T.C.
ERCİYES ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI

KİŞİSEL VERİLERİ KORUMA KURULU İLKE KARARLARI BAĞLAMINDA KİŞİSEL VERİ İHLALLERİ

Hazırlayan
Ahsen HAMURCU SÜMER

Danışman
Dr. Öğr. Üyesi Abdulkadir SAKA

Yüksek Lisans Tezi

Temmuz 2024, KAYSERİ

T.C.
ERCİYES ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI

KİŞİSEL VERİLERİ KORUMA KURULU KARARLARI BAĞLAMINDA KİŞİSEL VERİ İHLALLERİ

(Yüksek Lisans Tezi)

Hazırlayan
Ahsen HAMURCU SÜMER

Danışman
Dr. Öğr. Üyesi Abdulkadir SAKA

Temmuz 2024, KAYSERİ

BİLİMSEL ETİĞE UYGUNLUK

Bu çalışmadaki tüm bilgilerin, akademik ve etik kurallara uygun bir şekilde elde edildiğini beyan ederim. Aynı zamanda bu kural ve davranışların gerektirdiği gibi, bu çalışmanın özünde olmayan tüm materyal ve sonuçları tam olarak aktardığımı ve referans gösterdiğimi belirtirim.

Ahsen HAMURCU SÜMER

İmza

T.C.
ERCİYES ÜNİVERSİTESİ

Sosyal Bilimler Enstitüsü Müdürlüğü

Anabilim Dalı : Kamu Hukuku

Program Adı : Yüksek Lisans Tezi

Tez Başlığı : Kişisel Verileri Koruma Kurulu İlke Kararları Bağlamında Kişisel Veri İhlalleri

Yukarıda bilgileri verilen tez çalışmasının a) Giriş, b) Ana bölümler ve c) Sonuç kısımlarından oluşan (Kapak, Önsöz, Özet, İçindekiler ve Kaynakça hariç) toplam 160 sayfalık kısmına ilişkin 24/07/2024 tarihinde ***Turnitin*** intihal programından aşağıda belirtilen filtreleme uygulanarak alınmış olan özgünlük raporuna göre tezin benzerlik oranı**: %12'dir**.

Filtrelemeye **alıntılar dahil** edilmiştir. Filtrelemede **yedi (7) kelimeden daha az** örtüşme içeren metin kısımları hariç tutulmuştur.

Erciyes Üniversitesi Sosyal Bilimler Enstitüsü Tez İntihal Raporu Uygulama Esaslarını inceledim ve bu uygulama esaslarında belirtilen azami benzerlik oranlarına göre tez çalışmasının herhangi bir intihal içermediğini, aksinin tespit edilmesi durumunda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

Gereğini bilgilerinize arz ederim. 24/07/2024

Danışman: Dr. Öğr. Üyesi Abdulkadir SAKA Öğrenci: Ahsen HAMURCU SÜMER

KILAVUZA UYGUNLUK

"Kişisel Verileri Koruma Kurulu İlke Kararları Bağlamında Kişisel Veri İhlalleri" başlıklı Yüksek Lisans Tezi, Erciyes Üniversitesi, Sosyal Bilimler Enstitüsü, Tezsiz Yüksek Lisans Dönem Projesi Yazım Kılavuzuna uygun olarak hazırlanmıştır.

Hazırlayan	**Danışman**
Ahsen HAMURCU SÜMER	Dr. Öğr. Üyesi Abdulkadir SAKA

Kamu Hukuku Anabilim Dalı Başkanı

Prof. Dr. Cengiz GÜL

KABUL VE ONAY TUTANAĞI

Dr. Öğr. Üyesi Abdulkadir SAKA danışmanlığında **Ahsen HAMURCU SÜMER** tarafından hazırlanan **"Kişisel Verileri Koruma Kurulu İlke Kararları Bağlamında Kişisel Veri İhlalleri"** adlı bu çalışma jürimiz tarafından Erciyes Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı'nda Yüksek Lisans Tezi olarak kabul edilmiştir.

28/06/2024

Jüri :

Danışman : Dr. Öğr. Üyesi Abdulkadir SAKA

Üye : Prof. Dr. Fatih BİRTEK

Üye : Dr. Öğr. Üyesi Mustafa UYANIK

ONAY:

Bu tezin kabulü Enstitü Yönetim Kurulu'nun …. /…./…… tarih ve …….. sayılı kararı ile onaylanmıştır.

……. /…..…../ ……..…

Prof. Dr. Atabey KILIÇ

Enstitü Müdürü

ÖN SÖZ

Kişisel verilerin korunması hukuku alanında çalışmaya başlamamla birlikte avukat olarak sıklıkla karşılaşmış olduğum kişisel veri ihlalleri, bu konuya yönelik akademik bir çalışma yapma arzusunu doğurmuştur. Öncelikle, kişisel verilerin korunması hukuku ile beni tanıştırıp bana güvenerek bu alanda mesleğimi icra etmemi ve kendimi geliştirmemi sağlayan ve dolayısıyla aslında bu çalışmanın yazılmasına vesile olan Sayın Av. Arb. Nihat ŞİMŞEK'e ve Sayın Av. Arb. Nuriye ŞİMŞEK'e gönülden teşekkür ederim.

Tez yazım sürecinde hiçbir desteğini esirgemeyen, tecrübesi ve katkılarıyla rehberlik ederek bu çalışmanın şekillenmesinde anlayışla yardımcı olan kıymetli danışmanım Sayın Dr. Öğr. Üyesi Abdulkadir SAKA'ya; değerli katkıları sebebiyle Sayın Prof. Dr. Fatih BİRTEK ve Sayın Dr. Öğr. Üyesi Mustafa UYANIK'a teşekkür ederim.

Son olarak attığım her adımda yanımda olduklarını bildiğim canım aileme ve sadece bu süreçte değil, her zaman bana destek olan sevgili eşime teşekkürlerimi sunarım.

Ahsen HAMURCU SÜMER, Kayseri, 2024

KİŞİSEL VERİLERİ KORUMA KURULU İLKE KARARLARI BAĞLAMINDA KİŞİSEL VERİ İHLALLERİ

Ahsen HAMURCU SÜMER

Erciyes Üniversitesi Sosyal Bilimler Enstitüsü,
Yüksek Lisans Tezi, Temmuz 2024
Danışman: Dr. Öğr. Üyesi Abdulkadir SAKA

ÖZET

Türkiye'de yaşanan kişisel veri ihlallerini Türk veri koruma otoritesi olan Kişisel Verileri Koruma Kurulu İlke kararları ekseninde incelemeyi amaçlayan bu çalışma üç bölümden oluşmaktadır. Çalışmanın birinci bölümünde kişisel verilere ilişkin kavramsal açıklamalara yer verildikten sonra kişisel verilerin korunması hakkının dayanağı ve bu hakkın öneminden bahsedilmiştir. Kişisel verilerin korunmasına duyulan ihtiyaç, veri mahremiyeti ve veri güvenliğinin önemi de bu başlık altında incelenmiştir. Ardından kişisel verilerin korunmasına ilişkin uluslararası düzenlemeler ile Türk hukukunda konuya ilişkin kanuni düzenlemelere yer verilmiştir.

Kişisel veri ihlallerine ilişkin temel ilkeler ve kişisel verilerin korunmasına ilişkin denetim sistemine çalışmanın ikinci bölümünde yer verilmiştir. Veri işleme ve veri güvenliği ilkeleri ile veri işleme izni, kişisel verilerin korunmasına ilişkin temel ilkeler başlığı altında incelenmiştir. Devamında ise kişisel verilerin korunması hakkının korunmasına yönelik denetim sistemi incelenmiştir. Türk veri koruma otoritesi olan ve çalışmada ilke kararları incelenen Kişisel Verileri Koruma Kurumunun idari denetimine ilişkin detaylı açıklamalara yer verilmiştir.

Çalışmanın üçüncü ve son bölümünde ise veri ihlallerine ilişkin genel açıklamalara yer verilerek Kişisel Verileri Koruma Kurulunun ilke kararları doğrultusunda bu alanda yaşanan ortak sorunlar tespit edilmeye çalışılmıştır. Bu bağlamda etki değerlendirmesi, veri güvenliğine ilişkin yükümlülükler ve hesap verebilme zorunluluğu değerlendirilerek, ilke kararlarının veri koruma hukukuna katkısı açıklanmaya çalışılmıştır.

Anahtar Kelimeler : Kişisel Veri, Veri İhlali, İlke Kararı, Veri Güvenliği, Etki Değerlendirmesi.

PERSONAL DATA BREACHES IN THE CONTEXT OF THE PERSONAL DATA PROTECTION BOARD'S RESOLUTIONS

Ahsen HAMURCU SÜMER

Erciyes University Graduate School of Social Sciences
Master's Thesis, July 2024
Supervisor: Asst. Prof. Abdulkadir SAKA

ABSTRACT

This study, aiming to examine the personal data violations in Turkey within the framework of the principles decisions which are given the Turkish data protection authority, the Personal Data Protection Board, consists of three parts. The first part of the study provides conceptual explanations regarding personal data, followed by discussions on the basis of the right to personal data protection and the importance of this right. The need for the protection of personal data, the importance of data privacy, and data security are also examined under this heading. Subsequently, international regulations on the protection of personal data and legal regulations concerning the subject in Turkish law are discussed.

The second part of the study covers the fundamental principles related to personal data breaches and the audit system for the protection of personal data. Principles of data processing and data security, as well as consent for data processing, are examined under the title of fundamental principles for the protection of personal data. Furthermore, the audit system aimed at safeguarding the right to personal data protection is explored. Detailed explanations regarding the administrative supervision of the Personal Data Protection Authority, which is the Turkish data protection authority, and the board resolutions examined in the study are provided.

In the third and final part of the study, general explanations regarding data breaches are provided, and common problems in this field are attempted to be identified in line with the resolutions of the Personal Data Protection Board. In this context, the contribution of board resolutions to data protection law is explained by evaluating impact assessments, obligations related to data security, and the necessity of accountability.

Keywords: Personal Data, Data Breach, Board Resolutions, Data Security, Impact Assessment

İÇİNDEKİLER

KİŞİSEL VERİLERİ KORUMA KURULU İLKE KARARLARI BAĞLAMINDA KİŞİSEL VERİ İHLALLERİ

İKİNCİ BÖLÜM
KİŞİSEL VERİLERİN KORUNMASI HUKUKUNUN TEMEL İLKELERİ VE DENETİM SİSTEMİ

ÜÇÜNCÜ BÖLÜM

VERİ İHLALLERİ VE KİŞİSEL VERİLERİ KORUMA KURULU İLKE KARARLARI

SİMGELER VE KISALTMALAR LİSTESİ

108+	: Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması İlişkin Sözleşmede Değişiklik Yapılmasına Daire Protokol
95/46/EC	: AB Veri Koruma Direktifi
AB	: Avrupa Birliği
AİHS	: Avrupa İnsan Hakları Sözleşmesi
Akt	: Aktaran
AYM	: Anayasa Mahkemesi
BGYS	: Bilgi Güvenliği Yönetim Standartları
Bkz	: Bakınız
BM	: Birleşmiş Milletler
CD.	: Ceza Dairesi
CETS No:108	: Kişisel Verilerin Otomatik İşlem Sürecinde Korunması Hakkında Avrupa Konseyi Sözleşmesi
CETS No:181	: Denetleyici Makamlar ve Sınırötesi Veri Akışına İlişkin Ek Protokolü
CMK	: Ceza Muhakemeleri Kanunu
CNIL	: Fransız Veri Koruma Otoritesi Hürriyetler ve Bilişim Ulusal Komisyonu
E.	: Esas
E.T.	: Erişim Tarihi
Ed.	: Editör
GDPR	: Avrupa Birliği Genel Veri Koruma Tüzüğü
ICDPPC	: Uluslararası Veri Koruma Komiserleri Konferansı
ICO	: Bilgi Komisyonu Ofisi
IEC	: Uluslararası Elektroteknik Komisyonu
ISO	: Uluslararası Standardizasyon Kurumu
İYUK	: İdari Yargılama Usulü Kanunu
K.	: Karar
KEP	: Kayıtlı Elektronik Posta

Kurul	: Kişisel Verileri Koruma Kurulu
Kurum	: Kişisel Verileri Koruma Kurumu
KVKK	: Kişisel Verilerin Korunması Kanunu
md.	: Madde
MED	: Mahremiyet Etki Değerlendirmesi
No	: Numara
OECD	: Ekonomik İş Birliği ve Kalkınma Teşkilatı
OECD	: Ekonomik İş Birliği ve Kalkınma Teşkilatı
SPK	: Sermaye Piyasası Kurulu
TBK	: Türk Borçlar Kanunu
TBMM	: Türkiye Büyük Millet Meclisi
TCK	: Türk Ceza Kanunu
TDK	: Türk Dil Kurumu
TMK	: Türk Medeni Kanunu
Vd.	: Ve devamı
VERBİS	: Veri Sorumluları Sicil Bilgi Sistemi
VKED	: Veri Koruma Etki Değerlendirmesi
VUK	: Vergi Usul Kanunu
Yönetmelik	: Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik

TABLOLAR LİSTESİ

GİRİŞ

Günümüz dijital çağında, bireylerin kişisel verileri gizlilik endişeleri, kimlik hırsızlığı ve dolandırıcılık riskleri, hedefe yönelik reklamların artması, dijital ayak izlerinin etkisi ve veri güvenliği tehditleri gibi faktörlerin etkisiyle birlikte giderek daha büyük bir önem kazanmaktadır. Teknolojinin hızla ilerlemesiyle birlikte kişisel verilerin toplanması, işlenmesi ve saklanması süreçleri de artık sadece bireyler için değil, kişisel verileri uhdesinde bulunduran kuruluşlar ve hatta devletler için de kritik bir hal almıştır. Zira bu veriler, pazarlama stratejilerinin belirlenmesinden güvenlik önlemlerinin alınmasına, kamu politikalarının oluşturulmasından suçla mücadeleye kadar geniş bir yelpazede kullanılmakta ve bu verilere erişim, bilgi güvenliği ve mahremiyet konularında ciddi endişelere yol açmaktadır. Bu bağlamda, kişisel verilerin korunması sadece bir hukuki mesele olmaktan çıkıp toplumsal ve ekonomik bir gereklilik haline gelmiştir.

Türkiye gibi dijitalleşme sürecinde olan ülkelerde, kişisel verilerin korunması ve bu verilere ilişkin ihlallerin önlenmesi, bahsi geçen sebeplerden ötürü giderek önemini artırmaktadır. Türk hukukunda bu konulara ilişkin usul ve esaslar 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) ve ilgili düzenlemeler aracılığıyla belirlenmiştir. Ancak kanunların yanı sıra, uygulamadaki etkinlik ve denetim mekanizmalarının işlevselliği de bu alandaki başarıyı belirleyen önemli unsurlardan biridir.

Bu çalışma, Türkiye'de yaşanan kişisel veri ihlallerini ve bu ihlallerle mücadelede rol oynayan Kişisel Verileri Koruma Kurulu'nun ilke kararlarını ele almaktadır. Amacı, KVKK'nın belirlediği ilkeler doğrultusunda kişisel veri ihlallerinin nasıl ele alındığını ve bu bağlamda ortaya çıkan sorunları ortaya koymaktır. Bu nedenle çalışmanın öncelikli hedefi, kişisel verilerin korunması hakkının önemini, Türkiye'de kişisel veri ihlallerinin boyutlarını ve niteliğini anlamaktır.

Çalışma, kişisel verilere ilişkin kavramsal çerçeveden başlayarak kişisel verilerin işlenmesi ve işlemenin tarafları, kişisel veri korunması hakkı, kişisel verilerin önemi ve korunması ile uluslararası ve ulusal düzeydeki düzenlemeleri ve koruma mekanizmalarını ele almaktadır. Ardından, KVKK'nın belirlediği ilkeleri, veri güvenliği ilkeleri ve veri işleme izni gibi konular bu bölümde detaylı bir şekilde incelenmektedir. Ayrıca, kişisel verilerin korunmasına ilişkin Avrupa Birliği ve Türk hukukundaki denetim sistemi üzerinde durulmaktadır. Çalışmanın üçüncü bölümünde öncelikle ilgili kişinin, kişisel verileri üzerindeki hakları anlatılmaktadır. Zira kişisel veri ihlalleri doğrudan kişisel verinin sahibi olan ilgili kişiyi ilgilendirmektedir. İlgili kişinin haklarını bilerek verileri üzerinde hakimiyet sağlaması ve veri işleme sürecine katılması, bu süreçteki risklerin azaltılmasına yardımcı olmaktadır. Bu nedenle ilgili kişinin hakları ve hakların nasıl kullanılacağı detaylı şekilde ifade edilmektedir. Sonrasında veri ihlallerinin nasıl tespit edileceği ve tespit edilen ihlalin nasıl bildirileceği anlatılmaktadır. Ardından Kişisel Verileri Koruma Kurulunun İlke kararlarının tasnifi yapılmakta, bu kararların etkisi ve önemi irdelenmektedir. Son olarak, KVKK'nın ilke kararları doğrultusunda yaşanan ortak sorunlar ve çözüm önerileri tartışılmaktadır.

Bu çalışma ile literatürde ilk kez Kişisel Verileri Koruma Kurulunun ilke kararları doğrultusunda veri ihlallerine ilişkin risklerin azaltılmasına yönelik yapılan tespitlere ve çözüm önerilerine yer verilmektedir. Yaşanan veri ihlallerine yönelik risk türleri, riskin azaltılmasına yönelik etki değerlendirmesi türleri incelenmekte ve yaygın ihlaller için ilk defa örnek risk etki değerlendirmesi yapılmaktadır. Kişisel verilerin işlenmesi süreçlerindeki riskin en aza indirgenebilmesi için bilgi güvenliği ve veri güvenliği kavramları da incelenerek yaşanan ihlallerin sebepleri tespit edilmeye çalışılmaktadır.

Yapılan çalışma ile ilk kez gerçekleştirilen araştırma sonuçları ve çözüm önerileri doğrultusunda yenilikçi bir yaklaşım benimsenmektedir. Risk türleri ve etki değerlendirmesi türlerinin incelenmesi, veri güvenliği alanında teorik ve pratik kapsamlı bir analiz yapılması da bütüncül bir çalışmanın ortaya çıkmasını sağlamakta; pratik uygulanabilirlik açısından yol gösterici bir örnek ortaya çıkarılmaktadır. Böylece Türkiye'de kişisel verilerin koruması alanındaki mevcut veri ihlallerinin durumunun anlaşılması ve gelecekte kişisel verilerin korunması adına daha etkin bir koruma sağlanması için katkı sunması amaçlanmaktadır.

BİRİNCİ BÖLÜM

KİŞİSEL VERİLERİN KORUNMASI VE YASAL ÇERÇEVE

1.1. Kişisel Verilerin Korunması Hukukunun Dayanakları

1.1.1. Kişisel Verilerin Korunmasında Temel Kavramlar

1.1.1.1. Kişisel Veri

Türk Dil Kurumu (TDK) tarafından "kişisel" kelimesi "*Kişi ile ilgili, kişiye ilişkin, kişinin kendi malı olan, şahsi, zatî"*[1] şeklinde tanımlanmış; "veri" kelimesi ise *"bilgi, done, data*"[2] şeklinde tanımlanmıştır. Kişisel veri kavramı ise milli ve milletlerarası birçok hukuki düzenlemede olduğu gibi kişiyle ilgili olan bilgi şeklinde tanımlanabilir.

Veri koruma hukukunun temel uluslararası düzenlemelerinde kişisel veri benzer şekilde tanımlanmaktadır. Avrupa Konseyi tarafından düzenlenen 1981 tarihli 108 No'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nin[3] 2/a maddesinde kişisel veri, *"kimliği belirli ya da belirlenebilir bir gerçek kişi (ilgili kişi) hakkındaki tüm bilgiler kişisel verileri ifade eder"* şeklinde tanımlanmıştır. Avrupa Birliği tarafından 1995 yılında kabul edilen 95/46/EC Sayılı Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Direktifinde[4] ise kişisel veri, "*fiziksel, fizyolojik, zihinsel, ekonomik, kültürel veya sosyal kimliğine özel bir veya daha fazla faktöre veya bir kimlik numarasına atıf başta olmak üzere doğrudan veya dolaylı olarak tespit edilebilen bir tespit edilebilir kişi;*

---

1 "TDK Sözlük", (Erişim Tarihi 30.05.2023), https://sozluk.gov.tr/

2 "TDK Sözlük", (E.T. 30.05.2023), https://sozluk.gov.tr/

3 Avrupa Konseyi Anlaşma Serileri – No 108, (E.T. 08.12.2023), https://inhak.adalet.gov.tr/Resimler/Dokuman/2712020140848108_tur.pdf

4 Directive 95/46/EC Of The European Parliament and of The Council, (E.T. 08.12.2023), https://eur-lex. europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

tespit edilmiş veya tespit edilebilir gerçek kişiye (“veri öznesi) ilişkin herhangi bir bilgiyi kastedecektir” şeklinde tanımlanmıştır. Direktifin güncellenmesi ile 2016 yılında kabul edilen Avrupa Birliği Genel Veri Koruma Tüzüğü’nün (GDPR) 4. maddesinde[5] kişisel veri *“tanımlanmış veya tanımlanabilir bir gerçek kişiye (‘veri konusu’) ilişkin her türlü bilgi"* şeklinde ifade edilmiştir. Türk veri koruma hukukunun başlıca düzenlemesi olan 6698 sayılı Kişisel Verileri Koruma Kanunu (KVKK)’nda kişisel veri “*kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi*” olarak tanımlanmaktadır.

Kişisel verilerin korunmasına ilişkin düzenleyici metinlerdeki kişisel veri tanımlarına göre bir kişiye ait olan her türlü veri, kişisel veri özelliği taşımaktadır. "Her türlü veri" ifadesi kanun koyucular tarafından bilinçli bir şekilde seçilmiş olup bu ifade, kişisel veri kapsamının geniş yorumlanmasına olanak tanıyacak şekilde kullanılmıştır.[6] Zira KVKK’da da yapılan tanımda hangi bilgilerin kişisel veri olarak kabul göreceğine dair sınırlama yoktur. Kanunda, gelişen teknolojik imkanlar sayesinde türetilebilecek veri kategorilerini de kapsayacak biçimde geniş bir kişisel veri tanımı yapılmaktadır.[7] Bu nedenle bahsi geçen kişisel veri tanımının sınırlarının çizilmesi oldukça güçtür.[8] Kanuni

---

5 Art. 4 GDPR, Definitions, (E.T. 08.12.2023), https://gdpr-info.eu/art-4-gdpr/

6 Şehriban İpek Aşıkoğlu, *Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri*, (İstanbul: Oniki Levha Yayıncılık, 2018), 9.

7 Kişisel Verileri Koruma Kurumu, “6698 Sayılı Kanun’da Yer Alan Temel Kavramlar”, 14, (E.T. 08.12.2023) https://www.kvkk.gov.tr/Icerik/4187/6698-Sayili-Kanun'da-Yer-Alan-Temel-Kavramlar

8 Anayasa Mahkemesi tarafından verilen 12.11.2015 tarihli 2015/32 E. 2015/102 K. sayılı kararda *“kişisel veri kavramının teknolojik gelişmelere bağlı olarak çok farklı şekillerde ortaya çıkabileceğinden bu kapsama giren tüm verilerin kanun koyucu tarafından önceden öngörülebilmesi ve tek tek sayılabilmesi mümkün olmadığı; bununla birlikte gerek ulusal ve uluslararası mevzuat gerekse yargı içtihatları çerçevesinde "kişisel veri" kavramının, belirli veya kimliği belirlenebilir olmak şartıyla, bir kişiye ilişkin bütün bilgileri ifade ettiği kabul edildiği; bu nedenle kişisel veri kavramının bu çerçevede doktrin, uygulama ve yargı kararlarında belirlenerek anlam ve içeriğinin gelişip değişeceğinden kuşku olmadığı”* ifade edilmiştir. (AYM’nin aynı yöndeki kararları için bkz: E. 2013/122, K. 2014/74, 9.4.2014; E. 2014/149, K. 2014/151, 2.10.2014; E. 2013/84, K. 2014/183, 4.12.2014; E. 2014/74, K. 2014/201, 25.12.2014; E. 2014/180, K. 2015/30, 19.3.2015). Yargıtay 12. Ceza Dairesi, 2018/8466 E., 2019/9054 K. kararında da *“gerçek kişiyle ilgili her türlü bilginin kişisel veri olarak kabul edilmesi gerektiğinin belirtilmesi karşısında, her türlü kişisel verinin hukuka aykırı olarak başkasına verilmesi, yayılması ve ele geçirilmesi fiilleri TCK'nın 136. maddesindeki verileri hukuka aykırı olarak verme veya ele geçirme suçunu oluşturur. Bu nedenle herkes tarafından bilinen ve/veya kolaylıkla ulaşılması ve bilinmesi mümkün olan kişisel bilgiler de yasal anlamda “kişisel veri” olarak kabul edilmektedir. Ancak, verileri hukuka aykırı olarak verme veya ele geçirme suçunun uygulama alanının amaçlanandan fazla genişletilerek, uygulamada belirsizlik ve hemen her eylemin suç oluşturması gibi olumsuz sonuçların doğmaması için, somut olayın özellikleri dikkate alınarak titizlikle değerlendirme yapılması, olayda herhangi bir hukuk dalı tarafından kabul edilebilecek bir hukuka uygunluk nedeni veya bu kapsamda nazara alınabilecek bir hususun bulunup bulunmadığının saptanması ve sanığın eylemiyle hukuka aykırı hareket ettiğini bildiği ya da bilebilecek durumda olduğunun da tespit edilmesi gerekir.”* Yine Yargıtay 12. CD. 2013/10672 E., 2013/15772 K. sayılı ilamı da aynı yöndedir. Bu çerçevede, kişisel veri kavramının somut olay özelinde değişkenlik göstermesi, onun bağlam içinde değerlendirilmesi gerektiğini ortaya koymaktadır. Bkz: Mehmet

tanımdan yola çıkarak kişisel veri kavramının içerisine insanla ilgili maddi, gayrimaddi veya manevi her türlü değerin dâhil kabul edilebilmesi önünde bir engel bulunmamaktadır.[9] Bununla birlikte kişisel veri kavramının kapsamının belirli olması gerekmektedir. Aksi halde, kavram belirsizliği nedeniyle kişisel verilerin korunması da mümkün olmayacaktır.[10] Kişisel veri kavramının kapsamını belirleyen ise kanuni tanımlarda ifade edilen şu dört unsurdur: *Bir verinin bulunması, bir gerçek kişinin söz konusu olması, verinin gerçek kişiye ait olması,*[11] *veri sayesinde kişinin belirli ya da belirlenebilir olması*.

Verinin, anlamlı bir şekilde bir kişiye ilişkin olması o veriyi kişisel veri haline getirir.[12] İsim-soyisim, doğum tarihi, doğum yeri gibi kişinin doğrudan kesin tespitine imkân veren bilgiler kişisel veridir. Kişinin fiziksel, ekonomik, kültürel, sosyal veya psikolojik kimliğini yansıtan somut bilgiler içermesi veya kimlik, vergi, sigorta numarası gibi

---

Akçakoca, *Tıp Ceza Hukukunda Kişisel Sağlık Verilerinin Korunması,* (Ankara: Adalet Yayınevi, 2022), 36-38. Bu husus AYM'nin 2017/16849 başvuru numaralı, 19/10/2023 kararında da "*Anayasa'nın 20. maddesinin üçüncü fıkrasında güvence altına alınan kişisel verilerin korunmasını isteme hakkı yönünden inceleme yapılabilmesi için öncelikle anılan hak kapsamında korunması gereken bir kişisel verinin olup olmadığı belirlenmelidir. Anayasa hükmünün lafzı, konuya ilişkin uluslararası belgeler ve karşılaştırmalı hukuk dikkate alındığında belirli veya belirlenebilir bir gerçek ya da tüzel kişi hakkındaki her türlü bilgi kişisel veri olarak değerlendirilir. Ancak her davada ya da başvuruda Anayasa'nın 20. maddesinin üçüncü fıkrası anlamında bir kişisel veri bulunup bulunmadığı, davanın ve başvurunun kendine özgü koşulları dikkate alınarak tespit edilir. (E.Ü., § 59; Bestami Eroğlu, § 102; Bülent Kaya [GK], B. No: 2013/2941, 11/5/2016, § 49; Fatih Saraman [GK], B. No: 2014/7256, 27/2/2019, § 57; AYM, E.2013/122, K.2014/74, 9/4/2014; E.2014/149, K.2014/151, 2/10/2014; E.2013/84, K.2014/183, 4/12/2014; E.2014/74, K.2014/201, 25/12/2014; H.Ö., § 34).*" şeklinde ifade edilmiştir. Bu tanım, teknolojik ve sosyal gelişmelerle sürekli olarak gelişmekte ve evrilmektedir. Dolayısıyla kişisel veri kavramı, belirli kurallar ve normlar çerçevesinde şekillenen, esnek, otonom/özerk olmayan bir kavramdır.

9 Sami Sinan Akkurt, "Kişisel Veri Kavramının Hukukî Niteliğine İlişkin Yaklaşımlara Mukayeseli Bir Bakış", *Kişisel Verileri Koruma Dergisi,* 2 (2020): 20-32. 21, (E.T. 30.05.2023), https://dergipark.org.tr/tr/ pub/kvkd/issue/55487/726372

10 Murat Volkan Dülger, *Kişisel Verilerin Korunması Hukuku* (İstanbul: Hukuk Akademisi, 2020), 152.

11 Tüzel kişiler hükmi şahıslar olup bu kanunun korumasından yararlanamamaktadır. Bu noktada tüzel kişilere ait olup da gerçek kişi ile ilişkilendirilen verilerin durumunun ne olacağı uygulamada sıklıkla karşılaşılan bir sorundur. Avrupa Birliği Adalet Divanı, C-92/09 sayılı kararında tüzel kişiye ilişkin verilerin gerçek kişilerle ilişkilendirilmesi mümkünse tüzel kişinin veri koruma hukuku kapsamındaki korumadan yararlanabileceğine karar vermiştir. Bu nedenle tüzel kişiye ait olan ancak gerçek kişiyle ilişkilendirilen ve kişiyi belirleyebilen veriler de kişisel veri sayılabilecektir. Ancak şirketin adresi, unvanı gibi tüzel kişiye ait olup da gerçek kişiyle ilişkilendirilmesi mümkün olmayan veriler kişisel veri olmayacaktır. Bkz: Dülger, *Kişisel Verilerin Korunması,* 172.

12 Lothar Determann, *Kişisel Verilerin Korunması Uygulama Kılavuzu*, çev. Hilal Temel (İstanbul: On iki Levha Yayınları, 2021), XXVI.

herhangi bir kayıtla bağlantı kurulması halinde bir kişi belirlenebiliyorsa bu veriler de kişisel veri sayılacaktır.[13]

1.1.1.2. Özel Nitelikli Kişisel Veri

Özel nitelikli kişisel veriler hassas veriler olarak da ifade edilmektedir. Bu verilerin "hassas" yahut "özel" olarak nitelendirilmesinin sebebi, bu verilerin öğrenilmesi halinde ilgili kişi hakkında ayrımcılık yapılmasına veya mağduriyete neden olabilme niteliği nedeniyle[14] genel kişisel verilerden daha spesifik bir korumaya ihtiyaç duymasıdır. KVKK'nın 6. maddesinde sınırlı olarak sayılan özel nitelikli kişisel veriler, "*kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileridir."* Tahdidi şekilde belirtilen özel nitelikli kişisel veriler, kişisel verilere göre daha dar bir alana sahipken, Kanun'un korumasından daha fazla yararlanan bir bölgeyi ifade eder.[15]

Bir verinin özel nitelikli kişisel veri olması için yukarıdaki başlıkta bahsi geçen kişisel veri unsurlarını ihtiva etmesi gerekmektedir. Özel nitelikli kişisel veriler de genel kişisel veriler gibi kimliği belirli ya da belirlenebilir gerçek kişiye ait anlamlı bir veri olmalıdır. Kan grubu, ilaç bilgileri, muayene kayıtları gibi sağlık verileri; retina, parmak izi gibi biyometrik veriler; bir işçinin toplu iş sözleşmesinden kaynaklanan sendika bilgileri özel nitelikli kişisel verilere verilebilecek örneklerdendir.

1.1.2. Kişisel Verilerin İşlenmesi ve Tarafları

1.1.2.1. Veri İşleme

KVKK'nın "Tanımlar" başlıklı 3. maddesinin 1/e fıkrasında kişisel verilerin işlenmesi; "*kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi,*

---

13 Kişisel Verileri Koruma Kurumu, *Madde ve Gerekçesi ile Kişisel Verilerin Korunması Kanunu (Bilgi Notu) ve Kişisel Verilerin Korunmasına İlişkin Terimler Sözlüğü*, (Ankara: KVKK Yayınları, Mart 2019), 9.

14 Faruk Bilir, "6698 Sayılı Kişisel Verilerin Korunması Kanunu'na İlişkin Değerlendirme ve İnternet Çağında Kişisel Verilerin Korunması", *Anayasa Yargısı*, 37/2 (2020): 305-342, 328.

15 Dülger, *Kişisel Verilerin Korunması,* 177.

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" şeklinde tanımlanmaktadır. Bu tanım ile veri sorumlusunun yükümlülüklerinin ne kadar geniş bir yelpazede olduğu anlaşılmaktadır. Veri işleme faaliyeti, verinin elde edilmesinden başlayan ve devredilmesine kadar olan süreci kapsamakla birlikte bu sürecin ötesindeki aşamaları da içermektedir. Kanun koyucu, *"gibi"* ifadesiyle belirtilen faaliyetlerin belirli bir sınırlama içinde olmadığını açıkça ifade ederek sıralanan faaliyetler dışında gerçekleştirilen diğer veri işleme işlemlerinin de Kanun'un kapsamına dahil edilebileceğini vurgulamaktadır.[16]

Veri işleme faaliyetinin Kanun kapsamında belirtilen sürece dahil olabilmesi için tanımda da ifade edildiği üzere *"tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin[17] parçası olmak kaydıyla otomatik olmayan yollarla"* işlenmesi gerekmektedir. Zira bir bilginin kişisel veri özelliği taşıması ya da kişiyi temsil etmesi ancak bilginin işlenmesiyle mümkün olacaktır.[18] Kişisel veriler üzerinde bilişim sistemleri kullanılarak, yazılım veya donanım özellikleri vasıtasıyla önceden hazırlanan algoritmaların kullanılması suretiyle insan müdahalesi olmaksızın teknik destek ile bir faaliyette bulunulması kişisel verilerin "otomatik yolla" işlenmesi; kişisel verilerin işlemcisi olmayan cihazlar ile manuel olarak yani elle tutulması ise kişisel verilerin "otomatik olmayan yollarla" işlenmesidir.[19] Burada dikkat edilmesi gereken husus otomatik veya kısmen otomatik yollarla işlenen kişisel verilerin doğrudan Kanun kapsamındaki korumadan yararlanmasıdır. Otomatik olmayan yollarla işlenen kişisel verilerin Kanun kapsamında değerlendirilebilecek bir veri işleme faaliyeti olması için bu verilerin bir veri kayıt sisteminin parçası olması icap etmektedir.[20] Örnek vermek gerekirse, bir okulun

---

16 Mesut Serdar Çekin, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku*, (İstanbul: On İki Levha yayınları, 2. Baskı 2019), 50; Aşıkoğlu, *Avrupa Birliği ve Türk,* 111; Kişisel Verileri Koruma Kurumu, *100 Soruda Kişisel Verilerin Korunması Kanunu*, (Ankara: KVKK Yayınları, Aralık 2019), 21.

17 KVKK'nın 3/1-h maddesinde veri kayıt sistemi, *"kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi*" olarak tanımlanmaktadır.

18 Bayram Doğan, "Dijital Veri Uygulamalarında Kişisel Verilerin Korunması" İçinde *Güncel Gelişmeler Işığında Kişisel Verilerin Korunması Hukuku*, Editor: Bayram Doğan, 75-100, (Ankara: Adalet Yayınevi, 2022), 137.

19 Kişisel Verileri Koruma Kurumu, "Temel Kavramlar", s. 18,19.

20 Elif Küzeci*, Kişisel Verilerin Korunması,* (İstanbul: On İki Levha Yayıncılık, Mayıs 2020), 371; Dülger, *Kişisel Verilerin Korunması*, 183; Kişisel Verileri Koruma Kurumu, "Temel Kavramlar", s. 18

kütüphanesinden kitap temin eden öğrenci kayıtlarının elle tutulması, otomatik vasıtalardan yararlanılmasa bile bir veri kayıt sisteminin parçası olduğu için veri işleme faaliyeti olarak kabul edilebilecektir. Öte yandan kütüphaneye giren öğrencilerin yapay zekâ destekli bir kamera ile teşhis edilmesinde veriler kaydedilmese de otomatik yolla veri işleme sürecinin yürütüldüğü ifade edilebilecektir.[21]

1.1.2.2. Veri Sorumlusu ve Veri İşleyen

Kişisel veri hukuku, verilerin hukuka aykırı işlenmesi neticesinde "*veri sorumlusu"* ve "*veri işleyen*"in hukuka aykırı eyleminin sorumluluğunu taşıması esasına dayanır.[22] Başka bir ifade ile kişisel verilerin korunması hukuku açısından merkez kavramların veri işleyen ve veri sorumlusu olduğu söylenebilir.[23]

Veri sorumlusu Kanun'da; "*Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi*" olarak tanımlanmaktadır. Gerçek kişiler ve tüzel kişiler (kamu kurum ve kuruluşları, şirketler, dernekler veya vakıflar gibi) veri sorumlusu olabilir.[24] Tanımdaki kriterleri taşıyan bir tüzel kişi (örneğin bir şirket) bünyesinde kişisel veri işleme faaliyetinin gerçekleştirilmesi neticesinde veri sorumlusu tüzel kişinin bizzat kendisi olmaktadır. Aynı yönde, tanımdaki özellikleri taşıyan bir gerçek kişi (örneğin bir eczane) adına kişisel veri işleme faaliyeti gerçekleştirilmesi durumunda da veri sorumlusu bu gerçek kişidir.[25] Ancak her zaman veri sorumlusunun tespit edilmesi bu şekilde basit olmayabilir. Örneğin, bir şirketin işten ayrılan çalışanlarından birinin şirketin müşteri listesini izinsiz alması üzerine şirket sahibinin durumu bir avukata danışması durumunda; şirket sahibinin eski çalışanıyla alakalı kişisel verileri avukata vermesi üzerine, avukat da veri sorumlusu olur. Bu örnekte avukatın şirket adına iş yapıyor olması onu veri işleyen statüsüne sokmaz. Zira avukat elde ettiği kişisel verilerin nasıl işleneceğine kendisi karar

---

21 Hüseyin Murat Develioğlu, *6698 Sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku*, (İstanbul: On İki Levha Yayıncılık, 2017), 40.

22 Develioğlu, *6698 Sayılı Kişisel,* 42.

23 Çekin, *Avrupa Birliği Hukukuyla*, 52*;* Develioğlu, *6698 Sayılı Kişisel,* 42.

24 Kişisel Verileri Koruma Kurumu, *Madde ve Gerekçesi*, 9.

25 Kişisel Verileri Koruma Kurumu, *6698 Sayılı Kişisel Verilerin Korunması Kanunu Hakkında Doğru Bilinen Yanlışlar,* 31 (Ankara: KVKK Yayınları, Nisan 2020), 18.

verecektir.[26] Bu gibi durumlarda veri sorumlusunun tespit edilmesi için şu kriterlerin dikkate alınması; bahsi geçen kriterlere ilişkin karar veren kişinin veri sorumlusu olduğunun kabulü gerekmektedir:[27]

- *"Kişisel verilerin toplanması ve toplama usulü,*
- *Toplanacak kişisel veri çeşitleri,*
- *Toplanan kişisel verilerin hangi maksatla kullanılacağı,*
- *Hangi kişilerin kişisel verilerinin toplanacağı,*
- *Toplanan kişisel verilerin paylaşılıp paylaşılmayacağı,*
- *Toplanan kişisel veriler paylaşılacaksa kiminle paylaşılacağı,*
- *Kişisel verilerin ne kadar süreyle muhafaza edileceği."*

Bu kriterlerden hareketle veri sorumlusunun kişisel verilerin elde edilmesinden muhafaza süresinin sonuna kadar geçen zaman diliminde bahsi geçen kişisel veriler üzerindeki her türden işleme dair karar verme yetki ve yükümlülüğü vardır. Dolayısıyla veri işleme sürecinin tamamına ilişkin kapsam ve sınırlar veri sorumlusu tarafından belirlenir.[28] Bu yüzden veri sorumlusunun yukarıdaki kriterleri dikkate alabilecek konumda bulunması, gerçekleştirilecek veri işleme faaliyetleri açısından karar verme iradesinin oluşması açısından önemlidir. Veri kayıt sisteminin kurulması ve yönetilmesi yönünden ise veri sorumlusunun karar verici pozisyonda bulunması gerekmektedir.[29]

Veri işleyen ise *"veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi"* (KVKK md. 3/1-ğ) ifade etmektedir. Veri işleyenin eylemleri veri işlemenin daha çok teknik bölümleri ile sınırlıdır.[30] Buradaki en mühim kriterlerden biri veri işleyenin, işleme faaliyetinde herhangi bir menfaatinin bulunmaması

---

26 Kişisel Verileri Koruma Kurumu, "Veri Sorumlusu ve Veri İşleyen", 8, (E.T. 09.12.2023), https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/31d9c444-27a5-4a75-95b1-ca9bdb81ea5.pdf

27 Kişisel Verileri Koruma Kurumu, "Veri Sorumlusu ve Veri İşleyen", 2.

28 Dülger, *Kişisel Verilerin Korunması*, 189,190.

29 Aşıkoğlu, *Avrupa Birliği ve Türk,* 113.

30 Kişisel Verileri Koruma Kurumu, "Veri Sorumlusu ve Veri İşleyen", 2.

sadece veri sorumlusu adına hareket ediyor olmasıdır.[31] Ancak veri sorumlusu düzenleyeceği bir kişisel veri işleme sözleşmesi[32] ile veri işleyene aşağıda örnek olarak verilen konularda karar verme hakkını tanıyabilir:[33]

- *"Kişisel verilerin toplanması için hangi bilgi teknolojileri sistemlerinin veya diğer yöntemlerden yararlanılacağı,*
- *Kişisel verilerin hangi usulle muhafaza edileceği,*
- *Kişisel verilerin korunması için alınacak güvenlik tedbirlerinin ayrıntıları,*
- *Kişisel verilerin aktarımının hangi usulle gerçekleştirileceği,*
- *Kişisel verilerin saklanması ile ilgili sürelerin doğru tatbik edilebilmesi için kullanılacak yöntem,*
- *Kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesi usulü."*

Burada dikkat edilmesi gereken nokta, veri sorumlusunun veri işleyene yetki verdiği durumlarda veri sorumlusunun sorumluluğunun mevcudiyetidir. KVKK'nın 12. maddesi[34] doğrultusunda veri güvenliği ile getirilen yükümlülükler bakımından veri sorumlusu ve veri işleyen müteselsilen sorumludurlar. Söz konusu düzenlemenin lafzı doğrultusunda Kanunda belirtilen güvenlik tedbirlerinin ihlal edilmesi durumunda doğacak zararlardan veri sorumlusu ve veri işleyen müştereken sorumlu olacaktır.[35]

---

31 Dülger, *Kişisel Verilerin Korunması*, 209.

32 *"Veri işleme sözleşmesi, veri işleyenin, veri sorumlusunun başta amaç ve yönteme ilişkin olmak üzere tüm talimatları doğrultusunda veri işlemeyi taahhüt ettiği, bu işleme faaliyetinin karşılığında da veri sorumlusunun bir bedel ödemeyi taahhüt ettiği iki tarafa borç yükleyen isimsiz bir sözleşmedir*", bkz: Gamze Turan Başara, "Kişisel Veri İşleme Sözleşmesi", *Uyuşmazlık Mahkemesi Dergisi*, 8/16, (Aralık 2020): 57-90, 58.

33 Kişisel Verileri Koruma Kurumu, Veri Sorumlusu ve Veri İşleyen, 3.

34 KVKK madde 12- (1) Veri sorumlusu;
a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,
b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,
c) Kişisel verilerin muhafazasını sağlamak,
amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.
(2) Veri sorumlusu, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, birinci fıkrada belirtilen tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumludur.

35 Turan Başara, "Kişisel Veri İşleme", 67.

1.1.2.3. İlgili Kişi

İlgili kişi, kişisel verileri koruma hakkının öznesidir.[36] Kişisel verisi işlenen gerçek kişi, KVKK kapsamında ilgili kişidir. Diğer bir anlatımla ilgili kişi; fiziksel, psikolojik, biyolojik, ekonomik, sosyal veya toplumsal kimliğine özgü etkenlerine kişisel veri yoluyla atıf yapılarak herhangi bir şekilde tanımlanan gerçek kişiyi ifade etmektedir.[37] Kanunda belirtilen kişisel veri tanımından da yola çıkarak, kişisel verilerin korunması hakkına sahip ilgili kişi, belirli veya belirlenebilir gerçek kişidir.

Konuyla ilgili yasal düzenlemeler gerçek kişilerin verilerinin işlenmesi sürecinde hakkın korunmasına ilişkin kuralları, ilkeleri ve istisnaları ifade eder. Düzenlemelerin esas amacı, genel olarak ilgili kişilerin temel hak ve özgürlüklerini güvence altına almak iken özü itibariyle kişisel verilerin korunmasının sağlanmasıdır.[38]

1.1.3. Kişisel Verilerin Korunması Hakkı

1.1.3.1. Genel Olarak

İnsan hakları, kişilerin doğuştan elde ettiği dokunulamaz ve devredilemez haklar olarak kabul görmektedir. Kişi özgürlüklerini kapsayan haklar ise negatif statü hakları olarak da belirtilmekte olup bu haklar bireyleri devlete ve topluma karşı koruyan haklardır. Dolayısıyla koruyucu haklar şeklinde de tanımlanmaktadır.[39] Kişiliğin serbestçe geliştirilmesi hakkı olarak da açıklanan kişilik hakkının esas amacı; insan onurunu, bireyin dar yaşam alanını ve tüm bunların ana şartlarını teminat altına almaktır. Kişisel verilerin korunması hakkının dayanağını ise esasen insan onuruyla birlikte kişiliğin serbestçe geliştirilmesi hakkı oluşturmaktadır.[40] Öte yandan kişisel verilerin korunması hakkı kronolojik olarak daha eski birtakım temel hak ve özgürlükler ile yakından ilişkidir.

---

36 Küzeci, *Kişisel Verilerin Korunması*, 361.

37 Dülger, *Kişisel Verilerin Korunması,* 188.

38 Dülger, *Kişisel Verilerin Korunması,* 188.

39 Doğan Kılınç, "Anayasal Bir Hak Olarak Kişisel Verilerin Korunması", *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, 61/3 (2012): 1089-1169, 1098. https://kutuphane.dogus.edu.tr/mvt/pdf.php?pdf=-0013299&lng=0 E.T. 15.02.2023; aynı yönde bkz: Bayram Doğan, *Karşılaştırmalı Hukukta Anayasal Bir Hak Olarak Kişisel Verilerin Korunması Hakkı*, (Ankara: Adalet Yayınevi, 2022), 40-41; İntizar Sultanlı, "Anayasal Bir Hak Olan Kişisel Verilerin Korunması Hakkı ve Mahremiyet ile İlişkisi", *SÜAMYOD.*, 4/1 (2021): 23-34, 28.

40 Oğuz Şimşek, *Anayasa Hukukunda Kişisel Verilerin Korunması*, (İstanbul: Beta Yayınları, 2008), 132.

Bunların ilk sırasında özel hayatın gizliliğinin korunması hakkı gelmektedir[41] ki kişisel verilerin korunması hakkı başlı başına bir hak olarak düzenlenmeden önce kişisel veriler, büyük çoğunlukla özel hayatın gizliliği hakkı kapsamında korunmuştur. Bununla birlikte kişisel verilerin korunması hakkı; bilgi edinme hakkı, haberleşme özgürlüğü,[42] uluslararası düzenlemelerde adı geçen "*mahremiyet hakkı*", *"bireyin yalnız bırakılma hakkı"*[43] gibi birçok hakla ilişkilendirilebilir.

Kişisel verilerin korunması hakkının söz konusu haklar bağlamında insan hakları ile ilgisini kavrayabilmek adına ilk olarak kişisel verilerin korunmasının dayandığı temel çıkarın tespit edilmesi gerekmektedir.[44] Zira kişisel veri kavramının ilişkilendirileceği değer ve temel çıkar, kişisel verilerin korunması ile ulaşılmak istenen sonucu doğrudan etkileyecektir. Bu nedenle koruma sağlanmak istenen değerin ve çıkarın belirlenebilmesi de hak kavramının içinin doldurulmasına ve hakkın hangi amaca hizmet ettiğinin belirlenmesine bağlıdır.

1.1.3.2. Kişisel Verilerin Korunması ile İnsan Haklarının İlgisi

Kişisel verilerin korunması ile genel itibariyle bireylerin özel hayatlarının, kimliklerinin ve kişisel bilgilerinin güvende tutulması amaçlanır. Günümüzde teknolojik ilerlemeler ve dijitalleşmeyle birlikte kişisel verilerin toplanması, depolanması, işlenmesi ve paylaşılması giderek daha mühim bir hale gelmiştir. Bu bağlamda, kişisel verilerin korunmasıyla hem bireylerin mahremiyetinin ve kişisel bilgilerinin korunması hem de veri kullanımının adil ve yasal sınırlar içinde gerçekleşmesinin sağlanması hedeflenir.

Kişisel verilerin korunması kavramı, kişisel veri tanımından ve Avrupa hukuk sistemlerindeki korumaya ilişkin yaklaşımlardan yola çıkarak en temel anlamıyla *"kimliği belirli veya belirlenebilir gerçek kişiye ait olan her türlü bilginin gizliğinin ve mahremiyetinin sağlanması*" şeklinde tanımlanır. Başka bir deyişle bireyin kişisel verilerinin korunması KVKK'nın da gerekçesinde[45] de belirtildiği üzere kişisel veri

41 Küzeci, *Kişisel Verilerin Korunması,* 66.
42 Küzeci, *Kişisel Verilerin Korunması*, 66; Sultanlı, "Anayasal Bir Hak", 24.
43 Aydın Akgül, *Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması*, (İstanbul: Beta Yayınları, 2014), 163-169.
44 Dülger, *Kişisel Verilerin Korunması,* 77.
45 Kişisel Verileri Koruma Kurumu, "6698 Sayılı Kişisel Verilerin Korunması Kanununun Amacı ve Kapsamı", (E.T. 30.05.2023), https://www.kvkk.gov.tr/Icerik/4185/6698-Sayili-Kisisel-Verilerin-Korunmasi-Kanunu nun -Amaci-ve-Kapsami

işleme faaliyetlerinin kontrol altına alınması ve Anayasa'da belirtilen başta özel hayatın gizliliği olmak üzere temel hak ve özgürlükler ile kişilerin mahremiyetinin korunması, kişisel veri güvenliğinin sağlanmasıdır. Kişisel verilerin korunması, kişinin bizzat kendisinin korunması olup temel bir insan hakkıdır ve esasen kişinin bizzat koruma altına alınması amacı için kişisel verilerin korunması bir araç konumundadır.[46] Diğer bir deyişle verilerin korunması konusunda başlıca amaç korumaya mevzu "veri içeriği" değil, korunması gereken veri içeriği ile ilgili kişilerdir.[47]

Anglo-Amerikan hukuk sistemlerinde "kişisel veri" bir değer yerine ekonomik anlamda piyasa ürünü ve meta olarak değerlendirmeye tabi tutulmaktadır. Bu nedenle kişisel verinin mülkiyet veyahut fikri mülkiyet hakkı kapsamında korunmasına hizmet eden "ekonomik değer/hak" yaklaşımı benimsenmiştir.[48] Kıta Avrupası hukuk sistemlerinde kabul gören sosyal–hümanist yaklaşımda ise kişisel veri kavramı, veri ile kişi arasındaki bağlantıyı koparmaksızın korunmaya mecbur "insani değer" olarak tanımlanmış, kişisel veriler özel hayata saygı hakkı ve kendi kaderini tayin etme hakkı (self-determinasyon) doğrultusunda temel insan hakkı ile ilişkilendirilerek bu bağlamda "insani ve sosyal değer" yahut "temel insan hakkı" yaklaşımı benimsenmiştir.[49]

Kişilik hakları içinde özel hayat, hakkın kullanımının kişinin kendi kontrolünde olması ve başkasının müdahalesine rıza göstermemesi, temelinde kişinin özgürlük ve mahremiyetinin olması ve ihlali halinde kişilik haklarının kullanımına da zarar gelmesi nedeniyle ayrı bir öneme sahiptir.[50] "Veri güvenliği" kavramının konusu doğrudan veriler iken, "kişisel verilerin korunması" kavramı doğrudan özel hayatın gizliliği doğrultusunda

---

46 Faruk Bilir, "Kişisel Verilerin Korunması Kişinin Kendisinin Korunmasıdır", *TRT Akademi*, 6 (11) 2021., 172- 181, (E.T. 30.05.2023) https://dergipark.org.tr/tr/pub/trta/issue/60117/870971

47 Akt. Furkan Kaan Yüksek, "AİHM İçtihatlarında Kişisel Verilerin Korunması", *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, 25 (2023): 371-420, 374, (E.T. 14.06.2023), https://dergipark.org.tr/tr/pub/ deuhfd/issue/76624/1276294

48 Akkurt, "Kişisel Veri Kavramının", 21-22; Rabia Özkan, "Kişisel Veri Koruma Hukukunun Kişilik Hakkının Korunması Çerçevesinde Değerlendirilmesi", *Ankara Sosyal Bilimler Üniversitesi Hukuk Fakültesi Dergisi*, 3 / 2 (2021), 675 – 733, 682. https://doi.org/10.47136/asbuhfd.963013; S. Hilal Üçüncü, *Medeni Yargılama Hukukunda Kişisel Verilerin ve Sırların Korunması,* (İstanbul: Oniki Levha Yayıncılık, 2019), 38-42.

49 Özkan, "Kişisel Veri Koruma Hukukunun", 688; Üçüncü, *Medeni Yargılama Hukukunda*, 38-42; Akkurt, "Kişisel Veri Kavramının", 25.

50 Yasin Demir, "Kişisel Verilerin İhlalinin Psikolojik Yansımaları", İçinde *Güncel Gelişmeler Işığında Kişisel Verilerin Korunması Hukuku*, Editor: Bayram Doğan, 75-100, (Ankara: Adalet Yayınevi, 2022), 79,80.

insan haklarını baz almaktadır.[51] Bu çerçevede kişisel verilerin korunması hakkının kapsamı, koruduğu ve teminat altına almayı amaçladığı insan onurudur. Bununla birlikte korunması gerekli temel haklar içerisinde yer almaktadır. Zira anılan bu hak doğuştan gelen ve salt insan olmaktan kaynaklanan üstün bir değerdir.[52] Bununla birlikte kişisel veri kavramı, temel insan haklarının özel hukuktaki görünümü olan kişilik hakkı kapsamında yalnızca özel hayatın gizliliğine hasredilmemiştir. Bu kavramın; özgürlükler, insan onuru, şeref-haysiyet, ekonomik varlık ve bağımsızlık, enformasyonel özerklik (self – determinasyon) gibi birçok kişisel değer ile doğruca ilişkili ancak müstesna koruma rejimi nedeniyle bunlardan kısmen bağımsız müstakil bir kişisel değer olarak kabul edilmesi uygun görülmektedir.[53] Zira bir hak olarak kişisel verilerin korunması hakkının bazı durumlarda bilgi edinme hakkı, ifade hürriyeti, bilim hürriyeti, basın hürriyet gibi bazı hak ve hürriyetlerle çatışması halinde "pratik uyuşum ilkesi"[54] uygulanarak her somut vaka özelinde değerlendirme yapılmak suretiyle çatışan haklardan hangisine üstünlük sağlanması gerektiğine göre bu hak sınırlanabilecektir.[55]

Türk veri koruma hukukunda kişisel verilerin korunması ile ilgili mevcut düzenlemelere bakıldığında, Avrupa hukuk sistemlerinde benimsenen "insani değer" yaklaşımı doğrultusunda koruma sağlayan düzenlemeler çoğunluktadır. Öte yandan "ekonomik değer" yaklaşımının öngördüğü kapsamda koruma sunan düzenlemeler de mevcuttur. KVKK md.5 vd. düzenlemeleri ilk esnada, ekonomik değer yaklaşımını benimsemiş gibi görünse de Türk veri koruma hukukunun, kişisel veri kavramının niteliği ile ilgili olarak (Anayasa md. 20/3 hükmü doğrultusunda) insan hakkı, (Türk Medeni Kanunu md.23, 24, 26 vd.; Türk Borçlar Kanunu md.58 hükümleri doğrultusunda) kişilik hakkı (Anayasa md. 20/3; KVKK md. 1 vd. maddeleri dolayısıyla) ve müstakil hak görüşlerinden

---

51 Aktaran Yüksek, 374.

52 Doğan, *Karşılaştırmalı Hukukta Anayasal*, 39-40.

53 Akkurt, "Kişisel Veri Kavramının", 30

54 Pratik uyuşum ilkesi, haklar arasında bir çatışma çıkması durumunda, çatışan hükümlerin birlikte değerlendirilerek uygun bir çözüm geliştirilmesidir. Bu ilke ile birlikte anayasa normları arasında bir hiyerarşi kurulmadan, yani birini diğerine öncelemeksizin haklar arasında uyum sağlanarak bir çözüm bulunmaktadır. Bu şekilde, bir hak diğer bir hakkı ortadan kaldırmadan, dengeli bir düzen içinde korunur ve etkisini optimal düzeyde sürdürebilir. Bkz: Akt. Ömer Keskinsoy ve Semih Batur Kaya, "Anayasa Mahkemesi Kararlarını Biçimlendirme Çabası Olarak Yorum", *Hacettepe Hukuk Fakültesi Dergisi*, 11/1 (Haziran 2021): 63-105, 86. DOI: 10.32957/hacettepehdf.866047

55 Adnan Küçük, "1982 Anayasası'ndaki Temel Hak ve Hürriyetlerin Sınırlanması Rejimi Bağlamında Kişisel Verilerin Korunması Hakkının Sınırlanmasının Anayasaya Uygunluğu", İçinde *Güncel Gelişmeler Işığında Kişisel Verilerin Korunması Hukuku*, Editor: Bayram Doğan, 11-74, (Ankara: Adalet Yayınevi, 2022), 70; Bilir, "6698 Sayılı Kişisel", 310.

meydana gelen karma bir yaklaşımı kabullendiği yönünde izlenim uyandırmaktadır. Hatta Anayasa'da da kişisel verilerin ayrı bir madde ile koruma altına alınmış olması, Türk veri koruma hukukunda kişisel verilerin korunmasının sadece medeni hukuk bağlamında ekonomik değeri olan mutlak haklara ve/veya kişilik hakkına ilişkin korumayla bağlı kalmadığı, başka bir ifade ile daha geniş kapsamlı (multidisipliner) bir kişisel değer olarak kabul edildiğini göstermektedir. Ancak KVKK'nın 5, 8 ve 9. maddelerindeki hükümler ile resmin ve sesin korunmasına ilişkin fikir ve sanat eserleri mevzuatındaki koruma (Fikir ve Sanat Eserleri Kanunu md.84) göz önünde bulundurulduğunda Türk veri koruma hukuk sisteminin ekonomik–iktisadi yaklaşımı göz ardı etmediği de söylenebilir.[56]

1.1.4. Kişisel Verilerin Önemi ve Korunması

1.1.4.1. Kişisel Verilerin Korunmasına Duyulan İhtiyaç

Bilgisayar, merkezi veri bankaları ve interneti de kapsayan teknolojinin görünmez yan etkileri, kişisel verilerin korunmasına yönelik tepkileri doğurmuş; kişisel veri güvenliği ve gizliliği konusunda yaşanan endişeler kişisel verilerin korunması hukukun doğmasında ve temel ilkelerin belirlenmesinde etkili olmuştur.[57] Zira verilerin korunmasına yönelik endişelerin temelinde yatan kişisel verilerin kötüye kullanılması, yanlış ellerde kullanılması, çalınması veya manipüle edilmesi risklerine karşı bir savunma geliştirilmesi zorunlu hale gelmiştir. Nitekim gizlilik, içerisinde oldukça çeşitli beklentiler ve anlamlar barındıran bir konudur. Kişilerin gizlilik ile ilgili genel beklentisi, davranışının izlenmeye, takip edilmeye veya kaydedilmeye kişinin izni olmadan tabi tutulmayacağını ve ayrıca açıkladıkları bilgilerin gizli tutulacağını ve beklenmedik veya kötü amaçlı şekillerde kullanılmayacağını bilmeleri yönündedir. Gizlilik tanımlarında ifade edilen temel özellik ise bir kişinin kendisi hakkında bilgi edinme, kullanma, depolama, iletim ve yayılması üzerindeki kontrol kabiliyetidir. Kişinin kendisi ile alakalı verilere ilişkin kontrol yeteneği ayrıca "bilgi öz-determinasyonu" olarak ifade edilmiş olup kişisel bilgilerin kontrolü, özgürlük duygusu için de özellikle önemlidir.[58]

---

56 Akkurt, "Kişisel Veri Kavramının", 30.

57 Küzeci, *Kişisel Verilerin Korunması*, 46.

58 Vanmala Hiranandani, "Privacy and Security in the Digital Age: Contemporary Challenges and Future Directions", *The International Journal of Human Rights*, 15/7 (2011): 1091-1106, 1092.

Kişisel verilerin korunması kavramının hukuk sistemlerindeki yeniliği bir olgu olmakla birlikte veri koruma hukukunun temelleri görece eski zamanlara uzanmaktadır. 18. yüzyılın sonlarında, bir kişinin faaliyetlerinin sıkı şekilde takip edilmesi manasını taşıyabilecek biçimde ve geleneksel mahiyette izleme faaliyetlerinin yürütülmesi "gözetim" faaliyeti olarak adlandırılmış; bu gözetim işleri, kişilerin eylemlerinin veya iletişiminin sistematik şekilde araştırılması ve izlenmesi olarak kabul edilmiştir.[59] Kişilere ait verilerin bilinmesi, kayıt altına alınması ve işlenmesine ihtiyaç duyan toplumlar da bunun için araçlar geliştirmişlerdir.[60] 1890 yılında Harward Hukuk İncelemesi'nde (Harvard Law Review) yayımlanan [61] ve Amerika hukuk tarihinin en etkili makalelerinden biri kabul edilen[62] ve "mahremiyet hakkı" kavramını literatüre kazandıran[63] makalede gazete ve fotoğraf makinesi kullanımının gizlilik üzerine etkilerinin tartışılmaya başlanması ile gözetim faaliyetlerinin etkileri üzerine üretken çözümlere ulaşılması için çalışılmıştır. Kişisel verilerin korunmasının bir hak olarak düzenlenmesinin gerekliliğinin temelinde de kişisel verilerin gözetime tabi tutulması için geliştirilen gözetim teknolojilerine ilişkin gelişmelerin yarattığı etkiler yatmaktadır.[64] 1960'lı yıllara gelindiğinde mahremiyet ve teknolojinin savaşı, pilli mikrofonlar, portatif kayıt cihazları, tek bir hat ile kullanılmasına imkan sağlayan telefonlar ve yüksek çözünürlüklü kameralar gibi verilerin kayıt altına alınmasına imkan tanıyan cihazların ortaya çıkması ile mahremiyete yapılan saldırılar artmış ve saldırıların etkileri güçlenmiştir.[65] Dolayısıyla otomatik veri işleme teknolojilerinin gelişmesi ile ve kişisel verilerin bilgisayarla işlenmesinin etkileri nedeniyle modern anlamda kişisel verilerin korunması hakkı, ilk defa 1960'lı yıllarda Amerika'da ele alınmaya başlanmış; gizlilik

https://doi.org/ 10.1080/13642987.2010.493360, (E. T. 07.05.2023), https://www.tandfonline.com/loi/fjhr20

59 Dülger, *Kişisel Verilerin Korunması*, 66-67.

60 Aktaran Dülger, *Kişisel Verilerin Korunması,* 68.

61 Louis Brandeis ve Samuel Warren, "The Right to Privacy", *Harvard Law Review*, 4/5 (1890), 193-220. (E.T. 11.12.2023), https://www.jstor.org/ stable/1321160

62 "Harward Law Review", (E.T. 11.12.2023), https://faculty.uml.edu/sgallagher/Harvard-__law_review.htm

63 Oya Başar ve Sezen Kama Işık, "Dördüncü Kuşak Haklar ve Bilişim Teknolojilerinin Doğuşunda Mahremiyet Kavramına Karşılaştırmalı Bir Bakış", *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, 25/2 (Aralık 2019): 602,623. 619. DOI: 10.33433/maruhad.667577

64 Dülger, *Kişisel Verilerin Korunması,* 66. Aynı yönde bkz: Eliz Küzeci, *Kişisel Verilerim Korunması*, (İstanbul: On İki Levha Yayıncılık, Mayıs 2020), 20-24.

65 Başar ve Kama Işık, "Dördüncü Kuşak Haklar", 610.

ile ilgili tehditlerin tartışılmaya başlanması üzerine[66] Avrupa'da da 1960'lı yılların sonunda müzakere edilmeye geçilmiştir.[67]

Avrupa düzeyinde veri koruma ihtiyacı ilk kez, Avrupa Konseyi'nin Danışma Meclisi tarafından gündeme getirilmiştir. 31 Ocak 1968'de Meclis, modern bilimsel ve teknolojik gelişmelerin bireylerin gizliliği üzerindeki etkileri konusunda münazara yapmış, bireysel gizlilik için risk olan yahut olabilecek çeşitli tehditleri masaya yatırmıştır. Özellikle, bilgisayar veri bankalarının sunduğu sorunlar ele alınmış olup bu veri bankalarının, devlet organlarının ve özel firmaların bireyin kişiliği hakkında ayrıntılı bir resim oluşturmasına olanak sağladığı belirtilmiştir. Bu nedenle, bir veri bankasının işletimi için hangi kuralların geçerli olduğunu ve nelerin kabul edilemez olduğunu belirlemek için kuralların konulmasının gerektiği ifade edilmiştir.[68] Bu nedenle bireysel gizliliğin korunması konusunda ve bizatihi veri bankalarında kaydedilen bilgilerin doğru, güncel ve ilgili olmasını sağlamak için önlemler alınması ve bu doğrultuda bilginin elde edildiği amaç dışında kullanımının kısıtlanması, yetkisiz kişilerin erişiminin engellenmesi için bilgisayarlara elektronik güvenlik sistemlerinin kurulması, işletme personelinin mesleki sır hükümlerine bağlı olması ve son olarak, bireylerin kendileri hakkında kaydedilen bilgileri genel olarak bilmeye hakları olacağına ilişkin yasal düzenlemelerin yapılması için adımlar atılmıştır.[69]

---

66 Lee A. Bygrave, "Privacy and Data Protection in an International Perspective*", Stockholm Institute for Scandinavian Law*, 2(010):166-198. 166-170,167. (E.T. 17.05.2023), https:// scandinavianlaw.se/pdf/56-8.pdf; Doğan, *Karşılaştırmalı Hukukta Anayasal,* 44.

