Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü
Özel Hukuk Anabilim Dalı

KİŞİSEL VERİLERİN KORUNMASI YÜKÜMLÜLÜĞÜNÜN İHLALİNDEN DOĞAN HUKUKİ SORUMLULUK

Kemal KÜÇÜKKAVRUK

Yüksek Lisans Tezi

Ankara, 2023

KİŞİSEL VERİLERİN KORUNMASI YÜKÜMLÜLÜĞÜNÜN İHLALİNDEN DOĞAN HUKUKİ SORUMLULUK

Kemal KÜÇÜKKAVRUK

Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü
Özel Hukuk Anabilim Dalı

Yüksek Lisans Tezi

Ankara, 2023

KABUL VE ONAY

Kemal KÜÇÜKKAVRUK tarafından hazırlanan “Kişisel Verilerin Korunması Yükümlülüğünün İhlalinden Doğan Hukuki Sorumluluk” başlıklı bu çalışma, 09.06.2023 tarihinde yapılan savunma sınavı sonucunda başarılı bulunarak jürimiz tarafından yüksek lisans tezi olarak kabul edilmiştir.

Prof Dr. Erkan KÜÇÜKGÜNGÖR (Başkan)

Dr. Öğr. Üyesi Günhan GÖNÜL KOŞAR (Danışman)

Doç. Dr. Yıldız ABİK (Üye)

Doç. Dr. BURCU GÜLSEREN ÖZCAN BÜYÜKTANIR (Üye)

Dr. Öğr. Üyesi Tuğçe ORAL MANAV (Üye)

Yukarıdaki imzaların adı geçen öğretim üyelerine ait olduğunu onaylarım.

Prof.Dr. Uğur ÖMÜRGÖNÜLŞEN

Enstitü Müdürü

YAYIMLAMA VE FİKRİ MÜLKİYET HAKLARI BEYANI

Enstitü tarafından onaylanan lisansüstü tezimin tamamını veya herhangi bir kısmını, basılı (kağıt) ve elektronik formatta arşivleme ve aşağıda verilen koşullarla kullanıma açma iznini Hacettepe Üniversitesine verdiğimi bildiririm. Bu izinle Üniversiteye verilen kullanım hakları dışındaki tüm fikri mülkiyet haklarım bende kalacak, tezimin tamamının ya da bir bölümünün gelecekteki çalışmalarda (makale, kitap, lisans ve patent vb.) kullanım hakları bana ait olacaktır.

Tezin kendi orijinal çalışmam olduğunu, başkalarının haklarını ihlal etmediğimi ve tezimin tek yetkili sahibi olduğumu beyan ve taahhüt ederim. Tezimde yer alan telif hakkı bulunan ve sahiplerinden yazılı izin alınarak kullanılması zorunlu metinleri yazılı izin alınarak kullandığımı ve istenildiğinde suretlerini Üniversiteye teslim etmeyi taahhüt ederim.

Yükseköğretim Kurulu tarafından yayınlanan ***"Lisansüstü Tezlerin Elektronik Ortamda Toplanması, Düzenlenmesi ve Erişime Açılmasına İlişkin Yönerge"*** kapsamında tezim aşağıda belirtilen koşullar haricince YÖK Ulusal Tez Merkezi / H.Ü. Kütüphaneleri Açık Erişim Sisteminde erişime açılır.

- Enstitü / Fakülte yönetim kurulu kararı ile tezimin erişime açılması mezuniyet tarihimden itibaren 2 yıl ertelenmiştir. (1)
- Enstitü / Fakülte yönetim kurulunun gerekçeli kararı ile tezimin erişime açılması mezuniyet tarihimden itibaren ….. ay ertelenmiştir. (2)
- Tezimle ilgili gizlilik kararı verilmiştir. (3)

……/……/……

Kemal KÜÇÜKKAVRUK

[1] *"Lisansüstü Tezlerin Elektronik Ortamda Toplanması, Düzenlenmesi ve Erişime Açılmasına İlişkin Yönerge"*

*(1) Madde 6. 1. Lisansüstü tezle ilgili patent başvurusu yapılması veya patent alma sürecinin devam etmesi durumunda, tez **danışmanının** önerisi ve **enstitü anabilim dalının** uygun görüşü üzerine **enstitü** veya **fakülte yönetim kurulu** iki yıl süre ile tezin erişime açılmasının ertelenmesine karar verebilir.*

*(2) Madde 6. 2. Yeni teknik, materyal ve metotların kullanıldığı, henüz makaleye dönüşmemiş veya patent gibi yöntemlerle korunmamış ve internetten paylaşılması durumunda 3. şahıslara veya kurumlara haksız kazanç imkanı oluşturabilecek bilgi ve bulguları içeren tezler hakkında tez **danışmanının** önerisi ve **enstitü anabilim dalının** uygun görüşü üzerine **enstitü** veya **fakülte yönetim kurulunun** gerekçeli kararı ile altı ayı aşmamak üzere tezin erişime açılması engellenebilir.*

*(3) Madde 7. 1. Ulusal çıkarları veya güvenliği ilgilendiren, emniyet, istihbarat, savunma ve güvenlik, sağlık vb. konulara ilişkin lisansüstü tezlerle ilgili gizlilik kararı, **tezin yapıldığı kurum** tarafından verilir *. Kurum ve kuruluşlarla yapılan işbirliği protokolü çerçevesinde hazırlanan lisansüstü tezlere ilişkin gizlilik kararı ise, **ilgili kurum ve kuruluşun önerisi** ile **enstitü** veya **fakültenin** uygun görüşü üzerine **üniversite yönetim kurulu** tarafından verilir. Gizlilik kararı verilen tezler Yükseköğretim Kuruluna bildirilir.*
Madde 7.2. Gizlilik kararı verilen tezler gizlilik süresince enstitü veya fakülte tarafından gizlilik kuralları çerçevesinde muhafaza edilir, gizlilik kararının kaldırılması halinde Tez Otomasyon Sistemine yüklenir.

***** Tez **danışmanının** önerisi ve **enstitü anabilim dalının** uygun görüşü üzerine **enstitü** veya **fakülte yönetim kurulu tarafından karar verilir.***

ETİK BEYAN

Bu çalışmadaki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi, görsel, işitsel ve yazılı tüm bilgi ve sonuçları bilimsel ahlak kurallarına uygun olarak sunduğumu, kullandığım verilerde herhangi bir tahrifat yapmadığımı, yararlandığım kaynaklara bilimsel normlara uygun olarak atıfta bulunduğumu, tezimin kaynak gösterilen durumlar dışında özgün olduğunu, Dr. Öğr. Üyesi Günhan GÖNÜL KOŞAR danışmanlığında tarafımdan üretildiğini ve Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü Tez Yazım Yönergesine göre yazıldığını beyan ederim.

Kemal KÜÇÜKKAVRUK

ÖZET

KÜÇÜKKAVRUK, Kemal. *Kişisel Verilerin Korunması Yükümlülüğünün İhlalinden Doğan Hukuki Sorumluluk*, Yüksek Lisans Tezi, Ankara, 2023.

Bu çalışma kapsamında kişisel verilerin korunması yükümlülüğü, bu yükümlülüğünün hangi yollarla ihlal edilebileceği ve bu ihlallerden doğan hukuki sorumluluk incelenmiştir. Çalışmamız üç bölümden oluşmakta olup ilk bölümde kişisel verilerin korunması ihtiyacının doğuşundan başlayarak, kişisel veri tanımı, kapsamı ve mevzuatın gelişim süreci incelenmiştir. Yine aynı bölümde 6698 sayılı Kişisel Verilerin Korunması Kanunu ile bu Kanunun hazırlanmasında temel alınan mevzuat olan 95/46/AT sayılı Direktif ve bu düzenlemeyi ilga eden Avrupa Veri Koruma Tüzüğü karşılaştırılmıştır. İkinci bölümde kişisel verilerin korunmasına ilişkin temel kavramlar incelenmiş akabinde veri ihlallerinin neler olduğu konusu açıklanmıştır.

Üçüncü bölümde ise kişisel verilerin korunması yükümlülüğünün ihlalinden doğan hukuki sorumluluk incelenmiştir. Çalışmamızın üçüncü bölümü özellikle KVKK'da yer alan düzenlemelerin, genel hükümler çerçevesinde hukuki sorumluluğun şartlarının ve bu sorumluğun kapsamının değerlendirilmesi açısından önemlidir. Bu kapsamda mevcut yargı kararlarına, literatürdeki farklı görüşlere yer verilerek hukuki sorumluluk dayanakları ve başvurulabilecek hukuki yollar incelenmiştir.

Anahtar Sözcükler

Kişisel veri, kişisel verilerin korunması, maddi tazminat, manevi tazminat, hukuki sorumluluk, kusur.

ABSTRACT

KÜÇÜKKAVRUK, Kemal. *Legal Liability for Violation of the Obligation to Protect Personal Data*, Master Thesis, Ankara, 2023.

Within the scope of this study, the obligation to protect personal data, the ways in which this obligation can be violated and the legal responsibility arising from these violations are examined. Our work consists of three parts. In the first part, starting from the emergence of the need for the protection of personal data, the definition of personal data, its scope and the development process of the legislation were examined. Again in the same section, the Personal Data Protection Law numbered 6698 and the Directive 95/46/EC, which is the basis for the preparation of this Law, and the European Data Protection Regulation, which abolished this regulation, were compared. In the second part, the basic concepts related to the protection of personal data are examined and then the subject of data breaches is explained.

In the third part, the legal responsibility arising from the data breach is examined. The third part of our study is especially important in terms of evaluating the terms of legal responsibility and the scope of this responsibility within the framework of the regulations and general provisions of the KVKK. In this context, the basis of legal liability and the legal remedies that can be applied are examined by giving place to the existing judicial decisions and different opinions in the literature.

Keywords

Personal data, protection of personal data, material compensation, moral compensation, legal liability, fault.

İÇİNDEKİLER

KISALTMALAR

AB	:	Avrupa Birliği
ABD	:	Amerika Birleşik Devletleri
ABAD	:	Avrupa Birliği Adalet Divanı
Anlaşma 108	:	Kişisel Verilerin Otomatik İşleme Tâbi Tutulması Karşısında Bireylerin Korunması Sözleşmesi
AÜHF	:	Ankara Üniversitesi Hukuk Fakültesi
AÜHFD	:	Ankara Üniversitesi Hukuk Fakültesi
Aydınlatma Tebliği	:	Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ
BATIDER	:	Bankacılık ve Ticaret Enstitüsü Dergisi
Bkz.	:	Bakınız
C.	:	Cilt
CD	:	Ceza Dairesi
CGK	:	Ceza Genel Kurulu
E	:	Esas No
HD	:	Hukuk Dairesi
HGK	:	Hukuk Genel Kurulu
HMK	:	Hukuk Muhakemeleri Kanunu
K	:	Karar No
Kurul	:	Kişisel Verilerin Korunması Kurulu
Kurum	:	Kişisel Verilerin Korunması Kurumu
KVİS	:	Kişisel Veri İşleme Sözleşmesi
KVKK	:	Kişisel Verilerin Korunması Kanunu
OPI	:	Open Graph API
s.	:	Sayfa
S.	:	Sayı
T	:	Tarih
TBK	:	Türk Borçlar Kanunu
TCK	:	Türk Ceza Kanunu
TMK	:	Türk Medeni Kanunu
Tüzük	:	Avrupa Veri Koruma Tüzüğü
VERBİS	:	Veri Sorumluları Sicil Bilgi Sistemi

vd.	:	Ve Devamı
Veri Silme Yönetmeliği	:	Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik
YÜHFD	:	Yeditepe Üniversitesi Hukuk Fakültesi
95/46/AT	:	95/46/AT sayılı Direktif

GİRİŞ

Yirminci yüzyılın bittiği yirmi birinci yüzyılın başladığı dönemde insanlık tarım ve sanayi devrimlerinin ardından üçüncü büyük devrim olan bilişim devrimini yaşadı. Bilişim devrimi ise tüm beşeri faaliyetlerin sanal mecralara aktarılması anlamına gelen dijitalleşmeyi doğurdu.

Dijitalleşme yeni iş modellerini, platformları, sosyal medyayı yaratırken reklamcılık, ticaret, aracılık, iletişim gibi birçok faaliyetin biçimini de değiştirdi. İnsanlar günlük faaliyetlerinin büyük çoğunluğunu teknolojik cihazlarla yapmaya başladı ve bunun sonucunda çevrim içi mecralarda haracanan zaman arttı. Çevrim içi mecralarda harcanan zamanın artışı dijital platform ekosistemini artarak beslemeye devam etti.

Ancak bu ve buna benzer hizmetleri sunan dijital teşebbüsleri kullanabilmek için insanların kişisel verilerini paylaşmak zorunda kalmaları dijital dünyanın yadsınamaz gerçeğiydi. Nihayetinde çevrim içi alışveriş yapmak isteyen bir kullanıcı ismini ve soy ismini, ödeme bilgilerini, adresini ve hangi ürünlere ihtiyacı olduğunu satış yapan platformla paylaşmak zorundaydı. Aynı şekilde sevdikleriyle hayatındaki gelişmeleri paylaşmak isteyen biri sosyal medyaya üye olurken ve sosyal medya platformunu kullanırken isim soy isim, yaş, hobi, siyasi görüş, yaşadığı yer, konum, meslek, sosyal çevre gibi bilgileri doğrudan paylaşmak zorunda kalıyordu.

Bu bilgilerin bilişim sistemlerince kaydedilmesi, kişilerin profillenmesi ve ticari amaçlarla kullanılması sonucunda bu verilere sahip olan teşebbüsler rekabetçi açıdan çok büyük avantaj elde etmeye başladılar. Bu durumun olağan sonucu ise dijital hizmet sunana teşebbüsler kısa zamanda dünyanın en büyük şirketleri haline geldi. Google, Facebook, Amazon, Meta, Tencent, Disney, Netflix gibi şirketler yalnızca dijital hizmetler sunarak kısa sürede ve hızlı biçimde büyüdü.

Verinin bu denli büyük bir ekonomik değer taşıması şirketlerin veri işleme iştahlarını artırdı. Kişiler ise özel hayatlarını ve kişilik haklarını tehdit edecek nitelikteki verileri kendi rızaları ve yasal gereklilikler olmaksızın işleyenlere karşı savunmasız konumdaydı. İşte bu gelişmeler veri koruma hukukuna duyulan

ihtiyacı önemli ölçüde artırdı. Böylece oldukça yeni bir hukuk alanı olan kişisel verilerin korunması kısa sürede oldukça önemli hale geldi.

Özellikle AB ülkeleri kişisel verilerin korunması hakkını temel haklardan bir tanesi olarak kabul etmiş ve bu hakkı korumaya yönelik kapsamlı mevzuatlar hazırlamıştır. Öncelikle 95/46/AT hazırlanarak yürürlüğe konulmuş ancak AB üye ülkelerin mevzuatlarının uyumlaştırılması ve kişisel verilerin korunması amaçları için yetersiz kalması nedeniyle yeni bir mevzuat hazırlama ihtiyacı doğmuştur. Avrupa Birliği Genel Veri Koruma Tüzüğü (Tüzük) bu ihtiyacı karşılamak maksadıyla hazırlanan çok daha detaylı ve dijital gelişmelerin doğurduğu ihtiyaçları da kapsayan hükümler içeren bir mevzuattır. Bu nedenlerle Tüzük hazırlanarak uygulanmaya başlamış ve 95/46/AT ilga edilmiştir.

AB ülkelerindeki bu gelişmelerin akabinde 2010 yılında Anayasamızın 20. maddesine "*Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir.*" hükmü eklenmiş ve 95/46/AT temel alınarak Kişisel Verilerin Korunması Kanunu (KVKK) hazırlanmıştır. KVKK bugün hala yürürlükte olup ülkemizde kişisel verilerin korunmasına ilişkin idari sürecin temel yapısını düzenleyen mevzuat konumundadır.

Üç bölümden oluşan çalışmamız kapsamında birinci bölümde kişisel verilerin genel çerçevesi kapsamı, sınırları, kişisel verilerin korunması fikrinin ortaya çıkışı hususları ele alınmıştır. Kişisel verilerin korunması hakkının hukuki statüsü ve bağımsız bir hak olup olmadığı tartışmalarına değinilmiş sonuç olarak kişilik hakkı olarak değerlendirilmesi gerektiği tespit edilmiştir.

Akabinde mevcut AB düzenlemesi olan Tüzükte ve KVKK'da düzenlenen haklar ve sunulan olanaklar kıyaslanarak incelenmiş ve mevzuat anlamında KVKK'nın eksik olduğu noktalara eleştiriler getirilmiştir. Tüzükte yer alan bilgilendirme hakkı, düzeltme hakkı, unutulma hakkı, verilerin tasarımla korunması, veri işleme faaliyetini kısıtlama hakkı, çocuklara ait kişisel verilerin korunmasına yönelik hükümler, veri taşınabilirliği hakkı, erişim hakkı, itiraz hakkı, otomotik karar vermeye ilişkin haklar, varsayılan ayarlarla koruma gibi huşuların KVKK ile karşılaştırarak incelenmiştir. Tazminat hükümleri özelinde Tüzük hükümleri ve KVKK hükümleri AB'deki kişisel veri ihlallerinden doğan zararın tazminine ilişkin usule değinilmiştir.

İkinci bölümde veri koruma hukukunun temel kavramları olan veri işleme, veri kayıt sistemi, ilgili kişi, veri sorumlusu, veri işleyen, ortak veri sorumlusu kavramları incelenmiştir. Bu kavramlar KVKK ve Kurul tarafından hazırlanan ikincil mevzuat çerçevesinde ele alınmış ve ilgili kararlara değinilerek somutlaştırılmıştır. Yine aynı bölüm içerisinde kişisel verilerin korunması mevzuatının hangi yollarla ihlal edilebileceği mahkeme ve Kurul kararlarına yer verilerek incelenmiştir.

Üçüncü bölüm ise çalışma kapsamında detaylı olarak ele alınmak ve değerlendirilmek istenen kişisel veri ihlallerinden doğan sorumluluğun incelendiği kısımdır. Öncelikle genel hükümler çerçevesinde kişilik hakkı ihlali durumunda başvurulabilecek yollar ve başvuru şartları incelenmiş akabinde KVKK'da tazminata ilişkin hükümler ele alınmıştır. Özellikle KVKK'da yer alan düzenlemeler kapsamında kusur kelimesinin ilgili madde lafzında geçmemesi nedeniyle kusursuz sorumluluk olarak değerlendirilip değerlendirilemeyeceği analiz edilmiştir. KVKK m.11, 12 ve 14 hükümlerinde yoğunlaşılmış olup sorumluluğunun türünün tespiti için literatür ve içtihattan faydalanılmıştır. Bu noktada maddi manevi tazminat davaları ve açılabilecek diğer davalar tespit edilmiştir. Bu davalarda izlenecek usul, yetkili ve görevli mahkeme de bu bölümde incelenmiştir.

Özetle sonuç kısmında mevzuatın ve uygulamanın vaziyeti literatürden, yargı kararlarından ve AB ülkelerindeki uygulamalardan yola çıkılarak değerlendirilmiş ve çalışmada varılan sonuçlara yer verilmiştir.

1. BÖLÜM: KİŞİSEL VERİ KAVRAMI VE KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN MEVZUAT

1.1. KİŞİSEL VERİ KAVRAMINA İLİŞKİN GENEL ÇERÇEVE

Günümüzde kişisel veri kavramının tanımı ve özellikleri bilinmekle birlikte genel çerçevesi ve kapsamı hakkında tartışmalar mevcuttur. Bu başlık altında kişisel veri kavramının tanımı ve kapsamı, kişisel verilerin değeri, korunmasının önemi ve veri koruma hukukunun kronolojisi incelenecek olup ayrıca kişisel verinin hukuki niteliği tespit edilmeye çalışılacaktır.

1.1.1. Kişisel Verinin Korunması Fikri

Devletlerin toplumu düzenleyen ve bireyi koruyan kurallar koymaya başladığı ilk çağlardan itibaren kişilere ilişkin bazı bilgilerin gizli kalmasının istenebileceği fikri ortaya çıkmıştır. Bu istek belirli meslek gruplarının sır saklama yükümlülüğü getirmesini gerektirmiştir.

En eski mesleklerden biri olan hekimlik sır saklama yükümlülüğü olan mesleklerin başında gelmektedir. Sır saklama yükümlülüğü çerçevesinde hekimlerden hasta mahremiyetine ilişkin yemin etmeleri ve bu yemine sadık kalmaları beklenmektedir. 2500 yıl önce oluşturulan, Hipokrat yemini olarak bilinen ve hekimlik mesleğinin gereği olarak günümüzde de kullanılan[1] metinde "t*edavi sırasında veya tedavi dışında insan hayatında görüp işittiklerim hakkında sessiz kalacağım ve bu tür şeyleri konuşmayacağım.*" beyanı mevcuttur.[2] Kişisel mahremiyeti sağlamaya yönelik bu basit bir kuralın yüz yıllardır uygulanması iyiniyetli bir çaba olmakla birlikte modern hukuk kuralları ile desteklenmediği takdirde kişisel verilerin korunabilmesi için yetersizdir.[3]

Yüz yıllar önce benzeri bir sır saklama yükümlülüğü getirilmesi ihtiyacı duyulan bir diğer meslek grubu ise din adamlarıdır. Din adamları, meslekleri gereği kişilerin kendisi harici hiç kimsenin bilmesini istemeyeceği bilgileri

---

[1] 1973 yılında düzenlenen 27. Dünya Tıp Birliği toplantısında hekim hasta ilişkisinde yer alan gizliliğin kaynağının iki sebebe dayandığı ifade edilmiş olup bu sebepler hekimlerin sır saklama borcu ve hastaların kişisel dokunulmazlığıdır.

[2] **Başbuğ**, Aydın: Hekimin Yükümlülükleri ve Hukuki Sorumluluğu, II. Sağlık Hukuku Sempozyumu, Kuzey Kıbrıs Türk Cumhuriyeti, Lefke Avrupa Üniversitesi, 17-18 Mayıs 2010. s. 132.

[3] Nitekim hekim tarafından tanı veya tedavi sürecinde edinilen bilgiler kişisel sağlık verisidir. Bu veri grubu ise özel nitelikli veri olarak kabul edilmektedir. **Abik**, Yıldız: "Kişisel Sağlık Verilerinin Medeni Hukuk Bakımından Korunması", II. Uluslararası Tıp Hukuku Kongresi Bildirileri Kitabı (Ed. Hakeri/Doğan), Ankara 2018, s. 541.

edinebilmektedir. Ancak bu bilgileri toplumun diğer fertleriyle paylaşması ihtimali kişileri din hizmeti almaktan alıkoyabilir. Dolayısıyla insanlar verdiği bilgilerin güvende olduğundan emin olmak isteyecektir. Yine bu ihtiyaç üzerine din adamlarının da kendilerine aktarılan bilgileri mesleki sır olarak saklamaları gerekmektedir.

Bir diğer sık saklama yükümlülüğü ise avukatlık mesleğinde mevcuttur. Avukat müvekkil ilişkisi sebebiyle, avukatın öğrendiği bilgileri üçüncü kişilerle paylaşması yasaklamaktadır. Avukata yüklenen bu sorumluluğun amacı müvekkili ile arasındaki güven ilişkisine dayanarak elde ettiği bir takım bilgilerin üçüncü kişilere aktarılmasını engellemektir.[4] Sır saklama yükümlülüğünün hedefi kişisel verileri korumak olmamakla birlikte özel hayatın korunmasını amaçladığı değerlendirildiğinde sır saklama yükümlülüğü ve kişisel verilerin korunması hükümlerinin benzer amaçları taşıdığı görülmektedir.

Avukatlık Kanunu[5] m. 36'da yer alan düzenleme "*Avukatların, kendilerine tevdi edilen veya gerek avukatlık görevi, gerekse, Türkiye Barolar Birliği ve barolar organlarındaki görevleri dolayısıyla öğrendikleri hususları açığa vurmaları yasaktır.*" şeklindedir. Ancak ilerleyen bölümlerde aktarılacağı üzere veri koruma hukuku avukatlara sır saklama yükümlülüğüne göre çok daha kapsamlı yükümlülükler getirmektedir. Örneğin müvekkilin iletişim bilgileri sır olmamakla birlikte kişisel veri kapsamına dahil olduğundan sır saklama yükümlülüğü kapsamında korunmazken veri koruma hukuku kapsamında korunmaktadır.

Akademik anlamda bakıldığında ise kişisel verileri koruma fikri ilk kez 1890 yılında Amerika Birleşik Devletleri'nde (ABD) Samuel D. Warren and Louis Brandeis isimli iki avukat tarafından kaleme alınmıştır.[6] Ancak bu çalışma o dönem yalnızca kişisel verilerin korunmasına ilişkin ihtiyacı tespit etmeyi sağlamış, bir mevzuat çalışması yapılması için yeterli olmamıştır.

