaların uyumunu sağlayarak, veri koruma etki değerlendirmesi konularında talep halinde tavsiyelerde bulunup, denetim otoritesi ile iş birliği ile iletişimin sağlanması hususlarını yerine getirmelidir (39.md).

KVKK da "veri koruma görevlisi" kavramına yer verilmemiş olup, kurumların veri koruma görevlisi atama zorunluluğu bulunmamaktadır. Fakat buna ilişkin zorunlu bir hüküm bulunmamakta birlikte, yasak bir hükümde bulunmadığından veri sorumlularının isterlerse veri koruma görevlisi atayabilmeleri kanaatimizce mümkündür.

(6) Tasarımdan İtibaren Veri Koruma ve Veri Mahremiyeti İlkesi

Tasarımdan itibaren veri koruma ve veri mahremiyeti ilkesi belirli süredir mevcut olmakla birlikte GVKT ile hukuki düzenlemeye konu olmuştur[226]. Bu düzenleme ile veri sorumlusuna veri işleme faaliyetinde kullanılacak yöntemi belirleme ve verilerin işlenmesi sırasında veri koruma ilkelerinin etkili bir şekilde uygulamasını sağlamak üzere gerekli tedbirleri alma yükümlülüğü getirilmiştir.

---

[224] Çekin, ss.208-209.
[225] GVKT 38md.; Yasin Aydoğdu, "Kamu İdaresinde Kişisel Verilerin Korunması", **Selçuk Üniversitesi Hukuk Fakültesi Dergis**i, Cilt:29, Sayı:1, 2021, s.290.
[226] Dülger, s.108.

GVKT'nin 25.maddesinde düzenlenen bu ilkeye göre veri sorumlusu, bireylerin açık müdahalesi olmaksızın kişisel verilerinin belirsiz sayıda kişi tarafından ulaşılabilir olmamasını sağlaması gerekmektedir. Örneğin; bir sosyal medya sitesine yeni üye olan bir bireyin üyeliğinin ilk anında kişisel verileri kendiliğinden yeterli ve sınırlı sayıda diğer kullanıcılar ile paylaşılmalıdır. Kişinin adı-soyadı profilinde yer alacaksa da kişinin rızası olmaksızın kişinin diğer kullanıcılarla yaşı ve cep telefon numarasının paylaşılmaması bu duruma örnektir[227]. Kişinin cep telefonu ve yaşı ancak kişinin rızası ile sonradan paylaşılabilir hale gelecektir.

Tasarımdan itibaren veri koruma ve veri mahremiyeti ilkesinin kanaatimizce GVKT ile getirilmesinin sebebi veri ihlallerinin kişisel verilerin işlenmesi faaliyetinin en başında önlenmesini sağlamaktır. Burada öncelik veri güvenliği olup, kişilerin rızası olmaksızın verilerin paylaşılması engellenmek istenmiştir.

(7) Veri İhlali Bildirim Yükümlülüğü

Veri sorumlusu işlediği kişisel verilerin güvenliğini sağlayacak tedbirleri almalıdır. Veri sorumlusunun gerekli tedbirleri alması veyahut almaması halinde herhangi bir sebeple işlenen kişisel verilerin başkalarının eline geçmesi durumunda veri sorumluları GVKT hükümlerine göre veri ihlali bildiriminde bulunmalıdır.

GVKT'nin 4/12.maddesinde veri ihlali *"… iletilen, saklanan veya işlenen kişisel verilerin kazara veya yasa dışı yollarla imha edilmesi, kaybı, değiştirilmesi, yetkisiz şekilde açıklanması veya bunlara erişime yol açan bir güvenlik ihlalidir"* şeklinde tanımlanmıştır.

GVKT'nin 4/12.maddesinde belirtilen veri ihlalinin olduğu durumlarda GVKT'nin 33.maddesi uyarınca veri sorumlusu ihlalin gerçek kişilerin hak ve özgürlüklerine zarar vermesi düşük bir risk teşkil etmediği durumlarda, ihlali, yetkili denetim makamlarına bildirmelidir. İhlali öğrendiği an veri sorumlusu ihlal ile ilgili tam ve detaylı bilgiye sahip olmayabilir. Veri sorumlusu ihlali öğrendiği andan itibaren en kısa sürede elindeki mevcut bilgiler ile ihlali gerekli kurumlara bildirmeli, daha sonra ilave araştırmalar sonucunda ihlal ile ilgili ek bilgi edinirse ek bilgileri de öğrendiği andan itibaren en kısa sürede bildirmelidir. Örneğin; müşteri ve çalışanlarının kişisel verilerinin bulunduğu sistemine üçüncü kişilerle sızıldığını fark eden fakat kimin ne şekilde ne zaman sızdığını bilmeyen veri sorumlusu ihlali öğrenir öğrenmez bildirimde

[227] Uyarer, s.73.

bulunmalı diğer hususlarda araştırma yapmayı beklememelidir[228]. Bildirim gecikmeksizin ve mümkün ise ihlalin gerçekleştiğinin öğrenilmesi tarihinden itibaren her hâlükârda 72 saat içinde yapılmalıdır. 72 saatin geçirilmesi halinde veri sorumlusunun bu gecikmeyi gerekçesi ile birlikte bildirmelidir.

Veri sorumlusunca veri ihlal bildirimi yapılırken GVKT'nin 33.maddesi uyarınca; ihlalin gerçekleştiği ilgili veri sahibi kategorileri ve yaklaşık veri ihlalinin mahiyeti, kişisel veri ihlalinin olası sonuçları, kişisel veri ihlalinin olası olumsuz etkilerinin azaltılmasına yönelik tedbirler de dahil olmak üzere kişisel veri ihlalinin ele alınması için alınan veya alınması önerilen tedbirler açıklanarak veri ihlali bildirimi yapılır.

(8) İdari Yaptırımlar Yoluyla Koruma

GVKT, güçlü yaptırım seçenekleri ile modern ve kapsamlı bir şekilde kişisel verilerin korunmasını amaçlayarak, kişisel verilerin ihlali durumunda ihlallere karşı ilgiliye şikâyet hakkını öngörmüştür[229]. İlgili kişi; olağan yerleşim yeri, iş yeri, ihlalin gerçekleştiği iddia edilen yer denetim makamına kendisine ait kişisel verilerin GVKT'ye aykırı olarak işlendiğine dair şikâyette bulunabilir. Denetim makamı, ilgili kişiyi şikayetinin durumu hakkında bilgilendirir (77.md).

İlgili kişi, denetim makamının 3 ay içerisinde şikâyeti ele almaması, şikâyetin durumu ve sonucu hakkında bilgilendirilmemesi durumunda yasal yollara başvurabilir. Denetim makamı aleyhine açılan davalarda denetim makamının bulunduğu devlet mahkemeleri yetkilidir (78.md).

GVKT de veri koruma ihlallerinin olması durumunda idari para cezası verilmesi de öngörülmüştür. GVKT de yüksek meblağlı ceza miktarlarına yer verilmiştir. Bunun sebebi kanaatimce kişisel verilerin ihlali halinde cezaların etkili ve caydırıcı olmasını sağlayarak ihlallerin önüne geçmektir. GVKT'nin 83.maddesinde idari para cezalarına ilişkin hükme yer verilmiştir. Hükümde ceza miktarları belirlenirken veri işleme faaliyetinin amacı, kapsamı, ihlalden etkilenen kişi sayısı, kast, ihmal, ihlalin denetim makamlarına bildirip bildirilmemesi, gerekli önlemlerin alınıp alınmadığına ilişkin kriterler incelenmektedir.

---

[228] Dülger, s.250.

[229] İbrahim Barış Sayar,
"The Administrative Fines Regime of the General Data Protection Regulation and Its Impact ",**Kişisel Verileri Koruma Dergisi,** Cilt:3, Sayı:1, 2021, s.1.

GVKT'nin uygulama alanı ve kapsamı bölümünde açıklandığı üzere, GVKT yalnızca Avrupa Birliği sınırları içerisinde değil, Avrupa Birliği sınırları içerisinde veri işleme faaliyeti gerçekleştiren, Avrupa Birliği sınırları içerisinde mal ve hizmet sunan, kişilerin davranışlarını gözlemleyen veri sorumluları hakkında uygulanabileceğinden özellikle Google, Amazon, Facebook gibi şirketlere idari para cezası uygulanabilecektir. Nitekim, Fransa; Google şirketine kullanıcıları verilerin işlenmesi konusunda rıza vermeye zorladığı yönünde yapılan şikâyet üzerine 57 milyon dolar ceza kesmiştir[230].

[230] Uyarer, ss.67-68.

ÜÇÜNCÜ BÖLÜM
TÜRK HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASI

I. GENEL OLARAK

Türk Hukukunda kişisel verilerin korunmasına ilişkin yakın zamana kadar herhangi bir düzenleme bulunmamaktaydı. 2010 yılında Türkiye'de yapılan Anayasa değişikliğine kadar Türkiye Cumhuriyeti Anayasasında kişisel verilerin korunması hakkına temel hak ve özgürlükler içerisinde yer verilmemiştir. Kişisel verilerin korunması Türk Hukukunda 2010 yılı öncesinde Türkiye Cumhuriyeti (T.C) Anayasasında yer alan insan onuruna uygun şekilde hayat sürülmesi hakkı, 2.md de bulunan hukuk devleti ilkesi, 17.md bireyin maddi-manevi varlığını serbestçe geliştirme hakkı, 20.md özel hayatın gizliliği hakkı, 22.md haberleşmenin gizliliği, 25.md bulunan düşünce ve kanaatleri açıklamaya zorlanamama hakkı kapsamında korunmuştur[231]. Nitekim AYM'nin bu konuda birden çok kararı olmakla birlikte[232]; 2008 yılında kişisel verilerin korunması hakkında verdiği bir kararında, kişisel verilerin özel hayatın gizliliği ve düşünce özgürlüğü hakkı kapsamında değerlendirerek hüküm kurmuştur.

Bireylerin temel hak ve özgürlüklerinin daha etkin şekilde korunması, Avrupa ülkeleri ile gelişen ilişkiler, Türkiye'nin 108 sayılı Kişisel Verilerin Otomatik İşlemesi Karşısında Bireylerin Korunması Sözleşmesini ilk imzalayan ülkelerden biri olmasına rağmen uzun bir süre bu konuda somut bir adım atılmaması sebepleriyle[233] 12 Eylül 2010 tarihinde yapılan referandum yolu ile kişisel verilerin korunması hakkı ilk kez T.C Anayasasına girmiştir[234]. 1982 tarihli T.C Anayasası'nın "özel hayatın gizliliği" başlıklı 20.maddesine eklenen 3. fıkrası şu 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*

---

[231]Korkmaz, ss.268-275; Küzeci, ss.318-319; Öngün, s.94.

[232] Anayasa Mahkemesi Kararı, E. 1996/68, K. 1999/1 (19.01.2001 tarih ve 24292 sayılı R.G.); Anayasa Mahkemesi Kararı, K.T 20.03.2008, E. 2006/167, K. 2008/86 (25.06.2008 tarih ve 26917 sayılı R.G).

[233] Dülger, s.110

[234] Hakan Yıldırım ve Volkan Kaplan, "2010 Anayasa Değişikliğinin Bilişim Suçlarıyla Mücadele Politikası Bakımından Etkilerinin Analizi ve Bu Amaçla Kurulan Kuruluşların İncelenmesi", **Kamu Yönetimi ve Politikaları Dergisi,** Cilt:2, Sayı:3, 2021, ss:299-300.

öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."

Madde metninde kişisel verilerin korunması hakkı kapsamında bireye; verilere erişim hakkı, düzeltme ve silme haklarının, orantılılık ve amaca bağlılık ilkesine yer verildiği görülmektedir.

T.C Anayasasının 20/3.maddesi haricinde, Anayasanın 90.maddesi uyarınca da usulünce onaylanan uluslararası sözleşmeler kanun hükmünde olduğundan, AİHS 8.maddesi ve AİHM kararları ışığında kişisel verilerin korunması hukuku kapsamında ki gelişmeler Türk Hukuku açısından da bağlayıcıdır[235].

Çalışmamızın bu bölümünde 24 Mart 2016 yılında kabul edilen 7 Nisan 2016 tarihinde yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu ve önemli ilgili mevzuat hükümleri incelenecektir.

II. 6698 SAYILI KİŞİSEL VERİLERİN KORUNMASI KANUNU

A. Kanunun Amacı ve Kapsamı

KVKK'nın amacı 1.maddesinde *"Bu Kanunun amacı, kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektir."* şeklinde ifade edilmiştir. Kanunun lafzından KVKK'nın temel hedefinin kişi hak ve özgürlüklerini korumak olduğu söylenebilir. KVKK'nın 1.maddesinin gerekçesinde ise kanun çıkarılma amacının; kişisel verilerin işlenmesinin disiplin altına alınması, kişisel veriyi işleyen gerçek ve tüzel kişilerin işleme sırasında tabi oldukları yükümlülüklerin, usul ve esasların belirlenmesi olduğu ifade edilmiştir[236]. KVKK ile kanun koyucu; kişisel verilerin gelişigüzel-düzensiz şekilde işlenip yetkisiz üçüncü kişilerin eline geçmesini engelleyerek ilgili kişilerin temel hak ve özgürlüklerinin etkin şekilde korunmasını hedeflemiştir[237].

Kanunun kapsamından, kanunun içerdiği hükümlerin uygulama alanı bulacağı kişi ve hususlar anlaşılır. KVKK'nın 2.maddesinde kanunun kapsamı *"kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da*

---

[235] Derya Belgin, "Anayasa'nın 90. Maddesinde (7 Mayıs 2004) Yapılan Değişikliğin Getirdiği Sorunlar ve Çözüm Öneriler", **Ankara Barosu Dergisi**, Sayı:4, 2008, ss.110-113.
[236] Gemicioğlu, ss.5-6.
[237] Dülger, s.345; Korkmaz, s.276.

herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler" olarak ifade edilmiştir. Hükümden, kanunun uygulama kapsamının iki kısma ayrılarak verisi işlenen kişi ve veriyi işleyen kişi bakımından düzenleme yapıldığı görülmektedir.

Öncelikle verisi işlenen kişiler bakımından, KVKK'nın uygulanabilmesi için verileri işlenen kişilerin gerçek kişi olması gerekmektedir. Tüzel kişilerin verileri kanun kapsamının dışında bırakılmıştır[238]. Bununla birlikte tüzel kişilerin bünyesinde bulunan verilerin gerçek kişilerle ilişkilendirilebilir ve kişinin kimliğinin belirlenebilir kılması halinde ise bu verilerinde kanun kapsamında korunacağı da ifade edilmektedir[239].

Verileri işleyen kişiler noktasında ise kanun, tüzel kişi veya gerçek kişi ayrımı yapmamış kanun kapsamında verilerin korunması için işleme koşullarını düzenlemiştir. Verilerin otomatik veya kısmen otomatik yollarla ya da herhangi bir kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla gerçek kişi veya tüzel kişiler tarafından işlenmesi halinde kanun uygulama alanı bulacaktır. Otomatik ya da kısmen otomatik kayıt sistemleri otomatik yöntemlerle veri işleyen sistemlerdir. Tamamen veya kısmen otomatik kayıt işleme sistemlerinin ayrımında sistemin tamamen kendi başına mı yoksa insan müdahalesiyle çalışıp çalışılmadığına bakılmalıdır. Tam otomatik sistemlerde veri tamamen sistem aracılığıyla elde edilerek analiz edilmekte iken; kısmen otomatik veri kayıt sisteminde insan müdahalesi ile veri kaydedilmektedir. Örneğin; akıllı cep telefonları, bilgisayarlar, dronlar otomatik kayıt sistemleridir[240].

Herhangi bir veri kayıt sisteminin bir parçası olmakla birlikte, otomatik olmayan yollarla işlenen veriler kanun kapsamında korunmamaktadır. Gelişigüzel şekilde belirli kriterlere göre yapılandırılmayarak işlenen kişisel veriler bu kanunun uygulama alanı kapsamına girmemektedir. Örneğin; Hastanelerde tutulan hasta dosyaları kanun bakımından uygulama alanı bulacakken, müşterinin adı-soyadı ve telefon numarasını bir kâğıda yazıp mağazaya bırakması halinde bir veri kayıt sistemi bulunmadığından bu durum kanun kapsamında korunmayacaktır[241].

---

[238] Gazi Osman Güçlütürk, "Blok Zincir Üzerinde Depolanan Verilerin Kişisel Veri Niteliği ve Silinemezlik, Yok Edilemezlik Sorunu", **Kişisel Verileri Koruma Dergisi**, Cilt:1, Sayı:2, 2019, s.33.
[239] Dülger, s.347.
[240] Çekin, ss. 26-27.
[241] Çekin, s.28.

B. Kanunun Kapsamı Bakımından Öngörülen İstisnalar

KVKK'nın uygulama alanı ve kapsamı 2.maddesinde ifade edilmekle birlikte, kanunun 28.maddesinde "istisnalar" başlığı altında kanunun kapsam dışı bırakıldığı birtakım istisnalar düzenlenmiştir. Bu istisnalar tamamen ve kısmen kapsam dışında tutulan istisnalar olarak ikiye ayrılmıştır.

1. Tamamen Kapsam Dışında Bırakılan Haller

KVKK'nın istisnalar başlıklı 28.maddesinin 1. fıkrasında kanunun tamamen kapsam dışında bırakıldığı uygulanmadığı haller belirtilmiştir. Bu istisnaları incelemek gerekirse:

a. Kişisel Verilerin, Üçüncü Kişilere Verilmemek ve Veri Güvenliğine İlişkin Yükümlülüklere Uyulmak Kaydıyla Gerçek Kişiler Tarafından Tamamen Kendisiyle veya Aynı Konutta Yaşayan Aile Fertleriyle İlgili Faaliyetler Kapsamında İşlenmesi

Gerçek kişi verisini tamamen kendisiyle ilgili faaliyetlerinde işliyor veya bu kişinin verileri aynı konutta yaşayan aile fertleri tarafından aile içinde işleniyorsa bu veri işleme faaliyetleri kanunun uygulama alanı kapsamı dışında kalacaktır. Burada bir nevi kişisel verilerin işlenmesinde "ev içi kullanım" hali düzenlenerek istisna tutulmuştur. İstisnanın amacı, gerçek kişilerin veri işlerken gereksiz ve orantısız zorluklarla karşılaşmasının önlenmesidir[242].

Bu istisna, GVKT'nin 2.maddesinde düzenlenen "ev içi etkinlikler" hükmü ile benzerlik göstermekle birlikte KVKK ile GVKT arasında farklılıklar bulunmaktadır. GVKT de istisnanın kapsamı *"aynı konutta beraber yaşayan kişiler* "olarak ifade edilirken KVKK da *"aynı konutta yaşayan aile bireyleri*" ifadesi kullanılmıştır. Bu bakımdan KVKK'ya göre kişinin aynı evde beraber yaşadığı diğer kişi TMK bakımından aile ferdi değilse bu istisnanın kapsamında yer almayacaktır[243]. Bu

[242] Çekin, s.30.
[243] Küzeci, s.377.

sebeple aynı evde yaşayan ancak aile ferdi olmayan kişilerin bu kanun kapsamında tutulmaması eleştiri sebebi olmuştur[244].

Bu istisna hükmünden yararlanılabilmesi için kanunda belirtildiği üzere kişisel verilerin üçüncü kişilerle paylaşılmaması ve veri güvenliğine ilişkin yükümlülüklere uyulması gerekmektedir. Örneğin; özel bir güne ait aile içinde yapılan kutlamaya ilişkin fotoğrafın çekilerek telefona kaydedilmesi bu istisna kapsamındayken, bu fotoğrafın sosyal medyada paylaşılarak üçüncü kişilere gösterilerek alenileştirilmesi bu istisna kapsamında olmayacaktır[245].

b. Kişisel Verilerin Resmi İstatistik ile Anonim Hâle Getirilmek Suretiyle Araştırma, Planlama ve İstatistik Gibi Amaçlarla İşlenmesi

Kişisel verilerin resmi istatistik kapsamında işlenmesi halinde KVKK uygulanmayacaktır. Kanun koyucu burada resmi istatistiklerin türüne göre bir ayrım yapmadan tüm resmi istatistiklerin istisna oluşturduğunu ifade etmiştir. Örneğin; Türkiye de resmi istatistikleri tutma görevi Türkiye İstatistik Kurumuna (TÜİK) aittir. TÜİK tarafından adalet ve seçim, cezaevinde hükümlü sayıları hakkında yapılacak bir istatistik için kaydedilecek kişisel veriler KVKK hükümlerine tabi olmayıp, istisna teşkil edecektir[246]. Kanunda böyle bir istisnaya yer verilmesine rağmen, devletin bireyin verilerini devletin kendisinden dahi koruması gerektiği, devletin gücünün sınırlandırılması gerektiği ifade edilerek, istatistik oluşturmak amacıyla elde edilen kişisel verilerin dahi anonim hale getirilinceye kadar kişisel verilere hâkim olan ilkeler dahilinde işlenmesi gerektiği kanaatindeyim.

Kişisel verilerin resmi istatistik kapsamında işlenmesinin yanında anonim hale getirilmesi koşuluyla araştırma, planlama ve yapılan istatistik gibi amaçlarla işlenmesi de kanun uyarınca istisna kapsamındadır. KVKK da bu amaçla işlenen verilerin anonim hale ne zaman getirileceği tam olarak ifade edilmemek ile birlikte kişisel verilerin toplanması sırasında anonim hale getirilmesi de istisna kapsamındadır. Örneğin, seçim zamanlarında kişilerin hangi partilere oy vereceği araştırma şirketleri tarafından başlangıçta anonim halde toplanabileceği gibi toplanıp amaca ulaşıldıktan sonra da anonim hale getirilebilir[247].

---

[244] Mehmet Semih Öztekin, "Brezilya Veri Koruma Yasasının 6698 Sayılı Kişisel Verilerin Korunması Kanunu ile Mukayeseli Olarak İncelenmesi", **Kişisel Verileri Koruma Dergisi**, Cilt:3, Sayı:2, 2021, s.40.
[245]https://kvkk.gov.tr/yayinlar/ (05.03.2021), s.10.
[246] Dülger, ss. 350-351.
[247] Dülger, s.351.