67 Akgül, *Danıştay ve Avrupa İnsan*, 260. "Veri güvenliği kavramı da ilk kez 60-70li yıllarda Alman Hukuku'nda kullanılmıştır." aktaran Aybike Tunç, *Bulut Bilişim Sözleşmeleri*, (İstanbul: On İki Levha Yayıncılık, Kasım 2020), 105.

68 Avrupa Konseyi Danışma Meclisi, ulusal yasaların ve her ne kadar özel hayatın gizliliğini koruma altına alıyor olsa da Avrupa İnsan Hakları Sözlemesi'nin (AİHS) 8. maddesinin böyle bir belirlemenin yapılması için yeterli korumayı sağlayamadığını savunmuştur. Savunmanın gerekçesi ise AİHS'in 8. maddesi, 1950 yılında kabul edilen ve bilgisayarların insan haklarına yönelik tehdidin henüz fark edilmediği bir belgede yer aldığı ve ek olarak, 8. maddenin sadece kamu sektörünü kapsadığı çünkü mevcut veri bankalarının önemli bir kısmı özel firmalar tarafından işletilmekte olduğu olarak ifade edilmiştir. Bu tartışmanın sonucunda tartışılan sorunlar göz önünde bulundurularak, İnsan Hakları Sözleşmesi'nin 8. maddesinin ve üye devletlerin mevzuatlarının bireysel gizliliği yeterince koruyup korumadığı hususu ile bireysel gizlilik ve bilgisayarlar konusundaki sorunu incelemek için hazırlanan rapordan çıkan sonuç, ulusal ve Avrupa düzeyindeki mevcut yasaların bireysel gizliliği yeterince korumadığı olmuştur. Bkz: A.C. Evans, "European Data Protection Law." *The American Journal of Comparative Law*, 29/ 4 (1981): 571–582. (E.T. 12.05.2023) https://doi.org/ 10.2307/839754.

69 Evans, "European Data Protection Law." 82.

1970 yılında Almanya'nın Hessen eyaletinde kabul edilen "Veri Koruma Kanunu" isimli bölgesel kanun, bu alanda yapılan ilk düzenleme olmuştur.[70] Hessen Eyaleti'nde kabul edilen bu kanuni düzenlemeyi 1973 yılında İsveç'te kabul edilen "Veri Koruma Kanunu", 1977'de Almanya'da "Federal Almanya Veri Koruma Kanunu", 1978'te Fransa'da "Elektronik Veri İşlenmesi, Veriler ve Özgürlük Haklarına İlişkin Kanun"[71] , 1978'te Avusturya'da "Federal Kişisel Verilerin Korunması Kanunu", 1992'de İsviçre'de "Federal Veri Koruma Kanunu", 1998'te İngiltere'de "Veri Koruma Kanunu" takip etmiştir.[72] Amerika'da yapılan ilk düzenleme ise 1974 tarihli Özel Yaşamı Koruma Kanunu (Privacy Act) olmuştur.[73] Kişisel verilerin korunması hakkına yönelik yasal düzenlemelerin yapılması ile birlikte birçok ülkede zamanla pek çok düzenleme hayata geçirilmiştir. Kişisel verilerin korunması ihtiyacına yönelik uluslararası ve ulusal mevzuat ise aşağıdaki başlıklarda incelenmektedir.

1980'li yıllarla birlikte insan haklarının gelişmesi için devletler, ulusal mevzuatları ile tek taraflı kişisel verileri koruma düşüncesi yerine daha genele hitap eden kapsamlı uluslararası standarda sahip temel norm niteliğinde mevzuat oluşturmaya başlamışlardır.[74] Bu alanda kişisel verilerin uluslararası çapta daha nitelikli korunması ihtiyacına yönelik ilk uluslararası belge 28 Ocak 1981 tarihli "Avrupa Konseyi 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında bireylerin Korunması Sözleşmesi" olmuştur. Türkiye bu sözleşmeyi imzalayan ilk ülkelerden biri olsa da iç hukukta kişisel verilerin korunmasına ihtiyacı yönünde yasal bir düzenleme hayata geçirilmemiştir.[75]

Uluslararası düzeyde kişisel verilerin korunması için yapılan yasal düzenlemeler ile birlikte Türk hukukunda da kişisel verilerin korunması ihtiyacına yönelik harekete geçmek gerekmiştir. Avrupa Komisyonu tarafından 2008 yılında yayımlanan "Türkiye İlerleme Raporu"nda Türk hukuku açısından kişisel verilerin korunmasına yönelik kanuni düzenlemelerin hayata geçirilmesine ilişkin ifadelere yer verilmiştir: "*Özel hayat ve aile hayatına saygı ile özellikle kişisel verilerin korunması hakkına ilişkin olarak, Türkiye'nin*

70 Bilir, "Kişisel Verilerin Korunması", 314.
71 Akgül, *Danıştay ve Avrupa İnsan*, 163.
72 Çekin, *Avrupa Birliği Hukukuyla*, 6.
73 Şimşek, *Anayasa Hukukunda Kişisel*, 7.
74 Doğan, *Karşılaştırmalı Hukukta Anayasal*, 47.
75 Doğan, *Karşılaştırmalı Hukukta Anayasal*, 46.

mevzuatını veri korunması müktesebatı, özellikle de 95/46/EC sayılı Direktifle uyumlaştırması ve bu kapsamda tam bağımsız bir veri koruma denetim makamı tesis etmesi gerekmektedir. Türkiye'nin ayrıca hem Kişisel Verilerin Otomatik İşlem Sürecinde Korunması Hakkında Avrupa Konseyi Sözleşmesi'ni (CETS No:108), hem de bu sözleşmenin Denetleyici Makamlar ve Sınırötesi Veri Akışına İlişkin Ek Protokolü'nü (CETS No: 181) onaylaması gerekmektedir".[76] Yine Devlet Denetleme Kurulu'nun 2013 tarihinde yayımladığı raporda kişisel verilerin korunması ihtiyacı şu şekilde ifade edilmiştir:[77]

"*Bilişim teknolojilerindeki gelişmeler sonucunda;*

• Geleneksel yöntemlerle mümkün olmayan çok sayıda verinin toplanabilmesi,

• Daha önce dağınık yapılarca toplanan ve birbirinden ilişkisiz şekilde tutulan pek çok verinin merkezi olarak bir araya getirilmesi,

• Verilerin ileri teknolojik imkânlarla ve veri eşleştirme (data matching) ve veri madenciliği (data mining) gibi tekniklerle analize tabi tutulmak suretiyle, veriden yeni veriler üretme kapasitesinin artması,

• Verilere erişim, paylaşım ve transferin kolaylaşması ve maliyetinin düşmesi,

• Kişisel verilerin ticari işletmeler için kıymetli bir varlık ve ticari meta niteliği kazanması neticesinde özel sektör unsurlarınca yaratılan risklerin daha yaygın ve önemli boyutlara ulaşmış olması,

• Yabancı ülke istihbarat birimlerinin, terör ve suç örgütlerinin kişisel verileri ele geçirme veya bu sistemlere zarar verme yönündeki faaliyet ve saldırılarının artması,

• Banka ve kredi kartı dolandırıcılıkları başta olmak üzere, kişisel verileri hedef alan veya bunlar kullanılmak suretiyle işlenen suç olaylarının artması gibi hususlar kişilerin

---

76 Avrupa Komisyonu, 5 Kasım 2008 Sec (2008) 2699 Türkiye 2008 İlerleme Raporu (Com(2008) 674), 70, (E.T. 20.05.2023), https://www.ab.gov.tr/files/AB_Iliskileri/AdaylikSureci-/IlerlemeRaporlari/turkiye_ ilerleme_rap_2008.pdf

77 T.C. Cumhurbaşkanlığı Devlet Denetleme Kurulu, "Kişisel Verilerin Korunmasına İlişkin Ulusal ve Uluslararası Durum Değerlendirmesi ile Bilgi Güvenliği ve Kişisel Verilerin Korunması Kapsamında Gerçekleştirilen Denetim Çalışmaları", 27 / 11/ 2013, 2013 / 3, 778-779, (E.T. 20.05.2023), https://www. memurlar.net/ common/news/documents/439122/ddk56.pdf

mahremiyet alanını önemli derecede daraltmış ve kişisel verilerin korunması ihtiyacını en üst noktaya taşımıştır".

Bahsi geçen tüm gelişmeler karşısında Türk hukuk sisteminde de kişisel verilerin korunması hakkının anayasal teminata sahip olması zorunluluk haline gelmiş; kişisel verilerin korunması ve buna bağlı olarak uyulması gereken usul ve esasları düzenleyen ikincil düzenlemelerin hayata geçirilmesi amacıyla yasal düzenlemeler yapılmıştır.

1.1.4.2. Veri Mahremiyeti (Data Privacy)

Kişisel veri mahremiyeti, bireylerin kişisel verilerinin gizliliğini, güvenliğini ve kontrolünü ilgilendirir. Günümüzde, teknolojik gelişmeler ve dijitalleşmenin hızla ilerlemesiyle birlikte ve özellikle internet üzerinde yapılan işlemler, sosyal medya kullanımı, çevrimiçi alışveriş ve diğer dijital etkinlikler sonucunda birçok kişisel veri toplanmakta ve işlenmektedir. Bu veriler, bireylerin kimlikleri, sağlık bilgileri, finansal durumları, coğrafi konumları ve diğer özel bilgilerini içerebilmektedir. Dolayısıyla, kişisel veri mahremiyetinin korunması, bireylerin güvenliğini ve temel haklarını sağlamak açısından kritik bir öneme sahiptir.

Mahremiyet kavramının anlamına dair birçok görüş[78] olmakla birlikte kavramın, "başkaları tarafından görülmeksizin ve duyulmaksızın yalnız kalabilme hali", "kamuoyunun dikkatinde olmadan özgür olabilme hali", "gizlilik", "yalnız bırakılma hakkı; "bir kimsenin kendisine veya grubuna ulaşma gayreti üzerindeki seçici kontrolü", "özel hayatın gizliliği" ve benzeri ifadelerle tanımının yapıldığı görülmektedir.[79] Mahremiyet, bireylerin istenmeyen unsurlardan ayrı olduğu fiziksel alan arzusuyla birlikte, kişisel bilgilerini ifşa etme zamanını ve şeklini kontrol etme yeteneğini; veri mahremiyeti ise kişisel verilerin toplanması, saklanması, işlenmesi ve iletilmesinin nasıl kontrol edileceğini ifade eder.[80] Aynı zamanda veri mahremiyeti, veri sorumluları tarafından toplanan verilerin hukuka ve etik kurallara riayet edilerek işlenmesiyle veri

78 Mahremiyet kavramına ilişkin Avrupa ve Amerika yaklaşımlarına ilişkin detaylı inceleme için bkz: Başar ve Kama Işık, "Dördüncü Kuşak Haklar", 609-619.

79 Sultanlı, "Anayasal Bir Hak", 25.

80 Ayşe Nur Akıncı, "Büyük Veri Uygulamalarında Kişisel Veri Mahremiyeti", (T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı Uzmanlık Tezi, 2019), 58, (E.T. 13.05.2023), http://www.bilgitoplumu.gov.tr/wp-content/uploads/2019/04/ayse-nur-akinci-tez-WEB.pdf.

öznelerinin koruma altına alınması olarak da ifade edilebilir.[81] Hukuki açıdan bir hak olarak bakıldığında ise mahremiyet; vücut, veri ve haberleşme gizliliği üzerine odaklanmakta, kişiye ya da kişilere ait bilgilerin hangi koşullarda, ne kadarının ne zaman başkalarına aktarılacağına yönelik hakkı oluşturmaktadır.[82]

Avrupa hukuk sistemlerinde, mahremiyete hizmet eden araçlar genellikle "veri koruması (*data protection*)" terimiyle tanımlanır. Avrupa dışındaki hukuk sistemlerinde ise tercih edilen terimler genellikle "gizlilik *(privacy*)", "veri mahremiyeti (*data privacy*)" veya "bilgi gizliliği (*information privacy*)" korumasıdır.[83] Ancak Anglo-Sakson veri gizliliği kanunları ve Avrupa veri koruma kanunları arasında karşılaştırma yapılırken veri gizliliği ve veri koruması terimleri birbirinin yerine kullanılmaktadır.[84] Dolayısıyla "veri koruması veya güvenliği (*data protection*)" ve "gizlilik yahut mahremiyet (*privacy*)" kavramlarının tamamen eşanlamlı olduğunu varsaymak yanlış olur.[85] Bu kavramlar yakın ilişkili olsalar da en azından Avrupa hukuk sistemleri açısından bakıldığında aynı anlama gelmezler. "Veri koruması" genellikle, gizlilik korumasından daha geniş bir çıkarlar dizisine hizmet eden bir dizi norm için kullanılır. Bu normlar, gizlilik korumasıyla ilgili olduğunda ise yalnızca gizliliğin bilgi boyutuna odaklanmaktadır.[86] Başka bir ifade ile veri koruması gerçek kişilerin verilerinin korunmasını ifade etmekle birlikte odak noktası kişinin kendisi değil, kişiye ilişkin verilerdir.[87] Bu nedenle mahremiyet hususu Norveç, İsveç, Almanya örneğinde olduğu gibi kimi hukuk sistemlerinde kişilik hakları üzerinden tartışılmaktadır. Terminolojik farklılıklara rağmen bu tanımlamaların yer aldığı düzenlemelerin ortak noktası özellikle kişilerin gizlilik ve ilgili sair çıkarlarını korumaya yönelik olarak tasarlanmış olmasıdır.[88]

Veri mahremiyeti, veri sahiplerinin mahremiyeti ile veri paylaşımının taraflara sağlayacağı yarar arasındaki en makul dengeyi oluşturmaya çalışan zor bir sorunu da içinde barındırır. Verilerin toplanması ve paylaşılması sürecinde kontrolün verinin

---

81 Yılmaz Vural, "Veri Mahremiyeti: Saldırılar, Korunma ve Yeni Bir Çözüm Önerisi", *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, 4/2 (2018):21-34, 22, (E.T. 13.05.2023), https://dergipark.org.tr/tr/ download /issue-file/18543

82 Doğan, "Dijital Veri Uygulamalarında", 132.

83 Bygrave, "Privacy and Data", 166-170,180.

84 Determann, *Kişisel Verilerin Korunması* 19.

85 Bygrave, "Privacy and Data", 166; Determann, *Kişisel Verilerin Korunması*, 19.

86 Bygrave, "Privacy and Data", 167.

87 Determann, *Kişisel Verilerin Korunması*, 19.

88 Bygrave, "Privacy and Data", 166-170,180.

öznesinde kalması, veri mahremiyeti açısından mühim bir gerekliliktir. Bu süreçte verilerin hangi maksatla işleneceği, kimlerle paylaşılacağı, nerelere aktarılacağı şeffaf ve denetime elverişli derecede veri öznesi tarafından kontrol edilebilmelidir.[89] Zira veri mahremiyeti ya da gizliliği *(data privacy)* olmadan veri korumasına sahip olunabilse de veri koruması olmadan veri mahremiyetinin temini mümkün değildir. Çünkü veri güvenliği, verinin harici saldırganlar ve kötü niyetli içeridekiler tarafından tehlikeye atılmasına karşı korunmasını ilgilendirirken, veri mahremiyeti verinin nasıl toplandığını, paylaşıldığını ve kullanıldığını düzenlemektedir.[90] Başka bir ifade ile veri mahremiyetinin, veri güvenliğini de içine alan daha üst kavram olduğunu ifade etmek mümkündür. Veri mahremiyetinin odak noktası verilerin güvenli olarak saklanması ile birlikte verilerin elde edilmesi, yayılması ve kullanılması iken veri güvenliği daha çok verilerin güvenli olarak saklanmasıyla ilgilenir.[91]

Dijital teknoloji modern endüstriyel toplumların işleyişi için merkez haline geldikçe, geleneksel gizlilik kavramlarının parçalanması veri mahremiyetinin önemini ön plana çıkarmıştır. Lisanslar, araç ve seçmen kayıt listeleri, sağlık kayıtları ve nüfus kayıtları gibi çeşitli kaynaklardan elde edilen bilgileri satan yeni bir bilgisayar tabanlı, veri-toplama endüstrisi gelişmiştir.[92] Veri ekonomisinin yükselişiyle birlikte de veri işleyen gerçek veya tüzel kişiler veri toplama, paylaşma ve kullanma konusunda büyük bir öneme sahip olmuştur. Bir bireyin kendi alanında güvenli bir şekilde var olması ve kapalı kapılar ardında serbestçe düşüncelerini ifade etmesi, demokratik bir toplumda yaşam için önemlidir. Zira veri mahremiyeti, gizlilik hakkının güvencesidir.[93] Bu nedenle veri mahremiyetini düzenlemek için oluşturulacak en iyi çerçeve, kişilerin hangi bilgilerinin, neden, ne zaman ve kiminle paylaşıldığı ve nasıl kullanılacağını teftiş etmesinin sağlanmasıdır.[94]

---

89 Vural, "Veri Mahremiyeti: Saldırılar", 21-34.

90 Franca Colozzo, "Data Privacy and Its Identification." Dr. Arch. Franca Colozzo, 3 (2021), (E.T. 18.05.2023), https://www.academia.edu/100506335/Data_Privacy_and_its_identification

91 Aktaran Onur Selek, *Kişisel Verilerin Korunması ve Verileri Yok Etmeme Suçu (TCK m.138*), (İstanbul: On İki Levha Yayıncılık, 2021). 86.

92 Hiranandi, "Privacy and Security", 1094.

93 Colozzo, "Data Privacy and,", 5.

94 Dülger, *Kişisel Verilerin Korunması,* 24.

1.1.4.3. Veri Güvenliği İhlalleri (Data Breaches)

Kişisel verilerin korunması ile veri güvenliği arasında oldukça sıkı bir bağ vardır. Zira veri güvenliğinin sağlanması ile kişisel verilerin korunması sağlanmakta olup veri güvenliğine dair yükümlülüklerin belirlenmesi ve bu yükümlülüklere riayet edilmesi son derece önemlidir.[95] Çünkü veri güvenliğine ilişkin düzenlemeler ilgili kişilerin, kişisel bilgilere yetkisiz erişimi halinde ortaya çıkabilecek zararlardan korunmasını hedefler.[96] Bu hedef doğrultusunda da kişisel verilerin korunması sürecinde ortaya çıkabilecek risklere karşı her türlü teknik ve idari tedbirin alınması amacını güden ilke ise veri güvenliği ilkesi olarak tanımlanmaktadır. Bununla birlikte veri güvenliği ile kişisel verilerin korunması kavramlarını da karıştırmamak gerekir. Zira yukarıdaki başlıklarda da farklı perspektiflerden ifade edildiği üzere veri güvenliği ilkesi dar anlamda başlıca kişisel verilerin kendisinin korunmasını hedefleyen bir ilkedir. Kişisel verilerin korunması ise çok daha geniş bir kavram olup kişilerin temel hakları arasında yer almaktadır. Bu nedenle veri güvenliği ilkesi, kişisel verilerin korunması hakkının hukuki güvenliğinin sağlanmasının bir aracı sayılabilir.[97] Başka bir ifade ile kişisel verilerin güvenliği hakkı esasen temel hak ve özgürlüklerin teminat altına alınmasını sağlayan bir haktır.[98]

Mahremiyet bilincinin eksik olması ve yeterli önlemlerin alınmaması, mahremiyet odaklı birçok saldırının gerçekleşmesine neden olmaktadır. Bu tür veri ihlalleri, bireylerin ayrımcılığa veya mağduriyete uğramasından, toplumları ve ülkeleri hedef alan geniş çaplı tehditlere kadar çeşitli etkiler yaratabilir. Bu gibi mahremiyet odaklı ihlallerin en aza indirilmesi amacıyla mevcut saldırılar ve güvenlik eksikleri analiz edilerek, veri gizliliğini korumak için yeni yöntemler ve modeller geliştirilmesi gerekliliği doğmuştur. Kişisel verilerin yasalara uyumlu biçimde işlenmesi ve mahremiyetin korunması adına

---

95 Metin Turan, *Karşılaştırmalı Hukukta Kişisel Verilerin Korunması*, (Ankara: Seçkin Yayıncılık, 2021), 214, 215.

96 Determann, *Kişisel Verilerin Korunması*, 21.

97 Sedat Erdem Aydın. *AİHM İçtihatların Bağlamında Kişisel Verilerin Kaydedilmesi Suçu*. İstanbul: On İki Levha Yayıncılık, 2015, 121; Binnur Gürses, "Sosyal Paylaşım Ağlarında Kişisel Verilerin Güvenliği; Sorunlar ve Çözüm Önerileri", (İdari Uzmanlık Tezi, Bilgi Teknolojileri ve İletişim Kurumu, Ağustos 2013), 33.

98 Mehmet Şükrü Gündüz, *Uluslararası İnsan Hakları Açısından Kişisel Veri Güvenliği*, (Ankara: Adalet Yayınevi, 2022), 84.

teknik ve idari çalışmalar yürütülmesi, kişisel verilerin güvenliğinin sağlanması açısından büyük önem taşımaktadır.[99].

Türk hukukunda kişisel veri ihlalinin ne olduğunu konusunda açık bir tanıma yer verilmemiştir. Kişisel verilerin korunması konusunda temel kaynak olarak sayılabilecek Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) "kişisel veri ihlali" tanımını 4. maddesinde[100] "*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 ihlali"* şeklinde yapmıştır. KVKK'nın veri güvenliğini düzenleyen 12. maddesi kapsamında ise veri sorumlusunun veri işleme faaliyetlerinde gerekli güvenliği sağlamakla yükümlü olduğu veri sorumlusu tarafından işlenen kişisel verilerin hukuka aykırı şekilde üçüncü kişilerce ele geçirilmesi durumunda, veri güvenliği yükümlülüğünün ihlal edilmiş sayılacağı hüküm altına alınmıştır.[101] Kanun lafzından, veri ihlali durumu için kişisel verilerin başkaları tarafından elde edilmesi gerekliliği anlaşılmaktadır. Yani, kişisel verilerin izinsiz şekilde ele geçirilmesi veya yetkisiz kişilerin eline geçmesi durumu veri ihlali olarak kabul edilebilir. Düzenlemenin bu haliyle kişisel veri ihlalini GDPR'a göre oldukça dar yorumladığı da söylenebilir.[102]

1.2. Kişisel Verilerin Korunmasına İlişkin Mevzuat

Kişisel verilerin korunması alanındaki ulusal ve uluslararası düzenlemelerin başlıca esaslarını; kişisel verilerin korunması hakkının anayasal teminata kavuşturulması, kişisel verilerin temel ilkelere uygun olarak işlenmesi, kişisel verisi işlenen kişilerin haklarının yasal zeminde belirlenmesi, kişisel veri kütüğü sahiplerinin görev ve mesuliyetleri ile kişisel verilerin korunması konusunda etkin rol alacak bağımsız, tarafsız ve teknik olarak yeterli veri koruma otoritesinin hayata geçirilmesi oluşturmaktadır.[103]

---

99 Vural, "Veri Mahremiyeti: Saldırılar,", 22.

100 "Art. 4 GDPR, "Definitions".

101 Nur Sena Sevindi ve Muhammet Emin Ordu, "AB ve Türk Hukukunda Veri İhlalinin Tespiti ve Bildirim Süresinin Karşılaştırmalı Değerlendirmesi", *Kişisel Verileri Koruma Dergisi,* 5/1 (2023): 12-22, 13. (E.T. 01.08.2023), https://dergipark.org.tr/tr/download/article-file/3116868

102 Sevindi ve Ordu, "AB ve Türk Hukukunda", 14.

103 Aynı yönde bkz: Bilir, "6698 Sayılı Kişisel", 308.

1.2.1. Uluslararası Hukukta Kişisel Verilerin Korunması

1.2.1.1. OECD Düzenlemeleri

Ekonomik İş Birliği ve Kalkınma Teşkilatı (OECD), 23.09.1980 tarihinde Özel Yaşamın Gizliliğinin ve Sınır Ötesi Kişisel Veri Dolaşımının Korunmasına İlişkin Rehber İlkeler'i (OECD Rehber İlkeleri) kabul ederek kişisel verilerin korunması bahsini milletlerarası alana taşıyan ilk kuruluş olmuştur.[104] Hukuki açıdan tavsiye kararı niteliğinde olan OECD Rehber İlkeleri, kişisel verilerin korunmasına dair asgari gereklilikleri göstermektedir.[105] Yumuşak hukuk kuralı (soft law) olarak ifade edilen bu ilkeler her ne kadar kâğıt üzerinde ve doğrudan bir bağlayıcılığı olmasa da bir çok ülke tarafından kabul edildiğinde ilgili alanda temel referans kaynağı olarak hizmet etmektedir.[106]

Rehber ilkeler kişisel verilerin korunmasına yönelik politikaların oluşturulması ve kanuni düzenlemelerin hayata geçirilmesinde kıstas olarak kullanılan sekiz temel ilkeden oluşur:

"(1) Veri toplamanın sınırlı olması ilkesi,

(2) Veri niteliği ilkesi,

(3) Amacın belirli olması gerektiği ilkesi,

(4) Kullanımın sınırlanması ilkesi,

(5) Veri güvenliği ilkesi,

(6) Açıklık ilkesi,

(7) Bireyin katılımı ilkesi,

(8) Hesap verme zorunluluğu ilkesi."

---

104 Dülger, *Kişisel Verilerin Korunması,* 86; Küzeci, *Kişisel Verilerin Korunması,* 129.
105 Küzeci, *Kişisel Verilerin Korunması*,130.
106 Murat Volkan Dülger, "Avrupa Birliği Genel Veri Koruma Tüzüğü Bağlamında Kişisel Verilerin Korunması", *Yaşar Hukuk Dergisi*, 1/2 (2019): 71-174. 74.

1980 yılında belirlenen bu ilkeler değişen teknoloji, piyasa ve kullanıcı davranışları ile dijital kimliklerin giderek artan önemi nedeniyle 2013 yılında yeniden düzenlenmiştir.[107] Güncellenen ilkelerde iki ana tema göze çarpmaktadır. İlk olarak, gizlilik korumasının pratik uygulamasına odaklanılarak, risk yönetimi temelli bir yaklaşım benimsenmiştir. İkinci olarak, gizliliğin küresel boyutunu ele almak için daha fazla çaba gösterme gerekliliği vurgulanmıştır. Bu yeni ilkelerde ayrıca bazı yeni kavramlar tanıtılmıştır. Bunlar, etkili yasaların yanı sıra, modern çağda gizliliğin stratejik öneminin anlaşılması için hükümetin en üst düzeyinde koordine edilen geniş kapsamlı bir milli stratejinin gerekliliğini vurgulayan "Ulusal Gizlilik Stratejileri", gizlilik korumasının uygulanmasında temel operasyonel mekanizmalar olarak hizmet veren "Gizlilik Yönetim Programları" ve kişisel verileri etkileyen güvenlik ihlalleri durumunda bildirimleri kapsayan "Veri Güvenliği İhlal Bildirimi" gibi kavramlardır.[108]

1.2.1.2. Avrupa Konseyi Düzenlemeleri

Kişisel verilerin korunması hakkına yönelik en ayrıntılı düzenlemeler Avrupa Konseyi tarafından yapılmıştır.[109] "108 No'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi" kişisel verilerin korunması alanında bağlayıcılığı olan ilk milletlerarası sözleşmedir.[110] Türkiye, 28 Ocak 1981 tarihinde bu sözleşmeyi imzaladığında sözleşmeyi kabul eden ilk ülkelerden biri olmuştur. Kabul edilen Sözleşme, 17 Mart 2016 tarihinde 29656 sayılı Resmî Gazete'de yayımlanarak iç hukuka dahil olmuştur. Sözleşme, günümüzde "108 sayılı Sözleşme" olarak da bilinmektedir. Sözleşme'nin başlıca amacı her üye ülkede, uyruğu veya ikametgâhı fark etmeksizin gerçek kişilerin temel hak ve özgürlüklerini, özellikle de kendileri ile ilgili kişisel özellikteki verilerin otomatik yollarla işleme tâbi tutulması halinde özel hayat haklarını teminat altına almaktır.[111] 108 sayılı Sözleşme ile bireylerin kişisel verilerinin korunması ve gizliliğin sağlanması için bir çerçeve sunulmuş, her üye ülkenin bu hakları güvence altına alması amaçlanmıştır. Aynı zamanda iç hukuk bakımından da

---

107 "The OECD Prıvacy Framework", 3, (E.T. 03.08.2023), https://www.oecd.org/sti/i-economy/oecd_privacy framework.pdf

108 "The OECD Prıvacy Framework", 4.

109 Dülger, *Kişisel Verilerin Korunması,* 90.

110 Dülger, *Kişisel Verilerin Korunması,* 91.

111 Kişisel Verileri Koruma Kurumu, "Kişisel Verilerin Korunması Alanında Uluslararası ve Ulusal Düzenlemeler", (E.T. 03.08.2023), https://www.kvkk.gov.tr/Icerik/4183/Kisisel-Verilerin-Korunmasi-Alaninda-Uluslararasi-ve-Ulusal-Duzenlemeler

Sözleşmenin, Türkiye'nin sınır ötesi organize suçlar hususunda Avrupa Bölgesel Savcılık Teşkilatı şeklinde ifade edilen "Euro Justice" ile operasyonel iş birliği bağlamında katkıda bulunacağı değerlendirilmektedir.[112]

2018 yılında 108 sayılı Sözleşme güncellenerek *"Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması İlişkin Sözleşmede Değişiklik Yapılmasına Daire Protokol (108+)"*[113] kabul edilmiştir.[114] Bu protokol ile 108 sayılı Sözleşmedeki eksikler ortadan kaldırılmaya çalışılmıştır. Zira Sözleşme ile veri işleme faaliyetleri düzenlenmiş olsa bile faaliyetleri denetleyecek ve kontrol edecek bağımsız bir kuruluş öngörülmediğinden 108+'de denetleyici ve yetkili makamlar oluşturulmuş, sınıraşan veri akışına ilişkin düzenlemeler ortaya konmuştur.[115]

Avrupa Konseyi bünyesindeki düzenlemeler arasında yer alan Avrupa İnsan Hakları Sözleşmesi (AİHS) ise 1950'li yıllardan bu yana insan hakları alanında en önemli kaynaklardan biridir. AİHS'de kişisel verilerin korunması müstakil bir hak olarak düzenlenmese de 8. maddede yer alan "özel ve aile yaşamına saygı hakkı" kapsamında korumaya tabi tutulmaktadır. Aynı şekilde Avrupa İnsan Hakları Mahkemesi kararlarında da kişisel verilerin korunmasına ilişkin ilkelerin de çoğunlukla bu madde kapsamında değerlendirildiği görülmektedir.[116]

1.2.1.3. Avrupa Birliği Düzenlemeleri

Avrupa Birliği (AB), oluşumdaki temel amaçlarının yanı sıra kişisel verilerin korunması mecburiyetinin temel hak ve özgürlüklere dayandığını kabul etmiştir. Bu nedenle kişisel verilerin korunması hususunun demokratik ülkelerin kalkınmasında önemli rol oynamasından ötürü kanuni düzenleme için harekete geçmiştir. Bu doğrultuda kişisel verilerin uluslararası ilişkilerin ilerlemesinde etkili bir rolünün bulunması, vatandaşların veri güvenliğinin sağlanmasında pay sahibi olması ve kişisel verilerin korunması

---

112 Dışişleri Komisyonu Raporu: https://www.tbmm.gov.tr/sirasayi/donem26/yil01/ss28.pdf 'den aktaran Tahir Erdem, "Kişisel Verilerin Korunması Konusunda Son Gelişmeler", *Vergi Sorunları Dergisi,* 39/332 (2016), 97-115, 99. (E.T. 24.09.2023), www.idealonline.com.tr

113 "108+ Türkiye'de henüz yürürlüğe girmemiştir." bkz: Dülger, "Avrupa Birliği Genel", 78.

114 Dülger, "Avrupa Birliği Genel", 77.

115 Dülger, *Kişisel Verilerin Korunması*, 93.

116 Küzeci, *Kişisel Verilerin Korunması,* 151-164.

hakkının temel insan hakları içerisinde yer edinmesi için AB ve Birliğe üye ülkeler için düzenlemeler yapılmıştır.[117]

Kişisel verileri koruma hakkını da kapsayan özel hayatın korunması hakkı, 1950 Avrupa İnsan Hakları Sözleşmesi'nin bir parçasıdır. Sözleşme'de "*Herkes, özel ve aile hayatına, konutuna ve yazışmalarına saygı gösterilmesi hakkına sahiptir"* hükmü ile bu hak koruma altına alınmıştır. Ancak teknolojinin ilerlemesiyle birlikte Avrupa Birliği tarafından, kişisel verileri koruma adına daha spesifik ve modern koruma önlemlerini içeren müstakil düzenlemelere ihtiyaç duyulduğundan 1995 yılında Avrupa Birliği Veri Koruma Direktifi olarak ifade edilen *"95/46/EC sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi"* kabul edilmiştir. Direktif'le birlikte kişisel verilerin korunması için temel ilkeler belirlenmiş, belirlenen ilkeler veri koruma mevzuatının özünü oluşturmuştur. Buna göre meşruluk, amaç kısıtlama, şeffaflık, orantılılık, güvenlik ve kontrol ilkeleri hala güncelliğini koruyan veri koruma ilkelerinin temel taşları olmuştur.[118]

AB Veri Koruma Direktifi (95/46/EC), kişisel verilerin korunması hukukunda dünya çapında tasdik edilmiş bir çerçeve sunmuştur.[119] Bu Direktif ile kişisel verilerin kazara kaybını, yasadışı bir şekilde imha edilmesini ve verilere yetkisiz kişilerin erişimini önlemek için uygun teknik ve kurumsal tedbirlerin alınması hedeflenmiştir.[120] Ne var ki Direktif ile hedeflenen amaca ulaşılmamıştır. Zira AB Direktiflerinin AB üyesi ülkeler tarafından doğrudan uygulanamaması, Direktifte yer alan kuralların öncelikle iç hukuka uyarlanması gerekliliği nedenleriyle uygulama yeknesaklığı sağlanamamıştır.[121] Öte yandan sosyal ağlar, bulut bilişim, konum temelli hizmetler, akıllı kart ve benzeri teknolojik ilerlemeler ve küreselleşme ile kişisel verilere erişim, toplama ve kullanım

---

117 Dülger, *Kişisel Verilerin Korunması*, 94.

118 Dülger*, Kişisel Verilerin Korunması*, 95,96.

119 AB Veri Koruma Direktifi (95/46/EC), 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun hazırlanmasında önemli ölçüde yol gösterici olmuştur. Bkz: Dülger, "Avrupa Birliği Genel", 75; Bilir, "6698 Sayılı Kişisel", 315.

120 Ayşe Nur Akıncı, "Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirmesi", Çalışma Raporu-6, Kalkınma Bakanlığı Bilgi Toplumu Dairesi Başkanlığı Yayını, Ankara, 2017, 4-5. (E.T. 13.05.2023), http://www.bilgitoplumu.gov.tr/wp-content/uploads/2017/07/ AB_Veri _Koruma _Tuzugu.pdf

121 Dülger*, Kişisel Verilerin Korunması*, 96.

yöntemlerinin önemli ölçüde değişmiş olması da hedefe ulaşılamamasında etkili olmuştur.[122]

İnternetin bugünkü veri toplama aracına dönüşmeye başlaması ile birlikte AB tarafından, "kişisel verilerin kapsamlı bir koruma yaklaşımına ihtiyacı olduğu" gerekçesiyle 1995 Direktifi güncellenmiş, *"2016/679 Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR)"* 24 Mayıs 2016 tarihinde kabul edilmiş, yürürlük tarihi 25 Mayıs 2018 belirlenerek bu tarihten geçerli olmak üzere tüm kuruluşların yasayla uyumlu olması zorunlu hale getirilmiştir.[123] Böylece GDPR oldukça kapsamlı bir veri koruma çerçevesi sunmuştur. GDPR; ihlal bildirimi, erişim hakkı, unutulma hakkı, veri taşınabilirliği, veri mahremiyeti ve veri koruma görevlileri gibi [124] kişisel verilerin ve veri sahiplerinin daha etkili şekilde korunması, veri işleyenler ve veri kontrolörlerinin genişletilmiş yükümlülükleri ihtiva etmesi gibi köklü yenilikler getirmiştir.[125] Bununla birlikte kişisel verilerin işlenmesinde bir dizi temel prensip öngörülmüştür. Bu prensipler:[126]

- Hukuka ve dürüstlük kurallarına uygun, şeffaf işleme ilkesi *(lawfulness, fairness and transparency)*
- Kişisel verilerin belirli, açık ve meşru amaçlarla toplanması ilkesi *(purpose limitation)*
- Kişisel verilerin işleme faaliyeti için gerekli olduğu kadar, ilgili ve ölçülü biçimde işlenmesi ilkesi *(data minimisation)*
- Kişisel verilerin doğru, gerekli hallerde ve güncel tutulması ilkesi *(accuracy)*
- Kişisel verinin işleme amacı için gerekli olandan daha uzun süre tutulmaması ilkesi *(storage limitation)*
- Veri işlemenin güvenli olması gerekliliği *(integrity and confidentiality)*

122 Akıncı, "Avrupa Birliği Genel", 5.
123 "What is GDPR, the EU's new data protection law?", (E.T. 07.05.2023), https://gdpr.eu/what-is-gdpr/
124 Dülger, *Kişisel Verilerin Korunması*, 108.
125 Akıncı, "Avrupa Birliği Genel", 19.
126 Art. 5 GDPR "Principles relating to processing of personal data", https://gdpr-info.eu/art-5-gdpr/

- Hesap verilebilirlik *(accountability)* şeklindedir.[127]

1.2.1.4. Birleşmiş Milletler Düzenlemeleri

Kişisel verilerin korunması hakkı İnsan Hakları Evrensel Beyannamesi'nde müstakil bir hak olarak değil, 12. maddesinde düzenlenen özel hayatın gizliliği hakkı içerisinde; Birleşmiş Milletler Medeni ve Siyasi Haklara İlişkin Uluslararası Sözleşme'de ise mahremiyet hakkı içerisinde değerlendirilmiştir.[128]

İlerleyen teknolojik imkânlar ve bilgisayar kullanımının artması üzerine kabul edilen *"Bilgisayara Geçirilmiş Kişisel Veri Dosyalarının Düzenlenmesine İlişkin Rehber İlkeler (BM Rehber İlkeler)"* ise kişisel verilerin korunması hakkının açıkça düzenlendiği ilk BM düzenlemesi olması nedeniyle önem arz etmekte olup üye ülkelerin hukuki düzenlemelerinde bulunması gerekli olan asgari ölçütleri belirlemeyi amaçlamıştır.[129] "Hukuka uygunluk ve dürüstlük ilkesi", "doğruluk ilkesi", "amacın belirliliği ilkesi", "ilgili kişinin verilerine erişim hakkının bulunması ilkesi", "verilerin güvenliği ilkesi", "ayrımcılık yasağı ilkesi", "denetim ve yaptırım ilkesi", "sınır ötesi veri akışı ilkesi" Rehber İlkelerde düzenleme altına alınmıştır.

1.2.2. Türkiye'de Kişisel Verilerin Korunması

1.2.2.1. Anayasa Kapsamında Kişisel Verilerin Korunması

Kişisel verilerin korunması hakkının anayasal düzenlemelerle güvence altına alınması, bireylerin verilerinin gizliliğinin ve güvenliğinin sağlanması açısından büyük önem taşımaktadır. Bu hak mukayeseli hukukta iki temel yaklaşımla düzenlenmiştir. İlk yaklaşıma göre kişisel verilerin korunması genellikle "özel hayatın gizliliği," "hürriyet," "genel kişilik hakkı" gibi çeşitli haklarla birlikte ve bu haklar kapsamında doğrudan

---

127 Türk hukuku açısından da kişisel verilerin korunması adına yasal düzenlemeler oluşturmak için hazırlanan Devlet Denetleme Kurulunun raporunda da bu ilkelere yer verilmiştir. Bkz: "Kişisel Verilerin Korunmasına İlişkin Ulusal ve Uluslararası Durum Değerlendirmesi ile Bilgi Güvenliği ve Kişisel Verilerin Korunması Kapsamında Gerçekleştirilen Denetim Çalışmaları", 780.

128 Dülger, "Avrupa Birliği Genel", 75.

129 Dülger, "Avrupa Birliği Genel", 75-76.

düzenlenmekte ve korunmakta iken ikinci yaklaşıma göre ise kişisel verileri koruma hakkı, müstakil bir hak şeklinde düzenlenmiştir.[130]

Türk hukuku açısından bakıldığında kişisel verilerin korunması hakkının dayanağı olacak anayasal hükümlerin, 2010 yılında yapılan anayasa değişikliği öncesinde çeşitli haklarla birlikte mevcut olduğu görülmektedir. Bu bağlamda hukuk devleti ilkesi (md.2), bireyin maddi ve manevi varlığını serbestçe geliştirme hakkı (md.17), özel hayatın gizliliği hakkı (md.20), konut dokunulmazlığı (md.21), haberleşmenin gizliliği (md.22), dini ve vicdani kanaatleri açıklamaya zorlanamama (md.24), düşünce ve kanaatleri açıklamaya zorlanamama (md.25) maddeleri örnek gösterilebilecektir.[131] Ancak bu hakların ve özellikle özel hayatın gizliği hakkının kişisel verileri koruma hakkının korunması yönünden yeterli ve kapsamlı bir niteliğe sahip olmaması, bu bağlamda kişisel verilere özgü düzenleme yoluyla çok daha etkin ve nitelikli bir korumanın sağlanması ihtiyacının karşılanması amacıyla, özel hayatın gizliliğinin düzenlendiği Anayasanın 20. maddesine ayrı bir hüküm eklenerek kişisel verilerin Anayasada ayrıca düzenlenmesi gerekliliği ortaya çıkmıştır.[132] Bu doğrultuda 5982 sayılı ve 07.05.2010 tarihli Anayasa değişikliği ile 20. maddeye *"Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."*[133] şeklindeki 3. fıkra dahil edilmiştir. Değişikliğin nedeni ise "*Anayasada kişisel verilerin korunmasına yönelik dolaylı hükümler bulunmakla birlikte yeterli değildir. Mukayeseli hukukta ve tarafı olduğumuz uluslararası belgelerde de kişisel verilerin korunması önemle vurgulanmaktadır*."[134] şeklindeki ifade ile belirtilmiştir. Anlaşılacağı üzere, uluslararası hukuka atıf yapılarak kişisel verilerin korunması hukukunun önemi ve her geçen gün

130 Küçük, "1982 Anayasası'ndaki Temel", 40.
131 Kılınç, "Anayasal Bir Hak", 1131.
132 Küzeci, *Kişisel Verilerin Korunması*, 280' den aktaran Küçük, "1982 Anayasası'ndaki Temel", 42
133 "Türkiye Cumhuriyeti Anayasası", (E.T. 27.07.2023), https://www.anayasa.gov.tr/tr/mevzuat/anayasa/
134 Kişisel Verileri Koruma Kurumu, "Anayasal Bir Hak Olarak Kişisel Verilerin Korunmasını İsteme Hakkı", 4, (E.T.23.03.2024),https://www.kvkk.gov.tr/Icerik/4184/Anayasal-Bir-Hak-Olarak-Kisisel-VerilerinKorunma sini-Isteme-Hakki

geliştiği vurgulanmıştır Böylelikle açıkça ve en üst normda düzenlenen kişisel verilerin korunması hakkı ile Türkiye'de önemli bir hukuki temel oluşturulmuştur.[135]

1.2.2.2. Kişisel Verileri Koruma Kanunu Kapsamında Kişisel Verilerin Korunması

Kişisel verileri koruma hakkının doğrudan Anayasa'da düzenlendiği 2010 yılı öncesinde, bu hakkın müstakil olarak düzenlendiği bir kanun mevcut değildi.[136] Türkiye'de kişisel verilerin korunmasına yönelik müstakil bir kanun oluşturmak amacıyla ilk girişim 1989 yılında yapılmış ve bir komisyon kurulmuştur. Ancak bu komisyon, çalışmalarını sonuçlandıramadan dağılmıştır. Ardından 2000 yılında yeni bir komisyon kurulmuş ve üç yıl süren çalışmalarının ardından bir kanun tasarısı oluşturulmuştur. Ne var ki, hazırlanan tasarı çeşitli nedenlerle yasalaşmamıştır. Sonrasında, 2008 ve 2014 yıllarında Adalet Bakanlığı öncülüğünde yeni bir kanun tasarısı oluşturulmuş ve TBMM'ye sunulmuştur.[137] Ne var ki, bu kanun teklifleri yasama dönemi bittiği için uygulanamamış ve geçersiz kalmıştır. 2010 Anayasa değişikliği ile 20/3 maddeye eklenen *"...kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir*" şeklindeki hükmüyle kişisel verileri koruma hakkının kanunla düzenlenmesi öngörülmüş ise de bu kanun derhal çıkarılmamıştır. Anayasa değişikliği ile öngörülen 20/3 hükmünün gereği 24.03.2016 kabul tarihli 6698 sayılı Kişisel Verilerin Korunması Kanunu[138] ile gerçekleşmiştir.[139]

Uluslararası belgeler ve büyük ölçüde Avrupa Birliğine üye ülkelerin kişisel verileri koruma mevzuatına uyum sağlamak için yürürlüğe konulan 95/46/EC sayılı Direktif esas alınarak[140] ve mukayeseli hukuk uygulamaları ile ülke ihtiyaçları göz önünde tutularak hazırlanan KVKK[141], kişisel verilerin modern normlarda işlenmesini ve korunmasını

---

135 Doğan, *Karşılaştırmalı Hukukta Anayasal*, 86, 89.

136 Küçük, "1982 Anayasası'ndaki Temel", 44.

137 Kişisel Verileri Koruma Kurumu, "Kişisel Verilerin Korunması Kanunu ve Uygulaması", 16, (E.T. 02.08.2023),https://kvkk.gov.tr/yayinlar/K%C4%B0%C5%9E%C4%B0SEL%20VER%C4%B0LER%C4%B0N%20KORUNMASI%20KANUNU%20VE%20UYGULAMASI.pdf

138 7 Nisan 2016 tarih ve 29677 sayılı Resmî Gazetede yayımlanarak yürürlüğe girmiştir.

139 Küçük, "1982 Anayasası'ndaki Temel", 44.

140 Dülger, *Kişisel Verilerin Korunması*, 113; Küzeci, *Kişisel Verilerin Korunması*, 352.

141 Kanunlaştırma aşamasında TBMM Genel Kurulunda KVKK tasarısının yeterince görüşülüp tartışılmaması, tasarının kabul edilmesi öngörülen GDPR'a göre değil de 95/46/EC sayılı Direktife göre hazırlanması sıkça eleştirilmiş olup diğer eleştiriler için de bkz: Furkan Özarslan, "Türkiye'de Kişisel Verilerin Korunması Politikasının Analizi", (Yayımlanmamış Yüksek Lisans Tezi, Pamukkale Üniversitesi, 2022), 83.

kapsamaktadır. Bu bağlamda, Kanun'da kişisel verilerin işlenme şartları, kişisel verilerin işlenmesinde veri işleyen gerçek ve tüzel kişilerin sorumlulukları ile uygulanacak usul ve esaslar düzenlenmekte; bununla birlikte kanun kişisel verilerin sınırsız ve düzensiz şekilde toplanmasının, yetkili olmayan şahısların erişimine açılması, ifşası veya amaç dışı ya da kötüye kullanımı nedeniyle kişilik haklarının ihlal edilmesinin engellenmesi amacına da hizmet etmektedir.[142] Başka bir ifadeyle Kanun'un 1. maddesinde[143] ve madde gerekçesinde belirtildiği üzere, kişisel verilerin işlenmesi sürecinde kişilerin temel hak ve özgürlüklerini gözetmek, kişisel verileri işleyen gerçek ve tüzel kişilerin uyması gereken usul ve esasları düzenlemek ve böylece bu kişilerin sorumluluklarını belirlemek, mahremiyet hakkını ve kişisel veri güvenliği hakkını korumak, amaç olarak belirlenmiştir.[144] Daha geniş anlamıyla kişisel verilerin korunması hakkı sınırsız veya mutlak bir hak olmadığından kişisel verilerin korunmasına ilişkin düzenlemelerin esas amacı, hızla gelişen bilişim teknolojisinin sağladığı imkânlar ile bu teknolojinin dinamik yapısının getirdiği sorunlar karşısında temel hak ve hürriyetleri korumak ve bu iki menfaat ya da gelişme arasında denge kurmaktır.[145]

Kişisel Verileri Koruma Kanunu kapsamında yürürlüğe giren "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik"[146], "Veri Sorumluları Sicili Hakkında Yönetmelik"[147], "Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ"[148], "Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ"[149] de başlıca ikincil düzenlemelerdir.[150]

---

142 Doğan, *Karşılaştırma Hukukta Anayasal*, 120.

143 6698 sayılı Kanun'un 1. maddesinde Kanun'un amacı da şu şekilde hüküm altına alınmıştır: "*Kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ve uyacakları esas ve usulleri düzenlenmektir*".

144 "Kişisel Verilerin Korunması Kanunu ve Uygulaması", 20.

145 Doğan, *Karşılaştırma Hukukta Anayasal*, 125.

146 28 Ekim 2017 tarihli, 30224 sayılı Resmî Gazetede yayımlanmıştır. (E.T. 02.08.2023), https://www.resmigazete.gov.tr/eskiler/2017/10/20171028-10.htm

147 30 Aralık 2017 tarihli, 30286 sayılı Resmî Gazetede yayımlanmıştır. (E.T. 02.08.2023), https://www.resmigazete .gov.tr/eskiler/2017/12/20171230-7.htm

148 10 Mart 2018 tarihli, 30356 sayılı Resmî Gazetede yayımlanmıştır. (E.T. 02.08.2023), https://www.resmigazete.gov.tr/eskiler/2018/03/20180310-6.htm

149 10 Mart 2018 tarihli, 30356 sayılı Resmî Gazetede yayımlanmıştır. (E.T. 02.08.2023), https://www.resmigazete.gov.tr/eskiler/2018/03/20180310-5.htm

150 Turan, *Karşılaştırmalı Hukukta Kişisel*, 117.

1.2.2.3. Ceza Kanunu Kapsamında Kişisel Verilerin Korunması

Kişisel verilerin korunmasına ilişkin suç tipleri 1 Haziran 2005 tarihinde yürürlüğe giren 5237 sayılı Türk Ceza Kanunu (TCK)'nun özel hükümlerinde "kişilere karşı suçlar" başlıklı ikinci kısmının "özel hayata ve hayatın gizli alanına karşı suçlar" bölümünde düzenlenmiştir. Bu düzenlemelere göre TCK'nın 135. madde hükmünde "kişisel verilerin kaydedilmesi suçu", 136. madde hükmünde "verileri hukuka aykırı olarak verme veya ele geçirme suçu", 137. maddesinde bu suçların nitelikli halleri, 138. maddesinde "verilerin yok edilmemesi suçu", 140. maddesinde bu suçlara ilişkin tüzel kişiler hakkında uygulanacak güvenlik tedbirleri hüküm altına alınmıştır.[151]

KVKK'nın "Suçlar ve Kabahatler" 17/1. maddesinde "*Kişisel verilere ilişkin suçlar bakımından 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununun 135 ila 140 ıncı madde hükümleri uygulanır*" ifadesine yer verilerek, bahsi geçen kanun kapsamında olup olmadığına bakılmaksızın kişisel verilere ilişkin hukuka aykırılıklar bakımında TCK'ya atıf yapılarak, Kanun öncesinde de mevcut olan suç tiplerinin uygulanmasının sürdürüleceği ifade edilmiş, böylece KVKK ile TCK'nın 135 ile 140. maddeleri arasında

---

[151] Anayasa Mahkemesi bir kararında kişisel verilerin ceza hukuku kapsamında da korunması gerekliliğini şu şekilde açıklamıştır: "*Öncelikle devletin pozitif yükümlülüğünün, kişisel verilerin korunması kapsamında üçüncü kişilerin müdahalelerine karşı yasal altyapı oluşturulması yanında bu altyapının hakkın ihlaline etkili yargısal tepkiyi vermesi gerekliliğini de içerdiği vurgulanmalıdır. Bu bağlamda devletin kişisel verilerin korunması kapsamında kişisel verilerin hukuka aykırı olarak ele geçirilmesine, işlenmesine ve açıklanmasına yönelik önleyici tedbirler alması ve benzer durumların bir daha yaşanmaması için bunu yapanlara karşı caydırıcı yargısal tepki göstermesi gerekir. Bu yargısal tepkinin adli ceza biçiminde olması zorunlu değildir. Ancak bu tür müdahalelerin kanunda suç olarak düzenlenmesi hâlinde ceza soruşturması ve kovuşturmasının etkili bir biçimde yürütülmesinin sağlanması da devletin pozitif yükümlülüklerinin gereğidir (benzer değerlendirmeler için bkz. Ferhat Ölmez, B. No: 2018/20040, 10/3/2021, § 29; B.Y., B. No: 2018/30296, 7/9/2021, § 39; H.Ö., § 43). Dolayısıyla her durumda söz konusu yargısal sistemlerin etkili şekilde işletilmesi ve soruşturmalar ya da yargılamalar neticesinde yargısal makamlarca ulaşılan tüm sonuçların temel hakların içerdiği güvenceleri koruyacak şekilde ilgili ve yeterli gerekçelerle açıklanması gerekir (Ali Çığır, § 35; Erol Kumcu, § 35; H.Ö., § 41).*" (*İ.A.*, Başvuru No: 2017/16849, 19/10/2023, §56). (E.T. 10.07.2024), https://kararlarbilgibankasi.anayasa.gov.tr/BB/2017/16849
Bu noktada TCK'daki özel düzenlemeden bahsetmekte fayda bulunmaktadır. Ticari sır, bankacılık sırrı veya müşteri sırrı ile fenni keşif ve buluşlar veya sınai uygulamaya ilişkin kişisel veriler, TCK 239. madde kapsamında koruma altına alındığından TCK.135 vd. maddelerindeki suçun konusu oluşturmazlar. Bkz: Kayıhan İçel, "Ceza Hukuku Açısından Kişisel Verilerin Korunmasında "Kişisel Veri" ve "Hukuka Aykırılık" Kavramları", *İstanbul Barosu Dergisi*, 94/2 (Mart 2020): 15-23, 19. (E.T. 11.07.2024), https://www.istanbulbarosu.org.tr/files/yayinlar/dergi/doc/ibd20202.pdf#page=16
Bununla birlikte vergi mahremiyetinin ihlal edilmesi suçu da Vergi Usul Kanunu'nun (VUK) 362. maddesinde düzenlenmiş, yaptırımı için TCK 239. maddeye atıf yapılmıştır. Dolayısıyla bu kişisel verilere ilişkin özel düzenlemeler bulunması nedeniyle genel nitelikteki TCK 135 md. ve devamı hükümler uygulama alanı bulmayacaktır.

direkt olarak ilişki kurulmuştur.[152] 17/2. maddesinde ise "*Bu Kanun'un 7. maddesi hükmüne aykırı olarak; kişisel verileri silmeyen veya anonim hâle getirmeyenler 5237 sayılı Kanunun 138. maddesine göre cezalandırılır."* şeklindeki daha spesifik bir düzenleme ile koruma getirilmiştir.

TCK ile KVKK arasında birtakım farklılıklar da bulunmaktadır. Tüm hassas veriler, mahiyeti itibariyle KVKK'da ayrı bir korumaya tabi tutulmaktayken TCK tarafından sağlanan nitelikli korumadan yararlanamamaktadır. Kişilerin "biyometrik ve genetik verileri, mezhebi veya diğer inançları, kılık ve kıyafeti, ırkı, etnik kökeni, dernek veya vakıf üyeliği, ceza mahkumiyeti ve güvenlik tedbirleriyle ilgili verileri" suçun basit halini oluşturan TCK md.135/1'deki korumadan yararlanmaktadır. Öte yandan TCK'da "kişinin ahlaki eğilimi" şeklinde ifade edilen ve yalnızca TCK tarafından kabul edilen bu özel nitelikli kişisel veri, TCK md. 135/2'deki korumadan yararlanabilmektedir. Bu tür belirsizlikler kavram karmaşası ve uygulama zorluğu meydana getirdiğinden özellikle kanuni tanımlamalar söz konusu olduğunda KVKK'nın tek bir rehber olarak kabul edilmesi gerekmektedir.[153]

1.2.2.4. Medeni Kanun Kapsamında Kişisel Verilerin Korunması

Kişisel veri koruması, kişilik hakkı çatısı altında olmasına rağmen kişilik hakkının bağımsız bir uzantısı niteliğinde olması nedeniyle Türk Medeni Kanunu (TMK)'ndaki kişiliği koruyucu hükümlere başvurularak kişilik haklarının korunması mümkündür.[154] KVKK'nın 1. maddesinde de hüküm altına alındığı üzere Kanun'un başlıca amacı özel hayatın ve kişilik haklarının yasal koruma altına alınmasıdır ki bu husus TMK ile birebir ilgilidir. TMK'nın 24. maddesine bakıldığında, kişilik haklarına karşı gerçekleştirilen saldırılar hukuka aykırı kabul edilmekte, bu tür saldırıların muhatabı olan kişiler mahkemeden korunma talep edebilmektedir. Özellikle KVKK öncesinde, Anayasa'da yer

---

152 Murat Volkan Dülger, "Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması", *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi*, 3 (2016): 101-168, 119-120, (E.T. 02.07.2023), https://dergipark.org.tr/tr/download/article-file/1102227

153 Akçakoca, *Tıp Ceza Hukukunda*, 673,674.

154 Özkan, "Kişisel Veri Koruma Hukukunun", 708.

alan özel hayatın korunması ilkesi ile TMK 24. maddesi arasında sık sık ilişki kurularak, yargı içtihatlarında bu maddeye atıf yapıldığı gözlenmektedir.[155]

TMK'nın 24. maddesinde kişilik haklarının korunması, 25. madde ve devamında kişilik hakkı ihlal edilenlerin açacağı davalar;[156] Türk Borçlar Kanunu'nun (TBK) 49 ve devamındaki maddelerinde ise haksız fiillere karşı talep edilecek tazminatlar ile ilgili düzenlemelere yer verilmiştir. Anılan hükümler kişisel verilerin ihlal edilmesi durumunda ikame edilecek tazminat davalarında kullanılabilecektir.[157] Kişisel veri ihlali sonucu doğan zararın, ilgili kişinin şahsi değerlerinin azalması sonucu oluşması gerekmemektedir. Zarar görenin iktisadi değerlerinin azalması şeklinde bir zarar meydana gelme ihtimali de bulunmaktadır. Bu durumda zarar gören kişinin mülkiyet veya zilyetlik gibi temel koruma standartları sayesinde korunan hukuki değerlerinden biri ihlâl edilmiş olmasa dahi maddi zararının tazmin edilmesi imkânı bulunmaktadır.[158]

TMK ve TBK düzenlemeleri hem kişilik haklarına yönelik saldırıların önüne geçilmesinde hem de kişisel verilerin korunmasında hukuki zemin oluşturmaktadır. Ne var ki, bu alanın kendine has özelliği nedeniyle, genel hükümlerle kişisel verileri etkili bir biçimde korumak kolay olmamaktadır.[159] Zira kişisel verilerin korunmasına hâkim olan ana prensipler, büyük ölçüde önleyici koruma sağlamaktadır. Kişisel verilerin, sadece toplandıkları amaç için kullanılması gerekliliği, özel nitelikteki bazı veri türlerinin işlenmesinin genellikle yasak olması ve veri sahibi olan kişi veya kurumların bir sicile kaydedilmesi gibi ilkeler kişisel verilerin korunması hakkının ihlal edilmesini ve zararın oluşmasını engelleyici niteliktedir. Diğer bir deyişle, kişisel verilerin korunması, olası zararın doğmasını ve kişisel verilerin ihlal edilmesini önlemeye yönelik bir önleyici nitelik taşır.[160] Oysa, TMK ve TBK kapsamında getirilen koruma, genellikle saldırının gerçekleşmesinden sonra yahut ciddi bir saldırı tehlikesinin varlığı halinde işleyebilecek bir sistem öngörmektedir.[161] Saldırıya son verilmesi talebi, saldırı tehlikesinin önlenmesi

---

155 Bekir Gürses, "AB ve Türk Hukukunda Kişisel Verilerin Korunması- Mevzuat Uyumuna Yönelik Bir Değerlendirme", (Yayımlanmamış Yüksek Lisans Tezi, Marmara Üniversitesi, 2019) 17.

156 Özkan, "Kişisel Veri Koruma Hukukunun", 718-719.

157 Kılınç, "Anayasal Bir Hak", 1132

158 Damla Gürpınar, "Kişisel Verilerin Korunamamasından Doğan Hukuki Sorumluluk", *D.E.Ü. Hukuk Fakültesi Dergisi, Prof. Dr. Şeref ERTAŞ'a Armağan*, 19/ Özel Sayı (2017): 679-698, 689.

159 Kılınç, "Anayasal Bir Hak", 1132.

160 Küzeci*, Kişisel Verilerin Korunması,* 452.

161 Küzeci*, Kişisel Verilerin Korunması,* 452; Aşıkoğlu, *Avrupa Birliği ve Türk*, 101.

davası, saldırının hukuka aykırılığının tespiti davası, maddi ve/veya manevi tazminat davası ve menfaat devri talebi bu bağlamda örnek olarak verilebilir.[162]

Açıklanan nedenlerle KVKK kapsamında kişisel verilerin korunmasında temel ilkelerin önleyici korumaya odaklandığı, verilerin kötüye kullanılmasını ve veri ihlalini engellemeye çalıştığı; TMK ve TBK kapsamındaki korumanın ise daha çok gerçekleşen saldırı ve ihlallerin ardından telafi edici önlemler içerdiği söylenebilir.

1.2.2.5. Diğer Düzenlemeler

Türk hukukunda kişisel verilerin korunmasına ilişkin yukarıda zikredilen birincil kaynakların yanı sıra tali nitelikte de birçok yasal düzenleme bulunmaktadır. İş Kanunu, Türk Borçlar Kanunu, Türk Ticaret Kanunu, Bankacılık Kanunu, Banka ve Kredi Kartları Kanunu, Elektronik Haberleşme Kanunu, Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Hakkında Yönetmelik, Elektronik İmza Kanunu, Nüfus Hizmetleri Kanunu, Resmi İstatistiklerde Veri Gizliliği ve Gizli Veri Güvenliğine İlişkin Usul ve Esaslar Hakkındaki Yönetmelik, Tıbbi Deontoloji Tüzüğü,[163] Bilgi Edinme Kanunu, Polis Vazife ve Salahiyet Kanunu , Vergi Usul Kanunu, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğin Korunması Hakkında Yönetmelik, Ceza Muhakemesinde Beden Muayenesi, Genetik İncelemeler ve Fizik Kimliğin Tespiti Hakkında Yönetmelik, Ceza Muhakemesi Kanununda Öngörülen Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmelik bu düzenlemelere örnek olarak verilebilir.[164]

---

162 Develioğlu, *6698 sayılı Kişisel*, 47; Yücedağ, "Kişisel Verilerin Korunması", 126-135.

163 Önder Kutlu, Selçuk Kahraman, "Türkiye'de Kişisel Verilerin Korunması Politikasının Analizi", *Siyaset, Ekonomi ve Yönetim Araştırmaları Dergisi,* 5/4 (Ekim 2017): 45-62, 53. https://doi.org/10.25272/j.2147-7035 .2017.5.4.03.

164 Kılınç, "Anayasal Bir Hak", 1089-1169.

İKİNCİ BÖLÜM

KİŞİSEL VERİLERİN KORUNMASI HUKUKUNUN TEMEL İLKELERİ VE DENETİM SİSTEMİ

2.1. Kişisel Verilerin Korunmasına İlişkin Temel İlkeler

2.1.1. Veri İşleme İlkeleri

Veri işleme faaliyetlerinde hukuki uyumun ve belirli bir niteliğin sağlanması için uyulması gereken birtakım kurallar bulunması gerekmektedir. Bu nedenle veri koruması ile ilgili bütün düzenlemelerde konusu kişisel veri olan her türlü faaliyete ilişkin temel ilkeler belirlenmiştir.[165] Bu doğrultuda 95/46/EC sayılı Direktif'te "verilerin kaliteli olması ilkesi"[166] olarak ifade edilen ilkeler de baz alınarak 6698 sayılı Kanun kapsamında da veri işleme ilkeleri düzenlenmiştir. Veri işleme ilkelerini düzenleyen ve özellikle dikkat edilmesi gereken bu temel ilkeler KVKK'nın amacını oluşturur. Kişisel veri işleme faaliyetlerinin özünü teşkil eden bu ilkelere riayet edilmesi bir zorunluluk olup kişisel veri işleme koşullarının varlığı halinde dahi genel ilkelere uyulmadığı saptanırsa, hukuka aykırı bir kişisel veri işleme faaliyeti meydana gelmiş olacaktır.[167] Bu nedenle kişisel verilerin hukuka uygun olarak işlenmesi için belirlenen genel ilkelerin, kişisel verilerin korunması kapsamında tüm kanuni düzenlemelere uygun olması bakımından göz önüne alınması icap eder. Öte yandan veri koruma düzenlemelerine uygunluğun temelini genel

---

165 Dülger, *Kişisel Verilerin Korunması*, 260.

166 Küzeci, *Kişisel Verilerin Korunması*, 228.

167 Umniyahasghar Yosif, "Kişisel Verilerin İşlenmesi Şartları ve 6698 Sayılı Kişisel Verilerin Korunması Kanununun Ruhu Olarak Genel İlkeler", *Selçuk Üniversitesi Adalet Meslek Yüksekokulu Dergisi*, 4/1 (2021):1-22, 4. (E.T. 02.07.2023), https://dergipark.org.tr/tr/download/article-file/1748966

ilkeler oluşturmakla[168] birlikte Kanun'un 4. maddesinde yer verilen ilkeleri de 5. ile 9. maddeleri kapsayan "genel kaideler" kataloğu olarak nitelendirmek mümkündür.[169]

Kişisel verilerin korunmasına yönelik genel ilkeler Kanunun 4. maddesinde şu şekilde düzenlenmiştir:

"(1) Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir.