Kişisel verilerin korunması ile doğrudan ilgili olmamakla birlikte, 1948 yılında, İnsan Hakları Evrensel Beyannamesinin 12. maddesinde gizlilik hakkı

---

[4] **Boran Güneysu**, Nilüfer/**Memiş**, Burak: Kişisel Verilerin Korunması Kanunu Kapsamında Avukatın Yükümlülük ve Sorumlulukları, Anadolu Üniversitesi Hukuk Fakültesi Dergisi, C. 5, S. 2, 2019, s. 321.

[5] 19/3/1969 tarih ve 1136 sayılı Avukatlık Kanunu.

[6] **Warren**, D. Samuel/ **Brandeis**, Louis: "The Rigth to Privacy", Harvard Law Review, C. 4, S. 5, 1890, s. 197 vd.

eklenmiştir. Yalnızca kişinin özel hayatı, ailesi, konutu veya yazışmaları ile ilgili müdahalelere ve şeref ve şöhretine saldırılara karşı kanun ile koruma gerektiği ifade edilmiştir.[7]

1950 yılına gelindiğinde ise Avrupa İnsan Hakları Sözleşmesi'nin (AİHS) ayrı bir başlığı altında kişisel verilerin korunması düzenlenmemiştir. Ancak özel hayata ve aile hayatına saygı başlıklı 8. maddesinde özel hayatın gizliliğine ilişkin temel hükümlere yer vermiştir.[8] İleride detaylarına yer verilecek olmakla birlikte Anayasamızda ve TCK'da kişisel verilere ilişkin düzenlemelere özel hayatın gizliliği başlığı altında yer verilmektedir. Aynı zamanda literatürdeki bazı yazarlara göre kişisel verilerin korunması hakkı, özel hayatın gizliliği başlığı altında kategorize edilmelidir.[9] Dolayısıyla 1950'de AİHS'de yapılan bu değişikliğin veri koruma hukukuna katkı sağladığını kabul etmek yanlış olmayacaktır.[10]

1967 yılında ABD'de yürürlüğe giren Bilgi Edinme Özgürlüğü Yasası herkese devlet kurumlarından kendisiyle ilgili belgelere erişim talep etme hakkı vermiştir. 1980 yılında Ekonomik İşbirliği ve Kalkınma Teşkilatı, ticari işlemleri kaydetmek amacıyla artan bilgisayar kullanımı hakkında, veri koruma rehberi yayınlamıştır. 1981 yılına gelindiğinde Avrupa Konseyi, Kişisel Verilerin Otomatik İşleme Tâbi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'ni (Anlaşma 108) kabul ederek mahremiyet hakkını yasal bir zorunluluk haline getirmiştir. [11]

---

[7] İlgili hüküm "Hiç kimse özel hayatı, ailesi, meskeni veya yazışması hususlarında keyfi karışmalara, şeref ve şöhretine karşı tecavüzlere maruz bırakılamaz. Herkesin bu karışma ve tecavüzlere karşı kanun ile korunmaya hakkı vardır." şeklindedir.

[8] "*1. Herkes özel ve aile hayatına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahiptir. 2. Bu hakkın kullanılmasına bir kamu otoritesinin müdahalesi, ancak ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, dirlik ve düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlâkın veya başkalarının hak ve özgürlüklerinin korunması için demokratik bir toplumda gerekli olan ölçüde ve yasayla öngörülmüş olmak koşuluyla söz konusu olabilir."*

[9] İleride detaylı değinilecek olmakla birlikte katıldığımız görüş kişisel verilerin korunması hakkının bağımsız bir hak olduğu görüşüdür. Ancak Anayasamız, TCK ve bazı yargı kararlarında özel hayatın gizliliği hakkının altında kategorize edildiği görülmektedir.

[10] **Başalp,** Nilgün: Kişisel Verilerin Korunması ve Saklanması, Yetkin Yayınları, Ankara, 2004, s. 10.

[11] 8 Kasım 2001 tarih ve 181 sayılı Kişisel Verilerin Otomatik İşleme Tâbi Tutulması Karşısında Bireylerin Korunması Sözleşmesine Ek Denetleyici Makamlar ve Sınır Aşan Veri Akışına İlişkin Protokol ile ülkelerde kişisel verilerin korunması alanında görevli denetleyici veri koruma kurumu kurulması ve 108 sayılı Sözleşme'yi kabul etmeyen diğer ülkelere yapılacak veri aktarımlarına ilişkin standartlar getirilerek alıcı devlet veya uluslararası organizasyonların gerekli düzeylerde koruma sağlaması kuralları eklenmiştir. Yaşanan teknolojik gelişmeler gerekçe gösterilerek 18 Mayıs 2018'de 108 sayılı Kişisel Verilerin Otomatik Olarak İşleme Tâbi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'ni yenileyen Protokol ile bir takım değişiklikler yapılmıştır. Veri

1995 yılında Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bağlamında Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Birliği Konseyi Yönergesi Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin 95/46/AT sayılı Direktif[12] (95/46/AT) yürürlüğe konularak AB üyesi ülkelerin kişisel verilerin korunmasına ilişkin ulusal mevzuat hazırlaması ve bu mevzuatların birbiriyle uyumlu olması hedeflenmiştir.

AB üyesi ülkeler tarafından 2000 yılında kabul edilen AB Temel Haklar Şartı'nda, kişisel verilerin korunması hakkına da yer verilmiş ve temel bir insan hakkı olduğu ifade edilmiştir. Ardından kapsamlı bir mevzuat hazırlamak için çalışmalara 2012 yılında başlanmış ve yaklaşık 4 yıllık çalışma sonucunda, 2016 yılında Tüzük hazırlanmış ve AB parlamentosu tarafından onaylanmıştır. Tüzük, AB üyesi ülkelerin gerekli hazırlıkları yapabilmesi için tanınan iki yıllık sürenin dolduğu 2018 yılından itibaren uygulanmaya başlanmıştır.[13]

Ülkeler açısından bakıldığında ise kişisel verilerin korunmasını amaçlayan ilk düzenlemenin 1970 yılında Almanya'nın Hessen eyaletinde kabul edildiği bilinmektedir[14]. ABD'de 1974 yılında[15], İsveç'te[16], Fransa'da[17] ve Almanya'da[18] 1978 yılında, Lüksemburg'da 1979 yılında[19], kişisel verileri korumayı amaçlayan mevzuatlar yürürlüğe girmiştir. Ayrıca, İngiltere'de 1984 yılında Veri Koruma Kanunu[20], Kanada'da 1985 yılında Özel Yaşamın Gizliliği Yasası[21] uygulamaya konulmuştur.

Ülkeler tarafından hazırlanan ulusal mevzuatlar yukarıda yer verdiğimiz uluslararası rehberler ve mevzuatlar yayınlandıkça bu mevzuatlara uygun

---

koruma mekanizması genişletilmiş, şeffaflığa yönelik eklemeler yapılmış, amaç kısmı kapsamlı hale getirilmiştir.

[12] 24 Ekim 1995 tarihinde yürürlüğe giren 95/46/AT, 24 Mayıs 2016 tarihinde GDPR'nin yürürlüğe girmesiyle mülga hale gelmiştir.

[13] https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en Erişim Tarihi: 10.01.2023.

[14] 30 Eylül 1970 tarihli Essen Veri Koruma Kanunu (Hessisches Datenschutzgesetz).

[15] ABD Privacy Act (Gizlilik Kanunu).

[16] İsveç Veri Kanunu.

[17] 6 Ocak 1978 Bilgisayarlar, Veriler ve Özgürlüklere İlişkin Kanun.

[18] Federal Veri Koruma Kanunu.

[19] Veri Koruma Kanunu.

[20] https://www.legislation.gov.uk/ukpga/1984/35/enacted Erişim Tarihi:10.01.2023.

[21] Privacy Act (R.S.C., 1985, c. P-21).

biçimde yeniden düzenlenmiştir. Özellikle 95/46/AT ve Tüzük İngiltere'de dahil olmak üzere Avrupa ülkelerinin mevzuatlarını büyük ölçüde değiştirmiştir.[22]

Kişisel verilerin korunması fikri ve bu yolda atılan adımlar izlendiğinde veri işleme faaliyetinin yazının bulunuşu ile başladığını kabul ettiğimizde mevzuat gelişiminin veriyi otomatik biçimde işleyen sistemlerin gelişimi ile paralellik gösterdiği anlaşılmaktadır. Özellikle yirminci yüz yılın ikinci yarısından itibaren verilerin dijital ortama aktarılması ile veri işleme olanakları ve işlenen veri miktarı artmış buna paralel olarak da veri güvenliğini sağlamak zorlaşmıştır.

Veri güvenliğini sağlama ihtiyacına uygun biçimde 1970'lerden itibaren ulusal mevzuatlar hazırlanmış 2000'li yıllardan itibaren ise mevzuatlar çok daha detaylı koruma sağlamayı amaçlamıştır. Kişisel verilerin korunmasına kapsamına hangi veriler dahil olur kişisel veri tanım ve kapsamına girmeyen veriler hangileri belirlemek de tarihsel gelişimin sonunda mümkün olmuştur.

1.1.2. Kişisel Veri Kavramının Tanımı ve Kapsamı

1.1.2.1. KVKK Öncesi Dönemde Kişisel Verilerin Tanımı ve Kapsamı

KVKK'nın yürürlüğe girmesiyle birlikte kişisel veri tanımı ve kapsamı konusu netleşmiştir. Ancak KVKK öncesinde de çeşitli mevzuatlarda, yargı kararlarında ve literatürde farklı tanımlar mevcuttur.

Bunlardan ilki Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik[23] ile yapılmıştır. İlgili yönetmelikte, kişisel veri "*tanımlanmış ya da doğrudan veya dolaylı olarak, bir kimlik numarası ya da fiziksel, psikolojik, zihinsel, ekonomik, kültürel ya da sosyal kimliğinin, sağlık, genetik, etnik, dini, ailevi ve siyasi bilgilerinin bir ya da birden fazla unsuruna dayanarak tanımlanabilen gerçek ve/veya tüzel kişilere ilişkin herhangi bir bilgi*…" olarak tanımlanmıştır.

Yine KVKK öncesi süreçte Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik'te[24] kişisel veri kavramı "*belirli veya kimliği belirlenebilir gerçek ve tüzel kişilere ilişkin bütün bilgileri*" ve

---

[22] **Duman**, Berat: Anayasa Hukukunda Kişisel Verilerin Korunması, Doktora Tezi, Selçuk Üniversitesi, Konya, 2020, s. 12.
[23] 6 Şubat 2004 tarihli ve 25365 sayılı Resmi Gazete'de yayımlanan Yönetmelik.
[24] 24 Temmuz 2012 tarihli ve 28363 sayılı Resmi Gazete'de yayımlanan Yönetmelik.

kişisel veri gizliliğinin ihlali ise "*istem dışı, yetki dışı ya da yasa dışı olarak; kişisel verilerin tahrip edilmesine, kaybolmasına, iletilmesine, değiştirilmesine, depolanmasına veya başka bir ortama kaydedilmesine, işlenmesine, ifşa edilmesine ve söz konusu verilere erişilmesine neden olan güvenlik ihlali*" olarak tanımlanmıştır.

KVKK öncesi yargı kararlarında da kişisel veri tanımı yapılmamış olup kişisel veri kavramı yaşam şekline ilişkin veriler, ekonomik ve finansal veriler, bilişim alanına ilişkin veriler, sağlıkla ilgili veriler, politik kişisel veriler olmak üzere beş başlık altında tasnif edilmiştir.[25]

Yargıtay, bu tasnifi yaparken doktrinden yararlandığını ilgili kararda açıkça belirtmiştir. Atıf yapılan görüşler incelediğinde ise kişisel veri tanımlarının KVKK-3/d'de yer alan tanımlamaya benzer olduğu görülmektedir. Bu atıflardan biri "*Bireyin şahsi, mesleki ve ailevi özelliklerini gösteren, o bireyi diğer bireylerden ayırmaya ve niteliklerini ortaya koymaya elverişli her türlü bilgiyi ifade eder.*"[26] Şeklindeyken bir diğer ise "*Bir kişinin adı ve soyadı, yaşı, cinsiyeti, doğum yeri, dini, TC kimlik numarası, cinsel hayatı, cep telefonu numarası, medeni durumu, ailesi, işi, geliri, borçları, adresi, geçirdiği hastalıklar, özel zevkleri ve buna benzer bilgileri*"[27] olarak yer almaktadır. TCK 135. ve 136. maddeleri ile ilgili olarak yapılan değerlendirmede kişisel verilerin gizli olması gerekmediği, burada korunan değerin sır olmadığı da açıkça ifade edilmiştir. Dolayısıyla ilgili karardan, kişisel verilere ilişkin koruma sağlanmasının ilgilisi tarafından gizlenmesi ile ilgili olmadığı da anlaşılmaktadır.[28]

Kişisel veri kavramının tanımına ve kapsamına ilişkin literatürde başka görüşlerde mevcuttur. Küzeci, kişisel veri kavramını "*belirli veya belirlenebilir bir kişinin kimliğine, etnik kökenine, fiziksel özelliklerine, sağlık durumuna, genetik verilerine, öğrenim veya istihdam durumuna, ikamet adresine, kredi kartına, banka bilgilerine, emniyet bilgilerine, düşünce ve inanç durumuna, alışveriş alışkanlıklarına, telefon rehberine, fotoğrafına, bilgisayarının IP adresine, parmak izine, smslerine, e-maillerine, sosyal paylaşım sitelerindeki aktivitelerine, önceki*

[25] Esas No: 2012/12-510 Karar No: 2014/331 Karar Tarihi.17.06.2014.
[26] **Şen**, Ersan: Türk Ceza Kanunu Yorumu, Vedat Kitapçılık, İstanbul, 2006, s. 601.
[27] **Sırabaşı**, Volkan: İnternet ve Radyo- Televizyon Aracılığıyla Kişilik Haklarına Tecavüz, Adalet Yayınevi, Ankara, 2007, 2. Bası, s.195.
[28] **Dülger**, Murat: Veri Koruma Hukuku, Hukuk Akademisi, İstanbul 2019, s.579.

gün yediği yemeğe kadar varan çeşitli özelliklerini içeren her türlü bilgi" şeklinde verileri örnekleme yoluyla sayarak tanımlamaktadır.[29]

Lloyd'un kişisel veri tanımı ise daha dar kapsamlı olup[30] "*kişiyi dolaylı olarak tanıtan kamera kaydı, ses veya görüntüsü, biyometrik yöntemlerle kişiliğinin belirlenmesini sağlayan parmak izi, yüz, iris, yazı, ses tanıma gibi yöntemlerle elde edilen verileri de içeren her türlü kişisel bilgi*" şeklindedir. Ancak bu tanıma daha önemsiz görünen ya da kamuoyuna açıklanmış verilerin de dahil edilmesi gerekmektedir.[31]

Murray tarafından yapılan tanım ise daha genel olup, belirli veya belirlenebilir bir gerçek kişiye ilişkin tüm bilgileri kişisel veri olarak kabul edilmelidir.[32] Literatürdeki tanımlar birbirine benzer olmakla birlikte kapsam açısından farklar olduğu anlaşılmaktadır.

Anayasa Mahkemesi kararında[33] ise kişisel veriye ilişkin "*Kişisel veri kavramı, belirli veya kimliği belirlenebilir olmak şartıyla, bir kişiye ilişkin bütün bilgileri ifade etmektedir.*" tanımı yer almaktadır. Görüldüğü üzere KVKK öncesinde verilen bir karar olmasına rağmen ilgili kararda yer alan kişisel veri tanımı ve KVKK'de yer alan tanım oldukça benzerdir.

KVVK'nın tasarı aşamasında hazırlanan Adalet Komisyonu raporunun[34] genel gerekçe bölümünde "*bireylerin kimliklerini belirli hale getirmeye elverişli her türlü bilgi*" tanımı yapılmış, kimlik, iletişim, sağlık ve mali bilgileri ile özel hayatına, dini inancına ve siyasi görüşüne ilişkin bilgilerin kişisel veri olduğu açıkça ifade edilmiştir.

KVKK öncesi dönemdeki mevzuat, yargı kararları ve literatürde genel itibariyle kişisel verilerin tanımının oluştuğu ve kapsamının belirlendiği anlaşılmaktadır. Nitekim KVKK öncesi mevzuatta yer alan tanım ve günümüzde KVKK'da yer alan

---

[29] **Küzeci**, Elif: Kişisel Verilerin Korunması, XII Levha Yayınları, İstanbul, 2020, s. 128.
[30] **Lloyd**, Ian: Information Technology Law, 6th Edition, Oxford University Press, Oxford, 2011, s. 39.
[31] **Arınmış Uzun**, Sündüs: "Türkiye'de Kişisel Verilerin Korunması ve Vatandaş Algısının Ölçülmesi", Bilişim Teknolojileri Dergisi, C.: 14, S. 3, 2021. s. 207.
[32] **Murray**, Alan: Information Technology Law (The Law and Society), Oxford University Press, Oxford, 2019.
[33] Anayasa Mahkemesi E. 2013/122, K. 2014/74, E. 2014/122 K. 2015/123 para. 20, E. 2015/32, K. 2015/102,12.11.2015.
[34] https://www.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf Erişim tarihi:14.12.2022.

tanım[35] oldukça benzerdir. Ayrıca yargı kararları ve literatürde bugünküne paralel şekilde geliştiği görülmektedir.

1.1.2.2. KVKK Sonrası Dönemde Kişisel Verilerin Tanımı ve Kapsamı

KVKK'ye göre kimliği belirli veya belirlenebilir bir kişiyle ilişkilendirilebilen veriler kişisel veri olarak ifade edilmektedir.[36] KVKK'de yer alan bu tanımdan anlaşılacağı üzere gerçek kişi ile ilişkilendirilebilen tüm bilgiler bu kapsamda değerlendirilmektedir. Dolayısıyla kişisel veri teriminin kapsamı oldukça geniştir. Örnekleme yoluyla ifade etmek gerekirse kişinin harcamaları, gittiği adresler, girdiği internet siteleri, sosyal çevresi, alışkanlıkları, iş geçmişi dahil kişiyi belirlenebilir kıldığı durumda kişisel veri kapsamına girmektedir.

AB mevzuatına bakıldığında da Tüzük'nin 4. maddesinde[37] "*kişisel veri tanımlanmış veya tanımlanabilir bir gerçek kişiye ilişkin her türlü bilgi...*" olarak tanımlanmıştır. Kişisel veri tanımı ve kapsamı açısından bakıldığında KVKK öncesi yargı kararları, KVVK'de yer alan tanım, literatür ve AB mevzuatı arasında kayda değer bir farklılık olmadığı görülmektedir.

KVKK kişisel verileri kendi içerisinde genel nitelikli kişisel veriler[38] ise özel nitelikli kişisel veriler olmak üzere ikiye ayırarak incelemektedir. KVKK'nin 6. maddesinde "*Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri*" tek tek sayılarak özel nitelikli verilerin neler olduğu belirlenmiştir.

Literatürde bu ayrıma gerekçe olarak özel nitelikli kişisel verilerin doğrudan temel hak ve özgürlüklerle ilişkili olması ve KVKK'nın bu haklara ilişkin daha kapsamlı

---

[35] Kişisel veri tanımı KVKK m. 3/1-d hükmünde yapılmış olup ilgili başlıkta yer verilecektir.
[36] KVKK m. 3/1-d hükmü şu şekildedir: "*Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi…*"
[37] İlgili maddede *"... isim, kimlik numarası, konum verileri, çevrim içi tanımlayıcı ya da söz konusu gerçek kişinin fiziksel, fizyolojik, genetik, ruhsal, ekonomik, kültürel veya toplumsal kimliği...*" Örnekleme yoluyla kişisel veri olarak sayılmıştır.
[38] KVKK m. 6. hükmünde özel nitelikli kişisel veri tanımı açıkça yer alırken genel nitelikli kişisel veri şeklinde bir tanım mevcut değildir. Özel nitelik arz etmeyen kişisel veriler için genel nitelikli kişisel veri ifadesi kullanılmaktadır.

koruma amaçlaması gösterilmektedir.[39] Uygulamada hangi verinin özel nitelikli kişisel veri niteliğini haiz olduğunu tespit etmek her durumda kolay olmamaktadır.

Örneğin kişinin siyasi görüşüne ilişkin bir bilginin veya geçirdiği hatalığın, kullandığı ilacın özel nitelikli kişisel veri olduğunu tespit etmek zor değildir. Ancak yalnızca bu örnekler değil örneğin bir şirketin müşterilerinin helal yemek tercihini kaydetmesi, işçilerin sendika kayıt bilgileri, siyasi bir derneğin üye kayıtları da özel nitelikli kişisel veridir.[40]

KVKK çerçevesinde ülkemizde kişisel veri ve özel nitelikli kişisel veri tanımına giren hususlarda getirilen koruma kapsamı farklı olup açık rıza hususu anlatılırken değinilecektir. Ayrıca KVKK kapsamında tanımlanan ve kişisel veri kapsamına girmediği anlaşılan anonim veri isimli bir veri grubu daha mevcuttur. Veri grubunun kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilmesi veya kaynağı belirlenmesi imkânsız hale getirilmesi sonucu ortaya çıkan veri yığını anonim veri olarak ifade edilmektedir. Örneklendirmek gerekirse istatistiki veriler, pazarlama veya planlama gibi amaçlarla tutulan yığın haline getirilmiş ve kişilerden bağımsızlaşmış veriler anonim veri olarak ifade edilir ve kişisel veri olarak kabul edilmezler.[41]

Özellikle büyük veri işleme faaliyetleri ve büyük verinin birçok sektörde aktif biçimde kullanılmaya başlamasıyla birlikte anonim veri kavramı önem kazanmıştır. Veriye erişim imkânı olan teşebbüsler bu verileri veri sahibinden bağımsız hale getirip yaş, coğrafya, cinsiyet, ırk, hastalık, siyasi görüş gibi somut kriterlere göre tasnif ederek pazarlama, siyaset, sağlık, ilaç ve tedavi geliştirme gibi alanlarda kullanmaktadır. Bu noktada tekrar belirtmek gerekirki veri sahibi gerçek kişinin hiçbir şekilde anlaşılma olanağı kalmadığı için bu veriler kişisel veri olarak değerlendirilmez ve kişisel verilerin tabi olduğu koruma ve saklama süreçlerine de tabi tutulmaz.

KVKK'da da anonim veri kavramı tanımlanmış ve mevzuat kapsamında olmadığı açıklanmıştır. KVKK'nın tanımlar başlıklı m. 3-1/b hükmünde anonim veri "*Kişisel*

---

[39] **Sefer**, Oğuz: "Kişisel Verilerin Korunması Hukukunun Genel İlkeleri", Bilgi Ekonomisi ve Yönetimi Dergisi, C. 13 S. 2, 2018, s. 127.
[40] **Dülger**, Murat Volkan: "Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması", İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi C. 3 S. 2, 2016, s. 110.
[41] **Başalp,** s. 34.

verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesi" olarak tanımlanmıştır. Bu tanımdan anlaşıldığı üzere kimliği belirli veya belirlenebilir gerçek kişi ile ilişkilendirilemeyen veriler anonim veridir ve KVKK kapsamında kişisel veri olarak değerlendirilmemektedir.[42]

1.1.3. Kişisel Verilerin Korunmasının Önemi

Veriye sahip olmak her alanda ve tarihin her döneminde başlı başına bir avantajdır. Bir ülke, bölge, şehir ya da kişi hakkında veri sahibi olmak pazarlama, savaş, siyaset dahil olmak üzere her alanda sahip olana kolaylık sağlamaktadır.

Endüstrileşmenin ve ticaretin gelişmesiyle birlikte üretim ve ticaret hacmi artmış buna paralel olarak da pazarlamaya verilen değer artmıştır. Pazarlama, alıcının ihtiyacını tespit etmeyi ve bu ihtiyaca uygun ürünleri kişiye sunmayı hedeflemektedir. Kişilerin ihtiyaçlarının tespiti noktasında ise yaş, cinsiyet, gelir, aile büyüklüğü gibi kişi hakkında temel veriler önem arz etmektedir. Bu önem, verinin otomatik yöntemlerle işlenmeye başlaması, ticari amaçlarla daha yoğun kullanılması ve kişiye yönelik reklamların daha etkili hale gelmesiyle katlanarak artmıştır.

Kişilerin profillenmesi başka bir deyişle dijital kimlikler oluşturulması ve bu kimliklere ait farklı verilerin birbiriyle ilişkilendirilmeye başlanması ilgili kişiye, ilgi alanlarına yönelik öneriler getirmeyi kolaylaştırmaktadır. Bu kapsamda neredeyse tüm şirketler sabit öneriler sunmak yerine kişinin tüketim alışkanlıklarına, zevklerine ve eğilimlerine göre ürün farklılaştırmasına gitmektedir. Kişilere yönelik profillemeler geleneksel satış kanallarında da kullanılmakla birlikte dijital dünyada daha yaygın biçimde kullanılmaktadır.