KVKK 28.maddesinde “kişisel verilerin araştırma, planlama ve yapılan istatistik gibi amaçlarla” işlenmesinden bahsetmiş olduğundan kanun metnindeki “gibi” ifadesi istisna kapsamının yalnızca sayılan fiillerle sınırlı olmadığını örnekleme yapıldığını göstermekte olup bu maddede sayılan benzer hallerinde istisna kapsamında olabileceği söylenebilir.

c. Kişisel Verilerin Millî Savunmayı, Millî Güvenliği, Kamu Güvenliğini, Kamu Düzenini, Ekonomik Güvenliği, Özel Hayatın Gizliliğini veya Kişilik Haklarını İhlal Etmemek ya da Suç Teşkil Etmemek Kaydıyla, Sanat, Tarih, Edebiyat veya Bilimsel Amaçlarla ya da İfade Özgürlüğü Kapsamında İşlenmesi

Kişisel verilerin**;** millî savunma, millî güvenlik, kamu güvenliği, kamu düzeni, ekonomik güvenlik, özel hayatın gizliliği veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi halleri de KVKK’nın kapsamı dışında bırakılmıştır.

Konuya ilişkin KVK Kurulunun önüne gelen bir olayda, gerçek kişi, adının geçtiği bir gazetede köşe yazısının silinmesine ilişkin talep incelenmiştir. KVK Kurulu kararında; kamuyu ilgilendiren konumda bulunan kişi hakkında gazetede bulunan köşe yazısını ifade özgürlüğü ve basın özgürlüğü kapsamında olduğuna karar vermiştir[248].

KVK Kurulu önüne gelen başka bir olayda ise, bir gazetenin köşe yazısında şikâyet sahibinin oğluna ilişkin yer alan haberde, babasının kanser hastası olması sebebiyle işine ara verdiğine ilişkin bir habere yer verildiği dolayısıyla ilgili kişinin hassas nitelikli kişisel verisi olan sağlık verilerinin onayı dışında işlendiği ve üçüncü kişilerle paylaşıldığı ifade edilerek KVK Kurulundan gerekli işlemlerin yapılması talep edilmiştir. KVK Kurulu yaptığı inceleme de sağlık verilerinin hassas nitelikte kişisel verilerden olması ve ifade özgürlüğü ile kişilik hakları arasında çatışan haklar bakımından kişilik haklarının ifade özgürlüğünden üstün olduğu tespiti yapılarak karar verilmiştir[249].

KVK Kurulu tarafından verilen bu iki karar gözetildiğinde, kişisel verilerin korunması hakkı ile istisna kapsamında ifade özgürlüğü hakkının yarışması

[248]https://www.kvkk.gov.tr/Icerik/5262/Kisisel-Verileri-Koruma-Kurumu-Karar-Ozetleri# (01.05.2021)
[249] https://www.kvkk.gov.tr/Icerik/6663/2019-372 (01.05.2021)

durumunda insan haklarının temel ilkeleri gözetilerek, somut olaya göre değerlendirme yapılması gerektiği kanaatindeyiz[250].

d. Kişisel Verilerin Millî Savunmayı, Millî Güvenliği, Kamu Güvenliğini, Kamu Düzenini veya Ekonomik Güvenliği Sağlamaya Yönelik Olarak Kanunla Görev ve Yetki Verilmiş Kamu Kurum ve Kuruluşları Tarafından Yürütülen Önleyici, Koruyucu ve İstihbari Faaliyetler Kapsamında İşlenmesi

Devlet tarafından; milli savunma, kamu güvenliği, kamu düzeninin sağlanması için yetkilendirilmiş kurum ve kuruluşlarca işlenen kişisel veriler KVKK'nın kapsamına dahil edilmemiş, istisna tutulmuştur. Suç gelirlerinin aklanması gibi mali suçların araştırılması için mali istihbarat elde edilmek üzere işlenen kişisel verilerde kanun kapsamı dışındadır[251]. Bu istisna hükmün uygulanırken kişisel verilerin korunması hakkı ile kamu ve milli güvenlik kavramları arasında makul dengenin kurulması gerektiği ve kişisel verilerin işleme faaliyetinin her hâlükârda kişisel verilerin işlenmesi ilkelerine uygun yapılması gerektiğini düşünmekteyiz[252].

e. Kişisel Verilerin Soruşturma, Kovuşturma, Yargılama veya İnfaz İşlemlerine İlişkin Olarak Yargı Makamları veya İnfaz Mercileri Tarafından İşlenmesi

KVKK da bir suçun soruşturulması, kovuşturulması, infazı ya da bir özel hukuk uyuşmazlığında yargılamasının yapılması ve bunun sonucunda cebri icra işlemlerinin yapılması sırasında kişisel verilerin kaydedilmesi ve işlenmesi mutlak bir istisna olarak yer verilmiştir. Buradaki mutlak istisna kavramı kuralsızlık olarak anlaşılmamalıdır. Bu alanda çalışan yargı organları ve avukatlarca kişisel verilerin korunması amacıyla makul özenin gösterilmesi gerekmektedir[253].

---

[250] Küzeci, ss.380-381; Dülger, ss. 352-353.
[251] Kamile Türkoğlu Üstün, "Güvenlik Soruşturmalarında Kişisel Verilerin Korunması", **Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergis**i, Cilt:25, Sayı:2, 2021, ss.806-807.
[252] Küzeci, ss.355-356.
[253] Dülger, s.356.

2. Kısmen Kapsam Dışında Bırakılan Haller

KVKK'nın 28.maddesinin 2. fıkrasında belli durumlar ve şartlara özgü olarak kanunun bazı maddelerinden muaf tutulma halleri düzenlenmiştir. Hükme göre veri işleyen belirli şartlarda kişisel verileri işlerken KVKK'nın 10.maddesinde düzenlenen aydınlatma yükümlülüğünden, zararın giderilmesini talep etme hakkı dışında ilgili kişinin haklarının düzenleyen KVKK'nın 11.maddesinden, veri sorumlularının siciline kayıt yükümlülüğünü düzenleyen KVKK'nın 16.maddesinden muaf olacaktır. Geriye kalan, KVKK dan kaynaklanan sorumluluk ve yükümlülükler veri işleyen için devam edecek olup muafiyet sınırlı maddeler için uygulanacaktır. Bu halleri incelemek gerekirse:

a. Kişisel Veri İşlemenin Suç İşlenmesinin Önlenmesi veya Suç Soruşturması İçin Gerekli Olması

Suç işlenmesini önlemek veya suçun soruşturulmasının yürütülmesi için görevli kolluk memurlarınca bu amaçları gerçekleştirmek için yapılan kişisel verileri işleme faaliyeti KVKK'nın kısmen kapsam dışı bırakılan alanındadır. Örneğin, kolluk görevlisinin şüphelendiği kişinin kişisel verilerini işlemesi bu kapsamdadır. Kolluk görevlisinin suç konusu verilerin yok edilmemesi ve silinmesini önlemek için şüpheliye işlenen kişisel verileri hakkında bilgi vermemesi bu istisnaya örnek gösterilebilir[254]. Bu örnekte suçun ortaya çıkarılması ile kişisel verilerin işlenmesi sırasında arasında bir menfaat dengesi kurulduğunda suçun araştırılmasının ağır basacağını düşünmekteyiz[255].

b. İlgili Kişinin Kendisi Tarafından Alenileştirilmiş Kişisel Verilerin İşlenmesi

İlgili kişinin kendisine ait verileri bu yöndeki iradesini de açıkça ortaya koyacak şekilde alenileştirmesi durumunda kısmi istisna durumu söz konusu olacaktır. Örneğin, kişinin sosyal medya hesabında herkesin erişimine açık bir şekilde kişisel

[254] Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin Korunması Kanuna İlişkin Uygulama Rehberi,** KVKK Yayınları No:1**,** Ankara, 2019, s.44.
[255] Dülger, s.359.

verisini paylaşması bu kapsamda değerlendirilmektedir.[256]. Kişinin sosyal medya hesabını herkese açık hale getirmediği ve gizlilik ayarları ile bilgi ve fotoğraflarını yalnızca arkadaşlarıyla paylaştığı durumlarda ise kişinin sosyal medya hesaplarında bulunan arkadaşları tarafından bilgilerine ulaşılarak ekran görüntüsünün alınması istisna kapsamındayken; kişinin bilgilerine sosyal medya hesabında arkadaşı olmayan kişilerce ulaşılarak ekran görüntüsünün alınması bu istisna kapsamında olmayacaktır[257].

c. Kişisel Veri işlemenin Kanunun Verdiği Yetkiye Dayanılarak Görevli ve Yetkili Kamu Kurum ve Kuruluşları ile Kamu Kurumu Niteliğindeki Meslek Kuruluşlarınca, Denetleme veya Düzenleme Görevlerinin Yürütülmesi ile Disiplin Soruşturma veya Kovuşturması İçin Gerekli Olması

Kişisel verileri işleme faaliyeti kanundan kaynaklanıyorsa ilgili kişinin açık rızası aranmaksızın bu veriler işlenebilecektir. Kanunlarda yetkili kılınan kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için kişisel verilerin işlenmesinin gerekli olması halinde bu kurumlar kısmen KVKK'nın kapsamı dışında olacaktır.

d. Kişisel Veri işlemenin Bütçe, Vergi ve Mali Konulara İlişkin Olarak Devletin Ekonomik ve Mali Çıkarlarının Korunması İçin Gerekli Olması

Devletin kişisel verileri; millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi halinin mutlak istisna kapsamında olduğunu belirtmiştik. Bu hükümde bahsedilen kısmi istisna hali ise devletin; bütçe, vergi ve mali konulara ilişkin olarak istihbari faaliyetlerinin kapsamının dışında olan kişisel veri işleme faaliyetidir. Bu düzenleme de belirtilen istisna halinin son derece geniş

[256] Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin Korunması Kanuna İlişkin Uygulama Rehberi,** KVKK Yayınları No:1**,** Ankara, 2019, s.44.
[257] Dülger, s.360.

tutulması ve hiçbir koşulla sınırlandırılmaması eleştirilmektedir[258]. Kanaatimizce de devletin veri işleme faaliyeti mümkün olduğunca sınırlandırılarak kişisel verilerin korunmasına getirilecek herhangi bir sınırlamanın "demokratik bir toplum için gerekli olma" koşulunun karşılanması halinde söz konusu olması gerekmektedir.

C. Kişisel Verilerin İşlenmesinde Genel İlkeler

Kişisel verilerin işlenmesi sırasında uluslararası ve ulusal mevzuatta uyulması gereken temel ilkelere çalışmamızın birinci bölümünde detaylı olarak inceledik. Tekrara düşmemek adına bu başlık altında KVKK'nın da düzenlenen kişisel verilere ilişkin temel ilkelere kısaca değinilerek, konuya ilişkin KVK Kurumunun verdiği kararları inceleyeceğiz.

KVKK'nın 4.maddesinde kişisel verilerin işlenmesi sırasında uyulması gereken ilkelere yer verilmiştir. Bu ilkeler şöyledir:

a) Hukuka ve dürüstlük kurallarına uygun olma.
b) Doğru ve gerektiğinde güncel olma.
c) Belirli, açık ve meşru amaçlar için işlenme.
d) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma.
e) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme.

Kişisel verilerin işlenmesinde uygulanması gereken temel ilkeler KVK Kurulu kararlarına da konu olmuştur. Örneğin;

- Spor salonu hizmeti veren şirketin, spor salonuna üye olan kişilerin salona giriş-çıkış kontrolünde el okutma sistemini kullanarak biyometrik verilerini alması ve bu verilerin muhafazası ile şüphe duyulması nedeniyle üyeler tarafından KVK Kuruluna başvuru yapılmıştır. KVK Kurulu, spor salonuna girişte uygulanan el okutma sisteminin üyelerin açık rızası bulunsa dahi KVKK'nın 4.maddesinde bulunan kişisel verilerin işlenmesinde dikkat edilecek genel ilkelere aykırı olduğu tespit ederek veri sorumlusuna idari para cezası uygulamıştır. KVK Kurulu kararında veri sorumlusunun ölçülülük ilkesi ışığında ilgili kişilerden minimum düzeyde veri talep etmesi gerektiğini ifade etmiştir[259].
- Şikâyetçi; bir banka çalışanı tarafından kendisinin aranarak eşinin müdürü olduğu şirketle ilgili olarak eşine ulaşılamadığını eşiyle iletişim kurulması için kendisinden

[258] Küzeci, ss. 383-384.
[259] https://www.kvkk.gov.tr/Icerik/6738/2020-167 ,(03.05.2021).

yardım istendiğini ifade ederek, bankaya bankacılık işlemleri ile ilgili verdiği numarası ve bilgileri üzerinden eşiyle iletişim kurulmak üzere kendi kişisel bilgilerinin kullanılarak aranması hakkında KVK Kuruluna şikâyette bulunmuştur. KVK Kurulu, şikâyetçinin müşterisi bulunduğu bankaya bankacılık iş ve işlemlerinde kendisine ulaşılması için vermiş olduğu telefon numara bilgisinin, eşine ulaşılmasında yardımcı olunabilmesi amacıyla kullanılarak işlenmesinin, KVKK'nın 4.maddesinde düzenlenen kişisel verilerin işlenmesinde amaçla bağlantılı, sınırlı ve ölçülü olma ilkelerine aykırı olduğunu tespit ederek ilgili bankaya idari para cezası uygulamıştır[260].

Veri sorumluları ve veri işleyenlerin sorumluluğunun doğmaması, ilgili kişilerin mağduriyetine yol açılmaması adına kanaatimizce kişisel verilerin işlenmesinin her aşamasında temel ilkelere dikkat edilerek işleme faaliyetini gerçekleştirmeleri gerekmektedir.

D. Kişisel Verilerin İşlenmesinde Hukuka Uygunluk Halleri

KVKK'nın 5.maddesinin 1.fıkrasında kişisel verilerin, ilgili kişinin açık rızası olmaksızın işlenemeyeceği; 2.fıkrasında ise ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenebileceği durumlar düzenlenmiştir. Kural olarak kişisel verilerin işlenmesi hukuka aykırı bir durumdur. Kişinin rızası ve kanunun 5.maddesi ve 6.maddesine uygun olarak yapılan işleme faaliyetleri sonucunda hukuka aykırı olarak işlenen kişisel veriler hukuka uygun hale gelecektir[261].

KVKK'nın 5.maddesinde genel nitelikli kişisel verilerin işleme şartlarından bahsedilmişken, 6.maddesinde özel nitelikli kişisel verilerin işleme şartlarından bahsedilmiştir. Kişisel veri işleme faaliyetinde KVKK'nın 5.maddesi ve 6.maddesinde belirtilen şartlardan birinin bulunması halinde kişisel verilerin işlenmesi hukuka uygun olacak olup, çalışmamızın bu bölümünde KVKK'nın 5.maddesinin 2.fıkrasında sayılan kişisel verilerin işlenmesinde hukuka uygunluk nedenleri incelenecektir.

1. Açık Rıza

Açık rıza KVKK da düzenlenen hukuka uygunluk sebeplerinden birisidir. Hukuka aykırı yapılan bir veri işleme faaliyetinde ilgili kişinin rıza vermesi halinde fiil

[260] https://www.kvkk.gov.tr/Icerik/5545/2019-277,(03.05.2021).
[261] Develioğlu, s.51.; Dülger, s.388.

hukuka uygun hale gelecektir. Açık rızanın, KVKK da belirtilen diğer hukuka uygunluk sebepleri ile arasında hiyerarşik bir ilişki bulunmamakta olup, tüm hukuka uygunluk sebepleri açık rıza ile eşit derecede veri işleme faaliyetine etkisi bulunmaktadır[262].

KVKK'nın 3.maddesinde açık rıza, kişisel veri sahibinin belirli bir konuya ilişkin bilgilendirmeye dayanan ve özgür iradesiyle yaptığı açıklama şeklinde tanımlanmıştır. Kanundaki bu tanım 95/46/EC sayılı Yönergede yer alan tanım ile örtüşmektedir. Nitekim KVKK'nın hazırlanması aşamasında 95/46/EC sayılı Yönerge esas alınmıştır[263]. 95/46/EC sayılı Yönerge ile KVKK arasındaki temel fark KVKK kapsamında veri işleme faaliyetinin gerçekleştirilebilmesi için açık rızanın varlığının aranmasıdır. Açık rıza; KVKK'nın 5/1.maddesi ve 6/2.maddesinde sayılan kişisel veri işleme faaliyetlerinde aranmaktadır. Kanunda bahsedilen bu açık rızanın herhangi bir şekil şartı bulunmamaktadır. Açık rıza beyanı sözlü, yazılı, elektronik ortamda alınabilir. Ancak rıza alındığının ispatı veri sorumlularına aittir[264].

Açık rızanın hukuken geçerli olabilmesi için dört unsur bulunmaktadır[265]:

- Doğrudan kabul ve onay anlamına gelen bir irade beyanının varlığı: Kişisel verisi işlenen ilgili kişi kişisel verilerinin işlenmesine onay verdiğini açıkça ve kesin bir dille şüpheye yer verilmeyecek şekilde ifade etmelidir. İlgili kişinin davranış biçimleri ve davranışlarının yorumlanması yolu ile örtülü rıza yolu ile verilen rızalar açık rıza olmayacaktır[266].
- Belirli bir konuya ilişkin olması: İlgili kişi tarafından verilecek açık rıza; genel ifadelerden uzak, somut, belirli bir konuya ilişkin o konu sınırları içerisinde verilmelidir. İlgili kişinin genel bir ifade ile yaptığı ucu açık, belirsiz, neye ilişkin rıza verdiğinin anlaşılmadığı durumlarda yapılan irade açıklaması KVKK kapsamında "açık rıza" olarak kabul edilmez[267].
- Rızanın bilgilendirmeye dayanması: İlgili kişi, kişisel verilerinin işlenmesine açık rıza verirken neye rıza gösterdiğini, işlemenin amacı, içeriği, süresi bilgilendirilmiş olmalıdır. KVKK'nın 10.maddesine göre veri sorumlusunun ilgili kişiyi bilgilendirerek aydınlatması gerekmektedir. Veri sorumlusu tarafından, ilgili kişinin bilgilendirilmesinin sebebi ilgili kişinin özgür iradesiyle şüpheye yer vermeyecek

---

[262] Dülger, s.390.
[263]https://docplayer.biz.tr/25716160-Kisisel-verilerin-korunmasi-kanunu-tasarisi-1-541-ve-adalet-komisyonu-raporu.html (03.05.2021).
[264]Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi**, KVKK Yayınları, Ankara,2019, s.48.
[265] Saka ve diğerleri, s.31.; Dülger, s.391.
[266] Korkmaz, s.131.
[267] Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi,** KVKK Yayınları, Ankara, 2019, s.48.

şekilde kişisel verilerinin işlenmesine onay vermesidir. Veri sorumlusu tarafından ilgili kişiye bilgilendirme yapılırken teknik terim ve muğlak ifadelerden kaçınarak anlaşılır şekilde aydınlatma yapılmalıdır[268].

- Özgür iradeyle açıklanması: Açık rıza ilgili kişinin özgür iradesi ile hiçbir kişi ve durumun etkisi altında kalınmadan verilmelidir. Kişi bir hizmet veya üründen yararlanması için rıza göstermeye zorlanmamalı bu konuda kişi üzerinde baskı kurulmamalıdır. Cebir, hile, tehdit, hata yoluyla kişinin iradesi sakatlanarak alınan rızalar geçersizdir[269]. Örneğin; işçi-işveren ilişkisinde hiyerarşik bir ilişki bulunduğundan ilgili kişinin üzerinde baskı kurulup kurulmadığı özgür iradesinin ne yönde olduğu araştırılmalıdır[270]. Başka bir örnekte, bir hizmetten yararlanılmasının belirli koşullara bağlandığı hallerde, üyelik sözleşmesinin kurulması için kişinin parmak izinin alınması gibi durumlarda ilgili kişinin bu duruma ilişkin vermiş olduğu rıza zorunluluk olması sebebiyle özgür iradesini temsil etmeyeceğinden geçersiz olacaktır.[271]

Rızanın hukuka uygunluk sebebi olması için tüm bu şartların yanında, hukuka aykırı işlemeden önce veya en geç işleme anında verilmesi gerekmektedir. İşlemeden sonra verilen rıza hukuka uygunluk sebebi olmaz ancak hukuka aykırı işleme sebebiyle ilgili kişinin haklarını kullanmayacağına dair irade beyanı olarak kabul edilebilir[272]. İlgili kişi tarafından kişisel verilerinin işlenmesine ilişkin verilen rıza her zaman geri alınabilir.

2. Kanunlarda Açıkça Öngörülme

KVKK'nın 5.maddesinin 2. fıkrası uyarınca, KVKK dışında başka yasalarda veri sorumlularına kişisel verilerin işlenmesi için açık bir şekilde yetki verilmişse bu işleme faaliyeti hukuka uygun olarak kabul edilecektir. Veri sorumlusunun, bu durumda ilgili kişiden herhangi bir rıza almasına gerek bulunmamaktadır. Burada dikkat edilmesi gereken husus, veri işleme yetkisinin KVKK dışında başka bir kanunda öngörülmesi gerekmektedir. Cumhurbaşkanlığı kararnamesi, yönetmelikler, genelgeler gibi idarenin genel düzenleyici işlemleriyle hukuka uygun bir işleme

[268] Özdemir, s.170.
[269] Saka ve diğerleri, s.31.
[270] Korkmaz, s.132.
[271] Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi,** KVKK Yayınları, Ankara, 2019, s.50.
[272] Develioğlu, ss.56-57.

faaliyeti yapılamayacaktır[273]. Kanunda açıkça öngörülmesine dayanılarak veri sorumlularınca veri işlenmesi halinde KVKK uygulanamayacağından ilgili kişi KVKK dan kaynaklanan haklarını kullanamayacaktır. Örneğin: Kolluk birimleri tarafından bir suç soruşturması sebebiyle, 2559 sayılı Polis Vazife ve Salahiyet Kanununun[274] 5.maddesi uyarınca şüphelilerin parmak izlerinin alınması, 5352 sayılı Adli Sicil Kanunu[275] uyarınca Adalet Bakanlığının kişilerin ceza mahkûmiyetlerine ilişkin verilerini işlemesi, Türk Ticaret Kanunu[276] (TTK) uyarınca şirket genel kurul toplantılarında hazır bulunanlar listesinin tutulması bu istisna kapsamındadır[277].