(2) Kişisel verilerin işlenmesinde aşağıdaki ilkelere uyulması zorunludur:

a) Hukuka ve dürüstlük kurallarına uygun olma.

b) Doğru ve gerektiğinde güncel olma.

c) Belirli, açık ve meşru amaçlar için işlenme.

ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma.

d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme."

Belirtilen ilkelerin birbirinden net çizgilerle ayrılması bir hayli güçtür. Zira birtakım ilkeler diğerlerine rehberlik yapan kapsayıcı bir nitelik göstermekte, birçoğu da birbirini tamamlamaktadır.[170]

2.1.1.1. Veri İşleyenin Hukuka ve Dürüstlük Kurallarına Uygun Davranması

6698 sayılı Kanun'da yer alan ilkelerden biri olan "hukuka ve dürüstlük kurallarına uygunluk" ilkesi, Avrupa Birliği'nin 95/46/EC sayılı Direktifi ve 2016/679 sayılı Genel Veri Koruma Tüzüğü'ndeki "hukuka uygunluk *(lawfulness)*" ve "adil olma *(fairness)* " ilkeleriyle aynı anlamda değerlendirilebilir. Bu ilke, kişisel veri işleme aşamalarının

---

168 Nafiye Yücedağ, "Kişisel Verilerin Korunması Kanunu Kapsamında Genel İlkeler", *Kişisel Verileri Koruma Dergisi*, 1 /1 (2019), 47-63, 47, (E.T. 02.07.2023), https://dergipark.org.tr/tr/pub/-kvkd/issue/45759/566993

169 Çekin, *Avrupa Birliği Hukukuyla*, 61.

170 Küzeci, *Kişisel Verilerin Korunması,* 227.

başlangıcından bitişine kadar hukuki ve dürüst bir şekilde gerçekleştirilmesi gerektiğini vurgular.[171]

Türk hukukunda Anayasa'nın 20. maddesinde, kişisel verileri işlemenin kural olarak yasak olduğunu, ancak kanunda belirtilen hallerde ya da kişinin açık rızasıyla kişisel verilerin işlenebileceği belirtilmektedir. KVKK'nın 4/2-a maddesinde ise kişisel veri işlenmesi süreçlerinde hukuka ve dürüstlük kuralına uygun olma ilkesine uyulması zorunluluğu getirilmiştir.[172] Bu doğrultuda KVKK'nın 5. ve 6. maddesinde kişisel verilerin işlenmesinde hukuka uygunluk nedenleri belirtilmiş olup her koşulda KVKK 'nın 4. maddesiyle hüküm altına alınan genel ilkelere uygunluk sağlanmalıdır. Hükümdeki "dürüstlük kuralına uygun işleme" ifadesi, veri sorumlusunun kişisel verileri koruma yükümlülüğüne uygun davranarak ilgili kişilerin menfaatlerinin ve makul beklentilerinin göz önüne alınması, ilgili kişilerin güvenini haksız çıkaracak davranışlardan kaçınma, ilgili kişinin yanılgısından fayda sağlanmaması şeklinde anlaşılabilir.[173] Kişisel Verileri Koruma Kurumu tarafından kişisel verilerin işlenmesine ilişkin yayımlanan kılavuzda[174] da "*dürüstlük kurallarına uygunluğun, Medeni Kanunun 2. maddesinde düzenlenen dürüstlük kuralının, kişisel veriler işlenirken ihlal edilmemesi olduğu; kişisel verilerin korunması açısından ise dürüstlük kuralının kişilerin kendilerine veri işleme konusunda izin ya da emir veren hukuk kurallarına dayanarak gerçekleştirdikleri fiillerde, bu hukuk kuralının amacına göre mümkün olan en az miktarda veri işlemeleri, ilgili kişilerin öngöremeyeceği biçimde hareket etmemeleri gibi davranışları gerektirdiği*" ifade edilmiştir. Bu ilke özellikle "haklı beklenti", "haklı menfaat" gibi tarafların çatışan yararlarını dengelemeyi hedefleyen hükümler çerçevesinde önemli olacak, dahası kişisel verilerin işlenmesi için kural olarak verilmesi gereken açık rızanın özgür iradeye dayalı olup olmadığı, gereken önlemlerin alınıp alınmadığı sorularına cevap ararken de dikkate alınacaktır.[175]

---

171 Aktaran Yosif, "Kişisel Verilerin İşlenmesi", 4; Bilir "6698 Sayılı Kişisel", 320.

172 GDPR'da düzenlenen "şeffaflık/ şeffaf olma ilkesi (*transparency)"* KVKK'da ayrıca müstakil olarak düzenlenmemiş olup genel ilkelerin yansıması olarak değerlendirilmektedir.

173 Yücedağ, "Kişisel Verilerin Korunması", 49-50; Yosif, "Kişisel Verilerin İşlenmesi", 5; Çekin, Avrupa Birliği Hukukuyla, 63,64.

174 Kişisel Verileri Koruma Kurumu, "Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler", 3, (E.T. 04.08.2023), https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/32ff74f6-9798-405a-b3d2-b42d28423fde.pdf

175 Çekin, *Avrupa Birliği Hukukuyla,* 64.

Bu ilke, kural olarak yasaklanan kişisel veri işleme faaliyetinin yalnızca KVKK'da hüküm altına alınan durumlarda mümkün olmasını destekler niteliktedir. Başka bir ifade ile kişisel veri işleme faaliyetinin kural olarak yasaklandığı durumda, bu verilerin yasal ve meşru amaçlarla 6698 sayılı Kanun kapsamında işlenebilmesi için diğer ilkelere uygunluk sağlanması ile birlikte hukuka ve dürüstlük kurallarına da uygunluk aranması, kişisel verilerin korunmasını güçlendiren önemli bir nitelik taşır.[176] Kısaca ifade etmek gerekirse bu ilke aynı zamanda diğer veri koruma ilkelerine de kaynaklık etmektedir.[177]

2.1.1.2. Verilerin Doğru ve Gerektiğinde Güncel Olması

GDPR'ın 5/1-d maddesinde yer alan verilerin doğru ve gerektiğinde güncel olma ilkesi (*accuracy*), Kanunun 4/2-b hükmünde açıkça ifade edilmiştir. Kişisel veri, bir gerçek kişiyi belirlemeye yarayan bilgiler olarak tanımlandığına göre hakkında bilgi verilen kişiyi belirleyebilecek bilgiler doğru olmalıdır.[178]

Kişisel verilerin doğru ve gerektiğinde güncel tutulması ilkesi, kişisel veri işleme faaliyetlerinin güncelliğini yitirmemiş ve doğru olan kişisel verilere dayanarak gerçekleştirilmesini gerektirir. Bu ilkenin temelinde yatan husus ise doğru ve güncel olmayan verinin korunmasının sağlanmasının mümkün olmamasıdır. Yanlış tutulan veri, kişinin temel hak ve özgürlüklerine halel getirmesinin yanı sıra kişisel verilerinin işlenmesinden beklediği korumaya da ulaşamamasına sebebiyet verebilir.[179] Zira veriye erişme hakkı ile de yakından ilişkili olan bu ilkeden beklenen amaç, doğru ve güncel olan verinin korunmasının denetlenmesi olduğundan, bilgilerine ulaşamayan kişinin verinin doğruluğunu denetleme imkânı da ortadan kalkar.[180]

Bir üniversite hastanesi tarafından ilgili kişinin sağlık verilerinin idari bir uyuşmazlığa esas teşkil etmek üzere talep üzerine davalı kamu kurumuna aktarılması sonrasında kişisel veri sahibi şikayetçi olmuştur. Şikayet üzerine Kişisel Verileri Koruma Kurulunun 04/08/2022 tarihli ve 2022/790 sayılı kararında "*doktorun teşhis koyma amaçlı olarak hastaya sorduğu sorular sonucu elde ettiği, hastanın mevcut ya da geçmiş hastalıkları*

176 Yosif, "Kişisel Verilerin İşlenmesi", 5.
177 Küzeci, *Kişisel Verilerin Korunması,* 230.
178 Dülger, *Kişisel Verilerin Korunması,* 293
179 Dülger, *Kişisel Verilerin Korunması,* 294.
180 Küzeci, *Kişisel Verilerin Korunması,* 244.

hakkında kendisinden alınan bilgileri içeren hasta anamnez formunun hasta muayene bilgileri bölümüne doktor tarafından yanlış anlaşılarak "ara sıra tek tük esrar kullanmak zorunda kaldığını söylüyor" şeklinde yazıldığı belirtilen ifadeyi içeren formun kamu kurumuna teslimiyle birlikte, ilgili kişi hakkında Cumhuriyet Başsavcılığına suç duyurusunda bulunulduğu, yapılan soruşturma neticesinde ilgili kişi hakkında Cumhuriyet Başsavcılığının Kararı ile kovuşturmaya yer olmadığına dair karar verildiği

… İlgili kişinin Kanun'un 11'inci maddesinin (1) numaralı fıkrasının (d) bendi kapsamında "Anamnez Formu"nda geçen "esrar maddesi kullanıldığına ilişkin verilerin" düzeltilmesini talep etme hakkı dikkate alındığında; Kanun'un 4'üncü maddesinin (2) numaralı fıkrasının (b) bendinde yer aldığı üzere "doğru ve gerektiğinde güncel olma" ilkesine uygun olarak Kişisel Sağlık Verileri Hakkında Yönetmelik'in 13'üncü maddesi kapsamında, veri sorumlusu tarafından gerek kendi bünyesinde ve gerektiği takdirde ilgili kişiyi de yönlendirmek suretiyle İl Sağlık Müdürlüğü nezdinde gerekli işlemlerin yapılması ve sonucundan Kurula bilgi verilmesi hususunda veri sorumlusunun talimatlandırılmasına"[181] şeklinde verilen kararda doğru ve güncel olmayan verinin ilgilinin haklarına ne denli zarar verebileceği anlaşılmaktadır.

Kurumun bahsi geçen güncel kararında da görüleceği üzere Avrupa Birliği 1995/46 Sayılı Veri koruma Direktifi'nde "*kalite prensibi*",[182] Birleşmiş Milletlerin kabul ettiği Bilgisayarla İşlenen Kişisel Veri Dosyaları Hakkında Yönlendirici İlkelerde "*doğruluk*" şeklinde açıklanan verinin doğru ve güncel olması ilkesi[183] Kanunda düzenlenen ilgili kişinin verilerinin düzeltilmesini talep etme hakkı ile bağlantılıdır. Kişisel verilerin doğru ve güncel bir şekilde tutulması, veri sorumlusunun yararına olduğu gibi ilgili kişinin temel hak ve özgürlüklerinin güvenceye alınması bakımından da önem arz etmektedir. Bu noktada veri sorumlusunun aktif özen yükümlülüğü, veri sorumlusu eğer bu verilere dayanarak kişisel veri sahibiyle ilgili bir sonuç çıkarıyorsa geçerli olmaktadır. Bunun haricinde veri sorumlusu her koşulda ilgili kişinin bilgilerinin doğru ve güncel olmasını

181 "Kişisel Verileri Koruma Kurulunun 04/08/2022 tarihli ve 2022/790 sayılı Kararı", (E.T. 03.06.2023), https:// kvkk.gov.tr/Icerik/7574/2022-790

182 Kılınç, "Anayasal Bir Hak", 1120

183 Kılınç, "Anayasal Bir Hak", 1111.

sağlayacak kanalları açık tutmalıdır.[184] Zira bu ilke, kişisel verilerin güncelliğini saptayabilmek için veri sorumlusunun dayatmayla ve her zaman ilgili kişinin içinde bulunduğu yeni şartları araştırması şeklinde algılanamaz. Bu sebeple ilgilinin, kişisel bilgilerinde bir değişiklik meydana geldiğinde veri sorumlusuna bilgi vermesi gerekmektedir. Dolayısıyla veri sorumlusunun veri kanallarını açık tutması gereken bir sistem oluşturması gerekmektedir.[185]

Kişisel verilerin doğru tutulması ve güncel tutulması arasındaki farklılık bu ilkeye ilişkin özellikle dikkat edilmesi gereken noktadır. Kişisel verilerin güncel tutulma ihtiyacı gerektiği durumlarda söz konusu iken, doğru tutulmasının mutlak surette sağlanması gerekmektedir.[186]

2.1.1.3. Verilerin Belirli, Açık ve Meşru Amaçlar İçin İşlenmesi

GPDR'ın 5/1-b ve KVKK'nın 4/2-c hükümleri, kişisel verilerin belirli, açık ve meşru amaçlarla toplanması ve işlenmesinin önemini vurgular. Kişisel veriler, başlangıçta belirli amaçlar doğrultusunda toplanmalı ve bu amaçlar haricinde başka şekillerde işleme faaliyetine tâbi tutulmamalıdır. Bu hükümler, kişisel verilerin korunması ve veri işleme faaliyetlerinin şeffaf ve meşru bir şekilde yürütülmesi için önemli kuralları içermektedir.[187]

Amacın meşru olması ifadesinden, kişisel verilerin işlendiği hizmet veya işle bağlantılı ve bu amaçlar için gerekli olması anlaşılmaktadır. Kişisel verileri işleme amaçlarını sadece veri sorumlusu bilmemeli veya tahmin etmemelidir; aksi takdirde bu ilkeye aykırılık meydana gelecektir. Bu sebeple kişisel veri işleme amaçları açık rıza, aydınlatma, ilgili kişinin başvurularını cevaplama, Veri Sorumluları Siciline kayıt gibi hukuki işlemlerde belirlilik ve açıklık ilkesine uygun şekilde açıklanmalıdır. Bu süreçte hukuki ve teknik ifadelerden kaçınılarak, anlaşılması zor ifadelerden uzak durulmalıdır. Bu yaklaşım aynı zamanda dürüstlük ilkesine uyum açısından da oldukça mühimdir.[188]

---

184 Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin Korunmasına İlişkin Bankacılık Sektörü İyi Uygulamalar Rehberi*, (Ankara: KVKK Yayınları, Temmuz 2022), 90; Kişisel Verileri Koruma Kurumu, Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler Rehberi, 6.

185 Küzeci, *Kişisel Verilerin Korunması,* 244.

186 Dülger, *Kişisel Verilerin Korunması,* 293.

187 Yücedağ, "Kişisel Verilerin Korunması", 52.

188 "Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler", 9.

Amacın sınırlandırılması ilkesi, veri koruma düzenlemelerinde mühim bir rol oynar ve çoğu zaman diğer ilkelere temel bir dayanak oluşturur. İşlemenin, kişisel verilerin belirli, açık ve meşru amaçlarla toplanmasına ve kullanılmasına uygun olup olmadığı değerlendirmesi, işlemin amacına göre yapılır. Diğer bir ifadeyle verilerin nasıl işlendiği ve kullanıldığı, başlangıçta belirlenen amaca uygun olmalıdır. Bu sayede kişisel verilerin korunması ve veri işleme faaliyetlerinin yasal ve şeffaf bir biçimde sürdürülmesi sağlanır. Amacın sınırlandırılması ilkesi, veri koruma düzenlemelerinin temel prensibini oluşturur ve veri işlemenin etik ve hukuki çerçevede gerçekleştirilmesine önemli katkı sağlar.

2.1.1.4. Verilerin İşlendikleri Amaçla Bağlantılı, Sınırlı ve Ölçülü Olması

Verilerin amaca bağlı, sınırlı ve ölçülü olma ilkesi GDPR'da olduğu gibi "veri minimizasyonu" şeklinde de ifade edilmektedir. Veri minimizasyonu ilkesi, veri sorumlusunun ihtiyacı olandan çok veri temin etmemesi ve veri işleme amacına ulaşabilmek adına hangi verilerin işlenmesinin zorunlu olduğunu analiz etmesi; zorunlu olmayan veriler açısından yani kişisel verileri kullanmadan veya yalnızca bir kısmını kullanarak amacına ulaşmasının olası olması durumunda da ilk olarak bu yolu tercih etmesi gerektiği gibi konuları ihtiva etmektedir.[189] Bu ilkeye göre veri işleme faaliyetlerinde daha sonra doğması muhtemel ihtiyaçların giderilmesine yönelik veri işlenmesi yoluna gidilmemeli; veri işleme ile gerçekleştirilmesi istenen amaç arasında makul bir denge kurulmalı; başka bir deyişle kişisel veri işleme faaliyetinin amacı gerçekleştirmeye yetecek ölçüde olması gereklidir.[190] Ancak verinin işlenmeden önce belirtilen amacından başka amaçlarla kullanılmasında amaca bağlılık ilkesi sorun oluşturacaktır. Bu halde veri sorumlusu ya kişisel verilerin işlenmesi için kural olarak zorunlu olan ilgili kişinin açık rızasını tekrar alacak ya da md. 5/2 ve 6/4 kapsamında haklı sebeplerin uygulanabilir olup olmadığını değerlendirecektir. Bu konuda açıkça bir kanuni düzenleme mevcut değildir.[191]

189 Develioğlu, *6698 sayılı Kişisel,* 47; Yücedağ, "Kişisel Verilerin Korunması", 59.
190 "Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler", 11.
191 Çekin, *Avrupa Birliği Hukukuyla, 67.*

2.1.1.5.Verilerin Sınırlı Süre ile Muhafaza Edilmesi

Verilerin sınırlı süre ile muhafaza edilmesi ilkesi, veri minimizasyonu ilkesinin zamanla ilgili uygulama biçimidir.[192] Zira veri güvenliğinin sağlanmasının oldukça zor olması nedeniyle kişisel verilerin tutulması başlı başına bir risk oluşturmakta iken gerekli süre dışında verilerin tutulması kişisel verilerin korunması hukukunun temelini sağlayan bireysel özerklik, özel hayatın gizliliği ve kişinin maddi ve manevi bütünlüğü gibi değerlerinin zedelenmesine neden olabilir.[193]

Kişisel Verileri Koruma Kurumu'nun belirttiği üzere "*Kişisel verilerin "amaçla sınırlılık ilkesi" nin bir gereği olarak işlendikleri amaç için gerekli olan süreye uygun olarak muhafaza edilmesi gerekir. Kişisel verilerin saklanması için amaçla sınırlılık ilkesi uyarınca veri sorumlusu tarafından belirlenen saklama sürelerinin yanı sıra, veri sorumlusunun tabi olduğu ilgili mevzuat kapsamında da belirlenmiş saklama süreleri mevcuttur. Buna göre; veri sorumluları, ilgili kişisel veriler için mevzuatta öngörülmüş bir süre varsa bu süreye uyacak; eğer böyle bir süre öngörülmemişse verileri ancak işlendikleri amaç için gerekli olan süre kadar saklayabilecektir. Bir verinin daha fazla saklanması için geçerli bir sebep bulunmaması halinde, o veri silinecek, yok edilecek veya anonim hale getirilecektir. İleride tekrar kullanılabileceği düşünülerek ya da herhangi bir başka gerekçe ile kişisel verilerin muhafaza edilmesi yoluna gidilemeyecektir*."[194]

2.1.2. Veri Güvenliği İlkeleri

Dijital ortamlarda verilerin oluşturulması ve depolanması, verilere izinsiz erişimi kolaylaştırarak yasa dışı faaliyetlere zemin hazırlayabilir. Bu durum, çeşitli boyutlarda ciddiye alınması gereken bir konu olarak öne çıkmakta ve veri simsarlığı, siber saldırı, siber savaş, siber casusluk gibi kavramlarla tanımlanan tehditlerle ilişkilendirilmektedir. Bu bağlamda veri sorumluları arasındaki veri paylaşımında, veri entegrasyonu ve kullanıma hazır verilerde, bulut altyapısında verilerin depolanmasında, veri madenciliği, makine öğrenmesi ve yapay zekâ teknolojilerinin kullanımıyla ortaya çıkan riskler ve veriler üzerinde geliştirilen iş birliklerinde özel çıkarların göze çarpması ve Tablo 2.1'de

192 Yücedağ, "Kişisel Verilerin Korunması", 52.
193 Küzeci, *Kişisel Verilerin Korunması,* 245. Dülger, *Kişisel Verilerin Korunması,* 300-301.
194 "Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler", 13.

gösterilen hallerde kişisel verilerin gizliliği ve güvenliği daha da önem kazanmaktadır. Dolayısıyla kişisel verilerin korunması ve güvenliğinin sağlanması, veri paylaşımı ve kullanım süreçlerinin etik, yasal ve güvenli bir şekilde gerçekleşmesi için önemlidir.[195]

Tablo 2.1. Veri Güvenliğinde Etkili Olan Etkenler[196]

Verilerin Güvenliği	**Teknolojik Etkenler (altyapı)** • Verinin ortaya çıkmasını sağlayan teknolojilerin (RFID, SCADA, GPS, Bluetooth, sensörler, mobil, vb.) güvenlik altyapı noksanlığı • Vaktinde güncelleme ve bakım yapılmaması • Birbirine bağlı olma etkisi **Yönetimsel Etkenler** • Bilgi eksikliği nedeniyle gereken özenin verilmemesi, • Gereken insan kaynağının olmaması ve insan hatası • Örgütlenmiş birimin olmaması, • Dış kaynaklar sebebiyle (rekabet koşulları sebebiyle iş ortaklarının veri güvenliğine gereken önemi vermemesi gibi) • Güvenlik sistemlerinin teste tabi tutulması. **Sosyo-ekonomik Etkenler** • Veriyi üretenlerin farkındalık düzeyinin düşük olması, • Kaynak kısıtlılığı ve maliyetlerin fazlalığı
Verilerin Gizliliği	• Anonimleştirilen verilerin kişilerle bağlantı kurma potansiyeli (yetersiz anonimleştirme tedbiri) • Büyük verinin amacına uygun olmayan şekilde kullanılması • Verilerden yapılacak çıkarımların şeffaflık ilkesine aykırı yapılması (ayrımcılığın oluşması gibi) ve hatalı sonuçların bulunma olasılığı • Tüm verilerin elde edilme olasılığı ve veri minimizasyonundan uzaklaşılması • Verileri kötü niyetli kullanma ve üçüncü kişilerle izinsiz paylaşma

GDPR'da düzenlenen veri güvenliği ilkesine göre veri sorumlusu, işleme faaliyetinin doğası, kapsamı, amacı, teknolojik olanakları, maliyeti ve gerçek kişilerin haklarına etkileri gibi unsurları dikkate alarak, veri koruma ilkelerini etkili bir şekilde uygulamalıdır. Bu uygulama, işleme yöntemi belirlenirken ve işleme faaliyeti sırasında olmak üzere her iki aşamada da geçerlidir. Bu çerçevede, veri sorumlusu, işleme faaliyetinin gerçek kişilerin haklarına ve özgürlüklerine olası etkilerini ve riskleri

195 Levent Memiş ve Melikali Güç, "Akıllı Kentlerde Verinin Gizliliği ve Güvenliği: İlkeler ve Yaklaşımlar", *Güvenlik Bilimleri Dergisi*, UGK Özel Sayısı (Şubat 2020), 95-112. 96. DOI:10.28956/gbd.695936.

196 Memiş ve Güç, "Akıllı Kentlerde Verinin", 102.

değerlendirmelidir. Bu riskler, yetkisiz veya yasal olmayan veri işlemeye karşı koruma, ayrıca yanlışlıkla veri kaybı, imha ya da tahribata karşı önlemleri içerebilir. Veri koruma ilkelerinin etkili bir biçimde uygulanmasını teminen veri sorumlusu, uygun teknik ve organizasyonel önlemleri almalıdır. Bu tedbirler, veri güvenliğini artırmak ve veri sahiplerinin haklarını korumak amacıyla tasarlanmalıdır.[197] Örneğin, GDPR'ın 32. maddesi[198] uyarınca, veri sorumlusunun kişisel verilerin şifrelenmesi ya da kişisel verilere maskeleme/takma ad vermek için tedbirler alması gerekmektedir.[199]

Türk hukukunda ise veri güvenliği KVKK'nın 12. maddesinde "veri güvenliğine ilişkin yükümlülükler" şeklinde düzenlenmiştir. Kanun'da GDPR'daki detaylı düzenlemenin aksine veri sorumlusunun yükümlülükleri belirlenmiş, veri sorumlusunun *"kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek, kişisel verilerin muhafazasını sağlamak"* ile yükümlü olduğu hüküm altına alınmıştır. Kişisel Verileri Koruma Kurumu tarafından kişisel verilerin işlenme aşamalarında veri sorumlularının alması gereken teknik ve idari önlemler hususunda uygulamada netlik sağlanması ve uygulama açısından iyi örneklerin oluşturması adına Kişisel Veri Güvenliği Rehberi hazırlanmıştır.[200] Rehberde belirtilen veri güvenliğine ilişkin alınacak tedbirlerin; her veri sorumlusunun kendi organizasyonel yapısına, faaliyet alanına ve karşılaştığı risklere, şirketin büyüklüğüne, iş hacmine, korunan kişisel verinin niteliğine ve Tablo 2.1'de yer alan faktörlerin etkilerini sonlandırmaya yönelik unsurlara uygun olması gerekmektedir. Bu sebeple veri güvenliğinin sağlanmasına yönelik tek bir model belirlenmesi mümkün olmamaktadır.[201]

Bununla birlikte genel kabul görmüş veri güvenliği ilkeleri şu şekilde sıralanabilir:[202]

---

197 Dülger, "Avrupa Birliği Genel", 106; Aydın, *AİHM İçtihatları Bağlamında*, 121-122.

198 Art. 32 GDPR "Security of processing".

199 Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, "Chatbot Uygulaması ve ChatGPT Örneği Değerlendirme Raporu", 33, (E.T. 01.02.2024), https://cbddo.gov.tr/SharedFolderServer/Genel/21.Chatbot-Uygulamas%C4%B1-ve-ChatGPT-%C3%96rne%C4%9Fi-De%C4%9Ferlendirme-Raporu.pdf ; Dülger, "Avrupa Birliği Genel", 106.

200 Kişisel Verileri Koruma Kurumu, *Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler*), (Ankara: KVKK Yayınları, Ocak 2018), (E.T. 10.12.2023) https://www.kvkk.gov.tr/SharedFolderServer/-CMSFiles/7512d0d4-f345-41cb-bc5b-8d5cf125e3a1.pdf

201 "Veri Güvenliğine İlişkin Yükümlülükler", (E.T. 09.08.2023), https://www.kvkk.gov.tr/Icerik/2040/-Veri-Guvenligine-Iliskin-Yukumlulukler

202 Onur Korucu, *Veri Güvenliğinin İyileştirilmesinde Küresel Standart, Çerçeve ve En İyi Uygulamaların Hukuki Uyuma Desteği*, (Ankara: Adalet Yayınevi, 2021), 45; aynı yönde bkz: Gündüz, *Uluslararası İnsan Hakları,* 49.

1. **Verilerin Güvenli Ortamda Kullanılması:** Kişisel veya hassas verilerin, güvenli bir çevrede işlenmesi ve saklanması, veri güvenliği açısından temel bir ilkedir. Bu, verilerin yetkisiz erişimden, veri kaybından veya kötü niyetli kullanımdan korunmasını içerir.

2. **Yetkisiz Erişime ve Suistimallere Karşı Koruma:** Verilere yetkisiz erişimi engellemek ve veri suistimallerini önlemek, veri güvenliği politikalarının merkezinde yer alır. Bu, güçlü kimlik doğrulama, şifreleme ve güvenlik yazılımları kullanımını içerir.

3. **Farkındalık ve Eğitim:** Tüm kullanıcıların veri güvenliği politikalarına tam anlamıyla uymalarını sağlamak için farkındalık yaratmak ve eğitim vermek önemlidir. Çalışanların gizliliğinin ve veri güvenliğinin neden önemli olduğunu anlamaları gerekmektedir.

4. **Veri İhlali Bildirimleri:** Olası veri ihlallerini tespit etmek ve bunları hızla bildirmek için uygun iletişim kanallarının oluşturulması büyük bir önem taşır. Bu, etkili bir yanıtın hızlı bir şekilde sağlanmasına yardımcı olur.

5. **Düzenli Denetim ve İyileştirme:** Veri güvenliğinin sürekli olarak iyileştirilmesi için düzenli denetimler ve güvenlik açıklarının giderilmesi çalışmaları önemlidir. Bu, organizasyonun güvenlik politikalarının ve uygulamalarının sürekli olarak gözden geçirilmesini sağlar.

2.1.3. Veri İşleme İzni ve Özel Kategorilerdeki Veriler

2.1.3.1. Genel Olarak

Kişisel verilerin korunması hakkı ile verilerin işlenmesi hususunda koruma sağlanması amaçlanmaktadır. Ancak bu hak, kişisel veri sahibi olan ilgili kişiye ait verilerin, kati surette işlenmeyeceği, başkalarının erişimine açılmayacağı anlamına da gelmemektedir.[203]

[203] Küçük, "1982 Anayasası'ndaki Temel" 45.

2.1.3.2. Açık Rıza ve Hukuka Uygunluk Sebepleri

Kişisel veriler, kural olarak kişisel veri sahibinin bu doğrultuda vereceği açık rızası ile hukuka uygun şekilde işlenebilir. Genel kurala getirilen istisna haller ile de veri sahibinin açık rızasının olması şartı kaldırılarak kişisel verilerin korunması hakkının sınırlandığı görülmektedir. Bu istisna haller KVKK'da düzenlenmiştir. Buna göre:

"*a) Kanunlarda açıkça öngörülmesi.*

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

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

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

d) İlgili kişinin kendisi tarafından alenileştirilmiş olması.

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

f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması (KVKK md. 5/2)" hallerinden birinin yahut birkaçının bulunması halinde kişisel veriler, ilgilisinin açık rızası olmasa da işlenebilecektir. 1982 Anayasasının 20/3 maddesinde düzenlenen "*kişisel veriler ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin sınırlanmasına ilişkin esas ve usuller kanunla düzenlenir."* hükmü ile sınırlama rejimi olarak basit kanun kaydı benimsenmiştir.[204]

2.1.3.3. Özel Kategorilerdeki Veriler

Kural olarak özel nitelikli (hassas veriler) kişisel verilerin kişilerin açık rızası olmadan işlenmesi mümkün değilken, KVKK'nın 6/3. maddesinde sayılan "ağırlaştırılmış hukuka

[204] Küçük, "1982 Anayasası'ndaki Temel", 48.

uygunluk hallerinin"[205] mevcut olması durumunda açık rıza olmadan da işleme faaliyetinde bulunulması hukuka aykırılık oluşturmayacaktır:

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

Esasında 6. maddede belirtilen hukuka uygunluk sebeplerinin gerçekleşmiş olmasıyla, veri işleme açısından kesin işlem yasağının kalktığı kabul edilebilir. Zira Madde 29 Çalışma Grubu[206] tarafından önerilen yaklaşıma ve 06/2014 numaralı metinde Grubun belirttiği görüşe göre bahsi geçen hukuka uygunluk sebebinin maksadı ve sunduğu korumayı dikkate alarak, genel hukuka uygunluk nedenlerinin ayrıca uygulanıp uygulanmamasının belirlenmesi gerekmektedir. Başka bir ifade ile KVKK'nın 6/3. maddesinin, KVKK'nın 5. maddesindeki hukuka uygunluk nedenleri ile beraber uygulanması gerekmektedir. Daha detaylı ifade etmek gerekirse KVKK'nın 6/3. maddesi, sağlık ve cinsel hayata ilişkin kişisel verilerin belirli amaçlarla işlenmesine izin verir. Belirtilen amaçlar "kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi" konularını kapsar. Bu istisna hükmü, KVKK md. 5/1 hükmünde belirtilen açık rıza şartını gerektirmez. Öte yandan KVKK'nın 5. maddesinde düzenlenen diğer hukuka uygunluk nedenlerinden biri, belirtilen şartlara ek olarak gerçekleşmelidir. Yani, sağlık ve cinsel hayat verilerinden herhangi birinin sağlık hizmetleri ile finansmanının planlanması ve yönetimi, koruyucu hekimlik, kamu sağlığının korunması, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi gibi amaçlarla işlenmesi durumunda, KVKK'nın 5/2. maddesinde belirtilen hukuka uygunluk nedenlerinden en az birinin de

---

205 Develioğlu, *6698 sayılı Kişisel,* 69.

206 Madde 29 Çalışma Grubu, 95/46/EC sayılı Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Hakkındaki 24 Ekim 1995 tarihli Avrupa Parlamentosu ve Avrupa Birliği Konseyi Direktifi'nin 29. maddesi gereğince kurulmuştur. Verilerin korunması ve mahremiyeti üzerine bağımsız bir danışma kuruludur. Görevleri 95/46/EC sayılı Direktif'in 30. maddesinde ve 2002/58/EC sayılı Direktif'in 15. maddesinde tanımlanmıştır: (E.T. 05.07.2023), https://kisiselveriihlali.com/Anasayfa/3316/

geçerli olması gerekmektedir.[207] Bu yönde 7499 sayılı Kanun'un 33. maddesiyle 1/6/2024 tarihinde yürürlüğe giren bu maddede değişiklikler yapılmıştır.[208] Değişiklik ile birlikte 1/6/2024 tarihinden itibaren sağlık ve cinsel hayat verileri de dahil olmak üzere bütün özel nitelikli kişisel verilerin işlenmesi;

"*a) İlgili kişinin açık rızasının olması,*

b) Kanunlarda açıkça öngörülmesi,

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

ç) İlgili kişinin alenileştirdiği kişisel verilere ilişkin ve alenileştirme iradesine uygun olması,

d) Bir hakkın tesisi, kullanılması veya korunması için zorunlu olması,

e) Sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlarca, kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi ile sağlık hizmetlerinin planlanması, yönetimi ve finansmanı amacıyla gerekli olması,

f) İstihdam, iş sağlığı ve güvenliği, sosyal güvenlik, sosyal hizmetler ve sosyal yardım alanlarındaki hukuki yükümlülüklerin yerine getirilmesi için zorunlu olması,

g) Siyasi, felsefi, dini veya sendikal amaçlarla kurulan vakıf, dernek ve diğer kâr amacı gütmeyen kuruluş ya da oluşumların, tâbi oldukları mevzuata ve amaçlarına uygun olmak, faaliyet alanlarıyla sınırlı olmak ve üçüncü kişilere açıklanmamak kaydıyla; mevcut veya eski üyelerine ve mensuplarına veyahut bu kuruluş ve oluşumlarla düzenli olarak temasta olan kişilere yönelik olması," halinde mümkündür.

---

[207] Nafiye Yücedağ Göztepe, "Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu'nun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri", *İstanbul Hukuk Mecmuası*, 75/2 (2017): 765-790, 772,773. (E.T. 24.09.2023), www.idealonline.com.tr

[208] 12/3/2024 tarihli ve 32487 sayılı Resmî Gazete' de yayımlanmıştır. (E.T. 12.03.2024), https://www.resmi gazete.gov.tr/eskiler/2024/03/20240312-1.htm

Hassas verilerin işlenmesi için özel düzenlemeler varsa, bu düzenlemelerin gerektirdiği hukuka uygunluk sebeplerine uyulmalıdır. Bu husus, aynı zamanda genel hukuka uygunluk sebeplerinin de göz ardı edilemeyeceği anlamına gelir. Örneğin, hassas kişisel verilerden olan sağlık verilerinin işlenmesi, saklanması, aktarılması, silinmesi gibi veri işleme süreçlerinde Özel Hastaneler Yönetmeliği, Hasta Hakları Yönetmeliği, Kişisel Sağlık Verileri Hakkında Yönetmelik gibi özel hükümler içeren düzenlemelerin de dikkate alınması gerekmektedir.[209]

2.2. Kişisel Verilerin Korunmasına İlişkin Denetim Sistemi

2.2.1. Genel Olarak

Genel anlamıyla kişisel verilerin korunması, hak ehliyetini haiz gerçek kişilere ait kişisel verilerin işlenmesini kapsayan tüm faaliyetlerin denetim altına alınması, bunların düzenli şekilde yürütülmesi ve yönetilmesi; anayasal hak ve özgürlüklerin, kişilik haklarının, mahremiyet gibi hakların korunması bağlamında gerçekleştirilen idari, hukuki ve teknik faaliyetler olarak ifade edilebilir.[210] Kişisel verilerin korunmasına dair ilkelerin ve kuralların tatbiki ise kişilerin haklarına saygı gösterilmesi ve korunması hususunda temel faktör olduğu için kişisel verilerin korunması için getirilen kriterlerin doğru ve başarılı şekilde tatbik edilmesinde bağımsız denetim organlarının rolü oldukça büyük öneme sahiptir.[211]

Kişisel verilerin korunması ve işlenmesi arasında dengenin oluşturulması için dinamik bir müeyyide rejiminin geliştirilmesi zorunludur. Kişisel verilerin korunması hakkı ile veri temelli ekonomi arasında bir denge kurulması için de müeyyidelerin en son süreçte gündeme gelmesi gerekmektedir. Zararın giderilmesi durumunda ayrıca bağımsız bir idari yaptırım uygulatılmaması, idari yaptırımların en az ve en çok sınırı arasındaki makas dikkate alınarak hukuki belirlilik sağlamak adına belirlenen en düşük ve en yüksek aralıklarda yaptırım uygulanmalıdır. Yaptırım uygularken de tatbik edilecek nesnel ölçütlerin belirlenmesi, ağırlaştırıcı ve hafifleştirici ögelerin açıkça düzenlenmesi,

---

209 Fatih Birtek, "Kişisel Sağlık Verilerinin Silinmesi", içinde *Kişisel Verilerin Korunması Hukuku ve Bilgi Edinme Hukuku: Çeşitli Açılardan Bakış*, ed. Cemil Kaya, (İstanbul: On İki Levha Yayıncılık, Ağustos 2023), 499-500.

210 Turan, *Karşılaştırmalı Hukukta Kişisel*, 53.

211 Cemal Başar, *Türk İdare Hukuku ve Avrupa Birliği Hukuku Işığında Kişisel Verilerin Korunması*, (İstanbul: On İki Levha Yayınevi, 2020), 229.

mutlaka yaptırım uygulanması gerekli olduğu hallerde veri sorumlusuna daha etkili bir savunma hakkı verilmesi, sözlü savunma gibi usullerin tanınması, kademeli yaptırımlar uygulanması, idari istikrarı takip açısından idari yaptırım kararlarının gerekçeli ve detaylıca düzenlenmesi gerekmektedir.[212]

Türk veri koruma hukuku açısından kişisel verilerin korunmasına yönelik denetim mekanizmasının oluşturulmasında hukuki, teknolojik, ekonomik ve siyasi birtakım nedenler etkili olmuştur. Türkiye'nin de tarafı olduğu "CETS No:181" hükümlerine göre protokolde belirtilen prensiplerin sözleşmenin tarafı olan ülkelerin iç hukuklarında bulunup bulunmadığını denetlemekle görevli ve tam bağımsız denetleyici kurumlara ihtiyaç olduğu hüküm altına alınmıştır.[213] Yine 95/46/EC sayılı Direktif'te[214] de kişisel verilerin işlenmesine ilişkin ilkelerin icrasını takip etmek ve yönlendirmek adına işlevsel şekilde bağımsız olarak görev yapacak bir kurum oluşturulması öngörülmüştür.[215] Bu hukuki ve siyasi gelişmeler neticesinde Türkiye'nin Avrupa Birliği (AB) adaylık sürecinde idari organlarının ve hukuki yapısının AB şartnamesine uygunluğunun bir gereği olarak, kişisel verilerin korunması için bir denetim gücüne ihtiyaç hasıl olmuştur.[216]

Bir denetim mekanizması oluşturulması ihtiyacının sebepleri arasında sağlık verilerinin toplanması, güvenlik soruşturmaları, parmak izi toplanması, kamu arşiv kayıtlarının tutulması, telefon kayıtlarının tutulması, gibi hususlarda, idari organlarca kişisel verilerin korunması açısından birçok sorun yaşanması yatmaktadır.[217] Ayrıca kişisel bilgilerin sızdırılmasıyla ilgili Danıştay'a açılan davaların dosyalarında, bu sorunlarla mücadele edecek bir kurumun gerekliliğinin olduğunun belirtilmiş olması da bu sebepler arasında

---

212 Mehmet Bedii Kaya," Kişisel Verilerin İşlenmesi ve Korunması Arasında Denge". İçinde Güncel Gelişmeler Işığında Kişisel Verilerin Korunması Hukuku Marmara Hukuk Bilimsel Toplantılar Serisi – I. Editörler Leyla Keser Berber ve Ali Cem Bilgili. 33-68. İstanbul: On İki Levha Yayıncılık, 2020. 63.

213 Esin Gürsel, Fatih Düğmeci, "Yapısal Anlamda Türkiye Kişisel Verileri Koruma Kurumu'na İlişkin Bir Değerlendirme", *R&S- Research Studies Anatolia Journal*, 1/2 (2018): 318-329, 319, (E.T. 04.06.2023), https://dergipark.org.tr/tr/download/article-file/507084

214 95/46/EC sayılı Direktif yerini 25.05.2018 tarihinden sonra Avrupa Birliği "Genel Veri Koruması Tüzüğü" (GDPR)'ne bırakmıştır.

215 Başar, *Türk İdare Hukuku*, 235; Gürsel ve Düğmeci, "Yapısal Anlamda Türkiye", 319.

216 İsmail Sevinç, Niyazi Karabulut, "A Review on the Personal Data Protectıon Authorıty of Turkey", *Akademik Hassasiyetler*, 7/13 (2020), 449-472, 457. (E.T.02.09.2022), https://search.trdizin.gov.tr/tr/yayin/detay/ 377424/a-review-on-the-personal-data-protection-authority-of-turkey

217 Akgül, *Danıştay ve Avrupa İnsan,* 304,337.

yer almaktadır. Bu problemlerin teknolojik gelişmelerle birlikte ortadan kaldırılması ve kişisel verilerin bu sorunlar dikkate alınarak korunması amacı öngörülmüştür.[218]

Bu doğrultuda Türk hukuk sisteminde Avrupa Birliği üyesi devletlerin veri koruma kurullarının görevlerinde bağımsız otoriteler olarak kurulduğu ve uluslararası metinler dikkate alınarak kişisel veri işleme faaliyetlerine ilişkin denetim bağlamında Kişisel Verileri Koruma Kurumu kurulmuştur.[219] Bu doğrultuda kişisel verilerin korunmasına ilişkin denetleme sistemi Kişisel Verileri Koruma Kurumu ve Kişisel Verileri Koruma Kurulu olarak iki ayrı yapıdan oluşmaktadır.[220]

2.2.2. Avrupa Birliği Sistemi ve Denetim Mekanizması

GDPR (Genel Veri Koruma Tüzüğü[221]), Tüzük'ün icrası ile bunun Avrupa Birliği içerisinde tutarlı biçimde gerçekleştirilmesini sağlamak amacıyla farklı kurumlar kurulmasını ve bu kurumlar arasında iş birliğinin hayata geçirilmesini öngörmektedir. Bunlardan Avrupa Veri Koruma Kurulu, hukukî kişiliği haiz bir AB kuruluşu olarak tanımlanmıştır. Ek olarak her bir üye devletin bir veya daha fazla bağımsız denetim makamı oluşturması düzenlenmiştir.[222] Denetim makamı da *"GDPR'ın 51. maddesi uyarınca bir Üye Devlet tarafından kurulan bağımsız bir kamu makamı"* olarak tanımlanmıştır.[223] O halde 51. madde doğrultusunda denetim makamına ilişkin genel bilgiler şu şekilde sıralanabilir:

1. Denetim Makamının Temel Görevleri ve Sorumlulukları:

Her üye devlet, gerçek kişilerin temel haklarını ve özgürlüklerini korumak için kişisel verilerin serbest akışını kolaylaştırmak adına bir veya birden fazla bağımsız kamu makamını atar, bu makamlara "denetim makamı" denir.

---

218 Sevinç ve Karabulut, "A Review on the Personal", 457.
219 Başar, *Türk İdare Hukuku,* 235.
220 Sinem Göçmen Uyarer, *Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması*, (Ankara: Seçkin Yayınevi, 2020), 149
221 AB Başkanlığı, "95/46/EC sayılı Direktif'i yürürlükten kaldıran, gerçek kişilerin kişisel verilerin işlenmesi bakımından korunması ve bu tür verilerin serbest dolaşımı hakkında 27 Nisan 2016 tarihli ve (AB) 2016/679 sayılı Avrupa Parlamentosu ve Konsey Tüzüğü (Genel Veri Koruma Tüzüğü) (AEA ile ilişkili metin)" (E.T. 12.12.2023), https://www.ab.gov.tr/siteimages/resimler/Nihai-ABB-HCDB-GDPR.pdf .
222 Develioğlu, *6698 sayılı Kişisel,* 137
223 Genel Veri Koruma Tüzüğü, md.4/21.

2. Denetim Makamlarının İş Birliği ve Uyum Çabaları:

Her denetim makamı, bu düzenlemenin birliğin içinde tutarlı bir şekilde uygulanmasına katkıda bulunmak için çaba gösterir.

Bu hedef doğrultusunda, denetim makamları "İşbirliği ve Tutarlık (Bölüm VII)" çerçevesinde birbirleriyle ve Komisyon ile iş birliği yapar.

3. Birden Fazla Denetim Makamının Koordinasyonu:

Bir üye devlette birden fazla denetim makamı bulunuyorsa, ilgili üye devlet, bu makamlardan bir tanesini Kurulda temsil edecek denetim makamı olarak belirler.

Diğer denetim makamları için ise 63. maddeye[224] atıfta bulunulan tutarlılık mekanizmasına uyumu sağlamak üzere uygun bir mekanizma belirlenir.

AB sistemi içerisinde denetim makamlarının görevleri ise GDPR'ın 57. maddesinde ifade edilmiştir. Denetim makamlarının görevleri özetle şu şekilde ifade edilebilir:

- *"Tüzük'ün uygulanmasını gözetmek ve temin etmek,*
- *Riskler, kurallar, teminatlar ve haklar konusunda kamu farkındalığını artırmak,*
- *Gerçek kişilerin kişisel verilere ilişkin hak ve özgürlükleri konusunda danışmanlık sağlamak ve veri sorumlularını, işleyenleri yükümlülükleri konusunda bilinçlendirmek,*
- *Diğer denetim makamlarıyla işbirliği yaparak Tüzük'ün tutarlı bir şekilde uygulanmasını sağlamak,*
- *Kişisel veri ihlali şikayetlerini araştırmak, süreç ve sonuçlar hakkında bilgi sunmak,*
- *Tüzük'ün uygulanmasında tutarlılık sağlamak için diğer denetim makamları ile*

[224] Madde 63- Tutarlılık: Bu Tüzük'ün Birlik genelinde tutarlı bir şekilde uygulanmasına katkıda bulunulması amacıyla, denetim makamları, bu Kesimde belirtilen tutarlılık mekanizması vasıtasıyla, birbirleriyle ve gerekli olduğu hallerde, Komisyon ile iş birliği yapar.

işbirliği yapmak,

- *Kişisel verilerin korunmasına ilişkin araştırmalar yapmak,*
- *Standart sözleşme hükümlerini belirlemek, veri koruması etki değerlendirmesi gereklerini listelemek,*
- *İşleme işlemleri hakkında tavsiye vermek, davranış kuralları oluşturulmasını teşvik etmek, fikir bildirmek ve kuralları tasdik etmek,*
- *Sertifikasyon mekanizmalarını teşvik etmek, sertifikasyonları değerlendirmek ve akreditasyon süreçlerini yönetmek,*
- *Avrupa Veri Koruma Kurulu'nun faaliyetlerine katkı sağlamak, Tüzük ihlalleri ile uygulanan önemlere dair kayıtları tutmak,*
- *Sözleşmesel hüküm ve düzenlemelere izin vermek, bağlayıcı kurumsal kuralları tasdik etmek,*
- *Kişisel verilerin korunmasıyla ilgili diğer görevleri yerine getirmek"*

GDPR ile denetim otoritelerine araştırma, düzeltici ve istişari yetki çatısı altında pek çok yetki verilmiş; denetim makamları belirtilen çatı yetkilerin altında oldukça fazla yetki ile donatılmıştır. GDPR 58. maddede sayılan yetkiler şunları içerir:

Tablo 2.2. GDPR Uyarınca Denetim Makamlarının Yetkileri

Yetki Türü	Araştırma Yetkileri	Düzeltici Yetkiler	İstişarî Yetkiler
1. Veri Toplama	Veri sorumlularına, işleyenlere veya temsilcilere, gerekli bilgileri sağlamalarını emretme.	Tüzük'ü ihlal edebilecek veri sorumlularını veya işleyenleri uyarma.	Veri sorumlularına tavsiye (ön görüş) verme.
2. Denetleme ve Değerlendirme	Kişisel veri denetimleri yapma.	İşleme faaliyetleri Tüzük'ü ihlal eden veri sorumlularına veya işleyenlere kınama verme.	Devlet makamlarına, diğer kuruluşlara ve kamuya re'sen veya talep üzerine görüş bildirme.
3. Belgelendirme ve İhlal Bildirimi	Verilen sertifikaları değerlendirme.	Veri sorumlularına veya işleyenlere ilgili kişilerin taleplerine uymalarını emretme.	Kamu yararı için gerçekleştirilen görevin ifasına ilişkin işlemlerde ön görüşe başvurulması öngörülmüşse bu işlemelere izin verme.
4. İhlal Bildirimi ve Erişim Yetkisi	İhlal iddialarını veri sorumlusuna veya işleyene bildirme.	Veri sorumlularına veya işleyenlere, işleme faaliyetlerini belirli şekil ve sürede Tüzük'e uygun duruma getirmelerini emretme.	Taslak davranış kuralları hakkında fikir bildirme ve onaylama.
5. Veri Erişim ve Denetim	Veri sorumlusu veya işleyenden, görevlerinin ifası için gereken bütün kişisel veri ve bilgilere erişim elde etme.	Veri sorumlularına veri ihlallerini ilgili kişilere bildirmeyi emretme.	Sertifika kuruluşlarına akreditasyon verme
6. Hukuki Yetkilendirme ve İhtiyati Tedbirler	Birlik veya Üye Devlet hukukuna uygun şekilde veri sorumlusuna veya işleyene ait mekanlara ve kişisel veri işleme ekipmanlarına erişim elde etme.	İşleme yasağı gibi geçici veya kesin kısıtlamalara hükmetme.	Sertifika verme ve sertifika kriterlerini onaylama.
7. Özel Kurallar ve Gizlilik	Üye Devletler, belirli yetkileri kullanarak, meslekî veya benzer gizlilik yükümlülüğü altında olan veri sorumlularından veya işleyenlerden kişisel verilere erişim elde edilmesine özgü kurallar tesis etme	İlgili kişilerin düzeltme hakkı, silinme ve unutulma hakkı ile işlemenin sınırlandırılmasını talep hakkına ilişkin düzenlemelerin uygulanmasını ve bu kapsamda kişisel verilerin aktarıldığı kişilere bildirim yapılmasını emretme.	Standart kişisel verilerin korunması hükümleri öngörmek.
8.Hukuki Yaptırımlar ve Onay Yetkisi	İdari para cezasına hükmetme.	Sözleşmesel hükümleri onaylama.	
9. Uluslararası İlişkiler ve Anlaşmalar	Üçüncü ülke ya da uluslararası kuruluşta bulunan bir aktarılana veri akışının askıya alınmasını emretme.	İdari anlaşmaları onaylama.	
10. Kurumsal Kurallar ve Standardizasyon	Bağlayıcı kurumsal kuralları onaylama.		

Denetim otoritelerinin bu yetkileri, GDPR'nin gerekliliklerinin uygun bir şekilde uygulanmasını sağlayarak, kişisel verilerin işlenmesi ve korunması hususunda daha yüksek bir güvenlik düzeyi temin etmeyi amaçlamaktadır.

2.2.3. Türk Hukukunda Denetim Sistemi

Türk veri koruma hukukunda ilgili kişinin kişisel verisinin korunmasına yönelik hakları bu hususlarla ilgili temel kanun olan KVKK ile güvence altına alınmıştır. 6698 sayılı KVKK doğrultusunda öngörülen koruma sistemi kişisel verilerin idari yoldan korunmasıdır. Öte yandan Kanun, kendi içerisinde bir başvuru mekanizmasına ilişkin düzenlemeler yapmış olsa da kişisel verilerin korunması amacıyla genel hükümlere göre hak arama yolları da bulunmaktadır[225] ki bu yol yargısal yolla denetim usulünü içermektedir.

2.2.3.1. Kişisel Verilerin Yargısal Yolla Denetlenmesi

Kişisel verilerin korunması hakkına sahip olan kişi gerçek bir kişi olduğundan kişisel verilerin korunması hakkı ile bağlantılı birçok hakka sahip olmaktadır. Bu nedenle kişisel verilerin yalnızca idari denetim yoluyla ile korunması beklenmez. Nitekim KVKK'nın 14/3 maddesinde de *"kişilik hakları ihlal edilenlerin, genel hükümlere göre tazminat hakkı saklıdır."* hükmü ile yargısal yollara atıf yapılmıştır. 14. maddede sözü edilen genel hükümler, TMK'nın 24. ve 25. maddeleri ile TBK'nın 49. maddeleri ve devamında belirtilen hükümler[226] olup haksız fiil neticesinde zarara uğrayan kimse zararın tazminini isteyebilecektir.[227]

Veri sorumlusunun, veri işleyenin yahut kişisel veri ihlalini gerçekleştiren öznenin bir kamu kurum veya kuruluşu olması da mümkündür. Bu olasılıkta veri sorumlusu olan idarenin kişisel verilerin işlenmesine yönelik işlem ve eylemlerinin yasalara uygunluğu ve idarenin sorumluluğu ortaya çıkacaktır. İdare tarafından kişisel verilerin yasalara aykırı şekilde işlenmesi, bu işleme faaliyeti neticesinde ilgili kişinin maddi ve/veya

---

225 Samet Saygı, "6698 Sayılı Kanun'un Sistematiğinde Yargısal Başvuru Yolları", *Kişisel Verileri Koruma Dergisi.2020*, 2(2), 30-60. 38. (E.T. 10.02.2023), https://dergipark.org.tr/tr/pub/kvkd-/issue/58932/738180

226 Gürpınar, "Kişisel Verilerin Korunamamasından" 689.

227 Bu kapsamdaki detaylı açıklamalar "*1.2.2.4. Medeni Kanun Kapsamında Kişisel Verilerin Korunması*" ve "*3.1.2.1.6. Zararın Giderilmesini İsteme Hakkı"* başlığı altında yapıldığından işbu başlığa atıf yapmakla yetinmekteyiz.

manevi bir zararının meydana gelmesi, işleme faaliyeti ile zarar arasında uygun nedensellik bağı bulunması koşullarının varlığı halinde bu zarar nedeniyle idari mahkemelerde somut olayın şartlarına göre zararın tazmini istenebilecektir.[228] Zira burada idarenin hizmet kusurundan söz edilebilir.[229] Buna göre kişisel veriler bir idari işlem nedeniyle kanuna aykırı şekilde işlenmişse, ilgili kişinin bu idari işleme karşı dava açma süresi içinde iptal davası ikame etme olanağı vardır. Bununla birlikte bahsi geçen işlemden ya da işlemin icrasından uğranılan zararların tazmini, İdari Yargılama Usulü Kanunu'nun (İYUK) 12. maddesi doğrultusunda ikame edilecek tam yargı davası ile talep edilebilir. Öte yandan, ihlali meydana getiren vaka bir idari eylem nedeniyle doğmuşsa ilgili kişi, ilk olarak İYUK 13. madde uyarınca ilk olarak idareye başvuru yaparak zararının tazminini istemeli; bu talebin 30 gün içerisinde açıkça ya da 30 gün sonunda idarenin sükûtu sebebiyle zımnen reddedilmesinden sonra 60 günlük dava açma süresi içinde tam yargı davası açmalıdır.[230]

Kişisel verilerin özel hukuk ve idare hukuku ile korunmasının yeterli teminatı sağlamadığı kanaatine varan kanun koyucu ceza hukukunu devreye sokarak suç tanımları da yapmıştır. Böylelikle, kanun koyucu ceza hukukuna son çare (ultima raito) olarak başvurup bu hukuk dalının genel önleme amacından da faydalanarak kişisel verileri daha etkili biçimde koruma amacı gütmüştür.[231] Bu nedenle kişisel verilerin korunması açısından cezai denetim de mümkündür. Zira bir kişisel verinin suç konusu olma ihtimali de bulunmaktadır. TCK kapsamında "özel hayatın ve hayatın gizli alanına karşı suçlar" kapsamında 135. ve devamı maddelerinde kişisel verilerin ihlali halinde oluşabilecek suçlara ilişkin cezai müeyyideler öngörülmüştür.[232]

2.2.3.2. Kişisel Verilerin İdari Denetimi

Kişisel verilerin korunması sürecinde yargı dışı[233] denetim olarak da ifade edilen denetleme mekanizmalarının da işletilmesi mümkündür. Yargı dışı denetimin ilk

---

228 Akgül, *Danıştay ve Avrupa İnsan,* 263-272.
229 Gürpınar, "Kişisel Verilerin Korunamamasından", 694; Akgül, *Danıştay ve Avrupa İnsan*, 263,272.
230 Saygı, "*6698 Sayılı Kanun'un",* 39.
231 Zeynep T. Kangal, *Kişisel Verilerin Ceza ve Kabahatler Hukukunda Korunması*, (İstanbul: On İki Levha Yayıncılık, Eylül 2019), 53.
232 Bu kapsamdaki detaylı açıklamalara *"1.2.2.3. Ceza Kanunu Kapsamında Kişisel Verilerin Korunması"* başlığından bakılabilir.
233 Başar, *Türk İdare Hukuku*, 255.

basamağı ilgili kişinin kişisel verilerini işleyen veri sorumlusuna başvuru yaparak verileri üzerinde hakimiyet sağlamasıdır. Yargı dışı denetimin diğer bir basamağı ise kişisel verilerin korunmasına yönelik denetim yetkisini haiz olan Kişisel Verileri Koruma Kurumu tarafından yapılan idari denetimdir. İlgili kişi tarafından kişisel verilerinin idari yoldan denetlenmesine ilişkin yürütülecek süreç ve sonuçları ile Kurum'un denetleme süreçlerinden üçüncü bölümde bahsedileceğinden, konunun önemine binaen bu başlık altında idari denetimde yetkili olan Kişisel Verileri Koruma Kurumu ve Kişisel Verileri Koruma Kurulundan bahsedilecektir.

2.2.3.2.1. Kişisel Verileri Koruma Kurumu ve Görevleri

2.2.3.2.1.1. Genel Olarak

Kişisel verilerin işlenmesi sırasında, yasalara uygunluğun sağlanması ve koruma standartlarının yerine getirilip getirilmediğinin doğrulanması, bağımsız denetim organları veya başka ifadeyle veri koruma otoriteleri tarafından gerçekleştirilen kontrollerle sağlanır. Bu denetimler, bireylerin kişisel verilerinin güvende tutulmasını ve işlenmesinin yasal düzenlemelere uygunluğunu güvence altına alarak, gizlilik haklarının korunmasında önemli bir teminat oluşturur.

Ülkemizde kişisel verilerin korunması için bağımsız bir denetim makamı kurulmasının temeli olan hukuki düzenleme Türkiye'nin de tarafı olduğu Avrupa Konseyi'nin 108 sayılı sözleşmesidir. Sözleşme uyarınca, sözleşmede kabul edilen kişisel verileri koruma ilkelerinin Üye Devletlerin iç hukukunda uygulamaya konulması ve önlemlere uyulmasının sağlanmasını sağlamakla yükümlü bir veya daha fazla yetkili makamın tespit edilmesi ve bu denetleyici kurumların görevlerini tam bağımsızlıkla yürütmesi öngörülmüştür. Yine AB'nin 95/46/EC sayılı Direktif 'inin 28. maddesinde de benzerlik gösterir şekilde bağımsız bir denetim makamı öngörülmüştür.[234]

"Paris Prensipleri" olarak ifade edilen birtakım standartların yer aldığı Birleşmiş Milletler Genel Kurulu Kararı, Kişisel Verileri Koruma Kurumu'nun haiz olması gereken vasıfları

[234] Mutlu Kağıtçıoğlu. "Kişisel Verileri Koruma Kurumuna İdare Hukuku Çerçevesinden Bir Bakış", *İstanbul Kemerburgaz Üniversitesi Sosyal Bilimler Dergisi,* 1/2 (Kış 2016), 77-99, s. 94. (E.T. 03. 04.2022), https://dergipark.org.tr/tr/download/article-file/272994; Gürsel ve Düğmeci, "Yapısal Anlamda Türkiye", 319.

düzenleyen milletlerarası metindir. Kişisel verilerin korunmasına dair denetim kurumunu düzenleyen başkaca bir milletlerarası belge ise 2001 senesinde gerçekleştirilen Uluslararası Veri Koruma ve Mahremiyet Komiserleri Konferansı'nda alınan "Veri Koruma Otoritelerinin Akreditasyon İlkelerine İlişkin Karar"dır. Kararda belirtildiği üzere; denetim kurumlarının özerk ve bağımsız, kanun nezdinde kurulmuş, yürütme organına direkt olarak rapor verebilen kurumlar olması icap etmektedir. Öte yandan karar, bu kurumların kişisel verilerin korunmasına dair yapısal yeterliliği haiz ve milletlerarası düzenlemelerle paralellik gösteren kurumlar olması gerekliliğine dikkat çekmektedir.[235] Bununla birlikte kişisel verilerin işlenmesini denetleyen kontrol makamlarına başlıca üç yetki verilmiştir. Bu üç yetki; araştırma yapma, etkili faaliyet gösterme ve ihlal yaşandığında dava şikâyet hakkının kullanılmasıdır.[236]

"Kişisel Verileri Koruma Kurumu", 7 Nisan 2016 tarihinde Resmî Gazete' de yayımlanan 6698 Sayılı Kişisel Verilerin Korunması Kanunu ile Türkiye'nin idari teşkilatına dahil olmuştur. Anayasa'da düzenlenen özel yaşamın korunması ve temel hak ve hürriyetlerin korunması kapsamında, Kurumun misyonu kişisel verilerin korunmasını sağlamak ve bu konuda bilinç oluşturmaktır. Ayrıca, özel ve kamu aktörlerinin milletlerarası rekabet kabiliyetini artıran bir ortamın oluşturulması misyonuna da sahiptir. Buna uygun olarak, Kurumun vizyonu, kişisel verilerin korunması ve vatandaşlık farkındalığının meydana gelmesinde etkili ve milletlerarası yetkin bir kurum olmaktır. Belirtilen misyon ve vizyonu doğrultusunda, Kurumun özel hayatın gizliliğini gözetme, temel hak ve hürriyetlere saygı, taraflı olmama, bağımsızlık, güvenilirlik, etik prensiplere ve hukuku uyum, şeffaflık ve hesap verebilirlik, doğru ve nesnel karar alma, iş birliği ve katılım, milli ve milletlerarası seviyede hizmet etme gibi temel prensip ve değerlere sahip olduğu ifade edilebilir.[237]

235 Gürsel ve Düğmeci, "Yapısal Anlamda Türkiye", 319.
236 Akgül, *Danıştay ve Avrupa İnsan Hakları,* 155.
237 Sevinç ve Karabulut, "A Review on the Personal", 458

2.2.3.2.1.2. Kurumun İdari Teşkilattaki Yeri

Kişisel Verileri Koruma Kurumu yapısı itibariyle bağımsız idari otorite diğer bir ifade ile düzenleyici ve denetleyici bir kurumdur.[238] Zira Kurum, 5018 sayılı Kamu Malî Yönetimi ve Kontrol Kanununda "Düzenleyici ve Denetleyici Kurumlar" başlığı altında (III) Sayılı Cetvel içinde sayılmaktadır.[239] Türkiye'de bağımsız idari otoritelerin temel amacı piyasanın etkili kontrolünü yapmak suretiyle işleyişini sağlamak, düzenlemek ve gerekli önlemleri almaktır. Bu doğrultuda toplam kalite yönetiminin temel ilkeleri olan sonuç odaklı düşünme ve performans yönetimi, bağımsız kurumların başlıca özelliklerini oluşturmaktadır.[240]

Halihazırda var olan tüm düzenleyici ve denetleyici kurumlar gibi KVK Kurumu da kanunla kurulmuş, faaliyet alanı belirli, ilgili bakanlıkla hiyerarşik bağı olmayan ve idari vesayet denetimine çok sınırlı şekilde tabi olan[241]; düzenleme, denetleme, yaptırım uygulama gibi güçlü kamusal yetkilere sahip olan, özerk ve bağımsız statüyü haiz olan bir kurumdur. Kurum'un idari ve mali bakımdan özerk bir yapıda olması buradaki en mühim özelliktir. Zira kişisel veriler sadece özel kurumlara karşı değil kamu kurumlarına karşı da koruma altına alınmıştır.[242]

2.2.3.2.1.3. Kurumun Görevleri

Uluslararası Veri Koruma Komiserleri Konferansı'nın (ICDPPC) 2001 yılı toplantısında alınan "Veri Koruma Kurumlarının Akreditasyon İlkeleri" başlıklı kararda, kişisel verilerin korunması kurumlarının hukuki temel, özerklik ve bağımsızlık, uluslararası belgelere uygunluk ve uygun fonksiyonlar gibi dört temel ilkeye sahip olması

---

238 Kişisel Verileri Koruma Kurumunun, yerinden yönetim kuruluşları arasında bağımsız bir yer aldığına ilişkin detaylı açıklamalar için bkz: Başar, *Türk İdare Hukuku,* 244-246 ve Kağıtçıoğlu "Kişisel Verileri Koruma", 94.

239 Başar*, Türk İdare Hukuku,* 243.

240 Nesim Babahanoğlu, "Türk İdare Sisteminde Bağımsız İdari Otoriteler, Bağımsızlıkları ve Denetimleri Üzerine Bir Değerlendirme", *Anemon Muş Alparslan Üniversitesi Sosyal Bilimler Dergisi,* 9 (2021): 211-226, 216.

241 30473 sayılı Resmî Gazete'de yayımlanan 703 No'lu Kanun Hükmünde Kararname'nin 163. Maddesi ile Kişisel Verileri Koruma Kurumu, Cumhurbaşkanının görevlendireceği bir bakan ile ilişkilendirilmiştir. Bu nedenle Kurum, "ilişkili kuruluş" olarak nitelendirilebilir. Bkz: Gürsel ve Düğmeci, "Yapısal Anlamda Türkiye", 323. Kurumun sınırlı da olsa idari vesayet denetime tabi olmasına ilişkin görüş ve tartışmalara ilişkin detaylı açıklamalar için bkz: Kağıtçıoğlu. "Kişisel Verileri Koruma", 90, 92-95.