Kişiselleştirilmiş reklamcılık yöntemleri, kişinin zevklerine göre sayfa akışı sunan sosyal medya platformları tamamıyla kullanıcıdan topladığı verilere göre hizmetlerini kişiselleştirmektedir. Bu durumun sonuçları ise kişinin verilerinin daha değerli hale gelmesi, bu tür hizmetler sunabilmek için daha fazla veriye ihtiyaç duyulması ve teşebbüslerin veri toplamak için daha agresif davranmaya başlamasıdır. Nitekim veriyi doğru biçimde işlemeyi bilen şirketler son 20 yıllık süreçte rakiplerinin ciddi biçimde önüne geçmiştir. Özellikle e-ticaret, çok taraflı

[42] **Dülger**, Murat Volkan: Veri Koruma Hukuku, s. 110.

platform hizmetleri, arama motorları, sosyal medya hizmetleri, politik faaliyetler, sağlık hizmetleri, insan kaynakları alanlarda veriye sahip olmak rekabette büyük avantaj yaratmaktadır.

Özellikle "big tech" olarak isimlendirilen Amazon, Facebook, Google, gibi teşebbüsler verinin getirdiği avantajlarla yeni sektörlere girerken müşteri hedefleme ve ürün beklentileri gibi konularda avantaj elde ederken veriye erişimi olamayan şirketler ise dezavantajlı konuma gelmiştir. Büyük şirketler ellerindeki veri yığınları yardımıyla kişilerin ihtiyaçlarını daha doğru biçimde tespit ederek doğru alanlara yatırımlarını kaydırmayı başararak daha çabuk büyürken veriye erişemeyen teşebbüsler ise bir iş alanına girerken daha büyük belirsizliklerle karşı karşıya kalmaktadır.

Verinin çok kullanıldığı alanların başında üretim ve pazarlama geldiği kabul edilmekle birlikte siyasi alanda kullanımının da etkili olduğu görülmektedir. Kişilerin ideoloji ve eğilimlerinin tespit edilmesi ve bu eğilimleri tetiklemeye yönelik siyasi söylemlerin kullanılması arzusu politik alanda kişisel verilerin önemini artırmaktadır.

Nitekim son yılların en büyük veri sızıntılarından biri ticari alanda değil siyasi alanda oldukça önemli sonuçlar doğurmuştur. Facebook, 2010 yılından itibaren platform üzerinde çalışabilen çeşitli oyunlar, eğlenceli testler ve kullanıcı bilgilerinden faydalanabilen uygulamalar yazılmasına olanak tanıyan Open Graph API (OPI) isimli ara yüzü kullanıma sunmuştur.[43] Bu ara yüz aracılığıyla geliştiriciler kişilerin yaş, lokasyon, doğum yeri, beğenileri gibi bilgileri uygulamalarında kullanabiliyordu. Bu aynı zamanda kişileri gruplandırmak ve bilgileri üzerinden kişilik analizi yapmak isteyen biri için iyi bir fırsattı.

Cambridge Analytica isimli politik araştırma ve propaganda şirketi kişileri gruplandıran beşli kişilik testini uygulamak için Facebook'un OPI ile sunduğu bilgilerin yeterli olduğunu fark etmiştir. Akabinde Amazon'un Mechanical Turk hizmetini kullanarak Facabook kullanıcılarının Cambridge Analiytica'ya erişim izni vermesini sağlamıştır. Ancak Facebook'un, kullanıcılarının bilgilerini

[43] **Aksoy**, Abdulkadir/**Türkölmez**, Onur: "Dijital Çağa Demokrasiyi Çağırmak: Cambridge Analytica Skandalı", Journal of Political Administrative And Local Studies (JPAL) May 2020, Cilt:3, Sayı:1, s. 50.

arkadaşlarına görme imkanı sunan yapısı sayesinde birçok Facebook kullanıcısı izin vermediği halde Cambridge Analiytica veri havuzuna dahil olmuştur. 2018 yılında detayları ile ortaya çıkan bu veri sızıntısı skandalı sonrası ilgili şirketin elindeki veri havuzu kişilerin duygu durumuna göre sınıflandırılmasını sağlamış ve adaylar kampanyalarında doğru zamanda doğru söylemleri kullanarak veri sahiplerini büyük oranda manipüle etmeyi başarabilmiştir.[44]

Facebook veri sızıntısı iki yönüyle önemlidir. Bunlardan ilki veri sızıntısı sebebiyle veri sahiplerinin manipülasyona karşı savunmasız kalması ikincisi ise veriye sahip olmayan adayların rakiplerine karşı dezavantajlı kalmasıdır. 2016 ABD Başkanlık seçimlerinde homojen seçmen grupları oluşturmuş ve 4.000 ayrı reklam kampanyası yürütmüştür.[45] Rakip bir aday bir bölge veya şehir için bir veya birkaç reklam kampanyası yürütürken Cambridge Analiytica tarafından yürütülen kampanya çok daha etkili olmuştur.[46]

Diğer taraftan en fazla elde edilmek istenen veri gruplarından biri sağlık verileridir.[47] Veri ihlallerinin sektörlere göre dağılımını incelendiğinde sağlık verilerinin ilk sıralarda olduğu tespit edilmektedir.[48] Hastalıkların teşhis ve tedavi süreçleri ve önleyici sağlık faaliyetleri için doğru ve güvenilir verilere ihtiyaç duyulmaktadır. Kişisel sağlık verilerine erişen bir teşebbüs yaş gruplarına göre hastalıkların etkilerini, potansiyel sağlık risklerini, hastalıkların yayılım yöntemlerini, uzun vadede hastalıkların yaratacağı tehlikeleri bilecek ve rakip teşebbüslere göre avantajlı konuma gelecektir.[49] Bu nedenlerle sağlık verileri büyük ticari değere sahip olmakla birlikte aynı zamanda kişilerin en mahrem verileri konumundadır. Kişilik hakkı kapsamında, kişinin fiziki veya mental sağlığıyla ilgili veriler gizli kalması gereken bilgilerdir. Sağlık verileri, ilgili kişinin

---

[44] **Isaak**, Jim/**Hanna**, J. Mina: "User Data Privacy: Facebook, Cambridge Analytica, And Privacy Protection," Computer, 2018, C. 51, S. 8, s. 58.
[45] **Persily**, Nathaniel: "The 2016 US Election: Can democracy survive the internet?", Journal of Democracy C. 28, S. 2, 2017.
[46] **Evan**, Oddleifson: The Effects of Modern Data Analytics in Electoral Politics: Cambridge Analytica's Suppression of Voter Agency and the Implications for Global Politics, Political Science Undergraduate Review, C. 5, 2020, s. 47.
[47] **Long**, Cheng/ **Fang**, Liu/**Danfeng**, Yao: "Enterprise Data Breach: Causes, Challenges, Prevention, And Future Directions", Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, C. 7, S. 5, 2017, s.3.
[48] **Hicaham**, Hammouchi/**Othmane**, Cherqi/**Ghita**, Mezzour/**Mounir** Ghogho/**El Koutbi**, Mohammed: Digging Deeper İnto Data Breaches: An Exploratory Data Analysis Of Hacking Breaches Over Time, Procedia Computer Science, 2019, s. 151.
[49] **Belle**, Ashwin/**Thiagarajan**, Raghuram/**Soroushmehr**, Reza/**Navidi**, Fatemeh/**Beard**, Daniel/**Najarian**, Kayvan: Big Data Analytics In Healthcare, Biomed Research International, 2015.

özel hayatının en mahrem alanlarında biridir. Bu sebeplerle, herkesin özel hayatına saygıyı ve sağlık verilerinin gizliliğini talep hakkı mevcuttur.[50]

Kısaca değinilen örneklerden de anlaşılacağı üzere birçok alanda teşebbüsler açısından veri elde etmek rakiplerinin önüne geçme olanağı sunmaktadır. Bu olanak teşebbüslerin veri elde etme konusunda iştahını artırmakta olup kişisel verilerin korunması gerekliliği günden güne artmaktadır. Bir hizmeti sunan veya ürün satan bir teşebbüsün rıza dahilinde veya özel bir mevzuatın gereği olarak kişisel veri işlemesi elbette olağan ve daha iyi hizmet sunabilmek için gerekli bir durumdur. Nihayetinde veri setleri doğru biçimde işlendiğinde yine insanlığın faydasına sonuçlar doğurmaktadır. Birçok insan kendi zevkine göre sosyal medya akışları yaratılmasını veya aniden ortaya çıkan bir hastalığa kısa sürede tedavi bulunmasını isteyecektir. Bu sonuçları elde edebilmek için ise veri toplanması ve işlenmesi gerekmektedir.

Diğer taraftan bireyler kendi verilerinin ne düzeyde ve ne amaçla toplanacağını ve güvenliğinin nasıl sağlanacağını da bilmek isteyecektir. Dolayısıyla bireyler verilerinin işlenmesine izin verse dahi sürecin şeffaf biçimde yürütülmesini, verilerinin doğru biçimde korunmasını ve bu süreçlerin yetkili kamu otoritelerince denetlenmesini isteyecektir. Bu isteğin olağan sonucu da kişisel verilerin korunmasını hususunun son derece önemli olduğudur.

1.1.4. Kişisel Verilerin Korunması Hakkının Hukuki Niteliği

Verinin önemi başlığı altında aktardığımız üzere verinin ekonomik değeri mevcuttur bu nedenle pazarlama ve ürün geliştirme başta olmak üzere birçok alanda ihtiyaç duyulmaktadır. Ancak kişiler verilerinin sınırsız bir biçimde işlenmesini arzu etmemekte ve gizliliklerinin korunmasını beklemektedir. Bu beklentinin karşılığı olarak ortaya çıkan kişisel verilerin korunması hakkının hukuki niteliğini incelemek gerekmektedir.

Öncelikle ABD veri koruma hukukunda kişisel verilerin korunması hakkının temelinde ekonomik bir hak olduğu görüşü hakimdir.[51] Kişisel verilerin, kişiye ait olması nedeniyle arada mülkiyet bağı olduğunu iddia eden bir görüş mevcuttur.

---

[50] **Küçükgüngör**, Erkan: Tıbbi Kayıtlarda Sır Saklama Yükümlülüğü, Ankara Barosu III. Sağlık Hukuku Kurultayı, 7-8 Mayıs, Ankara 2011, s. 554.

[51] **Weber**, Rolf/**Dominic**, Staiger: Transatlantic Data Protection In Practice Basel, Springer, Basel, 2017, s. 39-54.

Ekonomik hak olduğu görüşünün temelinde verinin maddi değeri yatar ve bu görüş üretim ve ekonomik gelişme için şirketlerin veriye ihtiyaç duyduğunu varsayarak veri korumayı zorunlu seviyede tutmayı hedeflemektedir. Bu görüş kendi içinde ikiye ayrılmakta olup bunlarda mülkiyet hakkı olduğu görüşü ve fikri mülkiyet hakkı olduğu görüşleridir.

1.1.4.1. Mülkiyet Hakkı Olduğu Görüşü

Kişisel verileri ve kişi arasındaki hukuki ilişkinin mülkiyet hakkı kapsamında değerlendirilmesi gerektiği görüşüne göre veri tamamıyla bir eşyadır. Bu nedenle alma satma ve kiralama gibi hukuki ilişkilere konu olabilir.

21 yüzyılın getirdiği yeni ekonomide verinin petrol kadar değerli olduğunu savunan görüş kişisel verileri mülkiyet hakkı kapsamında ve oldukça sınırlı biçimde korumaktadır.[52] ABD örneğine bakıldığında veri koruma hukuku sağlık sektörü, adli kayıtlar ve bankacılık sektörü gibi birkaç alanda kişisel verilerin korunmasını amaçlayan mevzuattan ibarettir. Bu yaklaşıma göre kişi kendi mülkiyetindeki bir mal üzerinde tasarrufta bulunabildiği gibi verileri üzerinde de oldukça geniş biçimde tasarrufta bulunabilir.

1.1.4.2. Fikri Mülkiyet Hakkı Olduğu Görüşü

Kişinin düşünce ve emeğinin ürünü olarak değerlendirilen resim, film, kitap gibi eserler üzerinde fikri mülkiyet hakkı mevcuttur. Bu ürünler kişinin bireysel eseri niteliğindedir.

Fikri mülkiyet bireylere kendi eserleri üzerinde bir mülkiyet hakkı tanırken, veri koruma hukuku ise kişilerin verilerine yetkisiz erişimi engellemeyi hedeflemektedir. Bu görüşe göre adı geçen iki hukuk alanı, birlikte yeni bir hukuk alanı yaratmak için elverişli ortak zemine sahiptir. Kişi fikri mülkiyet hukuku kapsamında eserinin mülkiyetini üçüncü bir kişiye devredebilir ancak yine de bu eserle manevi bağını sürdürmesine engel değildir bu yaklaşımdan yola çıkılarak verinin de üçüncü kişilere verilebileceği ancak benzer bir manevi bağın devam edeceği savunulmaktadır.[53]

---

[52] **Karlıdağ**, Serpil: “Ekonomi Politik Açıdan Kişisel Verilerin Korunması”, Amme İdaresi Dergisi C. 46, S. 1, 2013, s. 138.
[53] **Küzeci**, s. 66.

İki hukuk alanı amaçları açısından birbirinden tamamıyla farklılaşmaktadır. Veri koruma hukuku veri sahibinin, kendi kişisel verileri üzerindeki haklarını korumayı, bu verilere izinsiz erişimleri engellemeyi, keyfi biçimde kişinin verilerinin kayıt edilmesi ve işlenmesini engellemeyi hedeflemektedir. Fikri mülkiyet hukuku ise bilim insanı, yazar, ressam veya eser niteliğinde üretim yapan benzeri mesleklerin eser üzerindeki haklarını korumayı amaçlamaktadır. Eser sahipleri fikri mülkiyet hakları kapsamında eserlerini satabilir, kiralayabilirler veya kullanım haklarını devrederek gelir elde edebilmektedir. Ancak veri koruma hukuku açısından baktığımızda verinin satılması, kiralanması veya benzer nitelikte maddi amaçlar için sunulmasını düzenleyen hükümler mevcut değildir.[54]

1.1.4.3. Temel İnsan Hakkı Olduğu Görüşü

ABD hukuk kökenli ekonomik hak yaklaşımlarına karşın Avrupa ve Türk hukukunda ağırlıklı olarak kabul gören görüş ise kişisel verilerin korunmasının temel bir insan hakkı olduğu görüşüdür.

Kıta Avrupası hukukuna göre kişisel verilerin korunması, verinin değerinin artması ve dijitalleşmenin bir sonucu olarak kişiliğin korunmasının bir parçasıdır ve zorunludur. Bu kapsamda yukarıda yer verdiğimiz kişisel verilerin korunması fikri başlığı altında değindiğimiz üzere kişisel verilerin korunması AİHS ve dahil olmak üzere AB tarafından hazırlanan birden fazla antlaşma ve mevzuatta insan hakkı olarak yer almıştır.[55]

1.1.4.4. Kişisel Verilerin Korunmasının Bağımsız Bir Hak Olduğu Görüşü

Kişisel verilerin korunmasını hakkının temel bir insan hakkı olduğu kıta Avrupası hukukunda kabul edilmekle birlikte bağımsız bir hak olup olmadığı hususu literatürde ve mahkeme kararlarında tartışmalıdır. Bu hususta iki farklı görüşün olduğu görülmektedir.

Bu görüşlerden ilki kişisel verilerin korunması hakkının özel hayatın gizliliği hakkının alt başlığı olduğudur. Bu görüşü savunanlara göre kişisel verilerin korunması hakkı, özel hayatın gizliliği hakkından çeşitli yönleriyle farklılaşan

---

[54] **Göçmen Uyarer**, Sinem: 6698 Sayılı Kişisel Verilerin Korunması Kanunu ve 5237 Sayılı Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması, Yüksek Lisans Tezi, Galatasaray Üniversitesi, İstanbul 2019, s. 9.

[55] Lizbon Sözleşmesi ve Anlaşma 108 kapsamında da kişisel verilerin korunması hakkı temel bir hak olarak kabul edilmiştir.

ancak yine benzer amaçları taşıyan bir haktır. Bir başka deyişle kişisel verilerin korunması hakkı, özel hayatın gizliliğinin özel bir görünümü olarak değerlendirilmelidir.[56]

Nitekim kişisel verilerin korunması hakkı, Anayasada özel hayatın gizliliği başlığı altında düzenlenmiştir. İleride değinileceği üzere benzeri bir sistematik TCK'da mevcuttur. Bunun yanı sıra kişisel verilerin korunması hakkını özel hayatın gizliliği hakkına dayandırarak gerekçelendiren yargı kararları da mevcuttur.[57]

İkinci görüş ise kişisel verilerin korunmasının özel hayatın gizliliği ile ilgisi olmakla birlikte ayrı bir hak olarak kabul edilmesi gerektiğidir. Aksi takdirde kişisel veri olmakla birlikte gizli olmayan bilgilerin üçüncü kişiler tarafından izinsiz işlenmesi ve kullanılması mümkün olacaktır. Kişisel verinin gizli olması zorunlu olmadığı gibi özel hayatla ilgili olmaması da mümkündür.

Yargıtay, mağdurun üzerinde damatlık ve eşinin üzerinde gelinlikle birlikte çekildikleri fotoğrafın ifşa edilmesinin özel hayatın gizliliğinin ihlal etmediği ancak TCK m. 136'da düzenlenen hukuka aykırı biçimde verileri verme veya ele geçirme suçu kapsamında değerlendirilebileceğine hükmetmiştir.[58]

Yine bir diğer Yargıtay kararında benzer biçimde kişinin gündelik kıyafetleriyle çekildiği ve kendi Twitter hesabında paylaştığı bir fotoğrafının, fotoğraf sahibinin rızası dışında, bir başkası tarafından Facebook üzerinden paylaşılması özel hayatın gizliliği kapsamında değerlendirilemeyeceği bu nedenle görüntü veya seslerin üçüncü kişilere duyurulması suretiyle özel hayatın gizliliğini ihlal suçundan mahkum edilemeyeceği ancak verileri hukuka aykırı olarak verme veya ele geçirme suçundan mahkumiyet hükmü kurulabileceğine hükmedilmiştir.[59]

İlgili yargı kararlarından da anlaşılacağı üzere özel hayatın gizliliği ve kişisel verilerin korunması uygulama alanı olarak benzeşmekle birlikte birebir örtüşmemektedir. Özel hayatın gizliliği hükümleri kapsamında kişinin

---

[56] **Kaya**, Kübra: "Özel Hayatın Gizliliği Hakkı ile Kişisel Verilerin Korunması Hakkı Bağlamında Ortaya Çıkan Bir Hak Olarak Unutulma Hakkının Değerlendirilmesi", Türkiye İnsan Hakları ve Eşitlik Kurumu Akademik Dergisi, C. 5 S. 8, 2022, s.181, **Çelik**, Yeşim: "Özel Hayatın Gizliliğinin Yansıması Olarak Kişisel Verilerin Korunması Ve Bu Bağlamda Unutulma Hakkı", Türkiye Adalet Akademisi Dergisi, S. 32, s. 391 vd.
[57] Danıştay 12. Dairesi'nin E. 2005/6811 K. 2006/1959 sayı ve 15.05.2006 tarihli kararı.
[58] Yargıtay 12. CD 2019/6342 E. , 2021/3092 K.
[59] Yargıtay 12. CD 2020/2426 E. , 2021/6589 K.

korunamadığı ve kişisel verilerinin kullanıldığı örnekler mevcuttur. Bu bilgiler ışığında kişisel verilerin korunması bağımsız bir haktır ve farklı bir menfaati korumaktadır yorumunu yapmak uygun olacaktır.

Kişisel verilerin korunmasının bağımsız bir hak olduğunun kabulüyle birlikte nitelik itibariyle kişilik hakkı olup olmadığı da incelenmelidir. Literatürde kişilik hakkı "*kişinin toplum içindeki saygınlığını ve kişiliğini serbestçe geliştirmesini sağlayan varlıkların tümü üzerindeki hak*" olarak tanımlanmaktadır.[60]Kişilik hakkı mutlak haklardandır dolayısıyla vazgeçilmesi ve devredilmesi olanaksızdır.[61]

Güncel Yargıtay içtihadında kişilik hakkı kavramı "…*kişi kavramını da içinde barındıran kişinin, kişi olmasından ötürü sahip olduğu, hak ve fiil ehliyeti ile hukuk düzeninin korunmaya değer bulduğu maddi ve manevi kişisel değerleri üzerindeki mutlak hak.*" şeklinde tanımlanmıştır.[62] Ancak kişilik hakkının kapsamına neler gireceğinin tespit kolay değildir.[63] Dolayısıyla uygulamada her bir olayda kişilik hakkının ihlal edilip edilmediği somut olayda değerlendirilmektedir.[64]

Kişisel verilerin korunması hakkı hukuki olarak kişilik hakkını temel almakla birlikte yukarıda açıklandığı üzere özel hayatın gizliliği kapsamında değil bağımsız bir hak olan "*kişisel verinin kaderini tayin hakkı- right to informational self-determination*" olarak tanımlanmış ve kişilik hakkı olarak kabul edilmiştir.[65]

---

[60] **Dural**, Mustafa/**Öğüz**, Tufan: Türk Özel Hukuku Cilt II Kişiler Hukuku, Filiz Kitabevi, İstanbul 2013, s. 100; **Canbolat**, Ferhat/**Gönül Koşar**, Günhan: Basın Yoluyla Kişilik Hakkının İhlalinin Tespitinde Kullanılan Yargıtay ve Avrupa İnsan Hakları Mahkemesi Ölçütlerinin Değerlendirilmesi, TBB Dergisi, S. 151, 2020, s. 265; **Kılıçoğlu**, Ahmet: Şeref, Haysiyet ve Özel Yaşama Basın Yoluyla Saldırılardan Hukuksal Sorumluluk, Turhan Kitabevi 4. Bası, Ankara, 2008, s. 3. **Zevkliler**, Kişiler Hukuku, s. 263; **Velidedeoğlu**, Hıfzı Velet: Türk Medeni Hukuku, İstanbul, 1961, s. 83; **Helvacı**, Gerçek Kişiler, s. 95; **Hatemi**, Hüseyin: Kişiler Hukuku, 8. Bası, XII Levha Yayıncılık, İstanbul, Eylül 2020, s. 66; **Serozan**, Rona: Kişiler Hukuku, 6. Bası, Vedat Kitapçılık, İstanbul 2015

[61] **Akipek,** Jale/**Akıntürk**, Turgut/**Ateş**, Derya: Türk Medeni Hukuku Başlangıç Hükümleri Kişiler Hukuku, Beta Yayınları, İstanbul, 2020, s. 345; **Özsunay**, Ergun: Gerçek Kişilerin Hukuki Durumu, İstanbul, 1979. s. 96; **Tandoğan**, Şahsiyetin Korunması, s. 12-13; **Zevkliler**, Kişiler Hukuku, s. 267; **Dural**/**Öğüz**, s. 100; **Oğuzman**/**Seliçi**/**Oktay**, s. 116.

[62] Yargıtay HGK, E: 2018/19-374, K: 2018/943, T: 25.04.2018

[63] **Serozan**, s. 455.

[64] **Özkan**, s. 36,37.

[65] **Hornung**, Gerrit/**Schnabel**, Christoph: Data Protection in Germany I: The Population Census Decision and The Right To Informational Self Determination, Computer Law & Security Report, 2009, C. 25, S. 1, s. 84.

Bu noktada hukuka aykırı biçimde gerçekleşen kişisel verilerin işleme faaliyetinin, aynı zamanda kişilik hakkı ihlâli teşkil edeceği anlaşılmaktadır.[66]

1.2. KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN MEVZUAT

Türkiye Anlaşma 108'i, 1981 yılında imzalamış ve böylece kişisel verilerin korunmasına ilişkin bir hukuki metni kabul etmiştir.[67] Ancak uzun yıllar boyunca ilgili sözleşmede yer alan hakkın mevzuatta düzenlenmesi konusuna değinilmemiştir.

İlk kez 2004 yılında[68] sektörel bir düzenlemede kişisel verilerin korunması amaçlanmış ardından 2005 yılında TCK'da kişisel verilerin korunmasını amaçlayan suç ve ceza hükümlerine yer verilmiştir. 2010 yılında Anayasanın "*Özel Hayatın Gizliliği*" başlıklı 20. maddesinin üçüncü fıkrasına ilgili hak eklenmiş ancak esas ve usullerini gösteren 6698 sayılı KVKK, 7 Nisan 2016 tarihinde yürürlüğe girmiştir.