3. Fiili İmkânsızlık Nedeniyle Rızasını Açıklayamayacak Durumda Bulunan veya Rızasına Hukuki Geçerlilik Tanınmayan Kişinin Kendisinin ya da Bir Başkasının Hayatı veya Beden Bütünlüğünün Korunması İçin Zorunlu Olması

KVKK 5.maddesinin 2(b) fıkrasının uygulanabilmesi için ilgili kişinin fiili imkânsızlık sebebiyle rızasını açıklayamayacak veya rızasına hukuki geçerlilik tanınmayacak bir durumda kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için kişisel verilerinin işlenmesinin zorunlu olması gerekmektedir. Somut olayın özelliklerine göre ilgili kişinin kişisel verilerinin işlenip işlenmeyeceğine rıza gösterip gösteremeyeceğinin burada mutlaka değerlendirilmesi gerekmektedir[278].

Suç teşkil eden bir eylem sebebiyle hürriyeti kısıtlanan bir kişinin kurtarılması ve şüphelinin yakalanması amacıyla, kendisinin veya şüphelinin telefon sinyalleri, kredi kartı kullanım ve araç takip sistemi bilgileri, kamera kayıtları vb. verilerin ilgili birimlerce kullanılarak yer tespitini yapılması; kaybolmuş bir kişinin bulunması amacıyla, telefon sinyali, araç trafik verisinin işlenerek yerinin belirlenmesi, bu hukuka uygunluk nedenine verilebilecek örneklerdendir[279].

---

[273] Dülger, s.392.
[274] 2559 sayılı Polis Vazife ve Salahiyet Kanunu, R.G. 04.07.1934- Sayı. 2559.
[275] 5352 sayılı Adli Sicil Kanunu, R.G. 25.05.2005- Sayı.25832.
[276] 6102 Sayılı Türk Ticaret Kanunu, R.G. 13.01.2011- Sayı.27846.
[277] Sündüs Arınmış Uzun, "Türkiye'de Kişisel Verilerin Korunması ve Vatandaş Algısının Ölçülmesi", **Bilişim Teknolojileri Dergisi**, Cilt:14, Sayı:3, 2021, s.214.
[278] Nafiye Yücedağ, "**Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri**", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Cilt:75, Sayı:2, 2017, ss.776-777.
[279] Kişisel Verileri Koruma Kurumu, **Örneklerle Kişisel Verilerin Korunması**, KVKK Yayınları No:29, Ankara, 2019, s.12.

4. Bir Sözleşmenin Kurulması veya İfasıyla Doğrudan Doğruya İlgili Olması Kaydıyla, Sözleşmenin Taraflarına Ait Kişisel Verilerin İşlenmesinin Gerekli Olması

KVKK'nın 5/2(c). maddesinde veri sorumlularının, ilgili kişi ile araların mevcut veya geçerli bir sözleşmenin ifası veyahut yeni bir sözleşme kurulması için gerekli kişisel verileri işleyebileceği ifade edilmiştir. Kanun koyucunun hükümde veri işleyen ile ilgili kişi arasındaki sözleşmesel bağ ile ifade etmek istediği tarafların birbirlerine hak ve borç yükledikleri sözleşmelerdir. Haksız fiilden veya sebepsiz zenginleşmeden doğan borç ilişkileri bu hüküm kapsamında değerlendirilmeyecektir[280] . Burada veri sorumluları tarafından işleme faaliyetinin yapılabilmesi için işlenecek kişisel verinin sözleşmenin kurulması ve ifası ile doğrudan ilgili, gerekli olması veri işleme faaliyetinin yapılmaması halinde sözleşmenin kurulamaması veya ifa edilememesi gerekmektedir. Örneğin;

- Sözleşme uyarınca edimlerin ifa edilmesi için alıcı taraf satıcının hesap numarasını isteyebilecektir. Banka, müşterisi ile kredi sözleşmesi yaparken müşterisinden ekonomik durumunu gösterir bilgi ve belgeleri talep edebilecektir[281].
- Online alışveriş sitesinden ürün sipariş eden bir tüketiciye ait adres ve iletişim bilgilerinin, kurulan mesafeli satış sözleşmesinin ifası için zorunluluk teşkil etmektedir[282].
- İşçiyle-işveren arasında iş sözleşmesi imzalanırken sözleşmenin ifası için gerekli olan bilgiler işveren tarafından işlenmelidir[283].

Sözleşme gereğince veri işleme faaliyetinin yapılabilmesi için yazılı bir sözleşme olması zorunluluk değildir. Sözlü, zımni olarak kurulmuş bir sözleşmenin ifasında da kişisel veriler hukuka uygun bir şekilde işlenebilecektir.

---

[280] Çekin, s.105.
[281] KVKK 5.Madde Gerekçesi.
[282] Dülger, s.397.
[283] İlyas Arslan, "Kişisel Verilerin Yabancı Unsurlu Sözleşmelere Aykırı Olarak İşlenmesinden veya Korunmamasından Kaynaklanan Uyuşmazlıklara Uygulanacak Hukukun Tespit", **İstanbul Hukuk Mecmuası,** Cilt:79, Sayı:1, 2021, s.165.

5. Veri Sorumlusunun Hukuki Yükümlülüğünü Yerine Getirebilmesi İçin Zorunlu Olması

Kişisel verilerin işlenmesi, veri sorumlusunun hukuki yükümlülüğünün yerine getirilmesi için zorunlu ise, işlemi KVKK 5/2(ç). maddesi uyarınca hukuka uygun hale gelecektir. Bu hukuka uygunluk sebebi kanunun diğer maddesinde hukuka uygunluk sebebi olarak kabul edilen kanunen öngörülmüş olma haliyle benzemekteyse de buradaki hukuka uygunluk sebebinde veri sorumlusu kanunen öngörülme sebebi dışında kalan hukuki yükümlülükleri sebebi ile veri işlemektedir. Kanun dışında kalan düzenlemelerle; mahkeme emirleri, usulünce verilmiş resmi makam talimatları, cumhurbaşkanı kararnamesiyle veri işlenmesi bu hukuka uygunluk sebebine örnek gösterilebilir. Bireyler arasında hüküm doğuran sözleşmeler bu kapsamda görülmemektedir[284]. Avukatların müvekkillerinin talimatlarını yerine getirirken yaptığı faaliyetlerin çoğu da bu kapsama örnek verilebilir[285].

GVKT'nin bu konuya ilişkin hükümlerinin uygulanmasında vergi, sosyal güvenlikle ilgili yükümlülükler, mahkemeye sunulması gereken deliller bu kapsamda görülmektedir[286].

6. İlgili Kişinin Kendisi Tarafından Alenileştirilmiş Olması

İlgili kişi tarafından alenileştirilen ve herkes tarafından bilinebilecek hale gelen verilerin açık rıza alınmaksızın işlenmesi KVKK'nın 5/2(d). maddesi uyarınca hukuka uygunluk sebebi olarak kabul edilecektir. Maddede belirtilen hükmün yorumlanması ve uygulanmasında bir kişinin kişisel verisinin herkes tarafından görülmesi o veriyi bu hukuka uygunluk sebebi kapsamında aleni yapmayacaktır. Örneğin; kişinin çalıştığı şirketin internet sitesinde fotoğrafının yayınlanması veya bir kişiye vekalet çıkarılması için Türkiye Cumhuriyeti Kimlik Numarasının bilinmesinin o kişilere ait kişisel verilerin artık aleni olduğu ve her yerde kullanılacağı kanun kapsamında korunmayacağı anlamına mı gelmektedir? Kanımızca ilgili kişinin verilerinin kamu ile paylaşılmış olmasının bu verilerin her yerde ve her durumda kullanılması anlamına gelmemektedir. Verilerin alenileştirme amacına ve nedenine bakılarak KVKK'nın

[284] Dülger, ss.402-405.
[285] Tevfik Mustafa Kartal, "Kişisel Verilerin Korunması: Türk Bankacılık Sektörü Üzerine Kavramsal Bir Değerlendirme", **Uluslararası Ekonomi Ve Yenilik Dergisi**, Cilt:4, Sayı:1, 2018, s.9.
[286] Develioğlu, s.62.

4.maddesinde düzenlenen genel ilkelere uygun hareket edilerek verilerin "işlendikleri amaçla bağlantılı, sınırlı ve ölçülü" olarak değerlendirilerek[287] sadece alenileştirme amacına uygun olarak işlenmesi alenileştirme amacı dışında işlenmemesi gerekmektedir.

Bu hukuka uygunluk sebebinin doğması için ayrıca alenileştirme fiilinin bizzat ilgili kişi tarafından yapılarak alenileştirme iradesinin ortaya konması gerekmektedir. Örneğin, kendisine ait muayenesi olan bir hekimin ad-soyad, telefon bilgilerinin yer aldığı kart bastırması ve bu kartları dağıtması kartta yer alan bilgilerin hekim tarafından alenileştirildiğini göstermektedir. Kartta yer alan telefon bilgisi ile hekimden tedavi için randevu alınmak üzere hekimin kişisel verileri işleyen ve hekimi arayan kişinin yaptığı işleme fiili hukuka uygun olacaktır. Fakat, hekimin kartvizitindeki bilgilerden yararlanarak ilaç şirketleri tarafından ilaç pazarlaması yapılmaya çalışılırsa bu konuda hekim aranırsa bu durum verilerin alenileştirilme sebebinin amacı dışında kalacağından hukuka aykırı olacaktır[288].

Konuya ilişkin KVK Kurulu tarafından verilen bir kararda, finansal güvence danışmanları tarafından alenileştirilen şirket internet sayfası üzerinden şirkette çalışan kişiden randevu istenmesinin alenileştirme amacına uygun olmadığına karar vererek şikayetçiyi haklı bulmuştur[289].

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

Veri sorumlusu; bir hakkın tesisi, kullanılması veya korunması için veri işlemek zorunda kalması halinde bu verileri işlemesi hukuka uygun olacaktır. KVKK'nın 5/2(e). maddesinde belirtilen hukuka uygunluk sebebinin uygulanması için veri işlemeyi zorunlu kılacak hakkın veri sorumlusuna ait olması da gerekli değildir, üçüncü kişilerin hakları bakımından zorunlu bir durum varsa bu durumda da hukuka uygun olarak veri işlenebilecektir[290]. Örneğin; işverenin kendisine karşı açılan davada ispat için davayı açan işçiye ilişkin bazı verileri kullanması veya vesayet altında ki bir kişinin menfaatlerinin korunması amacıyla vasisinin vesayet altında ki kişinin ekonomik bilgilerini tutması hukuka uygunluk sebebi olabilecektir[291].

---

[287] Küzeci, ss.398-399.
[288] Dülger, s.406.
[289] https://kvkk.gov.tr/Icerik/6623/2019-331,(04.05.2021)
[290] Dülger, s.412.
[291] Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi,** KVKK Yayınları, Ankara, 2019, s.77.

Genel ilkeler uyarınca bir hakkın tesisine hizmet etmeyen, hakkın tesisi için zorunlu olmayan, amacın gerçekleştirilmesi için ihtiyaç duyulmayan kişisel verilerin işlenmesinden de kaçınılması gerekmektedir[292].

8. İlgili Kişinin Temel Hak ve Özgürlüklerine Zarar Vermemek Kaydıyla, Veri Sorumlusunun Meşru Menfaatleri İçin Veri İşlenmesinin Zorunlu Olması

KVKK'nın 5/2(f). maddesinde ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla veri sorumlularının meşru menfaatleri için veri işleyebileceği öngörülmüştür. Bu hukuka uygunluk sebebi değerlendirilirken veri sorumlusu için ilk olarak *"meşru menfaat"* kavramının nasıl yorumlanacağının tespiti son derece önemlidir. KVKK ve gerekçesinde meşru menfaat kavramının tanımından ne anlaşılması gerektiği net olarak belirtilmemiş bu sebeple meşru menfaat kavramının geniş yorumlanması halinde kişisel verilerin korunması hakkının özüne zarar verebileceği öğreti de değerlendirilmiştir[293]. Konu AYM'nin önüne gelerek "meşru menfaat" kavramının belirsiz olması ve temel hak ve özgürlüklerin orantısız şekilde sınırlandırılması sebepleri iptal davasına konu olmuştur. AYM yapılan başvuruya ilişkin vermiş olduğu kararında, meşru menfaat kavramının belirsiz olduğunun söylenemeyeceğini meşru menfaat kavramının temel hak ve özgürlüklere zarar getirmemek şartıyla veri sorumluları arasında bir menfaat dengesinin gözetilerek değerlendirilmesi gereken bir ifade olduğunu belirtmiştir[294]. AYM kararı uyarınca kanunun (f) bendindeki hukuka uygunluk sebebinin uygulanabilmesi için öncelikle veri sorumlusunun meşru menfaatinin olup olmadığı tespit edilecek, eğer veri sorumlusunun meşru menfaati varsa kişinin temel hak ve özgürlüklerinin etkileyip etkilemediği incelenecektir.

KVK Kurulunun bu konuda meşru menfaat halinin tespit edilmesi esnasında dikkat edilecek hususlara ilişkin önemli bir kararı bulunmaktadır. Karara göre meşru menfaat halinin tespit edilirken veri sorumluları tarafından;

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

---

[292] Fatma Esenyel Hanaz, "Çevrimiçi Eğitimde Üniversite Öğrencilerinin Kişisel Verilerinin İşlenmesinin Hukuki Sebepleri", **Türkiye Barolar Birliği Dergisi**, Sayı:155, 2021, ss.424-425.
[293] Dülger, s. 413; Küzeci, s.401; Uyarer, s.134.
[294] Anayasa Mahkemesi Kararı, K.T 28.09.2017, E. 2016/125, K. 2017/143 (23.01.2018 tarih ve 30310 sayılı RG).

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

c) Meşru menfaatin halihazırda mevcut, belirli ve açık olması,

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

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

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

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

h) Kişisel verilerin işlenmesinde genel ilkelere uygunluğun sağlanması,

i) Bu kapsamda, kişinin temel hak ve hürriyetleri ile veri sorumlusunun meşru menfaatinin karşılaştırılarak denge testinin yapılması,

hususlarının değerlendirilmesi gerekmektedir[295].

İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması hali şu şekillerde örneklendirilebilir:

- İşveren, çalışanlarının temel hak ve özgürlüklerini gözeterek çalışanlarının maaşları, terfi ve sosyal haklarının düzenlenmesi gibi amaçlarla kişisel verilerini işleyebilir.[296].
- Şirket araçlarının iş haricinde kullanılmadığından emin olmak isteyen şirketin araçlara GPS cihazı yerleştirerek aracın ve aracı kullanan kişinin konum bilgisinin alınarak kişisel verilerin işlenmesi, bir işverenin çalışanların devamlılık durumlarını takip edebilmesi için işe giriş-çıkışlarında kimlik kartı okutulmasının zorunlu tutularak kişisel verilerinin işlenmesi meşru menfaate örnek olabilir[297].

[295] Kişisel Verileri Koruma Kurumunun 25.03.2019 tarihli 2019/78 sayılı Kararı.
[296] KVKK 5.madde gerekçesi.
[297] Dülger, ss.416-417

Kanaatimizce, meşru menfaat kavramının muğlak ve taraflarca farklı şekilde değerlendirilebileceği gözetilerek, her somut olay bazında ayrı ayrı değerlendirilerek temel hak ve özgürlükler esas alınarak dar yorumlanması gerekmektedir.

E. Özel Nitelikli Kişisel Verilerin İşlenmesinde Hukuka Uygunluk Nedenleri

Hassas veya özel nitelikli kişisel verilerin işlenmesi KVKK da ayrı bir başlık altında düzenlenmiştir. Bu tip veriler genel anlamda kişisel verilerden niteliği ve önemi itibari ile daha fazla korunmasına ihtiyaç duyulan kişilerin temel hak ve özgürlükleriyle yakından ilgili olan verilerdir.

KVKK'nın 6.maddesinin 1. fıkrasında 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 bilgileri kişinin özel nitelikli verileri olarak sayılmıştır. KVKK da belirtilen özel nitelikli kişisel verilerin sayımı sınırlı sayıda yapılmış olup, örnekleme yoluyla özel nitelikli kişisel verilerin kapsamının genişletilmesi mümkün değildir. Maddenin 2. fıkrasında ise özel nitelikli kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği ifade edilerek, özel nitelikli kişisel verilerin işlenmesi açık rıza koşuluna bağlanmıştır.

Maddenin 3.fıkrasında ise özel nitelikli kişisel verilerden cinsel hayat ve sağlık verilerini diğer özel nitelikli kişisel verilerden ayırarak farklı işlenme koşulları öngörülmüştür. Hükme göre kişilerin cinsel hayatı ve sağlık verileri dışındaki özel nitelikli kişisel verileri KVKK dışında diğer kanunlarda öngörülen haller dahilinde işlenebilecekken; kişinin sağlık ve cinsel hayatına ilişkin verileri ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilecektir. Kişilerin sağlık ve cinsel hayatlarına ilişkin verilerinin yasa ile öngörülme koşuluna yer verilmeksizin yetkili makamlarca işlenebilmesinin hüküm altına alınması öğretide eleştirilmektedir[298]. Zira temel hak ve özgürlükler Anayasanın 13.maddesinde belirtildiği üzere kanunla

[298] Küzeci, s.406.

sınırlanabilecek olup, kurum ve kuruluşlarca yapılacak yönetmelik, tüzük gibi düzenleyici işlemlerle sınırlandırılamayacaktır.

KVKK'nın 6.maddesi kapsamında özel nitelikli kişisel verilerin işlenmesine aşağıdaki haller örnek gösterilebilir:

- Adli Sicil Kanunu uyarınca kişilerin mahkûmiyet bilgilerinin Adalet Bakanlığınca, PVSK 5.maddesi uyarınca şüphelilerin parmak izleri adli makamlarca işlenebilir.
- İş Kanunu ve Sendikalar ve Toplu İş Sözleşmesi Kanunu uyarınca çalışanların sendika üyeliği bilgilerine ilişkin özlük dosyası tutularak verileri işlenebilir[299].
- Bir kişinin iki farklı sağlık kuruluşunda tedavi gördüğü durumlarda hastanın tedavisi amacıyla iki farklı sağlık kuruluşunda ki sağlık verileri birbirlerine aktarılabilir[300].
- Bir özel hastane tarafından gerçekleştirilen sağlık hizmetleri dolayısıyla SGK'dan hasta adına ödeme alınabilmesi için hastalarının sağlık verilerini işlemesi bu kapsamdadır[301].

KVKK 6.maddesinin ilk üç fıkrasında özel nitelikli kişisel verilerin işlenmesine ilişkin hususlar düzenlenmişken 4.fıkrasında bu verilerin işlenirken KVK Kurulu tarafından belirlenen yeterli önlemlerinde alınması gerektiği ifade edilmiştir. KVK Kurulu, kanunun son fıkrasındaki hüküm gereği 31.08.2018 tarihli kararını yayınlamıştır[302]. Karara göre, özel nitelikli kişisel verilerin güvenliğinin sağlanması için sistemli, kuralları net bir şekilde belli, yönetilebilir ve sürdürülebilir ayrı bir prosedür ve politikanın belirlenmesi gerektiği ifade edilmiştir. Bunun yanında özel nitelikli verilerin işlenmesi sürecinde yer alan çalışanların eğitilerek, onlarla gizlilik sözleşmesi yapılarak, belirli aralıklarla denetim yapılması gerektiği de ifade edilmiştir.

F. Kişisel Verilerin Silinmesi, Yok Edilmesi ya da Anonim Hale Getirilmesi

KVKK 7.maddesinde mevzuata uygun şekilde işlenen kişisel verilerin işlenme sebebinin ortadan kalması halinde resen veya ilgili kişinin talebi üzerine veri sorumluları tarafından silinmesi, yok edilmesi veya anonim hale getirilmesi gerektiği hüküm altına alınmıştır. KVKK dışında diğer kanunlarda düzenleme altına alınan kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin hükümler

[299] Dülger, s.422.
[300] Kişisel Verileri Koruma Kurumu, **Örneklerle Kişisel Verilerin Korunması**, KVKK Yayınları No:29, Ankara, 2019, s.21.
[301] Dülger, s.431.
[302] Kişisel Verileri Koruma Kurulunun 31.01.2018 tarihli 2018/10 sayılı Kararı.

saklı olup, bu konuya ilişkin KVKK dışında başka bir kanunda düzenleme yapılmışsa o kanun hükümleri uygulanacaktır. Örneğin, 5352 Sayılı Adli Sicil Kanunun da verilerin silinmesini, yok edilmesine ilişkin hükümler KVKK'ya göre öncelikle uygulanacaktır[303].

KVKK'nın 7.maddesinin 3.fıkrasında kişisel verilerin silinmesine, yok edilmesine veya anonim hâle getirilmesine ilişkin usul ve esasların yönetmelikle düzenleneceği belirtilmiştir. Kanunun ilgili maddesi kapsamında*" Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Haline Getirilmesi Hakkında Yönetmelik (KVK İmha Yönetmeliği)*" 28 Ekim 2017 tarihli ve 30224 sayılı Resmî Gazetede yayımlanarak 1 Ocak 2018 tarihinde yürürlüğe girmiştir.

KVK İmha Yönetmeliğin 4.maddesinde kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi imha olarak tanımlamıştır. KVK İmha Yönetmeliğin 8.maddesinde kişisel verilerin silinmesi kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi olarak tanımlanırken, KVK İmha Yönetmeliğin 9.maddesinde kişisel verilerin yok edilmesi kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemeyecek şekilde geri getirilemez ve tekrar kullanılamaz hale getirilmesi olarak tanımlanmıştır. Kişisel verilerin yok edilmesi, silinmesinden farklı olarak kişisel verilerin hiç kimse tarafından ulaşılamaması, geri getirilememesi, kullanılamaması anlamına gelmektedir. Kişisel verilerin yok edilmesi işleminde, adli bilişim veri kurtarma yazılımlarıyla dahi imha edilen kişisel verilere ulaşılamamaktadır[304].

KVK İmha Yönetmeliğin 10.maddesinde ise kişisel verilerin anonim hale getirilmesi kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi olarak tanımlanmıştır. Kişisel veriler anonimleştirilmesi işlemi sonucunda bunu yapan veri sorumlusu dahi geri dönüp ilgili kişiyi belirleyememelidir[305].