242 Uyarer, *Kişisel Verilerin Korunması,* 149.

öngörülmüştür. Toplantının karar metninde, veri koruma kurumları için bir kanun çerçevesinde kurulması, kuruma belirli dönemler için üyelerin atanması, görev ihmali, yetersizlik, görevin kötüye kullanımı gibi belirli koşullar altında üyelerin görevden alınması ve yasama veya hükümete doğrudan raporlama gibi çeşitli standartlar tanıtılmıştır.[243]

Bu standartlara uygun olarak Kurumun görevleri Kanun'un 20. maddesinde şu şekilde ifade edilmiştir:

"a) Görev alanı itibarıyla, uygulamaları ve mevzuattaki gelişmeleri takip etmek, değerlendirme ve önerilerde bulunmak, araştırma ve incelemeler yapmak veya yaptırmak.

b) İhtiyaç duyulması hâlinde, görev alanına giren konularda kamu kurum ve kuruluşları, sivil toplum kuruluşları, meslek örgütleri veya üniversitelerle iş birliği yapmak.

c) Kişisel verilerle ilgili uluslararası gelişmeleri izlemek ve değerlendirmek, görev alanına giren konularda uluslararası kuruluşlarla iş birliği yapmak, toplantılara katılmak.

ç) Yıllık faaliyet raporunu Cumhurbaşkanlığına, Türkiye Büyük Millet Meclisi İnsan Haklarını İnceleme Komisyonuna sunmak.

d) Kanunlarla verilen diğer görevleri yerine getirmek."

2.2.3.2.1.4. Gözetim ve Denetim Yetkisi

Düzenleyici ve denetleyici kurumlar kendilerine tanınmış yetkileri sebebiyle ilgili kanunlara ve düzenleyici işlemlere uygun davranılıp davranılmadığını kontrol etme yetkisini haizdirler. Kişisel Verileri Koruma Kurumu'na da resen ya da şikâyet üzerine kişisel verilerin kanunun öngördüğü biçimde işlenip işlenmediğini denetleme ve gerekirse geçici tedbirler alma yetkisi verilmiştir.[244] Zira kişisel verilerin korunması

[243] Sevinç ve Karabulut, "A Review on the Personal", 459; Kağıtçıoğlu "Kişisel Verileri Koruma", 79.
[244] Gürsel ve Düğmeci, "Yapısal Anlamda Türkiye", 324.

hususunda artan ihtiyaç nedeniyle Kişisel Verileri Koruma Kurumu kurulmuştur. Kurum denetleme yetkisini Kurul aracılığıyla kullanmaktadır.[245]

Kurum'un karar organı olan Kişisel Verileri Koruma Kurulu tarafından verilen "ilke kararları", Kurum'un gözetim ve denetim yetkisi ile bağdaşmaktadır. Nitekim idari yaptırım kararı içermeyen, ihbar üzerine yahut resen tespit edilen ihlalin yaygın olması durumunda uygulamadaki aksaklıkları gidermek amacı ile tesis edilen ilke kararları, Kurumun kendi alanındaki düzenleyici işlemlere ilişkin yetkisini kullanarak gözetim ve denetim yapması sonucu ortaya çıkmaktadır.[246] Öte yandan Kurul'a şikâyet yolu, denetleme yetkisinin kullanımında ön plandadır. Kurul'a yapılacak şikayetlerle ilgili 6698 sayılı Kanun'un 13., 14. ve 15. maddeleri incelendiğinde Kurul'un ve dolayısıyla Kurum'un, görevi ile ilgili konularda geniş bir denetleme yetkisi olduğunu söylemek mümkündür.[247]

2.2.3.2.1.5. Uyuşmazlık Çözme Yetkisi

Uyuşmazlık çözme yetkisi ve görevi kural olarak yargı organlarına ait iken istisnai durumlarda bağımsız idari otoritelerin faaliyet gösterdikleri alanların fazlaca teknik bilgi gerektirmesi nedeniyle bazı yetkilerin bu kurumlara bırakıldığı görülmektedir.[248] Uyuşmazlık çözme yetkisi yargı organlarının işleyişinden kaynaklanan birtakım aksaklıklara bir çözüm yolu olarak kabul edilmektedir.[249]

---

245 Besra Gülnaz, "Kişisel Verileri Koruma Kurumunun Yapısal ve İşlevsel Analizi", (Yayımlanmamış Yüksek Lisans Tezi, Mersin Üniversitesi, 2019), 70.

246 Deniz Hacıosmanoğlu, "Kişisel Verileri Koruma Kurumu Yapısı ve İşlevi", (Yayımlanmamış Yüksek Lisans Tezi, Ankara Üniversitesi, 2020), 81; Gülnaz, "Kişisel Verileri Koruma", 70.

247 Gülnaz, "Kişisel Verileri Koruma", 70-71.

248 Gürsel ve Düğmeci, "Yapısal Anlamda Türkiye", 324.

249 Örneğin bağımsız idari otoritelerden biri olan Sermaye Piyasası Kurulunun (SPK) uyuşmazlık çözme yetkisi bulunmaktadır. Borsa üyeleri arasında borsa işlemlerinden kaynaklanan uyuşmazlıklarla, borsa üyeleri ile müşterileri arasındaki uyuşmazlıkların borsa yönetim kurullarınca çözümlenebileceğini öngörmektedir. Aynı hükme göre borsa yönetim kurulu kararlarına karşı SPK'ye başvurulabilir; SPK'nın bu konudaki kararları nihaidir. Yine ihale sürecinde ortaya çıkan uyuşmazlıkların giderilmesi konusunda Kamu İhale Kurumuna uyuşmazlık çözme yetkisi verilmiştir. Kamu ihalelerinin yapılmalarından önce ihale aşamasında meydana gelen ya da geldiği iddia edilen uyuşmazlıkların yargı yoluna başvurulmadan önce yapılacak idari başvuru yolu ile giderilebilmesi mümkündür. Kamu İhale Kanunundaki düzenlemeler gereğince şikâyet ve itirazen şikâyet başvuruları yolu ile uyuşmazlık yargıya intikal ettirilmeksizin çözümlenebilecektir. Bkz: Aynur Cidecigiller. "Düzenleyici ve Denetleyici Kamu Kurumları Tarafından Uyuşmazlıkların Giderilmesi", *Gazi Üniversitesi Hukuk Fakültesi Dergisi XVIII* / 3-4 (Temmuz 2014): 491-504. 497-501. (E. T. 02.04.2022), https://dergipark.org.tr/tr/download/article-file/789132

KVKK'nın 13 ve 14. maddelerine göre veri sorumlusu ile bireyler arasında doğacak uyuşmazlıklarda, ilgili kişiler ilk olarak veri sorumlusuna başvuru yapacak ardından Kurula şikâyette bulunabilecektir. Kanunda başvuru yolu tüketilmeden şikâyet yoluna başvurulmayacağı belirtildiğinden Kurula şikâyet yolu ihtiyari bir başvuru olarak gündeme gelmektedir. Bu nedenle Kurumun karar organı olan Kurul aracılığı ile her bağımsız idari otoritenin yetkisinde bulunmayan kendine has metotlarla uyuşmazlık çözme işlevine de sahip olduğu görülür.[250]

2.2.3.2.1.6. Yaptırım Uygulama Yetkisi

Düzenleyici ve Denetleyici Kurumlar, yaptıkları denetimler sonucunda belirledikleri hukuka aykırılıkların ilgililerine karşı doğrudan doğruya yaptırım uygulama yetkisine sahiptir. Yaptırım uygulama yetkisi, bağımsız idari otoritelerin kendilerine bırakılan alanlarda düzenleme yapma ve bu düzenlemelere uygun faaliyet gösterilip gösterilmediğini denetleme yetkisinin bir uzantısıdır. KVKK'nın ''kabahatler'' başlıklı 18. maddesinde Kişisel Verileri Koruma Kurumu'nun yaptırım uygulama yetkisi düzenlenmiştir.[251] Buna göre;

- *"Aydınlatma yükümlülüğünü yerine getirmeyenlere 5.000 TL'den 100.000 TL'ye kadar,*

- *Veri güvenliğine ilişkin yükümlülüklerini yerine getirmeyenlere 15.000 TL'den 1.000.000 TL'ye kadar,*

- *Şikâyet üzerine ya da resen inceleme neticesinde kurul tarafından verilen kararları yerine getirmeyenlere 25.000 TL'den 1.000.000 TL'ye kadar,*

- *Veri Sorumluları Siciline kayıt ve bildirim yükümlülüğüne aykırı hareket edenlere 20.000 TL'den 1.000.000 TL'ye kadar,*

- *9. maddenin beşinci fıkrasında öngörülen bildirim yükümlülüğünü yerine*

250 Kağıtçıoğlu. "Kişisel Verileri Koruma", 89.
251 Gürsel ve Düğmeci, "Yapısal Anlamda Türkiye", 324.

getirmeyenler hakkında 50.000 Türk lirasından 1.000.000 Türk lirasına kadar,[252] *idari para cezası verilmektedir."*

Kanunda bahsi geçen miktarlar 5326 sayılı Kabahatler Kanunu'nun 17/7. maddesi uyarınca göre her takvim yılının başlangıcından itibaren geçerli olmak üzere 213 sayılı Vergi Usul Kanunu'nun mükerrer 298. maddesi hükümleri doğrultusunda o yıl için tespit ve ilan edilen yeniden değerleme oranında artırılmakta olup 2024 yılı[253] itibariyle %58,46'lık artışla:

- *"Aydınlatma yükümlülüğünü yerine getirmeyenlere 47.303 TL'den 946.308 TL'ye kadar,*
- *Veri güvenliğine ilişkin yükümlülüklerini yerine getirmeyenlere 141.934 TL'den 9.463.213 TL'ye kadar,*
- *Şikâyet üzerine ya da resen inceleme neticesinde kurul tarafından verilen kararları yerine getirmeyenlere 236.557 TL'den 9.463.213 TL'ye kadar,*
- *Veri Sorumluları Siciline kayıt ve bildirim yükümlülüğüne aykırı hareket edenlere 189.245 TL'den 9.463.213 TL'ye kadar"* idari para cezası verilmektedir.

Bahsi geçen bu idari para cezaları sadece gerçek kişi ve özel hukuk tüzel kişi veri sorumlusu açısından düzenlenecektir. İdari para cezasına konu olan eylemlerin kamu kurum ve kuruluşunda görevli memurlar ve diğer kamu görevlileri ile kamu kurumu niteliğindeki meslek kuruluşlarında görevli şahıslar tarafından gerçekleştirilmesi durumunda, bu kişiler hakkında disiplin hükümlerine göre işlem tesis edilecek ve Kurul'a bildirim yapılacaktır.[254]

Bağımsız idari otoritelere tanınan yaptırım yetkisi somut olayın özelliklerine göre kimi zaman zayıf kaldığı için bu otoriteler, etkili ve zorlayıcı bir önlem almak ve yaptırım

---

252 12/3/2024 tarihli ve 32487 sayılı Resmî Gazete'de yayımlanan 7299 sayılı Ceza Muhakemesi Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun değişikliği ile gelmiş olup 01.06.2024'te yürürlüğe girmiştir.

253 2017-2024 yılları için tespit ve ilan edilen yeniden değerleme oranında arttırılmış tutarlar için bkz: (E.T. 06.01.2024) https://kvkk.gov.tr/SharedFolderServer/CMSFiles/8833aad2-62c2-4a01-b147-fe97062678f3.pdf

254 Salih İnan, "Kişisel Verilerin Korunması Kapsamındaki Yaptırımlara Karşı Yargısal Başvuru Yolları: Karşılaştırmalı Bir İnceleme", *Kişisel Verileri Koruma Dergisi*, 3/2 (2021), 50-65, 54.

uygulamak adına konuyu yargı organlarına taşıyabilir; Kanunun suç saydığı eylem ve işlemlere karşı kendi yetki alanlarında olan kişi ve kurumların bu ihlallere karışması durumunda savcılığa başvurulması da mümkündür. KVKK hükümlerinin çiğnenmesi durumunda uygulanacak idari yaptırımların yanında ayrıca kanunda açıkça veri güvenliğine aykırılığın suç sayıldığı durumlarda Kurumun Cumhuriyet savcılıklarına başvurma yükümlülükleri bu duruma verilebilecek örnektir.[255]

2.2.3.2.2. Kişisel Verileri Koruma Kurulu ve Görevleri

Kurum özerkliğinin korunması, Kurum politikalarında istikrar ve sürekliliğin sağlanabilmesi, üzerinde herhangi bir siyasi baskı olmayan kişiler arasından seçilen uzmanlardan oluşturulacak bir kurul[256] ile gerçekleştirilebilecektir. Dolayısıyla Kişisel Verileri Koruma Kurumunun karar organı, kurul tipi yapılanma ile oluşturulmuş ve karar organına Kişisel Verileri Koruma Kurulu adı verilmiştir.[257] Kurul, KVKK ve diğer mevzuatla tanınan görev ve yetkilerini sorumluluğu kendisine ait olacak şekilde bağımsız olarak uygular ve kullanır. Görev alanı ile ilgili noktalarla alakalı hiçbir organ, makam, merci veya kişi, Kurula emir ve talimat veremez, tavsiye veya telkinde bulunamaz (KVKK md.21/1). Kurul, dokuz üyeden oluşur. Kurulun beş üyesi Türkiye Büyük Millet Meclisi (TBMM), dört üyesi Cumhurbaşkanı tarafından seçilir (KVKK md.21/2). TBMM tarafından Kurula üye seçimi KVKK'nın 21/5 maddesinde belirtilen usullere göre gerçekleştirilir. Kurula üye olabilmek için *"kurumun görev alanındaki konularda bilgi ve deneyim sahibi olmak, 657 sayılı Devlet Memurları Kanunu'nun 48 inci maddesinin birinci fıkrasının (A) bendinin (1), (4), (5), (6) ve (7) numaralı alt bentlerinde belirtilen nitelikleri taşımak, herhangi bir siyasi parti üyesi olmamak, en az dört yıllık lisans düzeyinde yükseköğrenim[258] görmüş olmak*" şartları aranır (KVKK md.21/3). Kurul üyelerinin görev süresi dört yıldır. Süresi biten üye yeniden seçilebilir. Görev süresi

---

255 Babahanoğlu, "Türk İdare Sisteminde", 218.

256 Kurul üyelerinin seçimine yönelik eleştiriler için bkz: Kağıtçıoğlu, "Kişisel Verileri Koruma", s. 84-87.

257 Gürsel ve Düğmeci, "Yapısal Anlamda Türkiye", 324.

258 Kanaatimizce, Kurul üyelerinin "*en az dört yıllık lisans düzeyinde yükseköğrenim görmüş olması*" şartı başlı başına yeterli değildir. Zira veri koruma hukukunun kendine has özellikleri nedeniyle özel uzmanlık gerektiren bir konu olduğu aşikardır. Bu nedenle bu alanda karar verici üyelerin konuya hâkim olan ya da olması beklenebilecek "bilgi, görgü ve diploma" anlayışına göre belirlenecek kriterlere göre seçilmesi daha uygun olacaktır.

dolmadan herhangi bir sebeple görevi sona eren üyenin yerine seçilen kişi, yerine seçildiği üyenin kalan süresini tamamlar (KVKK md. 21/8).[259]

2.2.3.2.2.1. Kurulun Görevleri

Kurul, Kurumun karar organıdır (KVKK md. 19/4). Kanun'un 22. maddesinde Kurulun görevleri belirlenmiştir:

"Kurulun görev ve yetkileri şunlardır:

a) Kişisel verilerin, temel hak ve özgürlüklere uygun şekilde işlenmesini sağlamak.

b) Kişisel verilerle ilgili haklarının ihlal edildiğini ileri sürenlerin şikâyetlerini karara bağlamak.

c) Şikâyet üzerine veya ihlal iddiasını öğrenmesi durumunda resen görev alanına giren konularda kişisel verilerin kanunlara uygun olarak işlenip işlenmediğini incelemek ve gerektiğinde bu konuda geçici önlemler almak.

ç) Özel nitelikli kişisel verilerin işlenmesi için aranan yeterli önlemleri belirlemek.

d) Veri Sorumluları Sicilinin tutulmasını sağlamak.

e) Kurulun görev alanı ile Kurumun işleyişine ilişkin konularda gerekli düzenleyici işlemleri yapmak.

f) Veri güvenliğine ilişkin yükümlülükleri belirlemek amacıyla düzenleyici işlem yapmak.

---

259 KVKK md. 21/10: Kurul üyeleri özel bir kanuna dayanmadıkça, Kuruldaki resmî görevlerinin yürütülmesi dışında resmî veya özel hiçbir görev alamaz, dernek, vakıf, kooperatif ve benzeri yerlerde yöneticilik yapamaz, ticaretle uğraşamaz, serbest meslek faaliyetinde bulunamaz, hakemlik ve bilirkişilik yapamazlar. Ancak, Kurul üyeleri, asli görevlerini aksatmayacak şekilde bilimsel amaçlı yayın yapabilir, ders ve konferans verebilir ve bunlardan doğacak telif hakları ile ders ve konferans ücretlerini alabilirler.
/11: Üyelerin görevleri sebebiyle işledikleri iddia edilen suçlara ilişkin soruşturmalar 2/12/1999 tarihli ve 4483 sayılı Memurlar ve Diğer Kamu Görevlilerinin Yargılanması Hakkında Kanuna göre yapılır ve bunlar hakkında soruşturma izni Cumhurbaşkanı tarafından verilir.
/12: Kurul üyeleri hakkında yapılacak disiplin soruşturması ve kovuşturmasında 657 sayılı Kanun hükümleri uygulanır.

g) Veri sorumlusunun ve temsilcisinin görev, yetki ve sorumluluklarına ilişkin düzenleyici işlem yapmak.

ğ) Bu Kanunda öngörülen idari yaptırımlara karar vermek.

h) Diğer kurum ve kuruluşlarca hazırlanan ve kişisel verilere ilişkin hüküm içeren mevzuat taslakları hakkında görüş bildirmek.

ı) Kurumun; stratejik planını karara bağlamak, amaç ve hedeflerini, hizmet kalite standartlarını ve performans kriterlerini belirlemek.

i) Kurumun stratejik planı ile amaç ve hedeflerine uygun olarak hazırlanan bütçe teklifini görüşmek ve karara bağlamak.

j) Kurumun performansı, mali durumu, yıllık faaliyetleri ve ihtiyaç duyulan konular hakkında hazırlanan rapor taslaklarını onaylamak ve yayımlamak.

k) Taşınmaz alımı, satımı ve kiralanması konularındaki önerileri görüşüp karara bağlamak.

l) Kanunlarla verilen diğer görevleri yerine getirmek."

Kurul'a Kişisel Verileri Koruma Kurulu Çalışma Usul ve Esaslarına Dair Yönetmelik'in 7. maddesinde, Kanun'un 22. maddesinde bahsedilen görevlere ek olarak birtakım görevler de verilmiştir. Kanundaki görevlere ek görevler şu şekildedir:[260]

1. *"Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin usul ve esasların belirlenmesi,*

2. *Yurt dışına veri aktarılabilmesi için yeterli korumaya sahip olan ve olmayan ülkelerin belirlenip ilan edilmesi,*

3. *Kişisel verilerin korunması, işlenmesi ve güvenliği ile ilgili sektörel uygulama esaslarının belirlenmesi,*

[260] Gülnaz, "Kişisel Verileri Koruma", 60.

4. *Akreditasyon, sertifikasyon, eğitim ve rehberlik konularında usul ve esasların belirlenmesi,*

5. *Kişisel verilerin korunması ile ilgili yurt içi ve yurt dışı projelerin yapılması ve yaptırılması,*

6. *Kişisel verilerin korunması konusunda kurum ve kuruluşların bilgilendirilmesi ve kamuoyuna yönelik farkındalık faaliyetlerinin gerçekleştirilmesi,*

7. *Ücret tarifeleri ile ilgili çalışmaların yapılması,*

8. *Üniversiteler ve ilgili diğer yurt içi ve yurt dışı kurum ve kuruluşlarla iş birliği ve koordinasyon çalışmalarının yürütülmesi."*

Kurulun çalışma usulü "Kişisel Verileri Koruma Kurulu Çalışma Usul ve Esaslarına Dair Yönetmelik"[261] ile detaylı şekilde açıklanmıştır. Kurul bahsi geçen görevlerini ise şu çalışma esasları çerçevesinde gerçekleştirir:[262]

1. *"Kurulun toplantı günlerini ve gündemini Başkan belirler. Başkan gereken hâllerde Kurulu olağanüstü toplantıya çağırabilir.*

2. *Kurul, başkan dâhil en az altı üye ile toplanır ve üye tam sayısının salt çoğunluğuyla karar alır. Kurul üyeleri çekimser oy kullanamaz.*

3. *Kurul üyeleri; kendilerini, üçüncü dereceye kadar kan ve ikinci dereceye kadar kayın hısımlarını, evlatlıklarını ve aralarındaki evlilik bağı kalkmış olsa bile eşlerini ilgilendiren konularla ilgili toplantı ve oylamaya katılamaz.*

4. *Kurul üyeleri çalışmaları sırasında ilgililere ve üçüncü kişilere ait öğrendikleri sırları bu konuda kanunen yetkili kılınan mercilerden başkasına açıklayamazlar ve kendi yararlarına kullanamazlar. Bu yükümlülük görevden ayrılmalarından sonra da devam eder.*

---

261 30242 sayılı ve 16 Kasım 2017 sayılı Resmî Gazetede yayımlanmıştır. (E.T. 08.09.2023), https://www.resmi gazete.gov.tr/eskiler/2017/11/20171116-7.htm

262 KVKK md. 23.

5. *Kurulda görüşülen işler tutanağa bağlanır. Kararlar ve varsa karşı oy gerekçeleri karar tarihinden itibaren en geç on beş gün içinde yazılır. Kurul, gerekli gördüğü kararları kamuoyuna duyurur.*

6. *Aksi kararlaştırılmadıkça, Kurul toplantılarındaki görüşmeler gizlidir.*

7. *Kurulun çalışma usul ve esasları ile kararların yazımı ve diğer hususlar yönetmelikle düzenlenir."*

Bu görevler, Kişisel Verileri Koruma Kurulu'nun geniş bir yelpazede faaliyet göstermesini ve kişisel verilerin korunmasıyla ilgili çeşitli alanlarda etkinliklerde bulunmasını sağlamaktadır.

2.2.3.2.2.2. Kurul Kararları ve Niteliği

Kişisel Verileri Koruma Kurulu Çalışma Usul ve Esaslarına Dair Yönetmelik'in 13. maddesinde Kurul'un şikâyet üzerine veya resen yapacağı incelemelerin ardından vereceği kararlarda belli niteliklerin olması gerektiği belirtilmiş olup "*karar veren Kurul üyeleriyle inceleme ve araştırmayı yapanların ad ve soyadları; tarafların ad, soyad, unvan, adres ve sıfatları; tarafların iddia ve beyanlarının özeti; iddia ve beyanların değerlendirmesi; kararın hukuki dayanağı; sonuç ve varsa karşı oy gerekçeleri*" ile Kurul'un vereceği diğer kararlarda ise "*karar veren Kurul üyelerinin ad soyadları, kararın konusu ve hukuki dayanağı, sonuç ile varsa karşı oy gerekçelerinin bulunması*" gerektiği ifade edilmiştir. Kurulun şikâyet üzerine vereceği kararlarda 60 gün içinde cevap verme yükümlülüğü tanınmışsa da Kurulun resen yapacağı incelemeler açısından herhangi bir süre söz konusu değildir.[263]

KVKK ve bu kanuna dayalı olarak düzenlenen Kişisel Verileri Koruma Kurulu Çalışma Usul ve Esaslarına Dair Yönetmelik'teki ilgili hükümlere bakıldığında, Kişisel Verileri Koruma Kurumunun karar verme özerkliğinin hukuki olarak sağlandığı anlaşılmaktadır. Kurum, Kurul aracılığı ile merkezi yönetimin müdahalesi olmaksızın bağımsız bir şekilde kararlar verebilir, bu kararlarla alakalı düzenlemeleri kendisi gerçekleştirebilir ve gerektiğinde kamuoyuna bilgi verebilir. Bu yetkiler, yasal düzenlemelerle açıkça

[263] Başar, *Türk İdare Hukuku*, 303.

tanımlanmıştır ve Kurul'un ve Kurum'un bağımsız ve özerk bir biçimde hareket etme kapasitesine sahip olduğunu vurgulamaktadır.[264] Bu doğrultuda Kurum'un karar organı olan Kurul'un geniş bir takdir yetkisi bulunmaktadır ki bu takdir yetkisinin kamu yararına kullanılması gerektiği şüphesizdir.[265] Öte yandan Kurula tanınan resen inceleme yetkisi sayesinde daha işlevsel bir koruma mekanizması oluşturulduğu da ifade edilebilir.[266]

264 Gülnaz, "Kişisel Verileri Koruma", 59.
265 Kağıtçıoğlu, "Kişisel Verileri Koruma", 90.
266 Başar, *Türk İdare Hukuku*, 301.

ÜÇÜNCÜ BÖLÜM

VERİ İHLALLERİ VE KİŞİSEL VERİLERİ KORUMA KURULU İLKE KARARLARI

3.1. İlgili Kişinin Kişisel Verileri Üzerindeki Hâkimiyeti ve Hakları

3.1.1. Genel olarak

Kişisel verilerin korunması hukuku dahilinde kişisel verisi işlenen ilgili kişiye, veri işleme sürecine farklı evrelerde dâhil olma imkânı tanıyan birtakım haklar tanınmıştır. Kanun'un 11. maddesinde düzenlenen haklar ilgili kişinin verileri üzerinde denetim yapabilmesini ve kişisel verilerin işlenmesindeki ilkelerin gerçekleşebilmesi için son derece önem arz etmektedir.[267]

Dijital ekonominin oldukça önemli olduğu bu çağda, büyük miktarda kişisel veriye erişim olanağı bulunan ve bu verileri işleyerek maddi değere çeviren veri sorumlularının imkânı ile kişisel verileri işlenen gerçek kişi şahısların imkânları arasında, bu verilerin kontrolüne ilişkin dengesizlik bulunduğu izahtan varestedir. Kişisel veri sahipleri ile veri sorumluları arasında verilerin işlenmesi aşamasında meydana gelen güç dengesizliğini en aza indirmek ve bireylere, kişisel verilerinin işlenmesi sürecinde verileri üzerinde daha çok kontrol sağlamaları amacıyla bu haklar tanınmıştır. Veri sorumlusu, ilgili kişiye tanınan bu hakların kullanılması için gereken zemini oluşturmak başka bir deyişle, ilgili kişinin kişisel verilerinin işlenme süreçlerine katılımı ve denetimi konusunda gereken

---

[267] Küzeci, *Kişisel Verilerin Korunması,* 247.

enstrümanları oluşturmak zorundadır.[268] Zira, zorunluluk aynı zamanda veri sorumlusuna yüklenen hesap verebilme zorunluluğu ile de bağlantılıdır. Kişisel verilerin korunması konusunda hesap verebilme zorunluluğu, veri sahiplerinin verilerinin nasıl işlendiğini ve hangi amaçlarla kullanıldığını bilmelerini ve bu konuda yetkililere bilgi vermelerini sağlar. Veri sorumlusunun idare olması halinde de idare açısından yönetimde açıklık ilkesi de teminat altına alınır.[269] Bu sayede, veri sahipleri verilerinin korunmasına ilişkin haklarını kullanabilir ve gerekirse önlem alabilirler. Konu ile bağlantılı olarak ilke kararlarında da görüleceği üzere kişisel veri ihlallerinin önüne geçilmesinin ilk aşamasında her zaman sorgulayan ve kişisel verileri ile ilgili bilgi sahibi olmak isteyen ilgili kişiler vardır.[270]

3.1.2. İlgili Kişinin Hakları

Kişisel verilerin korunması hakkı pek çok düzenleme ile güvence altına alınmış, kişisel verileri işlenen ilgili kişilere, verileri üzerinde birçok hak tanınmıştır. Bilgilerin geleceğini belirleme hakkına sahip olan ilgili kişinin haklarının etkin kullanımını sağlamak adına da başvuru, şikâyet, dava etme gibi denetim mekanizmaları da getirilmiştir. Buna göre kişisel verileri işlenen ve veri işleme sürecine dahil edilen ilgili kişi Kanun'un 11. maddesi doğrultusunda bilgilendirme, silme/düzeltme, kısıtlama, zararın giderilmesini talep etme şeklinde ifade edilebilecek başlıca haklara sahip olup bu hakları her zaman veri sorumlusuna başvuru yaparak kullanabilecektir. Haklarını kullanarak veri işleme sürecine dair bilgi sahibi olan ilgili kişi, edindiği bu bilgiler ışığında Kanun'da sayılan düzeltme, silme ve/veya yok etme, kişisel verilerin aktarıldığı diğer üçüncü kişilere bildirme, otomatik kararların konusu olmama, zararın giderilmesini isteme haklarını kullanabilir. Veri sorumlusunun, ilgili kişiye haklarını kullandırmaması yahut ilgili kişinin yerinde talebinin kabul edilmemesi halinde, ilgili kişinin genel hükümlere göre dava yolu ve yahut alanda düzenleyici ve denetleyici kurum olan başka bir deyişle bağımsız idari otorite olan Kişisel Verileri Koruma Kurumuna şikâyet hakkı bulunmaktadır. İlgili kişiye tanınan bu hakların kullandırılması, kişisel verileri işleyen

---

268 Serdar Çelikel, *Kişisel Verilerin Korunması Hukuku Kapsamında Veri Sorumlusu ve Veri Sorumlusunun Yükümlülükleri*, (Ankara Seçkin Yayıncılık, 2022), 157.

269 Başar, *Türk İdare Hukuku,* 261.

270 Çiğdem Aygözer Öngün, *Kişisel Verilerin Korunması Hukuku, Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil*, (İstanbul: Beta Yayıncılık, Ocak 2019), 215.

veri sorumluları açısından da kanuni bir yükümlülük olup şeffaflık ve hesap verebilirlik bakımından önem arz eder.

3.1.2.1. İlgili Kişinin Veri Sorumlusuna Başvuru Hakkı

İlgili kişi, KVKK'nın 11. maddesi çerçevesinde veri sorumlusuna her zaman başvurarak kendisi ile ilgili "*kişisel verilerinin işlenip işlenmediğini öğrenme, kişisel verileri işlenmişse buna ilişkin bilgi talep etme, kişisel verilerinin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme, yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme, kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme, kişisel verilerin silinmesini veya yok edilmesini isteme, kişisel verilerin düzeltilmesi, silinmesi veya yok edilmesine ilişkin işlemlerin kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme, işlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme, kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme*" haklarına sahiptir. Bu haklar, ilgili kişinin verileri üzerinde denetim yapabilmesini ve kişisel verilerin işlenmesindeki ilkelerin gerçekleşebilmesi için son derece elzemdir.[271] Veri sorumlusuna başvuru ise Kurum tarafından yayımlanan "Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ"[272] ile düzenlenen usul ve esaslara göre gerçekleştirilecektir.

3.1.2.1.1. Bilgilendirilme Hakkı

Kişisel verilerin korunması hakkından faydalanabilmek için hakkın özü itibariyle kişisel veri sahibinin, kendisiyle ilgili olan verileri üzerinde tam bir hâkimiyet kurabilmesi ve tasarruf yetkisini kullanabilmesi için verilerine ulaşması gerekmektedir. Bu sebepledir ki kişisel verilerin işlendiği tüm süreçlere ilişkin bilgi talep etme hakkı tüm uluslararası belgelerde olduğu gibi KVKK ile de düzenlenmiştir. Kanun'un 11/a, b, c, ç hükümleri uyarınca veri sahibi her zaman veri sorumlusuna başvurarak,

---

271 Küzeci, *Kişisel Verilerin Korunması*, 247.

272 30356 sayılı ve 10 Mart 2018 tarihli Resmî Gazete 'de yayımlanmıştır. (E.T. 17.12.2023), https://www. resmigazete.gov.tr/eskiler /2018/03/20180310-6.htm

- Kişisel verisinin işlenip işlenmediğini öğrenme,
- Kişisel verileri işlenmişse buna ilişkin bilgileri talep etme,
- Kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme
- Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme hakkına sahiptir.

GDPR'da erişim hakkı olarak düzenlenen bu hak[273] iç hukukumuzda bilgi talep etme hakkı olarak kaleme alınmıştır. Kişisel Verileri Koruma Kurulu (Kurul) 14.01.2020 tarihli 2020/13 sayılı kararında:

"ilgili kişinin KVKK'nın 11. Maddesinin 1/b hükmü uyarınca kendisiyle ilgili kişisel veriler işlenmişse buna ilişkin bilgi talep etme hakkının söz konusu veriye erişim hakkını da kapsadığını ve erişim hakkının, bilgi talep etme hakkını tamamlayarak ilgili kişinin, kişisel verileri üzerindeki haklarını kullanabilmesi için, kişisel verilerinin ne şekilde işlendiğine dair tam olarak bilgi sahibi olmasına imkan sağladığı ... işlenen kişisel verilerin, teknik/fiziki imkanların el verdiği ölçüde ve verinin muhtevasına/içeriğine ilgili kişi tarafından makul bir şekilde ulaşabilmesine imkan tanınmasını kapsadığına ..." karar vermiştir.[274]

Bilgi talep etme hakkının kullanılmasıyla aslında kişinin ihlal iddiası ile karşı karşıya kaldığı durumun temel sebebinin öğrenilmesi hedeflenmektedir ki bu husus ilgili kişinin başvurusuyla gerçekleşmektedir. İlgili kişinin haklarını kullanabilmesi için ilk olarak verilerine ilişkin bilgi alması icap etmektedir. İlgili kişi bu talep sonucunda alacağı yanıta doğrultusunda karar vermeli, Kanun'da belirtilen bir sonraki adım için kişi her koşulda, ilk olarak bilgi isteme hakkını kullanmalıdır.[275] Başka bir ifade ile ilgili kişinin kendi kişisel verilerine erişme hakkı; verinin doğruluğunu denetleme, düzeltme, sildirme ve

---

273 Göçmen Uyarer, *Kişisel Verilerin Korunması,* 145.

274 Dülger, *Kişisel Verilerin Korunması*, 479,480.

275 Betül Gürener, "Avrupa Birliği Genel Veri Koruma Tüzüğü ve Kişisel Verilerin Korunması Kanununa Göre İlgili Kişi Haklarının Karşılaştırılması" (Yayımlanmamış Yüksek Lisans Tezi, Atılım Üniversitesi. 2021) 62,63. (E.T.25.01.2023), https://tez.yok.gov.tr/UlusalTezMerkezi/-tezSorguSonucYeni.jsp

engelleme hakkının bir gereği olup kişiler yalnızca hangi verilerinin kim tarafından ne amaçla işlendiğini, saklandığını ve kullanıldığını öğrenerek verilerinin geleceğini belirleme hakkından faydalanabilir.[276]

İlgili kişinin kişisel verileri üzerinde kontrolünü gerçekleştirebilmesi için ilk olarak, bir kişinin kişisel verilerine sahip olabilen veri sorumlusu tarafından, verinin tam içeriği ve veri işleme süreçleri hakkında o kişi bilgilendirilmelidir.[277] Bu husus, veri sorumlularınca aydınlatma yükümlülüğünün yerine getirilmesi ile olası hale gelebilecektir. Aydınlatma yükümlülüğü, Kanun'da açıkça ifade edilmeyen ancak kişisel verileri koruma hukukunun genel ilkeleri arasında sayılan şeffaflık ve hesap verilebilirlik/verebilirlik ilkelerinin de bir gereğidir. Aynı zamanda bu yükümlülük, KVKK'nın 4/2-b maddesinde açıkça belirtilen verilerin doğru ve gerektiğinde güncel olması ilkesini hayata geçirmeye yöneliktir. Çünkü kendileri hakkındaki kişisel verilerin işlenip işlenmediğinden dahi habersiz olan ilgili kişilerin, bu verilerinin doğru ve güncel olup olmadığını denetleyebilmeleri mümkün olmayacaktır.[278]

Aydınlatma yükümlülüğünün içeriği KVKK m. 10'da belirlenmiştir. Buna göre; *"en geç kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişi, ilgili kişilere; veri sorumlusunun ve varsa temsilcisinin kimliği, kişisel verilerin hangi amaçla işleneceği, işlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceği, kişisel veri toplamanın yöntemi ve hukuki sebebi ile ilgili kişinin Kanun'un 11. maddesinde sayılan diğer hakları konusunda bilgi vermekle yükümlü"* tutulmuştur. Bu doğrultuda veri sorumlusu, ilgili kişilerin Kanun ile güvence altına alınan hakları kapsamında edinmek istediği bilgileri hiçbir gerekçe ile ilgili kişiden gizleyemez, kendisine yöneltilen taleplerden kaçınamaz.[279] Bilgilendirilen ilgili kişi daha sonra işlenen verisi ile verisinin silinmesini, düzeltilmesini isteme gibi Kanun'un ilgili haklarını içeren 11. maddesinde sayılan haklarını kullanabilir.[280]

---

276 Küzeci, *Kişisel Verilerin Korunması*, 253.
277 Gürpınar, "Kişisel Verilerin Korunamamasından", 683.
278 Çelikel, *Kişisel Verilerin Korunması*, 93.
279 Dülger, *Kişisel Verilerin Korunması*, 479.
280 Büşra Merve Kılınç Sucu, "Temel Hak Boyutuyla Kişisel Verilerin Korunması", (Yayımlanmamış Yüksek Lisans Tezi, Dokuz Eylül Üniversitesi, 2020), 89. https://tez.yok.gov.tr/UlusalTezMerkezi-/tezSorgu SonucYeni.jsp (E.T.27.01.2023)

3.1.2.1.2. Kişisel Verilerin Düzeltilmesini İsteme Hakkı

Kişisel verilerin korunması ile ilgili birçok uluslararası metin ile korumaya alınan ilgili kişinin kişisel verilerine ilişkin düzeltme talep etme hakkı Avrupa Birliği Temel Haklar Bildirgesi'nin "Kişisel Verilerin Korunması" başlıklı 8. maddesinde "*herkes, kendisi hakkında toplanmış olan bilgilere erişme ve bunlarda düzeltme yaptırma hakkına*" sahip olduğu şeklinde düzenlenmiş olup iç hukukumuzda esas olarak Anayasa ve KVKK ile güvence altına alınmıştır.

1980 yılında OECD tarafından kabul edilen "Mahremiyetin Korunması ve Kişisel Verilerin Sınır Ötesi Akısına ilişkin Rehber İlkeler" içerisinde bulunan "bireyin katılımı ilkesi" gereğince ilgili kişinin, "*veri sorumlusu vasıtasıyla ya da başka bir usulle kendisini ilgilendiren verilerin mevcut olup olmadığının onaylanmasını talep hakkı*" vardır. Bu hak uyarınca ilgili kişiye, "*kendisi ile ilgili veri işlenmesine itirazda bulunma ve itirazın kabul edilmesi durumunda kendisi ile ilgili verilerin silinmesini, düzeltilmesini, eksikliklerinin giderilmesini ya da değişim yapılmasını talep etme hakkı*" tanınmıştır. [281]

Veri sorumlusu açısından bakıldığında ise kişisel verilerin işlenmesi için uyulması gerekli ve zorunlu olan genel ilkelerden biri de "doğru ve gerektiğinde güncel olma" ilkesidir (KVKK md.4/2-b). Bu ilke ile kişisel verilerin düzeltilmesini talep etme hakkı birbiriyle uyum içerisindedir. Zira kişisel verileri işlenen ilgili kişiler, kendi kişisel verilerinin doğru şekilde işlenmesini ve belirli aralıklarla işlenen kişisel verilerinin doğruluğunun kontrol edilmesini talep ederken, hatalı yahut güncel olmayan verileri varsa bunların düzeltilmesini de talep edebilecektir.[282] Veri sorumlusuna yüklenen bu yükümlülük ile, ilgili kişiye de kişisel verilerinin düzeltilmesini isteme hakkı tanınmaktadır. Zira ilgili kişi yukarıda bahsi geçen ve bilgilendirilme hakkı kapsamında sayılan hakları kullandığında, ilgili kişinin kendisi hakkında tutulan eksik, hatalı veya güncel olmayan verilerine erişmek ve bu veriler hakkında bilgi olmak istemesinin pratikte bir anlamı olmayacaktır. Bu sebeple de ilgili kişiye kendisi ile alakalı yanlış kişisel verilerin ivedilikle düzeltilmesini isteme hakkı verilmiştir. Dolayısıyla ilgili kişinin usulüne uygun şekilde

---

281 Aktaran Kılınç, "Anayasal Bir Hak", 1110.

282 Onur Günbey, "Kişisel Verilerin Korunması Kanunu Kapsamında Veri Sorumlusunun Yükümlülükleri", (Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi, 2020), 60. https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp (E.T. 25.01.2023)

yaptığı düzeltme talebini alan veri sorumlusu, düzeltilmesi istenen kişisel verileri, talebin imkânsız olmaması, verilerin düzeltilmesinin aşırı çaba gerektirmemesi ve iddianın asılsız olmaması halinde düzeltmekle yükümlüdür.[283]

Türk hukukunda ilgili kişinin kişisel verilerinin düzeltilmesi hakkına yönelik özel bir düzenleme ise 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'da yer almaktadır. İlgili Kanun'un 9. maddesine göre "*internet ortamında haklarının ihlal edildiğini düşünen kişi, içerik sağlayıcısına, buna ulaşamaması halinde yer sağlayıcısına başvurarak kendisine ilişkin içeriğin yayından kaldırılması ve hazırladığı cevabın bir hafta süreyle internet ortamında yayımlanmasını isteyebilir*". Kişisel verilerin işlenmesinde oluşan hataların giderilmesine imkân veren bu kanun hükmü, verilerin korunmasında önemli bir araç olarak kullanılabilecektir.[284]

3.1.2.1.3. Kişisel Verilerin Silinmesini veya Yok Edilmesini İsteme Hakkı

Bilişim teknolojilerinin gelişmesi ile birlikte kişiler hakkında gerekli gereksiz oldukça verinin kaydedilir hale gelmesi veri kirliliğini meydana getirmektedir. Bu veri kirliliği sebebiyle de ilgili kişiye kişisel verilerinin silinmesi veya yok edilmesi hakkı getirilmiştir. Bu hak, ilgili kişi aleyhine herhangi bir zarar oluşmamış olsa dahi kullanılabilecektir.[285]

Kişisel verilerin silinmesi veya yok edilmesini isteme hakkı, veri koruma hukuku bakımından Avrupa ve Türk hukukunda değişik biçimde değerlendirilmekte olup, Avrupa'daki hukuk sistemlerinde "unutulma hakkı" kapsamında değerlendirilirken, Türk hukukunda doğrudan silme ya da yok etmenin istenebilmesi kapsamında değerlendirilmektedir.[286] Türk hukuk mevzuatında henüz kavramsal olarak doğrudan bir düzenleme olarak kendine yer bulamayan ve hali hazırda 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un 9/10 maddesinde dolaylı olarak,[287] Kişisel Verileri Koruma

---

283 Dülger, *Kişisel Verilerin Korunması*, 486.
284 Kılınç, "Anayasal Bir Hak", 1138.
285 Dülger, *Kişisel Verilerin Korunması*, 491.
286 Gürener, "Avrupa Birliği Genel, 64.
287 5651 sayılı Kanun'un 9/10. maddesinde "*İnternet ortamında yapılan yayın içeriği nedeniyle kişilik hakları ihlal edilenlerin talep etmesi durumunda hâkim tarafından, başvuranın adının bu madde kapsamındaki karara konu internet adresleri ile ilişkilendirilmemesine karar verilebilir. Kararda, Birlik tarafından hangi arama motorlarına bildirim yapılacağı gösterilir."* hükmü yer ilk bakışta

Kurulu kararları, Anayasa Mahkemesi kararları[288] ile yüksek yargı organlarının kararlarında değinilen[289] unutulma hakkının, Kurulun 2020/481 sayılı kararı[290] uyarınca bir üst kavram olarak değerlendirilebileceği belirtilmiştir.[291]

GDPR'ın 17. maddesinde "unutulma hakkı" olarak düzenlenen bu hak kapsamında veri sahibinin, veri sorumlusundan kendisini ilgilendiren kişisel verilerin ivedilikle silinmesini talep etme hakkı bulunmaktadır. Buna bağlı olarak veri sorumlusu, aşağıda belirtilen durumlardan birinin varlığı ve geçerli olması halinde, veri sahibinin kişisel verilerini gecikmeksizin silmekle yükümlüdür:[292]

- Kişisel verilerin işlenme veya toplanma amaçları doğrultusunda artık gerekli olmaması,
- Kişisel veri sahibinin işleme faaliyetinin dayanağı olan rızayı geri alması ve işleme faaliyetiyle alakalı başkaca kanuni bir dayanağın olmaması,

---

unutulma hakkı ile ilişkili görünmektedir. Unutulma hakkı, kişisel verisi işlenen kişilerin internet ortamında bulunan kişisel verilerinin arama sonuçlarında kendi adlarıyla bağlantılı olmamasını talep etme hakkı şeklinde tanımlanabilir. Yargıtay Hukuk Genel Kurulu'nun 2014/4-56 E., 2015/1679 K. sayılı ilamında unutulma hakkı "*üstün bir kamu yararı olmadığı sürece, dijital hafızada yer alan geçmişte yaşanılan olumsuz olayların bir süre sonra unutulmasını, başkalarının bilmesini istemediği kişisel verilerin silinmesini ve yayılmasının önlemesini isteme hakkı"* olarak tanımlanmaktadır. Bu doğrultuda unutulma hakkının istisnasını kamu yararıdır. 5651 sayılı Kanun'un 9/10. fıkrasındaki talep ile unutulma hakkı arasında her ikisinin de internete ilişkin olması nedeniyle ortak nokta bulunmakta olup sağladığı koruma göz önüne alındığında 5651 sayılı Kanun'un daha geniş koruma sağladığı söylenebilir. Bununla birlikte aksini savunan görüşler de mevcuttur. Bkz: akt. Aişe Sena Doğan, "Kişilik Hakkının 5651 Sayılı Kanun'un 9. Maddesi Kapsamında Korunması", *Bilişim Hukuku Dergisi*, 2/2 (Aralık 2020): 143-180, 166-167. (E.T. 09.07.2024), https://dergipark.org.tr/tr/download/article-file/1377099

288 Anayasa Mahkemesi, 03/03/2026 tarihli ve 2013/5653 başvuru numaralı N.B.B. başvurusunda Anayasa'da açıkça düzenlenmeyen unutulma hakkının, Anayasanın 5., 17., ve 20. maddelerinin doğal bir sonucu olduğunu ifade etmiştir. Bu kapsamda unutulma hakkının, internet ortamında bir haberin uzun süredir kolayca ulaşılabilir olması nedeniyle kişinin şeref ve itibarının zedelenmesi durumunda gündeme geleceği; hakkın amacının, internetin yaygınlaşması ve sağladığı faydalar sebebiyle ifade ve basın özgürlükleri ile kişilerin manevi varlığının geliştirilmesi hakkı arasında gerekli hassas dengenin kurulmasını sağlamak olduğu belirtilmiştir. Bkz: https://www.anayasa.gov.tr/media/3911/2013-5653.pdf (E.T. 04.07.2024)

289 Ezgi Akmenek, "Türk Hukukunda Kişisel Verilere Yönelik Unutulma Hakkı", (Yayımlanmamış Yüksek Lisans Tezi, İstanbul Üniversitesi, 2022), 86. (E.T.07.01.2023), https://tez.yok.gov.tr /UlusalTezMerkezi /tez SorguSonucYeni. jsp

290 Kişisel Verileri Koruma Kurulu'nun "Kişilerin Ad ve Soyadı ile Arama Motorları Üzerinden Yapılan Aramalarda Çıkan Sonuçların İndeksten Çıkarılmasına Yönelik Talepler ile ilgili olarak Kişisel Verileri Koruma Kurulunun 23/06/2020 Tarihli ve 2020/481 Sayılı Kararı" için bkz: (E.T.17.12.2023) https://www. kvkk.gov.tr /Icerik /6776/2020-481

291 Gürener, "Avrupa Birliği Genel", 64.

292 Dülger, *Kişisel Verilerin korunması*, 499-504; Dülger, "Avrupa Birliği Genel", 155-156.

- Kişisel veri sahibinin işleme faaliyetine itiraz etmesi ve veri işleme faaliyeti için başkaca önemli herhangi bir yasal nedenin mevcut olmaması,

- Kanuna aykırı şekilde veri işlenmiş olması,

- Veri sorumlusunun uymakla yükümlü olduğu birlik ya da üye devlet hukukundaki bir kanuni sorumluluğa uyumlu olması için kişisel verilerin silinmesinin zorunluluğu,

- Çocuklara verilen çevrimiçi hizmetler hükmü ile alakalı olarak toplanan kişisel verilerin söz konusu olması.

Türk hukukunda silme veya yok etme hususu, KVKK'nın 7. maddesi uyarınca kural olarak veri sorumlusunun yükümlülüğündedir. Bu bağlamda veri sorumlusunca işlenen kişisel verinin işleme amacının olmaması halinde veri sorumlusu tarafından kendiliğinde veya ilgili kişinin talebi üzerine bu işlem gerçekleştirilmelidir.[293] İlgili kişinin veri sorumlusundan kişisel verilerin silinmesini ya da yok edilmesini istemesi halinde işleyecek süreç Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik (Yönetmelik) ile düzenlenmiştir.[294] Yönetmelik'in 11. maddesinde "*kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa*" ilgilinin talebinde bahsettiği kişisel verilerinin silineceği, yok edileceği yahut anonim hale getirileceği; "*kişisel verileri işleme şartları tamamen ortadan kalkmış ve talebe konu veri üçüncü kişilere aktarılmışsa*" veri sorumlusunun durumu üçüncü kişiye bildireceği ve üçüncü kişinin bu Yönetmelik kapsamında gereken iş ve işlemlerin yerine getirilmesini temin edeceği düzenlenmiştir. Kişisel verilerin yasalara uygun şekilde işlenmesi adına uyulması gereken genel ilkelerin belirtildiği KVKK'nın 4/2-d hükmü uyarınca "*kişisel veriler ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmelidir*". Genel ilkeler, Kanun ve Yönetmelik hükümleri birlikte değerlendirildiğinde ilgili kişi KVKK'nın 11. maddesi doğrultusunda kişisel verilerin silinmesi veya yok edilmesi hakkını veri sorumlusuna yönelttiğinde veri sorumlusu:

- Kişisel veriler için ilgili oldukları mevzuatta bir saklanma süresi öngörülmesi

293 Gürener, "Avrupa Birliği Genel", 64-65.
294 Günbey, "Kişisel Verilerin Korunması", 141.

halinde, öngörülen süre dolmuşsa,

- Kişisel veriler için ilgili oldukları mevzuatta saklama süresi öngörülmüyor ancak veri işleme amacının gerektirdiği makul süre geçmişse,

- Belirlenen veri işleme amacı gerçekleşmişse ya da amacın gerçekleşmeyeceği anlaşılmışsa ve verilerin daha fazla elde tutulması için de başka bir hukuki dayanak kalmamışsa ilgili kişinin talebini yerine getirmelidir.[295]

Veri işleme amacına ilişkin ise her somut olayın özellikleri kendi içerisinde dikkate alınmak koşulu ile uygunsa şu kriterler dikkate alınabilecektir:[296]

- KVKK'nın 5. maddesinin 2. fıkra hükmünde ve özel nitelikli kişisel veriler için düzenlenen 6. maddesinin 3. fıkra hükmünde belirtilen veri sahibinin açık rızası olmadan kişisel verilerin işlenebileceği durumların ortadan kalkması halinde[297] (Kişisel verilerin işlenmesi için gereken hukuki dayanak değiştirilmiş yahut ilga edilmişse, taraflar arasında sözleşme kurulmamış, sözleşme kurulmuş ancak geçersiz bir sözleşme kurulmuş, sözleşme kendiliğinden sona ermiş, sözleşme feshedilmiş yahut sözleşmeden dönülmüşse vb.),

---

295 Çelikel, *Kişisel Verilerin Korunması*, 99.
Bu noktada "Devlet" tüzel kişisinin de bir veri sorumlusu olduğu göz önüne alındığında özellikle idari faaliyetler kapsamında tarafından işlenen kişisel verilere ilişkin sorunlar gündeme gelmektedir. Şüphelilerin tespiti ve delil toplanması amacıyla Polis Vazife ve Salâhiyet Kanunu md. 5, Ek md. 7 ve CMK 332. md. doğrultusunda adli mercilerin talebi üzerine kolluk tarafından toplanan verilerin "otomatik veri inceleme" yetkisiyle nasıl kullanılacağını açıkça düzenlenmemektedir. Bu durum, soruşturma konusu suçla ilgisi olmayan birçok kişinin kişisel ve hassas verilerinin sınırsız bir şekilde incelenmesine yol açmaktadır ki bu verilerin ne zaman ve nasıl imha edileceğine dair açık bir düzenleme bulunmamaktadır. KVKK'nın yeterli ve uygun güvence sağladığı düşünülse de bu Kanun'un 28/1-d md. hükmü uyarınca "*Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi*" Kanun'un kapsamı dışında bırakılmıştır. Ayrıca Kanun, suç önleme, soruşturma ve kovuşturma süreçlerinde veri sorumlusunun aydınlatma yükümlülüğünü de kaldırmıştır. Bu sebeple, otomatik veri incelemeleri konusunda KVKK, bireylerin kişisel verilerinin korunması açısından yeterli güvence sağlamamaktadır. Türk hukukunda, temel hak ve hürriyetlerin korunması açısından, şüphelilerin tespiti ve delil elde edilmesi amacıyla kamu kurumları ve özel kişiler tarafından tutulan verilerin elde edilmesi, incelenmesi, mevcut verilerle karşılaştırılması ve artık ihtiyaç kalmadığında silinmesine yönelik açık bir yasal düzenlemeye ihtiyaç olduğu açıktır. Bkz: Fatih Birtek ve Beyza Nur Topal, "Dijital İspat Aracı Olarak Sabit veya Ankesörlü Telefonlara İlişkin Arama Kayıtları ve Bu Kayıtların İspat Kuvveti", *Galatasaray Üniversitesi Hukuk Fakültesi Dergisi*, 2 (2023): 1137-1178, 1152-1153.

296 Turan, *Karşılaştırmalı Hukukta Kişisel,* 128-129.

297 Hilal Tuğba Öksüzoğlu, "6698 Sayılı Kişisel Verilerin Korunması Kanunu ve Avrupa Birliği Hukukunda Kişisel Verilerin Silinmesi ve Düzeltilmesi", *Bilişim Hukuku Dergisi*, 1/2 (2019): 185-242, 207-209. (E.T.27.01.2023), https://www.jurix.com.tr/article/32152

- Veri işleme açık rızaya dayalı olarak yapılmış olmasına rağmen ilgili kişi rızasını geri çekmişse,

- Veri işlemenin "hukuka ve dürüstlük kuralına" aykırı olduğu tespit edilmişse, veri sorumlusu resen yahut ilgilinin talebi üzerine yükümlülüğünü yerine getirmek durumundadır. Bu yükümlülüğü yerine getirmeyen veri sorumlularının ayrıca cezai sorumlulukları da bulunmakta olup kanunlarda belirtilen süreler geçmesine rağmen verileri sistem içerisinde yok etmekle sorumlu olanlar görevlerini ifa etmedikleri takdirde hapis cezasıyla cezalandırılabileceklerdir. TCK'nın 138. maddesi ile düzenlediği "kişisel verileri yok etmeme suçu" kişisel verilerin korunması açısından önem arz etmekte olup belirlenen yasal çerçeve nedeniyle kaydedilen verilerin öngörülen sürenin sonunda imha edilmesinin gerektiği hüküm altına almıştır.[298] Öte yandan kişisel verileri işleme koşullarının hepsinin ortadan kalkmadığı hallerde ilgili kişinin isteği veri sorumlusunca KVKK'nın 13/3 maddesi doğrultusunda sebepleri de açıklanmak suretiyle reddedilebilir (Yönetmelik m. 12/1-c).

3.1.2.1.4. Kişisel Verilerin Aktarıldığı Üçüncü Kişilere Bildirilmesini İsteme Hakkı

İlgili kişi usulüne uygun bir şekilde Kanun'da belirtilen ve yukarıda izah edilen silme veya düzeltme hakkını kullandıktan sonra veri sorumlusu tarafından bu talepler yerine getirildiğinde bu işlemlerin kişisel verilerin daha önce aktarılmış olduğu üçüncü kişilere bildirilmesini talep etme hakkına sahiptir.[299] Başka bir ifade ile veri sorumlusu; silme veya düzeltme talebine konu olan veriyi üçüncü kişilere aktardığında, verilerin aktarıldığı kişiye ya da herhangi bir şekilde veri işleme sürecine dahil olmuş olan başka veri sorumlularına da düzeltme ve silme hakkının kullanıldığına ilişkin bilgi vermelidir.[300] İlgili kişinin bu talebini mutlaka silme veya düzeltme işleminden sonra yöneltmesi şart olmayıp, iki talep de aynı anda veri sorumlusuna iletilebilir.[301]

---

298 Kılınç, "Anayasal Bir Hak", 1133.
299 Dülger, *Kişisel Verilerin Korunması*, 506.
300 Çelikel, *Kişisel Verilerin Korunması*, 101.
301 Dülger, *Kişisel Verilerin Korunması*, 506

3.1.2.1.5. Otomatik Karar Alınmasını Kısıtlama Hakkı

Otomatik karar alınması, verinin otomatik yollarla işlenmesi neticesinde insan müdahalesi olmadan karar alınmasını ifade eder.[302] Otomatik kararlar, bir otomatik veri işleme sürecine dayanarak verilmektedir fakat her koşulda sadece otomatik bir sürece dayanması gerekmemektedir. Başka bir ifadeyle, veri sorumlusunca, veri sahibinin kişisel verileri bir otomatik veri işleme sürecine dahil edilip bunun sonrasında bu veri işleme sürecinin sonuçları bir insan tarafından değerlendirilmeye tabi tutulursa, yine bir otomatik veri işleme sürecine dayanan karardan bahsedilecektir.[303]

Kişisel veri sahibi olan ilgili kişinin otomatik kararların konusu olmama hakkı kişisel özerklik ile yakından ilgilidir. Bu hak, ilk kez 1978 tarihli eski Fransız Veri Koruma Kanunu'nda (Bilgi Teknolojileri, Veri Dosyaları ve Bireysel Özgürlükler Kanunu)[304] düzenlenmiştir. 95/46/EC sayılı Direktif'in 15/1 maddesi uyarınca da "*her bireye kendisine yönelik hukuksal sonuçlar doğuran, kendisini önemli ölçüde etkileyen ve işindeki performansı, itibarı, güvenirliği, davranışları gibi kişisel durumların değerlendirilmesi saikiyle sadece otomatikleştirilmiş veri işlenmesine dayanan bir karara tabi olmama hakkı*" tanınmaktadır. Bu madde ile kişiye, insan müdahalesinin bulunmadığı kararların konusu olmama hakkı verilmektedir.[305] Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına İlişkin 108 Sayılı Sözleşmede de üye ülke vatandaşlarının temel hak ve hürriyetleri ile bilhassa kendisi ile alakalı kişisel verilerin otomatik işleme maruz bırakılması karşısında özel yaşama saygı hakkı teminat altına alınmaktadır.

Bu hak KVKK 11/g maddesinde *"işlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme"* hakkı olarak kaleme alınmıştır. Örnek vermek gerekirse bir otomobilin hızının trafik kameraları ile ölçülüp ve bu ölçüme binaen trafik cezası düzenlenmesi,

---

302 Dülger, *Kişisel Verilerin Korunması*, 506

303 Neslihan Kavak Güven, "Avrupa Birliği Genel Veri Koruma Tüzüğü Doğrultusunda Profilleme ve Otomatik Karar Alma" (Yayımlanmamış Yüksek Lisans Tezi, TOBB Ekonomi ve Teknoloji Üniversitesi, 2022), 31. (E.T.23.01.2023), https://tez.yok.gov.tr/UlusalTezMerkezi/tez-SorguSonucYeni.jsp

304 Kavak Güven, "Avrupa Birliği Genel", 42.

305 Küzeci, *Kişisel Verilerin Korunması*, 263; Emine Hizarcı, *6698 sayılı Kişisel Verilerin Korunması Kanunun AB Veri Koruma Hukuku Işığında Değerlendirilmesi*, (Ankara: Yetkin Yayınları,2020), 45.

otomobili kullanan şahsın hız sınırı üstünde araç kullandığı ile ilgili bir otomatik karar alma süreci;[306] işçilerin giriş çıkış takibinin kart okutularak yapıldığı bir işyerinde, yalnızca bu kayıtlara göre otomatik ücret kesilmesi süreci otomatik karar alma sürecidir.[307] Avrupa Birliği Adalet Divanı bir kararında kişisel verilerin internet sayfasına yüklenmesi işlemini otomatik şekilde gerçekleştirilen bir veri işleme olduğu yönünde değerlendirmede bulunmuştur.[308]

İlgili kişinin otomatik yollarla alınan karara itiraz edilebilmesi için Kanun hükmünde belirtildiği üzere otomatik yollarla alınan kararın ilgilisi aleyhine önemli etkiler doğuracak nitelikte olması gerekmektedir. Öte yandan hangi kararların ilgilisi üzerinde önemli etki doğuracağı ve Kanun maddesinde belirtilen "münhasırlık"tan kastın ne olduğuna dair açıklık yoktur.[309] Dolayısıyla aleyhe etkinin ve münhasıran otomatik yollarla kişisel veri işlemenin somut olayın özelliklerine göre değerlendirilmesi gerekmektedir. Örneğin, bir çevrimiçi TV platformunda kullanıcıların önceki izlenme tercihleri uyarınca yeni izleme seçeneklerinin sunulması halinde otomatik karar alma süreci işletilmişken, ilgili kişi açısından aleyhe bir sonuç doğmadığından itiraz hakkı bulunmamaktadır. İlgili kişinin otomatik karar alınmasını sınırlama hakkı mutlak olmayıp ilgili kişi ve veri sorumlusu arasında yapılan anlaşma gereğince sözleşmenin yerine getirilmesi için zorunlu olması, veri sorumlusunun uymakla yükümlü olduğu ve ilgili kişinin hakları, hürriyetleri ve meşru menfaatlerinin korunması için gerekli önlemlerin bildirildiği hukukun otomatik karar alım sürecine izin vermesi ve ilgili kişinin açık rızasının bulunması hallerinden en az birinin mevcudiyeti halinde bu hak kullanılamayacaktır.[310]

3.1.2.1.6. Zararın Giderilmesini İsteme Hakkı

İlgili kişi, kişisel verilerinin işlenmesinden ötürü meydana geldiğini iddia ettiği bir mağduriyet karşısında Kişisel Verileri Koruma Kurumuna (Kurum) şikâyet yolu veya genel olarak dava yolunu seçebilecektir. Dava yolunun tercih edilmesi halinde meydana

306 Kavak Güven, "Avrupa Birliği Genel", 32.
307 Dülger, *Kişisel Verilerin Korunması*, 507.
308 Judgment in Case, C-101/01 Bodil Lindqvist - Åklagarkammaren i Jönköping 06.11.2003, (E.T. 11.03.2024), https://curia.europa.eu/juris/liste.jsf?num=C-101/01; Hizarcı, *6698 Sayılı Kişisel,* 89.
309 Kavak Güven, "Avrupa Birliği Genel", 33.
310 Dülger, *Kişisel Verilerin Korunması*, 509.

gelen vakıanın Türk Ceza Kanunu kapsamına alınan bir suç olup olmadığı mühimdir. Zira ilgilinin karşılaştığı durumda TCK'yı ilgilendiren talepler mevcutsa, bu taleplerin yargı mercilerinin görev alanına girmesi nedeniyle Kurum tarafından değerlendirilmesi mümkün değildir.[311] Bu kapsamda ilgili kişinin mağduriyetine sebep olan fiil suç değil ise kişi zararın giderilmesi için önce veri sorumlusuna başvuracak, bu yolun tüketilmesinin ardından birtakım süreler doğrultusunda, veri sorumlusundan gelen bir yanıt olur ve yanıttan memnun kalmaz ya da hiçbir yanıt alamazsa Kurula şikâyet yolundan yararlanabilecektir.[312] Buna ek olarak ilgili kişinin şikâyet hakkını kullanması kişinin tazminat hakkını kullanmasına halel getirmeyeceğinden genel hükümlere göre dava açma hakkı da aynı zamanda kullanılabilecektir.[313]

İlgili kişinin veri sorumlusuna başvurusu karşısında veri sorumlusunun önünde KVKK 13 ve 14. maddeleri uyarınca üç seçenek vardır:

- Başvuru kabul edilerek talebin gereği yerine getirilecek,
- Reddetme gerekçesini de belirtmek suretiyle başvuruyu reddedip, ret cevabını yazılı veya elektronik ortamda ilgili kişiye bildirecek,
- 30 gün suskun kalarak başvuruyu zımni olarak reddetmiş sayılacaktır.

Bu aşamada veri sorumlusunun yükümlülüklerinin doğması için de kişisel verilerin kanuna aykırı şekilde işlenmesi, bu işleme faaliyetinden ötürü bir zararın doğması, zararın meydana gelmesine hukuka aykırı işleme faaliyetinin neden olması, başka bir ifade ile zarar ve fiil arasında uygun nedensellik bağının mevcudiyeti gerekmektedir.[314]

Veri sorumlusu, sorumluluk şartlarının doğması neticesinde ilgili kişinin talebini yerine getirdiği takdirde herhangi çekişme söz konusu değildir. Öte yandan veri sorumlusunun talebi doğrudan yahut zımnen reddetmesi veya talebi kısmen ya da tamamen karşılamaması nedeniyle Kurula şikâyet yoluna başvurulduğunda ne olacağı sorunu

311 Kişisel Verileri Koruma Kurumu, "İlgili Kişinin Hak Arama Yöntemleri", (E.T. 04.07.2024), 12-13, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/353d85d5-87df-4c91-b08e-b4f0991a80f4.pdf; Gürener, "Avrupa Birliği Genel", 77

312 Gürener, "Avrupa Birliği Genel", 78.

313 Başar, *Türk İdare Hukuku,* 279.

314 Akgül, *Danıştay ve Avrupa İnsan*, 263-272.

gündeme gelmektedir. Burada ilgili kişi Kurula şikâyet yoluyla veri sorumlusundan tazminat talep ettiğinde bu talebe olumsuz cevap vermek gerekecektir. Zira, Kurula şikâyeti düzenleyen Kanun'un 14/3. maddesinde, ilgili kişinin kişilik haklarının ihlal edilmesi durumunda, genel hükümlere atıf yapılarak tazminat talep edilebileceği ifade edilmekle, Kurulun tazminat belirleme işine girmemesi gerektiği bu işin genel mahkemelere bırakıldığı anlaşılmaktadır. "İlgili Kişinin Kişisel Verilerinin Hukuka Aykırı İşlendiği İddiası Kapsamında Veri Sorumlusu Bankadan Talep Ettiği Tazminat Talebinin Karşılanmaması Hakkında Kişisel Verileri Koruma Kurulunun 16/01/2020 Tarihli ve 2020/41 Sayılı Kararı"[315] da bu yöndedir.[316]

İlgili kişinin tazminat talepleri ile ilgili genel hükümlere atıf yapılmış olsa da ilgili kişi veri sorumlusuna karşı TMK'da yer alan diğer korunma ve dava yollarına da başvurabilecektir.[317] Zira TMK'nın 23. 24. ve 25. maddelerinde, kişilik hakkına yönelik bir saldırıyla karşı karşıya kalan kişinin bu saldırıya karşı nasıl koruma altına alınacağı ve saldırı karşısında kişiliğini korumak adına hangi yollara başvuracağına dair genel ilkelere yer verilmektedir. Bu doğrultuda kişisel veri sahiplerinin, kişisel verilerinin hukuka aykırı şekilde işlendiği ve bu nedenle zarara uğradığı gerekçesi ile genel hükümlere göre:

- Saldırı tehlikesinin önlenmesi,
- Saldırıya son verilmesi,
- Saldırının hukuka aykırılığının tespit edilmesi,
- Hükmün ilanı,
- Maddi tazminat,
- Manevi tazminat,

315 Kişisel Verileri Koruma Kurumu, İlgili Kişinin Kişisel Verilerinin Hukuka Aykırı İşlendiği İddiası Kapsamında Veri Sorumlusu Bankadan Talep Ettiği Tazminat Talebinin Karşılanmaması Hakkında Kişisel Verileri Koruma Kurulunun 16/01/2020 Tarihli ve 2020/41 Sayılı Kararı, (E.T. 17.12.2023) https://www.kvkk.gov.tr/Icerik/6714/2020-41

316 Çelikel, *Kişisel Verilerin Korunması,* 158.