Anayasa ve KVKK haricinde genel kanunlarda verilerin korunmasına ilişkin hükümler mevcuttur. Ancak kişisel verilerin korunmasına ilişkin detaylı hükümler ve veri koruma hukukuna ilişkin kavramlar KVKK'da ve ikincil mevzuatta düzenlenmiştir. Anayasada, KVKK'da, genel kanunlarda ve ikincil mevzuatta kişisel verilerin korunmasına ilişkin hükümlere aşağıda yer verilecektir.

1.2.1. Türkiye'de Kişisel Verilerin Korunmasını Düzenleyen Mevzuat

Bu başlık altında TR'de kişisel verilerin korunmasını düzenleyen genel mevzuat açıklanacak, veri koruma hukukuyla ilgili hükümlerden bahsedilecektir. Akabinde KVKK hükümleri ve ikincil mevzuat incelenecektir.

---

[66] **Taştan**, Furkan Güven: Türk Sözleşme Hukukunda Kişisel Verilerin Korunması, XII Levha Yayınları, İstanbul, 2017, s. 51; **Aksoy**, Hüseyin Can: Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması, Çakmak Yayınları s. 3; **Vuraloğlu**, Mehmet Oğuz: "Kişisel Verilerin İşlenmesi Suretiyle Kişilik Hakkı İhlalinde Kazancın Devri Talebi", YÜHFD, C. XV S. 1, 2020, s. 184.

[67] Eki olarak değerlendirilen 181 sayılı protokolü ise 2001 yılında imzalamıştır.

[68] 6.2.2004 tarih ve 25365 sayılı Resmi Gazete ile yürürlüğe giren Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik 24.07.2012 tarihinde yürürlükten kaldırılmıştır.

1.2.1.1. Türkiye'de Kişisel Verilerin Korunmasını Düzenleyen Genel Mevzuat

1.2.1.1.1. TC Anayasa'da Kişisel Verilerin Korunmasına İlişkin Hükümler

Anayasamızın özel hayatın gizliliğini korumayı amaçlayan 20/3. maddesine 12 Eylül 2010 tarihinde aşağıdaki hüküm eklenerek kişisel verilerin korunması hakkı düzenlenmiştir.

"*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...*"

Anayasal düzeyde koruma sağlanması zorunlu olmamakla birlikte kişisel verilerin korunmasına ilişkin anayasal düzenlemenin mevcut olması kişisel verilerin korunması hakkına önem verildiği biçiminde yorumlanmaya açıktır.[69] Ayrıca Anayasamızda eklenen kişisel verilerin korunmasına ilişkin düzenlemenin negatif statü hakları arasında yer alması veri güvenliği açısından devletin rolünü koruyucu bir statüde belirlemiştir.[70] Yani devlet hem kişisel alana müdahale etmemekle yükümlü kılınmakta hem de veri sahiplerini, veri işleyenlere ve üçüncü kişilere karşı korumakla yükümlü kılınmaktadır.

Anayasada yer alan hükümlerin ve taraf olunun uluslararası sözleşmelerin de bir gereği olarak KVKK hazırlanarak yürürlüğe konulmuştur. Ancak kişisel verilerin korunması bir hak olarak düzenlenmeden evvel TCK, TMK ve TBK'da kişisel verilerin korunmasına yönelik hükümler mevcuttur. Bu hükümlere ve yorumlarına ilgili başlıklar altında yer verilecektir.

1.2.1.1.2. Türk Ceza Kanunu'ndaki Kişisel Verilerin Korunmasına İlişkin Hükümler

TCK'nın Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar başlığı altında[71] 135-140. maddelerinde kişisel verilerin korunmasına ilişkin suçlar, nitelikli halleri ve

---

[69] ABD anayasal anlamda kişisel verilerin korunması hakkını kabul etmezken Kolombiya, Kanada, Honduras gibi ülkeler anayasal koruma sağlamayı tercih etmiştir.

[70] **Kılınç**, Doğan: "Anayasal Bir Hak Olarak Kişisel Verilerin Korunması", AÜHFD, C. 61 S. 3, 2012, s. 1099.

[71] TCK m. 132-140.

uygulanacak yaptırımlar düzenlenmiştir. TCK'da Kişisel Verilerin Kaydedilmesi Suçu (TCK 135), Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme Suçu (TCK 136), Verileri Yok Etmeme (TCK 138) olmak üzere üç farklı suç tanımlanmıştır.

TCK 137'de yukarıda yer verilen suçların nitelikli halleri, 139. maddede kişisel verilerin işlenmesine ilişkin suçların şikâyete tabi olduğu ve 140. maddede ise tüzel kişiler tarafından ilgili suçların işlenmesi halinde tüzel kişilere özgü güvenlik tedbirleri uygulanacağı düzenlenmiştir.

1.2.1.1.3. Türk Medeni Kanunu'ndaki Kişisel Verilerin Korunmasına İlişkin Hükümler

Yürürlükte olan 4721 sayılı Türk Medeni Kanununda kişisel verilerin korunmasını düzenleyen açık bir hüküm bulunmamaktadır. Ancak kişisel verilerin korunması hakkının kişilik hakkı olarak değerlendirilmesi[72] durumunda kişiliğin korunmasıyla ilgili hükümler olan TMK m. 23, 24 ve 25 hükümlerinin uygulanıp uygulanmayacağı hususu tartışılmalıdır.[73] Bu anlamda ilgili hükümleri veri koruma hukuku açısından incelemek uygun olacaktır.

TMK m. 23 kişilik haklarının sınırlaması ve kişilik haklarından vazgeçmeyi, m. 25 ilgili davaları düzenlemektedir. Kişilik haklarına saldırıyı düzenlemesi nedeniyle veri ihlallerine uygulanabilir görünen TMK 24. madde hükmü şu şekildedir:

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

Kişisel verilerin korunması hakkı, kişilik hakkı olarak değerlendirildiğinde TMK'da veri koruma hukuku alanını da kapsayan bir düzenlemenin mevcut olduğu kabul edilebilir. Bununla birlikte, soyut ve sınırları net olmayan bir düzenleme olması nedeniyle, KVKK'nın olmadığı bir hukuk düzleminde veri koruma hukukundan beklenen çözümü sunmaktan uzaktır.

---

[72] **Aksoy**, s. 35.
[73] **Akkurt**, Sinan Sami: "Kişisel Veri Kavramının Hukuki Niteliğine İlişkin Yaklaşımlara Mukayeseli Bir Bakış", Kişisel Verileri Koruma Dergisi, C. 2, S.1, 2020, s. 26.

Ancak KVKK'nın henüz yürürlüğe girmediği dönemde Yargıtay Hukuk Genel Kurulunun (HGK) unutulma hakkına dayanan kararında TMK m. 24'e atıf yaptığı görülmektedir.[74] İlgili kararın konusu bir cinsel taciz davasında yer alan isimlerin rumuzlanmaksızın mahkeme kararında yer aldığı haliyle bir ceza hukuku kitabına alınmasının haksız fiil teşkil ettiği ve manevi tazminata hükmedilmesi gerektiğidir.

İlgili kararda kişisel verilerin korunması hakkının kişilik hakkı ile ilişkili olduğu belirtilmiş, kişisel verilerin korunması hakkının amacının kişinin özel yaşamının korunması olduğu bunun da veri gizliliğinin güvence altına alınarak yapılabileceğine değinilmiştir. Aynı zamanda unutulma hakkına da değinilmiş olup özel hayatın gizliliğinin sağlanması olarak değerlendirilerek kişilik hakları arasında olduğu kabul edilmiştir.[75]

İlgili Yargıtay HGK kararından anlaşılacağı üzere kişisel verilerin korunması hakkı, kişilik hakkı olarak kabul edildiği takdirde TMK kapsamında yukarıda değinilen hükümler uygulama alanı bulabilmektedir. TMK kapsamında bir kişilik hakkı ihlali olduğu tespit edildiğinde bunun olağan bir sonucu olarak Türk Borçlar Kanununda (TBK) tazminata ilişkin hükümleri de uygulama alanı bulacaktır.[76]

1.2.1.1.4. Türk Borçlar Kanunu'ndaki Kişisel Verilerin Korunmasına İlişkin Hükümler

TBK'da doğrudan ve dolaylı biçimde kişisel verilerin korunmasını amaçlayan hükümler bulunmaktadır. Bu noktada öncelikle TBK'nın genel hükümlerine ardından özel hükümlerine bakarak ilgili hükümleri incelemek uygun olacaktır.

Hukuka aykırı biçimde kişisel verilerin işlenmesi veya mevzuat kapsamdaki yükümlülüklerinin gerektiği biçimde yerine getirilmemesi haksız fiil[77], sebepsiz zenginleşme, sözleşmeye aykırılık[78] ve vekaletsiz iş görme[79] hükümlerine yol

---

[74] Yargıtay HGK, E. 2014/56 K. 2015/1679 T. 17.6.2015 kararı.

[75] Yargıtay HGK tarafından alınan kararda şu ifade mevcuttur: "*Kişiye unutulma hakkının sağlanması ile birlikte özel hayatının gizliliği korunmuş olacaktır*" .

[76] Özel nitelikli kişisel veriler başta olmak üzere kişisel verilerin KVKK mevzuatının yanı sıra genel hükümler çerçevesinde de korunması gereklidir. **Abik**, Kişisel Sağlık Verilerinin Korunması, s. 536.

[77] **Gürpınar**, Damla: Kişisel Verilerin Korunamamasından Doğan Hukuki Sorumluluk , Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, C. 19 S. 3, 2017, s. 690.

[78] **Taştan**, s.120.

[79] **İmançlı**, Canan: Kişisel Sağlık Verilerinin Korunamamasından Doğan Özel Hukuk Sorumluluğu, XII Levha Yayınları, İstanbul 2020, s. 196, **Kılıçoğlu**, Ahmet: Medeni Hukuk, Turhan Kitabevi, Ankara 2016, s. 355.

açabilecek eylemlerdir.[80] İlgili hükümlerden hangilerinin uygulanabileceği veya uygulanıp uygulanamayacağının tespiti ancak somut olayda karşılaşınca tespiti mümkün olan hususlardır. Arada sözleşme ilişkisi olması, veri mahremiyetinin ihlal eden davranışın aynı zamanda haksız fiil oluşturup oluşturmadığı veya eylemin aynı zamanda vekaletsiz iş görme olarak nitelenip nitelenmeyeceğinin tespiti gerekmektedir.

Ayrıca kişisel verilerin korunması hakkının kişi hakkı olduğunu belirten görüşe göre TMK ve dolayısıyla TBK'nın uygulanacağını önceki başlıklarda belirtmiştir. TBK'nin kişilik haklarının zedelenmesi başlıklı m. 58'de yer alan düzenleme şu şekildedir:

"*Kişilik hakkının zedelenmesinden zarar gören, uğradığı manevi zarara karşılık manevi tazminat adı altında bir miktar para ödenmesini isteyebilir."*

Nitekim önceki başlık altında değinilen Yargıtay HGK kararında da TBK m. 58'e atıf yapılarak manevi tazminat ödenmesi gerektiğine hükmedilmiştir. TBK m. 58 hükmü KVKK'nın 14/3 maddesinde belirtilen tazminat hükmü sebebiyle de uygulama alanı bulabilecektir. İlgili maddede "*Kişilik hakları ihlal edilenlerin, genel hükümlere göre tazminat hakkı saklıdır.*" Hükmü yer almaktadır. Kişisel verilerin korunmasından doğan hukuki sorumluluk bu çalışmanın son bölümünde detaylı işleneceğinden detaylara girilmemekle birlikte tazminata ilişkin bir düzenlemenin KVKK'de yer almamasından genel hükümlere gidileceği yorumunu yapmak mümkündür.

1.2.1.2. Türkiye'de Kişisel Verilerin Korunmasın Düzenleyen Özel Mevzuat

1.2.1.2.1. Kişisel Verilerin Korunması Kanunu

2010 yılında kişisel verilerin korunması hakkının anayasaya eklenmesine rağmen temel mevzuat olan KVKK 6 yıl sonra yürürlüğe girmiştir. Arada geçen dönemde ise TCK hükümleri kapsamında kişisel verilerin korunmasına yönelik yargı kararları çıkmakla birlikte aşağıda yer vereceğimiz KVKK hükümleri mevcut olmadığından kişisel veri, veri işlenmesi, verinin anonimleştirilmesi gibi kavramlar uzun yıllar somutlaşmamıştır.

---

[80] Bu görüşler üçüncü bölümde detaylı biçimde tartışılacak olup bu bölümde yalnızca bahsedilecektir.

KVKK hazırlık sürecinde yürürlükte olan 95/46/AT ve Anlaşma 108 hükümleri esas alınmıştır.[81] İlgili direktif hükümleri incelendiğinde veri işleme kavramının temel alındığı, veri depolama ifadesinin bir işleme biçimi olarak değerlendirildiği, veri işlemeye ilişkin rıza, işleme şartları ve amaçların detaylı biçimde yer aldığı görülmektedir.[82]Bu direktif AB üyesi ülkelerin hazırlayacağı ulusal mevzuatların sınırlarını belirlemeyi hedeflemektedir. Bu bağlamda KVKK sistematiğini incelemek de uygun olacaktır.

KVKK'nın birinci bölümünde amaçları özel hayatın gizliliği ve kişilerin temel hak ve özgürlüklerin koruması, kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri, veri işleme ve saklama süreçlerinde uyacakları usul ve esasları düzenlemek olarak sayılmıştır. Kanunda yer alan düzenlemelere bakıldığında bu amaçlara yönelik hükümlere yer verilmiştir.

KVKK'nın ikinci bölümünde verilerin işlenme süreci, üçüncü bölümünde ilgili kişilerin hakları ve veri sorumlusunun yükümlülükleri, dördüncü bölümünde veri sorumlusuna başvuru ve sicile ilişkin hususlar, beşinci bölüm kişisel verilerin korunmasına ilişkin suç ve kabahatler düzenlenmiştir. Beşinci bölümde suçlar ayrıca düzenlenmeyip TCK 135-140. maddelere atıf yapılmış, kabahat oluşturan eylemler ise doğrudan düzenlenmiştir.[83]

KVKK verileri genel nitelikli veri ve özel nitelikli veri olmak üzere temelinde ikili bir ayrıma tabi tutmuştur. KVKK'nın 6. maddesinde özel nitelikli verilerin neler olduğu sayılmış ve bu verilere ilişkin veri işleme şartları genel nitelikli verilerden ayrılmıştır.

Kanun verilerin niteliklerinden bağımsız olarak ayrıca yurt içinde veri aktarılması ve yurtdışına veri aktarılması hususları düzenlenmiştir. Yurtdışına veri aktarılması kişinin açık rızasına veya belirli hallerde[84] Kurul'un vereceği izne bağlanmıştır. Kanun'un 9. maddesinde yer alan hükme göre açık rıza olmadan

---

[81] İlgili bölümde detaylı değinilecek olmakla birlikte Tüzük öncesi süreçte AB ülkelerinde uygulanan 95/46/AT'nin esas alınması, KVKK ve Tüzük arasında önemli farklılıkların oluşmasına yol açmıştır.

[82] **Elgesem**, Dag: "The Structure Of Rights In Directive 95/46/EC On The Protection Of İndividuals With Regard To The Processing Of Personal Data And The Free Movement Of Such Data", Ethics and Information Technology, S. 1, 1999, s. 284.

[83] KVKK m. 18.

[84] Bunlar KVKK m. 5/2 ve 6/3'te düzenlenmiş olup veri sahibinden izin alınmasını gerektirmeden veri işlenen hallerdir.

veri işlenen hallerde Kurul yurtdışına veri taşıma konusunda izin verirken verinin taşındığı ülkede yeterli koruma sağlanıp sağlanmadığı hususunu değerlendirmektedir. Eğer ilgili ülkede yeterli koruma sağlanmıyorsa bu durumda veri işleyenin gerekli düzeyde koruma sağlayacağını yazılı biçimde taahhüt etmesi gerekmektedir.

1.2.1.2.2. Kişisel Verilerin Korunması Hakkında İlke Kararları

KVKK'nın 15/6. maddesinde Kurul'a yapılan bir inceleme sonucunda sıklıkla ihlal yapıldığı düşünülen bir alanda ilke kararı alabilme yetkisi verilmiştir. Kurul ilke kararları ile bir kamu kurumuna veya bir sektörde faaliyet gösteren şirketlere yol gösterici olurken aynı zamanda birtakım yükümlülüklerde yükleyebilmektedir.[85] İlke kararları Kurumun benzer nitelikte çok sayıda ihlalle karşılaşmasını önleyerek iş yükünü azaltabileceği gibi aynı zamanda ülkemizde veri koruma kültürünün gelişmesine de katkı sunmaktadır.

Hukuki niteliği itibariyle ise ilke kararları genel, soyut ve objektif hükümler içermekte olup birel işlem niteliğinde değildir. Dolayısıyla KVKK ilke kararlarını yeni kurallar getiren düzenleyici işlemler olarak kabul etmek uygun olacaktır.[86]

1.2.1.2.3. Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmelik

Kişisel verilerin işlenmesi sürecine ilişkin KVKK ve ikincil mevzuatta düzenlemeler yer almaktadır. Ancak işlenen kişisel veriler bir süre sonra işlenme şartlarını kaybedebilir veya veri işleyen artık saklamak istemeyebilir. Bu gibi durumlarda işleme süreci boyunca hukuken korunan verinin akıbetinin düzenlenmesi gerekmektedir.

Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in (Veri Silme Yönetmeliği) m. 5 ve 6 hükümleri ile veri sorumlularının muhatapları aydınlatmak amacıyla bir veri saklama ve imha politikası oluşturması gerektiği düzenlenmiştir. Aynı zamanda silme, yok etme ve anonimleştirme

---

[85] Kurul'un 21/04/2022 tarih ve 2022/388 sayılı ilke kararı ile belediyelere ödeme ve borç hizmetleri konusunda dikkat etmesi gereken hususlar belirtilirken aynı zamanda kimlik doğrulamaya yönelik somut yükümlülükler getirildiği görülmektedir.

[86] **Başar**, Cemal: Türk İdare Hukuku ve Avrupa Birliği Hukuku Işığında Kişisel Verilerin Korunması, XII Levha Yayınları, İzmir, Haziran 2020, s. 291.

kavramları tanımlanmış ve teşebbüsün bu süreçlerde uyması gereken usul kuralları çizilmiştir.

1.2.1.2.4. Veri Sorumluları Sicili Hakkında Yönetmelik

Veri Sorumluları Sicili Hakkında Yönetmelik[87], veri işleme sürecine ilişkin karar alma yetkisine sahip olan veri sorumluları hakkındaki bilgileri şeffaf hale getirmeyi amaçlayan düzenlemedir. İlgili yönetmelik kapsamında veri sorumlularının veri işlemeye başlamadan evvel Veri Sorumluları Sicil Bilgi Sistemine kaydolması gerektiği (VERBİS), VERBİS'in tabi olduğu esaslar, kayıt yükümlülüğünün istisnaları, irtibat kişisi, veri sorumlusu temsilcisi kavramları ve görevleri tanımlanmıştır.

1.2.2. AB'de Kişisel Verilerin Korunmasını Düzenleyen Mevzuat

1.2.2.1. AB Temel Haklar Şartı

AB üyesi ülkeleri saygı göstermesi gereken temel hak ver özgürlüklerin kapsamını belirlemek amacıyla 7 Aralık 2000 tarihinde imzalanmıştır. Bağlayıcı hale gelebilmesi ise 1 Aralık 2009 tarihinde Lizbon Antlaşması'nın imzalanması ve kabulüyle gerçekleşmiştir.

AB Temel Haklar Şartı'nın 7. maddesinde özel hayatın gizliliği düzenlenmekte olup kişisel verilere ilişkin düzenleme bu maddeye eklenmek yerine ayrı bir başlıkta düzenlenmiştir. AB Temel Haklar Şartı'nın "Kişisel Bilgilerin Korunması" başlıklı 8. maddesinde "1. *Herkes, kendisine ilişkin kişisel bilgilerinin korunmasını isteme hakkına sahiptir.* 2. *Bu tür bilgiler, belirtilen amaçlar için ve ilgili kişinin muvafakatine veya yasada öngörülen başka meşru temele dayalı olarak adil şekilde kullanılmalıdır. Herkes, kendisi hakkında toplanmış olan bilgilere erişme ve bunlarda düzeltme yaptırma hakkına sahiptir.* 3. *Bu kurallara uyulması, bağımsız bir makam tarafından denetlenecektir.*" hükmü yer almaktadır.

AB üyesi ülkeler AB Temel Haklar Şartı ile bağlıdır ve uyup uymadıkları bağımsız bir otorite tarafından denetlenmektedir.

[87] 30/12/2017 tarih ve 30286 sayılı Yönetmelik.

1.2.2.2. 45/2001 ve 2018/1725 sayılı Veri Koruma Tüzükleri

Tüzük öncesi dönemde AB veri koruma hukukuna ilişkin çerçeve düzenleme olan 95/46/EC sayılı Direktif yürürlüktedir. İlgili mevzuat yalnızca AB üyesi devletler için geçerli olup AB kurum ve organlarının veri işleme faaliyetlerine ilişkin düzenleme barındırmamaktadır.[88] Bu eksikliği gidermek amacıyla 45/2001 sayılı AB Kurumları Veri Koruma Tüzüğü yürürlüğe konulmuştur.

AB organları veri işleme faaliyetlerini 2001-2018 arası dönemde 45/2001 sayılı Tüzük kapsamında yapmakta olup uygulama süreçlerinin denetimi amacıyla Avrupa Veri Koruma Denetçisi (European Data Protection Supervisor) kurulmuştur. Avrupa Veri Koruma Denetçisi bağımsız denetimin yanı sıra danışmanlık vermek ve koordinasyonu sağlamakla görevlidir.

2018 yılında Tüzük yürürlüğe girmiş ve 95/46/AT mülga hale gelmiştir. Akabinde 23 Ekim 2018 tarihinde 2018/1725 sayılı Tüzük kabul edilmiştir. Kamu kurumlarını veri işleme süreçleri, kamunun ihtiyaçları dikkate alınarak düzenlenmiş ve Tüzük'den farklı istisnalara yer verilmiştir.[89]

1.2.2.3. AB Genel Veri Koruma Tüzüğü

AB üye ülkelerinin mevzuatlarının uyumlu hale getirilmesi ve dijital tek pazar yaratma amacı[90] kapsamında birçok hukuk alanında tüzükler hazırlanmıştır. 1995 yılından itibaren uygulanan 95/46/AT sayılı Direktif'in ülkelerin mevzuatlarını uyumlu hale getirme konusunda yetersiz kalması nedeniyle kişisel verilerin korunması alanında Tüzük hazırlanmış[91] ve 2016 yılında Resmi Gazete'de yayınlanmıştır.[92]

Yürürlüğe giriş tarihi olarak 25 Mayıs 2018 tarihi belirlenmiş olup bu tarihten itibaren tüm üye ülkeler için bağlayıcı hale gelmiştir.[93] Bu nedenle kişisel verilerin korunmasına ilişkin kavramlar, veri işleme süreci ve veri işlemeye yönelik izinler, ihlal durumunda uygulanacak yaptırımlar ve kişisel verilerin korunması

---

[88] **Dülger**, Murat Volkan: Bilişim Suçları, Seçkin Yayınevi, Ankara, 2014, s. 38.
[89] **Dülger**, Bilişim Suçları, s. 39.
[90] https://ec.europa.eu/commission/presscorner/detail/en/IP_15_6321 Erişim Tarihi:04.01.2023.
[91] **Taştan**, s. 57.
[92] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL%3A2016%3A119%3ATOC Erişim Tarihi:04.01.2023.
[93] Bu tarihe kadar daha evvel de değindiğimiz üzere 95/46/AT sayılı Direktif AB üyesi ülkeler vatandaşlarının veri güvenliğini sağlamayı amaçlıyordu. Tüzük'ün m. 99 hükmü gereği yürürlüğe girmesiyle 95/46/AT sayılı Direktif yürürlükten kalkmıştır.

yükümlülüğünün ihlalinden doğan tazminat hususları da dahil olmak üzere kapsamlı düzenlemeler mevcuttur.

KVKK'nın hazırlanma sürecinde 95/46/AT sayılı Direktifi esas alması nedeniyle Tüzük ile arasında önemli farklar mevcuttur. Bu sebeple çalışma kapsamında Tüzük incelenirken KVKK ile karşılaştırılarak anlatılacaktır.

AB'de Tüzük ve Türkiye'de KVKK'nın düzenlediği konular, amaçları ve veri tanımı yönlerinden benzediği görülmektedir. Ancak Tüzük çok daha detaylı hükümler içerdiği gibi veri işleme sürecine ilişkin daha fazla düzenleme ihtiva ettiği görülmektedir.[94] Buradan yola çıkarak Tüzük'ün daha detaycı ve kazuistik bir düzenleme olduğunu söylemek uygun olacaktır.