KVKK'nın 16.maddesine göre KVK Kurumu tarafından tutulan veri sorumluları siciline kayıtlı olan veri sorumluları, iş süreçlerine bağlı olarak geliştirmiş oldukları kişisel işleme faaliyetlerini hakkında bir envanter oluşturmaktadır. Veri Sorumluları Yönetmeliğin 5.maddesi uyarınca kişisel veri işleme envanterine uygun olarak kişisel veri saklama ve imha politikası oluşturmak zorundadırlar. Veri sorumluları

---

[303] KVKK 7.madde gerekçesi.
[304] Dülger, s.605.
[305] Zübeyir Özçelik ve Ebru Aykan, "Sosyal Bilimlerde Büyük Veri Kullanımı, Veri Toplamada Akademik Çalışmalara Ne Tür Kolaylıklar Sağlayabilir?", **Anadolu Üniversitesi Sosyal Bilimler Dergisi**, Cilt:20, Sayı:3,2020, s:137.

hazırladıkları bu imha politikasında KVK İmha Yönetmeliğin 6.maddesi uyarınca periyodik imha süreleri, imhaya süreçlerine ilişkin bir takım asgari bilgilere yer vermelidir. Kişisel verilerin, silinmesi ya da anonim hale getirilmesinde imha politikasına uygun hareket edilmesi zorunludur. Kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesiyle ilgili yapılan bütün işlemler kayıt altına alınır ve söz konusu kayıtlar, en az üç yıl süreyle saklanır. Veri sorumlusu kişisel verilerin silinmesi, yok edilmesi, anonim hale getirilmesi işlemiyle ilgili uyguladığı yöntemleri ilgili politika ve prosedürlerinde açıklamakla yükümlüdür. Veri sorumlusu, KVK Kurulu tarafından aksine bir karar alınmadıkça, kişisel verileri resen silme, yok etme veya anonim hale getirme yöntemlerinden uygun olanını seçer[306].

G. Kişisel Verilerin Aktarımı

Kişisel verilerin aktarılması, kişisel verilerin işlenme türlerinden birisidir. Kanun koyucu konunun önemi sebebiyle bu işlenme türünü özel olarak düzenlemiş ve kendi içerisinde verilerin yurt içinde üçüncü kişilere ile verilerin yurtdışına aktarılması konusunda ikili bir ayrım yapmıştır. Kişisel verilerin aktarımı belirttiğimiz üzere aynı zamanda bir veri işleme faaliyeti olduğundan bu faaliyetler açısından işlemeye ilişkin genel ilkeler dikkate alınmalıdır[307].

Verilerin yurt içinde üçüncü kişilere aktarılması KVKK'nın 8.maddesinde düzenlenmiştir. Buradaki düzenlemenin kişisel verilerin işlenme koşuluyla hemen hemen aynı olduğunu söylemek gerekir. Nitekim Kanunun 8/1.maddesinde kişilerin açık rızası olmaksızın üçüncü kişilere veri aktarımı yasaklanırken, ikinci fıkrada Kanunun 5/2.maddesi ve 6/3.maddelerinde yer alan açık rızanın aranmadığı hukuka uygunluk hallerine atıf yapılmıştır. Bu noktada saptanan tek farklılık özel nitelikli kişisel verilerin aktarımında yeterli önlemlerin alınması koşulunun getirilmesidir[308]. Yeterli önlemlerin ne olduğuna KVK Kurulu karar verecektir.

Bir veri işleme faaliyetinin veri aktarımı olup olmayacağının tespiti her zaman kolay olmayabilir. Örneğin, TTK 195.madde ve devamında düzenlenen şirketler topluluklarının birbirleri arasında paylaşımların üçüncü kişiye aktarım sayılıp sayılmayacağını değerlendirmek gerekebilir. KVK Kurulu bu konuda verdiği bir kararında şirketler topluluğu içerisinde bulunan şirketlerin aralarındaki veri alış-

[306] Saka ve diğerleri, ss.54-58.
[307] Çekin, s.131.
[308] KVKK, 22/1(ç).

verişini veri aktarımı olarak değerlendirmiş ve veri aktarımında KVKK 8.maddesinin uygulanması gerektiğini ifade etmiştir[309].

KVKK'nın 9.maddesinde yurt içinde kişisel verilerin ilgilinin açık rızası olmaksızın aktarılamayacağı hususu tekrar edilerek, yurt dışı aktarımlar içinde aynı şart öngörülmüş fakat bu durumun istisnalarına yer vermiştir[310]. Bunlar KVKK'nın 5/2. maddesi ve 6/3.maddesinde belirtilen şartlara ek olarak aktarımın gerçekleşeceği ülkede kişisel verilerin korunması hukuku konusunda yeterli, etkin korumanın bulunması ya da Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmesi[311] ve KVK Kurulunun izni bulunmasıdır. Bu şartların sağlanması halinde ilgili kişinin açık rızası bulunmaksızın kişisel veriler yurtdışına aktarılabilecektir.

Kanunda belirtilen yeterli korumanın bulunduğu kişisel verilerin aktarılması kapsamında belirlenecek güvenli ülkeler KVK Kurulu tarafından belirlenip, ilan edilecektir. Ocak 2022 itibarıyla henüz güvenli ülkeler listesi KVK Kurulu tarafından yayınlanmamış, sadece yeterli korumanın bulunduğu ülkelerin benimsenmesinde uygulanacak kriterler yayınlanmıştır. Bu kriterlere göre KVK Kurulu aktarım yapılacak yabancı ülkelerde yeterli koruma bulunup bulunmadığına; Türkiye'nin taraf olduğu uluslararası sözleşmeleri, kişisel veri talep eden ülkeyle Türkiye arasında veri aktarımına ilişkin karşılıklılık durumuna, her somut kişisel veri aktarımına ilişkin olarak kişisel verilerin işlenme amaç ve süresine, kişisel verilerin aktarılacağı ülkenin konuyla ilgili mevzuatı ve uygulamasına, kişisel verilerin aktarılacağı ülkede bulunan veri sorumlusu tarafından taahhüt edilen önlemleri değerlendirerek karar verecektir[312].

Kişisel verilerin aktarımına ilişkin bir diğer düzenleme de KVKK'nın 9.maddesinin 5.fıkrasında yer almaktadır. Bu düzenlemeye göre uluslararası sözleşme hükümleri saklı kalmak üzere, Türkiye'nin ve ilgili kişilerin menfaatlerinin ciddi şekilde zarar göreceği durumlarda, ancak ilgili kamu kurum ve kuruluşunun görüşü alınarak Kurulun izni ile kişinin açık rızası olmaksızın yurtdışına veri aktarımı yapılabilecektir. Bu düzenleme objektif zarar ölçütünün nasıl tespit edileceği, görüşü

[309]https://www.kvkk.gov.tr/Icerik/5262/Kisisel-Verileri-Koruma-Kurumu-Karar-Ozetleri# (07.05.2021).
[310] KVKK, 9/2 md.
[311] Kurul tarafından taahhütnamede yer alması gereken asgari koşullara ilişkin form yayınlanmıştır. Bkz. https://www.kvkk.gov.tr/Icerik/6741/YURT-DISINA-KISISEL-VERI-AKTARIMINDA-HAZIRLANACAK-TAAHHUTNAMELERDE-DIKKAT-EDILMESI-GEREKEN-HUSUSLARA-ILISKIN-DUYURU, (05.05.2021).
[312] Kişisel Verileri Koruma Kurumunun 02.05.2019 tarihli 2019/125 sayılı Kararı.

alınacak kamu kurumunun belli olmaması, uygulamanın nasıl yapılacağı ve bunun gibi diğer sebeplerle eleştirilmiştir[313].

Kişisel verilerin aktarılması başlığı altında işlenmesi gereken bir diğer konu artan internet kullanımı sebebiyle kişisel verilerin internet sitesine yüklenmesinin veri aktarımı sayılıp sayılmayacağı hususudur. KVK Kurulunun e-posta sunucularına veri aktarımına ilişkin önemli bir kararı bulunmaktadır[314]. Kararda KVK Kurulu, e-postaların hizmet altyapısı sebebiyle yurt dışında merkezlerde tutulması durumunda bu durumun yurt dışına veri aktarımı olacağını tespit etmiştir. Bu karar veri sorumlularının ilgili kişilerin verilerini aktarırken mutlaka açık rızalarının alınması anlamına gelmekte olup ilgili kişilerin açık rızası alınmazsa veri işleme faaliyeti hukuka aykırı olacaktır.

Yaşadığımız çağda teknolojik altyapıların son derece gelişmesi sebebiyle kişilerin yaşamının daha da kolaylaşması için veri aktarımlarının yapılması kişiler açısından gereklilik arz etmektedir. Kanunda kişisel verilerin aktarılmasına ilişkin hükümlere yer verilirken bu hükümlerin düzenlenmesinin sebebi kişisel verilerin aktarılmasını yasaklamak değil bu verilerin işlenme faaliyetindeki genel ilkelere uyularak kişinin mağduriyetine yol açmayacak şekilde veri güvenliğinin sağlanarak aktarılmasını sağlamak olduğunu değerlendirmekteyiz. KVKK'nın veri aktarımına ilişkin istisnalar kısmında yer verilen "milli güvenlik", "suçun önlenmesi", "istihbari faaliyetler" kavramlarının sınırlarının belirlenmesi de bu yönden oldukça önemlidir. Bu kavramların sınırının çizilmemesi geniş yorumlanması halinde kişisel verilerin aktarımında yeterli koruma sağlanamayacak olup, kişilerin temel hak ve özgürlükleri zarar görebilecektir.

H. Veri Sorumlusunun Yükümlülükleri

Veri sorumlusunun yükümlülükleri KVKK da düzenlenmiştir. Veri sorumlusu KVKK'ya göre veri işleme faaliyetini yerine getirirken kanunda belirtilen genel ilkelerin yanında ilgili kişileri aydınlatma, veri güvenliğine ilişkin her türlü tedbirleri almakla yükümlüdür. Bu yükümlülere ek olarak veri sorumlusu; ilgili kişinin başvurusu üzerine kanunda öngörülen usullere uygun olarak ilgili kişinin başvurusuna cevap vermeli ve Veri Sorumluları Sicil Bilgi Sistemine (VERBİS) kayıt yaptırması gerekmektedir. Veri sorumlusunun yükümlülükleri bu bölümde incelenecektir.

---

[313] Küzeci, s.413.
[314] Kişisel Verileri Koruma Kurumunun 31.05.2019 tarihli 2019/157 sayılı Kararı.

1. Aydınlatma Yükümlülüğü

Kişisel Verileri Koruma Kanununda veri sorumlularına yüklenen en önemli yükümlülüklerden biri ilgili kişileri aydınlatma yükümlülüğüdür. Veri sorumlusu veri işleme faaliyetine başlamadan önce, verilerin işlenmesinden verilerin imha edilmesine kadar yürütülecek tüm bu süreçler hakkında ilgili kişileri bilgilendirmelidir.

KVKK'nın 10.maddesine göre veri sorumlusu veya yetkilendirdiği kişi ilgili kişilere; veri sorumlusunun ve varsa yetkilendirdiği kişinin kimliği, kişisel verilerin hangi amaçla işlendiği, işlenen verilerin kimlere hangi amaçla aktarılabileceği, veri toplama yöntemi ve hukuki sebebi, kanunda belirtilen hakları konusunda bilgi vermekle yükümlüdür. KVKK da yer alan bu ifadeler genel nitelikli ifadeler olup, aydınlatma yükümlülüğünün ne şekilde yapılacağı konusunda belirsizlikler bulunmaktadır. Bu belirsizlikleri gidermek aydınlatma yükümlülüğünün somutlaştırılması için KVK Kurulu tarafından "Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ" Resmî Gazete de yayınlanarak yürürlüğe girmiştir[315].

Tebliğ de aydınlatma yükümlülüğünün yerine getirilmesi konusunda bir şekil şartı aranmamıştır. Tebliğe göre veri sorumlusu ya da yetkilendirdiği kişi tarafından aydınlatma yükümlülüğü; yazılı, sözlü, çağrı merkezi, ses kaydı gibi fiziksel veya elektronik ortamlar kullanılmak suretiyle yerine getirilebilir. Veri sorumlusu veya yetkilendirdiği kişi, bu yöntemlerden hangisini kullanacağına kendisi karar verir[316].

Aydınlatma yükümlülüğü; internet sayfasında yer alan metin, duvarda bulunan bir levha, bilgi panosu, mobil uygulamalar, çağrı merkezleri aracılığıyla yapılabilir. Aydınlatma yükümlülüğünün yerine getirildiğinin ispatı veri sorumlusuna aittir. Aydınlatma yükümlülüğünün yerine getirilmesi ilgili kişinin talebine de bağlı değildir. Veri işleme faaliyetinin ilgili kişinin açık rızasına bağlı olmadığı ve KVKK dışında başka bir kanundan kaynaklandığı hallerde dahi aydınlatma yükümlülüğü yerine getirilmelidir[317].

Aydınlatma yükümlülüğü yerine getirilirken ilgili kişilerin okudukları, gördükleri ya da duyduklarında anlayabilecekleri kadar açık, sade, anlaşılabilir ve tereddüte yer

---

[315]Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ, R.G 10.03.2018 – Sayı.30356.

[316] Sümeyra Karınçu, **Kişisel Verilerin Korunması Kanunu Kapsamında Aydınlatma Yükümlülüğünün Yerine Getirilmemesi Kabahati**, (Yayınlanmamış Yüksek Lisans Tezi), İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü, İstanbul, 2019, ss.77-80.

[317]https://www.kvkk.gov.tr/Icerik/5394/Aydinlatma-Yukumlulugunun-Yerine-Getirilmesi-Rehberi, (05.01.2022), s.14.

bırakmayacak aydınlatmalar yapılmalı genel, muğlak ifadelere yer verilmemelidir. Konuya ilişkin KVK Kurulunca verilen bir kararda, veri sorumlusunun internet sitesinde aydınlatma metninde kişisel verilerin işlenmesine ilişkin "gibi amaçlar kapsamında işlenmektedir" ifadesine yer verilmesinin muhtemel başka amaçlar içinde kişisel verilerin işleneceği izleniminin yaratılmakta olduğunu bu sebeple aydınlatma metninin gözden geçirilerek muğlak ifadelere yer verilmemesi gerektiğine karar verilmiştir[318].

İlgili kişiye karşı, öncesinde aydınlatma yükümlülüğünü yerine getirmiş olan veri sorumlusunun veri işleme faaliyetinden sonra o veriyi işleme amacı değişirse, değişen amaç kapsamında aydınlatma yükümlülüğünü tekrar yeni işleme amacı içinde yapması gerekmektedir[319].

Kanaatimizce veri sorumlusu tarafından yapılacak aydınlatma yükümlülüğü sonucunda, ilgili kişiler kişisel verilerinin tüm işlenme faaliyetleri ve hakları konusunda bilgi sahibi olacak ve sahip oldukları hakları kullanarak kendi bilgilerinin geleceğini belirleyip veri sorumlularının veri işleme faaliyetinde şeffaflık ve hesap verebilmesini sağlayacaktır.

2. Veri Güvenliğine İlişkin Yükümlülükler

a. Genel Olarak

Kişisel verilerin güvenli şekilde işlenmesi ve tutulması veri güvenliğini sağlanması açısından son derece önemlidir. Veri sorumluları ve onun yetkilendirdiği veri işleyenler kişisel verilerin ilk defa elde edilmesinden başlayarak veriler imha edilinceye kadar her aşamada gerekli önlemleri alarak veri güvenlini sağlamalıdırlar. Veri güvenliğinin sağlanması işleme faaliyetinin sadece bir aşamasında gözetilmesi gereken bir durum olmayıp, gelişen ve değişen teknolojik güvenlik uygulamaları dikkate alınarak işleme faaliyetinin her aşamasında sürekli gözetilmesi gereken bir sorumluluktur[320].

KVKK'nın 12.maddesinde veri sorumlusunun "veri güvenliğine ilişkin yükümlülükleri" düzenlenmiştir. Maddeye göre veri sorumlusu kişisel verilerin hukuka aykırı olarak işlenmesi ve erişilmesini önleyerek, kişisel verilerin korunması amacıyla

[318] Kişisel Verileri Koruma Kurumunun 02.05.2019 tarihli 2019/122 sayılı Kararı.
[319] Dülger, s.529.
[320] Türkay Henkoğlu, "Kişisel Verileriniz Ne Kadar Güvende? Bilgi Güvenliği Kapsamında Bir Değerlendirme", **Arşiv Dünyası Dergisi**, Sayı:18-19, 2017, ss.47-48.

her türlü teknik ve idari önlemleri almak zorundadır[321]. Veri sorumluları alacakları önlem ve tedbirleri sektör bazında değerlendirilerek veri güvenliğine ilişkin riskleri de göze alarak belirlemelidir. Veri sorumlusunun kanunda açıkça yer verilmemesine rağmen veri güvenliğinin sağlanması ve sürdürülebilir şekilde devam ettirilmesi için işlenen verinin niteliği ve kapsamı gözetilerek veri yönetim sistemi oluşturabilmesi de mümkündür[322].

KVKK'nın 12.maddesi 2.fıkrasında kişisel verilerin işlenmesinde alınması gereken veri güvenliğine ilişkin önlemlerin sorumluluğunun kimlere ait olduğu düzenlenmiştir. Maddeye göre, kişisel verilerin veri sorumlusu adına başka bir kişi tarafından işlenmesi durumunda alınması gereken tedbirlere ilişkin veri sorumlusu ve yetkilendirdiği kişi müştereken sorumlu olacaktır[323]. Örneğin, muhasebe şirketi tarafından veri sorumlusuna ait şirket kayıtları tutuluyorsa veri güvenliğine ilişkin veri sorumlusu muhasebe şirketiyle birlikte müştereken sorumludur[324]. Maddenin 3. fıkrasında, veri sorumlusunun; kendi kurum ve kuruluşlarında bu kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak ve yaptırmak zorunda olduğu ifade edilmiştir. Veri sorumlusunun kanun uyarınca bu denetimi bizzat yapmasına zorunda olmayıp, belli aralıklarla uzman kuruluşlardan veri güvenliğine ilişkin rapor alarak da denetimi yaptırabilir. GVKT de gerekli denetimlerin yapılması ve risklerin minimum seviyeye indirmek üzere veri sorumlularına Veri Koruma Görevlisi belirlenmesi yükümlülüğü düzenlenmiştir. KVKK da bu konuda bir düzenleme bulunmamakla birlikte veri koruma görevlisi atanmasına ilişkin bir yasakta söz konusu olmadığından veri sorumluları tarafından gerekli denetimleri yaptırmak üzere veri koruma görevlisi atanabileceği değerlendirilmekteyiz. Maddenin 4.fıkrasında ise veri sorumluları ile veri işleyen kişilerin, öğrendikleri kişisel verileri görevi sırasında, sonrasında KVKK hükümlerine aykırı olarak açıklamayacağı düzenlenmiştir. Veri sorumlularının veri güvenliğine ilişkin yükümlülükleri görevden ayrılmalarından sonra dahi devam edecektir[325].Veri güvenliğine ilişkin KVK Kurulu tarafından verilmiş birçok karar mevcuttur.

---

[321] KVKK, 12/1.
[322] Çekin, s.193.
[323] Nilüfer Boran Güneysu, N. Ve Burak Memiş, "Kişisel Verilerin Korunması Kanunu Kapsamında Avukatın Yükümlülük ve Sorumlulukları", **Anadolu Üniversitesi Hukuk Fakültesi Dergisi,** Cilt:5, Sayı:2,2019, s:325.
[324]Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin Korunması Kanuna İlişkin Uygulama Rehberi,** KVKK Yayınları No:1**,** Ankara, 2019, s.97.
[325] Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin Korunması Kanuna İlişkin Uygulama Rehberi,** KVKK Yayınları No:1**,** Ankara, 2019, s.99.

KVK Kurulu; banka, noter, vergi dairesi, polis karakolları, mağaza ve market kuyrukları gibi kişisel verilerin sesli paylaşıldığı ortamlarda söz konusu verilerin ilgili olmayan kişilerce duyulmasını, görülmesini, öğrenilmesi veya ele geçirilmesini engelleyecek gerekli tedbirlerin alınması gerektiğine karar vermiştir[326].

KVK Kurulu başka bir kararında; bir veri sorumlusu nezdinde bulundukları pozisyon ve görev itibariyle kişisel verilere erişim yetkisi olan kişilerin yetkilerini kötüye kullanarak bu verileri kişisel amaçlarıyla üçüncü kişilerle paylaşılmasını önlemek için veri sorumlusunca gerekli her türlü tedbirin alınması gerektiğini ifade etmiştir[327].

KVK Kurulu Facebook hakkında verdiği bir kararında, bir çalışanın bilgisayarına şirket çalışanı olmayan yetkisiz 3.kişilerce erişilebilmesinin idari bir tedbirsizlik olduğunu ve ihlal tarihinden sonra çalışanlara güvenlik eğitimi verilmesinin veri güvenliği açısından eksiklik göstergesi olduğunu, bilişim ağlarında sızma olmasının şirket tarafından fark edilmemesinin teknik bir eksiklik olduğunu tespit ederek Facebook şirketine idari para cezası kesmiştir[328].

KVK Kurulu tarafından verilen bu kararlar, veri sorumlularına veri güvenliğine ilişkin alması gereken tedbirleri somutlaştırarak, veri sorumlarını aydınlatmak, veri sızıntıların önlenmesi sağlamak açısından oldukça önemlidir.

b. Kurula Bildirim Yükümlülüğü

Kişisel verilerin korunması alanında veri sorumlularınca yeterli idari ve teknik tedbirlerin alınmaması halinde veri sızıntıları gerçekleşebilmektedir. Veri sızıntıları sonucunda ilgili kişilerin ekonomik ve diğer kişilik hakları zarar görebilecektir. Bu noktada zararları asgari düzeye indirmek ve gerekli tedbirlerin alınması için veri sızıntısı konusunda ilgili kişi ve yetkili kuruluşlara bilgilendirilme yapılması son derece önemlidir[329]. Bu sebeple KVKK'nın 12/5.maddesinde kişisel verilerin hukuka uygun olmayan yollarla başkaları tarafından elde edilmesi halinde, veri sorumlularının durumu en kısa sürede ilgilisine ve KVK Kuruluna bildirmesi gerektiği düzenlenmiştir. Kurul gerekli hallerde ihlali Kurum internet sayfasında veya uygun göreceği bir ortamda yayımlayabilecektir.

[326] Kişisel Verileri Koruma Kurulunun 21.12.2017 tarihli 2017/62 sayılı Kararı.
[327] Kişisel Verileri Koruma Kurulunun 31.05.2018 tarihli 2018/63 sayılı Kararı.
[328] Kişisel Verileri Koruma Kurulunun 18.09.2019 tarihli 2019/269 sayılı Kararı.
[329] Küzeci, ss.415-417.