317 Develioğlu, *6698 Sayılı Kişisel*, 129.

- Vekaletsiz iş görme,

- Sebepsiz zenginleşme davası açma hakkı bulunmaktadır.[318]

Elbette ki bu başvuru yolları veri sorumlusunun özel hukuk kişisi olması halinde başka bir tabirle özel hukuk hükümlerine tabi gerçek veya tüzel kişi olması durumunda başvurulacak dava yollarıdır. Veri sorumlusu kamu kurumu olduğunda ise idare hukuku prensipleri uygulanacaktır. Veri sorumlusunun idare hukukuna tabi olması durumunda ilgili kişi, İYUK'a göre dava haklarını kullanabilir. Bu doğrultuda "*2.4.3.1. Kişisel Verilerin Yargısal Yolla Denetlenmesi*" başlığı altında ifade edildiği üzere özetle, ilgili kişinin idari yargıda iptal davası ve ihlal sebebiyle doğan zararın tazmin edilmesi için tam yargı davası açması imkân dahilindedir.

3.1.2.2. İlgili Kişinin Kurula Şikâyet Hakkı

Veri koruma hukukunca ilgili kişilere tanınan haklar, veri sorumlusuna başvuru yoluyla kullanılabilecektir. Zira ilgili kişinin haklarına yer verilen KVKK'nın 11/1. maddesinde, "*herkes, veri sorumlusuna başvurarak*" ifadesi kullanılarak bu hususa vurgu yapılmıştır.[319] Dolayısıyla öncelikle veri sorumlusuna başvuru yapan ilgili kişinin, bilgi talep etme başvurusuna yönelik veri sorumlusundan detaylı bir bilgilendirme yanıtı alması mümkünken; kişinin silme, düzeltme gibi bir işlemin uygulanmasına yönelik talebine karşı bu işlemin gerçekleştiğine ilişkin bir yanıt alması da olasıdır. Ancak ilgili kişinin başvurusuna yönelik yeterli ya da herhangi bir yanıt alamaması da mümkündür. Kanun, ilgili kişinin buna benzer değişken haller karşısında haklarını kullanması için ikili bir hak arama usulü düzenlenmiştir. İdare hukukunda düzenlenen ve merci tecavüzü olarak ifade edilen tanıma benzeyen biçimde Kanun, ilgili kişinin öncelikle veri sorumlusuna başvuru yapmasını; ardından şikâyet hakkı çerçevesinde Kurula başvuruda bulunmasını düzenlemiştir.[320] Bu sebeple öncelikle veri sorumlusuna başvuru yapmak zaruridir. Ancak, buradaki zorunluluk Kurula şikâyet yoluna başvuracak ilgililer için söz konusudur ki doğrudan dava yoluna gitmek isteyenler için veri sorumlusuna başvuru

318 Çelikel, *Kişisel Verilerin Korunması*, 197-218.; Saygı, "6698 Sayılı Kanun'un".
319 Çelikel, *Kişisel Verilerin Korunması*, 165.
320 Hizarcı, *6698 Sayılı Kişisel*, 161.

zorunluluğu yoktur.[321] Başka bir ifade ile Kanun ile düzenlenen veri sorumlusuna başvuru yapma ve şikâyet yolu, bireylerin genel hükümler uyarınca elinde olan dava haklarına seçenek oluşturmaktadır.[322] Öte yandan ilgili kişilerin kişisel veri ihlallerine hızlı müdahale edebilme şansı olması, masrafsız ve daha hızlı sonuç alması ve veri sorumlularının veri işleme süreçlerinin ilgili kişiler ve Kurul tarafından denetlenebilmesinin sağlanması mümkün olan başvuru ve şikâyet yollarını kullanması menfaatlerine olacaktır.[323]

İlgili kişinin haklarını nasıl kullanacağı ve bu aşamada veri sorumlusuna düşen yükümlülükler KVKK'nın 13. maddesinde ve Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'in 5. ve devamı maddeleri ile düzenlenmiştir. Bu doğrultuda "*ilgili kişi, yazılı veya kayıtlı elektronik posta (KEP) adresi, güvenli elektronik imza, mobil imza ya da ilgili kişi tarafından veri sorumlusuna daha önce bildirilen ve veri sorumlusunun sisteminde kayıtlı bulunan elektronik posta adresini kullanmak suretiyle veya başvuru amacına yönelik geliştirilmiş bir yazılım ya da uygulama aracılığıyla*" veri sorumlusuna başvuru yaparak 11. maddede belirtilen haklarını kullanabilecektir. Veri sorumlusu kendisine iletilen başvuruları işlevsel, hukuka ve dürüstlük kuralına uygun şekilde neticelendirmek üzere gereken bütün teknik ve idari önlemleri almakla sorumlu olup başvuruyu kabul eder ya da nedenini izah ederek reddeder. Yapılan başvurular kural olarak ücretsizdir.

Veri sorumlusu tarafından başvurunun reddedilmesi yahut alınan cevabın yeterli olmaması veya süresi içerisinde yanıt verilmemesi halinde ilgili kişi yanıtı öğrendiği tarihten itibaren 30 gün ve her hâlükârda 60 gün içerisinde Kişisel Verileri Koruma Kuruluna başvurarak şikâyet yolunu kullanabilecektir (KVKK md.14/1). Buradaki şikâyet yolu ihtiyari bir yol olup ilgili kişinin aynı zamanda somut olayın özelliklerine göre yukarıda *"1.2.2.4. Medeni Kanun Kapsamında Kişisel Verilerin Korunması"* ve *"3.1.2.1.6. Zararın Giderilmesini İsteme Hakkı"* başlığı altında anlatılan genel hükümler uyarınca tazminat isteme hakkı bulunmaktadır.[324] 3071 sayılı Dilekçe Hakkının

---

321 Oğulcan Özkan, *Kişisel Verilerin Korunması*, (Ankara: Yetkin Yayınevi, 2020). 161; Aygözer Öngün, *Kişisel Verilerin Korunması,* 217.

322 Saygı, "6698 Sayılı Kanun'un", 38.

323 Uyarer, *Kişisel Verilerin Korunması,* 155; Başar, *Türk İdare Hukuku*,285.

324 Kişisel Verileri Koruma Kurulu 29/06/2022 tarihli ve 2022/630 sayılı *"İlgili kişinin ameliyat sırasında çekilen fotoğraflarının veri sorumlusu hastanede çalışan bir doktorun sosyal medya*

Kullanılmasına Dair Kanun'un 6. maddesine göre bir dilekçede bulunması gereken zorunlu unsurları ihtiva etmeyen şikayetler dikkate alınmayacak olup usulüne uygun olarak yapılan başvurular incelemeye alınacak ve sonucuna Kurul tarafından karar verilecektir. Kurula yapılan bu şikâyet başvurusu Kişisel Verileri Koruma Kurumunun hukuki statüsü nedeniyle idari işlem niteliğindedir.[325] Dolayısıyla ilgili kişi tarafından Kurula yapılan şikâyet başvurusunun reddedilmesi yahut zımnen reddedilmesi halinde ilgili kişiler, bu karara karşı İYUK'taki düzenlemelere göre 60 günlük genel dava açma süresi içerisinde yetkili Ankara İdare Mahkemesi'nde dava ikame edebilirler.[326]

3.1.2.2.1. Şikâyete İlişkin İncelemenin Kapsam ve Sonuçları

Bir uyuşmazlığın Kurul önüne getirilebilmesi için KVKK'nın 15. maddesinde belirtilen durumlardan birinin meydana gelmiş olması gerekmektedir. Buna göre Kurul, ilgili kişiler tarafından yapılan şikâyet başvuru yolu ile yahut ihbar ya da başka bir yolla ihlal iddiasını öğrendiğinde ise kendi görev alanına gören konu ve alanlarda resen inceleme başlatabilecektir.

İnceleme yapıldığı sırada veri işleme faaliyetinin telafi edilmesi zor ya da imkânsız zararlar doğurması veya açık şekilde hukuka aykırılıklar içermesi durumda Kurul, veri işlenmesinin ya da verinin yurtdışına aktarılmasının durdurulması kararı verebilir. Yürütmenin durdurulması koşullarının bu durumda da kıyasen uygulanması zararın artmasının önüne geçilmesi bakımından önem arz etmektedir.[327] Kurulca şikâyet üzerine ya da resen gerçekleştirilen inceleme neticesinde bir ihlalin var olduğu anlaşılırsa, Kurul meydana gelen hukuka aykırılığın giderilmesi için vermiş olduğu kararı ilgililere tebliğ eder. Bu karar, kararın tebliğinden itibaren en geç 30 gün içerisinde uygulanmalıdır. Bu kararın süresinde ya da hiç yerine getirilmemesi halinde kabahat yaptırımı öngörülmüştür. Şikâyet üzerine ya da kendiliğinden yapılan inceleme neticesinde ihlalin yaygın olduğu belirlenirse Kurul tarafından ilke kararı da alınabilir.[328]

---

hesabında paylaşılması" ile ilgili vermiş olduğu kararda ilgili kişinin kendisine maddi tazminat ödenmesi durumunda Kurula şikâyette bulunmayacağına dair teklifine ilişkin yargı yoluna başvurulabileceği hususunda bilgilendirilmesine karar vermiştir. Kararın tam metni için bkz: (E.T. 03.06.2023), https://kvkk.gov.tr/Icerik/7567/2022-630

325 Başar*, Türk İdare Hukuku.*

326 Saygı, "6698 Sayılı Kanun'un", 53.

327 Hizarcı, *6698 sayılı Kişisel*, 165

328 Çelikel, *Kişisel Verilerin Korunması*, 161; Özkan, *Kişisel Verilerin Korunması*, 166.

3.1.2.2.2. Kabahat Yaptırımı

Kişisel verileri koruma hukukunu bir disipline bağlama maksadının sonucu olarak ortaya çıkan kabahat yaptırımları, Kanunun veri sorumlularına yüklediği yükümlülükleri hiç veya gereği gibi uygulamaması halinde söz konusu olabilmektedir.[329] 765 sayılı Türk Ceza Kanunu'nda cürüm ve kabahat olarak ikiye ayrılan suçlar, 5237 sayılı yeni Türk Ceza Kanunu'nda suç karşılığı uygulanacak yaptırımları hapis ve adli para cezaları şeklinde belirlemiştir. Böylece kabahatler genel itibariyle ceza kanunu dışında bırakılmışsa da tamamen müeyyidesiz bırakılmayarak 5236 sayılı Kabahatler Kanunu ile düzenlemiştir. Bu düzenleme ile ceza hukukunun konusu olan "kabahat" yerine, idare tarafından idari usullerle karar verilen "idari yaptırım" kavramı gelmiştir.[330] İdari yaptırımların idari işlem kimliği bulunmaktadır.[331] Dolayısıyla bu yaptırımlar, idari işlem kimliği nedeniyle idari düzeni muhafaza etmeye yönelik olarak tek yanlı ve icraidir.

6698 sayılı Kanun'un "kabahatler" başlığı altında düzenlenen fiillere karşı Kurulun idari yaptırım uygulama yetkisini kullanacağı haller düzenlenmiştir. KVKK'nın 18. maddesinde aydınlatma sorumluluğunu ifa etmeyen, veri güvenliğine ilişkin sorumlulukları icra etmeyen, Kurul tarafından verilen kararları uygulamayan ve Veri Sorumluları Siciline kayıt ve bildirim sorumluluğuna aykırı hareket eden, kişisel verilerin yurtdışına aktarımına ilişkin standart sözleşmenin 5 gün içinde Kurula bildirilmemesi[332] halinde gerçek ve özel hukuk tüzel kişileri hakkında Kurul tarafından idari para cezası uygulanacağı hüküm altına alınmıştır.[333] Kurul'un idari para cezası belirlemesine ilişkin kararlarına karşı Kabahatler Kanunun 3/1-a ve 27 maddeleri uyarınca kararın tebliğinden yahut tefhiminden itibaren en geç 15 gün içerisinde sulh ceza mahkemelerine başvurma

---

329 Çelikel, *Kişisel Verilerin Korunması,* 161

330 Rıza Saka, Ramazan Çağlayan ve Mahmut Koca, *Avrupa Birliği Hukuku, İdare Hukuku ve Ceza Hukuku Açısından Kişisel Verilerin İmhası,* (Ankara: Seçkin Yayıncılık, 2020), 321.

331 Özay İl Han, İdari Yaptırımlar, İstanbul 1985, s.135'ten aktaran Saka, Çağlayan ve Koca, *Avrupa Birliği Hukuku*, 322.

332 12/3/2024 tarihli ve 32487 sayılı Resmî Gazete' de yayımlanan 7299 sayılı Ceza Muhakemesi Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun değişikliği ile KVKK'nın kişisel verilerin yurtdışına aktarımını düzenleyen 9/5 maddesine eklenmiştir: "*Standart sözleşme, imzalanmasından itibaren beş iş günü içinde veri sorumlusu veya veri işleyen tarafından Kuruma bildirilir."* Bu hükme aksi davranış halinde ise yaptırım uygulanacağı 18/1-d maddesi ile hüküm altına alınmıştır. Mezkûr düzenleme 01/06/2024 tarihinde yürürlüğe girmiştir.

333 Kabahatlerin tipiklik, maddi unsurları, kusur ve özel görünüş şekilleri için detaylı açıklamalar için bkz.: Kangal, *Kişisel Verilerin Ceza.*

imkânı bulunmaktaydı.[334] Görüleceği üzere esasında idari işlemlerin yargısal denetiminin idari yargıda gerçekleştirilmesi uygulaması karşısında ayrıksı bir uygulamaya gidilerek 5236 sayılı Kanun ile "kabahatler" karşılığında öngörülen idari yaptırımların yargısal denetimi konusunda genel uygulamanın dışına çıkılarak adli yargı görevli kılınmıştı.[335] Düzenleyici ve denetleyici kurumların idari yaptırım kararlarının tabi olduğu yargısal denetim idari yargıda iken Kişisel Verileri Koruma Kurulunun idari yaptırım kararlarının denetim görevinin idari işlemlerin yargısal denetiminde uzman olmayan ceza mahkemelerine verilmesi yerinde değildi. Zira kabahatlerin suç olmaktan çıkarılmasının ardından idarece uygulanan idari yaptırımların yargısal denetiminin ceza mahkemelerine verilmesi esasında bir sorundur. İdari işlemin unsurlarını oluşturan şekil, yetki, sebep, konu ve amaç unsurlarının denetiminin idare mahkemeleri tarafından yapılması isabetli olduğundan Kurul tarafından verilen idari para cezasının yargısal denetiminin idari mahkemeler tarafından yapılması gerektiği[336] kanaati öğretide tartışılan bir konu iken isabetli bir şekilde Kanun değişikliğine gidilmiştir.

7499 Ceza Muhakemesi Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun[337] ile gelen değişiklikle KVKK'nın 18. maddesine 3. fıkra eklenmiş; "*Kurulca verilen idari para cezalarına karşı, idare mahkemelerinde dava açılabilir"* hükmüne yer verilerek idari yargı denetiminin önü açılmıştır. Bu değişiklik 01/06/2024 tarihinde yürürlüğe girmiş olup 01/06/2024 tarihi itibarıyla sulh ceza hâkimliklerinde görülmekte olan başvurular, bu hâkimliklerce görülmeye devam edecektir (KVKK Geçici Madde 3). Yine bu tarihe kadar idari para cezası ile birlikte idarî yargının görev alanına giren bir karar da ihdas edilmişse Kabahatler Kanunu'nun 27/8. maddesi doğrultusunda idari yaptırım kararına karşı iddia edilecek hukuka aykırılık savunmalarının, idari para cezası

---

334 Çelikel, *Kişisel Verilerin Korunması,* 163.

335 Saka ve Çağlayan ve Koca, *Avrupa Birliği Hukuku,* 326.

336 Saka ve Çağlayan ve Koca, *Avrupa Birliği Hukuku*, 329,330; Adem Akkır, "Kişisel Verileri Koruma Kurulu'nun Vermiş Olduğu Kararların Yargısal Denetimi". İçinde *Güncel Gelişmeler Işığında Kişisel Verilerin Korunması Hukuku Marmara Hukuk Bilimsel Toplantılar Serisi – I.* Editörler Leyla Keser Berber ve Ali Cem Bilgili. 163-184. İstanbul: On İki Levha Yayıncılık, 2020. Anayasa Mahkemesi'nin 2007/115 E., 2009/80 K. 26.11.2009 tarih ve 27418 sayılı Resmî Gazetede yayımlanan 5326 sayılı Kabahatler Kanunu'nun ilgili maddelerinin iptali istemi ile açılan davaya ilişkin kararın tamamına ve bizim de katıldığımız "*idari yaptırımlara karşı ilke olarak sulh ceza mahkemelerini yetkili kılan kuralın iptali gerektiğine*" ilişkin karşı oy yazısına ulaşmak için bkz: (E.T.10.06.2023) https://normkararlarbilgibankasi.anayasa.gov.tr/-Dosyalar/ Kararlar/ KararPDF/2009-80-nrm.pdf

337 12.03.2024 tarihli 32487 sayılı Resmî Gazete 'de yayımlanmıştır. (E.T. 12.03.2024), https://www.resmigazete .gov.tr /eskiler/2024/03/20240312-1.htm

ile beraber idari yargı merciinde ileri sürülebileceği unutulmamalıdır.[338] 01.06.2024 tarihinden sonra ihdas edilen idari para cezalarına karşı ise doğrudan idari yargıda dava açılabilir.

Bahsi geçen hususların yanı sıra bir suç dolayısıyla başlatılan soruşturma esnasında, KVKK'nın 18. maddesinde düzenlenen "kabahat"lerden birinin veya birkaçının vuku bulması halinde Cumhuriyet savcısı tarafından da yaptırım kararı verilebilir veya idari para cezası düzenlenmesi için Kurul'a bildirimde bulunabilir (5236 sayılı Kanun md. 23/1). Cumhuriyet Savcısı tarafından idari para cezası verilebilmesi için Kurul tarafından idari yaptırım kararı verilmemiş olması gerekmektedir (5236 sayılı Kanun md. 23/3). Kovuşturma aşamasında ise bir fiilin kabahat oluşturduğunun tespit edilmesi halinde Mahkeme tarafından da idari yaptırım kararı verilebilir (5236 sayılı Kanun md. 24).[339] Burada istisnai bir yetki söz konusu olmaktadır. Zira idari yaptırımların birer idari işlem olması sebebiyle bu konuda karar verme yetkisi idarededir. Savcıların verilen idari denetim yetkisinin hukuka aykırı olduğu iddiasına yönelik yapılan başvuruda, Anayasa Mahkemesi 2005/108, E. 2006/35 K. sayılı ilamı ile usul ekonomisi gereği hukuka aykırılık iddialarını reddetmiştir. Yine birçok Yargıtay kararında[340] mahkeme tarafından idari yaptırım kararı verilmesinde herhangi bir hukuka aykırılık olmadığına karar vermiştir.[341] Kanaatimizce bu düzenleme ve yaklaşım tarzı KVKK açısından isabetli değildir. Zira "kişisel verilerin korunması" hususu oldukça teknik bir konu olduğundan özel uzmanlık gerektiren bir alandır. Veri koruma hukukunun kendine özgü özellikleri olması sebebiyle ayrı bir idari süreç yürütülmesi gerektiğinden Kabahatler Kanun'un 23. ve 24. maddelerine istisna getirilerek bu konudaki idari yaptırım yetkisi sadece Kişisel Verileri Koruma Kurulu'na bırakılabilir.

338 İnan, "Kişisel Verilerin Korunması", 55.

339 Akkır, "Kişisel Verileri Koruma", 178,179

340 Yargıtay 19. CD., 25.09.2017 tarihli, 2016/15189 E., 2017/7224 K. sayılı ilamı; Yargıtay, 18. CD., 30.01.2017 tarihli, 2015/29255 E., 2017/803 K. sayılı ilamı; Yargıtay, 7. CD., T. 11.10.2022 tarihli, 2022/6584 E., 2022/13886 K. sayılı ilamı

341 Yunus Anıl Ay, "5326 Sayılı Kanun'un 23 ve 24'üncü Maddelerine Göre Cumhuriyet Savcısı ve Mahkeme 213 sayılı Kanun'da Öngörülen Vergi Cezalarını Kesebilir Mi?", *Çağ Üniversitesi Sosyal Bilimler Dergisi*, 20/1 (2023): 58-80, 59-65. (E.T. 11.07.2024), https://dergipark.org.tr/tr/download/article-file/3235627

Bir fiilin hem suç hem kabahat olması[342] durumunda nasıl bir yol izlenmesi gerektiğine dair açıklama yapmakta da fayda vardır. Kabahatler Kanunun 15/3 maddesinde yer alan "*suçtan dolayı yaptırım uygulanamayan hallerde kabahat dolayısıyla yaptırım uygulanacağı"* şeklindeki düzenlemeye göre bir fiil hem suç hem kabahat şeklinde ifade edilmişse yalnızca suçtan ötürü yaptırım uygulanabilir ("non bis in idem"). Dolayısıyla sadece suçtan dolayı müeyyide uygulanmayan durumlarda kabahat nedeniyle müeyyide uygulanır. Bu nedenle TCK'nın 135 vd. hükümlerinde bahsi geçen suçlar için suç nedeniyle yaptırım uygulanacağından idari para cezası yaptırımı uygulanamayacaktır.[343] Başka bir ifade ile kabahat doğuran fiilin, aynı anda suç teşkil etmesi durumunda ceza mahkemesinde mahkûmiyet kararı verilmişse Kabahatler Kanunu'nun 15/3. maddesi doğrultusunda idari yaptırım kararı verilemeyecektir. Failin hakkında ceza verilmesine yer olmadığı ya da kararı verilmesi halinde ise, özel kanunlarda hüküm bulunmamak şartıyla, kabahat açısından da sorumlu sayılmaması gerekmektedir. Bu nedenle idari yaptırım kararı yine verilemeyecektir. [344] Hem TCK'da ifade edilen, kişisel verilerin korunmasına yönelik suç eylemleri, hem de KVKK'da ifade edilen kabahat eylemleri birlikte değerlendirildiğinde, Kurul'un idari yaptırım uyguladığı durumların bir kısmında ihlal konusu fiilin esasında suç teşkil ettiği görülmektedir. KVKK'da, aynı anda (aynı fiile) hem idari yaptırım uygulanacağı hem de ceza yargılamasının gündeme geleceğine ilişkin bir düzenleme bulunmamaktadır. Bu nedenle Kurul'un, bir fiilin, suç teşkil ettiği ya da suç teşkil ettiğinden kuşkulandığı anda idari süreçten çekilmektedir. Zira fiilin Kabahatler Kanunu'nun 15/3. maddesi uyarınca suç dolayısıyla yargılanmasının güvencesinin sağlanması, TCK'nin 139. maddesi doğrultusunda şikâyete tabi olmayan bu suçlar için suçu bildirme sorumluluğunun ifasını da beraberinde getirecektir.[345] Öte yandan KVKK'de, 213 sayılı Vergi Usul Kanunu'nun 367. maddesinde olduğu gibi hem idari hem de cezai sonuçların olacağına dair açık bir düzenleme bulunmadığı sürece, Kabahatler Kanunu'ndaki genel kural olan 15/3. maddesi nedeniyle Kurul'un yaptırım

342 Suç ve kabahatlerin içtimaına ilişkin detaylı açıklamalar ve incelemeler için bkz: Aslıhan Kart ve Muammer Ketizmen, "Kabahatler Kanunu'nun İçtima Hükümleri Açısından Kişisel Verilerin Korunmasına İlişkin Suç ve Kabahatler ile Kurul'un İdari Ceza Kararlarına İlişkin Bir Değerlendirme", *Kişisel Verileri Koruma Dergisi.* 1/2 (2019), 17-29.

343 Akkır, "Kişisel Verileri Koruma", 180.

344 Kart ve Ketizmen, "Kabahatler Kanunu'nun İçtima", 19-20.

345 Kart ve Ketizmen, "Kabahatler Kanunu'nun İçtima", 28.

uygulama yetkisi ile ceza yargılamasının alanının sık sık çakışması ve bazen de çatışması ihtimali ortaya çıkabilir.[346]

3.2. Veri İhlalinin Tespiti

3.2.1. Veri İhlalinin Tespit Edilmesi

Veri ihlalinin nasıl tespit edileceği ile ilgili çerçevesi belirli bir kılavuz veya rehber bulunmamaktadır. GDPR'ın 33. maddesinde ihlalden haberdar olma tarihi veri ihlalinin tespit edildiği tarih olarak esas alınmıştır. Benzer şekilde 24.01.2019 tarih ve 2019/10 sayılı Kurul kararında da ihlalden haberdar olunması ile veri ihlal bildirim yükümlülüğünün başladığı belirtilmiştir. GDPR'da veri ihlalinin tespiti; potansiyel ihlalin somut olay bazında incelenmesi, sınıflandırılması ve tespit edilmesi olmak üzere üç adımda gerçekleştirilmektedir. KVKK'da ise yine potansiyel ihlalin incelenmesi ve tespiti mevcut iken, GDPR'daki gibi sınırları belirli bir sınıflandırma mevcut değildir. Madde 29 Çalışma Grubu rehberi uyarınca veri ihlalinin tespiti; ihlalin veri sorumlusu tarafından doğrudan tespiti, üçüncü kişilerin bildirimi üzerine öğrenilmesi veya veri işleyen tarafından tespiti şeklinde farklı türlerde gerçekleşebilir.[347]

Veri sorumlusu, ihlalin varlığını doğrudan tespit edebilir. Bu durumda, ihlalin gerçekleşip gerçekleşmediğini belirlemek için detaylı bir inceleme yapılır ve ihlalin kişisel veri koruma kurallarıyla uyumlu olup olmadığı değerlendirilir. İhlalin kapsamı belirlenirken, ihlalin sonuçları ve etkileri, ilgili kişilerin hakları ve özgürlükleri göz önünde bulundurulur. Öte yandan, veri ihlali üçüncü taraflar, medya veya diğer kurumlar gibi dış kaynaklardan bildirildiğinde veya tesadüfi bir şekilde ortaya çıktığında, bu da ihlalin tespitinde önemli bir rol oynar. Özellikle veri sızıntıları gibi durumlarda, ihlal genellikle önceden tespit edilmez ve dış kaynaklardan gelen bildirimlerle ortaya çıkar. Ancak, bu tür bir ihlalin gerçek olup olmadığını ve ihlal olarak kabul edilip edilmediğini doğrulamak için veri sorumlusu tarafından ayrıntılı bir araştırma yapılmalıdır. Madde 29 Çalışma Grubuna göre veri sorumlusu, ihlalin varlığını doğruladığında ihlalden haberdar olmuş sayılır. Bu nedenle, ihlalin teyit edilmesi ve bildirimin yapılması süreçlerini içeren araştırmalar, bildirim süresi içinde tamamlanmalıdır. Veri işleyen tarafından

346 Kart ve Ketizmen, "Kabahatler Kanunu'nun İçtima", 28
347 Sevindi ve Ordu, "AB ve Türk Hukukunda", 15.

gerçekleştirilen faaliyetler sırasında da veri ihlali olabilir. Bu durumda, veri işleyenin ihlali tespit ettiği an, veri ihlalinin başladığı an olarak kabul edilir. Haberdar olma kriteri KVKK'ya göre önemli olduğundan, veri işleyenin veri sorumlusuna ihlal hakkında bildirimde bulunduğu tarih, haberdar olma anının başlangıcı olarak kabul edilir.[348]

Öte yandan veri ihlalinin tespiti her zaman kolay olmadığından veri sorumlusu tarafından ihlal durumunda izlenecek yolu gösteren bir kılavuz oluşturulmalıdır. Bu kılavuz sayesinde veri güvenliği ihlallerinin belirlenmesi ve tasnifi sağlanabilecek, şu süreçlerin yürütülmesi için yöntemler belirlenebilecektir:[349]

- Veri güvenliği ihlal yönetiminin bir parçası olarak belirlenmiş hadiselerin raporlanması ve bu hadiselerin tasnifi için süreçlerin uygulanması,
- İhlal olaylarının tasnifinde kategori, aciliyet, etki, öncelik gibi unsurların saptanması,
- İhlal olaylarının ilişkili grup veya alana göre tasnifi
- İhlal bildirim sürecinde ilişkili tarafların organizasyonel sorumluluklarının tespit edilmiş olması ve gerekli yardımın sağlanması.

Bu süreçlerin etkili bir şekilde uygulanması, veri ihlallerinin tespiti ve yönetimi konusunda daha kapsamlı bir kavrayış sağlar. Böylece, veri güvenliği ihlalleriyle başa çıkmak ve bunları hızlı ve etkili bir şekilde ele almak, veri işleyen sıfatına sahip organizasyonun veri koruma standartlarına uyumluluk bakımından daha sağlam bir temel oluşturmasına yardımcı olur.

3.2.2. Veri İhlal Bildirimi

Veri ihlal bildirimi, veri ihlali yaşanması durumunda veri sorumlularının bu ihlalleri hızlı bir şekilde tespit ederek veri koruma otoritelerine bildirmesi gereken bir yükümlülüktür. Ancak, mevzuatta veri ihlali türlerinin net bir şekilde tanımlanmamış olması ve ihlal bildirimi için belirlenen yasal sürelerin her zaman olayın boyutuna veya teknik gereksinimlere uygun olmaması, veri sorumluları için bazı karışıklıklara yol açmaktadır. Bu nedenle, veri sorumlularının, herhangi bir ihlalin varlığını ve başlangıcını doğru bir

348 Sevindi ve Ordu, "AB ve Türk Hukukunda", 15-17.
349 Korucu, *Veri Güvenliğinin İyileştirilmesinde*, 46.

şekilde belirlemeleri önemli olup bu husus ihlali uygun bir şekilde ele alabilmek ve ihlalin etkilerini sınırlamak için gereklidir.[350] Başka bir ifade ile Kurula yapılacak bildirimin amacı ihlalin büyümesinin ve tekrarlanmasının önüne geçilmesidir. Bu doğrultuda veri sorumlusunun kusuru önem taşımamaktadır. Şöyle ki; bildirim yükümlülüğü kusur ve özen sorumluluğundan tamamıyla bağımsızdır.[351]

Madde 29 Veri Koruma Çalışma Grubu tarafından, 2017 yılında henüz GDPR yürürlüğe girmeden önce, veri ihlal bildirimlerine ilişkin bir rehber yayınlamış, kişisel veri ihlal türleri üç başlık altında düzenlemiştir. Bu doğrultuda, kişisel verilerin yetki olmadan veya yanlışlıkla her türden ifşası veya verilere erişilmesi "*gizlilik ihlali (confidentiality breach)"*; kişisel verilerin yetkili olmayanlar tarafından ya da yanlışlıkla imha edilmesi veya kaybedilmesi "*kullanılabilirlik*[352]*/ulaşılabilirlik ihlali (availability breach)"*; kişisel verilerin yetkili olmayanlar tarafından ya da yanlışlıkla değiştirilmesi faaliyeti ise *"bütünlük ihlali (integrity breach*)" olarak tasnif edilmiştir.[353] GDPR'ın 32. maddesi uyarınca, kişisel verilerin işlenmesi sürecinde, ihlallerin henüz doğmadan engellenerek, makul ve kabul edilebilir bir aşamada veri güvenliğinin sağlanabilmesine özel önem verilerek, bunun için gereken ön önlemlerin alınmasına yönelik, veri kontrolörü[354] ve veri işleyicisinin[355] yükümlülükleri düzenlenmiştir. GPDR'ın 33. maddesiyle de kişisel verilerin işlenmesi için güvenliğin temin edilmesine yönelik, veri kontrolörüne, ihlalin gerçekleştiğinin öğrenilmesinin ardından, ivedilikle ve her hâlükârda ihlalin öğrenilmesinden itibaren 72 saat içinde, yetkili denetim makamına bu durumu bildirme sorumluluğu da getirilmiştir.[356]

---

350 Sevindi ve Ordu, "AB ve Türk Hukukunda", 13.

351 Çekin, *Avrupa Birliği Hukukuyla,* 152-153.

352 Hasan Yılmaz, "TS ISO/IEC 27001 Bilgi Güvenliği Yönetimi Standardı Kapsamında Bilgi Güvenliği Yönetim Sisteminin Kurulması ve Bilgi Güvenliği Risk Analizi", *Denetişim*, 15 (2014): 45-59, 47. (E.T. 17.09.2023), https://dergipark.org.tr/tr/pub/denetisim/issue/22466/240291 .

353 İpek Çimen Bulut, "Avrupa Birliği Genel Veri Koruma Tüzüğü Kapsamında Getirilen Yeni Teknik ve Yaptırım Mekanizmalar", *Anadolu Üniversitesi Sosyal Bilimler Dergisi,* 20/2 (2020): 127-142. 129. (E.T. 04.07.2023), Microsoft Word - 8(127-142).docx (dergipark.org.tr)

354 GDPR md.4/7'ye göre veri kontrolörü tek başına ya da başkalarıyla birlikte kişisel verilerin işlenmesine dair amaçlar ve yöntemleri tespit eden gerçek veya tüzel kişi, kamu kuruluşu, kurumu ya da diğer herhangi bir organdır. Türk Hukukunda veri kontrolörü, veri sorumlusudur.

355 GDPR md.4/8'e göre veri işleyicisi kontrolör adına kişisel verileri işleyen bir gerçek ya da tüzel kişi, kamu kuruluşu, kurumu veya diğer herhangi bir organdır.

356 Çimen Bulut, "Avrupa Birliği Genel", 130.

KVKK'nın 12/5. maddesi uyarınca *"İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir."* İlgili madde doğrultusunda kişisel verilerin hukuka aykırı biçimde üçüncü kişiler tarafından ele geçirilmesi durumunda, veri sorumlusunun bu vaziyeti ivedilikle ilgilisine ve Kurula bildirmesi gerekmektedir. Kurulun 2019/10 sayılı ve 24.01.2019 tarihli kararında veri ihlal bildiriminin amacının, veri ihlali nedeniyle meydana gelebilecek olumsuz neticelerin bir an önce engellenmesi veyahut en aza indirilmesine olanak sağlayacak tedbirler alınmasını sağlamak olduğu ifade edilmiştir.[357] Kararın devamında *"6698 sayılı Kanuna kaynak teşkil eden Avrupa Birliğinin 95/46/EC sayılı Direktifini ilga eden Avrupa Genel Veri Koruma Tüzüğünde de veri ihlal bildirimlerine ilişkin olarak Direktifin aksine detaylı düzenlemelere yer verildiği dikkate alındığında Kurul tarafından bu konuda alınacak kararlar arasında herhangi bir uyumsuzluğa mahal verilmemesi ve uygulamada bir standartlaşma sağlanabilmesini teminen*" denilerek kişisel veri ihlali bildirim usul ve esasları belirlenmiştir:[358]

- "*Kanunun 12. maddesinin (5) numaralı fıkrasının "İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir…." hükmünde yer alan "en kısa sürede" ifadesinin 72 saat olarak yorumlanmasına ve bu kapsamda veri sorumlusunun bu durumu öğrendiği tarihten itibaren gecikmeksizin ve en geç 72 saat içinde Kurula bildirmesine, veri sorumlusunca söz konusu veri ihlalinden etkilenen kişilerin belirlenmesini müteakip ilgili kişilere de makul olan en kısa süre içerisinde, ilgili kişinin iletişim adresine ulaşılabiliyorsa doğrudan, ulaşılamıyorsa veri sorumlusunun kendi web sitesi üzerinden yayımlanması gibi uygun yöntemlerle bildirim yapılmasına,*

- *Veri sorumlusu tarafından Kurula haklı bir gerekçe ile 72 saat içinde bildirim yapılamaması halinde, yapılacak bildirimle birlikte gecikmenin nedenlerinin de Kurula açıklanmasına,*

---

357 "Kişisel Verileri Koruma Kurumu, "Kişisel Veri İhlali Bildirim Usul ve Esaslarına İlişkin Kişisel Verileri Koruma Kurulunun 24.01.2019 Tarih ve 2019/10 Sayılı Kararına İlişkin Duyuru", (E.T. 02.09.2023), https://www.kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirimi

358 Kişisel Verileri Koruma Kurumu, "Kişisel Veri İhlali Bildirim Usul ve Esaslarına Duyuru".

- *Kurula yapılacak bildirimde "Kişisel Veri İhlal Bildirim Formu"nun*[359] *kullanılmasına,*

- *Formda yer alan bilgilerin aynı anda sağlanmasının mümkün olmadığı hallerde, bu bilgilerin gecikmeye mahal verilmeksizin aşamalı olarak sağlanmasına,*

- *Veri sorumlusu tarafından veri ihlallerine ilişkin bilgilerin, etkilerinin ve alınan önlemlerin kayıt altına alınması ve Kurulun incelemesine hazır halde bulundurulmasına,*

- *Veri işleyen nezdinde bulunan kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde, veri işleyenin bu konuda herhangi bir gecikmeye yer vermeksizin veri sorumlusuna bildirimde bulunmasına,*

- *Veri ihlalinin yurtdışında yerleşik veri sorumlusu nezdinde yaşanması halinde, bu ihlalin sonuçlarının Türkiye'de yerleşik ilgili kişileri etkilemesi ve ilgili kişilerin sunulan ürün ve hizmetlerden Türkiye'de faydalanmaları durumunda, bu veri sorumlusu tarafından da aynı esaslar çerçevesinde Kurula bildirimde bulunulmasına,*

- *Veri ihlali gerçekleşmesi halinde veri sorumlusu tarafından kendi nezdinde kimlere raporlama yapılacağı, Kanun kapsamında yapılacak bildirimler ile veri ihlalinin olası sonuçlarının değerlendirilmesi hususunda, kendi nezdindeki sorumluluğun kimde olduğunun belirlenmesi gibi konuları içeren bir veri ihlali müdahale planı hazırlanarak belirli aralıklarla bu planın gözden geçirilmesine"*

karar verilmiştir. Veri sorumlusunun ilgili kişiye yapacağı veri ihlali bildiriminde bulunması gereken asgari kriterler ise Kurulun 2019/271 sayılı ve 18/9/2019 tarihli kararı ile düzenlenmiştir.[360]

KVKK'nın 12/5. maddesinin devamında *"Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir."* hükmü yer almaktadır. Bu doğrultuda ihlal bildirimi Kurula intikal ettiğinde Kurul, şu kriterler

359 İlgili form ve kılavuz için bkz: (E.T.15.05.2024), https://ihlalbildirim.kvkk.gov.tr/
360 Bilir, "6698 Sayılı Kişisel", 337.

doğrultusunda inceleme yaparak ihlalin ilan edilip edilmeyeceğine karar verir: İhlalden etkilenen kişisel verinin niteliği (özel nitelikli kişisel veri, dolandırıcılık ihtimaline karşı finans verisi gibi), ihlalden etkilenen kişi sayısı ve ihlalden etkilenen kişilere veri sorumlusu tarafından bildirim yapılamaması. Bu bildirimler Kurulca öncelikli iş olarak değerlendirilmektedir. Zira ilgili kişinin ihlal nedeniyle bir zararla karşı karşıya kalma ihtimali söz konusudur. Buna göre Kurul, bahsi geçen kriterlere göre değerlendirme yapıp gerekli görürse veri ihlallerini internet sitesinde yayınlamaktadır.[361] 2018 ila 2023 arasında Kurum'un internet sitesinde 218 adet veri ihlal bildirimine ilişkin kamuoyu duyurusu yapılmıştır.[362] Veri ihlali bildirimlerinin duyurulmasındaki amaç ise kanaatimizce veri sorumluları açısından şeffaflık ve hesap verebilirlik sağlamaktır. Aynı zamanda veri ihlalinden etkilenen kişilerin, kişisel veri güvenliğiyle ilgili muhtemel riskleri nedeniyle gerekli önlemleri (şifre değişikliği, virüs taraması, depolama, veri sorumlusuna başvuru gibi) almalarına imkân vermektir. Öte yandan veri ihlallerine ilişkin yapılan kamuoyu duyuruları, diğer veri sorumlularını da veri güvenliği önlemlerini artırmalarını, veri aktarımı konusunda daha tedbirli davranmaları konusunda bir uyarı mahiyetinde değerlendirilebilir.

Kurul tarafından yayımlanan faaliyet raporlarında[363] belirtildiği üzere 2022 yılında 260, 2021 yılında 330, 2020 yılında 228, 2019 yılında 139, 2018 yılında 28, 2017 yılında 1 adet veri ihlal bildirimi yapılmış; toplamda yapılan 986 adet veri ihlal dosyasında, sonuçlanan 693 dosya arasından 201 dosyada veri ihlali olduğu tespit edilmiştir.

Kurula herhangi bir bildirimin yapılmaması veya bildirimin zamanında yapılmaması halinde, Kurul bu veri ihlalinden bir şekilde haberdar olursa yine de veri sorumlusunun sorumluluğu gündeme gelecektir. KVKK uyarınca veri ihlalleri yaşandığında bir takım idari para cezası müeyyideleri uygulandığı ve kişilik hakları ihlal edilenlerin, genel

361 Tuba Kendir Tunalı, "Veri Sorumlusunun Yükümlülükleri" içinde *Kişisel Verilerin Korunması Alanında Yeni Gelişmeler Sempozyumu,* ed. Hüseyin Özcan ve Mehmet Başar ve H. Derya Osmanoğlu ve Ferhat Kayış, (Ankara: Adalet Yayınevi, 2021), 40.

362 (E.T. 12.03.2024), https://www.kvkk.gov.tr/veri-ihlali-bildirimi/

363 "Faaliyet Raporu", Kişisel Verileri Koruma Kurumu, (E.T. 07.09.2023), https://www.kvkk.gov.tr/Icerik/2094 /Faaliyet-Raporu

hükümlerde belirtildiği üzere tazminat hakkının da saklı olduğu[364] yukarıdaki bölümlerde açıklanmıştı.

3.3. Kişisel Verileri Koruma Kurulu İlke Kararları

3.3.1. İlke Kararları ve İlke Kararlarının Hukuki Niteliği

Kişisel verilerin korunması alanına ilişkin en önemli başlıklardan birini Kurulun vereceği kararlar oluşturmaktadır. Zira hukuk, Kanun ve ilgili kanuni düzenlemelerin yanı sıra içtihat ile bir bütün olmakta, sonradan yapılan düzenlemeler de genel olarak mevcut içtihatlar sayesinde eksik ya da hatalı olduğu fark edilen somut olaylar doğrultusunda yapılmaktadır.[365] Dolasıyla güncel olan ve henüz kapsam, içerik ve bilhassa uygulama şekli açısından belirsizlikler barındıran kişisel verilerin korunması hukukunun gelişmesi açısından ilke kararları oldukça büyük önem taşımaktadır.

İlke kararlarının yayınlanmasıyla, kişilerin ve veri sorumlularının dikkati çekilerek, benzer konularda sıklıkla karşılaşılan hukuka aykırı uygulamaların engellenmesi hedeflenmektedir. Bu şekilde, ilke kararlarıyla birlikte ilgili konulardaki hukuki standartlar netleştirilmekte ve toplumun bilinç düzeyinin artırılması hedeflenmektedir. Bu sayede, kişisel verilerin işlenmesi sürecinde hukuka uygunluk ve dürüstlük prensiplerine uyulması teşvik edilerek, potansiyel hukuka aykırı durumların önüne geçilmesi amaçlanmaktadır.[366] Bununla birlikte Kanunun uygulanması yönünde rehberlik yapan ilke kararları Kurulun karara konu olaya bakış açısı ile sonraki inceleme ve şikayetlerde takınacağı tavrı da gösterir.[367]

Kanunun 15/6. maddesinde *"şikâyet üzerine veya resen yapılan inceleme sonucunda, ihlalin yaygın olduğunun tespit edilmesi halinde Kurul, bu konuda ilke kararı alır ve bu kararı yayımlar.*" hükmü amirdir. Buna göre ilke kararı alınabilmesi için yasa hükümlerine aykırı uygulamaların yaygın olduğunun tespit edilmesi gerekir. Kurul, faaliyet gösterdiği alanda meydana geldiğini belirlediği yaygın ihlallere karşı yeni ilke

364 Ezgi Alımcı, "Kişisel Verilerin Korunması Hukuku ve Bankaların Güven Kuruluşu Olarak Kabul Edilmesi Kapsamında Banka Bünyesinde Gerçekleşen Veri İhlalinin Değerlendirilmesi." *Ankara Barosu Dergisi,* 80/1 (2022): 47-76, 57. DOI 10.30915/abd.1118300

365 Dülger, *Kişisel Verilerin Korunması,* 375.

366 Çelikel, *Kişisel Verilerin Korunması,* 161

367 Saka, Çağlayan ve Koca, *Avrupa Birliği Hukuku,* 39.

kararı alabileceği gibi ihtiyaç hasıl olduğunda önceden alınmış kararları mevcut gelişmeleri dikkate alarak ve gereksinimleri giderecek şekilde de güncelleyebilir.[368] Her şekilde Kurul tarafından alınan kararların, veri sorumlularınca icra edilmesi kanuni bir vazife olduğu için ilke kararları da tüm ilgililer açısından riayet edilmesi son derece mühim olan ve uygulanması gereken kararlardır.[369]

Kurumun bireysel işlem tesis etme yetkisi olduğu gibi düzenleyici işlem yapma yetkisi de bulunmaktadır. İdarenin düzenleyici işlem yapma yetkisi Anayasa'dan, kanundan, Cumhurbaşkanlığı kararnamesinden ve idari işlevin mahiyetinden kaynaklanabilir. Kurumun kişisel verilerin korunmasına ilişkin düzenleyici işlem yapma yetkisi de asli görevinden doğmaktadır. İlke kararı alma yetkisi kanunla tanınmıştır. Buradaki idari işlemin düzenleyici işlem olup olmadığı ismine göre değil, içeriğine göre tespit edileceğinden Kurulun ilke kararları soyut, genel, uygulamakla sona ermeyen kuralları içermesi nedeniyle düzenleyici işlem sayılır. Bu nedenle yargısal denetimi de yönetmeliklerle aynı kurallara tabidir.[370] Dolayısıyla da ilke kararları gerek kamu kurum ve kuruluşları gerek özel sektör için bağlayıcı niteliği haizdir.[371] Buna göre ilke kararı nedeniyle İYUK 2/1-a maddesi gereğince menfaati ihlal edilenler, ilke kararının yayımlanmasından itibaren 60 gün içinde ilk derece Mahkemesi olarak Danıştay'da iptal davası açabilecektir. Ancak ilke kararının bireysel karara dönüştüğü durumlarda durum farklılık arz etmektedir. İlke kararında belirtilen kurallardan birinin ihlal edilmesi nedeniyle ilgililer hakkında idari yaptırım uygulanması halinde düzenleyici işlem bireysel işleme dönüşeceği için hakkında idari yaptırım uygulanan sorumlu kişi hem hakkında uygulanan yaptırım için hem de ilke kararı için birlikte yahut ayrıca ilke kararının yayımlanmasından itibaren 60 günlük süre geçmiş olsa dahi yaptırım için öngörülen süre içinde ilke kararı için de dava açabilecektir.[372]

368 Başar, *Türk İdare Hukuku*, 292.
369 Saka, Çağlayan ve Koca, *Avrupa Birliği Hukuku*, 39.
370 Saka, Çağlayan ve Koca, *Avrupa Birliği Hukuku*, 309-314.; Başar, *Türk İdare Hukuku*, 292-293.
371 Başar, *Türk İdare Hukuku*, 293.
372 Saka, Çağlayan ve Koca, *Avrupa Birliği Hukuku*, 316,317.

3.3.2. Kişisel Verileri Koruma Kurulu'nun İlke Kararları Doğrultusunda Kişisel Veri İhlallerinin Tasnifi

Kişisel Verileri Koruma Kurulunun Haziran 2024 tarihi itibariyle 8 adet ilke kararı bulunmaktadır. Kararlarda belirtilen ve veri ihlaline neden olan durumlar karar bazında değil, ihlal bazında başlıklar halinde tasnif edilerek incelenmiştir.

3.3.2.1 Veri Güvenliğine İlişkin Veri Sorumlusunun Yükümlülüklerine Aykırılık

3.3.2.1.1. Kişisel Verilerin Hukuka Aykırı Olarak İşlenmesi

Kişisel Verileri Koruma Kurulunun 21/12/2017 tarihli ve 2017/61 sayılı ilke kararı[373] "hukuka aykırı veri işlenmesi" nedeniyle alınmıştır. Kurul tarafından alınan ilk ilke kararı olan bu karar "*rehberlik hizmeti veren internet sitelerinde/uygulamalarında kişisel verilerin korunması*" çerçevesinde incelemeleri kapsamaktadır. KVKK'ya aykırı şekilde ilgili kişilerin açık rızası alınmaksızın isimden telefon numarası yahut telefon numarasından isim sorgulanması biçiminde rehberlik hizmeti sunan internet siteleri/uygulamalarına yönelik intikal eden ihbar ve şikayetler kapsamında yapılan incelemede, internet sitelerinden ya da sosyal medya hesaplarından kişisel verileri toplayarak bu verilerin paylaşımını yapan isim veya telefon numarası sorgulayarak başkalarının telefon rehberine nasıl kaydedildiğini öğrenme konusunda hizmet sunan pek çok uygulama ve sitenin olduğu belirlenmiştir. Kurul, yasal dayanağı olmaksızın gerçekleştirilen veri işleme faaliyetinin Kanun'un 15/7. maddesi doğrultusunda durdurulmasına karar vermiştir.

Kurulun 16/10/2018 tarihli ve 2018/119 sayılı İlke kararında[374] da "*veri sorumluları ve işleyenler tarafından ilgili kişilerin e-posta adreslerine veya SMS ya da çağrı ile cep telefonlarına reklam bildirimleri/aramaları yönlendirilmesinin önüne geçilmesi*" için Kurula intikal eden birçok başvuru kapsamında yapılan incelemeler neticesinde ilgili kişilerin açık rızası olmadan ve Kanun'da belirtilen işleme şartları bulunmadan ilgili

---

373 Kişisel Verileri Koruma Kurumu, Rehberlik Hizmeti Veren İnternet Sitelerinde/Uygulamalarda Kişisel Verilerin Korunmasına Yönelik Kişisel Verileri Koruma Kurulunun 21/12/2017 Tarihli ve 2017/61 Sayılı İlke Kararı, (E.T. 16.01.2023), https://www.kvkk.gov.tr/Icerik/4113/2017-61.

374 Kişisel Verileri Koruma Kurumu, "Veri sorumluları ve veri işleyenler tarafından ilgili kişilerin e-posta adreslerine veya SMS ya da çağrı ile cep telefonlarına reklam bildirimleri/aramaları yönlendirilmesinin önüne geçilmesi " ile ilgili Kişisel Verileri Koruma Kurulunun 16/10/2018 Tarihli ve 2018/119 Sayılı İlke Kararı, (E.T. 16.01.2023), https://www.kvkk.gov.tr/Icerik/5299/2018-119

kişilere SMS gönderilmesi, telefonla arama yapılması, reklam içerikli e-postaların gönderilmesi şeklindeki veri işleme faaliyetlerinin Kanun'un 15/7 uyarınca derhal durdurulmasına karar vermiştir.

3.3.2.1.2. Kişisel Verilere Hukuka Aykırı Olarak Erişilmesi

Kurulun 21/12/2017 tarihli ve 2017/62 sayılı İlke kararında[375] "*banko, gişe, masa gibi hizmet alanlarında kişisel veri güvenliği ihlallerine ilişkin"* ihbarlar neticesinde yapılan incelemeler doğrultusunda kişisel verilere hukuka aykırı erişim olduğu tespit edilmiştir. Kararda, sağlık ve bankacılık sektörü önde olmak üzere birden fazla kişi ile bitişik nizamda hizmet verilen banko, gişe, masa gibi kısımlarda yetkisiz şahısların erişiminin engellenmesi gerektiği ifade edilmiştir. Bununa birlikte, aynı anda birbirine yakın yerde hizmet alanların birbirlerinin kişisel verisini görmesi, öğrenmesini yahut bir şekilde bilmesinin önüne geçecek şekilde önlemlerin alınmasına karar verilmiştir. Fiziki alanlarda da yetkisiz erişimin önüne geçilmesi için her türlü idari ve teknik önlemin alınması gerekliliği vurgulanmıştır.

Kurulun 31/05/2018 tarihli ve 2018/63 sayılı ilke kararında[376] ise elektronik ortamda bulunan kişisel verilerin güvenliğinin sağlanması noktasında inceleme yapılmış *"veri sorumlusu nezdindeki kişisel verilere erişim yetkisi bulunan personelin yetkisi ve amacı dışında söz konusu kişisel verileri işleme hususunun değerlendirilmesi"* hususuna ilişkin veri sorumlusu nezdinde yer aldıkları konum ya da görev itibariyle yetkileri aşarak ve/veya yetkileri kötüye kullanarak kişisel verilerin işlendiği amaca aykırı olarak kişisel verilerin işlenmesi ve/veya bu verilerin üçüncü kişilerle paylaşılmasının veri güvenliğini ihlal etmesinden ötürü Kanun'un 12. maddesi doğrultusunda gerekli önlemlerin alınması gerektiği ifade edilmiştir.

---

375 Kişisel Verileri Koruma Kurumu, Banko, Gişe, Masa gibi Hizmet Alanlarında Kişisel Verilerin Korunmasına Yönelik Kişisel Verileri Koruma Kurulunun 21/12/2017 Tarihli ve 2017/62 Sayılı İlke Kararı, (E.T. 16.01.2023), https://www.kvkk.gov.tr/Icerik/4114/2017-62

376 Kişisel Verileri Koruma Kurumu, Veri Sorumlusu Nezdindeki Kişisel Verilere Erişim Yetkisi Bulunan Personelin Yetkisi ve Amacı Dışında Söz Konusu Verileri İşlemesi Hususunun Değerlendirilmesine İlişkin 31/05/2018 Tarih ve 2018/63 Sayılı İlke Kararı, (E.T. 16.01.2023), https://www.kvkk.gov.tr/Icerik /5248/2018-63

Kişisel verilere uzaktan erişime ilişkin ise "*belediyelerin ödeme ve borç sorgulama hizmetleri hakkında"* verilen 21/04/2022 tarihli ve 2022/388 sayılı ilke kararında[377] ise belediyelerin çevrimiçi olarak hizmet sunduğu platformlara girişlerde iki aşamalı sorgulama sistemi kullanılarak kimlik doğrulama kontrolü uygulanmasının gerekliliği, aksi halde Kurula iletilen ihbarlarda belirtildiği üzere yalnızca kimlik numarası ile yapılan sorgulamaların yetkisiz üçüncü kişilerin verilere kötü niyetli erişim imkanı olması nedeniyle veri güvenliğinin ciddi derecede ihlal edileceği, bu nedenle işlenen kişisel verilerin muhafazasının ve güvenliğinin sağlanmasında risklerin tespit edilerek en aza indirgenmesi gerekliliğinin önemi vurgulanarak gerekli tedbirlerin alınması gerektiğine karar verilmiştir.

Kişisel verilerin işleme amacına uygun olarak işlenmesi gerektiği belirtilen 2018/119 sayılı ilke kararının devamında veri sorumlularının işleme amacına uygun olarak işlediği kişisel verilerin güvenliğini sağlamaya yönelik tedbirleri alması, verilere yetkisiz erişimin engellenmesinin veri sorumlusunun yükümlülüğü olduğu belirtilmiştir.

3.3.2.1.3. Kişisel Verilerin Muhafazasının Sağlanmaması

Kurulun 2018/119 sayılı ilke kararında "veri güvenliğinin sağlanması" için gerekli olan kişisel verilerin hukuka aykırı işlenmesi ve verilere hukuka aykırı erişimin önlenmesine ek olarak kişisel verilerin muhafazasını temin etmek adına uygun güvenlik düzeyinin sağlanması, bu hususu teminen her türlü idari ve teknik önlemin alınması gerektiği ifade edilmiştir.

"*Veri sorumluları tarafından kişilerin telefon numarası, e-posta adresi gibi iletişim kanallarına Kanuna aykırı şekilde gönderilen üçüncü kişilere ait kişisel veriler*" hakkında Kurulun 22/12/2020 tarihli ve 2020/966 sayılı ilke kararında[378] kişisel verilerin kaynağının doğruluğunun belirlenmesi, kişisel verilerin doğru olmaması nedeniyle ilgili kişilerin zarara uğramasının önüne geçilmesi için ilgili kişi tarafından beyan edilen

---

377 Kişisel Verileri Koruma Kurulu, Belediyelerin ödeme ve borç sorgulama hizmetleri hakkında Kişisel Verileri Koruma Kurulunun 21/04/2022 tarihli ve 2022/388 sayılı İlke Kararı, (E.T. 16.01.2023), https://www.kvkk. gov.tr/Icerik/7252/2022-388

378 Kişisel Verileri Koruma Kurumu, Veri sorumluları tarafından kişilerin telefon numarası, e-posta adresi gibi iletişim kanallarına Kanuna aykırı şekilde gönderilen üçüncü kişilere ait kişisel veriler hakkında Kişisel Verileri Koruma Kurulunun 22/12/2020 Tarihli ve 2020/966 sayılı İlke Kararı, (E.T. 16.01.2023), https:// www.kvkk.gov.tr/Icerik/6858/2020-966

iletişim bilgilerinin doğruluğuna yönelik (çift kademeli doğrulama, doğrulama linki/kodu gönderilmesi gibi) makul önlemlerin alınması lüzumlu görülmüştür. Ek olarak kişisel verilere hukuka aykırı şekilde erişimin engellenmesi ve verilerin muhafazasının sağlanması gerektiği ifade edilmiştir.

İlke kararlarında açıkça belirtilmemiş olsa da kişisel verilerin muhafazasının sağlanması gerektiği Kanun'un 12. maddesinde net bir şekilde ifade edilmektedir. "Veri güvenliğine ilişkin yükümlülükler" başlıklı hükümde "*veri sorumlusunun; a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek, c) Kişisel verilerin muhafazasını sağlamak, amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorunda*" olduğu açıkça belirtilmiştir. Kişisel verilerin muhafazasının sağlanması yükümlülüğü, verilerin hukuka aykırı işlenmesini ve kişisel verilere hukuka aykırı şekilde erişilmesinin önlenmesi sorumluluğunu da kapsamaktadır. "İşleme" kavramı, kaydetme, saklama, aktarma, erişme, imha etme gibi birçok veri işleme faaliyetini kapsadığından kişisel verilerin korunması için uygun güvenlik seviyesinin veri sorumlularınca sağlanması ile verilere hukuka aykırı erişim de engellenmiş olacak, veriler veri koruma hukukuna uygun şekilde işlenecektir. Bu nedenle ilke kararlarının hepsinde açıkça ifade edilmemiş de olsa kişisel verilerin muhafazasına yönelik önlemlerin alınması gerektiği açıkça ortadadır. Veri ihlallerinin yaşanmasının başlıca nedenlerinden biri kişisel verilerin gereği gibi muhafaza edilmemesidir ve bu hususun işin doğası gereği resen değerlendirilmesi gerekmektedir.

3.3.2.2. Kişisel Verilerin Hukuka Aykırı Olarak Aktarılması

Kurul, 23/12/2021 tarihli ve 2021/1304 sayılı "*araç kiralama sektöründe kara liste uygulamaları hakkında*" vermiş olduğu ilke kararında[379] kişisel verilerin hukuka aykırı olarak aktarılmasının veri ihlali olduğunu belirterek hükme ulaşmıştır. Buna göre kişisel verilerin aktarılmasında Kanun'un 8. maddesine uygun olarak işlem tesis edilmesi gerektiği, araç kiralama faaliyetlerinin kolluk kuvvetlerine bildirme zorunluluğunun bulunduğunu, bu nedenle Kanun'un 5/2-3 maddelerinde öngörülen "kanunlarda açıkça

[379] Kişisel Verileri Koruma Kurumu, Araç Kiralama Sektöründeki Kara Liste Uygulamaları Hakkında Kişisel Verileri Koruma Kurulunun 23/12/2021 Tarihli ve 2021/1304 Sayılı İlke Kararı, (E.T. 16.01.2023), https://www.resmigazete.gov.tr/eskiler/2022/01/20220120-10.pdf

öngörülmesi" ve "veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması" hukuki sebeplerine dayanarak araç kiralayan kişilerin verilerinin aktarılmasında herhangi bir hukuka aykırılık bulunmadığını belirtmiştir. Ancak "kara liste yazılımları"[380] kullanan diğer araç kiralama firmalarının da bu kişilerin verilerine

---

[380] Kara liste (blacklist), en genel anlamıyla *"şüphe altında tutulan veya güvensiz, sadakatsiz olarak değerlendirilen kişilerin veya kuruluşların özellikle bir hükümet veya bir organizasyon tarafından derlenen bir listesi*" olarak tanımlanabilir. Buna göre kara listede bulunan kişilerin güvenilirliği sorgulanabilecektir. Kara listeye ilişkin yazılımlar da bu listelerin teknolojik imkanlarla oluşturulması için ortaya çıkan programlardır. Bkz: (E.T. 21.01.2024), https://www.collinsdictionary.com/-dictionary/english/blacklist.
Bu noktada özellikle bankalar tarafından uygulanan "kara liste" uygulamaları ile dikkat çekmektedir. 5411 sayılı Bankacılık Kanunu ek madde 1/1'de "*Türkiye Bankalar Birliği nezdinde, kredi kuruluşları ile Kurulca uygun görülecek finansal kuruluşların müşterilerinin risk bilgilerini toplamak ve söz konusu bilgileri bu kuruluşlar ile gerçek veya tüzel kişilerin kendileriyle ya da onay vermeleri koşuluyla gerçek kişiler ve özel hukuk tüzel kişileri ile de paylaşılmasını sağlamak üzere Risk Merkezi kurulmuştur"* hükmü yer almaktadır. Bu doğrultuda bankalarca Kanun'un verdiği yetkiye dayanılarak ile kara liste uygulamaları kullandığı söylenebilir. Maddenin devamı uyarınca "*Risk Merkezi nezdinde bulunan sır niteliğindeki bilgileri, bu konuda kanunen yetkili kılınan mercilerden başkalarına açıklayanlar, hukuka aykırı olarak kendisi ya da başkası yararına kullananlar, yayanlar, verenler, aktaranlar veya ele geçirenler hakkında 159 uncu madde hükümleri uygulanır. Bu fıkrada tanımlanan suçların bir tüzel kişinin faaliyeti çerçevesinde işlenmesi halinde, ilgili tüzel kişi hakkında Türk Ceza Kanunu'nun tüzel kişilere özgü güvenlik tedbirlerine hükmolunur."* (Ek Madde 1/10). 73. maddede ise sır yükümlülüğü düzenlenmektedir. Kişisel Verileri Koruma Kurulunun 03.03.2020 tarihli ve 2020/191, 2020/192, 2020/193 ve 2020/194 sayılı kararlarında da bu husus ile ilgili karar verilmiştir. "*Risk Merkezindeki verilerin muhtelif faktoring şirketleri tarafından ihlal edildiğinin ihbar edilmesine ilişkin" kararlarda bahsi geçen uygulamaların hukuka aykırı olduğuna değil, "Risk Merkezi üzerinden yapılan sorgu adetlerinde dikkat çekici değişiklik gözlenen Faktoring Şirketleri hakkında Kurulumuza yapılan ihbarın incelenmesi neticesinde, ihbara konu kişisel veri işleme faaliyetlerinde; Kanunun 4 üncü maddesinde sayılan genel ilkelere riayet edilmediği; söz konusu faaliyetlerin Kanunun 12 inci maddesinin birinci fıkrasında düzenlenen kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak yükümlülüklerine aykırılık teşkil ettiği tespit edilmesi*" nedeniyle ilgili veri sorumluları hakkında idari para cezası verilmiştir. Dolayısıyla bankalarca uygulanan "kara listelerde" genel ilkelere ve kanuni ölçütlere uygun veri işleme süreci gerçekleştirilirse hukuka aykırılık söz konusu olmayacaktır.
Vergi uygulamalarında da bir takım "listeler" söz konusudur. Özellikle "vergi rekortmenleri" ve "vergi yüzsüzleri" listelerinin kamuoyu ile paylaşılmasında kişisel veri koruma hukukuna aykırılık olup olmadığı sorusu gündeme gelebilir. Bu noktada vergi rekortmenleri ve vergi yüzsüzleri listesinin kamuoyuna duyurulmasının şartlarının dayanağını VUK md. 5'in "*Mükelleflerin vergi tarhına esas olan beyanları, kesinleşen vergi ve cezaları ile vadesi geçtiği halde ödenmemiş bulunan vergi ve ceza miktarları Maliye Bakanlığınca açıklanabilir"* hükmüdür. 293 sıra nolu VUK Genel Tebliği'nde de Maliye Bakanlığınca bu kapsamda açıklamanın nasıl yapılacağı ile ilgili düzenlemeler yer almaktadır. Vergi rekortmenleri listelerinde, isminin açıklanmasını istemeyen vergi mükellefinin, bilgilerinin gizli kalması şeklindeki tercihi kabul görmekte iken vergi yüzsüzleri listesinde yer alan mükellefin böyle bir tercih hakkı bulunmamaktadır. Gerçek kişi mükelleflerin kişisel verilerinin ilan edilmesinde kanundan kaynaklanan hukuka uygunluk sebebi bulunmaktaysa mahremiyet ve kişilik hakları açısından itibar kaybı, kişilik haklarının zedelenmesi gibi sıkıntılar doğacağı açıktır. Bkz: Burcu Gülerci, *Türk Hukukunda Vergi Mahremiyetinin Sınırları,* (İstanbul: On İki Levha Yayıncılık, 2017), 72-73; Bununla birlikte bu kişilerin basın ve medya tarafından "vergi yüzsüzleri" olarak ilan edilmesinde kanaatimizce hukuka uygunluk bulunmamaktadır. Bilhassa en çok borcu olanlar listesine ile ilgili yapılan bu haberlere yönelik gerekli hukuki tedbirlere başvurulması önem arz etmektedir. Aynı yönde Bkz: Muhammet Durdu, "Mükellef Verilerinin Korunması ve Vergi Mahremiyeti", *Selçuk Üniversitesi Hukuk Fakültesi Dergisi*, 27/3 (2019): 589-623, 600-601. DOI: 10.15337/suhfd.578013

ulaşabildiği ve sisteme girilen bilgilerin uygulamayı kullanan sayısı bilinmeyen başka firmalara da aktarıldığı göz önüne alındığında kişisel verileri işlemenin Kanun'un 4. maddesinde belirtilen "genel ilkelere" aykırılık teşkil ettiği ve kişisel verileri işlenen kişilerin temel hak ve özgürlüklerinin ihlal edildiği, diğer sebeplerle birlikte bu uygulamaların kullanımına son verilmesi gerektiğine karar verilmiştir.