İki mevzuat arasındaki en temek fark uygulama alanları noktasında ortaya çıkmaktadır. KVKK'da kapsam olarak veri işleyen esas alınmış ve Türkiye sınırları içerisinde kişisel veri işleyen gerçek veya tüzel kişilere uygulanacağı düzenlenmiştir. Ancak Tüzük kapsam açısından yalnızca veri işleyeni değil verisi işleneni baz almış ve bölgesel kapsamını genişletmiştir.[95] Buna göre AB sınırları içerisinde ikamet eden hali hazırda hayatta[96] kişilerin verilerini işleyen gerçek ve tüzel kişiler, AB sınırları dışında veri işlese dahi Tüzük hükümlerine tabidir.[97] Veri işleyenin AB sınırları dahilinde olması veya AB hukukuna tabi bir gerçek veya tüzel kişi olması şartı aranmamaktadır.

Tüzük'ün tanımlar başlıklı m. 4. hükmünde veri kaydetme, düzenleme, yapılandırma, toplama, saklama, uyarlama, elde etme, veri üzerinde değişiklik yapma, yayma veya kullanıma sunma, uyumlaştırma ya da birleştirme, kısıtlama, veri silme veya veri imha kavramlarının açık biçimde tanımlandığı görülmektedir. KVKK'da ise bu kavramlar yukarıda açıklanıldığı üzere ikincil mevzuatla tanımlanmış, usul ve esasları çizilmiştir.

---

[94] İki mevzuat madde sayıları açısından kıyaslandığında dahi KVKK 31 maddeden oluşurken Tüzük 99 maddelik bir düzenlemedir.

[95] **Tikkinen-Piri**/**Markkula**, s. 138.

[96] Tüzük yalnızca hayatta olan kişilerin verilerine ilişkin koruma olanağı sunmaktadır. Ancak Tüzük gerekçesinin 27. maddesinde AB üyesi ülkelerin gerekli gördükleri takdirde ölülerin kişisel verilerinin işlenmesine ilişkin kurallar da koyabileceği düzenlenmiştir. **Papaioannou**, Georgios/ **Sarakinos**, Ioannis: The General Data Protection Regulation (GDPR, 2016/679/EE) and The (Big) Personal Data İn Cultural İnstitutions: Thoughts On The GDPR Compliance Process. In: ICADL 2018: Maturity and Innovation in Digital Libraries, Springer, Hamilton, 2018, s. 201-204.

[97] **Üzeltürk**, Hakan: Avrupa Birliği Genel Veri Koruma Düzenlemesi, Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, C.15, S. 2, 2018, S.161-179, s. 177.

Kişisel verilerin işlenebilmesi için gerekli olan açık rıza verilmesi şartına ilişkin olarak her biri veri işleme süreci için ayrı izin alınması gerektiği ve veri sorumlularının rızanın verildiğini ispatlaması gerektiği düzenlenmektedir. Ayrıca Tüzük'de rıza özgür olarak verilmiş belirgin, bilinçli ve açık işaret olarak tanımlanırken beyan veya açık onay şeklinde verilebileceği düzenlenmiştir.[98] KVKK'de ise bilgilendirme ve özgür iradeye kavramlarına vurgu yapılmasıyla yetinilmiş nasıl rıza verilebileceği hususuna değinilmemiştir.[99]

Veri işleme sürecinde, Tüzük'de kişisel veriler için rıza (consent) yeterli görülürken özel nitelikli kişisel veriler, yurtdışına transfer edilen veriler ve otomatik karar almaya tabi veriler için açık rıza aranmıştır.[100] KVKK'da ise yukarıda belirtildiği üzere yalnızca açık rıza (explicit consent) kavramına yer verilmiş ve işlenecek tüm veriler[101] için açık rıza verilmesi şartı aranmıştır.[102]

Veri sahibinin hakları açısından bakıldığında ise Tüzük bilgilendirme hakkı[103], erişim hakkı[104], düzeltme hakkı[105], unutulma hakkı[106], veri işleme faaliyetini kısıtlama hakkı[107], veri taşınabilirliği hakkı[108], itiraz hakkı[109], otomotik karar vermeye ilişkin haklar[110], çocuklara ait kişisel veriler, verilerin tasarımla korunması, varsayılan ayarlar, açık biçimde düzenlenmiştir.

Tüzük'de çocukların verilerinin korunması amacıyla hükümlere yer verilmiş olup çocuklar savunmasız kişi (*vulnerable natural persons*) olarak tanımlanmıştır. Çocukların verilerine ilişkin veri işleme rızası farklı düzenlenmiş ayrıca veri koruma ile görevli otoritelere çocukların verilerinin korunmasına ilişkin ek

---

[98] Tüzük m. 4. **Develioğlu**, Murat: 6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku, XII Levha Yayıncılık, İstanbul 2017, s. 52.
[99] KVKK m. 3.
[100] **Politou**, Eugenia/**Alepis**, Efthimios/**Patsakis**, Constantinos: "Forgetting Personal Data And Revoking Consent Under The GDPR: Challenges And Proposed Solutions", Journal Of Cybersecurity, C. 4 S.1, 2018, s.7.
[101] KVKK'da tüm veriler kavramı kişisel veriler, özel nitelikli kişisel veriler, üçüncü kişilere transfer, yurtdışına transfer edilen verileri kapsamaktadır.
[102] **Çelikel**, s. 163.
[103] Tüzük m. 5, 13, 14.
[104] Tüzük m. 15.
[105] Tüzük m. 16.
[106] Tüzük m. 17.
[107] Tüzük m. 18.
[108] Tüzük m. 20.
[109] Tüzük m. 21.
[110] Tüzük m. 22.

yükümlülükler getirilmiştir.[111] Ticari amaçlarla 16 yaşından küçük çocuk verilerinin kullanılması yalnızca yasal temsilci rızasıyla mümkün olduğu ancak üye devletlerin ulusal mevzuatın bu yaşı 13 yaşa kadar indirebileceği düzenlenmiştir.[112] Otoritelerin görevlerini düzenleyen 57. maddede çocuklarla ilgili veri işleme faaliyetlerine özel ilgi göstereceği hükmü yer almakta olup somut olarak özel ilgi ile nelerin ifade edildiği belirtilmemiştir.

Çocukların verilerinin işlenmesi ve rıza verme ehliyeti açısından bakıldığında ise KVKK'da herhangi bir düzenleme yer almamaktadır. Ancak rıza kişiye sıkı sıkıya bağlı bir hak olduğu için ancak hak ve fiil ehliyetine sahip gerçek kişinin kendisi tarafından kullanılabilecektir.[113] Sınırlı ehliyetsiz konumundaki ayırt etme gücüne sahip çocuklar için herhangi bir yaş gruplandırması yapılmaması, rıza verme açısından ayrı bir hüküm konulmaması eksiklik olarak yorumlanmaktadır.[114] Çocukların sosyal medya platformları başta olmak üzere birçok internet mecrasında yetişkinler kadar aktif olabildiği ve olası tehditlere karşı daha savunmasız olduğu dikkate alınarak açık bir düzenleme yapılmasının faydalı olacağı açıktır.[115]

Unutulma hakkı Tüzük'de düzenlenmeden önce de yargı kararlarıyla tanımlanmış bir hak olmakla birlikte dijitalleşme hızının artmasıyla birlikte mevzuatla düzenlenecek kadar önemli hale gelmiştir. Tüzüğün öncesi döneme giderek o dönem verilen yargı kararlarına bakacak olursak bir gizlilik arayışı göze çarpmaktadır. Arama motorlarının internet sitelerinin neredeyse tamamını indekslemesi ve bu arama motorlarına kişilerin adlarını yazarak tüm bilgilere erişilebilmesinin bir takım sonuçları oldu. Örneğin yıllar evvel basına yansıyan bir

---

[111] **Develioğlu**, s. 54.
[112] Tüzük m. 8.
[113] **Taştan**, s. 162-163, **Özdemir**, Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması, Seçkin Yayıncılık, Ankara 2009, s. 168.
[114] **Zor**, Abdülhamid: Veri Sorumlusunun Yükümlülükleri Ve Bu Yükümlülükleri İhlalinden Doğan Özel Hukuk Sorumluluğu, Yayınlanmamış Yüksek Lisans Tezi, İstanbul, 2020 s. 128.
[115] Çocuklara yönelik güncel veri ihlallerinden biri "*Tiktok*" olarak bilinen video sosyal paylaşım uygulamasının, 13 yaşın altındaki kullanıcılardan veri toplama politikalarıyla ilgilidir. ABD Federal Ticaret Komisyonu (Federal Trade Comission-FTC) tarafından gereçekleştirilen inceleme neticesinde, ilgili sosyal medya uygulamasının 13 yaş altındaki çocukların verilerini ebeveynelerinin iznin almadan işlediğini tespit etmiştir. Bu veri işleme politikasının Çocukların Çevrim içi Gizlilik Koruma Yasası'nı (The Children's Online Privacy Protection Act) ihlal ettiği gerekçesiyle, FTC 5.7 milyon ABD Doları idari para cezasına uygulnamasına karar verilmiştir. 27.02.2019 tarih ve 464703 sayılı FTC kararı. https://www.ftc.gov/news-events/news/press-releases/2019/02/video-social-networking-app-musically-agrees-settle-ftc-allegations-it-violated-childrens-privacy Erişim Tarihi: 23.03.2023.

olayın bugün hala kişi ismiyle erişilebilir olması büyük rahatsızlıklara neden oldu. İnsanlar adeta geçmişinden kaçamaz ve saklayamaz duruma getirildi.

İnsanlar hakkında yalnızca birkaç kelime ile arama yaparak kapsamlı bilgi edinebilmenin bir sonucu olarak kaybedilen gizlilik kavramı tekrar talep edilmeye başlandı. Bu konuda özel hayatın gizliliği ve haber alma hürriyeti arasında ince bir çizgi olduğu ve hangi hakkında daha korunmaya değer olduğunun tartışıldığı dönemde Costeja González v. Google Inc, Google İspanya kararı[116] tartışmaları büyük ölçüde bitirmiştir.

İlgili kararda veri sahibine ait temel hak ve özgürlüklerin de göz önünde bulundurulması ve adil kabul edilebilecek bir dengenin oluşturulması gerekeceği belirtilmiştir. Ayrıca kişisel verilerin eksik, yanlış, ilgisiz ve amacını aşacak biçimde tutulmaları; tarih, istatistik yahut bilimsel amaçlar açısından zorunlu olmadıkça öngörülen süreleri aşacak şekilde tutulmaları durumunda, veriler ve arama motoru sonuçlarında gösterilen bağlantıların kamu yararı gibi sıradışı ve özel bir durumun olmadığı durumlarda silinmesinin uygun olacağına hükmedilmiştir. Arama motorlarında yer alan kamuya açık bilgilerin içerik ve süre açısından tamamıyla sınırsız bir biçimde servis edilemeyeceği hükmü ilerleyen yıllarda mevzuata girmiştir.

Tüzük'ün m. 17 hükmünde, gerçek kişinin rızasını geri alması, veri işlemenin artık gerekli olmaması, hukuka aykırı biçimde verilerinin işlenmesi veya daha evvel mevcut hukuka uygunluk nedenlerinin ortadan kalkması nedenleriyle verilerin unutulma hakkı kapsamında değerlendirilerek silinmesi gerektiğini ifade etmektedir.[117]

Tüzük m. 25'te düzenlenen tasarımla ve varsayılan ayarlarla veri koruma olmak üzere iki kural getirmiştir. Bu kurallardan ilki uygulama ve internet siteleri gibi kullanıcıların faydalandığı dijital mecraların tasarım aşamasından itibaren veri korumaya elverişli biçimde hazırlanmasını ikincisi ise kullanıcının herhangi bir ayarı değiştirmeden ilk kullanmaya başladığı ayarlarla devam ettiği takdirde verilerinin korunuyor olmasını ifade etmektedir.

---

[116] Avrupa Birliği Adalet Divanı'nın C-131/12 sayılı ve 13 Mayıs 2014 tarihli kararı.

[117] **Nalbantoğlu**, Seray: "Bir Temel Hak Olarak Unutulma Hakkı", Türkiye Adalet Akademisi Dergisi, Sayı:35, 2018, s. 593.

Hazırlık aşamasında gözden geçirilmemiş ve test edilmemiş yazılımların kullanıma sunulması tasarımla veri koruma kuralının ihlaline örnek olarak verilebilir. Varsayılan ayarlarla veri koruma kuralının ihlaline örnek olarak ise bir platforma kaydolmuş kullanıcının herhangi bir kişisel verisinin varsayılan ayarları değiştirmediği takdirde üçüncü kişilerle paylaşılması gösterilebilir. Platformun varsayılan ayarları kişisel verilerin başkalarıyla paylaşılmamasına uygun şekilde kararlaştırılmalıdır.

Veri koruma etki değerlendirmesi, kişisel verilerin işlenmesi nedeniyle ortaya çıkan risklerin değerlendirilmesi ve olası risklerin tespit edilip risklerin en düşük seviyeye indirilmesi olarak tanımlanmaktadır.[118] Veri işleme faaliyetine başlamadan evvel, veri sorumlularının öz denetim yaparak ve verisi işlenen kişiler nezdinde meydana gelebilecek risklerin önlenmesine fayda sağlayabilecek bir uyum aracıdır.[119]

Tüzük m. 35/3'de veri koruma etki değerlendirmesi yapılması gereken başlıca haller sayılmıştır. Buna göre özellikle kişisel veriler ile ilgili profil çıkarma dahil olmak üzere otomatik işlemeye dayalı ve kişi ile ilgili hukuki sonuçlar doğuran veya veri sahibini önemli ölçüde etkileyen kararlar, özel nitelikli verilerin işlenmesi, mahkumiyet kararları ve ceza gerektiren suçlara ilişkin kişisel verilerin büyük çaplı olarak işlenmesi, herkese açık bir alanın sistematik bir şekilde izlenmesi örnekleme yoluyla sayılmıştır.[120] KVKK'da benzeri bir düzenlemeye yer verilmemiş olmakla birlikte Kurul kararlarında veri koruma etki değerlendirilmesi yapılması gerektiğine yer verilmektedir.

Tüzük'ün getirdiği yeniliklerden bir diğeri ise veri koruma görevlisidir (*data protection officer*). Veri koruma görevlisinin görev ve sorumlulukları şunlardır: Veri işleyen kurum veya kuruluşun kendisine, çalışanlarına bilgi ve görüş vermek, veri sorumlusu bünyesindeki çalışanların veri koruma hukuku kapsamında eğitilmesi, veri işleme ve gizlilik politikasının mevzuata uygunluğunun denetlenmesi, kişisel verilerin korunmasına etki analizi yapmak ve etkinliğine

---

[118] **Çimen Bulut**, İpek: "Avrupa Birliği Genel Veri Koruma Tüzüğü Kapsamında Getirilen Yeni Teknik ve Yaptırım Mekanizmaları", Anadolu Üniversitesi Sosyal Bilimler Dergisi, C.20 S. 2, s. 133.

[119] **Bilgin**, Metin/**Erkan**, Sema/**Atasu**, İdil/**Yılmaz**, Enes: Privacy Impact Assessment as a Tool for GDPR Compliance Preparation, Kişisel Verileri Koruma Dergisi, C.1 S. 2, 2019, s. 78.

[120] Tüzük m. 35/3.

ilişkin tavsiye vermek, veri koruma alanında yetkili otorite ile iş birliği yapmak gerekli hallerde irtibatı sağlamak.[121]

Veri koruma görevlisi veri işleyen ile otorite arasında köprü görevi üstlenmekte olup aynı zamanda teşebbüsün veri koruma hukuku ile ilgili bilgi sahibi olması ve veri koruma politikasındaki açıkların tespitine ilişkin görevlerde yüklenmiştir. KVKK'da düzenlenmeyen bir görevli olmakla birlikte VERBİS Yönetmeliği kapsamında düzenlenen irtibat kişisi ile benzeşmektedir.[122]

Bir veri işleme faaliyeti çerçevesinde tek veri kayıt sisteminin amaç ve yöntemleri birden fazla kişi tarafından birlikte belirlenmesi durumunda belirleyenler ortak veri sorumlusu olarak değerlendirilmektedir. Veri sorumlusu kavramından farkı veri işlemeye ilişkin amaç ve araçlara ilişkin kararların birden fazla kişi tarafından alınması ve buna bağlı olarak tek kişi yerine birden fazla kişinin sorumlu olmasıdır.

Her ortak veri işleme faaliyeti ortak veri sorumluluğu kavramını gündeme getirmeyecek olup sorumluluk için veri işleme sürecinde tarafların veri toplama ve işleme faaliyetine etkisine bakılmaktadır. Taraflar aynı veri işleme faaliyetinde ayrı ayrı veri sorumlusu olarak veya ortak veri sorumlusu olarak nitelendirilebilmesi mümkündür. Ortak veri sorumlusu kavramının sınırlarının belirlenmesi açısından Wirtschaftsakademie ve Facebook İrlanda Kararı[123] önemli bir karardır. Wirtschaftsakademie, Facebook üzerinden sayfa oluşturarak içerik üretmektedir ve sayfasının erişim sayısı, beğeni, paylaşım ve benzeri istatistiklerini görebilmek amacıyla "*Facebook Insights*" hizmetini etkinleştirmiştir. İlgili veriler Facebook tarafından kullanıcıların hesaplarına konumlandırılan tekil birer kullanıcı numarası içeren çerezler tarafından toplanmaktadır.

Avrupa Birliği Adalet Divanı kararında, Facebook'un veri işleme faaliyetine Wirtschaftsakademie'nin de kendi sayfasını ve kitlesi özelinde katıldığı, her iki veri sorumlusu da aynı amaç kapsamında ve aynı değişkenlere göre veri işleme

---

[121] **Keskinkılıç**, Gamze Nur: Veri Koruma Görevlisi, Yüksek Lisans Tezi, İstanbul Medipol Üniversitesi, İstanbul, 2021, s. 100.

[122] İrtibat kişisinin geniş yetkileri bulunmamakla birlikte veri sorumlusu ve Kurum arasında iletişimi sağlaması yönüyle benzemektedir. VERBİS m. 11'de düzenlenmiştir.

[123] Avrupa Birliği Adalet Divanı'nın 01.07.2016 başvuru, 5.6.2018 karar tarihli ve C-210/16 sayılı kararı.

faaliyetinde bulunduğu, bir sosyal medya platformu üzerinden veri işlemenin ortak sorumlu olmaya engel oluşturmayacağı ifadeleri yer almaktadır.

Kişisel verilerin korunmasına ilişkin Tüzük hükümlerine aykırı davranılması durumunda uygulanacak idari para cezaları m. 83'te düzenlenmektedir. Tüzük, veri koruma yükümlülüğünün ihlallerini kendi içerisinde iki gruba ayırmış ve ilk grup ihlal için, üst sınır 10.000.000 Euro'ya veya bir önceki mali yılın yıllık dünya çapındaki cirosunun %2'sinden yüksek olan meblağ olarak belirlemiştir.[124] İkinci ihlal grubu içinse üst sınır 20.000.000 Euro'ya veya bir önceki mali yılın yıllık dünya çapındaki cirosunun %4'sinden yüksek olan meblağ olarak belirlemiştir.[125]

Veri ihlalinden kaynaklanan özel hukuk sorumluluğu Tüzük'ün 82. maddesinde, "*Bu Tüzük'e ilişkin bir ihlal sonucu maddi veya manevi zarar gören herhangi bir kişi, yaşanan zarara ilişkin olarak kontrolör veya işleyiciden tazminat alma hakkına sahiptir.*" hükmü yer almaktadır. Tüzük veri ihlalinden doğan zararlardan veri işleyen ve kontrolöre birlikte sorumlu tutulmuştur. İlgili hükme benzer bir düzenleme KVKK'nın 14/3. maddesinde "*Kişilik hakları ihlal edilenlerin, genel hükümlere göre tazminat hakkı saklıdır.*" şeklinde yer almaktadır.[126] İlgili hükümlere ilişkin değerlendirme üçüncü bölümde yapılacaktır.

1.2.2.4. AB Veri Koruma Hukuku Kapsamında Özel Hukuk Sorumluluğu

Tüzük kapsamında kontrolörler ve işleyicilerin yükümlülükleri, veri sahibinin hak ve yetkileri ve veri işleme sürecine ilişkin temel kurallar belirlenmiştir. Bu düzenlemelerin yanı sıra veri koruma hukukuna aykırı davrananlara karşı gidilebilecek özel hukuk sorumluluğuna ilişkin düzenlemelerde mevcuttur. Tüzük'ün tazminat hakkı ve sorumluluk başlıklı 82. maddesinde aşağıda görülebileceği üzere maddi ve manevi zarar sebebiyle tazminat hakkını, tazminat talebinin kimlere yöneleceğini, kurtuluş kanıtı getirme imkanı, tazminat talebini karara bağlamaya yetkili makamları düzenlenmektedir.[127]

---

[124] Tüzük m. 83/4.
[125] Tüzük m. 83/5-6.
[126] İlerleyen bölümlerde bu düzenlemenin atıf yaptığı genel hükümler ve genel hükümlerin sunduğu tazmin olanakları incelenecektir.
[127] Tüzük m. 82 hükmünde yer alan düzenlemede kusur ifadesi geçmemektedir. Sorumluluğun türüne ilişkin tartışmalar üçüncü bölümde yapılacak olup tekrar ilgili bölümde değinilecektir.

"*1. Bu Tüzük'e ilişkin bir ihlal sonucu maddi veya manevi zarar gören herhangi bir kişi, yaşanan zarara ilişkin olarak kontrolör veya işleyiciden tazminat alma hakkına sahiptir.*

2. İşleme faaliyetine müdahil herhangi bir kontrolör bu Tüzük'ü ihlal eden işleme faaliyetinin sebep olduğu zarardan sorumludur. Bir işleyici, ancak bu Tüzük'ün özellikle işleyicilere yönelik yükümlülüklerine uyum göstermediği veya kontrolörün hukuka uygun talimatları dışında veya bu talimatlara aykırı hareket ettiği hallerde, işleme faaliyetinin sebep olduğu zarardan sorumludur.

3. Zarara sebep olan olaydan hiçbir şekilde sorumlu olmadığını kanıtlaması halinde, bir kontrolör veya işleyici bu sorumluluktan muaftır.

4. Birden fazla kontrolör veya işleyicinin ya da hem bir kontrol hem de bir işleyicinin aynı işleme faaliyetinde bulunduğu ve, 2 ve 3. paragraflar çerçevesinde, işleme faaliyetinin sebep olduğu herhangi bir zarardan sorumlu olduğu hallerde, veri sahibinin etkili bir şekilde tazminin sağlanması amacıyla, her kontrolör veya işleyici tüm zarardan sorumlu tutulur.

5. Bir kontrolör veya işleyicinin, 4. paragraf uyarınca, yaşanan zararı eksiksiz bir şekilde tazmin ettiği hallerde, söz konusu kontrolör veya işleyicinin aynı işleme faaliyetine müdahil diğer kontrolörler veya işleyicilerden zarardan sorumlu oldukları kısma tekabül eden tazminat kısmını, 2. paragrafta ortaya konan koşullar uyarınca, isteme hakkı bulunur.

6. Tazminat alma hakkının kullanımına ilişkin davalar 79(2) maddesinde atıfta bulunulan üye devletin hukuku çerçevesinde yetkin olan mahkemelerde açılır."[128]

KVKK'ya esas alınan ancak günümüzde yürürlükte olmayan 95/46/AT sayılı Direktifte ise bu husus m. 23 hükmünde şu şekilde düzenlenmiştir:

"*Üye Devletler, bu Direktif uyarınca kabul edilen ulusal hükümlerle uyumsuz herhangi bir işlemenin veya yasadışı bir işleme faaliyetinin sonucu olarak zarara*

[128] Tüzük'ün 79/2 hükmü "*Bir kontrolör veya bir işleyiciye karşı açılacak davalar kontrolör veya işleyicinin bir işletmesinin bulunduğu üye devletin mahkemelerinde açılır. Alternatif olarak, kontrolörün veya işleyicinin bir üye devletin kamu yetkilerinin kullanımı ile ilgili olarak hareket eden bir kamu kuruluşu olması haricinde, böylesi davalar veri sahibinin mutat meskeninin bulunduğu üye devletin mahkemelerinde açılabilir."* şeklindedir.

uğrayan herhangi bir kişinin, uğradığı zarar için denetleyiciden tazminat almaya hak kazanmasını sağlayacaktır.

Denetleyici, zarara yol açan olayda sorumlu olmadığını kanıtlarsa, kısmen ya da tamamen bu yükümlülükten muaf tutulabilir."