Veri sorumlusu tarafından KVK Kuruluna yapılacak ihlal bildiriminin amacı ihlalin büyümesi ve tekrar yaşanmasını önlemektir. Burada veri sorumlusunun veri ihlali konusunda bir kusurunun bulunup bulunmadığı bir önem taşımamaktadır[330].

KVKK'da yapılan düzenleme de veri ihlal bildiriminin ne kadarlık bir süre içerisinde yapılacağından bahsedilmemiş, bunun yerine "en kısa sürede" ifadesine yer verilmiştir[331]. KVK Kurulu "en kısa sürede" kavramını somutlaştırmak ve yanlış anlaşılmalara yol açılmaması için veri ihlali durumunda KVK Kuruluna yapılacak bildirimlerin süresinin 72 saat olarak yorumlanması gerektiğini açıklamıştır[332]. Kurul ayrıca veri ihlal bildirimlerinin nasıl yapılacağına ilişkin de internet sitesinde "Kişisel Veri Bildirim Formu" hazırlamıştır[333].

Veri sorumlusu tarafından ilgili kişiye yapılacak ihlal bildirimlerinde ise kanun ve Kurul tarafından en kısa süre kavramı açıklanmamış makul sürede bildirim yapılması gerektiği ifade edilmiştir[334]. KVK Kurulu tarafından veri sorumlusunun ilgili kişiye yapacağı ihlal bildiriminde bulunması gereken asgari bilgiler içerir karar yayımlanmıştır[335]. Söz konusu karar uyarınca veri sorumlusu tarafından ilgili kişiye yapılacak olan ihlal bildiriminde ihlalin ne zaman gerçekleştiği, hangi kişisel verilerin ihlalden etkilendiği, ihlalin olası sonuçları, ihlalin önlenmesi için alınan tedbirler açık sade bir dille açıklanmalıdır.

Veri sorumlusu tarafından ihlal bildiriminin zamanında yapılmaması halinde KVKK'nın 18/1(b). maddesi uyarınca yükümlülükleri yerine getirmeyenler hakkında idari para cezası uygulanacaktır. Nitekim bu konuda KVK Kurulu tarafından verilen birçok karar bulunmaktadır[336].

3. İlgili Kişiler Tarafından Yapılan Başvuruların Cevaplanması ve Kurul Kararlarının Yerine Getirilmesi Yükümlülüğü

KVKK'nın 13.maddesi uyarınca ilgili kişi, bu kanunun uygulanmasıyla ilgili taleplerini yazılı olarak veya KVK Kurulunun belirlediği diğer yöntemlerle veri sorumlusuna iletebilecektir. Veri sorumlusu kendisine ulaşan bu talebi en kısa sürede

---

330 Çekin, s.206.
331 KVKK, 12/5.
332 Kişisel Verileri Koruma Kurumunun 24.01.2019 tarihli 2019/10 sayılı Kararı.
333https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/e0413853-cd8c-428f-9315-2e8b3d874b46.pdf ,(08.05.2021).
334 Kişisel Verileri Koruma Kurumunun 24.01.2019 tarihli 2019/10 sayılı Kararı.
335 Kişisel Verileri Koruma Kurumunun 18.10.2019 tarihli 2019/271 sayılı Kararı.
336 Kişisel Verileri Koruma Kurumunun 18.09.2019 tarihli 2019/269 sayılı Kararı, Kişisel Verileri Koruma Kurumunun 16.05.2019 tarihli 2019/143-2019/144 sayılı Kararları.

ve en geç otuz gün içerisinde ücretsiz olarak sonuçlandıracaktır. Bu işlemin ayrıca bir maliyet gerektirmesi halinde veri sorumlusu ilgili kişiden KVK Kurulunca belirlenen tarife üzerinden ücret alabilecektir[337].

Veri sorumlusu yapılan başvuruyu kabul edebilir, reddedebilir veya süresi içerisinde yanıt vermeyebilir. Veri sorumlusu, ilgili kişinin talebini kabul ederse talebin gereğini yaparak, işlemin bir maliyeti gerektirmesi sebebiyle ücret alındıysa ücreti ilgili kişiye iade eder[338]. Veri sorumlusu ilgili kişi tarafından yapılan başvuruyu kabul etmez, cevap vermez veya verilen cevap ilgili kişi tarafından yeterli bulunmazsa ilgili kişi cevabı öğrendiği tarihten itibaren 30 gün ve herhalde başvuru tarihinden 60 gün içerisinde Kurula şikâyette bulunabilir[339].

4. VERBİS'e Kayıt Yükümlülüğü

Kişisel verilerin korunması hukukun önemli ilkelerinden biri şeffaflıktır. Veri işleme faaliyetinin dayanağı, amacı, kullanılan araçlar herkes için açık ve anlaşılır olduğu takdirde sürece dahil olan taraflardan her biri gerçekleştirilen işlemlerin hukuka uygun olup olmadığını denetleyebilecektir. KVKK da şeffaflık ilkesine hizmet eden en önemli unsurlardan birisi de VERBİS'e kayıt yükümlülüğüdür[340].

VERBİS, KVK Kurulu tarafından denetlenerek aleni olarak tutulan bir sicildir. KVKK'nın 16.maddesinde kişisel verileri işleyen gerçek ve tüzel kişilerin veri işlemeye başlamadan önce VERBİS'e kaydolması gerektiği, kanunun aynı maddesinde ayrıca VERBİS'e kayıt yükümlülüğünden istisna tutulacak veri sorumlularının kimler olduğuna KVK Kurulu tarafından karar verileceği belirtilmiştir. Yine KVKK'nın 16/5 maddesinde VERBİS'e ilişkin usul ve esasların yönetmelikle düzenleneceği ifade edilmiştir. Bunun üzerine Veri Sorumluları Sicili Hakkında Yönetmelik (VSSHY) Resmî Gazetede yayınlanarak yürürlüğe girmiştir[341].

VSSHY'nin 6.maddesinde VERBİS'in KVK Kurulu başkanı tarafından oluşturulacağını ve kurulması, işletilmesi için gerekli teknik ve idari tedbirlerin yine başkanlık tarafından alınması gerektiği ifade edilmiştir.

VERBİS'e kayıt yükümlülüğü veri işlemeye başlamadan önce doğmakla birlikte, bazı veri sorumlularının VERBİS'e kayıt yükümlülüğünden istisna

[337]Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ, R.G 10.03.2018 – Sayı.30356.
[338] KVKK, 13/3.md.
[339] KVKK, 14.md.
[340] Çekin, s.215.
[341] Veri Sorumluları Sicili Hakkında Yönetmelik, R.G 30.12.2017 – Sayı.30286.

tutulabilecektir. Bu durumda sicile kayıt yükümlülüğü bulunmamasına rağmen, bu veri sorumluları için daha sonra sicile kayıt yükümlülüğü doğarsa en geç 30 gün içerisinde sicile kaydolmaları gerekecektir. Veri sorumluları teknik, hukuki, fiili aksaklıklar neticesinde sicile kayıt yükümlülüklerini yerine getirememeleri durumunda KVK Kurulundan ek süre talep etme hakları da bulunmaktadır[342].

Veri sorumlularının VERBİS'e başvuruları kayıt yükümlülüğü kapsamında iletilecek bilgilerin VSSHY'e göre VERBİS'e yüklenmesi ile gerçekleşmiş olacaktır. Veri sorumluları, sicilde değişiklik yapmak istedikleri takdirde bu değişiklikleri VERBİS aracılığıyla 7 gün içerisinde bildirebileceklerdir. Veri sorumluları sicilinden veri sorumluları kaydını sildirmek isterse bu durum ancak veri sorumlusunun VERBİS'e kayıt yükümlülüğünün ortadan kalkması halinde kabul edilecektir. Veri sorumlusunun talebi KVK Kurulu tarafından kabul edilerek, kaydı silinse dahi görev yaptığı süreye ilişkin sorumluluk ve yükümlülükleri devam edecektir[343].

VSSHY'nin 15.maddesinde ve KVK Kurulu tarafından alınan kararlar[344] doğrultusunda örnekleme yoluyla saymak gerekirse; suç işlenmesinin engellenmesi amacıyla yapılan işleme faaliyetleriyle, noter, dernek, vakıf, sendika, avukatlar, çalışan sayısı elliden az ve yıllık mali bilançosu toplamı 25 milyon TL'den az olan veri sorumlularının VERBİS sistemine kayıt yükümlülüğü bulunmamaktadır. VERBİS'e kayıt yükümlülüğünden istisna edilen veri sorumlularının KVKK kapsamında diğer sorumlulukları devam etmektedir. Burada ki istisna sadece sicile kayıt yükümlülüğüne ilişkindir. İstisna tutulan veri sorumluları kişisel verileri işlerken KVKK'nın 4.maddesi uyarınca genel ilkelere uymak zorundadırlar[345].

VSSHY'de sayılan ve KVK Kurulu tarafından VERBİS'e kayıt sorumluluğundan istisna tutulan veri sorumluları dışında VERBİS'e kayıt yükümlülüğüne aykırı hareket edenler hakkında Kurul tarafından idari para cezası uygulanacaktır[346].

VERBİS'in oluşturulması ve yükümlülükleri ihlal eden veri sorumluları hakkında idari para cezası kesilmesi ülkemizde eleştiri konusu olmuştur. Zira 95/46/EC sayılı Yönergeden alınan veri sorumluları sicili oluşturulması düzenlemesi GVKT ile

---

[342] VSSHY 8.md.
[343] VSSHY 14.md.
[344] Kişisel Verileri Koruma Kurumunun 02.04.2018 tarihli 2018/32 sayılı Kararı, Kişisel Verileri Koruma Kurumunun 28.06.2018 tarihli 2018/68 sayılı Kararı; Kişisel Verileri Koruma Kurumunun 18.08.2018 tarihli 2018/87 sayılı Kararı; Kişisel Verileri Koruma Kurumunun 19.07.2018 tarihli 2018/87 sayılı Kararı.
[345] Küzeci, s.432; Dülger, ss.245-246.
[346] KVKK 18 md.

kaldırılmıştır. GVKT mevzuatında şu anda sicile kayıt yükümlülüğü bulunmamaktadır. VERBİS'e kayıt yükümlülüğü hukuki açıdan öğretide gerekli görülmese de kişisel verileri koruma hukukuna ve rejimine yeni adapte olan ülkemizde farkındalık ve güven ortamının artırılması adına bu yükümlülüğün var olması gerektiği de düşünülmektedir[347].

III. KİŞİSEL VERİLERİN KORUNMASI YOLLARI

Kural olarak kişisel verilerin işlenmesi kanuna aykırıdır. Ancak belirli şartların varlığı veya işlenme faaliyetinin yasayla düzenlenmesi halinde yapılan işlem hukuka uygun hale gelmektedir. Bu sebeple kural olarak veri işleme faaliyetinin hukuka aykırı olduğu gözetilerek Türk Hukukunda bir takım kişisel verileri koruma yolları düzenlenmiştir. Türk Hukukunda kişisel verilerin korunması yolları özel kanunlarla düzenlenmiş olmakla birlikte genel koruma yollarının da bu konuda çıkabilecek uyuşmazlıklara uygulanabileceğini düşünmekteyiz[348].

Bu bölümde öncelikle KVKK da düzenlenen koruma yolları olan veri sorumlusuna başvuru, KVK Kuruluna şikâyet, idari yaptırımlar ve KVKK da atıf yapılan TCK kapsamında belirlenen cezai yaptırımlar incelenecek, sonrasında TMK ve TBK yer alan genel hükümler dahilinde öngörülen koruma yolları ve dava türleri açıklanacaktır.

A. Kişisel Verilerin Korunması Kanunda Öngörülen Koruma Yolları

1. Veri Sorumlusuna Başvuru Yoluyla Koruma

KVKK'nın "veri sorumlusuna başvuru" başlıklı 13.maddesinde veri sahibinin yazılı olarak veya KVK Kurulunun belirleyeceği diğer yöntemlerle veri sorumlusuna başvurabileceği düzenlenmiştir. Ayrıca konuya ilişkin ayrıntıları düzenleyen Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ (VSBT)[349] KVK Kurulu tarafından kabul edilmiştir[350].

---

[347] Dülger, s.246.
[348] Özdemir, ss.187-227.; Develioğlu, ss. 126-130.
[349] Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ, R.G 10.03.2018 – Sayı.30356.
[350] Kişisel Verileri Koruma Kurumunun 23.07.2019 tarihli 2019/225 sayılı Kararı.

Tebliğe göre ilgili kişi; veri sorumlusuna yazılı, e-imza, e-posta adresi veya başvuruya ilişkin geliştirilmiş yazılım-uygulama aracılığıyla yapabilir[351]. Başvuruda ilgili kişinin ad, soyad ve başvuru yazılı ise imzası, Türkiye Cumhuriyeti vatandaşları için T.C. kimlik numarası, yabancılar için uyruğu, pasaport numarası veya varsa kimlik numarası, tebligata esas yerleşim yeri veya iş yeri adresi, varsa bildirime esas elektronik posta adresi, telefon ve faks numarası, talep konusunun bulunması zorunludur[352].

Başvuru halinde, veri sorumlusu azami 30 gün süre içerisinde başvuruyu cevaplamalıdır[353]. Veri sorumlusu yapılan başvuruyu kabul edebilir, reddedebilir veya süresi içerisinde yanıt vermeyebilir. Veri sorumlusu, ilgili kişinin talebini kabul ederse talebin gereğini yapmalı; ilgili kişinin talebini reddederse red kararının gerekçesini açıklayarak ilgili kişiye bildirmelidir. Veri sorumlusu cevabı ilgili kişiye yazılı olarak verebileceği gibi elektronik ortamda da bildirebilir. İlgili kişinin başvurusuna yazılı olarak cevap verilecekse, on sayfaya kadar ücret alınmaz. On sayfanın üzerindeki cevaplar için her sayfa başı 1 Türk Lirası işlem ücreti alınabilir. Başvuruya cevabın CD, flash bellek gibi bir kayıt ortamında verilmesi halinde veri sorumlusu tarafından başvurucudan talep edilebilecek ücret kayıt ortamının maliyetini geçemez[354]. Veri sorumlusu, ilgili kişinin talebini kabul ederse işlemin bir maliyeti gerektirmesi sebebiyle ücret alındıysa ücreti ilgili kişiye iade eder.

2. Şikâyet Yoluyla Koruma

İlgili kişi, veri sorumlusuna başvurusunun reddedilmesi, verilen cevabın yetersiz bulunması veya süresinde cevap verilmemesi hallerinde, cevabı öğrendiği tarihten itibaren otuz ve herhalde başvuru tarihinden itibaren altmış gün içinde KVK Kuruluna şikâyette bulunabilir[355].

İlgili kişi, veri sorumlusuna başvurmadan KVK Kuruluna şikâyet başvurusunda bulunamaz. Kanun da bu konuda aşamalı bir başvuru sistematiği öngörülmüş böylelikle uyuşmazlıkların belli bir kısmının veri sorumluları tarafından çözülerek KVK Kurulunun yoğun bir iş yüküyle karşı karşıya kalması engellenmek istenmiştir[356]. Buna

[351] VSBT, 5/1md.
[352] VSBT, 5/2md.
[353] KVKK, 13/2 md.
[354] VSBT, 7md.
[355] KVKK, 14 md.; Ayrıntılar için bakınız Kişisel Verileri Koruma Kurulunun 24.01.2019 tarihli 2019/9 sayılı Kararı.
[356] KVKK, 14 md. gerekçesi.

ek olarak, kanunda kişilik hakkı ihlal edilenlerin genel hükümlere göre tazminat haklarının saklı olduğu ifade edilmiştir. Bu ifadeden ilgili kişinin KVK Kuruluna başvuruda bulunmaksızın veri sorumlusuna karşı tazminat davası açabileceği anlaşılmaktadır[357].

Şikâyet üzerine veya ihlal iddiasını öğrenmesi durumunda resen, görev alanına giren konularda KVK Kurulu gerekli incelemeyi yapar. Söz konusu inceleme kapsamında Kurul veri sorumlularından bir takım bilgi ve belge isteyebilir. Kurul tarafından devlet sırrı niteliğindeki bilgi ve belgeler haricinde istenen bilgi ve belgeler veri sorumluları tarafından 15 gün içerisinde KVK Kurulana gönderilmeli veya yerinde inceleme yapılmasına imkân sağlanmalıdır.

KVK Kurulu şikâyet üzerine talebi inceleyerek ilgililere bir cevap verir. Şikâyet tarihinden itibaren altmış gün içinde cevap verilmezse talep reddedilmiş sayılır. KVK Kurulu tarafından yapılan inceleme sonucunda, ihlalin varlığının anlaşılmasa hâlinde KVK Kurulu tespit ettiği hukuka aykırılıkların veri sorumlusu tarafından giderilmesine karar vererek ilgililere kararı tebliğ eder. Bu karar, tebliğden itibaren gecikmeksizin ve en geç otuz gün içinde yerine getirilir[358]. Veri sorumlusu, KVK Kurul kararını süresi içerisinde yerine getirmezse KVK Kurulu, KVKK'nın 18.maddesi uyarınca veri sorumlusu hakkında idari para cezasına hükmedebilir.

KVK Kurulu, yaptığı inceleme sonucunda veri sorumlusu tarafından yapılan ihlalin yaygın olduğunu karar verirse ilke kararı alabileceği gibi telafisi güç ve imkânsız zararların doğması ve hukuka aykırılığın açık olması halinde veri işlenmesinin veya verinin yurt dışına aktarılmasının durdurulmasına da karar verebilir[359].

3. İdari Yaptırım Yoluyla Koruma

İdari para cezası kişisel verilerin korunması alanında en sık karşılaşılan yaptırım türlerinden biridir. KVKK'nın *"Kabahatler"* başlıklı 18.maddesinde; aydınlatma yükümlülüğünü, veri güvenliğine ilişkin yükümlülüklerini, KVK Kurul kararlarını uygulamayan, veri sorumluluğu siciline kayıt ve bildirim yükümlülüğüne aykırı hareket eden veri sorumluları hakkında hangi yükümlülüğü ihlal ettiğine bağlı olarak değişen miktarlarda idari para cezasına hükmedilmesi öngörülmüştür. Düzenleme de KVKK'nın 4.maddesinde belirtilen genel ilkelere aykırı hareket eden

[357] Öngün, s.217.
[358] KVKK, 15/4,5 md.
[359] KVKK, 15/6,5 md.

veri sorumlularına yönelik herhangi bir idari para cezası belirlenmemiştir. Maddede öngörülen idari para cezaları veri sorumlusu olan gerçek kişilerle özel hukuk tüzel kişileri hakkında uygulanır. Verilen idari para cezalarına karşı idari yargı yolu açıktır.

İdari para cezasına konu KVKK'nın 18.maddesinde sayılan eylemlerin kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları bünyesinde işlenmesi halinde ise o kurumda görev yapılan kişiler hakkında disiplin hükümlerine göre işlem yapılacak ve sonucu Kurula bildirilecektir.

KVKK da yapılan düzenlemelerde idari para cezalarının alt sınırı ile üst sınırı arasında oldukça fark bulunmaktadır. Cezaların üst sınırı alt sınırının 20 katı ile 66 katı arasında değişkenlik göstermektedir. Bu tercih sebebi KVKK'nın gerekçesinde; söz konusu kabahatlerin çok farklı ekonomik güce sahip gerçek ve tüzel kişiler hakkında uygulanacak olması sebebiyle yaptırım uygulanmasında hakkaniyeti sağlamak amacıyla yapıldığı ifade edilmiştir. Örneğin, küçük bir aile şirketiyle ülke çapında faaliyet gösteren şirketler grubunun kanun hükümlerini ihlal etmesi durumunda belirlenecek idari para cezaları arasında farklılık olacaktır[360]. Bu noktada en azından idari para cezasının miktarlarının belirlenmesinde esas alınacak ölçütlerin yasa metninde belirtilmesi yerinde olacağı düşünülmektedir[361]. Zira, GVKT de idari para cezasının alt ve üst sınırı arasında geniş bir aralık belirlenmesi yerine şirketlerin cirosu esas alınarak idari para cezasına hükmedilmesi gerektiği düzenlenmiştir[362]. Nitekim Fransa'da, Türk Hukukunda KVK Kurulunun Fransız muadili olan "Hürriyetler ve Bilişim Ulusal Komisyonu (CNIL)" idari para cezasının şirketlerin yıllık cirosunun %4'üne kadar uygulanabilmektedir[363].

Kanaatimce kişisel verileri koruma hukukuna ve rejimine yeni adapte olan ülkemizde uygulama alanlarının gelişmesi ve idari yaptırım pratiklerinin artmasıyla idari para cezaları da makul ve belirli standartlara göre hukuki güvenlik ve belirlilik ilkeleri çerçevesinde zaman içerisinde değişerek güncellenecektir.

B. Cezai Yaptırımlar Yoluyla Koruma

KVKK 17.maddesinde kişisel verilere ilişkin suçlar bakımından TCK'nın 135.maddesi ile 140.maddelerinin uygulanacağı belirtilerek TCK'ya atıf yapılmış,

---

360 KVKK, 18 md.gerekçesi.
361 Küzeci, s.440.
362 GVKT, 83 md.
363 Salih İnan, "Kişisel Verilerin Korunması Kapsamındaki Yaptırımlara Karşı Yargısal Başvuru Yolları: Karşılaştırmalı Bir İnceleme", **Kişisel Verileri Koruma Dergisi**, Cilt:3, Sayı:2, 2021, ss.57-59.

ayrıca KVKK'nın 7.maddesine aykırı olarak kişisel verileri silmeyen, anonim hale getirmeyen kişiler hakkında TCK'nın 138.maddesine göre cezalandırılacağı ifade edilmiştir.

TCK'nın ilgili maddelerinde kişisel verilere ilişkin üç adet suç tipi öngörülmüştür. Bunlar kişisel verilerin hukuka aykırı olarak kaydedilmesi (TCK 135.md), verileri hukuka aykırı şekilde verme, yayma ve ele geçirme (TCK 136.md) ve verileri yok etmeme (TCK 138.md) suçlarıdır. TCK da kişisel verilerin hukuka aykırı olarak kaydedilmesi, verilmesi, ele geçirilmesi, yayılması ve yok edilmemesi suç teşkil eden beş eylem tipi olarak sayılmıştır. Ancak KVKK da düzenlenen veri işleme faaliyeti çok daha geniş kapsamlıdır. Verilerin üzerinde gerçekleştirilen her türlü işlem veri işlemedir. Örneğin, verileri hukuka aykırı olarak birisi değiştirir, aktarırsa bu kişiye ilgili ceza hükümleri uyarınca ceza uygulanacak mıdır? Kanaatimizce, ceza hukukunun temel ilkelerinden olan "kıyas yasağı" ve "suç ve cezaların kanuniliği" ilkeleri gözetilerek bu fiillerinden dolayı ilgili kişiye TCK kapsamında ceza verilemeyecektir[364].