3.3.2.3. Kişisel Verilerin Elde Edildiği Kaynağın Belirli Olmaması

"*Veri sorumluları tarafından kişilerin telefon numarası, e-posta adresi gibi iletişim kanallarına Kanuna aykırı şekilde gönderilen üçüncü kişilere ait kişisel veriler*" hakkında Kurulun 22/12/2020 tarihli ve 2020/966 sayılı ilke kararında ulaşım, turizm, e-ticaret, telekomünikasyon gibi farklı alanlarda hizmet veren veri sorumlularının kişisel veri içeren belgelerin ilgilisine gönderilmesi amacıyla kişinin e-posta veya telefon numaralarını işlediği ancak kişisel verilerin doğru ve gerektiğinde güncel olma ilkesiyle de paralel olarak kişisel verilerin elde edildiği kaynağın belirli olması gerektiği, bu nedenle veri güvenliğinin sağlanması adına makul önlemlerin alınması gerektiği, paylaşılan bilgilerin doğruluğunun teyit edilmesini sağlayacak yeterli güvenlik tedbirlerinin alınması gerektiğine karar verilmiştir.

3.3.2.4. Kişisel Verilerin Hukuka Aykırı Şekilde Elde Edilmesi

Kişisel verilerin hukuka aykırı biçimde ele geçirilmesi TCK kapsamında suç teşkil etmektedir. 5237 sayılı Kanunun 136. maddesinde "*verileri hukuka aykırı olarak verme veya ele geçirme*" suçu düzenlenmiştir. Bu doğrultuda suç konusu olabilecek veri işleme faaliyeti gerçekleştiren veri sorumluları nedeniyle Kurula yapılan ihbar ve şikayetler neticesinde üç farklı ilke kararı verilmiştir.

Kurul, 18/10/2019 tarihli ve 2019/308 sayılı ilke kararında[381] kişisel verilerin elde edildiği kaynağın belirli olması gerektiğini belirtmiş olmasının yanı sıra, hukuk büroları, finans, gayrimenkul danışmanlık, sigorta gibi alanlarda hizmet veren bazı kişi ve kuruluşlarca farklı usullerle temin edilen veriler üzerinden kişilerin kimlik ve iletişim bilgilerinin

[381] Kişisel Verileri Koruma Kurumu, Hukuka Aykırı Olarak Elde Edilen Veriler Üzerinden Vatandaşların Kimlik ve İletişim Bilgileri Gibi Kişisel Verilerinin Sorgulanmasına İmkân Tanıyan Yazılım/Program/Uygulamalara
Yönelik Kişisel Verileri Koruma Kurulunun 18/10/2019 Tarihli ve 2019/308 Sayılı İlke Kararı, (E.T. 16.01.2023), https://www.kvkk.gov.tr/Icerik/6568/2019-308

sorgulanmasını sağlayan yazılım/program/uygulamaların kullanıldığının belirlenmiş olması nedeniyle veri güvenliğine ilişkin yükümlülüklerine aykırı davranan veri sorumluları hakkında TCK kapsamında gereken adli işlemlerin tesis edilmesi adına Cumhuriyet Başsavcılıklarına bildirim yapılacağı, görev alanına giren konularla ilgili ise idari yaptırım uygulanacağı yönünde karar vermiştir.

Kurulun 2017/61 sayılı "*rehberlik hizmeti veren internet siteleri/uygulamaları*" hakkında vermiş olduğu ilke kararında kişisel verilerin Kanun'un 5. ve 6. maddelerinde düzenlenen veri işleme şartlarının bulunmadığı, bu nedenle faaliyetlerin durdurulması gerektiği, bu faaliyetlere son verilmediği takdirde TCK uyarınca "verileri hukuka aykırı olarak ele geçirme" suçunun işlendiği gerekçesiyle adli sürecin başlatılması için hareket edileceğine karar verilmiştir.

"*Veri sorumluları veya veri işleyenler tarafından ilgili kişilerin e-posta adreslerine veya SMS ya da çağrı ile cep telefonlarına reklam bildirimleri/aramaları yönlendirilmesinin önüne geçilmesini teminen"* Kurulca alınan 2018/119 sayılı ilke kararında ise ilgili kişilerin açık rızaları bulunmadan ya da Kanunun veri işleme şartlarından en az biri olmadan veri işleme faaliyeti sürdüren veri sorumluları ve/veya veri işleyenlerin bu faaliyetlerinin hukuka aykırı olması sebebiyle derhal durdurulmasına karar verilmiştir. Aksi takdirde işlenen kişisel verilerin hukuka aykırı şekilde ele geçirilmiş olma ihtimali değerlendirilerek TCK md. 136 kapsamında Cumhuriyet Başsavcılığına ihbarda bulunulacağı ifade edilmiştir.

3.3.2.5. Kişisel Verilerin İşlenmesinde Genel İlkelere Aykırılık

Kişisel verilerin işlenmesi faaliyetleri esnasında uyulması zorunlu olan genel ilkeler[382] Kanunun 4. maddesinde belirtilmiştir. Veri işleme faaliyetlerinde genel ilkelere uyulmaması, faaliyeti hukuka aykırı hale getirecektir. Kurulun 2020/966 sayılı ilke kararında veri sorumlusu tarafından kişilerin e-posta, telefon numarası ve benzeri iletişim kanallarına hukuka aykırı biçimde gönderilen üçüncü kişilere ait verilerle ilgili vermiş

[382] KVKK md. 4/2: Kişisel verilerin işlenmesinde aşağıdaki ilkelere uyulması zorunludur:
a) Hukuka ve dürüstlük kurallarına uygun olma.
b) Doğru ve gerektiğinde güncel olma.
c) Belirli, açık ve meşru amaçlar için işlenme.
ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma.
d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme.

olduğu kararda, genel ilkeler içinde sayılan "kişisel verilerin doğru ve gerektiğinde güncel tutulma" ilkesine aykırı olarak kişisel veri sahipleri aleyhine veri işleme faaliyetlerine son verilerek kişisel verilerin korunması adına gerekli güvenlik tedbirlerinin alınması ve verilerin doğru ve gerektiğinde güncel tutulması için gereken mekanizmaların oluşturulması yönünde karar verilmiştir. Zira kişisel verilerin doğruluğunun sağlanabilmesi açısından kişisel verilerin elde edildiği kaynağın belirli olması gerekmektedir.

Kurul, yukarıda zikredilen 2021/1304 sayılı "kara liste uygulamaları hakkında" vermiş olduğu kararında araç kiralayan kişisel veri sahiplerinin verilerinin, kara liste uygulaması kullanıcısı olan ve sayısı bilinmeyen birçok araç kiralama firması ile paylaşılması hususunda da veri işleyen açısından Kanunda belirtilen genel ilkelerden "hukuka ve dürüstlük kurallarına uygun olma", "belirli, açık ve meşru amaçlar için işlenme", "amaçla bağlantılı, sınırlı ve ölçülü olma" ilkelerine aykırılık olduğunu belirtmiştir.

3.3.2.6. İlgili Kişinin Haklarının Kullandırılmaması

Kurulun "*araç kiralama sektöründeki kara liste uygulamaları hakkında*" vermiş olduğu 23/12/2021 tarihli ve 2021/1304 sayılı ilke kararında diğer ilke kararlarında bahsedilmeyen bir noktaya değinilmiştir. Söz konusu karara göre araç kiralama firmaları tarafından "kara liste" özelliği içeren yazılımlar kullanılarak kendi müşterileri olan araç kiralayan gerçek kişilerin kişisel verilerinin işlendiği belirtilmiştir. İşlenen veriler içinde, araçların kullanımı esnasında oluşan olumsuzlukları ya da araç kiralama firmasının yorumlarını da kapsayan bilgilerin bulunduğu ifade edilmiştir. Bu bilgilerin araç kiralama firmaları tarafından sonraki kiralamalar için karar alırken kullanılmak üzerine işlendiği üstelik bu verilerin işlendiği kara liste yazılımlara başka araç kiralama firmalarının da erişim imkânı olduğu tespit edilmiştir. Bu uygulamaların ilgili kişinin hakları bakımından değerlendirildiğinde kişisel veri sahibinin haklarını kullanmasının önünde engel teşkil ettiği sonucu ortaya çıkmaktadır. Kara liste uygulamasının doğası gereği şahıs hakkında olumsuz neticeye ulaşılması ve yapılan profilleme neticesinde kişi hakkında ortaya çıkan olumsuz sonucun kimler tarafından biliniyor olduğu ilgili kişi tarafından bilinmemektedir. Bu sebeple ilgili kişinin, Kanun'un 11. maddesinde belirtilen haklarını veri sorumlusu nezdinde ileri sürmesi güçleştiğinden kara liste uygulamalarına son verilmesi gerektiğine karar verilmiştir.

3.3.2.7. Kişisel Veri İhlallerinin Değerlendirilmesi

Kişisel Verileri Koruma Kurulu'nun ilke kararı alması gerektiren yaygın ihlaller incelendiğinde, ihlallerin özellikle veri sorumlusunun veri güvenliği ile ilgili sorumluluklarını tam anlamıyla yerine getirmemesinden kaynaklandığı anlaşılmaktadır. Kişisel verilerin hukuka aykırı biçimde işlenmesi, kişisel verilere hukuka aykırı şekilde erişilmesi ve kişisel verilerin muhafazasının sağlanmaması unsurlarının çatısı olan "*veri güvenliği yükümlülükleri*", veri ihlalleri incelenmesinde ön planda olmalıdır. Zira Kurul'a intikal eden ihbar ve şikayetlerin büyük çoğunluğuna bakıldığında, verilen ilke kararlarının oransal olarak veri güvenliği yükümlülüklerine aykırı faaliyetler olduğu ortaya çıkmaktadır. Bu doğrultuda Kurul tarafından verilen ihlal kararlarına ilişkin sınıflandırma şu şekilde yapılabilir:

Tablo 3.1. İlke Kararı Alınmasına Neden Olan İhlallerin Tasnifi[383]

İhlal Türü	Açıklama	Karar Sayısı
Kişisel Verilerin Hukuka Aykırı Olarak İşlenmesi (md.12)	Kişisel verilerin yasal dayanağı olmaksızın veya veri sahibinin rızası dışında işlenmesi (Veri sorumlusunun kişisel veri güvenliğiyle ilgili yükümlülüklerini yerine getirmemesi veya ihlal etmesi)	2
Kişisel Verilere Hukuka Aykırı Erişilmesi (md. 12)	Yetkisiz kişilerin kişisel verilere erişmesi veya izinsiz bir şekilde verilere ulaşması (Veri sorumlusunun kişisel veri güvenliğiyle ilgili yükümlülüklerini yerine getirmemesi veya ihlal etmesi)	4
Kişisel Verilerin Muhafazasının Sağlanmaması (md. 12)	Veri sorumlusunun gerekli güvenlik önlemlerini almadığı veya veri güvenliğini sağlamada ihmalkâr davrandığı durumlar	2
Kişisel Verilerin Hukuka Aykırı Olarak Aktarılması (md. 8-9)	Kişisel verilerin yasal dayanağı veya veri sahibinin rızası olmaksızın başka bir kişi veya kuruluşa aktarılması.	1
Kişisel Verilerin Hukuka Aykırı Şekilde Elde Edilmesi (md.5-6)	Kişisel verilerin izinsiz veya hukuka aykırı bir şekilde elde edilmesi.	3
Kişisel Verilerin Elde Edildiği Kaynağın Belirli Olmaması (md.4)	Veri sorumlusunun kişisel verileri yasal yollarla toplama yükümlülüğünü yerine getirmemesi	1
Kişisel Verilerin İşlenmesinde Genel İlkelere Aykırılık (md.4)	Kişisel verilerin işlenmesinde veri koruma ilke ve standartlarına uyulmaması.	2
İlgili Kişinin Haklarının Kullandırılmaması (md.11)	Veri sahibinin taleplerine uygun şekilde haklarının sağlanmaması veya engellenmesi.	1

[383] İlke kararlarında spesifik olarak belirtilen hususlar dikkate alınarak hazırlanmıştır.

İhlal kararı alınmasına neden olan ihlal türleri 8 başlık altında verilmiş olsa da bahsi geçen ihlallerin keskin çizgilerle birbirinden ayrılması mümkün değildir. Örnek vermek gerekirse, "kişisel verilerin hukuka aykırı olarak aktarılması", "kişisel verilerin hukuka aykırı şekilde elde edilmesi", "kişisel verinin elde edildiği kaynağın belirli olmaması", "kişisel verilerin işlenmesinde genel ilkelere aykırılık" hususları genel anlamı ile bakıldığında KVKK md. 12'de belirtilen "hukuka aykırı olarak işleme" başlığı altında da değerlendirilebilecektir. Zira Kanun'un 3. maddesinde kişisel verilerin işlenmesi *"kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem"* şeklinde tanımlanmıştır. Bu nedenle daha önce de belirtildiği üzere bu ihlallerin değerlendirilmesinde işin doğası gereği veri güvenliği yükümlülükleri de dikkate alınmalıdır. Yine "kişisel verilerin işlenmesinde genel ilkelere aykırılık" hususu, "kişisel verilerin hukuka aykırı olarak işlenmesi" ve "kişisel verilerin elde edildiği kaynağın belirli olmaması" başlığı altında da değerlendirilebilecektir. Nitekim Kanun'un 4. maddesinde ifade edilen "kişisel verilerin işlenmesindeki genel ilkeler" veri işlemenin tüm süreçlerinde her şart ve koşulda uyulması gereken emredici ilkelerdir. Bu ilkelere aykırı veri işleme faaliyeti hukuka aykırı veri işleme olarak değerlendirilecektir. Öte yandan genel ilkelerde belirtilen "doğru ve gerektiğinde güncel olma (KVKK md. 4/2-b)" ilkesi nedeniyle, kaynağı belirli olmayan verinin işlenmesi genel ilkelere aykırılık oluşturacak, bu sebeple hukuka aykırı veri işleme sonucu doğacaktır.

Veri koruma hukukunun geniş bir kapsama ve dinamik bir yapıya sahip olması, birbirini bağlayan ve birlikte değerlendirilmesi gereken bir dizi prensip ve ilkeye dayanması sebebiyle veri ihlalini ortaya çıkaran nedenler net bir şekilde sınırlandırılamamaktadır. Bu açıklamalar doğrultusunda "İlke Kararı Alınmasına Neden Olan İhlallerin Tasnifi", İlke Kararlarında spesifik olarak ifade edilen ve vurgulanan ifadelere dayalı olarak yapılmıştır.

3.3.3. Kişisel Verileri Koruma Kurulunun İlke Kararlarının Veri Koruma Hukuku Standartlarının Belirlenmesinde Rolü

İncelemeye alınan ilke kararlarında teknolojinin getirdiği imkanlar ile veri mahremiyetinin ne denli ihlal edildiği görülmektedir. Zira bir kişinin rızası olmadan kendine "özel" olarak sakladığı alana, yetkisiz üçüncü kişiler tarafından müdahale edilmektedir. Kurul tarafından alınan ilke kararları spesifik başvurulara ilişkin belirli konulara dair incelemeler sonucunda verilmiş olsa da kararların kıyas ile benzeri olaylara uygulanması mümkündür. Veri mahremiyetinin sağlanması için özellikle "gizlilik" kavramının çerçevesinin çizilmesi ve içinin doldurulması açısından hukuka aykırı veri işlenmesinin önlenmesi ve kişisel verilerin yasal yollarla elde edilmesi gerektiğine ilişkin ilke kararları yol gösterici olmaktadır.

Kurulun aldığı ilke kararlarının arasında gündelik yaşamda yoğun hizmet alınan birimler ve çok sık kullanılan uygulamalar ön sırada gelmektedir.[384] 2013 yılında yayınlanan Devlet Denetleme Kurulu'nun Kişisel Verilerin Korunmasına İlişkin Ulusal ve Uluslararası Durum Değerlendirmesi ile Bilgi Güvenliği ve Kişisel Verilerin Korunması Kapsamında Gerçekleştirilen Denetim Çalışmaları Raporunda *"Bankacılık, sigortacılık, telekomünikasyon, kargo, sağlık, turizm, eğitim, çağrı merkezi ve pazarlama hizmetleri gibi pek çok alanda faaliyet gösteren işletmelerin bilgi sistemleri büyük hacimde kişisel veriyi bünyelerinde barındırmaktadır. Bu şirketlerin, hangi tür kişisel verileri ne şekilde toplayabilecekleri, bunları hangi amaçlarla kullanabilecekleri, kimlerle paylaşabilecekleri, ne kadar süre tutabilecekleri, hangi süre sonunda silecekleri, almaları gereken güvenlik tedbirleri ile kişisel verisi bulunan kişilerin bu verilere erişim, sildirme, düzelttirme gibi haklarını nasıl kullanabileceklerine ilişkin olarak sektör bazlı düzenlemelerin bazı istisnalar dışında yapılmadığı; buna bağlı olarak kişisel veri ihlallerine yönelik denetimlerin gerçekleştirilemediği, ihlallerin tespit edilemediği ve yaptırıma bağlanamadığı, bu nedenlerle özel kesim açısından kişisel verilerin korunmasındaki boşluk ve risklerin önemli boyutlara ulaştığı ve acil önlem alınması gerektiği"*[385] değerlendirilmiştir. Aradan geçen 10 yılda ilke kararı alınmasına neden olan ihlallerin yaşandığı kuruluşların çoğunlukla aynı olduğu ve Kurula yapılan başvuruların

[384] Hizarcı, *6698 sayılı Kişisel,* 165.

toplumda sıklıkla karşı karşıya kalınan önemli problemlere yönelik olduğu görülmektedir. Tablo 2.1'de yer alan veri gizliliğini ve güvenliğini etkileyen faktörlerin etkileri yaşanan ihlallerde ortaya çıkmaktadır.

Bu doğrultuda, Kurulun kararları ve uyguladığı yaptırımların hem başvuru sahipleri hem de toplum için tatmin edici olduğu düşünülmektedir. Çünkü genel olarak analiz edilen kararlara bakıldığında, Kurulun, kişisel verilerin hukuka aykırı işlenmesinin engellenmesi için veri sorumlusunun yasaya ve düzenlemelere dayanarak gerekli tüm teknik ve idari önlemleri alma yükümlülüğüne büyük önem verdiği görülmektedir. Öte yandan, kararlarda bahsedilen sorunlar hala toplumda sıkça karşılaşılan sorunlardır. Kişisel verilerin korunmasıyla ilgili kanunlar ve düzenlemeler öngörülmesine rağmen ve Kurum bu hukuka aykırı faaliyetler üzerinde denetim faaliyetlerini gerçekleştirse de birçok çevrimiçi platformun hala kişisel verileri kullanmaya, depolamaya ve paylaşmaya devam ettiği bilinmektedir. İnsanların hala kişisel verilerin korunması konusundaki haklarını bilmemeleri, yaşanan ihlallerin en önemli nedenlerinden biri olduğu düşünülmektedir. Bu çıkarım, kuruma yapılan başvuru sayısı ve Kurulun bir yılda verdiği karar sayısı dikkate alınarak yapılabilmektedir.[386] Bununla birlikte Kurum tarafından etkin bir denetim mekanizması kurulmuş ve denetimlere bağlı olarak yaptırım süreçleri yürütülmektedir. Ancak Kurumun belirli bir sektöre yönelik düzenleme yetkisinin bulunmaması, başka bir ifade ile Kurumun dar anlamda faaliyet gösterme görevi bulunmaması nedeniyle her bir veri sorumlusunu periyodik ve rutin olarak denetlemesi beklenemeyecektir. Bu nedenle de veri koruma hukuku alanının düzenlenmesi gayreti ile alınan ilke kararları ile veri sorumlularının varsa hukuka aykırılıklarının hukuka uygun hale getirilmesinin sağlanması ve hukuka aykırılıkların gerçekleşmeden engellenmesi hedeflenmektedir. Ek olarak teknolojik gelişmelerin veri ihlallerini hızlandırması, veri koruma alanının oldukça dinamik bir yapıya sahip olması nedeniyle gündeme ve güncele ayak uydurulması da ilke kararları ile sağlanmaktadır. Zira 6698 sayılı Kanunun güncel gelişmelere uygun şekilde yorumlanarak alınan ilke kararları sayesinde içtihat

386 Sevinç ve Karabulut, "A Review on the Personal", 464.

oluşturulması, veri sorumluları açısından yol gösterici olmakta, bu sayede veri koruma hukukunun gelişimine büyük katkı sağlamaktadır.[387]

Kişisel verilerin korunması alanında en önemli görev, Kişisel Verileri Koruma Kurumu'na aittir. Kurum, etkili bir şekilde çalıştığında kişisel verilerin uyumunu sağlamak, haksız uygulamaları önlemek, standartlaşmayı sağlamak ve uyum maliyetlerini azaltmak için rehberlik edecek bir rol üstlenecektir. Özellikle hukuka uygunluk sınırlarını net bir şekilde belirleyerek aşırı korumacı politikaların oluşumunu engelleyecek ve kişisel verilerin korunmasıyla birlikte katma değerli hizmetlerin geliştirilmesi, veri temelli ekonomiye geçiş gibi hedeflere katkıda bulunacaktır. Kurum, bu hassas dengeyi başarıyla sağladığında KVKK'ya uyum süreci kısa bir süre içinde tamamlanabilecektir.[388]

3.4. İlke Kararları Doğrultusunda Ortak Sorunlar

3.4.1. Kişisel Verilerin Korunmasında Risk Etki Değerlendirmesi

3.4.1.1. Risk ve Risk Yönetimi

Kişisel verilerin korunmasında en önemli hususlardan biri hiç şüphesiz ki risk yönetimidir.[389] Özellikle yapay zekâ teknolojileri gibi hızla gelişim gösteren teknolojiler karşısında kişisel veri sahipleri bakımından meydana gelebilecek risklerin yönetilmesi veri koruma hukuku ile yakından ilişkilidir.[390]

Madde 29 Çalışma Grubu tarafından risk, "*bir olayın ve sonuçlarının, ciddiyet ve olasılık açısından tahmin edilen bir senaryosu*" olarak ifade edilmiştir. Risk kavramına dair pek çok tanım bulunsa da en genel anlamı ile *"olası şartlar içerisinden bir tehdidin bir varlık üzerinde zafiyet açığa çıkarması ve kuruma zarar verebilecek başarılı bir atak gerçekleştirme olasılığı"* olarak tanımlamak mümkündür.[391] Risk yönetimi ise bir

---

387 Seçil Koyuncu, "KVKK Tarafından Yayımlanan İlke Kararları", (5. e-Safe Kişisel Verileri Koruma Zirvesinde Sunulan Bildiri, Ankara, Mayıs 17, 2022). (E.T. 05.09.2023), https://www.youtube.com/-watch?v =LBfugRBV57I

388 Kaya, "Kişisel Verilerin Korunmasında", 64.

389 Akıncı, "Büyük Veri ve", 128.

390 Öykü Beste Bayram, "Bir Uyum Aracı Olarak Veri Koruma Etki Analizinin Türk Hukuku Bakımından Değerlendirilmesi". *Kişisel Verileri Koruma Dergisi* 4 / 1 (Haziran 2022): 38-53. 43. (E.T. 05.07.2023), https://dergipark.org.tr/tr/pub/kvkd/issue/70820/1117742

391 Korucu, *Veri Güvenliğinin İyileştirilmesinde*, 53.

organizasyonun veya bir işletmenin karşılaşabileceği riskleri tanımlama, analiz etme, değerlendirme, kontrol etme ve yönetme sürecidir. Temel amacı, belirlenen riskleri en aza indirmek veya kabul edilebilir seviyelere getirmek için stratejiler ve önlemler geliştirmektir. Risk yönetimi, organizasyonun güvenlik açıklarını belirlemesine, operasyonel verimliliği artırmasına ve olumsuz etkilerin en aza indirilmesine yardımcı olur. Ayrıca, yasal uyumluluğun sağlanması, itibarın korunması ve sürdürülebilirliğin desteklenmesi gibi önemli faydalar sağlar.[392]

Risk, kavramsal olarak ele alındığı andan itibaren farklı perspektiflerle değerlendirilmektedir. "Geleneksel Yaklaşım", kurum değerini koruma odaklıdır ve riski genellikle olumsuz bir faktör olarak görmekte, subjektif bir bakış açısıyla ele almayı tercih etmektedir. Bu anlayışta, riskin ön planda tutulan yönü genellikle zarar ve olumsuz etkilerdir. Diğer taraftan "Yeni Yaklaşım", riski bir fırsat olarak değerlendirir ve onu ölçülebilir bir faktör olarak kabul eder. Bu perspektife göre, risklerin kurum çapında bütünsel bir şekilde yönetilmesi önemli olup riskler sadece bir tehdit değil, aynı zamanda elde edilecek değerlerin bir parçası olarak da görülmelidir.[393]

GDPR kapsamında risk tanımı yapılmış olmasa da riskin unsurları belirtilmiştir. Buna göre risk "gerçekleşme ihtimali olan" ve "gerçekleşmesi halinde bireylerin hak ve hürriyetleri üstünde meydana getireceği etkinin ağırlığı" unsurlarından oluşmaktadır. Bu doğrultuda kişisel verilerin korunmasında risk, veri işleme faaliyetlerinin kişileri olumsuz etkileme veya bireylere zarar verme ihtimali şeklinde ifade edilebilir.[394] Kişisel verilerin korunması açısından risk yönetimi ise kişisel verilerin işlenmesi sürecinde ihlallerin henüz gerçekleşmeden önüne geçilmesi, veri güvenliğinin sağlanması adına uygun ve yeterli tedbirlerin alınmasıdır.[395] Başka bir ifade ile kişisel verilerin korunmasında risk yönetimi, kişisel verilerin işlenmesi, saklanması ve paylaşılmasıyla ilgili potansiyel risklerin tanımlanması, analiz edilmesi, değerlendirilmesi ve yönetilmesi sürecidir. Temel amacı, kişisel verilerin güvenliğini sağlamak ve veri ihlallerini önlemek veya minimize

---

392 Akıncı, "Büyük Veri ve", 128.

393 Uğur Tokmakcı, "Kişisel Verilerin Korunmasına Risk Temelli Yaklaşım", içinde *Kişisel Verilerin Korunmasına Uzman Bakış Uzmanlık Tezleri Derleme Çalışması,* ed. Pınar Çağlayan Aksoy ve Hüseyin Can Aksoy, (Ankara: KVKK Yayınları, No 44, 2023), 118.

394 Aktaran Tokmakcı, "Kişisel Verilerin Korunmasına", 119.

395 Çimen Bulut, "Avrupa Birliği Genel", 131.

etmektir.[396] Mahremiyet alanında risk yönetimi, veri kaynakları ve veri kalitesi gibi faktörlerin yanı sıra kullanım amaçlarının hassasiyetini de göz önüne almaktadır. Veri ihlallerinin önüne geçilmesinin yanında, veri analiz süreçlerinin irdelenerek hataların ve yanlışlıkların hangi aşamada meydana geldiğinin tespit edilmesine yardımcı olmaktadır. Mahremiyet risk değerlendirmesinin etkili olabilmesi adına, tüm potansiyel zararları ile faydaları göz önünde bulunduracak şekilde kapsamlı bir çalışma gerekmektedir.[397]

Risk yönetimi kavramı, farklı odak noktalarına çeşitlenmekte ve belirgin özelliklere göre alt başlıklara ayrılmaktadır. Dolayısıyla her alanın kendine özgü yaklaşımı ve odak noktası bulunmaktadır. Bu nedenle, veri sorumluları risk yönetimi stratejilerini geliştirirken her bir alanın özelliklerini dikkate almalı ve en etkili sonuca ulaşmayı hedefleyen bir yaklaşım benimsemelidir. Bu bağlamda risk yönetimi, kişisel verilerin korunmasında risk yönetimi ve mahremiyet alanında risk yönetimi kavramları şu şekilde özetlenebilir:

Tablo 3.2. Risk Yönetimi Türleri

Başlık	Tanım	Özellikler	Farklılıklar
Risk Yönetimi	Organizasyonların potansiyel riskleri tanımlama, analiz etme, değerlendirme ve yönetme süreci.	- Tüm organizasyonlar için evrensel bir kavramdır. - İş süreçlerini ve veri yönetimini kapsar.	- Kişisel verilerin korunması sadece bir alt kategorisidir. - Mahremiyet odaklı olmayabilir.
Kişisel Verilerin Korunmasında Risk Yönetimi	Kişisel verilerin işlenmesi, saklanması ve paylaşılmasıyla ilgili potansiyel risklerin tanımlanması, analiz edilmesi, değerlendirilmesi ve yönetilmesi süreci.	-Kişisel verilerin özel bir tür veri olduğu vurgulanır. - Veri koruma yasalarına uygunluk gerektirir. -Veri ihlalleri kişisel mahremiyet ihlallerine yol açabilir.	Genel risk yönetimi ile aynı prensipleri kullanır, ancak odak noktası kişisel verilerin korunmasıdır.
Mahremiyet Alanında Risk Yönetimi	Kişisel mahremiyetle ilgili potansiyel risklerin tanımlanması, analiz edilmesi, değerlendirilmesi ve yönetilmesi süreci.	-Özellikle kişisel mahremiyetin korunması üzerinde durur. -İnternet, iletişim ve izleme teknolojileri gibi alanları içerir.	Genel risk yönetimi ve kişisel verilerin korunması ile bağlantılıdır, ancak daha geniş bir odak noktasına sahiptir.

396 Akıncı, "Büyük Veri ve", 128.
397 Akıncı, "Büyük Veri ve", 127.

Bilgi güvenliğin sağlanması risk yönetimi ile ilgilidir. Bu gizliliği korumak için uygulanan güvenlik kontrolleri de risk temelli bir şekilde seçilmelidir.[398] Mahremiyet alanında risk yönetimi odaklı yaklaşım, tamamen yeni bir yaklaşım değildir. Bu yaklaşım, OECD Mahremiyet İlkeleri'nde sayılan güvenlik tedbirleri ilkesiyle uyumlu olup veri koruma etki değerlendirmesiyle de yakından ilişkilidir.[399]

3.4.1.2. Kişisel Verilerin Korunmasında Etki Değerlendirmesi

Etki değerlendirmesi genel itibariyle bir projenin, politikanın, programın veya işlemin; belirli bir sürecin, topluluğun veya çevrenin üzerindeki olası etkilerini değerlendirmek amacıyla yapılan bir analiz ve değerlendirme sürecidir.[400] Başka bir ifade ile halihazırda bulunan veya yürürlüğe girdirilmesi planlanan bir düzenlemenin, bir projenin ya da bir planın ileride doğması muhtemel olan tesirlerinin belirlenmesi ile olumsuz tesirlerin giderilmesi sürecidir.[401] Çevresel Etki Değerlendirme Yönetmeliğinde[402] tanımı yapılan çevresel etki değerlendirmesinden yola çıkarak etki değerlendirmesini, "*gerçekleştirilmesi planlanan projelerin olabilecek olumlu ve olumsuz etkilerinin belirlenmesinde, olumsuz yöndeki etkilerin önlenmesi ya da zarar vermeyecek ölçüde en aza indirilmesi için alınacak önlemler ile teknoloji alternatiflerinin belirlenerek değerlendirilmesinde ve projelerin uygulanmasının izlenmesi ve kontrolünde sürdürülecek çalışmaları*" şeklinde de tanımlamak mümkündür.[403]

Modern yönetimde teknolojik gelişmelerden ötürü artan risklere karşı etkili bir koruma aracı olan etki değerlendirmeleri; ekonomi, sağlık, çevre, sosyal alanlar, iklim, teknoloji gibi pek çok sektörde başvurulan bir süreç olmaya başlamıştır. Çevresel etki

---

398 Stephen D. Gantz ve Daniel R. Philpott, "Chapter 16 – Privacy" içinde *FISMA and the Risk Management Framework,* ed. Stephen D. Gantz ve Daniel R. Philpott, (Waltham: Syngress, 2013): 445-480, 445. https://doi. org/10.1016/B978-1-59-749641-4.00016-3.

399 Akıncı, "Büyük Veri ve", 128.

400 Muhittin Tataroğlu, "Mahremiyet Sorunlarının Önlenmesinde Mahremiyet Etki Değerlendirmesi (MED)", *Yönetim ve Ekonomi Dergisi,* 20/1 (2013), 263 – 289, 266. (E.T. 03.12.2023), https://dergipark.org.tr /en/pub/yonveek/issue/13698/165807

401 Akt. Erkan Ağıralan, "Bilgi Güvenliği, Kişisel Verilerin Korunması ve Mahremiyet Etki Değerlendirmesi", (Yayımlanmamış Yüksek Lisans Tezi, Polis Akademisi, 2015), 55.

402 29.07.2022 tarihli, 31907 sayılı Resmî Gazetede yayımlanmıştır. (E.T. 21.01.2024) https://www.mevzuat. gov.tr/mevzuat?MevzuatNo=39647&MevzuatTur=7&MevzuatTertip=5

403 1996 yılında mahremiyet etki değerlendirmesine ilişkin kanuni tanımlama yokken Blair Stewart da çevresel etki değerlendirmesi tanımından yola çıkarak mahremiyet etki değerlendirmesini tanımlamıştır. Bkz: Blair Stewart, "Privacy impact assessments", *Privacy Law & Policy Reporter***,** 3/4 (1996), (E.T. 27.01.2024), https://www8.austlii.edu.au/cgi-bin/viewdoc/au/journals/PLPR/-1996/39.html#

değerlendirmesi, iklim etki değerlendirmesi, stratejik çevre etki değerlendirmesi, sosyal etki değerlendirmesi, bütçe etki değerlendirmesi, sağlık etki değerlendirmesi, bütünleşik etki değerlendirmesi ve düzenleyici etki analizi etki değerlendirme türlerinden bir kaçıdır.[404] Kişisel verilerin korunması açısından da veri işleme süreçlerinde risklerin belirlenmesi ve risklerin olumsuz etkilerinin önüne geçilmesi açısından mahremiyet etki değerlendirmesi (*privacy impact assessment*) ve veri koruma etki değerlendirmesi (*data protection impact assessment*) başlıkları ön plana çıkmaktadır.

3.4.1.2.1. Mahremiyet Etki Değerlendirmesi

Mahremiyet etki değerlendirmesi (*privacy impact assessment*), veri koruma ve gizlilik literatüründe önemli bir rol oynamakta olup kişisel verilerin kullanımlarının olası gizlilik etkilerini değerlendiren bir süreçtir. Bu süreçte kişisel bilgilerin işlenmesinin veri sorumlusu için etkileri ve riskleri saptanarak kuruluşların bu riskleri hafifletme veya sonlandırma amacıyla kişisel verileri nasıl toplamaları, saklamaları ve işlemeleri gerektiği belirlenir.[405] Başka bir ifade ile mahremiyet etki değerlendirmesi (MED), kişisel olarak tanımlanabilir bilgilerin nasıl işlendiğinin analizi sürecidir ve yasal düzenlemelere uyum sağlamak, bilgi sistemleri veya faaliyetlerle ilişkilendirilen gizlilik risklerini belirlemek ve gizlilik risklerini azaltma yollarını değerlendirmek için yapılır.[406]

Kavramın en erken kullanımı 1994 yılında Ontario yasama organına sunulan ve ‘‘Erişim ve Gizlilik Etkilerinin Önceden Düşünceli Değerlendirilmesi’’ başlığını taşıyan belgede “bilgisayar bilgi sistemlerinin tanımında belirtilen şekilde bir mahremiyet etki değerlendirmesi yapılmasını gerektiren bir yönetmelik” öneren madde ile olmuştur.[407] Bir mahremiyet etki değerlendirme metodolojisi geliştirip yayımlayan Avrupa'daki ilk ülke ise Birleşik Krallık olmuştur. Bilgi Komisyonu Ofisi (Information Commissioner’s

---

404 Ağıralan, ““Bilgi Güvenliği, Kişisel”, 55; Tataroğlu, “Mahremiyet Sorunlarının Önlenmesinde”, 267-269.

405 Metin Bilgin, Sema Erkan, İdil Atasu ve Enes Yılmaz, “Privacy Impact Assessment As a Tool for GDPR Compliance Preparation”, *Kişisel Verileri Koruma Dergisi*, 1/2 (Aralık 2019): 75-86, 80. (E.T. 21.01.2024), https://dergipark.org.tr/tr/download/article-file/904860. Benzer yönde bkz. Tataroğlu, “Mahremiyet Sorunlarının Önlenmesinde”, 279.

406 U.S. Department of Agriculture, “Privacy Impact Assessments”, (E.T.25.01.2024), https://www.usda.gov/ home/privacy-policy/privacy-impact-assessments

407 Roger Clarke, “Privacy impact assessment: Its origins and development”, *Computer Law & Security Review*, 25/2 (2009): 123-135, 127. https://doi.org/10.1016/j.clsr.2009.02.002

Office- ICO), Aralık 2007'de bir MED El Kitabı[408] yayınlamıştır.[409] Sonrasında da kullanımı yaygınlaşan MED, ciddi şekilde gizlilik ihlali yapma eğilimini ve hızla gelişen bilgi teknolojilerinin yıkıcı etkilerini hafifletmek için veri işleyenler açısından bir panzehir olarak görülmüştür.[410] MED'in bir nevi "erken uyarı mekanizması" olarak ifade edilmesi de mümkündür.[411]

MED, mahremiyetle ilgili çalışmalara liderlik eden profesyonellerin, tasarım aşamasından itibaren mahremiyeti korumak için kullandığı standart bir süreçtir. Birçok ürün ve hizmet geliştiren kurum ve kuruluş, ürünün değeri ve maliyet etkinliği gibi faktörleri değerlendirmenin yanı sıra mahremiyet etki değerlendirmelerini kullanarak tasarım aşamasında rekabet avantajı elde etmeye çalışmaktadır. Ayrıca, bu süreçleri kullanmak kurumsal mahremiyet risklerini tanımlamak ve azaltmak konusunda da fayda sağlamaktadır. Bu hem müşterilerin mahremiyetlerini korumak hem de kurumun itibarını güçlendirmek için kritik bir rol oynamaktadır.[412] Kişisel veri işleyen organizasyonlar da risk kategorileri içerisinde yer alan "gizlilik" hususunu daha profesyonelce yönetmesi gerektiğinden risklerin tanımlanması ve yönetilmesi, gereksiz maliyetlerden kaçınılması, yetersiz çözümlerin önüne geçilmesi (eklenti çözümler de olarak adlandırılan gizlilik problemlerinin çıktığı anda çözüm üretilmesinin önüne geçilmesi), güven ve itibar kaybının önlenmesi veya yasal gereksinimler gibi sebeplerle mahremiyet etki değerlendirmesi yapmaktadır.[413]

MED hem sorunların hem de çözümlerin ortaya çıkarılması sürecidir.[414] Bu yönüyle mevcut gizlilik sorunları analizinden daha fazlası olup geleceğe dönük ve geniş kapsamlı analiz yapar. Büyük ölçüde, yalnızca yasal uyumluluk konularına değil, aynı zamanda "bunu yapmalı mıyız?" ve "bunu yapmanın daha iyi bir yolu var mı?" sorularına yanıt

---

408 2009 yılında güncellenen el kitabı için bkz: ICO, "Privacy Impact Assessment Handbook Version 2.0.", (E.T. 28.01.2024),https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2013/09-/PIAhandbookV2.pdf

409 Information Commissioner's Office, "Privacy impact assessment and risk management", 4 Mayıs 2013, (E.T. 28.01.2024), https://ico.org.uk/media/about-the-ico/consultations/2055/pia-and-risk-management-full-report-for-the-ico.pdf

410 Clarke, "Privacy impact assessment:", 123.

411 ICO, "Privacy impact assessment", 20.

412 Mustafa Alkan ve Turhan Menteş ve Mehmet Ali İnceefe, *Kişisel Verileri Koruma El Kitabı, Teknik Uygulama ve Uyumluluk*, (Ankara: Nobel Yayınları, 2020), 203-204.

413 ICO, "Privacy Impact Assessment Handbook Version 2.0.", 5.

414 Clarke, "Privacy impact assessment:", 124

vermede yer alan seçimlere yöneliktir.[415] Dolayısıyla MED bir gizlilik denetimi, iç risk değerlendirmesi veya kurumsal risk gizlilik stratejisi değildir.[416] Öte yandan kurumsal gizlilik stratejileri belirli olan, risk değerlendirmesi yaparak gizlilik denetimleri uygulayan sorumlular, MED sürecine daha kolay uyum sağlayacaklardır. Zira bu aşamalar MED sürecinin basamaklarını oluşturur.[417]

Etkili bir mahremiyet etki değerlendirmesi sürecinin sonucunda "*projenin gizlilik etkilerinin belirlenmesi, bu etkilerin tüm paydaşların bakış açılarından değerlendirilmesi, projenin ve özelliklerinin, etkilenecek olan organizasyonlar ve kişiler tarafından kabul edilebilirliğinin anlaşılması; daha az gizliliği ihlal edici alternatiflerin belirlenmesi ve değerlendirilmesi; gizlilik üzerindeki olumsuz etkilerin önlenmesi için yolların belirlenmesi; gizlilik üzerindeki olumsuz etkilerin azaltılması için yolların belirlenmesi; gizlilik üzerindeki olumsuz etkilerin kaçınılmaz olduğu durumlarda, bunları haklı çıkaran iş gereksinimlerinin netleştirilmesi; ve sonuçların belgelenmesi ve yayımlanması*" elde edilmesi beklenen ideal sonuçlardır.[418]

MED ve veri koruma etki değerlendirmesi (VKED) bazı kaynaklarda eş anlamlı ifadeler olarak kullanılsa da kavramların aynı olduğunu varsaymak mümkün değildir.[419] Zira MED, gizliliğin tüm boyutlarını dikkate alan bütünsel bir yaklaşım sunmakta iken veri koruma etki değerlendirmeleri, yasal uygunluğa odaklanmak ve GDPR'ye uygun şekilde veri işlemek için kullanılmaktadır. Başka bir ifade ile veri koruma etki değerlendirmesi yalnızca kişisel verilerin gizliliği etkilerini incelerken; MED, kişisel verilerin korunmasıyla sınırlı tutulmayıp kişinin bedensel mahremiyeti, kişisel iletişim gizliliği, kişinin davranışlarının gizliliği ve kişisel verilerin gizliliğini kapsayan[420] gizliliğin tüm boyutlarını ele almaktadır.[421]

---

415 Stewart, "Privacy impact assessments".

416 Clarke, "Privacy impact assessment:", 124-125.

417 Stewart, "Privacy impact assessments".

418 ICO, "Privacy Impact Assessment Handbook Version 2.0.", 7.

419 Kavramların aynı anlamda kullanıldığı eserler için bkz: Tokmakcı, "Kişisel Verilerin Korunmasına", 129; Kaya, "Kişisel Verilerin Korunmasında", 1885.

420 Roger Clarke, "Privacy Impact Assessment in Australian Contexts", *Murdoch University Electronic Journal of Law 72*, 15/1 (2008): 72-93, 73. (E.T. 27.01.2024), https://www8.austlii.edu.au/cgi-bin/viewdoc/au/journals/MurdochUeJlLaw/2008/5.html?context=1;query=1996%20PLPR%2039%20or%20PLPR%201996%2039;mask_path=; ICO, "Privacy Impact Assessment Handbook Version 2.0.", 14.

421 Paul De Hert, "A Human Rights Perspective on Privacy and Data Protection Impact Assessments" içinde *Privacy Impact Assessment. Law, Governance and Technology Series vol 6.*, ed.: David Wright

3.4.1.2.2. Veri Koruma Etki Değerlendirmesi

Veri koruma etki değerlendirmesi/analizi, özellikle yeni teknolojilerin kullanıldığı veri işlemlerinde işlemin doğası, kapsamı, bağlamı ve amacı dikkate alındığında gerçek kişilerin hak ve hürriyetleri yönünden yüksek risk oluşturabileceği hallerde, veri sorumlusunun bu işleme başlamadan önce planlanan faaliyetlerin kişisel verilerin korunması üzerindeki etkisini değerlendirdiği bir yöntemdir.[422]

95/46/EC sayılı Direktif'in revize edilerek GDPR'ın kabul edilmesinin amacı da dijital ortamda daha etkili ve tutarlı bir kişisel veri koruması sağlamak olmuştur. Bu süreçte sürekli olarak vurgulanan nokta, *"mevcut veri koruma prensiplerinin geçerli kaldığı*"; değişmesi gereken şeyin, "*mevcut veri koruma prensiplerinin daha iyi uygulanmasını sağlayacak önlemler ve mekanizmalar*" olduğu noktasıdır. GDPR'a göre de etkin veri korumasının pratikte sağlanması ise GDPR'nin 35. maddesinde[423] öngörülen veri koruma etki değerlendirmesi yapma yükümlülüğü ile somutlaşmaktadır.[424] Bu değerlendirme, fiziksel etmenler ve bilişim sistemleri gibi unsurların, kişisel verilerin gizliliğini etkileme ve ihlal etme potansiyeline sahip olduğu durumlarda kullanılır. Bu mekanizma, verinin gizliliği açısından kontrolün sağlanması için bir denetim mekanizması görevi görür. Bu tür risk analizleri, özellikle gelişmiş ülkeler olmak üzere dünya genelinde giderek yaygınlaşmaktadır. Zira teknolojik ilerlemelerle birlikte otomatik veri işleme teknikleri ve süreçleri, ekonomik hedeflere odaklanarak hızla gelişmiş ve çeşitlenmiştir. Ancak bu otomatik işlemler, temel hak ve özgürlüklerin korunmasını hedeflemediğinden kişisel veri ihlallerinde artış yaşanmıştır. Bu durum, veri koruma etki değerlendirmesi yönteminin önemini ortaya koymaktadır. Veri koruma etki değerlendirmesi, amaçlanan veri işleme faaliyetlerinin olası etkilerini ve sonuçlarını inceleyerek, olası ihlallere karşı

---

ve Paul De Hert, P., (Dordrecht: Springer, 2012), 34. https://doi.org/10.1007/978-94-007-2543-0_2; Clarke, "Privacy impact assessment:", 124; ICO, "Privacy Impact Assessment", 114, 151; akt. Ağıralan, "Bilgi Güvenliği, Kişisel", 65.

422 Develioğlu, *6698 sayılı Kişisel,* 112; aynı yönde Bayram, "Bir Uyum Aracı", 41.

423 GDPR md. 35: Özellikle yeni teknolojiler kullanıldığında ve işleme faaliyetinin mahiyeti, kapsamı, bağlamı ve amaçları dikkate alındığında bir işleme türünün gerçek kişilerin hakları ve özgürlükleri açısından yüksek bir riske sebebiyet vermesinin muhtemel olduğu hallerde, kontrolör, işleme faaliyetinden önce, öngörülen işleme faaliyetlerinin kişisel verilerin korunmasına olan etkisine ilişkin bir değerlendirme yapar.

424 Katerina Demetzou, "Data Protection Impact Assessment: A tool for accountability and the unclarified concept of 'high risk' in the General Data Protection Regulation", *Computer Law & Security Review*, 35/6 (2019), 2. https://doi.org/10.1016/j.clsr.2019.105342

önlemler alınmasını sağlamaktadır. Daha önce de ifade edildiği üzere, GDPR'nin 35/1. maddesi gereği, ileri teknoloji kullanılarak gerçekleştirilen ve kişisel veri ihlal riskinin yüksek olduğu işlemlerden önce, olumsuz neticelerin önceden hesaplanarak önlenmesi veya en aza indirgenmesi için önceden tedbir almak amacıyla veri koruma etki değerlendirmesi yapılması zaruridir. Öyle ki bu zorunluluk sorumluluk ve hesap verilebilirlik ilkesinin bir yansımasıdır.[425] Zira sorumluluğun nasıl yerine getirildiğinin gösterilmesi ve sorumluluğun yerine getirilmesinin ispatlanması da VKED ile mümkün olmaktadır. Kanun koyucunun buradaki amacı veri sorumlularına ek külfetler yüklemek değil, mevcut kurallara "de facto" ve etkin uyumun sağlanmasını gerçekleştirmektir.[426]

GDPR'nin öngördüğü risk temelli yaklaşıma uygun olarak VKED, sadece işlemenin *"gerçek kişilerin hak ve özgürlüklerine yönelik yüksek bir riskle sonuçlanması muhtemel"* olduğunda gereklidir. Dolayısıyla her türlü veri işleme faaliyeti için VKED zorunlu değildir. Öte yandan hangi işleme faaliyetinin *"gerçek kişilerin hak ve özgürlüklerine yönelik yüksek bir risk doğuracağının"* tespit edilmesi için risklerin sürekli olarak değerlendirilmesi gerekir.[427] Bu sebeple veri koruma etki değerlendirme süreci oldukça dinamiktir.[428] Veri koruma etki değerlendirmesi yapılırken Madde 29 Çalışma Grubunun rehberinde belirtilen; "*değerlendirme veya puanlama, yasal veya benzeri önemli etkiye sahip otomatik karar verme, sistematik izleme, hassas veri, geniş kapsamda işlenmiş veri, eşleşen veya birleştirilmiş veri setleri, ilgili kişiye ilişkin hassas veriler, yenilikçi kullanım, teknolojik veya kurumsal çözümleri uygulamak, veri işlemenin kendi içinde ilgili kişinin bir hakkını kullanmasını, bir hizmeti kullanmasını veya sözleşme yapmasını*" değerlendirerek karar verilebilecektir.[429] Veri koruma etki analizi raporu neticesinde, bir veri işleme faaliyetinin kritik riskler doğuracağı anlaşılırsa, veri sorumlusunun bu faaliyete başlamadan evvel ilgili denetim makamının görüşünü alması gerekmektedir. Ek olarak, bu yükümlülük GDPR'da "ön değerlendirme" başlığı altında da belirtilmiştir. Bu ön değerlendirme, riskli veri işleme faaliyetlerini daha yakından incelemeyi ve ilgili

---

425 Çimen Bulut, "Avrupa Birliği Genel", 134; Akıncı, "Büyük Veri ve", 83; Aşıkoğlu, *Avrupa Birliği ve*, 201

426 Demetzou, "Data Protection Impact", 2-3.

427 Tokmakcı, "Kişisel Verilerin Korunmasına", 121; benzer yönde bkz.: Atakan Yalçın, "Avrupa Birliği Genel Veri Koruma Tüzüğünde Hesap Verilebilirlik Araçları", içinde *Kişisel Verilerin Korunmasına Uzman Bakış Uzmanlık Tezleri Derleme Çalışması,* ed. Pınar Çağlayan Aksoy ve Hüseyin Can Aksoy, (Ankara: KVKK Yayınları, No 44, 2023), 758.

428 Kaya, *"Kişisel Verilerin Korunmasında"*, 1886.

429 Bayram, "Bir Uyum Aracı" 44-46.

denetim makamının rehberliğini almayı amaçlar.[430] Ek olarak GDPR'a göre veri koruma etki değerlendirmesinde yer alması gereken asgari özellikler arasında, kişisel veri işlemenin amacının ve izlenen meşru menfaatlerin açıklanması, işlemenin gerekliliği ve orantılılığı ile ilgili kişilere yönelik riskleri içermesi, tespit edilen risklere yönelik alınan tedbirlerin belirtilmesi bulunmaktadır. Bu özellikleriyle veri koruma etki analizinin, en temel hesap verebilirlik aracı olduğunu söylemek mümkündür.[431]

VKED birkaç aşamadan oluşmaktadır. Analiz aşaması sürecin başlangıcı olup ilk basit risk değerlendirmesinin yapıldığı aşamadır. "Eşik analizi (*threshold analysis*)" olarak da tanımlanan bu kısımda kişisel veri işleme faaliyetinin yüksek risk oluşturup oluşturmadığı incelenmektedir. Bu aşamada yüksek risk tespit edilirse VKED uygulama gerekliliği ortaya çıkmaktadır ki bundan sonraki süreç hazırlık aşamasını oluşturmaktadır. GDPR'ın md. 35/7a uyarınca hazırlık aşamasında planlanan işleme faaliyetlerinin ve işlemenin amaçlarının sistematik bir açıklaması yapılmalı ve bir sonraki aşama olan uygulama aşaması için organizasyon yapılmalıdır. Uygulama aşamasında, hazırlık aşamasında toplanılan bilgiler kullanılarak risk tespiti ve risk analizi yapılır. Bu sürecin sonunda veri minimizasyonunun sağlanması, kişisel verilerin amaca uygun kullanılması, kişisel verilerin gizliliğinin sağlanarak yetkisiz erişimin önlenmesi, verilerin doğru ve güncel olması, veri işleme sürecinin şeffaflığı, veri konularının herhangi bir zamanda bildirim, erişim, düzeltme, engelleme ve silme haklarını gerçekten kullanabilme yani müdahale edilebilirlik sonuçlarına ulaşması gerekmektedir.[432] Görüleceği üzere veri koruma etki analizi sonucunda elde edilmesi beklenen hedefler KVKK'nın 4. maddesinde belirtilen kişisel verilerin işlenmesinde uyulması gereken genel ilkelere de uygunluk göstermektedir.

3.4.1.2.3. Risk Etki Değerlendirmesi

Kişisel verilerin işlenmesi her zaman potansiyel riskler içerir.[433] Öte yandan bütün veri işleme faaliyetleri aynı düzeyde risk taşımaz, bu nedenle veri sorumlularının bütün veri

---

430 Aşıkoğlu, *Avrupa Birliği ve*, 203.
431 Kaya, *"Kişisel Verilerin Korunmasında"*, 1886.
432 Michael Friedewald, Ina Schiering, Nicholas Martin ve Dara Hallinan, "Data Protection Impact Assessments in Practice", içinde Computer Security, ESORICS 2021 International Workshops, (October 4-6, 2021) Darmstadt, Germany,
433 Akt. Bayram "Bir Uyum Aracı", 43; benzer yönde bkz: Yalçın, "Avrupa Birliği Genel", 757.

işleme faaliyeti için aynı önlemleri alması mantıklı değildir. Bunun yerine, etkili bir veri koruma etki değerlendirmesi yapabilmek adına kişisel verilerin korunması konusunda hangi faktörlerin risk oluşturduğu ve bu riskin olasılığı ile hassasiyetinin nasıl değerlendirileceği ile ilgili objektif ve ortak bir anlayışa ihtiyaç vardır. Bu şekilde, uygun önlemler alınarak kişisel verilerin korunması konusunda etkin bir fayda sağlanabilir.[434] Başka bir ifadeyle veri korumasında riskin ne olduğunu tanımlamak yeterli değildir. Aynı zamanda, veri sorumlusunun ciddiyeti ve olasılığı nasıl değerlendirmesi gerektiği konusunda ortak bir yaklaşımın olması da önemlidir.[435] Uygun güvenlik düzeyinin tespit edilmesi için aktarılan, saklanan veya değişik şekilde işlenen kişisel verilerin yanlışlıkla veyahut hukuka aykırı biçimde tahrifi, kaybedilmesi, değiştirilmesi, izin olmadan ifşası veya erişilmesi öncelikli olmak üzere veri işlemenin barındırdığı riskler dikkate alınır.[436]

Risk etki değerlendirmesi, belirli risklerin, o risklerin gerçekleşmesi durumunda ortaya çıkacak etkilerin ve bu etkilerin olasılıklarının sistematik bir şekilde değerlendirildiği bir süreçtir. Bu yöntem, veri sorumlularının riskleri tanımlamalarına, önceliklendirmelerine ve risklere karşı uygun tedbirleri planlamalarına yardımcı olur. Risk etki değerlendirmesi aşağıdaki adımları içermelidir:

1. **Risk Tanımlama:** İlk adım, organizasyonun karşılaşabileceği olası risklerin tanımlanmasıdır. Bu riskler, iç ve dış tehditler, olumsuz olaylar veya belirsizlikler olabilir.

2. **Risk Analizi:** Belirlenen risklerin detaylı bir şekilde analiz edildiği aşamadır. Bu aşamada, risklerin olasılıkları, etkileri ve riskin süresi değerlendirilir.

3. **Risk Değerlendirmesi:** Risklerin etkisi ve olasılığı birleştirilerek riskler önceliklendirilir. Bu, organizasyonun hangi risklere daha fazla odaklanması gerektiğini belirlemesine yardımcı olur.

434 Akt. Bayram "Bir Uyum Aracı", 43.
435 Demetzou, "Data Protection Impact", 5.
436 Develioğlu, *6698 sayılı Kişisel,* 107.

4. **Risk İzleme ve Kontrol:** Risk etki değerlendirmesi, organizasyonun riskleri yönetmesine yardımcı olur. Risklerin izlenmesi ve kontrol altında tutulması, gerektiğinde önlemlerin alınmasını sağlar.

Risk etki değerlendirmesi, organizasyonların daha iyi kararlar almalarına, kaynakları daha etkili bir şekilde kullanmalarına ve potansiyel risklere karşı hazırlıklı olmalarına yardımcı olur. Ayrıca, yasal gerekliliklere uymak ve itibar kayıplarını önlemek için de önemlidir.[437] Zira uygulanacak somut yöntemlerin ve alınacak önlemlerin belirlenmesi için "risk" bir kriterdir.[438]

3.4.1.3. İlke Kararları Doğrultusunda Risk Etki Değerlendirmesi

Kişisel verilerin işlenmesinde ortaya çıkacak risklerin değerlendirilmesi ve yapılacak değerlendirme neticesinde işleme faaliyetine yönelik bir denetim makamına başvuru yapılması KVKK'da düzenlenmemiştir. Kanuni bir düzenleme olmaması veri sorumlularının risk değerlendirmesi yapmasını engellemeyecektir. Zira veri güvenliğinin sağlanması için bu değerlendirmenin yapılması gereklidir. Kişisel Verileri Koruma Kurumu da yayımlamış olduğu "Yapay Zekâ Alanında Kişisel Verilerin Korunmasına Dair Tavsiyeler"de[439] "*kişisel veri işleme temelli yapay zekâ çalışmalarında, kişisel verilerin korunması açısından yüksek risk öngörülüyorsa, mahremiyet etki değerlendirmesi uygulanması ve veri işleme faaliyetinin hukuka uygunluğuna bu çerçevede karar verilmesi",* "*hesap verebilirlik ilkesinin tüm aşamalarda gözetilmesi gerektiği*" ve "*kişisel verilerin korunmasına yönelik risk değerlendirme prosedürleri benimsenmesi ve sektör/uygulama/donanım/yazılım temelinde bir uygulama matrisi oluşturulması gerekliliği*" hususlarına dikkat çekmiştir. Öte yandan bazı kurum ve kuruluşlar için ISO 27001 Bilgi Güvenliği Yönetim Standartlarının (BGYS) gerektirdiği standartları kurumların bilgi güvenliği sistemine uygulaması zorunluluğu bulunmaktadır.[440] ISO 27001 BGYS standardı kurumun risk yönetimini ve risklerini

---

437 Aynı yönde bkz.: Ağıralan, "Bilgi Güvenliği, Kişisel", 38; Bilgin, Erkan, Atasu ve Yılmaz, "Privacy Impact Assessment", 84.

438 Demetzou, "Data Protection Impact", 5.

439 Kişisel Verileri Koruma Kurumu, "Yapay Zekâ Alanında Kişisel Verilerin Korunmasına Dair Tavsiyeler", (E.T. 24.01.2024), https://www.kvkk.gov.tr/Icerik/7048/Yapay-Zeka-Alaninda-Kisisel-Verilerin-Korunmasi na-Dair-Tavsiyeler

440 ISO 27001 Bilgi Güvenliği Yönetim Sistemi Belgesi alma zorunluluğu bulunan sektörler için bkz: (E.T. 17.03. 2024), https://www.isokalitebelgesi.com/iso-27001-belgesi-kimler-hangi-sektroler-sirketler-firmalar-alabilir-zorunlumudur

tanımlayan süreçleri belgeleyerek; kurumun bilgi varlıklarını, riskleri, kabul edilebilir riskleri, risk faktörünü azaltabilecek riskleri tanımlayarak risk yönetimi modelleyerek riskleri azaltmak veya ortadan kaldırmayı amaçlamaktadır.[441]

Kurul tarafından yapay zekâ alanında işlenen verilerin korunmasına ilişkin mahremiyet etki değerlendirmesi yapılması tavsiye edilmişse de veri işleme faaliyetlerinin yalnızca yapay zekâ alanında ve bu yöntem ile olmadığı açıktır. Öte yandan Kurul'un veri koruma etki değerlendirmesi yerine mahremiyet etki değerlendirmesine atıf yapmış olması da veri işleme süreçlerindeki risklere geniş perspektiften bakılması gerektiği şeklinde yorumlanabilecektir. Yine risk temelli yaklaşıma uygun olarak ISO 27001 standartlarının benimsenmesi de veri ihlallerinin önüne geçilmesi açısından risk yönetimi kriterlerinin uygulanması, veri ihlal süreçlerinin mahremiyet etki değerlendirmesinden de geniş olan risk yönetimi bazında ele alınabileceği şeklinde anlaşılabilir. Aynı zamanda veri sorumlusunun, veri güvenliğinin sağlanması için alması gereken önlemlerde risk analizleri ve değerlendirmelerine yer verilmiş olması da bu yorumu desteklemektedir.

Kişisel verilerin işlenmesi süreçlerinde risk, kişisel verilerin ihlal edilmesi ve ihlalin yaratacağı etkilerdir. Gerek MED gerekse VKED kişisel veri ihlali yaşanmadan önce başlatılması gereken süreçlerdir. Her ne kadar risk etki değerlendirilmesi veri ihlali öncesinde başlatılması gereken bir süreç olsa da burada veri ihlali risklerini ele alırken, yaygın ihlallerin doğurduğu olası risklerin belirlenmesi ve süreçteki risklerin geniş bir bakış açısıyla incelenmesi gerekliliği nedeniyle, risk etki değerlendirmesi terimi ve yöntemi tercih edilmiştir. Açıklamalar ışığında Kişisel Verileri Koruma Kurulunun ilke kararları doğrultusunda yaygın olarak yaşanan kişisel veri ihlallerinin risk etki değerlendirmesi şu şekilde yapılabilir:

441 Ali Durdu, "Bilgi Sistemlerinde Riskler ve Risk Yönetimi", içinde *Uzmanların Kaleminden Farklı Boyutlarıyla Risk ve Risk Yönetimi,* ed. Hakan Karabacak, (Ankara: Gazi Kitabevi, Temmuz 2021), 200.

1. **Kişisel Verilerin Hukuka Aykırı Olarak İşlenmesi (md.12):**

- **Risk Tanımlama**: İşlenen kişisel verilerin izinsiz ya da hukuka aykırı bir biçimde kullanılması veya ifşa edilmesi potansiyel bir risk oluşturur.
- **Risk Analizi**: Hangi tür verilerin ne şekilde işlendiğinin detaylı analizi yapılmalıdır. Veri güvenliği önlemlerinin ne kadar etkili olduğu değerlendirilmelidir.
- **Risk Değerlendirmesi (Olası Etki)**: Hukuka aykırı veri işleme riskinin, müşteri güveninin sarsılması ve yasal yaptırımlarla sonuçlanma gibi ciddi etkileri olabilir.
- **Risk İzleme ve Kontrol**: Veri işleme süreçlerinin düzenli olarak izlenmesi, izinsiz erişim girişimlerinin tespiti ve veri güvenliğinin güncellenmesi gibi önlemler alınmalıdır.

2. **Kişisel Verilere Hukuka Aykırı Erişilmesi (md. 12):**

- **Risk Tanımlama**: Kişisel verilere yetkisiz erişim, veri ihlali riskinin artmasına neden olur.
- **Risk Analizi**: Hangi verilere erişim sağlandığı, kimlerin erişebildiği ve erişim izinlerinin nasıl yönetildiği detaylı olarak incelenmelidir.
- **Risk Değerlendirmesi (Olası Etki)**: Hukuka aykırı erişim riski, gizlilik ihlalleri, itibar kaybı ve yasal sorunlar gibi ciddi sonuçlar doğurabilir.
- **Risk İzleme ve Kontrol**: Erişim izinleri periyodik olarak gözden geçirilmeli, izinsiz girişimler tespit edilmeli ve erişim kontrolü güçlendirilmelidir.

3. **Kişisel Verilerin Muhafazasının Sağlanmaması (md. 12):**

- **Risk Tanımlama**: Kişisel verilerin yeterince korunmaması, veri güvenliği riskini artırır.

- **Risk Analizi**: Veri saklama ve koruma politikalarının gözden geçirilmesi, fiziksel ve dijital güvenlik önlemlerinin incelenmesi gerekir.
- **Risk Değerlendirmesi (Olası Etki)**: Veri koruma eksiklikleri, veri kaybı, veri sızıntısı ve yasal yaptırımlar gibi sonuçlar doğurabilir.
- **Risk İzleme ve Kontrol**: Güvenlik sistemlerinin düzenli olarak kontrol edilmesi ve güncellenmesi, veri kaybını önlemek için yedekleme stratejilerinin belirlenmesi gerekmektedir.

4. Kişisel Verilerin Hukuka Aykırı Olarak Aktarılması (md. 8-9):

- **Risk Tanımlama**: Kişisel verilerin yasalara aykırı bir şekilde aktarılması veya paylaşılması kişisel veri güvenliğini ve gizliliğini tehlikeye atabilen önemli bir risk oluşturur.
- **Risk Analizi**: Hangi aşamalarda hataların meydana gelebileceği ve yasadışı veri elde etmenin nasıl gerçekleşebileceği analiz edilir.
- **Risk Değerlendirmesi (Olası Etki)**: Yasal yaptırımlar, itibar kaybı, müşteri güveninin zedelenmesine neden olabilir.
- **Risk İzleme ve Kontrol**: Veri transfer politikalarının gözden geçirilmesi, izin süreçlerinin yeniden değerlendirilmesi, veri aktarımının şifrelenmesi, gerekmektedir.