İlgili Direktif ve Tüzük hükümleri incelendiğinde net biçimde tazminat hakkının tanındığı görülmektedir. Her iki hükümde de veri sorumlusuna sorumlu olmadığını kanıtlama yükümlülüğü yüklenmiştir. Bu hususlara burada yer verilmekle birlikte asıl KVKK'da yer alan m. 11-ğ ile birlikte üçüncü bölümde sorumluluğun niteliği kapsamında tartışılacaktır.

Tüzük veri ihlalleri nedeniyle tazminat talep edilebileceğini ve bu tazminat talebinin nasıl yapılacağını oldukça açık biçimde düzenlemesine karşın tazminat hesabının nasıl yapılacağı hususunda bir düzenleme getirmemiştir.

Ülke uygulamalarına bakıldığında ise Tüzük'ün ihlal edilmesi nedeniyle ödenen ciddi tazminatlara rastlamanın mümkün olmadığı görülmektedir. Bu durumun temel nedeninin veri ihlalinin parasal değerinin tespitinin somut ve objektif biçimde yapılmasının zorluğundan kaynaklandığı anlaşılmaktadır.

Örnek bir olay üzerinden ilerlersek ortalama bir kredi kartına ait bilgilerin 0,85 ila 30 ABD doları (USD) arasında olduğu ve web sitesi yönetim kimlik bilgilerinin değerinin 2 ila 30 ABD doları arasında olduğu hesaplanmaktadır.[129] Konusu kredi kartı veya internet sitelerinin yönetici bilgileri olan veri ihalleri dahil bakıldığında ise şimdiye kadar ulusal mahkemeler tarafından hükmedilen meblağlar, davacı başına 250 € ile 5.000 € arasında değişmektedir, bu oran ihlal konusunun ortalama 20 katı sevesindedir.[130] Tazminatın hesaplanması özünde kişisel verilerin korunması hukukunun değil sorumluluk hukukunun alanına girmektedir.

Yine tazminatın hangi şartlar altında doğacağı ve nasıl tespit edileceği hususundaki bir diğer dava da Avusturya'da görülmüştür. Avusturya Posta Servisi[131] tarafından kişisel verileri işlenerek algoritma tarafından aşırı sağ partilere oy verebilir şeklinde profillenen ilgili kişi durumun utanç verici olduğunu

[129] OECD, Exploring the Economics of Personal Data – A Survey of Methodologies for Measuring Monetary Value (2013).
[130] Ülkemizde kişisel verilerin izinsiz işlenmesi nedeniyle ortalama kişisel verileri fiyatlayan bir çalışma mevcut değildir.
[131] Avusturya posta servisinin tam adı "Österreichische Post AG" şeklindedir.

ileri sürerek 1.000 EURO manevi tazminat talepli dava açmıştır. Avusturya temyiz mahkemesi ABAD'dan görüş istemiş ve bu kapsamda bir takım sorular yöneltmiştir. Bu sorulardan iki tanesi tazminata ilişkin olup AB üyesi ülkelerin veri ihlali kaynaklı tazminat taleplerine bakışını anlamak açısından önemlidir.

Sorulardan biri Tüzük m. 82 hükmü kapsamında tazminat ödenmesi için Tüzük hükümlerinin ihlal edilmesinin yeterli olup olmadığı eğer yeterli değilse başvuranın zarar görmüş olmasının zorunlu olup olmadığıdır. ABAD, hukuki sorumluluğun cezai bir amacının olmadığını ifade ederek tazminata için yalnızca Tüzük'ün m. 82 hükmünün ihlal edilmesini yeterli görmemiştir. Böyle bir tazminat ödenmesi için manevi anlamda rahatsız olmanın yeterli olmayacağı ifade edilmiştir.

Bir diğer soru ise veri ihlali, rahatsızlık ve üzüntü hissinin ötesinde bir ağırlık yaratıyorsa, bu ağırlık manevi zarar olarak değerlendirilip manevi tazminat ödenip ödenmeyeceğine ilişkindir. ABAD, manevi tazminata ilişkin değerlendirmenin toplumda hakim olan algı ve düşünceyi dikkate alarak ulusal mahkeme tarafından yapılması gerektiğini ifade etmiştir. Mahkeme ABAD'dan alınan hukuki görüş çerçevesinde manevi tazminat ödenmesine gerek olmadığı sonucuna ulaşmıştır.[132]

Veri ihlalleri nedeniyle oluşan zararın tazminine ilişkin AB uygulamasının başvuru usulünün incelenmesi de gerekmektedir. Veri koruma hukukundan doğan hukuki sorumluluk açısından doğrudan idari başvuru ile sonuç alınabilen herhangi bir AB ülkesi mevcut değildir. AB genelindeki uygulama mahkemeye başvurulması ve mahkeme sonucunda tazminat alınması şeklindedir. Ancak AB ülkelerinde ülkemiz hukukuna göre usulen kolaylık sağlayan class action (toplu dava) türü bulunmaktadır.

Toplu davalarda aynı eylem veya davranıştan dolayı mağdur olan kişileri temsilen açılmakta olup ortak hukuki menfaat davacıya değil ortak sebeple adına dava açılan topluluğun tamamına aittir.[133] AB üyesi ülkelerde yaşayan vatandaşların

[132] UI v Österreichische Post AG, Case C-300/21.
[133] **Şahin**, Murat/**Çelik Şahin**, Hande: "Toplu Hak Aramada Etkin Bir Yol Olarak Mukayeseli Hukukta ve Türk Hukukunda Sınıf Davaları", İstanbul Hukuk Mecmuası, C. 72, S. 1, 2014, 383-410, s. 383 vd.

kişisel veri ihlalleri de dahil birçok konuda tazminat almalarını kolaylaştıran Toplu Dava Direktifinden de bahsetmek uygun olacaktır.[134]

14 Kasım 2020 tarihinde kabul edilen ve 25 Haziran 2023 tarihinden tüm üye ülkelerden uygulanmaya başlayacak olan Toplu Dava Direktifi'ne göre aynı veri ihlalinden doğan zarardan dolayı üye ülkeler toplu dava hakkı tanıyacak ve iç hukuklarında opt out mekanizması getirebilecektir. Daha açık bir ifadeyle toplu davaya katılım için vekalet veya katılım talebi gerekmeksizin aksini belirtmeyen tüm mağdurlar adına sürecin yürütülmesi mümkün olacaktır.[135] Bu sistemi ülkelerin iç hukuklarına uyarlamasıyla birlikte veri ihlalinden doğan tazminat miktarlarının artmasını beklemek yanlış olmayacaktır.

---

[134] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32020L1828 Erişim Tarihi: 08.03.2023.

[135] **Agulló**, Diego: "Directive 2020/1828 On Representative Actions For The Protection Of The Collective İnterests Of Consumers: An Overview", UNIO - EU Law Journal, C. 8, S. 1, 2022, s. 131.

2. BÖLÜM: KİŞİSEL VERİLERİN KORUNMASI YÜKÜMLÜLÜĞÜ VE BU YÜKÜMLÜLÜĞÜN İHLALİ

2.1. KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN TEMEL KAVRAMLAR

Veri koruma hukukunun daha net anlaşılabilmesi için KVKK ve ikincil mevzuatta düzenlenen kavramların daha açık ifade edilmesi uygun olacaktır. Veri sorumlusu, somut olayda veri sorumlusunun nasıl tespit edileceği, veri işleyen veri sorumlusu ayrımı, anonim hale getirme, ilgili kişi, otomatik işleme, veri kayıt sistemi kavramları bu bölümde açılanacaktır.

Veri koruma hukukunun konusunu oluşturan eylem kişisel verilerin işlenmesi süreci olduğundan bu süreçte uygulanacak usul ve esaslar KVKK'da düzenlenmektedir. Kişisel verilerin işlenmesi KVKK'da "*Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi...*" biçiminde tanımlanmıştır.

Tüzük'ün 4/2 maddesinde ise "*...kişisel veri veya kişisel veri setleri üzerinde gerçekleştirilen toplama, kaydetme, düzenleme, yapılandırma, saklama, uyarlama veya değiştirme, elde etme, danışma, kullanma, iletim yoluyla açıklama, yayma veya kullanıma sunma, uyumlaştırma ya da birleştirme, kısıtlama, silme veya imha gibi herhangi bir işlem veya işlem dizisi*" olarak tanımlanmıştır.

Otomatik sistemle veri işleme bilişim sistemleri aracılığıyla yapılan kişisel veri işleme faaliyeti olarak, otomatik olmayan yöntem ise insan tarafından yapılan kişisel veri işleme faaliyeti olarak anlaşılmaktadır. Bu ayrım veri işleme eyleminin mevzuatta düzenlenen koruma kapsamına girip girmeyeceği hususunda önem arz etmektedir. Otomatik yöntemlerle yapılan veri işleme faaliyeti her durumda Kanun kapsamına girerken insan eliyle yapılan veri işleme faaliyeti yalnızca veri kayıt sisteminin bir parçasıysa veri koruma hukukunun uygulama alanına dahildir.

Otomatik yöntemlerle veri işlemenin her şartta veri koruma hukukunun konusuna dahil olması işlenen veri miktarı ve veri işleme teknikleri ile ilgilidir. Dijital

ekonominin ilerlemesiyle birlikte veri ekonomik anlamda çok ciddi bir değer haline gelmiştir. Özellikle büyük veri[136] kavramının hayatımıza girmesiyle birlikte insan tarafından işlenmesi ve kullanılması mümkün olmayan hacimde veriler otomatik yöntemlerle işlenmeye ve bu verilere göre kişiler profillenmeye başlanmıştır.

Büyük hacimlerdeki verinin kısa süre içerisinde ve kontrolü kolay olmayan biçimde işlenmesi bir insanın elle yaptığı veri işlemeye göre daha tehlikeli görülmüş ve tüm otomatik veri işlemeler veri koruma hukuku kapsamına alınmıştır. Dijital veri işleme faaliyetinin kapsamına dair bir sınır koymak ise oldukça zordur. Her gün yeni bir teknoloji ile farklı bir amaç için farklı bir verinin işlenmeye başlanması mümkün olduğundan veri işleme faaliyeti sınırlı bir kavram değildir.[137]

Diğer taraftan KVKK'da ve ikincil mevzuatta dijital veri işleme faaliyetinin sınırlarına ilişkin herhangi bir hüküm mevcut değildir. Dolayısıyla herhangi bir biçimde bir kişisel verinin hard disk, sunucu veya CD'de depolanması da veri işleme olarak nitelendirilebilecektir.[138] Ancak fiziki olarak yapılan veri kaydetme işlemlerinin veri işleme olarak değerlendirilmesi için aranan şartlar farklıdır. Eğer fiziki veri işleme bir kayıt sistemi dahilinde yapılıyorsa veri koruma hukukunun kapsamına girmektedir. Konunun daha net anlaşılabilmesi için veri kayıt sistemi kavramının açıklanması gerekmektedir.

2.1.1. Kişisel Verilerin İşlenmesinde Uyulması Gereken İlkeler

Veri koruma hukuku kapsamında kişisel verilerin işlenmesi sürecinde kabul gören bazı ilkeler mevcuttur. İlkeler konulmasıyla amaç veri işleme faaliyetinin temel esaslar çerçevesinde şeffaf ve güvenli bir biçimde gerçekleşmesidir. İlgili ilkelere verinin elde edilmesinden imha edilmesine kadar her aşamada uyulması beklenmektedir.

Bu ilkeler, Anlaşma 108'de, 96/45/AT'de, Tüzük'de ve KVKK'da yer almaktadır. Ancak veri işleme sürecini düzenlemeyi amaçlayan bu ilkeler birebir aynı değildir.

---

[136] Türü açısından karmaşık ve hacim açısından hızlı biçimde artan veri big data olarak isimlendirilmiştir. Daha açık bir ifadeyle veriler hızlı oluşturuluyorsa, veri büyütü oldukça büyükse ve veriler birden fazla türdeyse big data olarak ifade edilmektedir. Büyük veri, kavramın Türkçe karşılığı olarak kullanılmaktadır. **Laney**, Doug: 3D Data Management: Controlling Data Volume, Velocity, and Variety, 2001, Meta Group, S. 949, s.1.

[137] **Başalp**, s. 15.

[138] https://kvkk.gov.tr/SharedFolderServer/CMSFiles/185c2130-8070-4b2b-a91e-1d48322ca352.pdf Erişim Tarihi: 19.01.2023.

KVKK'nın m. 4 hükmünde sayılan "Genel İlkeler", Anlaşma 108 ve 95/46/AT hükümlerini esas almıştır. Ancak Tüzük m. 5. İlkelere ilişkin kavramların daha detaylı açıklandığı ve kapsamlarının genişletildiği anlaşılmaktadır.

KVKK'da düzenlenen kişisel veri işleme faaliyetinde uyulması beklenen ilkeler, Tüzük'de düzenlenen ilkeler ile farklılaştığı noktalara değinilecek aktarılacaktır.

2.1.1.1. Hukuka ve Dürüstlük Kuralına Uygunluk

Genel hükümler çerçevesinde bir işlemin hukuka uygun olması olmazsa olmaz bir kuraldır. Hukuka uygunluk ibaresi ile ifade edilmek istenen TMK m. 2'de olduğu gibi genel kabul gören hukuk normları ve ilgili olabilecek bütün mevzuata uygunluktur.

KVKK m. 4/2-a hükmünde "*hukuka ve dürüstlük kuralına…*" biçiminde düzenlenirken Tüzük m. 5/1-a hükmünde "…*hukuka uygun, adil ve şeffaf bir biçimde…*" işleneceği ifade edilmiştir. Her iki mevzuatta da yer alan hukuka uygun olma ifadesi ile yukarıda belirttiğimiz üzere geniş bir biçimde ilgili tüm mevzuat ve uluslararası hukuk ilkelerine uygun olma anlaşılmalıdır.[139]

KVKK 4/2-a'da düzenlenen dürüstlük kuralı, TMK m. 2 kapsamında düzenlenen dürüstlük kuralının özel bir görünümüdür. İlgili hükme göre veri sorumlusu ve ilgili kişinin dürüstlük kuralına uygun biçimde hareket etmesi gerekmektedir.

Hukuka uygunluk veya dürüstlük kuralına uygunluk kavramları KVKK'da detaylandırılmamıştır. Kanımızca hukuka uygunluk ve dürüstlük kuralına uygunluk kavramlarının tanımlanmaması bir eksiklik olmayıp uygulamada Kurul kararlarıyla şekillendirilecek hususlardır. Ayrıca Kurum tarafından yayınlanan terimler sözlüğünde ilgili kavrama ilişkin açıklama mevcuttur. Buna göre dürüstlük kavramı ilgili kişiye haber vermeksizin hiçbir biçimde kişisel verisinin işlenmemesi, işlenen verinin herhangi bir haksızlığa yol açacak biçimde kullanılmaması, toplanma amacı dışına çıkılmaması ve makul sayılabilecek beklentilerin karşılanmasıdır.[140] Dürüstlük kuralı ilkesi diğer veri işleme ilkelerini kapsayan bir ilkedir.

---

[139] **Küzeci**, s 206.

[140] https://www.kvkk.gov.tr/Icerik/5388/Madde-ve-Gerekcesi-ile-Kisisel-Verilerin-Korunmasi-Kanunu-Bilgi-Notu-ve-Kisisel-Verilerin-Korunmasina-Iliskin-Terimler-Sozlugu Erişim Tarihi: 08.04.2023.

Kurul'un geçmiş kararlarına bakıldığında belediye çalışanlarının iş yerine giriş çıkışını denetlemek maksadıyla parmak izi okuma sistemi kullanılmaması ve kaydedilen verilerin ilgili kişinin talebine rağmen silinmemesi inceleme konusu olmuştur. Kurul belediye çalışanının biyometrik verisinin açık rızası dışında işlendiğini tespit etmiştir. Ayrıca ilgili çalışan açık biçimde talep etmesine rağmen yollanan evrak konusunda bilgi belge talebi yazılması nedeniyle veri silme talebine cevap vermemesini dürüstlük kuralına aykırı bulmuştur.[141]

2.1.1.2. Doğru ve Gerekliyse Güncel Olma

Veri sorumlusunu ve ilgili kişiyi korumaya yönelik bir ilkedir. İşlenen veriler hem veri sorumlusunun hem de ilgili kişi üzerinde sonuç doğurmaktadır. Veri sorumlusu kişisel verileri önceden belirlediği bir işte kullanmak maksadıyla işlemektedir. İlgili kişi ise bir amaç uğruna bu verilerin işlenmesine rıza vermektedir.

Verileri yanlış veya güncelliğini yitirmiş olması beklenen amacın gerçekleşmesini engelleyecektir. Ayrıca ilgili kişinin güncel olmayan veya yanlış verilerinin işlenmesi sebebiyle maddi veya manevi zararının doğması mümkündür.[142] Örneğin bir kamu kurumundan tebligat bekleyen ilgili kişinin adresinin yanlış işlenmesi veya adresinin güncellenmemesi durumunda kişinin tebligat yapılamaması nedeniyle mağduriyeti doğabilir.

Kişiler bu ilke kapsamında kendisiyle ilgili verilerin doğru işlenmesini talep etme ve doğruluğunu kontrol etme hakkına da sahiptir.[143] Ayrıca Kurul ilke kararıyla ilgili kişi hakkında bir sonuca sebep olabilecek kişisel verilerin doğru ve güncel olmasının sağlanması konusunda veri sorumlusunun aktif özen yükümlülüğü bulunması gerektiğini ifade etmiştir.[144]

Kurul'un bir diğer kararında ise ilgili kişinin bireysel borçlarına ilişkin bilgilerin, ortağı olduğu bir şirkete ait iletişim numaralarına gönderilmesi bu ilkeye aykırı bulunmuştur. İşlenen ve kullanılan iletişim bilgilerin doğru ve güncel olmaması ihlal tespiti için yeterli görülmüştür.[145]

---

[141] 01/12/2020 tarih ve 2020/915 sayılı Kurul kararı.
[142] **Taştan**, s. 50.
[143] **Başalp**, s. 37.
[144] 22/12/2020 tarih ve 2020/966 sayılı Kurul ilke kararı.
[145] 19/01/2023 tarihli ve 2023/78 sayılı Kurul kararı.

Telekomünikasyon sektöründe ticari faaliyetlerine devam eden bir veri sorumlusu üçüncü kişilere ait mobil faturaların ilgili kişinin e posta adresine gönderilmesinin doğru ve güncel biçimde veri işleme olarak değerlendirilemeyeceği tespit edilmiştir. Ayrıca kararda veri sorumlunun bir yükümlülüğü olduğu da ifade edilmiştir. Buna göre veri sorumlusu verilerin doğruluğunu proaktif bir şekilde sağlamalıdır.[146]

İlgili kararlar çerçevesinde veri işleme sürecine ilişkin bu ilkenin amacının veri sorumlusunu ve aynı zamanda ilgili kişiyi korumak olduğu anlaşılmaktadır. Ayrıca Kurul içtihadında sergilenen yaklaşımdan veri sorumlusunun bu ilke kapsamında aktif biçimde veri doğruluğunu ve güncelliğini sağlama yükümlülüğü olduğu anlaşılmaktadır.

2.1.1.3. Belirli, Açık ve Meşru Amaçlar İçin İşlenme

Veri sorumlusunun her bir veriyi işlerken belirli bir amaç için işliyor olması gerekmektedir. İşlenen veri yalnızca bu amaç için kullanılabilir ve amaç ortadan kalktığında da verinin uygun yöntemlerle silinmesi gerekmektedir. Veri işleme amacını ve işlenen verinin kapsamını ilgili sicile bildirmenin arkasındaki sebeplerden bir tanesi de belirli ve açık biçimde veri işlemenin sağlanmasıdır. İlgili kişi veri işleme amacını kesin ve net biçimde öğrenebilmeli ve rızasını buna göre verip vermeyeceğini kararlaştırabilmelidir.[147] Ayrıca, ilgili kişinin net olmayan amaçlarla veri işlenmesine rıza göstermesi, verilerin korunma hukukunun hedeflerinden bir tanesi olan kendi geleceğini belirleme ilkesi açısından değerlendirildiğinde de uygun olmayacaktır.[148]

Meşru amaçlarla işleme ise veri işleme süreciyle hedeflenen hususların hukuken meşru bir zemine dayanmasını ve veri işleme sebebiyle menfaat dengesi güdülmesini ifade etmektedir. Aynı zamanda KVKK m. ve m. 6 hükümlerinde veri işlemenin hukuki gerekçelerine değinilmiştir.[149] İşlenen veri ve yapılan faaliyet arasında bir zorunluluk ilişkisi olması beklenmektedir. Örnekle somutlaştırmak

---

[146] Kurul'un 08/09/2022 tarih ve 2022/925 sayılı kararında "… *söz konusu kişisel verilerin doğruluğunu sağlamak amacıyla proaktif bir yaklaşımla gerekli tedbirleri almamasının*…" ifadeleri yer almaktadır.

[147] Tüzük 5/1-b'de aynı ilkenin benzer kapsamda yer aldığı görülmektedir.

[148] **Özer Deniz**, s. 84.

[149] Tüzük m. 6'da da veri işlemenin hukuka uygunluğu huşu kapsamlı düzenlenmiştir. Hukuka uygunluk kavramını açıklamak adına iki mevzuatın da açık ve anlaşılır olduğunu söylemek yanlış olmayacaktır.

gerekirse bir e ticaret platformunun siyasi görüşlere ilişkin bilgileri işlemesi meşru bir amaç olarak kabul edilmeyecektir.

2.1.1.4. İşlendikleri Amaçla Bağlantılı, Sınırlı ve Ölçülü Olma

Tüzük m. 5/1-c ve KVKK m. 4/2-ç hükümlerinde kapsamları benzer düzenlemeler yer almaktadır. Her iki hükümde veri minimizasyonu olarak ifade edilen ilkeyi işaret etmektedir. Veri minimizasyonu ile sağlanması beklenen fayda verileri amaca uygun biçimde işlemektir.[150] Bu anlamda bir önceki başlıkta açıkladığımız ilke ile de tamamlayıcı olduğunu ifade etmek uygun olacaktır.

Veri minimizasyonu ilkesi Tüzükte "*yeterli, yerinde ve gerekli olanla sınırlı*" verilerin işlenmesi gerektiği belirtilirken KVKK'da "*bağlantılı, sınırlı ve ölçülü*" ifadeleriyle veri işlemede asgarileştime ve minimizayon ilkesi işaret edilmiştir. Veri minimizasyonu hususunu netleştirmek için uygulamada nasıl ele alındığına bakmak fayda sağlayacaktır.

Veri sorumlusu konumundaki üniversite tarafından herkese açık konumdaki internet sitesi üzerinden herkesin erişebileceği bir sayfada öğrenci ve akademisyenleri bilgilendirme amacını aşacak biçimde ilgili kişinin adres, soruşturma geçirip geçirmediği, komisyon görüşü ve hakkındaki kaleme alınmış görüş yazıları da dahil birçok kişisel verinin yayınlanmasının veri minimizasyonu ilkesine aykırı olduğuna hükmedilmiştir. İlgili karardan hareketle bir verinin kaydedilmesi sonrasında da veri minimizasyonu ilkesinin uygulandığı görülmektedir.[151]

Kurul'un bir yasal bahis sitesinin veri işleme politikasına ilişkin şikayeti değerlendirdiği kararında temel iletişimin cep telefonu numarası üzerinden sağlanmasına rağmen e posta verisinin işlenmesini veri minimizasyonu ilkesine aykırılık olarak değerlendirmiştir.[152] Karar özetinde yer alan "*hiç işlenmemiş olsa da veri sorumlusunun üyelerine sunduğu hizmetleri aksatmayacağı anlaşılan*" değerlendirmesi Kurul'un veri minizasyonu konusuna bakışını net biçimde göstermektedir. İlgili kararlar ışığında bu ilkeyi eğer bir veri hizmeti sunman için zorunlu değilse işlenmemeli biçiminde özetlemek uygun olacaktır.

---

[150] **Tamò-Larrieux**, Aurelia: Designing for Privacy and its Legal Framework: Data Protection by Design and Default for the Internet of Things, 2018 Heidelberg, Springer, s.91.
[151] 04/11/2021 tarih ve 2021/1127 sayılı Kurul kararı.
[152] 01/09/2022 tarihli ve 2022/853 sayılı Kurul kararı.

2.1.2. Veri Kayıt Sistemi

Kişisel verilerin işlenmesi sürecinin önemli ve karmaşık kısımlarından bir diğeri ise veri kayıt sistemi oluşturulmasıdır. KVKK otomatik olmayan veri işlemelerin mevzuat kapsamında değerlendirilebilmesi için veri kayıt sistemi kapsamında işlenmesini şart koşmuştur.