TCK'nın 135/1.maddesinde kişisel verileri hukuka aykırı olarak kaydedilen kişiler hakkında bir yıldan üç yıla kadar hapis cezası öngörülmüştür. Ayrıca kanunun devamında 2. fıkrasında kişilerin siyasi, felsefi veya dini görüşlerine, ırk kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bu suçun işlenmesi halinde cezaların yarı oranda arttırılacağı ifade edilmiştir. TCK'nın 135.maddesinin 2. fıkrasında özel nitelikli kişisel verilerin hukuka aykırı olarak kaydedilmesi durumunda cezada artırım yapılacağı öngörülmüştür. Fakat burada TCK da belirlenen özel nitelikli kişisel veriler kategorisi ile KVKK da belirlenen özel nitelikli kişisel veriler arasında bir uyumsuzluk bulunmaktadır. Kişilerin "ahlaki eğilimleri" TCK'da özel nitelikli kişisel veri olarak öngörülmüşken, KVKK da bu husus düzenlenmemiştir. Öte yandan KVKK da özel nitelikli kişisel veri olarak yer alan kişilerin etnik kökeni, dini inançları, ceza mahkumiyeti, dernek ve vakıf üyelikleri TCK kapsamında özel nitelikli kişisel veri olarak kabul edilerek cezada artırım sebebi yapılmamıştır. TCK ile KVKK arasındaki uyuşmazlıkların giderilerek uyumlu hale getirilmesinin uygulama açısından faydalı ve gerekli olduğunu düşünmekteyiz[365].

---

[364]Murat Volkan Dülger, "Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması", **İstanbul Medipol Üniversitesi Hukuk Fakültesi** Dergisi, Cilt:3, Sayı:2, 2016, (Ceza Normlarıyla), s.163.
[365] Küzeci, ss.444-445.

Kişisel verileri hukuka aykırı olarak bir başkasına veren, yayan ya da ele geçiren kişiler TCK 136.maddesi uyarınca iki yıldan dört yıla kadar hapis cezasıyla cezalandırılır. Suçun konusunun, Ceza Muhakemesi Kanununun [366](CMK) 236.maddesi 5. ve 6. fıkraları uyarınca kayda alınan beyan ve görüntüler olması durumunda verilecek ceza bir kat oranda artırılacaktır.

Kişisel verilerin hukuka aykırı olarak kaydedilmesi, verilmesi ve ele geçirilmesi suçlarının, kamu görevlisi tarafından veya görevinin verdiği yetkiyi kötüye kullanarak işlenmesi halinde verilecek ceza yarı oranında artırılacaktır.

KVKK ve diğer kanunlar uyarınca kişisel verileri hukuka uygun olarak işleyen kişiler, verileri işleme sebepleri ortadan kalktıktan sonra bu verileri silmeli, yok etmeli veya anonim hale getirmekle yükümlüdür. Bu kişiler yükümlülüklerini yerine getirmez ve işledikleri kişisel verileri silmez, yok etmez ve anonim hale getirmezse TCK 138.maddesi uyarınca bir yıldan iki yıla kadar hapis cezasına çarptırılacaktır. Suçun konusunun CMK hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması hâlinde verilecek ceza bir kat artırılacaktır.

TCK'nın 139.maddesinde TCK'da belirtilen kişisel verilerin korunmasına ilişkin suçların soruşturma ve kovuşturulmasının şikâyete bağlı olduğu belirtilmiş, söz konusu suçların tüzel kişiler tarafından işlenmesi halinde tüzel kişilere özgü güvenlik tedbirlerine hükmedileceği hüküm altına alınmıştır.

C. Genel Düzenlemelerde Yer Alan İmkanlar Yoluyla Koruma

Kişisel verileri koruyucu bazı hükümler medeni hukuk kapsamındadır. Bunun sebebi kişisel verileri koruma hakkının özel hayatın gizliliği hakkı da gözetilerek kişilik hakkının bir parçası olmasıdır. Kişisel veriler ile doğrudan ilişkili olan kişinin onur ve saygınlığı, özel yaşamı, sır alanı kişilik hakkı kapsamında değerlendirilmektedir[367]. Kişilik hakkına ilişkin koruma yolları bu sebeplerle kişisel verileri korunması içinde söz konusu olacaktır[368]. Zira bu hususun bir gereklilik olduğunu da ifade etmek isteriz. KVKK da kişisel verilerin korunmasına ilişkin hükümler çoğunlukla önleyici tedbirler içermektedir. Örneğin; kişisel verilerin sadece toplandığı amaç için kullanılacak olması, özel nitelikli kişisel verilerin işlenmesinin kural olarak yasak olması, sicile kayıt

[366] 5271 Sayılı Ceza Muhakemesi Kanunu, R.G. 04.12.2014 – Sayı.25673.
[367] Küzeci, ss.446-448.
[368]Abdullah Ömeroğlu, "Kişilik Haklarının Alkaya-Türkiye Davası Bağlamında Kişisel Verilerin Korunması Hukukuna Göre İncelenmesi ", **Uyuşmazlık Mahkemesi Dergisi,** Sayı:15, 2020, s.333.

yükümlülüğü gibi ilkeler bir zararın, kişisel verilerin korunması hakkının ihlal edilmesini önleyici niteliklidir. TMK da kişilik hakkının korunması için yapılan düzenlemelerse bireylerin kişisel verilerine saldırının gerçekleşmesi sonrasında yapılacak saldırının önlenmesi, durdurulması ve bunun gibi düzenlemeleri içermektedir.

Bu sebeplerle bu başlık altında TMK ve TBK [369](Türk Borçlar Kanunu)'da düzenlenen maddeler uyarınca kişisel verilerin korunması alanında uygulanabilecek dava türleri incelenecektir.

1. Önleme Davası

TMK 25/1.maddesinde kişilik haklarının ihlal edilme tehlikesi altında olan kişilerin hâkimden saldırı tehlikesinin önlenmesini isteyebileceği öngörülmüştür. Henüz mevcut olmamakla birlikte birtakım eylem ve makul belirtilerden yola çıkılarak çok yakın bir gelecekte kişilik hakkına karşı gerçekleşmesi yüksek bir ihtimal olarak görülen hukuka aykırı saldırılara karşı açılan bir dava türüdür. Burada aranacak saldırı tehlikesi ciddi ve yakın olmalıdır. Önleme davasında gerçekleşmesi muhtemel bir saldırının teşebbüs aşamasında önlenmesi amaçlanmaktadır[370]. Örneğin, veri sorumlusunun gerekli veri güvenliği önlemlerini almaması sonucunda kişinin e-posta içeriklerinin hackerlar tarafından ele geçirilme tehlikesinin ortaya çıkması halinde ilgili kişi kişilik hakkına saldırı tehlikesinin önlenmesini hâkimden talep edebilir[371].

Önleme davasının davacısı verileri hukuka aykırı olarak işlenme tehlikesi altında olan ilgili kişi, davalısı kişisel verilere işleyen veri sorumlusu ve veri işleyendir. Davanın açılması için davalının kusuru aranmaz[372].

Önleme davası, niteliği itibariyle de bir eda davasıdır. Bu sebeple davacı tarafın başvurusu üzerine hâkim dava sonucunda kişilik hakkı saldırısının engellenmesine yönelik bir karar verebilecektir. Karar İcra İflas Kanunun (İİK)[373] 30.maddesi uyarınca icra edilecektir. Mahkeme kararının icra edilmemesi halinde İİK 343.maddesinde belirtilen tazyik hapsi uygulanacaktır.

---

[369] 6098 Sayılı Türk Borçlar Kanunu, R.G.11.01.2011 – Sayı.27386.
[370] Turan Atlı, "Kişilik Haklarının İhlali Durumunda İnternet Erişiminin Engellenmesi", **Necmettin Erbakan Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:3, Sayı:1, 2020, ss.11-12.
[371] Öngün, s.287.
[372] Öngün, s.287.; Develioğlu, s.132.
[373] İcra İflas Kanunu, R.G. 09.06.1932 – Sayı.2128.

2. Durdurma Davası

Kişilik hakkına saldırı yapılması halinde açılacak bir diğer dava türü durdurma davasıdır. Bu dava türünde kişilik hakkı ihlal edilen kişi sürmekte olan saldırının durdurulmasını hâkimden isteyebilir[374]. Burada kişilik hakkına yönelmiş hala devam etmekte olan bir saldırı olması gerekmektedir. Saldırı bitmişse veya henüz başlamamışsa durdurma davası açılmaz. Saldırı bitmişse açılan durdurma davası konusuz kalacak, saldırı henüz başlamamışsa başlamayan eylemin durdurulması söz konusu olmayacaktır[375]. Burada durdurma davasının hedefi devam etmekte olan hukuka aykırı durumun sona erdirilmesidir. Örneğin, kişinin resminin rızası dışında işletmeci tarafından kendi firmasının reklam yüzü olarak kullanılması durumunda bu haksız eylem devam ettiği müddetçe durdurma davası açılabilir[376]. Aynı zamanda kişisel verileri hukuka aykırı yollarla elde edilen kişiler verilerinin yurt dışına aktarılmasının durdurulmasını isteyebilir.

Durdurma davası pratikte, şeref ve haysiyete, mesleki ve ticari değerlere ve özel hayata karşı yapılan saldırılarda kullanılır. Bu davanın kişinin haklarının daha etkin korunması için TMK 25/2.maddesinde yer alan düzeltmenin, kararın yayınlanması ve üçüncü kişilere bildirilmesiyle birlikte istenmesinin daha faydalı olacağı düşünülmektedir[377]. Bunun sebebi, çoğu zaman kişilik haklarına yapılan haksız saldırılar sona erdiğinde bu fiiller haksız olmasına rağmen başkalarının zihninde farklı şekilde anlaşılarak kişiler hakkında bir takım olumsuz değer yargıları oluşmaktadır. Saldırının kişilerin zihninde beliren olumsuz değer yargılarının kaldırılması ise ancak kararın ve düzeltmenin yayınlanarak üçüncü kişilere duyurulmasıyla söz konusu olacaktır.

Durdurma davası doğrudan açılabilecek bir dava olmakla birlikte uygulama da başka bir davanın yanında ihtiyati tedbir kararı alınması talebiyle de aynı menfaat elde edilebilmektedir. Durdurma davası sonucu verilen karar İİK 30.maddesi uyarınca icra edilecek olup, mahkeme kararının icra edilmemesi halinde İİK 343.maddesinde belirtilen tazyik hapsi uygulanabilecektir.

---

374 TMK 25/1 md.
375 Mine Kaya, "Telekomünikasyon Alanında Kişilik Haklarının Korunması", **Ankara Barosu Dergisi,** Sayı:4, 2010, ss.293-294.
376 Özdemir, s.193.
377 Özdemir, s.194.; Develioğlu, s.130.

3. Tespit Davası

Kişilik hakkı saldırıya uğrayan kişiler saldırının hukuka aykırı olduğunun tespitini hâkimden isteyebilirler[378]. Bu davayla istenilen amaç gerçekleşmiş ve etkileri sürmekte olan hukuka aykırı davranışların tespitinin yapılmasıdır[379].

Tespit davası, kişinin eda davası açamadığı durumlarda açılabilir. Eda davası açma imkânın bulunduğu durumlarda tespit davası açılamaz[380]. Kişilik haklarına saldırı ihtimali belirdiğinde önleme davası, saldırı devam ederken durdurma davası açılacağından tespit davasının açılmasında kişinin hukuki yararı yoktur. Çünkü eda davasında, dava konusu fiilin hukuka aykırı olup olmadığının tespiti her halükârda yapılmaktadır.

Kişilik haklarına karşı yapılan saldırı sona ermişse, kişi tarafından önleme, durdurma davası ve saldırıyı yapan kişinin kusuru olmaması halinde tazminat davası açılamayacağından bu durumda tespit davası açılabileceği tarafımca düşünülmektedir.

Tespit davası sonucunda hâkimin verdiği karar eda hükmü içermez, hâkim dava konusunun hukuka aykırılığına ilişkin tespit kararı verir. Tespit kararı TMK 25/2.maddesi uyarınca davacının isteği üzerine ayrıca üçüncü kişilere bildirilerek yayınlanabilir.

Kişisel verilerin korunmasında, tespit davasına pek başvurulmadığı hukuka aykırılığın tespitiyle durdurulması için KVKK da belirlenen genel hükümler yoluyla çözüm yolu arandığı uygulama da görülmekte olup bu sebeple tespit davasının daha ziyade genel kişiliğin korunması haklarında uygulandığı düşünülmektedir[381]. Örneğin, kişisel verileri hukuka aykırı işlenen kişi bu hukuka aykırılığın durdurulmasını talep edebilir. İlgili kişinin bu talebi kendi içerisinde işleme fiilinin hukuka aykırı olup olmadığının tespitini de içermektedir[382].

---

[378] TMK 25/1 md.
[379] Öngün, s.289.
[380] Özdemir, s.188.
[381] Öngün, s.291.
[382] Özdemir, s.188.

4. Sebepsiz Zenginleşme Davası

Kişilik hakkına herhangi bir saldırı olması durumunda zarar verenin bu saldırı nedeniyle elde ettiği kazancın TBK'nın 77.maddesi uyarınca iadesi sebepsiz zenginleşme davası yoluyla istenebilir.

Sebepsiz zenginleşme davasının açılabilmesi için talepte bulunacak kişinin kişilik haklarına hukuka aykırı olarak saldırıda bulunulması, saldırı sonucunda saldırıda bulunulan kişinin fakirleşerek, saldırıda bulunan kişinin zenginleşmesi ve bu zenginleşme ile fakirleşme arasında uygun illiyet bağının bulunması gerekmektedir. Söz konusu zenginleşmenin istenmesi için saldırıda bulunan kişinin kusuru aranmaz[383]. Burada amaç kişilik hakkı ihlal edilen kişinin uğradığı saldırı sonucu oluşan zararının telafi edilmesidir. Sebepsiz zenginleşme davalarında iade edilecek tutar kişinin zenginleşmesinden fazla olamayacaktır. Örneğin; İşletmeci, aboneleriyle mevcut sözleşmesi sona ermesine rağmen ilgili kişisel verileri silmeyip kendi bünyesinde bulunan alışveriş firmasının müşteri hizmetlerine aktarması sonucu pazar payını yüksek göstererek önemli bir ihaleyi kazanırsa işletmecinin eski abonelerine karşı sebepsiz zenginleşmesi söz konusu olacaktır[384].

Sebepsiz zenginleşme davasının kişisel verilerin korunması hukuku açısından açılabilmesi için kişisel veri işleme faaliyetinin hukuka aykırı olması ve bu işleme faaliyeti sebebiyle veri işleyen kişilerin zenginleşerek verisi işlenen kişinin fakirleşmesi ve zenginleşme ile fakirleşme arasında bir illiyet bağının bulunması gerekmektedir. Hukuka uygun olarak işlenen kişisel veriler açısından sebepsiz zenginleşme davasının ileri sürülmesi mümkün değildir[385].

5. Vekaletsiz İş Görme Davası

TMK 25/3.maddesine göre kişilik hakkına saldırıda bulunan kişi, bu saldırı sonucunda birtakım kazançlar elde etmişse, TBK'nın 530.maddesinde düzenlenen vekaletsiz iş görme hükümleri doğrultusunda zarar gören bu kazancın kendisine ödenmesini isteyebilir.

---

[383] Rona Serozan, "Sebepsiz İktisap"ta Yoksullaşma Öğesine Yer Var Mıdır?", **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi,** Cilt:22, Sayı:3, 2016, ss.2499-2500.

[384] Öngün, s.294.

[385] Samet Saygı, "6698 Sayılı Kanun'un Sistematiğinde Yargısal Başvuru Yolları ", **Kişisel Verileri Koruma Dergisi,** Cilt:2, Sayı:2, 2020, s.33.

Vekaletsiz iş görme davasını açabilmenin şartlarından biri, saldırıda bulunan kişinin başkasına ait bir işi ilgili kişinin izin ve onayını almaksızın görerek bu kazancı elde etmesidir. Veri sahibinin resimlerini reklam amaçlı kullanması mümkünken bunu yapmadığı halde işletmecinin veri sahibinin rızası olmaksızın bu fotoğrafı reklamlarda kullanması bu duruma örnektir[386].

İkinci bir şart, vekaletsiz iş gören kişinin bu haksız kullanım sayesinde kazanç elde etmesidir. Burada önemli olan husus, elde edilen kazancın ilgili kişinin elde etmek istemediği veya elde edemeyeceği bir kazanç olmasıdır. Vekaletsiz iş görme davasını maddi tazminat davasından ayıran hususta budur. Çünkü maddi tazminat davasında davalı ilgili kişinin elde etmek istediği, elde edebileceği bir kazancı elde etmekteyken; vekaletsiz iş görme davasında vekaletsiz iş gören kişi tarafından elde edilen kazanç ilgili kişinin elde edemeyeceği kar kaybı olmayan bir kazançtır. Mektup, hatıra veya benzeri yazıların muhatabın rızası alınmaksızın yayınlanarak bundan bir kazanç elde edilmesi sonucunda kişilik hakları zarar gören kişi bu kazancın vekaletsiz iş görme hükümleri doğrultusunda kendisine iadesini isteyebilmesi bu duruma örnektir[387].

Vekaletsiz iş görme davasını, sebepsiz zenginleşme davasından ayıran kıstas sebepsiz zenginleşme davalarında verisi hukuka aykırı olarak işlenen kişinin malvarlığında bir azalma, fakirleşme meydana gelip gelmemesidir. Vekaletsiz iş görme davalarının açılması için başkalarının malvarlığında azalma meydana gelerek kişinin fakirleşmesi şartı aranmamaktadır. Elde edilen kazancın iadesi için hukuka aykırı olarak ilgili kişinin verisinin kullanılması yeterlidir[388].

6. Maddi Tazminat Davası

KVKK'nın 14/3.maddesinde kişilik hakları ihlal edilenlerin tazminat hakkı saklı tutulmuştur. KVKK'nın bu maddesi uyarınca hukuka aykırı olarak saldırıya uğrayan kişi bu zararın tazminini isteyebilir. TMK'nın 25/3.maddesinde kişilik hakkına yapılan haksız saldırılara karşı maddi tazminat davası açılabileceği öngörülmüştür. Maddi tazminat davasının amacı da hukuka aykırı fiil sebebiyle ilgili kişinin doğan zararın tazminidir.

---

386 Öngün, s.296.
387 Ali Ozan Yıldız, "Mektup, Hatıra ve Benzeri Yazıların Kişilik Hakkı Kapsamında Korunması ", **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, Cilt:25, Sayı:1, 2019, ss.465-466.
388 Özdemir, ss.203-204.

Maddi tazminat davasının açılabilmesi için hukuka aykırı bir eylem, hukuka aykırı eylemi yapan kişinin kusurlu olması, bu eylem sonucunda bir zararın meydana gelmesi ve bu hukuka aykırı eylemle zarar arasında illiyet bağının bulunması gerekmektedir. Örneğin, bir telefon operatörünün ünlü bir sanatçının faturasını ödemediği bilgisini kamuoyuna açıklaması sonucu sanatçıya yapılan iş teklifinin geri çekilmesi, bir mağazada bulunan gizli kamera kayıtlarının yayınlanması sonucunda mağaza da gerçekleşen müşteri kaybı, bir bankanın borsa da işlem gören şirketlerinin gizli sırlarını açıklaması maddi tazminat davasının konusunu oluşturabilir[389].

Kişisel verilerin korunması hukukuna konu maddi tazminat davasının açılabilmesi için davalının gerekli özen yükümlülüklerini yerine getirmeyerek, veri güvenliği ilkesini ihlal ederek ilgili kişinin zararına yol açması gerekmektedir. Burada davalının sorumlu tutulabilmesi için kast veya ihmal aranmaktadır. Kast durumunda kişi hukuka aykırı eylemlerinin neticesini bilerek ve isteyerek davranmaktayken; ihmal, kişinin hal ve şartların gerektirdiği özeni göstermeyerek davranmasıdır.

Maddi tazminat davalarında davacı zarar miktarını ispatla yükümlüdür. Hukuka aykırı bir fiil sonucunda oluşan zararlar, yoksun kalınan kar ve fiili zarar olarak ortaya çıkar[390]. Fiili zarar, saldırıya uğrayan kişinin malvarlığının aktifinde meydana gelen azalma veya pasifinde meydana gelen artıştır. Yoksun kalınan kar ise haksız fiil sebebiyle mal varlığında meydana gelmesi engellenen malvarlığında artışı ifade eder. Kişisel verilerin hukuka aykırı olarak işlenmesi halinde çoğunlukla oluşan maddi zarar yoksun kalınan kardır[391]. Zararın miktarının ispatı her zaman kolay olmayabilir. Davacı tarafından zararının miktarı ispatı tam olarak yapılamazsa hâkim olayların akışına, zarar görenin sosyo-ekonomik durumuna, almış olduğu tedbirlere bakarak zarar miktarını belirleyecektir. Maddi zararın hesaplanacağı an, kişilik hakkına saldırı yapıldığı andır[392].

Maddi tazminat davaları, zarar görenin zararı ve tazminat yükümlüsünü öğrendiği tarihten başlayarak iki yıl ve her halde fiilin işlendiği tarihten on yılın geçmesiyle zaman aşımına uğrar[393].

[389] Öngün, s.276.
[390] Develioğlu, s.134.
[391] Korkmaz, s.209
[392] Öngün, s.276.
[393] TBK 72 md.

7. Manevi Tazminat

Kişisel verilerin korunması yolunda inceleyeceğimiz son dava türü manevi tazminat davasıdır. Manevi tazminat davası TMK 25/3.maddesi ve TBK'nın 58.maddesinde düzenlenmiştir. Kişilik haklarına yapılan saldırı sonucunda manevi zarara uğrayan kişi bu hükümler doğrultusunda dava açabilir. Burada belirtilen manevi zarar, kişinin yapılan saldırı sonucunda duyduğu acı, elem ve üzüntüdür. Davanın amacı kişilik hakkına yapılan saldırı sonucunda oluşan acı, üzüntünün giderilerek kişinin ruhi dengesinin tekrar sağlanmasıdır[394].