5. Kişisel Verilerin Hukuka Aykırı Şekilde Elde Edilmesi (md.5-6):

- **Risk Tanımlama**: Kişisel verilerin yasalara aykırı bir şekilde elde edilmesi veya toplanması.
- **Risk Analizi**: Hangi aşamalarda hataların meydana gelebileceği ve yasadışı veri elde etmenin nasıl gerçekleşebileceği analiz edilir.
- **Risk Değerlendirmesi (Olası Etki)**: İtibar kaybı, yasal yaptırımlar, müşteri güveninin sarsılmasına neden olabilir.

- **Risk İzleme ve Kontrol**: Veri toplama süreçlerinin gözden geçirilmesi, kullanıcı onaylarının güçlendirilmesi, veri toplama politikalarının yeniden düzenlenmesi, erişim kontrollerinin güçlendirilmesi, izinsiz veri elde etme girişimleri tespit edilebilir hale getirilmesi gerekmektedir.

6. Kişisel Verilerin Elde Edildiği Kaynağın Belirli Olmaması (md.4):

- **Risk Tanımlama**: Kişisel verilerin elde edildiği kaynağın belirli olmaması, veri kaynaklarının izlenememesi veya kontrol altına alınamaması potansiyel bir risk oluşturur.

- **Risk Analizi**: veri toplama süreçlerindeki zayıf noktalar ve uyumsuzluklar incelenerek veri kaynaklarının belirlenmesi ve takibi için kullanılan mevcut sistemlerin etkinliği değerlendirilir.

- **Risk Değerlendirmesi (Olası Etki)**: Veri bütünlüğü kaybı, güvenilirlik sorunları, yasal uyumsuzluk nedeniyle idari ya da cezai yaptırımlara neden olabilir.

- **Risk İzleme ve Kontrol**: Veri kaynaklarının belirlenmesi için sistemlerin güncellenmesi, veri akışlarının izlenmesi; izleme, raporlama, kontrol ve denetim mekanizmalarının kurulması gerekmektedir.

7. Kişisel Verilerin İşlenmesinde Genel İlkelere Aykırılık (md.4):

- **Risk Tanımlama**: Kişisel verilerin işlenmesinde genel ilkelere uyulmaması kanuna aykırı veri işleme faaliyetidir. Hukuka aykırı kullanım her türlü potansiyel riski oluşturur.

- **Risk Analizi**: Veri işleme süreçlerindeki mevcut uygulamaların mevzuata uygunluğu değerlendirilir.

- **Risk Değerlendirmesi (Olası Etki)**: Yasal yaptırımlar, müşteri güveninin sarsılması, itibar kaybına neden olabilir.

- **Risk İzleme ve Kontrol**: İşlem süreçlerinin revize edilmesi, iç denetimlerin sıklaştırılması, mevcut veri işleme politikaları ve prosedürlerinin güncellenmesi

ve iyileştirilmesi, çalışan eğitimlerinin ve farkındalık artırma faaliyetlerinin düzenlenmesi gerekmektedir.

8. İlgili Kişinin Haklarının Kullandırılmaması (md.11):

- **Risk Tanımlama**: İlgili kişilerin haklarının yeterince kullanılmaması veya korunmamasıdır.
- **Risk Analizi**: İlgili kişilerin haklarının kullanılmamasına veya kısıtlanmasına neden olabilecek süreçler ve uygulamalar incelenerek hangi aşamalarda hataların oluşabileceği, hangi durumların ilgili kişilerin haklarını etkileyebileceği analiz edilir.
- **Risk Değerlendirmesi (Olası Etki)**: Yasal yaptırımlar, müşteri güveninin sarsılması, itibar kaybına neden olabilir.
- **Risk İzleme ve Kontrol**: İlgili kişilere erişim haklarının güçlendirilmesi, taleplere zamanında yanıt verilmesi, ilgili kişilere yönelik iletişim kanallarının güçlendirilmesi ve alınan önlemlerin sürekli takip edilmesi gerekmektedir.

Bahsi geçen değerlendirmeler örnek olarak verilmiştir. Her veri sorumlusunun risk, olasılık ve etki değerlendirmesi kendi özel koşullarına dayanmalıdır. Eğer veri sorumlusu için bir riskin olasılık ve etki derecesi daha yüksek veya daha düşükse buna göre düzenleme yapılabilir. Her durumda organizasyonların kendi spesifik veri işleme süreçleri ve koşulları göz önüne alınarak risk değerlendirmesi yapmaları önemlidir. İhtiyaç halinde bu değerlendirmeleri gözden geçirmek ve ayarlamak veri koruma stratejilerini daha iyi bir şekilde optimize etmelerine yardımcı olacaktır. Kişisel veri ihlallerinin yaşanmasının engellenmesi ya da en aza indirilmesi adına gerekli olan etki değerlendirmesi kullanımının yaygınlaşması için biz dizi strateji uygulanması gerekmektedir. Mahremiyet, veri koruma veya risk etki değerlendirmesinin olası kullanımı ve faydaları hakkında da farkındalık gerekmektedir. Öte yandan kanaatimizce veri sorumlusunun veri güvenliğini sağlamaya yönelik yükümlülüklerinin düzenlendiği KVKK'nın 12. maddesinde değişiklik yapılması faydalı olabilir. GDPR md.35 ve

devamı[442] düzenlemeleri göz önüne alınarak 12/1. maddede yer alan "*1) Veri sorumlusu; a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek, c) Kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır."* hükmünün devamına "*Veri sorumlusu, veri işleme faaliyetlerinin kişilerin hak ve özgürlüklerine yönelik yüksek risk oluşturmasının muhtemel olması durumunda, veri işleme faaliyetine başlamadan önce, faaliyetlerin kişisel verilerin korunması üzerindeki etkisinin değerlendirmesini yapmakla yükümlüdür. Bu etki değerlendirmesi, özellikle riskin azaltılması, kişisel verilerin korunmasının sağlanması ve güvenlik tedbirlerini içermelidir.*" minvalinde bir düzenleme getirilmelidir. Yapılan değerlendirme neticesinde veri güvenliğine ilişkin yükümlülüklerin yerine getirilmesi durumunda dahi yüksek risk söz konusu ise veri işleme faaliyeti öncesinde Kurul'a başvuru yapılmasına ilişkin Kanun'un 12/3 maddesine[443] de ek bir hüküm eklenmelidir. GDPR gereğince etki değerlendirmesinin özellikle gerekli olduğunun belirtildiği haller olan "*kamuya açık alanların büyük ölçekte takip edilerek sistematik izlenerek veri işlemesinin yapılması, özel kategorilerdeki verilerin büyük ölçekte işlenmesi, gerçek kişilere ait verilerin sistematik olarak değerlendirilmesi ve bu değerlendirmeye dayalı olarak yasal sonuçlar doğuran veya benzeri şekilde önemli ölçüde etkileyen kararlar alınmasını sağlanması*" gibi veri işleme faaliyetlerine ilişkin esasların da bir yönetmelik veya rehber ile düzenlenmesi gerekmektedir.

3.4.2. Bilgi Güvenliği ve Veri Güvenliğinin Sağlanması

Veri sorumlusunun KVKK ve GVKT kapsamında en temel yükümlülüklerinden biri, işlediği kişisel verilerin idari ve teknik boyutta güvenliğini ve gizliliğini temin etmektir. Yasal yükümlülük olarak düzenlenen ve ihlali halinde yaptırımlar öngörülen bu yükümlülüğün ihlali halinde, veri ihlali ortaya çıkmaktadır.[444]

---

442 Recital 84, 89, 90, 91, 92. (E.T.07.07.2024), https://gdpr-info.eu/recitals/

443 KVKK md. 12/3: "*Veri sorumlusu, kendi kurum veya kuruluşunda, bu Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorundadır*."

444 Sevindi ve Ordu, "AB ve Türk Hukukunda", 13.

3.4.2.1. Bilgi Güvenliği ve Veri Güvenliği

Veri güvenliği ile kişisel verilerin korunması kavramları birbirinden farklıdır. Veri güvenliği daha çok teknik unsurları içeren bir kavram olup amacı belirli standartlara uyum sağlamaktır. Öte yandan veri güvenliği ve özellikle Kanunun 12/1. maddesinde ifade edilen hükümler, Kanunun 1. maddesinde işaret edilen hakların korunmasına hizmet eden gerekli teknik yöntemleri içermektedir. Ek olarak, teknik ve idari tedbirler Kanun'da öngörülen hukuka uygunluk sebeplerini de tamamlamaktadırlar. Zira her ne kadar Kanunun 12/1. maddesinde belirtilen yükümlülükler tek başına hukuka uygunluk sebebi olmasa da bahsi geçen sorumlulukların hukuka uygunluk sebeplerinin yanında dikkate alınmaları zorunludur.[445]

Veri güvenliği, bilgi güvenliğinin bir parçası olarak ifade edilir ve bilgi güvenliği politikaları, bir organizasyonun gizli, stratejik ve spesifik bilgilerin yönetimini, korunmasını, güvenli yöntemlerle paylaşımını ve uyumunu düzenleyen kurallar ve uygulamalar bütünüdür.[446] Kişisel verilerin korunması için bilgi güvenliği tedbirleri, verilerin elde edilmesinden imha edilmesine kadar süren aşamalarda etkin bir güvenlik zinciri oluşturur. Bu zincir, bilginin işlenmesine katılan tüm aktörler için belirli bir düzeyde sorumluluk getirir. Bilgi güvenliği zinciri, verilerin güvende tutulmasını sağlamak için teknik ve hukuki önlemlerin birleşimini temsil eder. Bu sebeple, teknik tedbirlerin yanında, hukuki yükümlülükler çerçevesinde veri sorumlusu olarak faaliyet gösteren idari personelin de sorumluluklarını yerine getirmesi son derece önemlidir. Bu husus, veri koruma sürecinin her aşamasında, veri güvenliği ve gizliliği sağlama konusundaki sorumluluklarını ifa etmelerini içerir. Yani, veri sorumlularının sadece teknik önlemlere değil, aynı zamanda yasal ve idari gereksinimlere de dikkat etmeleri gerekmektedir.[447] Başka bir ifade ile bilgi güvenliği, esasında tehditleri bertaraf etmekten önce riskleri belirleyip yönetmek ile ilgili süreçleri ifade etmektedir. Bu doğrultuda yüksek düzeyde bilgi güvenliği için teknik, operasyonel ve kurumsal kontrollerin hepsinin birden gözden geçirilmesi gerekmektedir. Bütünsel olarak bakıldığında ilgili

---

445 Çekin, *Avrupa Birliği Hukukuyla,* 145.

446 Korucu, *Veri Güvenliğinin İyileştirilmesinde,* 43.

447 Türkay Henkoğlu, "Kişisel Verileriniz Ne Kadar Güvende? Bilgi Güvenliği Kapsamında Bir Değerlendirme", *Arşiv Dünyası,* 2017/1 (2017): 46-56, 47-48. (E.T. 24.09.2023), www.idealonline.com.tr

teknolojik altyapının ilk aşamada sağlanması gerekmektedir. Kurumsal planlama kapsamında ise personelin eğitimi, iş sürekliliği planlamasının yapılması gibi bilgi güvenliğinin teknik olmayan kısımlarının da ele alınması hedeflenmektedir.[448]

Bilginin korunan niteliği "gizlilik, bütünlük ve kullanılabilirlik" olmak üzere temel olarak üç kriterden oluşur. Bu unsurlar, bilgi güvenliğinin ana hedeflerini ifade eder ve bilgi güvenliği, bu üç temel unsur arasında bir denge kurmayı amaçlar.[449] Genel olarak, bilgi varlıkları göz önüne alındığında, gizlilik, bütünlük ve kullanılabilirlik arasında bir denge bulunması tercih edilir. Ancak, özellikle elektronik ortamdaki bilgi güvenliği söz konusu olduğunda, gizlilik ve bütünlük daha fazla vurgulanır. Bu durumda, bilgiye erişilebilirlik ve güvenlik arasındaki denge üzerinde daha fazla odaklanmak ve güvenlik stratejilerini bu çerçevede geliştirmek önemlidir.[450] Veri güvenliğinin sağlanması için oluşturulan kurumsal bilgi güvenliği politikaları, kurum ve kuruluşlarda bilgi güvenliği yönetiminin sağlanması ve bilgi güvenliği çerçevesinin tespit edilmesi amacıyla tüm bilgi güvenlik faaliyetlerini kapsamaktadır ki bu kurallar yönlendirici kurallar bütününü oluşturmaktadır. Bu kurumsal dokümanlar, organizasyonun bilgi kaynaklarına ve ortamlarına erişim izni bulunan tüm çalışanlar, iş ortakları ve dış hizmet sağlayıcıları için geçerli olan kurumsal dokümanları içerir ve bunlara uyulması için gereken talimatları belirler.[451]

Bilgi güvenliği ile veri güvenliği kavramlarını şu şekilde açıklamak mümkündür:

1. **Kapsam:**

- Bilgi Güvenliği: Bilgi güvenliği, bir organizasyonun tüm bilgi varlıklarını, bu varlıkların bütünlüğünü, gizliliğini ve erişilebilirliğini korumayı amaçlar. Bu husus, sadece verileri değil, aynı zamanda bilgisayar sistemlerini, ağları, yazılımları, süreçleri ve insan faktörünü de içerir.
- Veri Güvenliği: Veri güvenliği, sadece organizasyonun sahip olduğu verilerin güvenliğini ele alır. Bu, verilerin bütünlüğünü, gizliliğini ve erişilebilirliğini

448 Mehmet Serdar Güzel, "Bilgi Güvenliği (Information Security)", içinde *Siber Ansiklopedi: Siber Ortama Çok Disiplinli Bir Yaklaşım*, ed. Naci Akdemir ve Can Ozan Tuncer, (Ankara: Pegem Akademi, Ağustos 2021), 40.
449 Henkoğlu, "Kişisel Verileriniz Ne Kadar", 49; Yılmaz, "TS ISO/IEC 27001 Bilgi Güvenliği", 47.
450 Henkoğlu, "Kişisel Verileriniz Ne Kadar", 49.
451 Korucu, *Veri Güvenliğinin İyileştirilmesinde*, 43.

korumak için alınan önlemleri içerir. Veri güvenliği, bilgi güvenliği kavramının daha dar bir alt kümesidir.

2. **Odak Noktası:**

- Bilgi Güvenliği: Bilgi güvenliği, organizasyonun tüm süreçlerini ve varlıklarını korumayı hedefler. Bu, siber saldırılara karşı genel bir koruma sağlamayı amaçlar ve organizasyonun iş sürekliliğini sürdürmesine yardımcı olur.
- Veri Güvenliği: Veri güvenliği, özellikle organizasyonun sahip olduğu verilerin korunmasına odaklanır. Bu, verilerin yetkisiz erişimden korunmasını ve veri kaybını önlemeyi amaçlar.

3. **Kapsamın Daraltılabilirliği:**

- Bilgi Güvenliği: Bilgi güvenliği, organizasyonun genel güvenlik stratejilerini ve politikalarını içerir, bu nedenle daha geniş bir kapsama sahiptir ve daha geniş bir perspektiften ele alınır.
- Veri Güvenliği: Veri güvenliği, sadece organizasyonun sahip olduğu belirli verilere odaklandığı için daha dar bir kapsama sahiptir.

"Verinin" içerdiği en önemli özellik bir bilgiyi ihtiva etmesidir.[452] Bu nedenle her iki kavram da organizasyonlar için önemlidir ve sık sık birlikte ele alınır. Bilgi güvenliği, veri güvenliği dahil olmak üzere bir dizi alt konuyu içerir ve organizasyonların siber tehditlere karşı savunma sağlaması için bütüncül bir yaklaşım benimsemelerini gerektirir.

3.4.2.2. Veri Sorumlusunun Sorumluluğu

Kişisel verileri belirli bir organizasyon kapsamında işleme faaliyetine tâbi tutan veri sorumlularının uhdesinde bulunan kişisel verileri koruması adına bir dizi önlemler alması gerekmektedir. Bu önlemler arasında, veri sorumlusunun veri güvenliğine ilişkin yükümlülüklerini yerine getirmesi hususu da yer almaktadır ki bu yükümlülük, veri ihlallerinin yaşanmaması için en önemli adımı oluşturmaktadır. Zira İlke Kararlarına bakıldığında da veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi nedeniyle ilgili kişilerin haklarını kullanarak Kurula ihbar ve şikâyette bulunduğu, verilen İlke

[452] Şerafettin Ekici, *Bilişim ve Teknoloji Hukuku*, (Ankara: Seçkin Yayınları, 2023), 308.

Kararlarının çoğunun veri güvenliğine ilişkin yükümlülüklere aykırı faaliyetler olduğu görülmektedir.

Defaatle ifade edildiği üzere KVKK'nın 12. maddesinde yer alan "*Veri sorumlusu; a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek, c) Kişisel verilerin muhafazasını sağlamak, amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbiri almak zorundadır"* hükmü ile veri sorumlusunun veri güvenliği ile ilgili yükümlülükleri belirlenmiştir. Görüleceği üzere veri güvenliğine ilişkin yükümlülükler Kanunda genel ifadelerle düzenlenmiş olup veri güvenliği ile alakalı yükümlülükleri düzenleme adına düzenleyici işlem yapma yetkisi ve görevi Kurula verilmiştir.[453] Bu doğrultuda Kurul tarafından kişisel verilerin işlenme süreçlerinde veri sorumlularının alması gereken idari ve teknik önlemler hususunda uygulamada netlik sağlanması ve uygulama açısından iyi örneklerin oluşturulması maksadıyla Kişisel Veri Güvenliği Rehberi ("Rehber") hazırlanmıştır.[454] Bunun yanı sıra sektörel bazda işlenen kişisel verilerin vasfına göre Kurul tarafından ek önlemler alınmasına karar verilebilecektir.[455]

Tarihsel olarak bilginin temel özellikleri (gizlilik, bütünlük, kullanılabilirlik) değişmemiş olsa da bilginin işlenmesi, depolanması ve transferi gibi süreçlerde önemli değişiklikler yaşanmıştır. Bu değişiklikler, bilgi güvenliği önlemlerinin türünü ve ağırlığını da etkilemiştir. Gelecek nesillere aktarılacak bilgi varlıklarının güvenliği için dikkate alınması gereken önemli unsurlar şunlardır: teknoloji, bilgi güvenliği politikaları ve eğitim/farkındalık. Ancak, her biri ayrı ayrı ele alınmalı ve belirli bir güvenlik stratejisi için bir araya getirilmelidir. Güvenlik önlemleri bir sistem yaklaşımı içinde değerlendirildiğinde, teknik önlemler, idari önlemler ve bilgi hukuku, bütünleşik bir sistemin parçalarını oluştururlar. Yani, güvenlik stratejisi oluştururken teknoloji kullanımı, idari tedbirler ve uygun hukuki düzenlemelerin bir arada ele alınması önemlidir. Bu yaklaşım, bilgi güvenliği konusunda daha kapsamlı ve etkili bir koruma sağlar.[456]

---

453 Kişisel Verileri Koruma Kurumu, "Veri Güvenliğine İlişkin Yükümlülükler", (E.T. 17.09.2023), https://www .kvkk.gov.tr/ Icerik/2040/Veri-Guvenligine-Iliskin-Yukumlulukler

454 Kişisel Verileri Koruma Kurumu, *Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)*, 2.

455 Saka ve Çağlayan ve Koca, *Avrupa Birliği Hukuku*, 38.

456 Henkoğlu, "Kişisel Verileriniz Ne Kadar", 49.

Teknolojinin sağladığı imkanlar ve oluşturduğu tehlikeler göz önüne alındığında daha önce de belirtildiği üzere kişisel verilerin korunmasında salt hukuki yöntemlerle sınırlı kalınmamalı teknoloji destekli yollar da esas alınmalıdır. Şöyle ki; veri sorumlusundan işlevsel ve güvenilebilir bir koruma geliştirmesi için gereken tüm tedbirleri alması beklenir. Özellikle teknoloji geliştikçe veri işleyene karşı olan tedbir beklentisi de doğru orantıda artacaktır. Öte yandan her teknolojik gelişmenin akabinde kanun koyucudan yasal düzenleme yapması beklenemeyecektir. Bu nedenle veri işleyenin "gerekli tedbirleri" almasının öngörüldüğü esnek düzenlemeler benimsenmektedir. Bu doğrultuda bilhassa ölçülülük ilkesi göze çarpmaktadır. Nitekim işlenen verinin niteliği ve temel hak ve hürriyetlere karşı yapılabilecek olası müdahale göz önüne alındığında bu müdahalenin en az seviyeye indirilmesi adına uygun ve gereken önlemlerin alınması gerekmektedir.[457] Başka bir anlatım ile söz konusu yükümlülükler mutlak bir neticeyi gerekli kılmamaktadır. Zira veri sorumlusunun her türlü müdahaleyi önleme yükümlülüğü yoktur. Kanunda belirtilen düzenlemede sonuca bağlı bir sorumluluk halinden bahsedilmemektedir. Hüküm ile veri sorumlusunun kendi üzerine düşen tedbirleri alması durumunda artık sorumluluktan kurtulabileceği belirtilmektedir. Dolayısıyla bahsi geçen kapsamda bir özen sorumluluğu durumundan bahsetmek daha isabetli görünmektedir.[458] Ek olarak veri sorumlusunun alması gereken önlemlere ilişkin dinamik bir süreç yürütülmesi gerekmektedir. Kişisel veri işleme faaliyetlerine ilişkin alınacak önlemler ihtiyaca göre şekillendiği için gerektiğinde güncelleme yapılmalı gerekirse yeni tedbirler alınmalıdır.

Açıklamalar doğrultusunda veri sorumlusunun kişisel verilerin muhafazası yükümlülüğü bağlamındaki tedbirleri idari ve teknik tedbirler olarak 2 ana başlık altında incelenebilir.

3.3.2.2.1. İdari Tedbirler

İdari tedbirler, kişisel veri işleme süreçlerini etkili bir şekilde yönlendirmek ve korumak amacıyla alınan yönetimsel önlemleri içermektedir. Belirtilen tedbirler kişisel veri işleme envanterinin hazırlanmasından kurumsal politika ve prosedürlerin geliştirilmesine, sözleşmeler ve gizlilik taahhütnamelerinden iç denetim ve risk analizlerine kadar bir dizi

457 Çekin, *Avrupa Birliği Hukukuyla*, 11,12.
458 Çekin, *Avrupa Birliği Hukukuyla,* 145.

kritik adımı içermektedir. Ayrıca, iş sözleşmeleri ve disiplin yönetmeliklerinin düzenlenmesinden kurumsal iletişim ve eğitim stratejilerine kadar uzanan önemli konuları ele alarak, veri güvenliği kültürünün oluşturulmasını ve sürdürülmesini desteklemeyi amaçlamaktadır.

Tablo 3.3. İdari Tedbirler[459]

İdari Tedbirler ve Stratejiler	Açıklama
Kişisel Veri İşleme Envanteri Hazırlanması	• Kurum içinde işlenen kişisel verilerin belirlenmesi ve envanterin oluşturulması. • Veri envanterinin düzenli olarak güncellenmesi ve değişikliklerin izlenmesi.
Kurumsal Politikalar ve Prosedürler	• Erişim politikalarının oluşturulması ve sınırlanması. • Bilgi güvenliği politikalarının tanımlanması ve uygulanması. • Veri kullanımı, saklama ve imha politikalarının geliştirilmesi.
Sözleşmeler ve Gizlilik Taahhütnameleri	• Veri sorumlusu ve veri işleyen arasındaki sözleşmelerin düzenlenmesi. • Çalışanlardan gizlilik taahhütnameleri alınması.
İç Denetim ve Risk Analizleri	• Kurum içi periyodik ve rastgele denetimlerin düzenlenmesi. • Veri güvenliği risk analizlerinin yapılması ve risklerin belirlenmesi.
İş Sözleşmesi ve Disiplin Yönetmeliği	• Kanuna uygun hükümlerin iş sözleşmelerine eklenmesi. • Disiplin yönetmeliğinin kişisel veri güvenliği ihlallerini içerecek şekilde düzenlenmesi.
Kurumsal İletişim ve Eğitim	• Kriz yönetimi planlarının oluşturulması ve uygulanması. • İlgili kişileri (kurul, müşteriler vb.) veri güvenliği ihlalleri hakkında bilgilendirme süreçlerinin belirlenmesi. • Çalışanlara düzenli veri güvenliği eğitimleri verilmesi.
VERBİS[460] Bildirimi	• Kişisel veri işleme faaliyetlerinin VERBİS'e bildirilmesi ve güncel tutulması.

İlke kararı alınmasına neden olan ve Tablo 3.1.'de sınıflandırılmış olarak belirtilen "*kişisel verilerin hukuka aykırı olarak işlenmesi (md.12), kişisel verilere hukuka aykırı erişilmesi (md 12) kişisel verilerin muhafazasını sağlanmaması (md. 12), kişisel verilerin*

459 Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler) esas alınarak hazırlanmıştır.

460 Veri Sorumluları Sicil Bilgi Sistemi (VERBİS) çalışan sayısı 50'den fazla olan veya yıllık bilançosu 100 milyon TL'den fazla olan veya ana faaliyet alanı özel nitelikli kişisel veriler olan veri sorumlularının kayıt olmak zorunda olduğu bir sicildir. Sicile kayıt yükümlülüğüne ilişkin ayrıntılı düzenlemeler 30 Aralık 2017 tarihli ve 30286 sayılı Resmî Gazete' de yayımlanarak 01 Ocak 2018 tarihinde yürürlüğe giren "Veri Sorumluları Sicili Hakkında Yönetmelik" ile yapılmıştır. Bunun haricinde Kurul tarafından yayımlanan VERBİS Kılavuzunda konuya ilişkin açıklayıcı bilgilere yer verilmiştir.

hukuka aykırı olarak aktarılması, kişisel verilerin hukuka aykırı şekilde elde edilmesi, kişisel verilerin elde edildiği kaynağın belirsiz olması, kişisel verilerin işlenmesinde genel ilkelere aykırılık, ilgili kişinin haklarının kullandırılmaması" olaylarında veri güvenliğinin sağlanmasına ilişkin idari tedbirlerin eksikliği söz konusudur. Bu doğrultuda:

1. İlgililere veri güvenliği ihlalleri hakkında bilgilendirme yapılmaması ve/veya çalışanlara düzenli veri güvenliği eğitimleri verilmemesi gibi kurumsal iletişim ve eğitim eksikliğine dayalı farkındalığın oluşmadığı

2. Veri güvenliği risk analizlerinin ve iç denetimlerinin yapılmadığı,

3. Kişisel veri envanteri ve kişisel verilerin işlenmesi, saklama, erişim, aktarma gibi kurumsal politika ve prosedürlerin gereği gibi ya da hiç düzenlenmediği anlaşılmaktadır.

Kurumsal iletişim ve eğitimin veri sorumlusu organizasyonunda en temel idari tedbir olduğu, farkındalık eğitimleri doğrultusunda güvenilir ve işlevsel güvenlik zincirinin oluşturulacağı ve buna bağlı olarak kurumsal politika ve prosedürlerin öneminin anlaşılacağı şüphesizdir. Eğitim eksikliği nedeniyle veri sorumlusunun sorumluluk bilinci yetersiz kaldığından bahsi geçen tedbirlerin alınmaması sonucunda ihlallerin yaşanması kaçınılmazdır. Veri sorumlusunun gerçekten de Kanuna uyumlu hale gelmesi için bünyesinde bulunan herkesin veri koruma hukuku hakkında yeterli bilinç seviyesine ulaşması gerekmektedir. Kişisel verilerin korunması hakkı merkezli olarak alınacak eğitim ile farkındalık oluşacak ve sorumluluklar öğrenilecektir. Eğitimin kapsamı kişisel verilerin korunmasına ilişkin bilgilendirme ve bilinçlendirmeyi, veri sorumlusu için oluşturulan ya da oluşturulacak kurumsal dokümanların ve kuralların mahiyetini, kurumsal politikalara ve kurallara aykırı davranış halinde kurumsal ve kişisel bazda ortaya çıkabilecek sorun, yükümlülük ve yaptırımları kapsamalıdır.[461]

Veri güvenliği konsepti oluşturularak, kişisel verilerin korunmasına hizmet edecek nitelikteki idari ve teknik tedbirler ile bu tedbirlerin muhtemel sonuçlarının tespit edilmesi; ardından bu konseptin gerçekten işleyip işlemediğinin ve ne kadar işlevsel

[461] Dülger, *Kişisel Verilerin Korunması*, 842.

olduğunun test edilmesi gerekmektedir. Bu amaca hizmet etmek için yapılacak olan ve yukarıda "risk etki değerlendirmesi" başlığı altında incelendiği şekilde risk analizi çerçevesinde sistematik risk kaynakları belirlenecek ve akabinde korunması teminat altına alınan haklar açısından tehlikeli olan risk kaynaklarına karşı nasıl tedbir alınması gerektiği konusu değerlendirilecektir.[462] Bu analiz, tüm risk kaynaklarını esas alan genel bir hukuka uygunluk analizi olmayıp, kişisel verilerin işlenmesini konu edinen süreç ile ilgili ve sınırlıdır.[463] Bu analizin yapılabilmesi için de öncelikle kişisel veri envanteri hazırlanmalıdır. Kişisel veri envanteri;[464] "*veri sorumlusu bünyesinde işlenen kişisel verilerin kategorilerini, veri işleme amaçlarını, alıcı gruplarını, saklama sürelerini, veri konusu kişi grubunu, yabancı ülkeye aktarımını, veri güvenliği tedbirlerini gösteren"* envanterdir. Envanterde bulunması gereken hususlar asgari olarak tanımlanmış olup veri sorumlusunun ihtiyacı doğrultusunda farklı başlıklar da buraya eklenebilecektir. Doğru şekilde oluşturulan envanter neticesinde veri sorumlusu bünyesinde bulunan kişisel verilerin korunması sürecine ilişkin doğru risk analizi yapılabilecek, kurumsal dokümanlar işlevsel şekilde hazırlanabilecek, alınması gereken doğru veri güvenliği tedbirleri net bir şekilde belirlenebilecektir. Yine yukarıda bahsi geçen "etki değerlendirme" yöntemleri kullanılarak sürecin sağlıklı bir şekilde yürütülmesi de mümkün olabilecektir.

Veri sorumlusunun kişisel veri işleme süreçlerini açıkça ortaya çıkaran veri koruma politikaları oluşturması gereklidir. Kişisel veri işleme ve koruma politikası, özel nitelikli kişisel verilerin korunması politikası, veri saklama ve imha politikası, olay yönetim politikası, kişisel veri aktarım politikası, talep ve veri ihlali yönetim prosedürü, disiplin politikası, gizlilik ve güvenlik politikası, çerez politikası gibi veri sorumlusunun faaliyet alanına uygun kurumsal dokümanları hazırlaması gerekmektedir. Bahsi geçen kurumsal politika ve prosedürler veri sorumlusu bünyesinde gerçekleşen kişisel veri işleme süreçlerinin Kanun doğrultusunda yürütülmesini sağlamak ve bu şekilde yürütüldüğünü gösterebilmek açısından zorunludur. İlke kararlarında da görüleceği üzere veri işleme süreçlerine ilişkin kurumsal politika ve prosedürlerin oluşturulmaması yahut

462 Aynı yönde bkz.: Yalçın, "Avrupa Birliği Genel", 757- 758.
463 Çekin, *Avrupa Birliği Hukukuyla,* 147.
464 Kişisel veri envanterinin tanımı Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'te ve Veri Sorumluları Sicili Yönetmeliği'nde yapılmıştır.

oluşturulmuşsa bile Kanuna uygun şekilde oluşturulmaması veri ihlallerine sebep olmaktadır.

3.4.2.2.2. Teknik Tedbirler

Kişilerin özgürlük alanları ile ters orantılı biçimde ilerleme gösteren teknolojik gelişmeler nedeniyle kişilerin temel hak ve hürriyetlerine dair tehdit ve tehlikeler artmaktadır.[465] 2023 yılı itibariyle 9 milyar verinin siber saldırıya uğraması ve saldırıların küresel ekonomiye faturasının 8 trilyon dolar[466] olduğu göz önüne alındığında durumun vahameti ortaya çıkmaktadır. İşte bu tehdit ve tehlikelerden en önemlisi siber suçlar olup siber saldırıların önüne geçilebilmesi açısından teknik tedbirlerin alınması büyük önem arz etmektedir.[467]

Siber suç kavramı tek ve kesin bir tanıma sığmayan oldukça geniş bir kategorideki suç eylemlerini ve davranışlarını ifade eden çatı terimdir. Genel olarak ifade etmek gerekirse siber suç, kanun dışı eylemlerde bulunmak için örgütsel ağlar ve genel ağ gibi bilgi sistemleri aracılığı ile bilgisayar veya diğer elektronik araçların kullanılması olarak ifade edilmektedir.[468] Siber tehdit de siber suç tanımı ile bağlantılı olarak "bilgi güvenliğine zarar verme ihtimali olan tüm faaliyetler" olarak tanımlanabilecektir.[469] Siber tehditlere karşı verilerin, bilginin ve bilginin temel özellikleri olan "gizliliğinin", "bütünlüğünün" ve "kullanılabilirliğinin" korunması öncelik teşkil etmektedir. "CIA Üçgen Modeli" olarak da bilinen bu yaklaşımda *gizlilik*, kişisel mahremiyeti ve özel bilgileri koruma yolları dahil olmak üzere bilgiye erişim ve ifşaya ilişkin yetkili kısıtlamaların korunmasını; *bütünlük*, depolama, işleme ve aktarım sürecinde verilerin yetkisiz bir

---

465 Gündüz, *Uluslararası İnsan Hakları,* 57.

466 Şehriban Kıraç, "Türkiye'deki genel siber tehditlerin sayısı 2023 yılında 2022'ye kıyasla yüzde 5 arttı", *Cumhuriyet,* 09.03.2024. https://www.cumhuriyet.com.tr/bilim-teknoloji/turkiyedeki-genel-siber-tehditlerin-sayisi-2023-yilinda-2022ye-2183667

467 Bahri Öztürk ve Serkan Seyhan ve Elif Altınok Çalışkan, *Kişisel Verilerin Korunması Hukuku Teorik ve Pratik Çalışma Kitabı*, (Ankara: Seçkin Yayıncılık, 2022), 104.

468 Aktaran Alper Bilgiç, "Siber Suç (Cybercrime)", içinde *Siber Ansiklopedi: Siber Ortama Çok Disiplinli Bir Yaklaşım*, ed. Naci Akdemir ve Can Ozan Tuncer, (Ankara: Pegem Akademi, Ağustos 2021), 487.

469 Ali Gök, "Siber Tehdit (Cyber Threat), içinde *Siber Ansiklopedi: Siber Ortama Çok Disiplinli Bir Yaklaşım*, ed. Naci Akdemir ve Can Ozan Tuncer, (Ankara: Pegem Akademi, Ağustos 2021), 498.

şekilde değiştirilmesinin önüne geçilmesini; *kullanılabilirlik* ise bilgiye zamanında ve güvenli bir biçimde erişimi ifade etmektedir.[470]

Siber güvenliğin en önemli unsurlarından biri olan veri güvenliği, elektronik, dijital ve iletişim sistemlerindeki verinin yetkisiz ifşa ve değişikliklerden korunması yöntemleridir. Kavramsal olarak siber güvenlik, veri güvenliğini barındırmaktadır.[471] Bu aşamada veri güvenliğinin sağlanması ve kişisel veri ihlallerinin önlenmesi veya en aza indirgenmesi sadece veri güvenliği risklerinin ortadan kaldırılması ile mümkün olmaktadır.[472] Teknik açıdan kişisel veri güvenliği risklerinin engellenmesi veya en düşük seviyeye getirilebilmesi için Kişisel Veri Güvenliği Rehberi'nde belirtilen tedbirlerin alınması gerekmektedir.

470 Aktaran Gök, "Siber Tehdit (Cyber Threat)", 500.
471 Korucu, *Veri güvenliğinin İyileştirilmesinde*, 39.
472 Korucu, *Veri güvenliğinin İyileştirilmesinde*, 122.

Tablo 3.4. Teknik Tedbirler[473]

Teknik Tedbirler ve Siber Güvenlik Unsurları	Açıklama
Erişim Kontrolleri ve Siber Güvenlik	
- *Yetki Matrisi*	Veri erişim yetkilerini tanımlar ve sınırlar.
- *Yetki Kontrol*	Veriye erişim kontrolünü sağlar ve yetkilendirme işlemlerini yönetir.
- *Erişim Logları*	Kullanıcıların veri erişim aktivitelerini kaydeder ve izler.
- *Kullanıcı Hesap Yönetimi*	Kullanıcı hesaplarını oluşturur, günceller ve erişimi yönetir.
- *Ağ Güvenliği*	Ağ trafiğini izler, güvenlik duvarları ve güvenli ağ yapıları kurar.
- *Uygulama Güvenliği*	Uygulama güvenliği önlemleri uygular ve yazılım güvenliği sağlar.
Veri Güvenliği ve Yönetimi	
- *Şifreleme*	Verileri şifreleyerek gizliliği ve bütünlüğü korur.
- *Sızma Testi*	Güvenlik açıklarını tespit etmek için aktif sızma testleri gerçekleştirir.
- *Saldırı Tespit ve Önleme Sistemleri*	Saldırıları algılar ve önler.
- *Log Kayıtları*	İlgili olayların log kayıtlarını tutar ve analiz eder.
- *Veri Maskeleme*	Hassas verileri gizler veya değiştirir.
- *Veri Kaybı Önleme Yazılımları*	Veri kaybını izler ve önler.
Altyapı ve Yedekleme	
- *Yedekleme*	Verilerin düzenli yedeklemesini yapar ve kurtarma süreçlerini oluşturur.
- *Ağ Altyapısı Güvenliği*	Ağ altyapısının güvenliğini sağlar.
- *Veri Depolama ve Yedekleme*	Kişisel verilerin güvenli bir şekilde saklanmasını ve yedeklenmesini yönetir.
Bilgi Teknolojileri Tedariği ve Bakımı	
- *Sistem Tedarik ve Geliştirme*	Bilgi teknolojileri sistemlerinin temin edilmesi, geliştirilmesi ve bakımı.
Siber Güvenlik Yönetimi ve Takibi	
- *Siber Güvenlik Politikaları*	Siber güvenlik politikalarının oluşturulması ve uygulanması.
- *Kişisel Veri Güvenliği Takibi*	Kişisel veri işleme faaliyetlerinin güvenli bir şekilde takip edilmesi.
- *Ortam Güvenliği*	Kişisel veri içeren ortamların fiziksel güvenliğinin sağlanması.

İlke kararı alınmasına neden olan yukarıda sınıflandırılmış halde belirtilen haller olan "*kişisel verilerin hukuka aykırı olarak işlenmesi (md.12), kişisel verilere hukuka aykırı erişilmesi (md 12) kişisel verilerin muhafazasını sağlanmaması (md. 12), kişisel verilerin hukuka aykırı olarak aktarılması, kişisel verilerin hukuka aykırı şekilde elde edilmesi, kişisel verilerin elde edildiği kaynağın belirsiz olması*" olaylarında veri güvenliğinin

[473] Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler) esas alınarak hazırlanmıştır.

sağlanmasına ilişkin idari tedbirler eksikliği gibi teknik tedbirlerin eksikliği de söz konusudur. Bu doğrultuda öncelikle:

1. Yetki matrisi ve yetki kontrol gibi erişim kontrolleri, uygulama güvenliği gibi siber güvenlik önlemlerinin alınmaması,

2. Veri güvenliği yönetiminin ve risk analizlerinin yapılmaması,

3. Siber güvenlik politikaları ve ortam güvenliği gibi siber güvenlik yönetimi ve takibinin yapılmadığı anlaşılmaktadır.

İçerisinde bulunduğumuz dijital çağda mahremiyetin ve veri güvenliğinin sağlanması adına alınması gereken teknik önlemlerin önemi en üst seviyeye çıkmıştır. Zira gelişen dijital teknolojiler sebebiyle hem kişisel verilerin toplanma ve çeşitli şekillerde işlenme kapsam ve niteliklerinde reform boyutunda farklılıklar meydana gelmiş, hem internet kullanımının artması sonucu sınırlar arası veri trafiği sıklaşmış, hem de özellikle bulut teknolojiler, veri madenciliği, Büyük Veri (Big Data), yapay zeka gibi teknik ve uygulamaların yoğun kullanımı nedeniyle, bireylerin kişisel verileri üzerindeki kontrolleri giderek zayıflayarak, bu verilerin yetkisiz üçüncü kişilerce işlenme oranları artmıştır.[474] Zira internet üzerinde bırakılan her iz, kişisel bilgilere farkında olunmadan üçüncü kişilerin yetkisiz erişimine olanak tanımaktadır.[475] Bu nedenle dijital olarak tutulan verinin korunabilmesi ve/veya sanal ortamda gerçekleşebilecek "*program manipülasyonu, sahtekârlık ve taklit, erişim araçlarının çalınması, kimlik çalma, ticari bilgi çalma, istihbarat amaçlı faaliyetler, takip ve gözetleme, hackleme, virüsler, solucanlar (worms), truva atları (slammer, msblaster, sobig vb.), ajan yazılım (spyware), spam, hizmeti durduran saldırılar ve tehditlere*"[476] karşı teknik tedbirlerin alınması zaruridir.[477]

---

474 Çimen Bulut, "Avrupa Birliği Genel", 138.

475 Özel Sebetçi, Aslıhan Topal, Mehmet Can Hanaylı ve Gizem Gürel Dönük, "Dijital Ortamda Kişisel Veri Güvenliği ve Sosyal Medya Reklamcılığı Üzerine Bir Değerlendirme", *Kesit Akademi Dergisi*, 4/ 16 (2018), 389-409, 393.

476 Yılmaz, "TS ISO/IEC 27001 Bilgi Güvenliği", 48.

477 Siber güvenliğin sağlanması için alınması gereken tedbirlere ilişkin detaylı açıklamalar için bkz: Türkiye Bilişim Derneği, *Veri Uzayı Raporu*, (Ankara: Türkiye Bilişim Derneği, Kasım 2023), (E.T. 15.03.2024) https://www.tbd.org.tr/pdf/kamubib-calisma-grubu/veri-uzayi-calisma-grubu-raporu-2023.pdf

Kişisel verilerin siber saldırılara karşı korunabilmesi için öncelikle bu yönde bir politika oluşturulmalıdır. Teknoloji okuryazarlığının artırılması sağlanarak bireyin mahremiyete yönelik bilinçlendirme ve bilgilendirmesi sağlanmalı;[478] akabinde asgari olarak masaüstü sistem güvenliği, zararlı yazılım güvenliği, kişisel güvenlik duvarı gibi önlemleri içeren prosedürler belirlenerek sistemlere uygulanmalıdır. Yetkisiz erişimlere engel olmak açısından gerek fiziken azami gizliliği sağlayacak gerekse elektronik ortamda bulunan ve "*Gizlilik: Bilgi ya da kaynakların gizlenmesi; Orijinallik: Bilginin kaynağından emin olmak; Güvenilirlik: Veri ya da kaynağın uygunsuz ya da yetkisizce değiştirilmediğinden emin olmak; Kullanılabilirlik: istenildiği zaman veri ve kaynakların ulaşılabilir durumda olması*" prensiplerini içeren erişim güvenliğini sağlayamaya yönelik uygulamalar hayata geçirilmelidir.[479] Bu kapsamda iç tehditlere daha büyük önem verilmelidir. Zira yapılan araştırmalar,[480] bilişim sistemlerine yönelik en büyük tehdidin iç tehditler olduğunu ve bilişim sistemlerinin yüzde 68'inin iç tehditlere karşı daha zayıf olduğunu göstermektedir.[481] Veri sorumlusu bünyesi içinde işlenen kişisel verilerin korunması kontrolünün sağlanması için veri sorumlusu ile birlikte bilgi güvenliği yetkilisinin de belli olması önemli olduğundan bilgi güvenliği politikaları içinde bu yetkinin verileceği kişi tanımlanarak sorumluluk paylaşımı daha belirgin hale getirilmelidir. Bu sayede hiyerarşik yapı içinde sorumluluk alması gereken idari yöneticilerin de sorumluluğunun açıklanması imkânı elde edilecektir.[482]

3.4.2.2.3. Özel Nitelikli Kişisel Verilerin İşlenmesinde Alınması Gereken Tedbirler

Özel nitelikli verilerin genel nitelikteki verilerden daha ayrı bir korumaya sahip olması gerektiği daha önce ifade edilmişti. KVKK'nın 6/4. maddesinde "*Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır*." hükmü bulunmaktadır.

---

478 Yılmaz, "TS ISO/IEC 27001 Bilgi Güvenliği", 48.

479 Önder Şahinaslan, Ender Şahinaslan, Emin Borandağ ve A.Mutalip Sahinaslan, "Güvenli Bir Toplum İçin Son Kullanıcı Siber Güvenliği", Akademik Bilişim 2013 – XV. Akademik Bilişim Konferansı Bildirileri 23-25 Ocak 2013 – Akdeniz Üniversitesi, Antalya, (E.T.21.10.2023), https://ab.org.tr/ab13/kitap/eski/49.pdf

480 Son yıllarda yaşanan siber güvenlik vakalarına ilişkin detaylı istatistikler için bkz: Nevzat Güngör, *İç Denetimde Bilgi Teknolojileri ve Siber Güvenlik*, (Ankara: Gazi Kitabevi, Aralık 2021), 116-118.

481 Henkoğlu, "Kişisel Verileriniz Ne Kadar", 53-54.

482 Henkoğlu, "Kişisel Verileriniz Ne Kadar", 52-53.

Bu kapsamda, “Rehber”de belirtilen uygun güvenlik düzeyini temin etmeye yönelik teknik ve idari tedbirlerin yanı sıra Kanunun 22/1 hükmünün (ç) ve (e) bentleri doğrultusunda özel nitelikli kişisel veri işleyen veri sorumluları tarafından alınması gereken yeterli tedbirler Kişisel Verileri Koruma Kurulu tarafından aşağıdaki şekilde belirlenmiştir:[483]

[483] "Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" ile ilgili Kişisel Verileri Koruma Kurulunun 31/01/2018 Tarihli ve 2018/10 Sayılı Kararı, Kişisel Verileri Koruma Kurumu, (E.T. 17.09.2023), https://www.kvkk.gov.tr/Icerik/4110/2018-10

Tablo 3.5. Özel Nitelikli Kişisel Verilerin İşlenmesinde Alınması Gereken Tedbirler[484]

Özel Nitelikli Kişisel Verilerin Güvenliği ve İşlenmesi Tedbirleri	Açıklama
Politika ve Prosedürler	
- *Politika ve Prosedür Belirleme*	Özel nitelikli kişisel verilerin güvenliği için ayrı politika ve prosedürlerin belirlenmesi.
- *Eğitimler*	Çalışanlara düzenli olarak kanun ve özel nitelikli kişisel veri güvenliği eğitimleri verilmesi.
- *Gizlilik Sözleşmeleri*	Çalışanlar arasında gizlilik sözleşmelerinin imzalanması.
- *Yetkilendirme ve Kontrol*	Verilere erişim yetkilerinin net olarak tanımlanması ve periyodik yetki kontrollerinin yapılması.
- *Görev Değişiklikleri ve Ayrılma İşlemleri*	Çalışanların görev değişikliklerinde veya işten ayrıldıklarında erişim yetkilerinin kaldırılması ve envanterin iade alınması.
Elektronik Ortam Güvenliği	
- *Kriptografik Muhafaza*	Verilerin kriptografik yöntemlerle güvenli bir şekilde muhafaza edilmesi.
- *Kriptografik Anahtar Yönetimi*	Kriptografik anahtarların güvenli ve ayrı ortamlarda saklanması.
- *Log Kayıtları*	Tüm veri işleme aktivitelerinin güvenli olarak loglanması.
- *Güvenlik Güncellemeleri ve Testler*	Güvenlik güncellemelerinin sürekli takip edilmesi, güvenlik testlerinin düzenli olarak yapılması ve sonuçların kayıt altına alınması.
- *Yazılım Yetkilendirme ve Güvenlik Testleri*	Verilere erişim için kullanılan yazılımların yetkilendirilmesi ve güvenlik testlerinin yapılması.
- *Uzaktan Erişim Güvenliği*	Uzaktan erişim gerekiyorsa en az iki kademeli kimlik doğrulama sisteminin kullanılması.
Fiziksel Ortam Güvenliği	
- *Ortam Güvenliği*	Verilerin fiziksel ortamının güvenliği, yangın, su baskını ve hırsızlığa karşı önlemler alınması.
- *Yetkisiz Erişim Engellemesi*	Fiziksel ortamın yetkisiz giriş çıkışlara karşı korunması.
Veri Aktarımı	
- *Şifreli E-posta veya KEP*	Verilerin e-posta yoluyla aktarılması gerekiyorsa şifreli olarak gönderilmesi.
- *Taşınabilir Ortamlar*	Verilerin taşınabilir ortamlarla aktarılması gerekiyorsa kriptografik yöntemlerle şifrelenmesi ve güvenli saklama.
- *Farklı Sunucular Arası Aktarım*	Verilerin farklı sunucular arasında VPN veya sFTP ile güvenli bir şekilde aktarılması.
- *Kağıt Ortamı Aktarımı*	Verilerin kağıt ortamında aktarılması durumunda gizlilik dereceli belgeler formatında gönderilmesi ve gerekli fiziksel güvenlik önlemlerinin alınması.

[484] Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler) esas alınarak hazırlanmıştır.

İlke kararlarında özel nitelikli kişisel verilerle alakalı spesifik bir durum söz konusu olmasa da veri güvenliği ihlallerinin önüne geçilmesi için özel nitelikli kişisel verilerin işlenme süreçlerinde de belirtilen tedbirlere azami düzeyde uyulması gerekmektedir.

3.4.2.2.4. Veri Güvenliği Tedbirlerine İlişkin Değerlendirmeler

Kişisel veri işleyen veri sorumlusu; veri işleme, aktarma, saklama, imha etme gibi tüm veri işleme süreçlerinde veri güvenliğini sağlamakla yükümlüdür. Yukarıdaki başlıklarda da ifade edildiği üzere her bir veri sorumlusu tarafından iştigal ettiği faaliyet alanı, veri işleme yoğunluğu, temas ettiği gerçek kişi sayısı, yurtdışına veri aktarımı yapılıp yapılmadığı gibi birçok değişken göz önünde bulundurularak veri güvenliğini sağlamak için asgari düzeyde idari ve teknik tedbirin alınması zorunludur. Bu husus veri ihlallerinin önüne geçilmesi açısından en önemli yükümlülüktür.

Veri sorumlularının, veri güvenliğinin sağlanması hususunda yerine getirmesi gereken yükümlülüklerden biri de denetim sorumluluğudur. KVKK'nın 12/3. maddesine göre veri sorumlusu, kendi kurumunda ya da kuruluşunda bu kanunun hükümlerini uygulamaya yönelik gereken denetimleri yapmak ya da yaptırmakla sorumludur. Bu bağlamda, bağımsız denetim kurumları oluşturulabilir, bu kurumlar tarafından veri sorumlularının KVKK'ya uyum ve kişisel verileri işleme süreçlerinin denetlenmesi sağlanabilir. Bu denetimler sonucunda uygunluk sertifikası almayı başaran veri sorumluları ve veri işleyenlere, gerekli yetkinliklerini kanıtlayan bir sertifika verilebilir. Bu yaklaşım, GDPR md. 81'de bahsedilen, veri işleyenin belirlenmiş bir davranış kurallarına (etik ilkeler) veya onaylanmış bir sertifikasyon mekanizmasına bağlılığının, veri sorumlusunun yükümlülüklerini yerine getirmesini göstermek için bir ölçüt olarak kullanılabileceğine atıfta bulunarak desteklenmektedir.[485]

3.5. Hesap Verebilme Zorunluluğu

Değişen veri koruma ve mahremiyet düzlemleri, çeşitli faktörlerin etkisiyle yeni riskler ve sorunlar ortaya çıkarmıştır. Bunlar arasında siber risklerin özelliği, analitik ve yapay zekâ uygulamaları nedeniyle kişisel verilerin işlenmesinde artış yaşanması, pek çok veri işleme ve saklama ortamının ortaya çıkması, sektörel düzenlemelerin yaygınlaşması gibi

485 Çelikel, *Kişisel Verilerin Korunması,* 112.

konular yer almaktadır. Bu değişimler, mevcut veri koruma yaklaşımlarının yetersiz kaldığını ortaya çıkarmıştır. Bu bağlamda, "hesap verebilirlik"[486] ilkesi, etkin bir çözüm olarak ortaya çıkmıştır. Hesap verebilirlik ilkesi, sadece mevzuata uyum sağlamaktan daha fazlasını gerektiren bir paradigma değişikliğini temsil etmektedir. Bu prensip, veri sorumlularının veri koruma düzenlemelerine uyum sağlamak için gerekli ve etkili önlemleri almasını ve bunları gerektiğinde kanıtlamasını zorunlu kılar. Yani hesap verebilirlik ilkesi, kişisel verilerin korunmasıyla ilgili sürekli bir denetimin olduğunu, denetimin etkili bir şekilde uygulandığını ve düzenli olarak kontrol edildiğini ispatlamayı ifade eder. Bu ilke, yeni ortaya çıkan riskler ve sorunlar karşısında daha güçlü bir veri koruma ve mahremiyet çerçevesi oluşturmayı amaçlamaktadır.[487] İlke aynı zamanda ilgili kişilerin kişisel verilerinin en üst düzeyde korunmasını sağlayan bir ilkedir ki kişisel verilerin işlenmesi sürecinde sorumluluk sistemini oluşturur.[488]

Hesap verebilirlik, "uyumun temel bir ilkesi" olarak nitelendirilmekte ve "yükselen teknolojiler ve işletme modelleri tarafından ortaya çıkarılan uyum zorluklarıyla başa çıkmak için bir araç" olarak ifade edilmektedir.[489] Hesap verebilirlik kavramı ilk kez 1980'de OECD Rehberlerinde temel bir veri koruma ilkesi olarak ortaya çıkmış;[490] hesap verebilirlik ilkesi uluslararası metinlerde farklı bağlamlarda ele alınmıştır. Uluslararası Standardizasyon Kurumu (International Organization for Standardization- ISO) tarafından ve Uluslararası Elektroteknik Komisyonu'nun (International Electrotechnical Commission- IEC) iş birliği ile düzenlenen "Bilgi Teknolojileri- Güvenlik Teknikleri- Gizlilik Çerçevesi" ISO/IEC 29100 Standardı" ("ISO 29100") hesap verebilirlik ilkesinin

---

486 Hesap verebilir olmak, kişinin "hesap verebilir olarak hazır" olması anlamı taşır; fakat hesap verdiği veya vereceği anlamı taşımaz. "Hesap verirlik" ise kendi içinde hesap verebilir olmayı içerdiği gibi, mutlak surette hesap verileceği ve hesap verme faaliyetinin bir düzene bağlanmış olduğunu da ifade eder. "Hesap verirlik" terimi hesap verme işleminin geçmişte gerçekleşmiş ve ilerde de gerçekleşecek olduğuna dair bir belirlilik içerir. En önemlisi de keyfilik veya kişisellik içermez. Hesap anlamındaki "*account*" terimi ile bir şeye yapmaya yeterlilik veya yetkinlik anlamındaki "*ability*" kelimelerinden türetilen "*accountability*" kelimesinin de "hesap verilebilirlik" olarak değil, "hesap verirlik" olarak tercümesi daha doğrudur. Zira hesap verilebilirlik hesap soranın ya da verenin kişisel hareketlerine bağlı olarak bir belirsizlik içermektedir. Ancak literatürde çoğunlukla "hesap verilebilirlik" olarak kullanılmaktadır. Bkz: Mehmet Gün, *Türkiye'nin Orta Demokrasi Sorunları ve Çözüm Yolu*, (İstanbul: Gün +, 2018 2. Baskı), 247.

487 Mehmet Bedii Kaya, "Kişisel Verilerin Korunmasında Yeni Paradigma: Hesap Verebilirlik İlkesi", *İstanbul Hukuk Mecmuası* 78/4 (2020): 1859-1897, 1859. (E.T. 02.07.2023), https://dergipark.org.tr/tr/download/ article-file/1573623

488 Kaya, "Kişisel Verilerin Korunmasında", 1882.

489 Demetzou, "Data Protection Impact Assesment", 4.

490 Demetzou, "Data Protection Impact Assesment", 3.

gerekliliklerinin icra edilmesi adına dokuz kriter belirlemiştir. Bahsi geçen kriterler şu şekildedir:[491]

"(1) Mahremiyetle ilgili tüm politikaların, prosedürlerin, uygulamaların belgelenmesi ve yayınlanması,

(2) Organizasyonda belirli bir kişiye (uygun olduğu ölçüde organizasyon dışında başkalarına da devredilebilir) mahremiyetle ilgili politikaların, prosedürlerin ve uygulamaların icra edilmesi görevinin verilmesi,

(3) Kişisel bilgiyi üçüncü kişilere aktarırken sözleşmeler veya zorunlu iç politikalar gibi diğer yöntemler aracılığıyla alıcı üçüncü kişinin aynı ölçüde mahremiyet korumasını sağlayacağını temin etme (uygulanabilir mevzuat uluslararası veri transferlerine ilişkin ilave yükümlülükler içerebilir),

(4) Kişisel bilgiye erişecek veri sorumlusunun çalışanlarına uygun eğitimin verilmesi,

(5) Etkin bir iç şikâyet yönetim ve tazmin prosedürü oluşturulması,

(6) Esaslı zarara yol açabilecek mahremiyet ihlalleri ve çözüm için alınan tedbirler hakkında ilgilileri bilgilendirme (meğer ki yasaklanmış olsun, örneğin soruşturma süreçlerinde),

(7) Bazı hukuki rejimlerde zorunlu olduğu üzere ve ilgili riskin seviyesine bağlı olarak ilgili tüm mahremiyet paydaşlarına (örneğin, veri koruma otoriteleri) mahremiyet ihlallerine ilişkin bildirim yapma,

(8) Şikâyet eden kişisel veri ilgililerinin uygun ve etkin yaptırımlara sahip olmasına ve/veya mahremiyet ihlali ortaya çıkmışsa düzeltme, silme eski hale iade gibi tazmin yollarına erişmesine izin verme,

(9) Gerçek kişinin mahremiyetini ihlal olmadan önceki döneme getirmek zor veya imkansızsa bu tür durumlara yönelik tazminat prosedürlerini geliştirme".

Gözetim faaliyetleri insan hakları açısından değerlendirildiğinde, hesap verilemezlik ve zararsız bir amaç için toplanan bilgilerin farklı bir amaç için kullanılması sonucu doğabilir. Kullanıcıların yetkilerini aştığı veya kötüye kullandığı durumlarda kimin neye eriştiği, hangi verileri değiştirdiği, düzeltmesi gereken bilgileri güncellemediği

[491] Kaya, "Kişisel Verilerin Korunmasında", 1876, 1877.

konusunda hesap verebilirlik son derece önemlidir. Büyük gözetim veri tabanları, çok sayıda "güvenilir kullanıcı"ya başka bir ifade ile sisteme tam erişime sahip olan ve denetim kayıtlarını değiştirebilen, bu sayede kayıtlardaki izlerini silebilen kullanıcılara izin verir. Veri tabanı kullanımı sıkı bir şekilde izlenmeli, kullanıcılarının ve eylemlerinin bir kaydı korunmalı ve kötüye kullanımı önlemek için kayıt altına alınmalıdır.[492]

Veri sorumlusu, GDPR'de düzenlenen kriterlere uygun davranmakla mükellef olmakla birlikte bu hususu ispatla yükümlüdür. Bu amaçla veri sorumlusu, uygun idari ve teknik önlemleri almalıdır. GDPR'ın lafzında veri sorumlusunun hesap verebilirliğinden bahsedilmiş olsa da birtakım sorumluluklar altında olan veri işleyenin de bu kriterlere uygun davrandığına dair hesap verebilir vaziyette olması gereklidir. Bu çerçevede izlenmesi gereken prosedürler ve oluşturulacak sistemler, veri işlemenin meydana getirdiği risk ve verinin niteliğine göre farklılık gösterecektir. Bu ilkeye uygun davranışa örnek vermek gerekirse veri sorumluları ve veri işleyenler işleme faaliyetleri ile ilgili kayıt tutabilir ve gerekirse bu kayıtları denetim makamına sunabilir, belli durumlarda kişisel verilerin korunması ile alakalı hususlarda görev yapacak bir veri koruma görevlisi atanabilir, bir işleme türünün gerçek kişilerin hakları ve hürriyetleri bakımından yüksek bir riske neden olmasının ihtimal dahilinde olduğu durumlarda, işleme faaliyetine başlamadan evvel veri koruma etki değerlendirmesi yapabilir, özel ve olağan durumlarda veri korunmasını sağlayabilir, veri sahiplerinin haklarını kullanabilmesi adına usul ve prosedürler uygulayabilir, onaylanmış davranış kuralları veya sertifikasyon mekanizmalarına bağlı kalabilir. Madde 29 Çalışma Grubu tarafından hesap verme zorunluluğu; veri sorumlusunun, işleme faaliyetleri kapsamında ve olağan koşullarda veri koruma kurallarına uygunluk sağlayacak önlemler alması ve veri koruma kurallarına uygun davranıldığını veri sahipleri ve denetim makamlarına sunması gereken belgeleri hazır bulundurması sorumluluğu şeklinde özetlemiştir.[493] Hesap verebilirlik mekanizmalarının hukuki yapısı iki kademeden oluşmaktadır. İlk basamakta tüm veri sorumluları için bağlayıcılığı bulunan temel kanuni sorumlulukları barındırırken, ikinci

492 Hiranandani, "Privacy and Security", 1098.
493 Dülger, "Avrupa Birliği Genel Veri", 106,107.

basamakta kanunda düzenlenen öngörülen asgari seviyenin üzerinde, gönüllülük esasına dayanan hesap verebilirlik sistemleri vardır.[494]

3.6. Kişisel Verileri Koruma Kurulunun İlke Kararlarının Veri Koruma Hukuku Gelişimine Katkısı

3.6.1. Kişisel Verileri Koruma Kurumu Bağlamında Değerlendirmeler

Kişisel Verileri Koruma Kurumunun misyonu "*Anayasa da öngörülen özel hayatın gizliliği ile temel hak ve özgürlüklerin korunması kapsamında, ülkemizde kişisel verilerin korunmasını sağlamak ve buna yönelik farkındalık oluşturarak bilinç düzeyini geliştirmek, aynı zamanda veri temelli ekonomide özel ve kamusal aktörlerin uluslararası rekabet kapasitelerini artırıcı bir ortam oluşturmak*" şeklinde ifade edilmiş; vizyonu ise "*Kişisel verilerin korunmasında etkin, buna ilişkin kültürün oluşturulmasında öncü, uygulamaları ile uluslararası alanda söz sahibi bir kurum olmak*" olarak belirlenmiştir. Kurumun, temel değerleri ve çalışma ilkeleri ise *"kişisel verilerin güvenliği ve gizliliğini gözeten, suistimali önleyen düzenlemeleri belirlemek ve uygulamak*" olarak ifade edilmiştir.[495]

6698 sayılı Kişisel Verilerin Korunması Kanunu, Türk hukukunda kişisel verilerin korunması yönünde düzenlemeleri içermektedir. Kanun'un 4. maddesinde belirtilen genel veri koruma ilkelerine uygun olarak kişisel verilerin işlenmesi gerekmektedir. Bu ilkeler, "hukuka ve dürüstlük kurallarına uygun olma, doğru ve güncel olma, belirli, açık ve meşru amaçlar için işlenme, amaçla bağlantılı, sınırlı ve ölçülü olma ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme" şeklinde sıralanmıştır. Hal böyle olsa da hesap verebilirlik ilkesi ve veri koruma etki değerlendirmesi ve benzeri hesap verebilirlik ilkesini destekleyen uyum araçları Kanunda düzenlenmemiştir. Kişisel Verileri Koruma Kurumu, Kanunda herhangi bir düzenleme olmaksızın, uygulamalarında[496] şeffaflık ve hesap verebilirlik ilkesine önem vermektedir.

---

494 Yalçın, ""Avrupa Birliği Genel", 753.

495 KVKK 2022 Faaliyet Raporu, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/aae3c721-9da4-43c7-95a6-8d14e6413a36.pdf E.T. 22.06.2023

496 KVK Kurulunun "Veri sorumlusunun kanuni yükümlülüğünü yerine getirmek için işlediği kişisel verileri meşru menfaat çerçevesinde kullanma talebiyle Kuruma yapmış olduğu başvuru" ilke ilgili 25/03/2019 tarihli ve 2019/78 Sayılı Kararında "*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*

Kurum, hesap verebilirlik ilkesinin destekleyicisi olan uyum araçlarına ise doğrudan atıfta bulunmamaktadır. Ancak, yapay zekâ alanında kişisel veri işleme temelli çalışmalarda[497] yüksek risk öngörülen durumlarda mahremiyet etki değerlendirmesi yapılması ile veri işleme süreçlerinin hukuka uygunluğuna bu kapsamda karar verilmesi önerisi sunulmaktadır.[498]

Kurum'un uygulamalarında hesap verebilirlik ilkesi ve uyum araçları, Avrupa Birliği veri koruma hukukuyla doğru orantılı olacak biçimde yorumlanmaktadır. Ancak, hesap verebilirlik ilkesi ve ilgili yükümlülüklerin yasal olarak tanımlanması önemlidir. Bu nedenle, hesap verebilirlik ilkesi ve veri koruma etki değerlendirmesi gibi yapıların kanunda açıkça belirtilmesi gerekmektedir. Bu sayede hukuki güvenlik ve belirlilik ilkesi gözetilerek kişisel verilerin etkili bir şekilde korunması sağlanabilir.[499]

Kişisel Verileri Koruma Kurumu ile küresel bazdaki diğer kişisel verilerin korunması otoriteleri arasında küçük ölçekli bir karşılaştırma yapıldığında, Türk kurumunun kurumsal ve operasyonel yapılarının ve uygulamalarının yeni kurulmuş bir kurum olarak tatmin edici düzeyde olduğu görülebilir. Bununla birlikte, Kurumun daha etkili olabilmesi için bazı yeniliklere ihtiyaç duyulmaktadır.