KVKK'nın 3/1-h maddesinde veri kayıt sistemi "*Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistem...*" olarak tanımlanmıştır. Tanımdan anlaşılacağı üzere elektronik veya fiziki ortamda veri kayıt sistemi oluşturulmasının önünde bir engel bulunmamaktadır. Diğer taraftan bir kâğıda rastgele herhangi kişisel verilerin belirli kriterler kullanılmadan kaydedilmesi bir KVKK koruması kapsamında kişisel veri işleme olarak kabul edilmeyecektir.[153]

Tüzük'ün 4. maddesinde tanımlanan dosyalama sistemi, KVKK'da düzenlenen veri kayıt sistemine karşı gelmektedir. İlgili tanıma göre "*işlevsel veya coğrafi bir temelde merkezi, ademi-merkezi veya dağınık olarak spesifik kriterlere göre erişilebilen yapılandırılmış herhangi bir kişisel veri dizisi*" dosyalama sistemidir. Ayrıca KVKK'ya paralel biçimde otomatik olmayan yollarla işlenen verilerin Tüzük kapsamında korunması için dosyalama sistemi kapsamında tutulması gerekmektedir.

Uygulamada kişisel verilerin bir veri kayıt sistemi kapsamında mı yoksa gelişi güzel mi kaydedildiğinin tespiti kolay değildir. Veri kayıt sisteminin tespitini kolaylaştırmak için doğrudan Kurum tarafından yayınlanan açıklayıcı bir dokuman bulunmamaktadır. Ancak İngiltere Veri Koruma Otoritesi (ICO) tarafından yayınlanan dosyalama sistemi ile ilgili sorular dokümanında belirli kriterle göre veri kayıt sisteminin tespitinin mümkün olduğu ifade edilmiştir.

ICO, tarafından yayınlanan dokuman birden fazla yöntem sunmaktadır. Bunlardan ilki ısı testi (*temp test*) olarak ifade ettikleri yöntemdir.[154] Bu teste göre işe yeni başlamış bir stajyer kişisel verilere ilişkin kayıtlara bakarak istediği veriyi kolayca bulabiliyorsa veri kayıt sisteminin mevcut olduğu anlaşılmalıdır.

---

[153] Kişisel Verilerin Korunması Kanunu Hakkında Sıkça Sorulan Sorular, 2018, s. 30.
[154] Dawson-Damer v Taylor Wessing LLP [2017] EWCA Civ 74 (16 February 2017).

Diğer yöntemde ise somut olayda üç sorunun sorulması yoluyla veri kayıt sisteminin varlığı tespit edilmeye çalışılır.[155] Bunlardan ilki kayıt yönteminde verilere kolay erişilmesi hedefleniyor mu? İkinci soru bireysel özelliklere göre veriler sınıflandırılmış mı? Örneğin isimlerine göre bir sınıflandırma yapılmış olabilir. Üçüncü soru ise kayıtlar verilere kolay erişmek amacıyla herhangi bir yöntemle tasnif edilmiş mi? Eğer bu üç sorunun cevabından bir tanesi olumluysa veri kayıt sisteminin varlığı için yeterli kabul edilmektedir.

Dosyalama sisteminin tespitine ilişkin bir diğer karar Finlandiya Veri Koruma Kurulu ve Finlandiya Yüksek Mahkemesi tarafından verilmiştir. Kapı kapı dolaşarak vaaz veren Yehova'nın Şahitleri Topluluğu isimli cemaat mensupları, uğradıkları evlerde görüştükleri kişiler hakkında din, inanç, isim, yaş gibi bilgileri kaydetmektedir. Bu notların amacı daha sonra bu bölgeyle iletişime geçecek kişiler için yol gösterici olmasıdır.

Fin Veri Koruma Denetçisi[156] fiziki olarak sürdürülen bu veri işleme faaliyetlerini, konuyu Fin Veri Koruma Kurulu gündemine götürmüştür. Fin Veri Koruma Kurulu, Yehova'nın Şahitleri Topluluğu'nun veri işleme ilkelerine uymadığını belirterek altı aylık boyunca kişisel verilerin toplanmasına ilişkin faaliyetlerinin yasaklanacağına hükmetmiştir. Cemaat mensupları tarafından tutulan ve daha sonra aynı bölgeye gidecek üyelere yol göstermek amacıyla topluluk içinde paylaşılan notlar oldukça basit olsa da, bu notların kaydediliş biçimi nedeniyle dosyalama sistemi kapsamına girdiği tespit edilmiştir.

İlgili kararın dosyalama sistemi kavramına ilişkin değerlendirme bölümünde, eğer kapı kapı vaaz etme sırasında toplanan isimler ve adresler ile temasa geçilen kişilerle ilgili diğer bilgilerden oluşan bir dizi kişisel veri sonraki kullanımlar için kolayca tekrar bulunabilmelerini sağlayan kriterlere göre yapılandırılmışsa, böyle bir veri setinin bu konsepte girmesi için veri sayfalarının, özel listeler veya diğer arama yöntemlerini içermesinin gerekli olmadığı ifade edilmiştir.[157]

Ziyaret ettikleri kişilerden birden fazla amaçla kişisel veri toplayan ve cemaatin diğer üyeleriyle paylaşan görevliler, ilgili kişilere verilerin toplanması ve işlenmesi

---

[155] ICO, dosyalama sistemi ile ilgili sıkça sorulan sorular, https://ico.org.uk/media/1592/relevant_filing_systems_faqs.pdf Erişim Tarihi:20.01.2023.
[156] Fin Veri Koruma Denetçisi'nin resmi adı Tietosuojavaltuutettu'dur.
[157] Para. 62.

ile ilgili hiçbir bilgi vermeden ziyaretlerini gerçekleştirmiştir. Cemaatin kapı kapı dolaşarak vaaz verme faaliyeti Finlandiya Veri Koruma Kurulu tarafından yasaklanmış; ayrıca Finlandiya Danıştayı tarafından ABAD'dan bu kararın yasallığı hakkında görüş istenmiştir. ABAD, kişilerin rızası olmaksızın, erişebilecek kişi sayısı bilinmeksizin risk taşıyacak şekilde işlendiği yönünde görüş bildirmiştir.[158] Finlandiya Yüksek Mahkemesi'nin ABAD'a yönelttiği 4 soru incelendiğinde yukarıda yer verdiğimiz kriterlerden faydalanıldığı açıkça anlaşılmaktadır.

Türkiye'de somut bir kriter konulmadığı gibi İngiltere'de yayınlanan dokümanın da her bir olay bazında uygulanarak o olay bazında sonuç verecek bir yöntem olduğu görülmektedir. Dolayısıyla tüm veri işleme faaliyetlerini genel olarak veri kayıt sistemi veya veri kayıt sistemi değil biçiminde niteleyecek bir yöntem mevcut değildir. Yetkili veri koruma otoritesinin her bir vakada veri kayıt sistemi olup olmadığını somut biçimde incelemesi ve hakkaniyete göre karar vermesi gerekmektedir.

2.1.3. İlgili Kişi

KVKK'nın m. 3-1/ç'de düzenlenen ilgili kişi kavramı "*kişisel verisi işlenen gerçek kişiyi*" ifade etmektedir. KVKK'da ilgili kişi olarak tanımlanmakla birlikte veri öznesi veya veri sahibi olarak kullanımlar da mevcuttur.

İlgili kişi kavramının somutlaşması adına örnek vermek gerekirse bir iş başvurusu yapan gerçek kişi özgeçmişinde yer alan bilgiler bakımından ilgili kişi sıfatına sahiptir. Diğer taraftan bir polis tarafından tutulan olay yeri inceleme tutanağında bilgileri yer alan gerçek kişiler, tutanakta ismi ve imzası olan polis memuru dahil olmak üzere ilgili kişi sıfatına sahiptir.

Somut olayda kişisel verisi işlenen her bir gerçek kişi ilgili kişi olarak nitelendirilmektedir. Buradan anlaşılacağı üzere bir veri işleme faaliyetinde birden fazla ilgili kişi olması mümkündür. Günümüzde yapılan veri işleme faaliyetlerinde ise aynı veri işleme faaliyeti kapsamında milyonlarca kişinin verisinin işlendiğini biliyoruz. İnternet servis sağlayıcıları, sosyal medya platformları, telefon

[158] **Gültekin Várkonyi**, Gizem: "Avrupa Birliği Genel Veri Koruma Tüzüğü Kapsamında Gerçek Kişilerin Kişisel Sosyal Robot Kullanımından Doğabilecek Sorumlulukları", Kişisel Verileri Koruma Dergisi, C. 2 S. 2, s. 26.

operatörleri gibi birçok veri sorumlusu aynı hizmet kapsamında milyonlarca müşterisinin kişisel verilerini işlemektedir. Bu veri işleme faaliyeti kapsamında verisi işlenen herkes ilgili kişi sıfatını haizdir.

2.1.4. Veri Sorumlusu

KVKK'nın m. 3/ı hükmünde düzenlenen veri sorumlusu kavramı "*Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi*..." olarak tanımlanmıştır. Veri sorumlusu, veri kayıt sitemini kuran ve yöneten, veri işleme sürecinde kişisel verilerin hangi amaçla ve yöntemle işlendiğini tespit eden gerçek veya tüzel kişilerdir.

İlgili tanımdan da anlaşılacağı üzere veri sorumlusu veri işleme sürecinin en önemli aktörü konumundadır. Veri işleme sürecinde tüm kararları alan, veri kayıt sistemini belirleyen ve işlediği verileri korumakla yükümlü olan veri sorumlusudur. Veri sorumlusunun, veri işleme faaliyetinde gerçekleşecek bir hukuka aykırılık nedeniyle hukuki ve cezai sorumluluğu bulunmaktadır. Veri sorumlusunun sorumluluğu yalnızca kendi himayesindeki verilerden ibaret olup kimse kontrolü altında olmayan kişisel verilerden dolayı sorumlu tutulmayacaktır. Hukuki bir zorunluluk nedeniyle veri işliyor olması veri sorumlusu sıfatını kaldırmayacağı gibi aydınlatma, veri güvenliğini sağlama ve sicile bildirme vb. yükümlülüklerini de kaldırmayacaktır. [159]

Gerçek kişi tarafından kurulan veri kayıt sistemi çerçevesinde yürütülen veri işleme faaliyetinde veri sorumlusu sıfatı ilgili gerçek kişiye aittir. Kamu hukuku veya özel hukuk tüzel kişileri açısından bakıldığında da benzer bir tablo olduğu görülmektedir. Tüzel kişiler kendi kurdukları ve yönettikleri veri kayıt sistemi kapsamında veri sorumlusu sıfatını haiz olup hukuki ve cezai sorumluluk ilgili tüzel kişilik hakkında doğmaktadır.

Veri sorumlusu kavramının karşılığını tam anlamıyla belirleyebilmek için uygulamada karışması mümkün olan veri işleyen kavramıyla birlikte değerlendirmek gerekmektedir.

---

[159] Veri Sorumlusunun benzer kavramlarla farkı ifade edildikten sonra veri sorumlusunun hukuki ve cezai sorumluluğuna değinilecektir.

2.1.4.1. Veri İşleyen- Veri Sorumlusu Farkı

KVKK'da veri işleyen kavramı "*veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi*" şeklinde tanımlanmıştır. İlgili başlıkta verilen veri sorumlusu tanımı ve yukarıda verilen veri işleyen tanımı birlikte değerlendirildiğinde iki kavram arasındaki temel fark olan karar verme süreci veri sorumlusunun yetkisindeyken veri işleyen karar alma sürecinde etkisiz konumdadır. Veri kayıt sistemi veri sorumlusu tarafından kurulur ve yönetilir veri işleyen kendisine verilen yetkiye dayanarak veri işlemektedir.[160]

Veri işleyen uygulamada bağımsız bir tüzel kişi, veri sorumlusu tüzel kişinin iş ortağı veya bağımsız çalışan bir gerçek kişi olabilir. Aralarında yalnızca veri işleme ilişkisi kapsamında bir hukuki ilişki kurulup bunun haricinde hiç bir hukuki temasları olmayabilir.

Somut örneklerle açıklamak gerekirse uygulamada oldukça yaygın karşılaşılan örneği bulut sunucu sistemi kullanan kişiler ve bulut sunucu hizmet sunan teşebbüslerdir. Veri boyutlarının her geçen gün artması ve fiziki depolama sistemlerinin yetersiz kalması sonucu bulut sistemler yaygın biçimde kullanılmaya başlamıştır. Bulut sisteminde veriler uzak sunucuda depolanmakta olup bu sunucu veri sorumlusu tarafından yönetilmemektedir. Veri sorumlusu otomatik veri kayıt sistemini başlattığında program bulut sunucu üzerinde kişisel verileri işlemeye başlayacaktır.

Bulut sunucu örneğinde veri kayıt sistemini oluşturan ve yöneten yine veri sorumlusu olan gerçek veya tüzel kişidir.[161] Bulut sunucu hizmeti sunan teşebbüs ise yalnızca veri sorumlusu tarafından belirlenen sistemin uygulamasını sağlamakta ancak veri işlenmesinden bir menfaat elde etmemektedir. Diğer taraftan bulut sunucu hizmeti sunan teşebbüs ve veri kayıt sistemini kuran veri sorumlusu arasında hiyerarşi de bulunmaması gerekmemektedir.

Örneklerden anlaşılacağı üzere veri işleme süreci genellikle tek gerçek veya tüzel kişi tarafından tamamlanmadığından uygulamada veri sorumlusu kavramının tespiti kolay olmamaktadır.

---

[160] **Taştan**, s. 71 vd.

[161] **Başara**, Gamze Turan: "Kişisel Veri İşleme Sözleşmesi", Uyuşmazlık Mahkemesi Dergisi, S.16, 2020, s. 66.

Kurum tarafından yayınlanan veri sorumlusu ve veri işleyeni ayrıt etmeye yönelik dokümanda, belirli konularda kimin karar verdiğine odaklanılması gerektiği belirtilmiştir.[162] İlgili dokumana göre, kişisel verinin toplanmasına, toplanma yöntemine, toplanacak veri türlerine, kullanım amaçlarına, kimlerin verilerinin toplanacağına, ilgili verilerin paylaşılıp paylaşılmayacağına ve kiminle paylaşılacağına, verilerin ne kadar süreyle saklanacağına kimin karar verdiği kriterlerine göre somut olayda veri sorumlusu belirlenecektir.

Diğer taraftan veri sorumlusunun ilgili dokümandan veri sorumlusunun bir takım yetkileri veri işleyene devretmesi veri işleyenin sıfatının değişmesine yol açmayacaktır. Kişisel verilerin toplanması sürecinde kullanılacak sistemler ve metotlar, saklanacağı yöntem, korunması amacıyla alınacak güvenlik önlemleri, aktarımı yapılacaksa yapılacağı yöntem, saklanmasına ilişkin mevzuattaki sürelerin doğru uygulanabilmesi uygun metot, silinmesi, yok edilmesi ve anonim hale getirilmesi yöntemleri veri işleyen tarafından belirlenebilir.

Veri işleme sürecinde veri işleyen kendi yönettiği bilişim alt yapısına ilişkin kararlar alabilir. Bu durum veri işleyen sıfatından çıkıp veri sorumlusu olarak sorumlu tutulmasına yol açmayacaktır.

Veri sorumlusu ve veri işleyen ilişkisini somut ve sık karşılaşılan örnekler üzerinden incelemeye devam edecek olursak bir veri işleme faaliyetinde tek veri sorumlusu olması zorunlu değildir. Aynı olayda birden fazla veri işleme faliyeti olması birden fazla veri sorumlusu bulunmasına yol açacaktır.

Çevrim içi satış yapan bir şirketin, ödeme altyapısı sunan bir şirketle anlaşarak alıcıların verilerini işlenmesi durumda; ödeme altyapısı sunan şirket satıcının veri işleyeni değil veri sorumlusudur. Sebeplerini inceleyecek olursak ödeme altyapısı sunan şirket sağlıklı biçimde ödeme alabilmek için ürün satın alanlardan hangi verilerin toplanması gerektiğine kendisi karar vermektedir. İşlediği verilerin kullanım amaçlarını kendisi belirlemektedir. Ürün satışından bağımsız olarak doğrudan kişisel verileri işlenen müşterilere kendi hüküm ve şartlarını uygulamaktadır. Ayrıca ödeme alması nedeniyle kredi kartı bilgilerinin silinmesi gibi tabi olduğu hukuki yükümlülükler mevcuttur. Aynı olayda ürün satışı aşamasındaki veri işleme faaliyeti için veri sorumlusu çevrim içi ürün satan

[162] https://www.kvkk.gov.tr/Icerik/4195/Veri-Sorumlusu-ve-Veri-Isleyen Erişim Tarihi: 17.01.2022.

şirketin kendisiyken ödeme aşamasında işlenen veriler için veri sorumlusu doğrudan ödeme altyapısı sunan şirkettir.

2.1.4.2. Ortak Veri Sorumlusu

Tüzük'ün açıkladığımız bölümde aktardığımız üzere ortak veri sorumlusu kavramı Tüzük'de açıkça düzenlenen bir sıfatken KVKK'da benzeri bir düzenleme mevcut değildir.[163] Ancak Kurul bazı kararlarında ortak veri sorumluluğuna ilişkin tespitler yapmıştır.

Araç kiralama yazılımı yapan ve satan firmalar tarafından, araç kiralayan kişilerin kişisel verilerini işleyen ve işlenen verilerin araç kiralama firmaları arasında veri paylaşılmasını sağlayan program Kurum tarafından incelenmiştir. İnceleme sonucunda ilgili program hakkında verilen Kurul kararında[164] ortak veri sorumlusu kavramına ilişkin tespitler mevcuttur.

Araç kiralama şirketlerine yazılım hizmeti sunan teşebbüsler tarafından geliştirilen ve satılan yazılımda tüm araç kiralama şirketlerini tek çatı altında toplanmaktadır. Yazılım üzerinden şirketler arasında bilgi akışını sağlanmakta, sisteme kayıtlı araçlar takip edilmekte, trafik cezası vb. durumları anlık takip edilmektedir. Ancak yazılım üzerinden paylaşılan ve takip edilen hususlar bunlardan ibaret değildir. Araç kiralama şirketleri daha kendi aralarında müşteri bazlı olarak kara liste uygulaması da yapmakta olup bu kapsamda kara listeye aldıkları kişilerin kişisel verilerini birbiriyle paylaşmaktadır.

İlgili kararda araç kiralama firmaları ve araç kiralama yazılımı üreten ve satan şirketlerin ortak veri sorumlusu sıfatı ile hareket ettiği tespiti yer almaktadır. Ortak veri sorumlusunun tespitine için bakılan kriterlere incelendiğinde ise "*ortak bir amacın varlığı ve kişisel verilerin işlenmesindeki temel araçların birlikte belirlenmesi ortak veri sorumluluğunu beraberinde getirmekte...*" ifadesi dikkat çekmektedir. Dolayısıyla ortak veri sorumlusu tespiti için ortak amaç ve temel amaçların birlikte belirlenmesi kriterleri mevcuttur. Ayrıca taraflardan bir tanesi işlenen verilere erişemese ve yükümlülükler eşit paylaşılmasa dahi ortak veri sorumlusu sıfatının kalkmayacağı kararda yer almaktadır.

---

[163] 95/46/AT sayılı Direktif'te veri sorumlusu tanımı "tek başına veya başkalarıyla ortaklaşa" ibaresini içerirken KVKK'da veri sorumlusu tanımı benzeri bir ibareyi içermemektedir.
[164] 23/12/2021 tarihli ve 2021/1303 sayılı Karar.

İlgili kararda her iki ortak veri sorumlularının hukuki ve cezai sorumlulukları da tartışılmış ve her bir somut olay için "*işlenen verinin ilk ve son kullanıcısının kim olduğu; veri girişini kimin yaptığı; hangi amaçla söz konusu verinin girildiği; verinin değiştirilmesine veya silinmesine yahut aktarılmasına kimin karar verdiği; veriyi toplayan dışında kalan veri sorumlularının bu veri ile hangi faaliyetleri gerçekleştirdiği*" hususlarına bakılması gerektiği ifade edilmiştir.

Kurul tarafından Temmuz 2022 tarihli, Kişisel Verilerin Korunmasına İlişkin Bankacılık Sektörü İyi Uygulamalar Rehberi'nde tüm birlikte veri işleme faaliyetlerinin müşterek sorumluluk doğurmayacağı belirtilmiştir. Diğer bir deyişle verileri birbiriyle paylaşan kişiler her durumda ortak veri sorumlusu kabul edilmemektedir. Ortak veri sorumlusu olmanın tek şartının veri işleme faaliyetinin amacını ve vasıtaları yani veri işleme sürecinde kullanılacak aracı birlikte belirlemek olduğu belirtilmiştir.[165] Ayrıca ilgili rehberde taraflar arasında yapılacak sözleşmenin veri işleme sürecine ilişkin yükümlükleri açık biçimde içermesinin somut olayda tarafların sorumluluk sınırlarının tespitini kolaylaştıracağı ifade edilmiştir.

2.1.5. Veri Sorumluları Sicili

KVKK'nın 16. maddesinde Kurul gözetimi altında ve kamuya açık biçimde veri sorumluları sicili tutulması gerektiği düzenlemiştir. Kurul tarafından belirlenen veya KVKK'da yer alan istisnalar[166] haricinde veri işlemek isteyen kişiler veri sorumluları siciline kayıt olmak zorundadır.[167] Kurul, 2018/75 sayılı kararı ile arabuluculuk faaliyeti yürüten kişileri VERBİS'e kaydolma yükümlülüğünden muaf tutmuş ancak bu kararla ilgili bir gerekçe açıklamamıştır. Ancak çok sayıda arabulucu olması nedeniyle her birinin veri sorumlusu olarak VERBİS'e girmesine ihtiyaç görülmediği düşünülmektedir.[168]

İlk bölümde yer verildiği üzere ülkemizde veri sorumluları sicili olarak VERBİS[169] kurulmuş olup Ekim 2018 tarihinden itibaren kullanılmaya başlanmıştır. VERBİS'e kaydedilecek bilgiler KVKK'da ve ilgili yönetmelikte açıkça sayılmakta

---

[165] Kişisel Verilerin Korunmasına İlişkin Bankacılık Sektörü İyi Uygulamalar Rehberi, s. 20.
[166] Kurul ilgili maddede belirtilen şartları sağlayan veri sorumlularının VERBİS'e kaydolmaktan muaf tutabilir.
[167] KVKK m. 16/2.
[168] **Dülger**, Murat Volkan: Kişisel Verileri Koruma Kurulu'nun 18 Ağustos 2018 Tarihli Resmi Gazete'de Yayınlanan Kararlarına İlişkin Değerlendirme, s. 6.
[169] https://verbis.kvkk.gov.tr/ Erişim Tarihi: 03.02.2023.

olup bunlar, veri sorumlusunun, varsa veri sorumlusunun temsilcisinin kimlik ve adres bilgileri, kişisel verilerin işlenme amaçlarının nelerden ibaret olduğu, işlenecek verinin konusu kişi grupları ve bu kişi gruplarına ait veri kategorileri, kategorilerin kapsamı vb. konulardaki açıklamalar, işlenen verilerin aktarılabileceği alıcılar, ülke dışına aktarılabilecek kişisel veriler hakkında bilgi, kişisel verilerin güvenliğini sağlamak amacıyla alınan önlemler ve verilerin işlendiği amaç için gerekli azami süredir.[170]

VERBİS ile amaçlanan verisi işlenen kişiye yani veri sahibine şeffaflık sağlamaktır. Veri sahibi, veri sorumlusunun ismini girdiğinde[171] işlenen verinin kategorisini, işlenme amaçlarını ve ne kadar süre saklanacağını görebilmektedir. Böylece kişisel verilerin işlenmesi süreci veri sahibi açısından da daha açık, şeffaf ve somut hale gelmektedir. VERBİS üzerinden sorgulama yapan kişi, işlenen verilerin hukuka aykırı biçimde işlendiğini tespit ettiği takdirde Kurul'a şikayet veya veri sorumlusuna bildirme hakkına sahiptir. Bu yönüyle VERBİS, KVKK m. 10'da düzenlenen aydınlatma yükümlülüğünün yerine getirilmesine de yardımcı olmaktadır.

2.2. KİŞİSEL VERİ İHLALLERİ

Kişisel verilerin korunması yükümlülüğü kapsamında veri sorumlularının ve üçüncü kişilerin sorumluluklarına ilişkin mevzuata birinci bölümde yer vermiştik. Kişisel veri ihlalleri, kişisel verilerin korunmasını amaçlayan hükümlerin ihlal edilmesi suretiyle oluşmaktadır. Bu nedenle öncelikle veri işleme sürecine ilişkin yükümlülüklere değinilecek akabinde bu yükümlülükleri ihlal eden davranışlara yer verilecektir.