Manevi tazminat davasının açılabilmesi için hukuka aykırı bir eylem, hukuka aykırı eylemi yapan kişinin kusurlu olması, bu eylem sonucunda manevi bir zararın meydana gelmesi ve bu hukuka aykırı eylem ile manevi zarar arasında uygun illiyet bağının bulunması gerekmektedir. Kişisel verilerin korunması alanında ise manevi tazminat talebi kişisel verilerin hukuka aykırı olarak işlenerek kullanılması halinde söz konusu olacaktır. Örneğin; kişinin telefonlarının dinlenerek kayda alınması, çok gizli resimlerin internet ortamında yayılması manevi tazminat davasının konusunu oluşturabilir[395].

Manevi tazminat davasında maddi tazminat davasında öngörüldüğü gibi ispat yükü davacıdadır. Ancak, manevi tazminatın maddi tazminattan farklı olarak somut olarak ispatı daha zordur. Zira kişiye yapılan saldırı sonucunda uğranılan manevi zarar elle tutulur gözle görülür kayıtlarla ispat edilememektedir. Hâkim bu durumda somut olayın özelliklerine, manevi zarar sonucu oluşabilecek duygu kaybı ve dışa yansıyan görüntüleri dikkate alarak karar verecektir[396]. Manevi tazminat davası sonucunda verilecek tazminat miktarını belirleme konusunda hâkime takdir hakkı da verilmiştir[397]. Hâkim saldırının derecesi, kullanılan araçlar, saldırının sürekliliği gibi somut olayın özelliğine bakarak zarar verenin kastı hariç hafif ihmalinin bulunduğu durumlarda tazminatta indirim yapabilecektir.

TBK 58.maddesi uyarınca hâkim, manevi tazminatın ödenmesi yerine, zararın başka bir şekilde giderilmesine de karar verebilir. Hâkim gerekçe göstererek başka diğer tazminat şekillerine karar verebilir. Diğer tazmin şekillerine özür dileme, kınama, mahkeme kararının yayınlanması gibi örnekler verilebilir[398].

---

394 Develioğlu, s.135.
395 Öngün, s.281.
396 Özdemir, s.221.
397 TBK 50-51 md.
398 Oğuz Sadık Aydos, "Basın Yoluyla Kişilik Hakkı İhlallerinde Manevi Tazminat ", **Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Hukuk Dergisi**, Cilt:16, Sayı:2, 2012, s.23.

TMK’nın 25.maddesi uyarınca manevi tazminat talebi karşı tarafça kabul edilmedikçe devredilemez. Miras bırakan tarafından ileri sürülmüş olmadıkça mirasçılara geçmez.

TBK’nın 72.maddesi uyarınca manevi tazminat davaları, zarar görenin zararı ve tazminat yükümlüsünü öğrendiği tarihten başlayarak iki yıl ve her halde fiilin işlendiği tarihten on yılın geçmesiyle zaman aşımına uğrar.

SONUÇ

Bilişim dünyasında sürekli yaşanan gelişmeler neticesinde her bir kişi, veri üretir konuma gelmiştir. Dünyanın her tarafında internetin yaygın kullanımı ile beraber sosyal medya kullanımı da oldukça artmıştır. Akıllı telefonlar, akıllı saatler, tabletlerin insan yaşamının ayrılmaz bir parçası haline gelerek insan yaşamının çok önemli bir noktasında bulunduğu söylenebilir. Bu gelişmeler ışığında haliyle veri miktarında artışa bağlı olarak veri işleme faaliyetleri de artmıştır. Bu sebeple de kişisel veri işleme faaliyetlerinin belirli temel prensipler ve kurallar çerçevesinde yapılması gerekmektedir. Belirli temel prensipler ve kurallar gözetilmeksizin hukuka aykırı olarak yapılan veri işleme faaliyeti kişilerin temel hak ve özgürlüklerini, kişi mahremiyetini açısından kişi menfaatlerinin zedelenerek maddi, manevi zararlara yol açabilir. Bu sebeple de kişisel verilerin korunması için bir takım hukuk düzenlemeler yapma zarureti doğmuştur. Dünyada kişisel verilerin korunmasına ilişkin ilk yasal düzenleme 1970 yılında Almanya'nın Hessen eyaletinde yapılmıştır. Sonra ki yıllarda, birçok Avrupa ülkesinde de bu düzenleme takip edilerek kişisel verilerin korunması için çeşitli düzenlemeler yapılmıştır. Uluslararası alanda kişisel verilerin korunmasına yönelik ilk düzenleme OECD tarafından yayınlanan tavsiye niteliğinde ki Rehber İlkelerdir. Devletler açısından hiçbir bağlayıcılığı olmayan bu metnin sonraki yıllarda ülkeler tarafından yasalar oluştururken ülkelerin yararlandığı bir kaynak olarak ulusal mevzuatlara temel oluşturmuştur. OECD'nin yayınladığı Rehber İlkelerden sonra Avrupa Konseyi kişisel verilerin korunmasına ilişkin uluslararası önem taşıyan 108 Sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesini yayınlamıştır. 108 Sayılı Sözleşme, OECD Rehber İlkelerinden farklı olarak sözleşmeye taraf devletler açısından bağlayıcıdır. 1981 yılında kabul edilen 108 sayılı Sözleşmenin, 1981 yılından bugüne gerçekleşen teknolojide ki gelişmeler gözetilerek güncellenerek yenilenmesi gerekmiş, bunun üzerine çalışmalar başlatılarak yapılan çalışmalar sonucunda 18.05.2018 tarihinde sözleşmenin revize edilmiş hali olarak Sözleşme 108+ metni kabul etmiştir.

Kişisel verilerin korunması hukukunun anavatanı olarak kabul edilen Avrupa Birliği konuya ilişkin ilk kapsamlı gelişkin mevzuatı 95/46/EC Sayılı Yönergedir. Türk Hukukunda kişisel verilerin korunması hakkının temelini oluşturan 6698 Sayılı Kişisel Verilerin Korunması Kanunu, Avrupa Birliğinin 95/46/EC Sayılı Yönergesi esas alınarak düzenlenmiştir. 95/46/EC Sayılı Yönerge yürürlüğe girdikten sonra kişisel verilerin hızla boyut değiştirmesi, kişisel verilerin günümüz şartlarına uygun şekilde

güvence altına alınması, 2013 yılında NSA analisti Edward Snowden tarafından veri sızıntılarına ilişkin ifşaatta göze alınarak 2018 yılında Avrupa Birliği GVKT yürürlüğe girmiştir. GVKT uygulama alanı ve kapsamı bakımından yalnızca AB üye ülke devletleri için değil, Avrupa Birliği üye devletleri ile ekonomik bağlarını sürdürmek isteyen diğer dünya devletleri açısından da küresel bir öneme sahiptir. GVKT dünya çapında uygulanabilir niteliktedir. Bu durumda tüm dünyada GVKT'ye uyum sağlanabilmesi için düzenlemeler yapılarak kişisel verilerin korunması için önlemlerin artırılmasına sebep olmuştur. Çalışmamız kapsamında GVKT'nin getirdiği yenilikler uluslararası etkileri açıklanmaya çalışılmıştır. 6698 Sayılı KVKK'nın GVKT'den önce yürürlüğe girmesi Türk Hukukunda 95/46/EC Sayılı Yönergenin etkisinin daha fazla hissettirmekle birlikte GVKT ile ortak düzenlemelerde bulunmaktadır. Bunlardan biri kişisel verilerin işlenmesinde alınan rızaya ilişkindir. 95/46/EC Sayılı Yönerge de sadece hassas nitelikli kişisel verilerin işlenmesi için açık rıza koşulu bulunmaktayken, KVKK ve GVKT'de tüm veri işleme işlemleri bakımından açık rızanın zorunlu olduğu öngörülmüştür. GVKT de düzenlenen önemli hususlardan biri unutulma hakkının yasalaşmasıdır. Unutulma hakkı, Avrupa Birliği sınırları dahilinde ki Mahkemelerde ve Türk Mahkemelerinde yıllarca tartışılan yargı kararlarına konu olmuş bir haktır. KVKK da her ne kadar unutulma hakkı açıkça mevzuatta düzenlenmemiş ise de uygulamada verilen yargı kararları doğrultusunda bu hakkın Türk Hukukunda uygulanabileceği söylenebilir. Bunların yanında GVKT de yer alan önemli yeniliklerden birkaçı tasarımdan ve varsayılan ayarlarla veri koruma, veri koruma görevlisi, veri koruma etki değerlendirmesi kavramlarıdır. Türk Hukukunda bu kavramlar mevzuatta açıkça düzenlenmemiştir. Bu sebeple bu kavramların Türk Hukukunda da benimsenerek gerekli yasal düzenlemelerin yapılması gerekmektedir. Bu ilke ve kavramların Türk Hukukunda uygulanması veri ihlal ve veri sızıntılarını önemli derecede önleyecektir.

Çalışmamız kapsamında kişisel verilerin korunması ihtiyacı ile birlikte kişisel verilerin hukuki niteliğine ilişkin görüşler incelenmiş, kişisel verilerin ekonomik yönüyle daha çok ilgilenen mülkiyet hakkı ve fikri mülkiyet hakkı görüşünün kişisel verilerin niteliğiyle örtüşmediği düşünülmektedir. Kişisel verilerin özel hayatın gizliliği hakkı çerçevesinde insan hakkı olarak düşünüldüğü görüş fikri mülkiyet ve mülkiyet hakkı görüşlerine göre daha makul olmakla birlikte, özel hayatın gizliliği hakkı kişisel verilerin korunmasında yetersiz kaldığı gözetilerek kişisel verilerin ayrı bir hak alanı olarak değerlendirilmesi gerektiğini düşünmekteyim.

Avrupa Birliği Hukuku mevzuatları ve Türk Hukukunda kişisel verilerin işlenmesine yönelik genel ilkeler ve kişisel verilerin işlenmesinde hukuka uygunluk

nedenleri çalışmamızda incelenmiştir. Kişisel verilerin işlenmesi hakkının özünü veriler işlenirken uygulanması gereken temel ilkeler oluşturmaktadır. Bu nedenle veri işleme faaliyetinde yer alan temel aktörler veri işleyen ve veri sorumlusu veri işleme faaliyetlerini yürütürken bu genel prensipleri her zaman gözeterek veri işlemelidirler. Aksi durumda yapılan veri işleme faaliyeti hukuka aykırı olacaktır. Buna ek olarak veri sorumlusunun veri işlerken uyması gereken yükümlülükler ve verisi işlenen ilgili kişilerin hakları çalışmamızda incelenmiştir.

Çalışmamızın son kısmında ise kişisel verilerin Türk Hukukunda korunması yolları incelenmiştir. İlgili kişi KVKK'dan kaynaklanan haklarının yanında TMK ve TBK da ki ilgili hükümler doğrultusunda genel hükümler doğrultusunda zararlarını talep edebilecektir. Türk hukukunda ilgili kişiler kişisel verilerin korunmasına yönelik talepleri için doğrudan yargı yoluna başvuracakları gibi KVVK da öngörülen veri sorumlusuna başvuru ve sonrasında KVK Kuruluna şikâyet yoluna gidebilecektirler. KVK Kurul kararlarının uygulanmaması veyahut veri sorumluluğu siciline kayıt ve bildirim yükümlülüğüne aykırı hareket eden veri sorumluları hakkında KVKK Kurumu idari para cezası kesebilecektir. Türk Hukukunda özel hukuk hükümleri yanında kişisel verilerin kişisel verilerin hukuka aykırı olarak kaydedilmesi, verilmesi, yayma ve ele geçirme, verileri yok etmeme hallerinde cezai yaptırımlarda öngörülmüştür. KVKK ile TCK arasında kişisel verilerin işlenmesi fiillerinin tanımı ve işlerliği arasında uyumsuzluk bulunmakla birlikte ilgili uyumsuzlukların giderilerek mevzuatların daha uyumlu ve işler hale getirilmesinin uygulama açısından faydalı ve gerekli olduğunu düşünmekteyiz.

Türk Hukukunda kişisel verilerin korunmasına yönelik hukuki düzenlemeler Avrupa Birliği'ne kıyasla oldukça geç çıkarılmıştır. Avrupa Birliğinde kişisel verilerin korunmasına yönelik çalışmaların üzerinden uzunca bir süre geçtiği gözetilerek Avrupa Birliğinin ilgili mevzuatları uyarınca bu mevzuatlardan yararlanılarak veri işleyen ve ilgili kişilerin hak ve yükümlülüklerine yönelik ülkemizde bilinçlendirilme yapılması gerekmektedir. Her ne kadar son zamanlarda kişisel verileri koruma hukuku çok göz önünde ise de ülkemizde pek çok kişi kişisel verinin ne anlama geldiğini bilmemektedir. Kişilerin verileri hakkında söz sahibi olarak verilerinin işlenmesinin hukuka uygun olarak yapılmasını talep etmesi ve bunun yapılmaması halinde hakkını arayarak gerekli hukuki yollara başvurması oldukça önemlidir. Türk Hukukunda kişisel veri kavramı yeni bir kavram olsa da KVK Kurumunun çeşitli bilgilendirmeleri ve KVK Kurul kararlarıyla kişisel verilerin korunmasına ilişkin eksikliklerin giderilerek veri koruma hukuku konusunda aydınlatmaların yapıldığını söylemek mümkündür.

Ülkemizde kişisel verilerin korunması hukuku yeni bir alan olsa da bu alanda büyük ilerlemeler kaydedilerek çağdaş toplumlar seviyesinde kişi haklarına saygılı şekilde kişisel verilerin korunması ülkemiz açısından hedeflerimizden biri olmalıdır.

KAYNAKÇA

Akgül, Aydın. **Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması,** Beta Yayınları, İstanbul, 2014.

Akif, Sadık. **Uluslararası Hukukta Kişisel Verilerin Korunması**, (Yayınlanmamış Yüksek Lisans Tezi), Anadolu Üniversitesi Sosyal Bilimler Enstitüsü, Eskişehir, 2020.

Aksoy, Hüseyin ve Mesut Halıcıoğlu, "E-Gizlilik Tüzüğü Çalışmaları Işığında Türk Hukukunda Elektronik Haberleşmenin Gizliliğinin Korunması", **Kişisel Verileri Koruma Dergisi,** Cilt:2, Sayı:2/1,2020, ss:2-3.

Akkurt, Sami Sinan. "Kişisel Veri Kavramının Hukukî Niteliğine İlişkin Yaklaşımlara Mukayeseli Bir Bakış", **Kişisel Verileri Koruma Dergisi**, Cilt:2, Sayı:1, 2020, ss.21-22.

Aksoy, Hüseyin Can. **Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması,** Çakmak Yayınları, Ankara, 2010.

Altıner, Bilal. "Birleşmiş Milletler: Amacı, Gelişimi, Etkinliği, Uluslararası Güvenliğe Katkısı ve Geleceği", **Avrasya Sosyal ve Ekonomi Araştırmaları Dergisi,** Cilt: 1, Sayı:1, 2014 ss. 1-2.

Altundiş, Mehmet. "Tıbbi Kişisel Verilerin Tutulması ve Korunması Yükümlülüğü ve İdarenin Bu Yükümlülüğünü Yerine Getirmemesinden Doğan Sorumluluğu", **Türkiye Adalet Akademisi Derneği,** Sayı:28, 2016, s.316.

Arsava, Füsun Ayşe. "AB Temel Haklar Şartının AB Hukuku ile İlişkisi", **Uyuşmazlık Mahkemesi Dergisi,** Sayı:7, 2016, ss.155-159.

Arslan, İlyas. "Kişisel Verilerin Yabancı Unsurlu Sözleşmelere Aykırı Olarak İşlenmesinden veya Korunmamasından Kaynaklanan Uyuşmazlıklara Uygulanacak Hukukun Tespit", **İstanbul Hukuk Mecmuası,** Cilt:79, Sayı:1, 2021, s.165.

Aşıkoğlu, Şehriban İpek. “Veri Sorumlularının Aydınlatma Yükümlülüğü Avrupa Birliği ve Türk Hukukunda”, **Kişisel Veri Koruma Dergisi,** Cilt:1, Sayı:2, 2019, s.43.

Atabey, Ayça, Melis Mert ve Leyla Keser Berber. “E-Gizlilik Tüzük Taslağının Son Versiyonu Üzerine Düşünceler”, **Kişisel Verileri Koruma Dergisi**, Cilt:1, Sayı:2, 2019, ss. 67-73.

Atasoy, Kemal “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.121

Atlı, Turan. “Kişilik Haklarının İhlali Durumunda İnternet Erişiminin Engellenmesi“, **Necmettin Erbakan Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:3, Sayı:1, 2020, ss.11-12.

Atlı, Turan. “Kişisel Verilerin Önleyici, Koruyucu ve İstihbari Faaliyetler Amacıyla İşlenmesi”, **Necmettin Erbakan Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:2, Sayı:1, 2019, s.10.

Aydoğdu, Yasin. “Kamu İdaresinde Kişisel Verilerin Korunması”, **Selçuk Üniversitesi Hukuk Fakültesi Dergis**i, Cilt:29, Sayı:1, 2021, s.290.

Aydos, Oğuz Sadık. “Basın Yoluyla Kişilik Hakkı İhlallerinde Manevi Tazminat “, **Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Hukuk Dergisi**, Cilt:16, Sayı:2, 2012, s.23.

Başalp, Nilgün. **Kişisel Verilerin Korunması ve Saklanması**, Yetkin Yayıncılık, Ankara, 2004.

Başalp, Nilgün. “Avrupa Birliği Veri Koruması Genel Regülasyonunun Temel Yenilikleri**”, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, Cilt 21, Sayı 1, 2015, ss.85-87.

Başara, Turan Gamze. **"Kişisel Veri İşleme Sözleşmesi"**, Uyuşmazlık Mahkemesi Dergisi, Sayı:16, 2020, ss.64-67.

Belgin, Derya. "Anayasa'nın 90. Maddesinde (7 Mayıs 2004) Yapılan Değişikliğin Getirdiği Sorunlar ve Çözüm Öneriler", **Ankara Barosu Dergisi**, Sayı:4, 2008, ss.110-113.

Bulut, Metin. "Özel Bir Hukuksal Koruma ve Veri Kategorisi Alanı: Hassas Kişisel Veriler", **Ankara Barosu Dergisi,** Cilt:78, Sayı:3, 2020, s.123.

Bulut, Serkan. "Söylemin Kapatılma ve Açımlama Savaşımında Edward Snowden", **Üsküdar Üniversitesi Etkileşim Dergisi**, Sayı:3, 2019, ss.131-134.

Bulut, Çimen. "Avrupa Birliği Genel Veri Koruma Tüzüğü Kapsamında Getirilen Yeni Teknik ve Yaptırım Mekanizmaları", **Anadolu Üniversitesi Sosyal Bilimler Dergisi,** Cilt:20, Sayı:2, 2020, ss.127-129.

Büken, Örnek ve Zeybek Ünsal. "Kişisel Verilerin Korunması Kanununun Biyomedikal Alana Yansımaları Açısından Değerlendirilmesi", **Hacettepe Hukuk Fakültesi Dergisi**, Cilt:7, Sayı:2, 2017, ss:48-49.

Çalık, Tacettin. " Birleşmiş Milletler Organlarının İnsan Hakları ile İlişkisi", **İnönü Üniversitesi Hukuk Fakültesi Dergisi**, Özel Sayı, Cilt:2, 2015, s.1094.

Çekin, Mesut Serdar. **Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku**, On İki Levha Yayıncılık, İstanbul, 2020,

Çelik, Yeşim. "Özel Hayatın Gizliliğinin Yansıması Olarak Kişisel Verilerin Korunması ve Bu Bağlamda Unutulma Hakkı, **Türkiye Adalet Akademisi Derneği**, Sayı:32, 2017, ss.397-398.

Çelikel, Serdar. "Kişisel Verilerin İşlenmesinde, Açık Rıza Hukuka Uygunluk Nedeninin, 95/46 Sayılı Direktif ve GDPR ile Karşılaştırmalı Olarak İncelenmesi**", Uyuşmazlık Mahkemesi Dergisi,** Sayı:17, 2021, ss.168-169.

Dal, Ufuk. “Avrupa Birliği Genel Veri Koruma Tüzüğünün Ülke Dışı Uygulama Yetkisi ve Bu Yetkinin Uluslararası Hukukta Meşruiyeti”, **Kişisel Verileri Koruma Dergisi**, Cilt:1, Sayı:1, 2019, ss.24-29.

Deniz, Miray Özer. “İşçilerin Özel Nitelikli Kişisel Verilerinin Korunması ve Bundan Doğan Sorumluluk”, **Türkiye Adalet Akademisi Dergisi**, Sayı:45, 2021, s.361.

Develioğlu, Hüseyin Murat. **6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku**, On İki Levha Yayıncılık, İstanbul, 2017.

Dülger, Murat Volkan. **Bilişim Suçları ve İnternet İletişim Hukuku**, Seçkin Yayıncılık, Ankara, 2018.

Dülger, Murat Volkan. “Avrupa Birliği Genel Veri Koruma Tüzüğü Bağlamında Kişisel Verilerin Korunması”, **Yaşar Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:1, Sayı:2,71, 2019, ss.98.

Dülger, Murat Volkan. “İnsan Hakları ve Temel Hak ve Özgürlükler Bağlamında Kişisel Verilerin Korunması”, **İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:5, Sayı:1, 2018, ss.88-89.

Dülger, Murat Volkan. “Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması”, **İstanbul Medipol Üniversitesi Hukuk Fakültesi** Dergisi, Cilt:3, Sayı:2, 2016, s.163.

Elmalıca, Hasan. “Bilişim Çağının Ortaya Çıkardığı Temel Bir İnsan Hakkı Olarak Unutulma Hakkı”, **Ankara Üniversitesi Hukuk Fakültesi Dergisi,** Cilt:65, Sayı:4, 2016, s.1611.

Gemicioğlu, Bora ve Zeynephan Gemicioğlu, **Kişisel Verilerin Korunması Mevzuatı Uluslararası Düzenlemeler ve İçtihatları**, On iki Levha Yayıncılık, İstanbul, 2019.

Güçlütürk, Gazi Osman. “Blok Zincir Üzerinde Depolanan Verilerin Kişisel Veri Niteliği ve Silinemezlik, Yok Edilemezlik Sorunu”, **Kişisel Verileri Koruma Dergisi**, Cilt:1, Sayı:2, 2019, s.33.