İngiltere'nin kişisel verilerin bağımsız otoritesi olan Bilgi Komisyonu Ofisi (Information Commissioner's Office - ICO) faaliyetleri web sitesi üzerinden analiz edildiğinde, Kişisel Verileri Koruma Kurumunun faaliyetlerine nazaran farklılıklar olduğu görülmektedir. ICO, danışma ziyaretleri, veri koruma denetimleri, araştırmalar, izleme faaliyetleri gerçekleştirmiş ve genel bakış raporları, yıllık raporlar, parlamenterlere ve yasa yapıcılara yönelik politika görüşleri, araştırma yayınları gibi yayınlar yapmıştır. Karşılaştırmada ICO'nun KVKK'dan daha fazla faaliyeti ve uygulaması olduğu görülmektedir. Özellikle en önemli fark olarak görülen, ICO'nun daha bağımsız bir şekilde faaliyet göstermesi, KVKK'nın daha çok şikayetler üzerinden hareket etmesidir. Örneğin, ICO'nun 2017

---

personel nezdinde değil, kurumsal olarak geneli etkileyecek şekilde) gibi şeffaf ve hesap verilebilir nitelikleri haiz kriterlerin esas alınması" gerektiğine vurgu yapılmıştır. Karar metni için bkz: (E.T. 05.07.2023), https://www.kvkk.gov.tr/Icerik/5434/2019-78

497 "Yapay Zekâ Alanında Kişisel Verilerin Korunmasına Dair Tavsiyeler", (E.T. 05.07.2023), https://www.kvkk. gov.tr/Icerik/7048/Yapay-Zeka-Alaninda-Kisisel-Verilerin-Korunmasina-Dair-Tavsiyeler.

498 Bayram, "Bir Uyum Aracı Olarak", 48.

499 Bayram, "Bir Uyum Aracı Olarak", 49.

Nisan ve 2018 Mart arasında İngiltere'deki 16 üniversite üzerine yaptığı genel bakış raporunda, ICO tarafından gözlemler, takip araştırmaları, fiziksel ziyaretler ve telefon konferansları yapılmıştır.[500] Bu faaliyetler sonucunda iyi uygulama alanları, geliştirilmesi gereken alanlar ve detaylı olarak açıklanan ve metin içinde önerilerde bulunulan gelişim alanları belirlenmiştir. Ayrıca ICO, kamu kurumlarını ve özel kuruluşları izlemek suretiyle uygulamaları konusunda önerilerde bulunmaktadır. Sonuç olarak, karşılaştırmadan görüldüğü gibi, ICO'nun KVKK'ya kıyasla çok daha fazla başvuru ve şikâyet aldığı görülmektedir. Bu nedenle ICO daha güçlü bir uygulama yetkisine sahiptir. Örneğin, ICO, müşterilerin kişisel bilgilerini bir siber saldırı sırasında koruyamayan Uber'e 385.000 sterlinlik bir para cezası vermiştir[501] ve kullanıcıların kişisel bilgilerini koruyamadığı için Facebook'a 500.000 sterlinlik para cezası vermiştir.[502] Bu karşılaştırmadan anlaşıldığı üzere, ICO'nun daha geniş bir yaptırım gücü vardır ve daha aktif bir şekilde faaliyet göstermektedir. Türkiye'de ise Kurumun faaliyetleri ve uygulamaları ise hala gelişme aşamasındadır ve daha etkili olabilmesi için bazı iyileştirmeler gerekmektedir. Daha fazla bağımsızlık, danışmanlık ziyaretleri, denetimler, araştırmalar ve genel bakış raporları gibi daha kapsamlı faaliyetlerin yapılması, Türkiye'nin Kişisel Verileri Koruma Kurumu'nun etkinliğini artırmaya yardımcı olabilir. Ayrıca, şikayetlere daha hızlı ve etkili bir şekilde yanıt verilmesi ve uygulama alanında daha güçlü yaptırımların uygulanması da önemlidir. Bu şekilde, Türkiye'nin Kişisel Verileri Koruma Kurumu da uluslararası örneklerle daha yakın bir seviyede olabilir ve kişisel verilerin korunması hususunda daha güvenilir bir kurum haline gelebilir.[503]

Fransız Veri Koruma Otoritesi Hürriyetler ve Bilişim Ulusal Komisyonu (“Commission Nationale de l’Informatique et de Libertés”, “CNIL”), “kontrol etme ve yaptırım uygulama”, “bilgilendirme ve hakları koruma”, “görüş verme”, “tahmin etme ve yenileştirme” şeklinde dört başlık altında toplanabilen yetkilere sahiptir. Her ne kadar

---

500 ICO, “Findings from ICO information risk reviews of information security in the higher education sector”, (E.T. 25.11.2023), https://ico.org.uk/media/action-weve-taken/audits-and-advisory-visits/2614196/20190124 -information-risk-review-report-higher-education-sectorpdf.pdf.

501 ICO fines Uber £385,000 over data protection failings, Retrieved from https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/11/ico-fines-uber-385-000-over-data-protection-failings/ akt. Sevinç ve Karabulut, "A Revıew on the Personal”, 464-465.

502 ICO issues maximum £500,000 fine to Facebook for failing to protect users‟ personal information, Retrieved from https://ico.org.uk/about-the-ico/news-and-events/news-and-*İsmail Sevinç, Niyazi Karabulut* 470 blogs/2018/10/facebook-issued-with-maximum-500-000-fine/ akt. Sevinç ve Karabulut, "A Revıew on the Personal”, 464-465.

503 Sevinç ve Karabulut, "A Revıew on the Personal”, 464-465.

KVK Kurumu ile benzer nitelikte yetkilere sahip olduğu görülse de CNIL'in mahalde inceleme yapma yetkisi göze çarpmaktadır. Mahalde inceleme yapma yetkisine ilişkin olarak CNIL'in gündüz 06.00 ila gece 21.00 saatleri arasında görevleri yürütülmesi adına özel mülkte kontrol yetkisini kullanabileceği ilgili yasada hüküm altına alınmıştır. Ek olarak, CNIL denetimden en geç 24 saat önce Cumhuriyet Savcılığına bilgi vermekle mükelleftir.[504] Yine CNIL tarafından verilen idari para cezalarına bakıldığında ise cezaların 20 milyon Euro'ya kadar çıkılabildiği, fakat bahse konu özne bir şirket olursa şirketin dünya çapında senelik cirosunun %4'üne kadar para cezası verildiği görülmektedir.[505] Bu bağlamda Fransız otoritesinin daha etkin bir denetim yürütme eğilimde olduğu yorumu yapılabilir. Zira verilen cezaların oranlarına ve yöntemine bakıldığında veri sorumluları nezdinde caydırıcı bir etkisi olduğu söylenebilecektir. Örnek vermek gerekirse, Kurumun zamanında VERBİS kaydı yaptırmayan veri sorumlularına ilişkin bir etkili denetim yapmaması, Kurum tarafından verilen sürenin defalarca uzatılması, buna rağmen VERBİS kaydını yaptırmayan veri sorumlularına resen herhangi bir ceza verilmemesi veri sorumluları nezdinde caydırıcı bir husus olmaktan çıkmıştır. Uygulamaya bakıldığında pek çok veri sorumlusu VERBİS kaydı yapmadığında yasal yükümlülüklerden muaf olduğu gibi bir bilinçte olduğundan kişisel verilerin korunması noktasında ihmalkâr davranmaktadır. Bu husus da doğal olarak veri ihlallerinin önünü açmaktadır. Ülkemizdeki mevcut durumda VERBİS kaydı yapılmasına ilişkin yahut VERBİSE kayıt zorunluluğu olmasa dahi kanuni yükümlülüklerin yerine getirilmesi gerektiğine ilişkin zorunluluğa dair farkındalık oldukça azdır. Bu farkındalık eksikliğine ilişkin yapılacak düzenlemeler ve gerekirse CNIL örneğinde olduğu gibi mahalde yapılacak incelemelerle Kurum'un etkinliği artırılabilecektir. Bununla birlikte VERBİS kaydı yaptırma zorunluluğuna ilişkin çemberin genişletilmesinin, Kurumun veri ihlallerine ilişkin denetimini de kolaylaştırabilecek bir husus olduğu düşünülmektedir. Hesap verebilirlik ilkesi ile uyum içerisinde olan bu kayıt zorunluluğu, veri sorumlularının veri ihlallerine karşı veri güvenliğinin sağlanması için savunma içerisinde olduğunu göstermektedir. Bu noktada VERBİS kaydı yaptırması gereken organizasyonlara ilişkin çemberin genişletilmesi gerekirken yeterli ilerlemenin kaydedilmemesi denetim noktasında eksiklik oluşturmaktadır.

504 İnan, "Kişisel Verilerin Korunması", 60.
505 İnan, "Kişisel Verilerin Korunması", 60.

3.6.2. İlke Kararları Doğrultusunda Değerlendirmeler

Kişisel verilerin korunması, modern toplumların en önemli hukuki konularından biridir ve bu alandaki düzenlemeler sürekli olarak evrilmektedir. Kanunlar ve ilgili düzenlemeler, kişisel verilerin işlenmesi ve korunmasına dair genel çerçeveyi oluştururken, pratikte ortaya çıkan belirsizlikler ve yeni durumlarla başa çıkabilmek için ilke kararları büyük önem taşımakta, yaygın olarak yaşanan kişisel veri ihlalleri neticesinde alınan kararlar olması sebebiyle veri koruma hukukunun gelişiminde kritik bir rol oynamaktadır.

Kurulun ilke kararlarının veri koruma hukukuna vermiş olduğu en önemli katkılardan biri veri sorumlularına ve diğer ilgili taraflara rehberlik sağlamasıdır. Bu husus, veri sorumlularının ve kişisel veri sahiplerinin kişisel verilerin korunmasıyla ilgili mevzuata uygun hareket etmelerine yol gösterici olmakla birlikte kişisel verilerin korunmasıyla ilgili belirsizlikleri gidermeye ve yasal düzenlemelerin yorumlanmasına yardımcı olmaktadır. Böylece, veri sorumluları ve ilgililer için netlik sağlanarak hangi durumlarda hangi önlemlerin alınması gerektiği konusunda rehberlik sunulmaktadır. Bununla birlikte bir takım hukuki belirsizlikleri giderme ve uygulamada tutarlılık da sağlamaktadır. Yine kişisel verilerin korunması ile alakalı en iyi uygulamaların ve standartların gelişime katkıda bulunulmaktadır. Böylece ulusal standartlara uyum sağlanmakla birlikte uluslararası uyumu artırmaya yardımcı olmaktadır.

İlke kararlarının veri koruma hukuka önemli katkıları olsa da yaşanan veri ihlalleri göz önüne alındığında kararların yeterli olmadığı da görülmektedir. Şöyle ki ilke kararlarında belirtilen gerekli idari ve teknik tedbirlerin neler olduğu ve bunların nasıl uygulanacağına dair açık ve detaylı bilgiler verilmemesi aynı ihlallerin tekrarlanmasına sebebiyet verebilecektir. İlke kararlarının rehberlik görevi göz önüne alındığında kararların yeterince açık olmaması, veri sorumlularının kararların gerekliliklerini anlamasını ve uygulamasını güçleştirebilir. Bu nedenle Kurulun "belediyelerin ödeme ve borç sorgulama uygulamaları" ya da "banko, gişe gibi hizmet verilen alanlar" hakkında verilen kararlarında olduğu gibi bütün ilke kararlarında daha açıklayıcı ve spesifik kararlar verilmelidir ki; veri ihlallerinin önüne geçilmesi açısından uygulamada bütünlük ve tutarlılık sağlanmalıdır. Bununla birlikte ilke kararlarında, farklı sektörlere özgü riskler

ve gereklilikler daha ayrıntılı bir şekilde ele alınabilir. Böylece farklı sektörlerde faaliyet gösteren kurumların sürece daha etkili bir şekilde uyum sağlamasına yardımcı olunabilir.

Ek olarak ilke kararlarına açıkça bağlayıcılık atfedilmesi de önemlidir. KVKK'nın ilke kararlarının düzenlendiği 15/6. maddesinde yer alan "*Şikâyet üzerine veya resen yapılan inceleme sonucunda, ihlalin yaygın olduğunun tespit edilmesi hâlinde Kurul, bu konuda ilke kararı alır ve bu kararı yayımlar. Kurul, ilke kararı almadan önce ihtiyaç duyması hâlinde, ilgili kurum ve kuruluşların görüşlerini de alabilir.*" hükmünün devamına "*Kurulun ilke kararları, benzer hukuki konularda tüm veri sorumluları veya veri işleyen gerçek kişiler ile özel hukuk tüzel kişileri için bağlayıcıdır.*" hükmü getirilmelidir. Böylece ilke kararlarına da aykırı hareket edenlere ilişkin bu Kanun'un 18 inci maddesinin birinci fıkrasının (c) bendinde öngörülen idari para cezası uygulanabilir. Keza ilke kararlarında belirtilen tedbirlerin etkin bir şekilde uygulandığını ve veri ihlallerinin önüne geçildiğini doğrulamak için düzenli denetim ve izleme mekanizmaları oluşturulabilir. Bu doğrultuda Kanun veya Yönetmelik ile Kurulun görevleri arasına "*ilke kararlarının uygulanmasını izlemek ve denetlemek amacıyla düzenli aralıklarla denetimler yapma ve bu denetimler sırasında, ilke kararlarına uyulup uyulmadığını tespit etmek amacıyla veri sorumlularının ve veri işleyenlerin kayıtları ve uygulamaları inceleme yetkisi*" verilebilir.

Nihayetinde ilke kararları ile belirlenen standartlar ve belirlenecek iyi uygulama örnekleri, veri işleme süreçlerindeki farkındalık, hesap verebilme mekanizmalarının etkili bir işletilmesi ile olası ihlallerin önüne geçilmesi sağlanabilecektir.

SONUÇ

Teknolojinin hızla ilerlemesiyle birlikte bilgiye erişimin oldukça kolaylaşması ve kişisel verinin içerisinde bir bilgiyi de içermesi nedeniyle kişisel verilerin korunması hakkının müstakil olarak korunması gerekliliği ortaya çıkmıştır. Veri gizliliğinin ve mahremiyetinin günden güne önemli hale gelmesiyle birlikte de gerek uluslararası gerek ulusal çerçevede özel yaşamın gizliliği dahilinde koruma altına alınan kişisel verilerin korunması hususu başlı başına bir hak olarak yasal zemine oturtulmuştur. Bu bağlamda kişisel verilerin işlenmesinde genel ilkeler, veri işleme şartları gibi prensipler belirlenerek verilere yetkisiz erişim, verilerin ifşası, verilerin yasal olmayan yollardan elde edilmesi gibi sorunların önüne geçilmeye çalışılmıştır. Bu prensiplerin etkin bir şekilde uygulanmaması halinde kişisel verilerin ihlal edilmesi sonucu gündeme gelebilecektir.

Türk veri koruma hukukunda 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun), bireylere tanınan kişisel veri koruma hakkını ve bu hakka ilişkin genel ilke ve esasları belirlemiştir. Kanunun uygulanması ve denetlenmesi için kurulan Kişisel Verileri Koruma Kurumu (Kurum), kişisel veri ihlallerini önlemek ve kişisel veri güvenliğini sağlamak adına önemli bir rol üstlenmektedir. Kurumun burada denetim rolü, kişisel verilerin korunması için önemli bir denge unsuru oluşturur. Kurum, bir yandan bireylerin veri mahremiyetini ve gizliliğini koruma amacı güderken diğer yandan veri sorumlularının veri tabanlı faaliyetlerini sürdürmelerine olanak sağlar. Bu denge, dijital çağın karmaşık ve hızla değişen dinamiklerinde özellikle önemlidir. Zira Kanunun etkili bir şekilde uygulanması ve kişisel veri ihlallerinin önlenmesi, dijital toplumun sürdürülebilirliği ve bireylerin haklarının korunması için elzemdir. Kurumun karar organı olan Kişisel Verileri Koruma Kurulu (Kurul) aracılığı ile vermiş olduğu ilke kararları da veri ihlallerinin önlenmesi için gereken hukuki çerçevenin çizilmesinde önemli rol oynamaktadır.

İlke kararları, yaygın olarak yaşanan veri ihlallerine karşı Kurul tarafından alınan kararlardır. Kurulun faaliyet göstermeye başladığı günden bugüne kadar toplamda 8 tane ilke kararı verilmiştir. Kararların içeriğine bakıldığında yaygın olarak meydana gelen veri ihlalinin Kanunun 12. maddesinde belirtilen veri sorumlusunun veri güvenliği tedbirlerine ilişkin yükümlülükleri yerine getirilmemesi sebebiyle ortaya çıktığı görülmektedir. Bu doğrultuda veri sorumluları bünyesinde kurumsal iletişim ve eğitim eksikliğine dayalı farkındalığın oluşmaması, veri güvenliği risk analizlerinin ve iç denetimlerinin yapılmaması, kurumsal politika ve prosedürlerin gereği gibi ya da hiç düzenlenmemesi, siber güvenlik önlemlerinin alınmaması, veri güvenliği yönetiminin ve risk analizlerinin yapılmaması, siber güvenlik yönetimi ve takibinin yapılmamasının veri ihlallerine zemin hazırladığı görülmektedir. İlke kararları da bu gibi faktörlerden kaynaklanan sorunlara çözüm getirilmesini amaçlayarak aynı zamanda veri sorumlularının kişisel verilerin korunması konusundaki yasal yükümlülüklerini yerine getirmesi için bir rehber olmaktadır. İlke kararlarının rolü de bu noktada ortaya çıkmaktadır. İncelenen kararlarda görüldüğü üzere kişisel veri ihlallerinin önlenmesini ve kişisel verilerin korunmasını sağlamak için gereken hukuki çerçevenin oluşturulması, veri sorumlularının bilinçlendirilmesi ve uygun güvenlik önlemlerinin alınmasını sağlanmaktadır. İlke kararları bu özellikleri itibariyle kişisel veri ihlallerinin azaltılması ve veri koruma standartlarının yükseltilmesi için kritik bir öneme sahiptir.

İlke kararlarının taşıdığı önemin yanı sıra kişisel verilerin etkin bir şekilde korunması adına iyileştirilmelerin yapılması gerektiği de açıktır. 6698 sayılı Kanun'un görece yeni bir kanun olması sebebiyle uygulamada yaşanan belirsizlikler de veri ihlallerine neden olmaktadır. Bu noktada, Kişisel Verileri Koruma Kurumu'nun rolü büyük önem taşımaktadır. İlke kararlarının uygulamadaki belirsizliklere karşı bir rehber olduğu düşünüldüğünde, standartların geliştirilmesi için daha etkin bir denetim ile ilke kararlarının sayısının artırılması gerektiği ve Kanun'un 15/6. maddesine "ilke kararlarının bağlayıcı" olduğu hükmünün eklenmesi gerektiği düşünülmektedir. Ayrıca, henüz Kanun kapsamında yer almayan ancak önemli bir gereksinim olan "etki değerlendirmesi" metoduna yönelik çalışmaların yapılması ve Kanun'un 12/3. maddesine bu yönde bir hüküm eklenmesi önemlidir. Zira etki değerlendirmesi, kişisel verilerin işlenmesinin potansiyel etkilerini önceden belirleyerek uygun önlemlerin alınmasına olanak tanımaktadır. Bu sayede, veri ihlallerinin önlenmesi ve hesap verebilirliğin sağlanması

mümkün olacaktır. Tüm bu adımların atılması, kişisel verilerin etkin bir biçimde korunmasını sağlayacak ve veri ihlallerinin önüne geçilmesine yardımcı olacaktır. Bu süreçte, Kişisel Verileri Koruma Kurumu'nun liderlik rolü ve etkin denetim mekanizmalarının varlığı büyük önem taşımaktadır. Ancak sadece yasal düzenlemelerin yeterli olmayacağı, aynı zamanda uygulamadaki mevcut sorunların belirlenmesi ve çözüm odaklı adımların atılması gerektiği unutulmamalıdır.

KAYNAKÇA

Ağıralan, Erkan. "Bilgi Güvenliği, Kişisel Verilerin Korunması ve Mahremiyet Etki Değerlendirmesi". Yayımlanmamış Yüksek Lisans Tezi, Polis Akademisi, 2015.

Akçakoca, Mehmet. *Tıp Ceza Hukukunda Kişisel Sağlık Verilerinin Korunması,* Ankara: Adalet Yayınevi, 2022.

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

Akıncı, Ayşe Nur. "Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirmesi". Çalışma Raporu-6, Kalkınma Bakanlığı Bilgi Toplumu Dairesi Başkanlığı Yayını, Ankara, 2017. (E.T. 13.05.2023), http://www.bilgitoplumu.gov.tr /wpcontent/uploads/2017/07/AB_Veri_Koruma_Tuzugu.pdf

Akıncı, Ayşe Nur. "Büyük Veri Uygulamalarında Kişisel Veri Mahremiyeti". T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı Uzmanlık Tezi, 2019. (E.T. 13.05.2023), http://www.bilgitoplumu.gov.tr/wp-content/uploads/2019/04/ayse-nur-akinci-tez-WEB.pdf.

Akkır, Adem. "Kişisel Verileri Koruma Kurulu'nun Vermiş Olduğu Kararların Yargısal Denetimi". İçinde *Güncel Gelişmeler Işığında Kişisel Verilerin Korunması Hukuku Marmara Hukuk Bilimsel Toplantılar Serisi – I.* Editörler Leyla Keser Berber ve Ali Cem Bilgili. 163-184. İstanbul: On İki Levha Yayıncılık, 2020.

Akkurt, Sami Sinan Akkurt. "Kişisel Veri Kavramının Hukukî Niteliğine İlişkin Yaklaşımlara Mukayeseli Bir Bakış", *Kişisel Verileri Koruma Dergisi*, 2 (2020): 20-32. (E.T. 30.05.2023), https://dergipark.org.tr/tr/pub/kvkd/issue/55487/726372

Akmenek, Ezgi. "Türk Hukukunda Kişisel Verilere Yönelik Unutulma Hakkı". Yayımlanmamış Yüksek Lisans Tezi, İstanbul Üniversitesi, 2022. (E.T. 07.01.2023) https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

Alımcı, Ezgi. "Kişisel Verilerin Korunması Hukuku ve Bankaların Güven Kuruluşu Olarak Kabul Edilmesi Kapsamında Banka Bünyesinde Gerçekleşen Veri İhlalinin Değerlendirilmesi." *Ankara Barosu Dergisi.* 80/1 (2022): 47-76. DOI 10.30915/abd.1118300

Alkan, Mustafa ve Turhan Menteş ve Mehmet Ali İnceefe. *Kişisel Verileri Koruma El Kitabı, Teknik Uygulama ve Uyumluluk*. Ankara: Nobel Yayınları, 2020.

Aşıkoğlu, Şehriban İpek. *Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri.* İstanbul: Oniki Levha Yayıncılık, 2018.

Avrupa Komisyonu, 5 Kasım 2008 Sec (2008) 2699 Türkiye 2008 İlerleme Raporu, (Com (2008) 674), (E.T. 20.05.2023), https://www.ab.gov.tr/files/AB_Iliskileri/AdaylikSureci /IlerlemeRaporlari/turkiye_ilerleme_rap_2008.pdf

Avrupa Konseyi Anlaşma Serileri – No 108, (E.T. 08.12.2023), https://inhak. adalet.gov.tr/Resimler/Dokuman/2712020140848108_tur.pdf

Avrupa Parlamentosu ve Konsey Tüzüğü (Genel Veri Koruma Tüzüğü) (AEA ile ilişkili metin)", (E.T. 12.12. 2023), https://www.ab.gov.tr/siteimages/resimler/Nihai-ABB-HCDB-GDPR.pdf

Ay, Yunus Anıl. "5326 Sayılı Kanun'un 23 ve 24'üncü Maddelerine Göre Cumhuriyet Savcısı ve Mahkeme 213 sayılı Kanun'da Öngörülen Vergi Cezalarını Kesebilir Mi?". *Çağ Üniversitesi Sosyal Bilimler Dergisi*. 20/1 (2023): 58-80.

Aydın, Sedat Erdem. *AİHM İçtihatların Bağlamında Kişisel Verilerin Kaydedilmesi Suçu*. İstanbul: On İki Levha Yayıncılık, 2015.

Aygözer Öngün, Çiğdem. *Kişisel Verilerin Korunması Hukuku, Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil*. İstanbul: Beta Yayıncılık, Ocak 2019.

Babahanoğlu, Nesim. "Türk İdare Sisteminde Bağımsız İdari Otoriteler, Bağımsızlıkları ve Denetimleri Üzerine Bir Değerlendirme". *Anemon Muş Alparslan Üniversitesi Sosyal Bilimler Dergisi.* 9 (2021): 211-226.

Başar, Cemal. *Türk İdare Hukuku ve Avrupa Birliği Hukuku Işığında Kişisel Verilerin Korunması*. İstanbul: On İki Levha Yayınevi, 2020.

Başar, Oya ve Sezen Kama Işık, "Dördüncü Kuşak Haklar ve Bilişim Teknolojilerinin Doğuşunda Mahremiyet Kavramına Karşılaştırmalı Bir Bakış", *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, 25/2 (Aralık 2019): 602,623. DOI: 10.33433/maruhad.667577

Bayram, Öykü Beste. "Bir Uyum Aracı Olarak Veri Koruma Etki Analizinin Türk Hukuku Bakımından Değerlendirilmesi". *Kişisel Verileri Koruma Dergisi* 4 / 1 (Haziran 2022): 38-53. 43. (E.T. 05.07.2023), https://dergipark.org.tr/tr/pub/kvkd/issue/70820/1117742

Bilgiç, Alper. "Siber Suç (Cybercrime)". İçinde *Siber Ansiklopedi: Siber Ortama Çok Disiplinli Bir Yaklaşım*, ed. Naci Akdemir ve Can Ozan Tuncer. Ankara: Pegem Akademi, Ağustos 2021.

Bilgin, Metin ve Sema Erkan ve İdil Atasu ve Enes Yılmaz. "Privacy Impact Assessment As a Tool for GDPR Compliance Preparation". *Kişisel Verileri Koruma Dergisi*. 1/2 (Aralık 2019): 75-86. (E.T. 21.01.2024) https://dergipark.org.tr/tr/download/article-file/904860.

Bilir, Faruk. "6698 Sayılı Kişisel Verilerin Korunması Kanunu'na İlişkin Değerlendirme ve İnternet Çağında Kişisel Verilerin Korunması", *Anayasa Yargısı*, 37/2 (2020): 305-342.

Bilir, Faruk. "Kişisel Verilerin Korunması Kişinin Kendisinin Korunmasıdır", *TRT Akademi*, 6 (11) 2021., 172- 181, (E.T. 30.05.2023) https://dergipark.org.tr/tr/pub/trta/issue/60117/870971

Birtek, Fatih ve Beyza Nur Topal. "Dijital İspat Aracı Olarak Sabit veya Ankesörlü Telefonlara İlişkin Arama Kayıtları ve Bu Kayıtların İspat Kuvveti". *Galatasaray Üniversitesi Hukuk Fakültesi Dergisi*. 2 (2023): 1137-1178.

Birtek, Fatih. "Kişisel Sağlık Verilerinin Silinmesi". İçinde *Kişisel Verilerin Korunması Hukuku ve Bilgi Edinme Hukuku: Çeşitli Açılardan Bakış*. ed. Cemil Kaya, 481-505. İstanbul: On İki Levha Yayıncılık, Ağustos 2023.

Brandeis, Louis ve Samuel Warren. “The Right to Privacy”, *Harvard Law Review*, 4/5 (1890), 193-220. (E.T. 11.12.2023) https://www.jstor.org/stable/1321160

Bygrave, Lee A. “Privacy and Data Protection in an International Perspective*”, Stockholm Institute for Scandinavian Law*, 2(010):166-198. (E.T. 17.05.2023), https://scandinavianlaw. se/pdf/56-8.pdf;

Cidecigiller, Aynur. “Düzenleyici ve Denetleyici Kamu Kurumları Tarafından Uyuşmazlıkların Giderilmesi”. *Gazi Üniversitesi Hukuk Fakültesi Dergisi XVIII*. 3-4 (Temmuz 2014): 491-504. (E. T. 02.04.2022), https://dergipark.org.tr/tr/download/article-file/789132

Clarke, Roger “Privacy impact assessment: Its origins and development”. *Computer Law & Security Review*. 25/2 (2009): 123-135. https://doi.org/10.1016/j.clsr.2009.02.002

Clarke, Roger. “Privacy Impact Assessment in Australian Contexts”. *Murdoch University Electronic Journal of Law 72*. 15/1 (2008): 72-93. (E.T. 27.01.2024), https://www8.austlii.edu.au/cgibin/viewdoc/au/journals/MurdochUeJlLaw/2008/5.html?context=1;query=1996%20PLPR%2039%20or%20PLPR%201996%2039;mask_path=

Colozzo, Franca. “Data Privacy and Its Identification.” Dr. Arch. Franca Colozzo, 3 (2021), (E.T. 18.05.2023), https://www.academia.edu/100506335/Data_Privacy_and_its_identification

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, “Chatbot Uygulaması ve ChatGPT Örneği Değerlendirme Raporu”, (E.T. 01.02.2024), https://cbddo.gov.tr/SharedFolderServer /Genel/21.Chatbot-Uygulamas%C4%B1-ve-ChatGPT-%C3%96rne%C4%9Fi-De%C4%9 Ferl endirme-Raporu.pdf

Çekin, Mesut Serdar. *Avrupa Birliği Hukukuyla Mukayeseli olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku*. İstanbul: On İki Levha yayınları, 2. Baskı, 2019.

Çelikel, Serdar. *Kişisel Verilerin Korunması Hukuku Kapsamında Veri Sorumlusu ve Veri Sorumlusunun Yükümlülükleri*. Ankara: Seçkin Yayıncılık, 2022.

Çimen Bulut, İpek. “Avrupa Birliği Genel Veri Koruma Tüzüğü Kapsamında Getirilen Yeni Teknik ve Yaptırım Mekanizmalar”. *Anadolu Üniversitesi Sosyal Bilimler Dergisi.* 20/2 (2020): 127-142. (E.T. 04.07.2023) Microsoft Word - 8(127-142).docx (dergipark.org.tr)

De Hert, Paul. “A Human Rights Perspective on Privacy and Data Protection Impact Assessments”. İçinde *Privacy Impact Assessment. Law, Governance and Technology Series vol 6*., ed.: David Wright ve Paul De Hert, P., (Dordrecht: Springer, 2012). https://doi.org/10.1007/978-94-007-2543-0_2;

Demetzou, Katerina. “Data Protection Impact Assessment: A tool for accountability and the unclarified concept of ‘high risk’ in the General Data Protection Regulation”. *Computer Law & Security Review*, 35/6 (2019). https://doi.org/10.1016/j.clsr.2019.105342

Demir, Yasin. “Kişisel Verilerin İhlalinin Psikolojik Yansımaları”, İçinde *Güncel Gelişmeler Işığında Kişisel Verilerin Korunması Hukuku*. Editor: Bayram Doğan, 75-100, Ankara: Adalet Yayınevi, 2022.

Determann, Lothar. *Kişisel Verilerin Korunması Uygulama Kılavuzu*, çev. Hilal Temel, İstanbul: On iki Levha Yayınları, 2021.

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

Directive 95/46/EC Of The European Parliament and of The Council, (E.T. 08.12.2023), https: //eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

Doğan, Aişe Sena. “Kişilik Hakkının 5651 Sayılı Kanun’un 9. Maddesi Kapsamında Korunması”. *Bilişim Hukuku Dergisi.* 2/2 (Aralık 2020): 143-180, 166-167. (E.T. 09.07.2024), https://dergipark.org.tr/tr/download/article-file/1377099

Doğan, Bayram. “Dijital Veri Uygulamalarında Kişisel Verilerin Korunması” İçinde *Güncel Gelişmeler Işığında Kişisel Verilerin Korunması Hukuku*, Editor: Bayram Doğan, 75-100, Ankara: Adalet Yayınevi, 2022.

Doğan, Bayram. *Karşılaştırmalı Hukukta Anayasal Bir Hak Olarak Kişisel Verilerin Korunması Hakkı*, Ankara: Adalet Yayınevi, 2022.

Durdu, Ali. “Bilgi Sistemlerinde Riskler ve Risk Yönetimi”. İçinde *Uzmanların Kaleminden Farklı Boyutlarıyla Risk ve Risk Yönetimi,* ed. Hakan Karabacak. Ankara: Gazi Kitabevi, Temmuz 2021.

Durdu, Muhammet. “Mükellef Verilerinin Korunması ve Vergi Mahremiyeti”. *Selçuk Üniversitesi Hukuk Fakültesi Dergisi*. 27/3 (2019): 589-623. DOI: 10.15337/suhfd.578013

Dülger, Murat Volkan. "Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması". *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi*. 3 (2016): 101-168. (E.T. 02.07.2023) https://dergipark.org.tr/tr/download/article-file/1102227

Dülger, Murat Volkan. “Avrupa Birliği Genel Veri Koruma Tüzüğü Bağlamında Kişisel Verilerin Korunması”. *Yaşar Hukuk Dergisi*. 1/2 (2019): 71-174.

Dülger, Murat Volkan. *Kişisel Verilerin Korunması Hukuku*. İstanbul: Hukuk Akademisi, 2020.

Ekici, Şerafettin. *Bilişim ve Teknoloji Hukuku*. Ankara: Seçkin Yayınları, 2023.

Erdem, Tahir. “Kişisel Verilerin Korunması Konusunda Son Gelişmeler”. *Vergi Sorunları Dergisi.* 39/332 (2016), 97-115. (E.T. 24.09.2023) www.idealonline.com.tr

Evans, A.C., “European Data Protection Law.” *The American Journal of Comparative Law*, 29/ 4 (1981): 571– 582. https://doi.org/10.2307/839754.

Friedewald , Michael ve Ina Schiering, Nicholas Martin ve Dara Hallinan. “Data Protection Impact Assessments in Practice”. İçinde Computer Security, ESORICS 2021 International Workshops, (October 4-6, 2021) Darmstadt, Germany.

Gantz, Stephen D. ve Daniel R. Philpott, "Chapter 16 – Privacy". İçinde *FISMA and the Risk Management Framework*. ed. Stephen D. Gantz ve Daniel R. Philpott, (Waltham: Syngress, 2013): 445-480. https://doi.org/10.1016/B978-1-59-749641-4.00016-3.

GDPR, (E.T. 08.12.2023), https://gdpr-info.eu/

Gök, Ali. "Siber Tehdit (Cyber Threat) içinde *Siber Ansiklopedi: Siber Ortama Çok Disiplinli Bir Yaklaşım*, ed. Naci Akdemir ve Can Ozan Tuncer. Ankara: Pegem Akademi, Ağustos 2021.

Gülerci, Burcu. *Türk Hukukunda Vergi Mahremiyetinin Sınırları*. İstanbul: On İki Levha Yayıncılık, 2017.

Gülnaz, Besra. "Kişisel Verileri Koruma Kurumunun Yapısal ve İşlevsel Analizi". Yayımlanmamış Yüksek Lisans Tezi, Mersin Üniversitesi, 2019.

Gün, Mehmet. *Türkiye'nin Orta Demokrasi Sorunları ve Çözüm Yolu*. İstanbul: Gün +, 2018 2. Baskı.

Günbey, Onur. "Kişisel Verilerin Korunması Kanunu Kapsamında Veri Sorumlusunun Yükümlülükleri". Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi, 2020. (E.T. 25.01.2023) https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

Gündüz, Mehmet Şükrü. *Uluslararası İnsan Hakları Açısından Kişisel Veri Güvenliği.* Ankara: Adalet Yayınevi, 2022.

Güngör, Nevzat. *İç Denetimde Bilgi Teknolojileri ve Siber Güvenlik*. Ankara: Gazi Kitabevi, Aralık 2021.

Gürener, Betül. "Avrupa Birliği Genel Veri Koruma Tüzüğü ve Kişisel Verilerin Korunması Kanununa Göre İlgili Kişi Haklarının Karşılaştırılması". Yayımlanmamış Yüksek Lisans Tezi, Atılım Üniversitesi. 2021.

Gürpınar, Damla. "Kişisel Verilerin Korunamamasından Doğan Hukuki Sorumluluk". *D.E.Ü. Hukuk Fakültesi Dergisi, Prof. Dr. Şeref ERTAŞ'a Armağan*. 19/ Özel Sayı (2017): 679-698.

Gürsel, Esin ve Fatih Düğmeci, "Yapısal Anlamda Türkiye Kişisel Verileri Koruma Kurumu'na İlişkin Bir Değerlendirme". *R&S- Research Studies Anatolia Journal*. 1/2 (2018): 318-329. (E.T.04.06.2023) https://dergipark.org.tr/tr/download/article-file/507084

Gürses, Bekir. "AB ve Türk Hukukunda Kişisel Verilerin Korunması- Mevzuat Uyumuna Yönelik Bir Değerlendirme". Yayımlanmamış Yüksek Lisans Tezi, Marmara Üniversitesi, 2019.

Gürses, Binnur. "Sosyal Paylaşım Ağlarında Kişisel Verilerin Güvenliği; Sorunlar ve Çözüm Önerileri". İdari Uzmanlık Tezi, Bilgi Teknolojileri ve İletişim Kurumu, Ağustos 2013.

Güzel, Mehmet Serdar. "Bilgi Güvenliği (Information Security)". İçinde *Siber Ansiklopedi: Siber Ortama Çok Disiplinli Bir Yaklaşım*, ed. Naci Akdemir ve Can Ozan Tuncer. Ankara: Pegem Akademi, Ağustos 2021.

Hacıosmanoğlu, Deniz. "Kişisel Verileri Koruma Kurumu Yapısı ve İşlevi". Yayımlanmamış Yüksek Lisans Tezi, Ankara Üniversitesi, 2020.

Henkoğlu, Türkay. “Kişisel Verileriniz Ne Kadar Güvende? Bilgi Güvenliği Kapsamında Bir Değerlendirme”. *Arşiv Dünyası*, 2017/1 (2017): 46-56. (E.T. 24.09.2023), www.idealonline.com.tr

Hiranandani, Vanmala. “Privacy and Security in the Digital Age: Contemporary Challenges and Future Directions”, *The International Journal of Human Rights*, 15/7 (2011): 1091-1106. https://doi.org/10.1080/13642987.2010.493360, (E. T. 07.05.2023), https://www.tandfonline. com/loi/fjhr20

Hizarcı, Emine. *6698 sayılı Kişisel Verilerin Korunması Kanunun AB Veri Koruma Hukuku Işığında Değerlendirilmesi*. Ankara: Yetkin Yayınları,2020.

https://kararlarbilgibankasi.anayasa.gov.tr/BB/2017/16849, (E.T. 10.07.2024),

https://kisiselveriihlali.com/Anasayfa/3316/ (E.T. 05.07.2023),

https://kvkk.gov.tr/SharedFolderServer/CMSFiles/8833aad2-62c2-4a01-b147 fe97062678f3.pdf (E.T. 06.01.2024)

https://normkararlarbilgibankasi.anayasa.gov.tr/Dosyalar/Kararlar/KararPDF/2009-80nrm.pdf (E.T. 10.06.2023)

https://www.anayasa.gov.tr/tr/mevzuat/anayasa/ (E.T. 27.07.2023)

https://www.collinsdictionary.com/dictionary/english/blacklist (E.T. 21.01.2024).

https://www.kvkk.gov.tr/veri-ihlali-bildirimi/ (E.T. 12.03.2024)

https://www.lexpera.com.tr/ictihat/arama

https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=39647&MevzuatTur=7&MevzuatTertip=5 (E.T. 21.01.2024)

https://www.resmigazete.gov.tr/eskiler/2017/10/20171028-10.htm (E.T. 02.08.2023),

https://www.resmigazete.gov.tr/eskiler/2017/12/20171230-7.htm (E.T. 02.08.2023),

https://www.resmigazete.gov.tr/eskiler/2018/03/20180310-5.htm (E.T. 02.08.2023),

https://www.resmigazete.gov.tr/eskiler/2018/03/20180310-6.htm (E.T. 02.08.2023),

https://www.resmigazete.gov.tr/eskiler/2018/03/20180310-6.htm (E.T. 17.12.2023)

https://www.resmigazete.gov.tr/eskiler/2024/03/20240312-1.htm

https://www.resmigazete.gov.tr/eskiler/2024/03/20240312-1.htm (E.T. 12.03.2024)

ICO, “Findings from ICO information risk reviews of information security in the higher education sector”, https://ico.org.uk/media/action-weve-taken/audits-and-advisory-visits/2614 196/20190124-information-risk-review-report-higher-education-sectorpdf.pdf. (E. T. 25.11. 2023)

ICO, fines Uber £385,000 over data protection failings, Retrieved from https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/11/ico-fines-uber-385-000-over-data-protection-failings/ (E.T. 25.11.2023)

ICO, issues maximum £500,000 fine to Facebook for failing to protect users‟ personal information, Retrieved from https://ico.org.uk/about-the-ico/news-and-events/news-and-*İsmail Sevinç, Niyazi Karabulut* 470 blogs/2018/10/facebook-issued-with-maximum-500-000-fine/ (E.T. 25.11.2023)

ICO. “Privacy Impact Assessment Handbook Version 2.0.”, (E.T. 28.01.2024), https://www.huntonprivacyblog.com/wpcontent/uploads/sites/28/2013/09/PIAhandbookV2.pdf

Information Commissioner’s Office. “Privacy impact assessment and risk management”, 4 Mayıs 2013, (E.T. 28.01.2024), https://ico.org.uk/media/about-the-ico/consultations/2055/pia-and-risk-management-full-report-for-the-ico.pdf

ISO 27001 Bilgi Güvenliği Yönetim Sistemi Belgesi alma zorunluluğu bulunan sektörler https://www.isokalitebelgesi.com/iso-27001-belgesi-kimler-hangi-sektroler-sirketler-firmalar-alabilir-zorunlumudur (E.T. 17.03.2024)

İçel, Kayıhan. “Ceza Hukuku Açısından Kişisel Verilerin Korunmasında “Kişisel Veri” ve “Hukuka Aykırılık” Kavramları”. *İstanbul Barosu Dergisi*. 94/2 (Mart 2020): 15-23, (E.T. 11.07.2024), https://www.istanbulbarosu.org.tr/files/yayinlar/dergi/doc/ibd20202.pdf#page=16

İnan, Salih. “Kişisel Verilerin Korunması Kapsamındaki Yaptırımlara Karşı Yargısal Başvuru Yolları: Karşılaştırmalı Bir İnceleme”. *Kişisel Verileri Koruma Dergisi*. 3/2 (2021), 50-65.

Judgment in Case, C-101/01 Bodil Lindqvist - Åklagarkammaren i Jönköping 06.11.2003, https://curia.europa.eu/juris/liste.jsf?num=C-101/01 (E.T. 11.03.2024),

Kağıtçıoğlu, Mutlu. “Kişisel Verileri Koruma Kurumuna İdare Hukuku Çerçevesinden Bir Bakış*”. İstanbul Kemerburgaz Üniversitesi Sosyal Bilimler Dergisi.* 1/2 (Kış 2016), 77-99. (E.T. 03. 04.2022) https://dergipark.org.tr/tr/download/article-file/272994

Kangal, Zeynep T. *Kişisel Verilerin Ceza ve Kabahatler Hukukunda Korunması*. İstanbul: On İki Levha Yayıncılık, Eylül 2019.

Kart, Aslıhan ve Muammer Ketizmen. “Kabahatler Kanunu'nun İçtima Hükümleri Açısından Kişisel Verilerin Korunmasına İlişkin Suç ve Kabahatler ile Kurul’un İdari Ceza Kararlarına İlişkin Bir Değerlendirme”. *Kişisel Verileri Koruma Dergisi.* 1/2 (2019), 17-29.

Kavak Güven, Neslihan. “Avrupa Birliği Genel Veri Koruma Tüzüğü Doğrultusunda Profilleme ve Otomatik Karar Alma”. Yayımlanmamış Yüksek Lisans Tezi, TOBB Ekonomi ve Teknoloji Üniversitesi, 2022. (E.T. 23.01.2023), https://tez.yok.gov.tr/UlusalTez Merkezi/ tezSorguSonucYeni.jsp

Kaya, Mehmet Bedii. "Kişisel Verilerin Korunmasında Yeni Paradigma: Hesap Verebilirlik İlkesi*", İstanbul Hukuk Mecmuası*. 78/4 (2020): 1859-1897.

Kaya, Mehmet Bedii. “Kişisel Verilerin İşlenmesi ve Korunması Arasında Denge”. İçinde Güncel Gelişmeler Işığında Kişisel Verilerin Korunması Hukuku Marmara Hukuk Bilimsel Toplantılar Serisi – I. Editörler Leyla Keser Berber ve Ali Cem Bilgili. 33-68. İstanbul: On İki Levha Yayıncılık, 2020.

Kendir Tunalı, Tuba. “Veri Sorumlusunun Yükümlülükleri” içinde *Kişisel Verilerin Korunması Alanında Yeni Gelişmeler Sempozyumu.* ed. Hüseyin Özcan ve Mehmet Başar ve H. Derya Osmanoğlu ve Ferhat Kayış. Ankara: Adalet Yayınevi, 2021.

Keskinsoy, Ömer ve Semih Batur Kaya. “Anayasa Mahkemesi Kararlarını Biçimlendirme Çabası Olarak Yorum”. *Hacettepe Hukuk Fakültesi Dergisi* 11/1 (Haziran 2021): 63-105. DOI: 10.32957/hacettepehdf.866047

Kılınç Sucu, Büşra Merve. “Temel Hak Boyutuyla Kişisel Verilerin Korunması”. Yayımlanmamış Yüksek Lisans Tezi, Dokuz Eylül Üniversitesi, 2020.

Kılınç, Doğan. “Anayasal Bir Hak Olarak Kişisel Verilerin Korunması”, *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, 61/3 (2012): 1089-1169, (E.T. 15.02.2023), https://kutuphane.dogus.edu.tr/mvt/pdf.php?pdf=0013299&lng=0;

Kıraç, Şehriban. “Türkiye’deki genel siber tehditlerin sayısı 2023 yılında 2022’ye kıyasla yüzde 5 arttı”. *Cumhuriyet*. 09.03.2024, https://www.cumhuriyet.com.tr/bilim-teknoloji/turkiyedeki-genel-siber-tehditlerin-sayisi-2023-yilinda-2022ye-2183667

Kişisel Verileri Koruma Kurumu, "Veri sorumluları ve veri işleyenler tarafından ilgili kişilerin e-posta adreslerine veya SMS ya da çağrı ile cep telefonlarına reklam bildirimleri/aramaları yönlendirilmesinin önüne geçilmesi " ile ilgili Kişisel Verileri Koruma Kurulunun 16/10/2018 Tarihli ve 2018/119 Sayılı İlke Kararı, https://www.kvkk.gov.tr/Icerik/5299/2018-119 (E.T. 16.01.2023)

Kişisel Verileri Koruma Kurumu, “İlgili Kişinin Hak Arama Yöntemleri”, (E.T. 04.07.2024), https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/353d85d5-87df-4c91-b08e-b4f0991a80f4.pdf

Kişisel Verileri Koruma Kurumu, “Kişisel Veri İhlali Bildirim Usul ve Esaslarına İlişkin Kişisel Verileri Koruma Kurulunun 24.01.2019 Tarih ve 2019/10 Sayılı Kararına İlişkin Duyuru”, https://www.kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirimi (E.T.: 02.09.2023)

Kişisel Verileri Koruma Kurumu, 25/03/2019 tarihli ve 2019/78 Sayılı Kişisel Verileri Koruma Kurulu kararı, https://www.kvkk.gov.tr/Icerik/5434/2019-78 (E.T. 05.07.2023)

Kişisel Verileri Koruma Kurumu, 29/06/2022 tarihli ve 2022/630 sayılı Kişisel Verileri Koruma Kurulu kararı, https://kvkk.gov.tr/Icerik/7567/2022-630 (E.T. 03.06.2023)

Kişisel Verileri Koruma Kurumu, Araç Kiralama Sektöründeki Kara Liste Uygulamaları Hakkında Kişisel Verileri Koruma Kurulunun 23/12/2021 Tarihli ve 2021/1304 Sayılı İlke Kararı, https://www.resmigazete.gov.tr/eskiler/2022/01/20220120-10.pdf (E.T. 16.01.2023)

Kişisel Verileri Koruma Kurumu, Banko, Gişe, Masa gibi Hizmet Alanlarında Kişisel Verilerin Korunmasına Yönelik Kişisel Verileri Koruma Kurulunun 21/12/2017 Tarihli ve 2017/62 Sayılı İlke Kararı, https://www.kvkk.gov.tr/Icerik/4114/2017-62 (E.T. 16.01.2023)

Kişisel Verileri Koruma Kurumu, Belediyelerin ödeme ve borç sorgulama hizmetleri hakkında Kişisel Verileri Koruma Kurulunun 21/04/2022 Tarihli ve 2022/388 sayılı İlke Kararı, https://www.kvkk.gov.tr/Icerik/7252/2022-388 (E.T. 16.01.2023)

Kişisel Verileri Koruma Kurumu, Hukuka Aykırı Olarak Elde Edilen Veriler Üzerinden Vatandaşların Kimlik ve İletişim Bilgileri Gibi Kişisel Verilerinin Sorgulanmasına İmkân Tanıyan Yazılım/Program/Uygulamalara Yönelik Kişisel Verileri Koruma

Kurulunun 18/10/2019 Tarihli ve 2019/308 Sayılı İlke Kararı, https://www.kvkk.gov.tr/Icerik/6568/2019-308 (E.T. 16.01.2023)

Kişisel Verileri Koruma Kurumu, İlgili Kişinin Kişisel Verilerinin Hukuka Aykırı İşlendiği İddiası Kapsamında Veri Sorumlusu Bankadan Talep Ettiği Tazminat Talebinin Karşılanmaması Hakkında Kişisel Verileri Koruma Kurulunun 16/01/2020 Tarihli ve 2020/41 Sayılı Kararı", (E.T. 17.12.2023) https://www.kvkk.gov.tr/Icerik/6714/2020-41

Kişisel Verileri Koruma Kurumu, Kişilerin Ad ve Soyadı ile Arama Motorları Üzerinden Yapılan Aramalarda Çıkan Sonuçların İndeksten Çıkarılmasına Yönelik Talepler ile ilgili olarak Kişisel Verileri Koruma Kurulunun 23/06/2020 Tarihli ve 2020/481 Sayılı Kararı, https://www.kvkk.gov.tr/Icerik/6776/2020-481 (E.T. 17.12.2023)

Kişisel Verileri Koruma Kurumu, *Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler*). Ankara: KVKK Yayınları, Ocak 2018.

Kişisel Verileri Koruma Kurumu, Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" ile ilgili Kişisel Verileri Koruma Kurulunun 31/01/2018 Tarihli ve 2018/10 Sayılı Kararı, https://www.kvkk. gov.tr/Icerik/4110/2018-10 (E.T. 17.09.2023)

Kişisel Verileri Koruma Kurumu, Rehberlik Hizmeti Veren İnternet Sitelerinde/Uygulamalarda Kişisel Verilerin Korunmasına Yönelik Kişisel Verileri Koruma Kurulunun 21/12/2017 Tarihli ve 2017/61 Sayılı İlke Kararı, https://www.kvkk.gov.tr/Icerik/4113/2017-61 (E.T. 16.01.2023).

Kişisel Verileri Koruma Kurumu, Veri sorumluları tarafından kişilerin telefon numarası, e-posta adresi gibi iletişim kanallarına Kanuna aykırı şekilde gönderilen üçüncü kişilere ait kişisel veriler hakkında Kişisel Verileri Koruma Kurulunun 22/12/2020 Tarihli ve 2020/966 sayılı İlke Kararı, https://www.kvkk.gov.tr/Icerik/6858/2020-966 (E.T. 16.01.2023)

Kişisel Verileri Koruma Kurumu, Veri Sorumlusu Nezdindeki Kişisel Verilere Erişim Yetkisi Bulunan Personelin Yetkisi ve Amacı Dışında Söz Konusu Verileri İşlemesi Hususunun Değerlendirilmesine İlişkin 31/05/2018 Tarih ve 2018/63 Sayılı İlke Kararı, https://www.kvkk.gov.tr/Icerik/5248/2018-63 (E.T. 16.01.2023)

Kişisel Verileri Koruma Kurumu. "6698 Sayılı Kanun'da Yer Alan Temel Kavramlar". (E.T. 08.12.2023), https://www.kvkk.gov.tr/Icerik/4187/6698-Sayili-Kanun'da-Yer-Alan-Temel-Kavramlar

Kişisel Verileri Koruma Kurumu. "6698 Sayılı Kişisel Verilerin Korunması Kanununun Amacı ve Kapsamı". (E.T. 30.05.2023), https://www.kvkk.gov.tr/Icerik/4185/6698-Sayili-Kisisel-Verilerin-Korunmasi-Kanununun-Amaci-ve-Kapsami

Kişisel Verileri Koruma Kurumu. "Anayasal Bir Hak Olarak Kişisel Verilerin Korunmasını İsteme Hakkı", (E.T. 23.03.2024), https://www.kvkk.gov.tr/Icerik/4184/Anayasal-Bir-Hak-Olarak-Kisisel-Verilerin-Korunmasini-Isteme-Hakki

Kişisel Verileri Koruma Kurumu. "Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler", (E.T. 04.08.2023),

https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/32ff74f6-9798-405a-b3d2b42d28423fde.pdf

Kişisel Verileri Koruma Kurumu. “Kişisel Verilerin Korunması Alanında Uluslararası ve Ulusal Düzenlemeler”. (E.T. 03.08.2023), https://www.kvkk.gov.tr/Icerik/4183/Kisisel-Verilerin-Korunmasi-Alaninda-Uluslararasi-ve-Ulusal-Duzenlemeler

Kişisel Verileri Koruma Kurumu. “Kişisel Verilerin Korunması Kanunu ve Uygulaması”. (E.T. 02.08.2023), https://kvkk.gov.tr/yayinlar/K%C4%B0%C5%9E%C4%B0SEL%20VER%C4%B0LER%C4%B0N%20KORUNMASI%20KANUNU%20VE%20UYGULAMASI.pdf

Kişisel Verileri Koruma Kurumu. “Veri Güvenliğine İlişkin Yükümlülükler”. (E.T. 09.08.2023), https://www.kvkk.gov.tr/Icerik/2040/Veri-Guvenligine-Iliskin-Yukumlulukler

Kişisel Verileri Koruma Kurumu. “Veri Sorumlusu ve Veri İşleyen”. (E.T. 09.12.2023), https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/31d9c444-27a5-4a75-95b1-1ca9bdb81ea5.pdf

Kişisel Verileri Koruma Kurumu. “Yapay Zekâ Alanında Kişisel Verilerin Korunmasına Dair Tavsiyeler”. (E.T. 24.01.2024), https://www.kvkk.gov.tr/Icerik/7048/Yapay-Zeka-Alaninda-Kisisel-Verilerin-Korunmasina-Dair-Tavsiyeler

Kişisel Verileri Koruma Kurumu. *100 Soruda Kişisel Verilerin Korunması Kanunu*. Ankara: KVKK Yayınları, Aralık 2019.

Kişisel Verileri Koruma Kurumu. *6698 Sayılı Kişisel Verilerin Korunması Kanunu Hakkında Doğru Bilinen Yanlışlar,* 31, Ankara: KVKK Yayınları, Nisan 2020.

Kişisel Verileri Koruma Kurumu. *Kişisel Verilerin Korunmasına İlişkin Bankacılık Sektörü İyi Uygulamalar Rehberi*. Ankara: KVKK Yayınları, Temmuz 2022.

Kişisel Verileri Koruma Kurumu. *Madde ve Gerekçesi ile Kişisel Verilerin Korunması Kanunu (Bilgi Notu) ve Kişisel Verilerin Korunmasına İlişkin Terimler Sözlüğü*. Ankara: KVKK Yayınları, Mart 2019.

Korucu, Onur. *Veri Güvenliğinin İyileştirilmesinde Küresel Standart, Çerçeve ve En İyi Uygulamaların Hukuki Uyuma Desteği*. Ankara: Adalet Yayınevi, 2021).

Koyuncu, Seçil. “KVKK Tarafından Yayımlanan İlke Kararları”. 5. e-Safe Kişisel Verileri Koruma Zirvesinde Sunulan Bildiri, Ankara, Mayıs 17, 2022. (E.T. 05.09.2023), https://www.youtube.com/watch?v=LBfugRBV57I

Kutlu, Önder ve Selçuk Kahraman. "Türkiye’de Kişisel Verilerin Korunması Politikasının Analizi". *Siyaset, Ekonomi ve Yönetim Araştırmaları Dergisi.* 5/4 (Ekim 2017): 45-62. https://doi.org/10.25272/j.2147-7035.2017.5.4.03.

Küçük, Adnan. “1982 Anayasası’ndaki Temel Hak ve Hürriyetlerin Sınırlanması Rejimi Bağlamında Kişisel Verilerin Korunması Hakkının Sınırlanmasının Anayasaya Uygunluğu”, İçinde *Güncel Gelişmeler Işığında Kişisel Verilerin Korunması Hukuku*, Editor: Bayram Doğan, 11-74, Ankara: Adalet Yayınevi, 2022.

Küzeci, Elif. *Kişisel Verilerin Korunması,* İstanbul: On İki Levha Yayıncılık, Mayıs 2020.

Memiş, Levent ve Melikali Güç. “Akıllı Kentlerde Verinin Gizliliği ve Güvenliği: İlkeler ve Yaklaşımlar”. *Güvenlik Bilimleri Dergisi*. UGK Özel Sayısı (Şubat 2020), 95-112. DOI:10.28956/gbd.695936.

Öksüzoğlu, Hilal Tuğba. “6698 Sayılı Kişisel Verilerin Korunması Kanunu ve Avrupa Birliği Hukukunda Kişisel Verilerin Silinmesi ve Düzeltilmesi”. *Bilişim Hukuku Dergisi*, 1/2 (2019): 185-242. (E.T.27.01.2023), https://www.jurix.com.tr/article/32152

Özarslan, Furkan. “Türkiye’de Kişisel Verilerin Korunması Politikasının Analizi”. Yayımlanmamış Yüksek Lisans Tezi, Pamukkale Üniversitesi, 2022.

Özkan, Oğulcan. *Kişisel Verilerin Korunması*. Ankara: Yetkin Yayınevi, 2020.

Özkan, Rabia. “Kişisel Veri Koruma Hukukunun Kişilik Hakkının Korunması Çerçevesinde Değerlendirilmesi”, *Ankara Sosyal Bilimler Üniversitesi Hukuk Fakültesi Dergisi*, 3 / 2 (2021), 675 – 733, https://doi.org/10.47136/asbuhfd.963013

Öztürk, Bahri ve Serkan Seyhan ve Elif Altınok Çalışkan. *Kişisel Verilerin Korunması Hukuku Teorik ve Pratik Çalışma Kitabı*. Ankara: Seçkin Yayıncılık, 2022.

Saka, Rıza ve Ramazan Çağlayan ve Mahmut Koca. *Avrupa Birliği Hukuku, İdare Hukuku ve Ceza Hukuku Açısından Kişisel Verilerin İmhası.* Ankara: Seçkin Yayıncılık, 2020.

Saygı, Samet. “6698 Sayılı Kanun’un Sistematiğinde Yargısal Başvuru Yolları”. *Kişisel Verileri Koruma Dergisi.2020*, 2(2), 30-60. (E.T. 10.02.2023), https://dergipark.org.tr/tr/pub/kvkd/ issue/58932/738180

Sebetçi, Özel, Aslıhan Topal, Mehmet Can Hanaylı ve Gizem Gürel Dönük. “Dijital Ortamda Kişisel Veri Güvenliği ve Sosyal Medya Reklamcılığı Üzerine Bir Değerlendirme”. *Kesit Akademi Dergisi*, 4/ 16 (2018), 389-409.

Selek, Onur. *Kişisel Verilerin Korunması ve Verileri Yok Etmeme Suçu (TCK m.138*). İstanbul: On İki Levha Yayıncılık, 2021.

Sevinç, İsmail ve Niyazi Karabulut. "A Revıew on the Personal Data Protectıon Authorıty of Turkey", *Akademik Hassasiyetler*. 7/13 (2020), 449-472. (E.T. 02.09.2022), https://search.trdizin.gov.tr/tr/yayin/detay/377424/a-review-on-the-personal-data-protection-authority-of-turkey

Sevindi, Nur Sena ve Muhammet Emin Ordu. “AB ve Türk Hukukunda Veri İhlalinin Tespiti ve Bildirim Süresinin Karşılaştırmalı Değerlendirmesi”. *Kişisel Verileri Koruma Dergisi.* 5/1 (2023): 12-22. (E.T. 01.08.2023), https://dergipark.org.tr/tr/download/article-file/3116868

Stewart, Blair. “Privacy impact assessments”. *Privacy Law & Policy Reporter*. 3/4 (1996), (E.T. 27.01.2024), https://www8.austlii.edu.au/cgi-bin/viewdoc/au/journals/PLPR/1996/39. html#

Sultanlı, İntizar. “Anayasal Bir Hak Olan Kişisel Verilerin Korunması Hakkı ve Mahremiyet ile İlişkisi”, *SÜAMYOD*., 4/1 (2021): 23-34.

Şahinaslan, Önder, Ender Şahinaslan, Emin Borandağ ve A.Mutalip Sahinaslan. “Güvenli Bir Toplum İçin Son Kullanıcı Siber Güvenliği”. Akademik Bilişim 2013 – XV.

Akademik Bilişim Konferansı Bildirileri 23-25 Ocak 2013 – Akdeniz Üniversitesi, Antalya, (E.T. 21.10.2023), https://ab.org.tr/ab13/kitap/eski/49.pdf

Şimşek, Oğuz. *Anayasa Hukukunda Kişisel Verilerin Korunması*, İstanbul: Beta Yayınları, 2008, 132.

T.C. Cumhurbaşkanlığı Devlet Denetleme Kurulu. "Kişisel Verilerin Korunmasına İlişkin Ulusal ve Uluslararası Durum Değerlendirmesi ile Bilgi Güvenliği ve Kişisel Verilerin Korunması Kapsamında Gerçekleştirilen Denetim Çalışmaları". 27 / 11/ 2013, 2013 / 3, 778-779. (E.T. 20.05.2023), https://www.memurlar.net/common/news/documents/439122/ddk56 .pdf

Tataroğlu. Muhittin "Mahremiyet Sorunlarının Önlenmesinde Mahremiyet Etki Değerlendirmesi (MED)". *Yönetim ve Ekonomi Dergisi,* 20/1 (2013), 263 – 289. (E.T. 03.12.2023), https://dergipark.org.tr/en/pub/yonveek/issue/13698/165807

TDK Sözlük, (E.T. 30.05.2023), https://sozluk.gov.tr/

The OECD Prıvacy Framework, (E.T. 03.08.2023), https://www.oecd.org/sti/ieconomy/oecd_ privacy_framework.pdf

Tokmakcı, Uğur. "Kişisel Verilerin Korunmasına Risk Temelli Yaklaşım". İçinde *Kişisel Verilerin Korunmasına Uzman Bakış Uzmanlık Tezleri Derleme Çalışması.* ed. Pınar Çağlayan Aksoy ve Hüseyin Can Aksoy. Ankara: KVKK Yayınları, No 44, 2023.

Tunç, Aybike. *Bulut Bilişim Sözleşmeleri*, İstanbul: On İki Levha Yayıncılık, Kasım 2020.

Turan Başara, Gamze. "Kişisel Veri İşleme Sözleşmesi". *Uyuşmazlık Mahkemesi Dergisi*. 8/16, (Aralık 2020): 57-90.

Turan, Metin. *Karşılaştırmalı Hukukta Kişisel Verilerin Korunması*. Ankara: Seçkin Yayıncılık, 2021.

Türkiye Bilişim Derneği, "Veri Uzayı Raporu", Ankara: Türkiye Bilişim Derneği, Kasım 2023. (E.T. 15.03.2024) https://www.tbd.org.tr/pdf/kamubib-calisma-grubu/veri-uzayi-calisma-grubu-raporu-2023.pdf

U.S. Department of Agriculture. "Privacy Impact Assessments". (E.T. 25.01.2024), https://www.usda.gov/home/privacy-policy/privacy-impact-assessments

Uyarer, Sinem Göçmen. *Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması*. Ankara: Seçkin Yayınevi, 2020.

Üçüncü, S. Hilal. *Medeni Yargılama Hukukunda Kişisel Verilerin ve Sırların Korunması.* İstanbul: Oniki Levha Yayıncılık, 2019.

Vural, Yılmaz. "Veri Mahremiyeti: Saldırılar, Korunma ve Yeni Bir Çözüm Önerisi". *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*. 4/2 (2018):21-34. (E.T. 13.05.2023), https://dergipark.org.tr/tr/download/issue-file/18543

Yalçın, Atakan. "Avrupa Birliği Genel Veri Koruma Tüzüğünde Hesap Verilebilirlik Araçları". İçinde *Kişisel Verilerin Korunmasına Uzman Bakış Uzmanlık Tezleri Derleme Çalışması,* ed. Pınar Çağlayan Aksoy ve Hüseyin Can Aksoy. Ankara: KVKK Yayınları, No 44, 2023.

Yılmaz, Hasan. “TS ISO/IEC 27001 Bilgi Güvenliği Yönetimi Standardı Kapsamında Bilgi Güvenliği Yönetim Sisteminin Kurulması ve Bilgi Güvenliği Risk Analizi”. *Denetişim*. 15 (2014): 45-59. (E.T. 17.09.2023) https://dergipark.org.tr/tr/pub/denetisim/issue/22466/240291

Yosif, Umniyahasghar. “Kişisel Verilerin İşlenmesi Şartları ve 6698 Sayılı Kişisel Verilerin Korunması Kanununun Ruhu Olarak Genel İlkeler”. *Selçuk Üniversitesi Adalet Meslek Yüksekokulu Dergisi*. 4/ 1 (2021):1-22, 4, (E.T. 02.07.2023), https://dergipark.org.tr/tr/download/article-file/1748966

Yücedağ Göztepe, Nafiye. “Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu’nun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri”. *İstanbul Hukuk Mecmuası*. 75/2 (2017): 765-790. (E.T. 24.09.2023) www.idealonline.com.tr

Yücedağ, Nafiye. “Kişisel Verilerin Korunması Kanunu Kapsamında Genel İlkeler”. *Kişisel Verileri Koruma Dergisi*. 1 /1 (2019), 47-63. (E.T. 02.07.2023), https://dergipark.org.tr/tr/pub/kvkd/issue/45759/566993

Yüksek, Furkan Kaan. "AİHM İçtihatlarında Kişisel Verilerin Korunması", *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, 25 (2023): 371-420, (E.T. 14.06.2023), https://dergipark.org.tr/tr/pub/deuhfd/issue/76624/1276294

“Faaliyet Raporu”, Kişisel Verileri Koruma Kurumu, (E.T. 07.09.2023), https://www.kvkk.gov.tr/Icerik/2094/ Faaliyet-Raporu

“İlgili form ve kılavuz”, (E.T. 15.05.2024), https://ihlalbildirim.kvkk.gov.tr/

“What is GDPR, the EU’s new data protection law?” (E.T. 07.05.2023), https://gdpr.eu/what-is-gdpr/

2022 Faaliyet Raporu, Kişisel Verileri Koruma Kurumu, (E.T. 22.06.2023), https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/aae3c721-9da4-43c7-95a68d14e6413 a36.pdf