Gündüz Fatma Ebru ve İsmail Yazıcıoğlu, “Bilgi Edinme Hakkı Çerçevesinde Kişisel Verilerin Korunması”**, Anayasa Yargısı Dergisi**, Cilt:38, Sayı:1, 2021, s.174.

Güneş, Ahmet M. “Avrupa Birliği Yönergelerinin Doğrudan Etkisi”, **Ankara Üniversitesi Hukuk Fakültesi Dergisi,** Cilt 58, Sayı 2, 2009, ss.287-290.

Güneysu, Nilüfer Boran ve Burak Memiş. “Kişisel Verilerin Korunması Kanunu Kapsamında Avukatın Yükümlülük ve Sorumlulukları”, **Anadolu Üniversitesi Hukuk Fakültesi Dergisi,** Cilt:5, Sayı:2,2019, s:325.

Gür, Berna Akçalı. “Uluslararası Hukuk ve AB Hukuku Boyutuyla Kişisel Verilerin Yurtdışına Aktarılması”, **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, Cilt:25, Sayı:2, Prof. Dr. Ferit Hakan Baykal Armağanı, 2019, s.852

Gürsel, Esin ve Fatih Düğmeci. “Yapısal Anlamda Türkiye Kişisel Verileri Koruma Kurumuna İlişkin Bir Değerlendirme”, **R&S Research Studies Anatolia Journal**, Cilt:1, Sayı:2, 2018, s.321.

Gürses, Bekir. **AB ve Türk Hukukunda Kişisel Verilerin Korunması Mevzuat Uyumuna Yönelik Bir Değerlendirme,** (Yayınlanmamış Yüksek Lisans Tezi), Marmara Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2019.

Hanaz, Fatma Esenyel. “Çevrimiçi Eğitimde Üniversite Öğrencilerinin Kişisel Verilerinin İşlenmesinin Hukuki Sebepleri”, **Türkiye Barolar Birliği Dergisi**, Sayı:155, 2021, ss.424-425.

Henkoğlu, Türkay. “Kişisel Verileriniz Ne Kadar Güvende? Bilgi Güvenliği Kapsamında Bir Değerlendirme”, **Arşiv Dünyası Dergisi**, Sayı:18-19, 2017, ss.47-48.

İnan, Salih. “Kişisel Verilerin Korunması Kapsamındaki Yaptırımlara Karşı Yargısal Başvuru Yolları: Karşılaştırmalı Bir İnceleme”, **Kişisel Verileri Koruma Dergisi**, Cilt:3, Sayı:2, 2021, ss.57-59.

Karakaş, Muhammed Emin. “Dijital Geçmişin İnternet Erişiminden Kaldırılması "Unutulma Hakkı" ve Türk Hukukunda Görünümü”, **Necmettin Erbakan Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:3, Sayı:2, 2020, ss.281-282.

Karınçu, Sümeyra. **Kişisel Verilerin Korunması Kanunu Kapsamında Aydınlatma Yükümlülüğünün Yerine Getirilmemesi Kabahati**, (Yayınlanmamış Yüksek Lisans Tezi), İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü, İstanbul, 2019.

Kartal, Tevfik Mustafa. “Kişisel Verilerin Korunması: Türk Bankacılık Sektörü Üzerine Kavramsal Bir Değerlendirme”, **Uluslararası Ekonomi Ve Yenilik Dergisi**, Cilt:4, Sayı:1, 2018, s.9.

Kaya, Mehmet Bedii. “Kişisel Verilerin Korunmasında Yeni Paradigma: Hesap Verebilirlik İlkesi”, **İstanbul Üniversitesi Hukuk Mecmuası**, Cilt:78, Sayı:4, 2020, s.1869.

Kaya, Mine. “Telekomünikasyon Alanında Kişilik Haklarının Korunması“, **Ankara Barosu Dergisi,** Sayı:4, 2010, ss.293-294.

Keser, Yıldırım. “Tüketicinin Kişisel Verisinin İşlenmesinde Açık Rıza”, **Selçuk Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:28, Sayı:3, 2020, ss.1193-1196.

Kılıçoğlu, Ahmet. **Borçlar Kanunu**, Turhan Kitabevi, Ankara, 2011.

Kılınç, Doğan. “Anayasal Bir Hak Olarak Kişisel Verilerin Korunması”, **Ankara Üniversitesi Hukuk Fakültesi Dergisi,** Cilt:61, Sayı:3, 2012, s.1099.

Kişisel Verilerin Koruma Kurumu, **100 soruda Kişisel Verilerin Korunması Kanunu**, KVKK Yayınları No:3, Ankara, 2019.

Kişisel Verilerin Koruma Kurumu, **Örneklerle Kişisel Verilerin Korunması**, KVKK Yayınları No:29, Ankara, 2019.

Kişisel Verileri Koruma Kurumu, **KVKK Yayınları, Kişisel Verilerin Korunması Kanunu Hakkında Sıkça Sorulan Sorula**r, Ankara,2019.

Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin Korunması Kanuna İlişkin Uygulama Rehberi,** KVKK Yayınları No:1**,** Ankara, 2019.

Kontoğlu, Sena. "Madde 29 Veri Koruma Çalışma Grubu Avrupa Adalet Divanı'nın 13 Mayıs 2014 Tarihli Google Unutulma Hakkı Kararının Uygulanması Hakkında Yönerge Avrupa Adalet Divanı'nın "Google İspanya Ve Google Inc Karşı Agencıa Espanola Deproteccıo De Datos Aepd Ve Marıo Costejagonzalez Tarafından Açılan" Davada Verilen C-131/12 Kararının Uygulanması Hakkında Yönerge", **Küresel Veri Çeviri Hukuk Dergisi**, Cilt:6, Sayı:21, 2016, ss.1-2.

Korkmaz, İbrahim. **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, Seçkin Yayınları, Ankara, 2017.

Küpeli, Ceren. "Şiddet Mağduru Kadınların Unutulma Hakkı", **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, Cilt:22, Sayı:1, 2016, ss.234-235.

Küzeci, Elif. **Kişisel Verilerin Korunması**, On iki Levha Yayıncılık, İstanbul, 2020.

Metin, Yüksel. "Avrupa Birliği Temel Haklar Şartı", **Ankara Üniversitesi Siyasi Bilimler Fakültesi Dergisi,** Cilt:57, Sayı:4, 2002, ss.46-47.

Nurata, Zeynep Ceren. "Hukuksal, Örgütsel ve Etik Bir Sorun Olarak İşyerinde Elektronik Gözetim", **Gazi İşletme ve İktisat Dergisi**, Cilt:7, Sayı:3, 2021, s.217.

Nalbantoğlu, Seray. "Bir Temel Hak Olarak Unutulma Hakkı", **Türkiye Adalet Akademisi Dergisi,** Sayı:35, 2018, s.589.

Ocak, Ayşenur. "Hakları Dengelemek: Unutulma Hakkı İfade Özgürlüğüne Karşı", **Türkiye Adalet Akademisi Dergisi,** Sayı:33, 2018, ss.515-516.

Ömeroğlu, Abdullah. “Kişilik Haklarının Alkaya-Türkiye Davası Bağlamında Kişisel Verilerin Korunması Hukukuna Göre İncelenmesi “, **Uyuşmazlık Mahkemesi Dergisi,** Sayı:15, 2020, s.333.

Öngün, Çiğdem Ayözger. **Kişisel Verilerin Korunması Hukuku**, Beta Yayıncılık, İstanbul, 2019.

Özçelik, Zübeyir ve Ebru Aykan. “Sosyal Bilimlerde Büyük Veri Kullanımı, Veri Toplamada Akademik Çalışmalara Ne Tür Kolaylıklar Sağlayabilir?”, **Anadolu Üniversitesi Sosyal Bilimler Dergisi**, Cilt:20, Sayı:3,2020, s:137.

Özdemir**,** Hayrunnisa. **Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması,** Seçkin Yayıncılık, Ankara, 2009.

Özlük, Betül. “Mülkiyet ve Zilyetlik Üzerine Düşünceler”, **Selçuk Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:27, Sayı:1, 2019, ss.142-143.

Öztan, Bilge. **Medeni Hukukun Temel Kavramları**, Turhan Kitabevi Yayınları, Ankara,2009,

Öztekin, Mehmet Semih. “Brezilya Veri Koruma Yasasının 6698 Sayılı Kişisel Verilerin Korunması Kanunu ile Mukayeseli Olarak İncelenmesi”, **Kişisel Verileri Koruma Dergisi**, Cilt:3, Sayı:2, 2021, s.40.

Paşaoğlu, Cengiz ve Emel Cevheroğlu, “Bulut Bilişim Sistemleri Kapsamında Kişisel Verilerin Şifreleme Yöntemleri ile Korunması”, **Bilişim Teknolojileri Dergisi**, Cilt:13, Sayı:2, 2020, s:191.

SalihPaşaoğlu, Yaşar ve Burcu Değirmencioğlu, “Unutulma Hakkının Bir İnsan Hakkına Dönüşme Yolculuğu”, **Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:24, Sayı:2, 2020, ss:369-371.

Saka, Rıza, Mahmut Koca ve Ramazan Çağlayan, **Avrupa Birliği Hukuku, İdare Hukuku, Ceza Hukuku Açısından Kişisel Verilerin İmhası,** Seçkin Yayıncılık, Ankara, 2020.

Sayar, İbrahim Barış. "The Administrative Fines Regime of the General Data Protection Regulation and Its Impact", **Kişisel Verileri Koruma Dergisi,** Cilt:3, Sayı:1, 2021, s.1.

Saygı, Samet. "6698 Sayılı Kanun'un Sistematiğinde Yargısal Başvuru Yolları", **Kişisel Verileri Koruma Dergisi,** Cilt:2, Sayı:2, 2020, s.33.

Serozan, Rona. "Sebepsiz İktisap"ta Yoksullaşma Öğesine Yer Var Mıdır?", **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi,** Cilt:22, Sayı:3, 2016, ss.2499-2500.

Sirmen, Leyla. **Eşya Hukuku,** Yetkin Yayınları, Ankara, 2018.

Solmaz, Eren. "Avrupa İnsan Hakları Mahkemesi Kararlarının "Kişisel Verilerin Korunmasına Katkısı", **İstanbul Üniversitesi Hukuk Mecmuası**, İdare Hukuku ve İlimleri Dergisi, Cilt:18, Sayı:1, 2018, ss.63-67.

Şimşek, Oğuz. **Anayasa Hukukunda Kişisel Verilerin Korunması**, Seçkin Yayınları, Ankara, 2008.

Takçı, Hidayet ve Pelin Canbay. " Kişisel Verilerin Korunmasında Öznitelik Tabanlı Gizlilik Etki Değerlendirmesi Yöntemi", **Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi,** Cilt:32, Sayı:4, 2017, ss:1301-1302

Tekgül, Cansu Akgün. "Brüksel 1Bis Tüzüğü ile Avrupa Birliği Genel Veri Koruma Tüzüğü Çerçevesinde Kişisel Verilerin İhlaline İlişkin Özel Hukuk Uyuşmazlıklarında Milletlerarası Yetki Kuralları", **Hacettepe Hukuk Fakültesi Dergisi**, Cilt:9, Sayı:1, 2019, ss.260-261.

Tekin, Nurullah.“ Kişisel Verilerin Korunması İle İlgili Türkiye'deki Kanun Tasarısının Avrupa Birliği Veri Koruma Direktifi Işığında Değerlendirilmesi”, **Uyuşmazlık Mahkemesi Dergisi**, Sayı: 4, 2014, ss.226-227.

Turan, Metin. **Karşılaştırılmalı Hukukta Kişisel Verilerin Korunması**, 4 Baskı, Seçkin Yayıncılık, 2021.

Turhan, Aydın. “İnsan Hakkı Kuşakları Arasındaki Tamamlayıcılık İlişkisi”, **İnönü Üniversitesi Hukuk Fakültesi Dergisi,** Cilt:4, Sayı:2, 2013, ss.359-360.

Uçak, Murat. “Kişisel Verilerin Ölümden Sonra Korunması”, **İstanbul Medeniyet Üniversitesi Hukuk Fakültesi Dergisi,** Cilt:6, Sayı:10, 2021, ss.113-114.

Uçak, Murat. “Kişisel Verilerin Korunması Hukukunun Genel İlkeleri”, **Bilgi Ekonomisi ve Yönetimi Dergisi**, Cilt:13, Sayı:2, 2018, s.121.

Uçak, Murat ve Serdar Çelikel. “Kişisel Verilerin İşlenmesinde, Açık Rıza Hukuka Uygunluk Nedeninin, 95/46 Sayılı Direktif ve GDPR ile Karşılaştırmalı Olarak İncelenmesi”, **Kişisel Verileri Koruma Dergisi,** Cilt:3, Sayı:1, 2021, s.54.

Umniyahasghar, Yosif. “Kişisel Verilerin İşlenmesi Şartları ve 6698 Sayılı Kişisel Verilerin Korunması Kanunun Ruhu Olarak Genel İlkeler”, **Selçuk Üniversitesi Adalet Meslek Yüksekokulu Dergisi,** Cilt:4, Sayı:1, 2021, s.20.

Uyarer, Sinem Göçmen. **Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması**, Seçkin Yayıncılık, Ankara, 2019.

Uygun, Murat. **Avrupa Birliğinin 95/46 Sayılı Veri Koruma Yönergesi Işığında Kişisel Verilerin Korunması,** (Yayınlanmamış Yüksek Lisans Tezi), Gazi Üniversitesi, Sosyal Bilimler Enstitüsü, Ankara, 2010.

Uzun, Sündüs Arınmış. “Türkiye'de Kişisel Verilerin Korunması ve Vatandaş Algısının Ölçülmesi”, **Bilişim Teknolojileri Dergisi**, Cilt:14, Sayı:3, 2021, s.214.

Üstün, Kamile Türkoğlu. “Güvenlik Soruşturmalarında Kişisel Verilerin Korunması”, **Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergis**i, Cilt:25, Sayı:2, 2021, ss.806-807.

Yıldırım, Hakan ve Volkan Kaplan. “2010 Anayasa Değişikliğinin Bilişim Suçlarıyla Mücadele Politikası Bakımından Etkilerinin Analizi ve Bu Amaçla Kurulan Kuruluşların İncelenmesi”, **Kamu Yönetimi ve Politikaları Dergisi,** Cilt:2, Sayı:3, 2021, ss:299-300.

Yıldız, Ali Ozan. “Mektup, Hatıra ve Benzeri Yazıların Kişilik Hakkı Kapsamında Korunması “, **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, Cilt:25, Sayı:1, 2019, ss.465-466.

Yılmaz, Berrak. **Türk Anayasa Mahkemesi ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması**, (Yayınlanmamış Doktora Tezi), Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü, Ankara, 2019.

Yücedağ, Nafiye. “**Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri**”, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Cilt:75, Sayı:2, 2017, ss.776-777.

Yücedağ, Nafiye. “Kişisel verilerin korunması kanunu kapsamında genel ilkeler”, **Kişisel Verileri Koruma Dergisi,** Cilt:1, Sayı: 1, 2019, s.49.

Yüksel, Armağan Ebru Bozkurt. **Bulut Bilişiminde Kişisel Verilerin Korunması**, Yetkin Yayınları, Ankara, 2016.

Zeybek, Çağrı Uysal. “Google’ın Yeni Gizlilik Politikası Google Inc. Tarafından 1 Mart 2012 Tarihinde Yayımlanan Politikasının Kişisel Verilerin Korunması İlkeleri İle Uyumluluğu Ve Avrupa Birliği’nin 95/46/EC Sayılı Veri Koruma Direktifi Açısından Değerlendirilmesi”, **Hacettepe Hukuk Fakültesi Dergisi,** Cilt:3, Sayı:1, 2013, s.106.

Online Kaynaklar

Avrupa Konseyi**,** "Kişisel verilerin işlenmesine ilişkin olarak bireylerin korunmasına ve bu tür verilerin serbest dolaşımına ilişkin Avrupa Parlamentosu ve Konseyi'nin 24 Ekim 1995 tarihli 95/46/EC sayılı Direktifi", https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML, (17.12.2020).

ABAD, "Google Spain SL ve Google Inc. v Agencia Española de Protección de Datos (AEPD) ve Mario Costeja González.", https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131, (20.04.2021)

ARTICLE 29 DATA PROTECTION WORKING PARTY,"Opinion 4/2007 on the concept of personal data",https://www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf, (19.01.2020).

ABAD, "Bodil Lindqvist", https://curia.europa.eu/juris/liste.jsf?num=C-101/01, (20.12.2021).

Dijital Güvenlik**, "**İşte Facebook ve Google'ın size dair sahip olduğu tüm veriler" https://www.dijitalguvenlik.org/arama-motorlari/iste-facebook-ve-googlein-size-dair-sahip-oldugu-tum-veriler/, (20.04.2021).

European Court of Human Rights, "Turkey- Mustafa Sezgin Tanrıkulu", https://hudoc.echr.coe.int/tur#%20, (14.05.2021).

European Court of Human Rights, ""L.H./Letonya, https://www.echr.coe.int/Documents/FS_Data_TUR.pdf,(14.05.2021).

European Court of Human Rights, "CASE OF KLASS AND OTHERS v. GERMANY", https://hudoc.echr.coe.int/tur (14.05.2021).

European Court of Human Rights, "CASE OF GASKIN v. THE UNITED KINGDOM", https://hudoc.echr.coe.int/tur (14.05.2021).

Kişisel Veri koruma Kurumu, “Veri Sorumlusu ve Veri İşleyen”, https://www.kvkk.gov.tr/Icerik/4195/Veri-Sorumlusu-ve-Veri-Isleyen, (14.05.2021).

Kişisel Verileri Koruma Kurumu, “ Yurt Dışına Veri Aktarımında Hazırlanacak Taahütnamelerde Dikkat Edilmesi Gereken Hususlara İlişkin Duyuru”, https://www.kvkk.gov.tr/Icerik/6741/YURT-DISINA-KISISEL-VERI-AKTARIMINDA-HAZIRLANACAK-TAAHHUTNAMELERDE-DIKKAT-EDILMESI-GEREKEN-HUSUSLARA-ILISKINDUYURU,(27.12.2020)

Kişisel Verileri Koruma Kurumu, " Ulaşım Hizmeti Sunan Bir Mobil Uygulama Kapsamında İşlenen Kişisel Veriler Hakkında”, https://www.kvkk.gov.tr/Icerik/6717/2020-65, (28.12.2020)

Kişisel Verileri Koruma Kurumu, "Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler”,https://www.kvkk.gov.tr/Icerik/6717/2020-65, (21.12.2020)

Kişisel Verileri Koruma Kurumu, “Kişisel Verileri Koruma Kurulunun 09.12.2019 tarihli 2019/372 K. Sayılı Kararı”, https://www.kvkk.gov.tr/Icerik/6663/2019-372, (01.05.2021).

Kişisel Verileri Koruma Kurumu, “Kişisel Verileri Koruma Kurulunun 27.02.2020 tarihli 2020/167 K. Sayılı Kararı”, https://www.kvkk.gov.tr/Icerik/6738/2020-167,(05.01.2022).

Kişisel Verileri Koruma Kurumu, “İş Başvurusu Sürecinde İşlenen Kişisel Verilerin Hukuka Aykırı Şekilde Paylaşılması”, https://www.kvkk.gov.tr/Icerik/5262/Kisisel-Verileri-Koruma-Kurumu-Karar-Ozetleri#, (07.05.2021).
Kişisel Verileri Koruma Kurumu, “Kişisel Verileri Koruma Kurulunun 07.11.2019 tarihli 2019/294 K. Sayılı Kararı”, https://kvkk.gov.tr/Icerik/6623/2019-331 ,(04.05.2021).

Kişisel Verileri Koruma Kurumu, “Kişisel Verileri Koruma Kurulunun 01.10.2019 tarihli 2019/331 K. Sayılı Kararı”, https://www.kvkk.gov.tr/Icerik/6556/2019-294, (05.01.2022).

Kişisel Verileri Koruma Kurumu, “Kişisel Verileri Koruma Kurulunun 18.09.2019 tarihli 2019/277K. Sayılı Kararı”, https://www.kvkk.gov.tr/Icerik/5545/2019-277, (03.05.2021)

Kişisel Verileri Koruma Kurumu, “Kişisel Veri İhlali Bildirim Formu”, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/e0413853-cd8c-428f-9315-2e8b3d874b46.pdf, (08.05.2021)

Kişisel Verileri Koruma Kurumu, “Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ” https://www.resmigazete.gov.tr/eskiler/2018/03/20180310-5.htm, (20.04.2021)

OECD, “Mahremiyetin Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin OECD Yönergeleri”,https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm, (30.12.2021)

Sputnik News, “ ABD ile Avrupa Birliği Arasında ki Veri Transferi Anlaşması Avrupa Adalet Divanına Takıldı”, https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf(01.01.2022);%20https://tr.sputniknews.com/20200716/abd-ile-ab-arasindaki-veri-transferi-anlasmasi-avrupa-adalet-divanina-takildi-kisisel-veriler-1042468896.html, (03.01.2021).

Türk Dil Kurumu, “Güncel Türkçe Sözcük”, https://sozluk.gov.tr/,(17.12.2020).

The Guardian, “Campbell, Mirror'a karşı gizlilik davasını kazandı”, 27.03.2002, https://www.theguardian.com/media/2002/mar/27/pressandpublishing.privacy, (18.04.2021)

Unitad Nations, “Guidelines for the Regulation of Computerized Personal Data Files, Adopted by General Assembly resolution 45/95 of 14 December 1990”, https://www.refworld.org/pdfid/3ddcafaac.pdf, (20.12.2021)

Türkiye Büyük Millet Meclisi,” Kişisel Verilerin Korunması Kanunu Tasarısı

(1/541) ve Adalet Komisyonu Raporu", https://docplayer.biz.tr/25716160-Kisisel-verilerin-korunmasi-kanunu-tasarisi-1-541-ve-adalet-komisyonu-raporu.html, (03.05.2021).

Vikipedi, Tıklama Akışı, https://tr.wikipedia.org/wiki/, (25.04.2021).

29.Madde Veri Koruma Grubu, "GOOGLE İSPANYA VE INC V. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD) VE MARIO COSTEJA GONZÁLEZ" C-131/12 HAKKINDA AVRUPA BİRLİĞİ ADALET MAHKEMESİNİN UYGULANMASINA İLİŞKİN WP225 KILAVUZU", https://ec.europa.eu/newsroom/article29/items, (19.01.2020).