Kişisel verilere ilişkin yükümlülüklerin tespiti maksadıyla KVKK ve TCK incelenmesi uygun olacaktır. KVKK'nın m. 10 düzenlemesinde aydınlatma yükümlülüğü, m. 12 düzenlemesinde veri güvenliğine karşı yükümlülükler, 15. maddesinde Kurul tarafından verilen kararları yerine getirmeme, 16. maddesinde

---

[170] KVKK m. 16 ve Veri Sorumluları Sicili Hakkında Yönetmelik m. 7/2, 9 ve 10'da düzenlenmiştir.
[171] https://verbis.kvkk.gov.tr/Query/Search adresinden veri sorumlusu adıyla sorgulama yapılabilmektedir.

düzenlenen kayıt ve bildirim yükümlülüğüne[172] aykırı davranma hususları düzenlemiştir.[173]

TCK'nın ilgili hükümleri olan 135-140. maddelerine bakıldığında kişisel verilerin korunması yükümlülüğüne ilişkin üç suç mevcuttur. Bu suçlar TCK'nın 135. maddesinde düzenlenen kişisel verilerin kaydedilmesi, 136. maddesinde düzenlenen verilerin hukuka aykırı olarak verme veya ele geçirme ve 137. maddesinde yer alan verileri yok etmeme suçlarıdır.

Genel itibariyle KVKK kapsamında getirilen yükümlülükler ve TCK'da yer alan düzenlemelerin birbiriyle tamamlayıcı olduğu, KVKK kapsamında kabahat olarak ifade edilen hususların ise yine aynı doğrultu da kişisel verilerin korunması hakkını sağlamayla doğrudan ilgili olduğu görülmektedir. Çalışma kapsamında kişisel verilerin korunması yükümlülüğünün ihlali olarak ifade edilecek bu haller Kurul kararları ve öğretiye yapılan atıflarla incelenecektir.

2.2.1. Aydınlatma Yükümlülüğü

Veri sorumlusunun aydınlatma yükümlülüğü KVKK'nın 10. maddesinde düzenlenmiş olup ilgili maddeye göre kişisel verilerin elde edilmesi sırasında doğrudan veri sorumlusu veya yetkilendirdiği kişinin veri sahibine belirli bilgileri vermesi gerekmektedir. Bu bilgiler veri sorumlusunun ve eğer temsilcisi varsa temsilcisinin de kimliği, verinin işlenme amacı, işlenen verilerin kimlere aktarılma ihtimali olduğu ve aktarılma amaçları, verinin hangi yöntemle toplanacağı ve hukuki dayanağı, ilgili kişinin haklarının[174] neler olduğudur. Veri sorumlusu bu

---

[172] Bahsi geçen kayıt ve bildirim yükümlülüğü ile Veri Sorumluları Siciline gereken kaydın yapılması ifade edilmektedir. Kayıt yükümlülüğünün kapsamı ve sicil hakkında bilgi bu bölümde aktarılacaktır.

[173] **Kart**, Aslıhan/**Ketizmen**, Muammer: Kişisel Verilerin Korunmasına İlişkin Suç ve Kabahatler, C.1 S. 2, 2019, 17-29, s. 25.

[174] KVKK m. 11'de ilgili kişinin hakları düzenlenmektedir: "…*a) Kişisel veri işlenip işlenmediğini öğrenme, b) Kişisel verileri işlenmişse buna ilişkin bilgi talep etme, c) Kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme, ç) Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme, d) Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini, isteme, e) 7 nci maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme, f) (d) ve (e) bentleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme, g) İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme, ğ) Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme...*"

kapsama uygun biçimde yükümlülüğünü yerine getirmediği takdirde idari para cezası ile cezalandırılmaktadır.[175]

Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ[176] (Aydınlatma Tebliği) ile aydınlatma yükümlülüğü açıklanmış ve bu yükümlülük kapsamında veri sorumlusu veya yetkilendirdiği kişinin uyacağı usul ve esaslar düzenlenmiştir. Ancak veri sorumlusunun muhatabını aydınlatma yükümlülüğü sadece KVKK'da değil ayrıca özel mevzuatlarda da yer almaktadır.

Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik m. 9 hükmünde trafik ve konum verilerinin işlenebilmesi durumunda elektronik haberleşme hizmeti sunan şirketlere veri türleri, veri işleme amacı ve süresine ilişkin veri sahiplerine (abonelere/kullanıcılara) bilgi verme yükümlülüğü getirilmiştir. Elektronik haberleşme sektörü regüle edilen bir sektördür. Bu nedenle kişisel verilerin korunması maksadıyla getirilen genel düzenlemelere ek olarak kullanıcıyı korumayı hedefleyen önlemlerin getirilmesi olağandır.

Yukarıda yer verildiği üzere basit ve sınırları belirli bir yükümlülük olmasına karşın Kurul tarafından aydınlatma yükümlülüğüne aykırı davrandığı tespit edilen veri sorumluları mevcuttur. Bu noktada yükümlülüğün amacı ve bu amaca nasıl ulaşılabileceği de önem arz etmektedir. Aydınlatma yükümlülüğü temelinde bilgilendirmeyi amaçlamakta olup bu amaca ulaşabilmesi için muhatabının anlayabileceği açıklıkta yapılması gerekmektedir.[177] Kullanılan dil doğru biçimde anlaşılabilmek için oldukça önemlidir. İlgili kişinin anlaması mümkün olmayan zorunlu olmadığı halde teknik terimler ve ilgisiz bilgiler içeren, gerekenden uzun ve karmaşık, birden fazla anlama gelen ifadeler barındıran aydınlatma metinleri ile bu yükümlülüğünün yerine getirilmesi mümkün değildir.[178]

---

[175] KVKK m. 18'de kabahatler başlığıyla her bir ihlale uygulanacak idari para cezası düzenlenmiş olup 18/1-ç "*a) 10 uncu maddesinde öngörülen aydınlatma yükümlülüğünü yerine getirmeyenler hakkında 5.000 Türk lirasından 100.000 Türk lirasına kadar*"

[176] Resmi Gazete Tarihi: 10.03.2018 Resmi Gazete Sayısı: 30356.

[177] **Braun**, Cihan Avcı: Kişisel Verilerin İşlenmesinde Rıza, Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, C.15 S.1, 2018, 13-35, s. 24.

[178] **Özer Deniz**, Miray: Özel Nitelikli Kişisel Verilerin İşlenmesi ve Bundan Doğan Sorumluluk, XII Levha Yayınları, İstanbul, 2022, s. 105.

Kurulun çevrim içi platform üzerinden iş başvurusu alan bir şirketler topluluğunun aydınlatma yükümlülüğüne ilişkin kararında[179] aydınlatma metninin okunduğu ve açık rıza verildiğine dair tek onay kutucuğu bulunması incelenmiştir. Aydınlatma metninin okunduğu ve ilgili kişilerin kişisel verilerinin işlenmesine açık rıza verildiğine dair seçme haklarının da tanındığı bir yapıya geçilmesi gerektiği tespit edilmiştir. Bu amaçla açık rıza metninin onaylandığının ispatını sağlayacak iki onay seçeneği sunan bir ara yüz ile ayrıştırılması konusunda veri sorumlusunun talimatlandırılması uygun görülmüştür.

Aydınlatma yükümlülüğünün kim tarafından yerine getirileceği hususundaki tereddüt üzerine Kurul tarafından inceleme yapılmıştır. Yapılan inceleme sonucunda alınan kararda bizzat veri sorumlusu tarafından veya yetkilendireceği kişi tarafından yerine getirilebileceği konusunda veri sorumlusuna seçim hakkı tanındığına hükmedilmiştir[180]. Yine aynı kararda aydınlatma yükümlülüğünün tek taraflı beyanla yerine getirilebileceği ve yerine getirildiğinin ispat yükünün veri sorumlusuna ait olduğu ifade edilmiştir.

Bir diğer Kurul kararında[181] ise kişisel verilerin işlenmesini hizmet şartı olarak koyan internet sitesinin aydınlatma yükümlülüğünü yerine getirmediği tespit edilmiştir. İlgili kararda aydınlatma metninin, Aydınlatma Tebliği'nin gereklerine uygun biçimde düzenlenmediği, dolayısıyla ilgili metnin Aydınlatma Tebliği'nde yer alan hükümler dikkate alınmak suretiyle güncellenmesi, ayrıca yukarıda yer verilen karardaki içtihatla paralel biçimde aydınlatma yükümlülüğü ve açık rızanın alınması işlemlerinin ayrı ayrı yerine getirilmesi gerektiğine hükmedilmiştir.

Veri koruma hukuku kapsamında aydınlatma yükümlülüğün temelde iki yolla ihlal edildiği görülmektedir. Bunlardan birincisi aydınlatma metninin KVKK ve Aydınlatma Tebliği'ne uygun biçimde hazırlanması ikincisi ise açık rızaya ilişkin onayın ayrıca alınmasıdır.

2.2.2. Veri Güvenliğine Karşı Yükümlülükler

Uygulamada en sık karşılaşılan kişisel veri ihlali türü veri sızıntılarıdır. Veri sızıntılarının sık yaşanmasının sebebi genellikle bilişim konusundaki teknik

[179] 26/07/2018 tarihli ve 2018/90 sayılı Kurul kararı.
[180] 30/01/2020 tarihli ve 2020/71 sayılı Kurul kararı.
[181] 08/07/2019 tarih ve 2019/206 sayılı Kurul kararı.

zafiyetlerdir. Ayrıca personelin veri koruma hukuku kapsamında bilgi sahibi olmaması gibi idari sorunlar da sıklıkla veri güvenliğini ihlal etmektedir. Bu eksiklikler nedeniyle veri güvenliğine karşı yükümlülüklerin[182] ihlaline sıklıkla rastlanmaktadır.

İlgili maddede veri sorumlusunun[183] kişisel verilerin hukuka aykırı biçimde işlenmesini önlemek, işlenen kişisel verilere erişilmesini önlemek ve muhafazasını sağlamak olmak üzere üç görevi olduğu ifade edilmiştir. Aynı zamanda bu amaçları gerçekleştirmeye elverişli güvenlik önlemlerini, her türden teknik ve idari tedbirleri önceden alma yükümlülüğü düzenlenmiştir. Ancak eğer kişisel verilerin koruması amacıyla alınan tedbirler yeterli olmazsa veri sorumlusunun ilgili kişiye ve Kurul'a bildirim yükümlülüğü de mevcuttur.[184]

2.2.2.1. Tedbir Alma Yükümlülüğü

Madde hükmünün lafzından tedbirleri kendi içerisinde idari ve teknik olmak üzere ikiye ayırdığı anlaşılmaktadır. İdari tedbirler yönetim ve organizasyon ile ilgili hususlardan oluşurken teknik tedbirler ise bilişim altyapısı ve bu altyapının kullanımı ile ilgilidir. Veri güvenliğine ilişkin idari ve teknik tedbirleri Kurum'un Kişisel Veri Güvenliği Rehberi[185] ve öğreti ışığında değerlendireceğiz.

2.2.2.1.1. İdari Tedbirler

Veri sorumlusunun olası bir veri güvenliği tehdidini en aza indirmek için alması gereken idari tedbirlerin neler olduğuna dair veri güvenliği rehberinde açıklama yer almakla birlikte idari tedbir tanımı yapılmamıştır.

İlgili rehberin içeriğine bakıldığında idari tedbirlerin kapsamına kişisel veri işleme envanteri hazırlanması, detaylı kurumsal politikalar oluşturulması[186], veri sorumluları veya veri sorumlusu ile veri işleyen arasında sözleşmeler ve gizlilik taahhütnameleri hazırlanması, veri güvenliğini sağlamaya yönelik kurum içi denetimler yapılması[187], risk analizi yapılması, iş sözleşmeleri ve disiplin yönetmeliklerine KVKK hükümlerine uygun maddeler eklenmesi, kurumsal

---

[182] KVKK m. 12.
[183] KVKK m. 12/2'de eğer veri sorumlusu adına işleyen bir gerçek ve tüzül kişi varsa müşterek sorumluluk doğacağı düzenlenmiştir.
[184] KVKK m. 12/5.
[185] https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf Erişim Tarihi:07.02.2023.
[186] Erişim, Bilgi Güvenliği, Kullanım, Saklama ve İmha vb.
[187] Denetimler periyodik ve/veya rastgele olabilir.

iletişim[188], veri güvenliği ve KVKK hükümleri hakkında eğitim ve farkındalık çalışmaları, VERBİS'e bildirimlerin zamanında yapılması girmektedir.[189]

İdari tedbirler incelendiğinde insan kaynakları ve hukuk konularıyla yakından ilgili kurallar olduğu görülmektedir. İnsan kaynakları ile ilgili olan bölüm kişisel verilere erişimi olan çalışanların veri güvenliğine ilişkin bir takım eğitimlerden geçirilmesi ve kişisel verilerin korunması mevzuatına uygun davranıp davranılmadığının denetlenmesidir. İdari tedbirlerin hukuki tarafını ise sözleşme ilişkileri, gizlilik taahhütnameleri, iş sözleşmeleri ve disiplin yönetmeliği hazırlanması süreçleri oluşturmaktadır.

Uygulamada idari tedbirlerin yerine hangi yollarla yerine getirildiği incelenmiş ve idari tedbirler kapsamında veri sorumlularının sıklıkla aldığı tedbirler tespit edilmiştir. Bu kapsamda veri sorumlularının kişisel veri envanteri hazırladığı, veri işleme politika belgesi oluşturduğu, veri saklama ve imha politikası belgesi oluşturduğu, kamera izleme politika belgesi oluşturduğu, verbis kaydı yaptığı, kişisel veri içeren gereksiz evraklar temizlediği, kurumsal e posta adreslerinin altına kişisel verilerin kullanılması ve gizliliği hakkında bilgilendirme metni eklediği, kurumsal internet sayfalarına veri işleme politika metni eklediği, aydınlatma metni ve başvuru formu koyduğu, veri işleyen varsa farkındalık eğitimleri verildiği, çalışanlara veri koruma hukuku eğitimi verildiği anlaşılmıştır.[190]

İlgili bölümde Kurul'un, idari ve teknik tedbirlerin alınmadığını tespit eden kararlarına yer verilecektir. Kurul'un somut olayda veri koruma amacıyla veri sorumlularından beklediği tedbirlerin kapsamı tespit edilmeye çalışılacaktır.

2.2.2.1.2. Teknik Tedbirler

KVKK'nın 12. maddesi kapsamında alınması beklenen teknik tedbirler: Yetki matrisi tutulması ve bu matrise göre yetki kontrolü sağlanması, tüm kullanıcıların erişim kayıtlarının tutulması, kullanıcıların hesap yönetiminin güvenli hale getirilmesi, kullanıcıların ağ güvenliğinin sağlanması, uygulamaların kullanım esnasında yaratabileceği veri güvenliğine ilişkin hataların azaltılması, iletilen ve

[188] Kriz yönetimi, kurul ve ilgili kişiyi bilgilendirme süreçleri, itibar yönetimi vb.
[189] Kişisel Veri Güvenliği Rehberi s. 29.
[190] **İnciroğlu**, Kübra/ **Öge**, Ercan: "İnsan Kaynakları ve Bilgi İşlem Departmanlarının İşletmelerde Kişisel Verilerin Korunmasındaki Rolü: Farklı Sektörlerden Örnek Olay Çalışmaları", Journal of International Social Research, C. 12, S. 65, 2019, s. 1433-1454, s. 1447.

saklanan verinin doğru biçimde şifrelenmesi, düzenli aralıklarla veri işlenen bilişim sistemlerine sızma testi yapılması, saldırı tespit ve önleme sistemleri kurulması, tüm kullanıcıların log kayıtlarının tutulması, veri maskeleme, sistemden veri çıkışını önleyen veri kaybı önleme yazılımları (DLP) kullanılması, veri yedekleme uygulamaları kurulması, bilişim sistemlerini koruyan güvenlik duvarlarının aktif edilmesi, tehditlere önlemeye elverişli biçimde güncellenen anti-virüs programları, gerekli olmayan kişisel verileri silme, yok etme veya anonim hale getirme, şifreleme sürecinin anahtar yönetimidir.

İdari tedbirlerin amacı kişileri eğiterek ve farkındalıklarını artırılarak olası bir hatanın önüne geçmek ve veri sızıntılarını engellemektir. Ayrıca risk analizi yaparak veri ihlalini önlemeye çalışmak ve denetim mekanizmasını aktif tutarak bir veri ihlalini en kısa zamanda tespit etmek de idari tedbirlerin bir parçasıdır. Teknik tedbirler ise hem veri sorumlusu bünyesindeki yetkisiz çalışanların verilere erişimini bilişim alt yapısı ile engellemeyi hem de üçüncü kişilerin işlenen kişisel verilere erişmesini engellemeyi amaçlamaktadır. Bu noktada teknik tedbirlerin daha ziyade kullanılan bilişim sistemlerindeki hata payını en aza indirmeyi hedeflendiğini ifade etmek yanlış olmayacaktır.

Rehberde yer alan teknik tedbirler siber güvenliği sağlanmasını, kişisel veri içeren dijital ortamların güvenliğinin teminini, gerekli bilgi teknoljilerinin oluşturulmasını, kişisel verilerin sağlıklı biçimde yedeklenmesini ve yetkisiz kişilerce erişimin önlenmesini hedefleyen tedbirlerdir. Tedbir içeriklerinden anlaşılacağı üzere bu tedbirler teknoloji altyapısı ve yönetimi ile doğrudan ilgilidir.

Kurul kararları incelendiğinde en sık karşılaşılan veri güvenliği sorunun veri sızıntısı olduğu anlaşılmaktadır.[191] Veri sızıntısı, veri sorumlusu tarafından erişim yetkisi verilen biri veya üçüncü bir kişi tarafından kişisel verilerin elde edilmesidir.

Uygulamada ne kadar önlem alınırsa alınsın dijital ortamdaki bir verinin tam anlamıyla güvenli olduğunu ve hiç bir biçimde ele geçirilemeyeceğini ifade etmek mümkün olmayacaktır. Nitekim dünya çapında bilenen büyük teknoloji teşebbüslerinden dahi büyük veri sızıntıları yaşandığı bilinmektedir.[192]

---

[191] **Özkan**, Oğulcan: Kişisel Verilerin Korunması, Ankara Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk Anabilim Dalı, Yüksek Lisans Tezi, s. 174.

[192] İlk bölümde veri sızıntısına ilişkin global örnekler verilmiştir.

Dolayısıyla burada veri sorumlusundan beklenen en iyi uygulamaları esas alarak verileri güvende tutmak için çabalamasıdır.

2.2.2.1.3. İdari ve Teknik Tedbirlere İlişkin Kurul Kararları

Bu başlıkta veri sorumlusunun idari ve teknik tedbirleri alamaması nedeniyle sorumlu tutulduğu Kurul kararları incelenecektir. Kurul'un benzer nitelikte çok sayıda kararı olması nedeniyle farklı tedbirlere değinen kararlara yer vermeye çalışacağız.

Veri sorumlusu banka nezdinde yaşanan veri sızıntısı hakkında Kurul kararında[193] bankanın 346 müşterisinin şube ve hesap no, isim soy ve isim bilgileri, cep telefonu numaraları ve belirli bir yatırım firmasına yolladıkları işlem tutarı bilgilerinin sızdırıldığı anlaşılmaktadır.

İlgili kararda bir çalışanın e-posta ile üçüncü kişilere bu verileri ilettiği dolayısıyla veri sorumlusunun verdiği eğitimin yetersiz olduğu, DLP yazılımı mevcut olmasına rağmen e-postanın tespit edilemediği, ilgili e-postanın atılmasına dayanak olacak hiç bir sebebin bulunmadığı tespitleri yer almaktadır. Bu tespitler ışığında Kurul gerekli idari ve teknik tedbirlerin alınmadığını değerlendirmiş ve KVKK m. 12/1 hükmüne aykırılık nedeniyle m. 18/1-b kapsamında 225.000 TL idari para cezası uygulanması gerektiğine karar vermiştir.

Kurul'un bir diğer kararında[194] ise veri sızıntısının, veri sorumlusu sigorta şirketinin taşeron çalışanının[195] sistemlerinde tutulmakta olan 91 kişiye ait isim-soy isim, iletişim, araç plaka bilgilerinin bulunduğu listeyi kendine tanımlanan kurum e-posta adresinden şahsi e-posta adresine göndermesiyle gerçekleştiği tespit edilmiştir. Ayrıca veri sorumlusu şirketin tüm çalışanlarına kişisel verilerin korunması eğitimini almadığı ve DLP sisteminin anahtar kelime tespit sistemi ile çalıştığı ancak gönderilen e-postada bu anahtar kelimelerin hiç birinin yer almaması nedeniyle uyarı vermediği hususları ilgili kararda yer almaktadır.

---

[193] 26/11/2019 tarihli ve 2019/352 sayılı Kurul kararı.
[194] 07/05/2020 tarih ve 2020/357 sayılı Kurul kararı.
[195] Sigorta şirketinin çağrı merkezi çalışanı tarafından veri sızıntısının gerçekleştirildiği kişinin veri sorumlusunun taşeron çalışanı olduğu anlaşılmaktadır.

Kurul bu bilgiler ışığında yeterli teknik ve idari tedbirlerin alınmadığına hükmetmiş ve KVKK m. 12 hükmünün ihlal edildiğini tespit etmiştir.[196] Karar metninden veri sorumlusunun çalışanlarına veri koruma hukuku eğitimi[197] aldırmasının önemli bir kriter olduğu ancak yalnızca teknik tedbir aldırmasının tek başına yetmeyebileceği anlaşılmaktadır.

S Şans Oyunları AŞ[198] bünyesinde gerçekleşen veri sızıntısına ilişkin Kurul kararında şirketin üyelerinden birinin, veri sorumlusuna ulaşarak kullanıcılara ait telefon numarası ve şifrelerini yenileme amaçlı toplu SMS firması tarafından yollanan üye numaralarının bulunduğu bir dosyanın çevrim içi faaliyet gösteren illegal bahis sitelerinde dolaştığı bilgisi vermesiyle şirketin ihlalden haberdar olduğu ifade edilmektedir.

Ancak şirket kim tarafından ve ne zaman veri sızıntısının gerçekleştiği hususlarında bilgi sahibi olmadığını ifade etmektedir. Kurul tarafından ihlal tarihinin bilinmemesi denetim eksikliği, ilgili verilerin ne zaman çekildiğinin bilinmemesi ise teknik ve idari kusur olarak değerlendirilmiştir. Şirketin bahsi geçen listede yer alan üyelerin %90'ının sisteme hiç giriş yapmadığı yönündeki savunması ise verilerin niteliğini değiştirmeyeceği için kabul görmemiştir.

Kurul bu bilgiler ışığında yeterli teknik ve idari tedbirlerin alınmadığına ve denetim yükümlülüğünün sağlıklı biçimde yürütülmediğine hükmetmiş ve KVKK m. 12 hükmünün ihlal edilmesi sebebiyle m. 18/1-b kapsamında 90.000 TL idari para cezası uygulanması gerektiğine karar vermiştir.

Bir başka veri sızıntısına ilişkin Kurul kararı ise Clickbus Seyahat Hizmetleri AŞ bünyesinde yaşanan veri sızıntısı hakkındadır. Adli bilişim uzmanlarının raporuna göre sunucuya uzaktan erişime izin verecek biçimde kodların değişitirilerek ihlale yol açıldığı, toplamda 67.519 kişinin etkilendiği, sızıntının iki ay boyunca devam ettiği, ihlal tespitinden itibaren 4 gün daha ihlalin sürdüğü tespit edilmiştir.

---

[196] KVKK m. 12 hükmünün ihlal edilmesi sebebiyle m. 18/1-b kapsamında 90.000 TL idari para cezası uygulanması gerektiğine karar vermiştir.
[197] İçerik itibariyle sabit bir eğitim olmamakla birlikte kişisel veriyi tanımaya ve koruma yükümlülüklerinin neler olduğunu anlamaya yönelik personelin eğitilmesi olarak anlaşılmaktadır.
[198] www.tuttur.com üzerinden şans oyunları hizmeti sunmaktadır.

Kurul, kaynak kodda değişiklik yapılabilmesinin önemli bir güvenlik açığı olduğuna, 2 ay süreyle sızıntının devam etmesinin denetim yapılmadığını işaret ettiği ifade edilerek KVKK m. 12 hükmünün ihlal edildiğini tespit etmiştir.[199]

2.2.2.2. Bildirim Yükümlülüğü

2.2.2.2.1. Bildirim Yükümlülüğüne İlişkin Genel Olarak

Veri güvenliğine ilişkin ihlal gerçekleşmesinin ardından veri sorumlusu durumu mümkün olan en kısa zamanda ilgili kişiye ve Kurul'a bildirmekle yükümlüdür.[200] İlgili madde metninde bildirimin ne şekilde yapılacağı, sürenin nasıl yorumlanacağı ve bildirimde nelerin yer alması gerektiğine ilişkin somut bilgiler yer almamaktadır.[201]

Kurul veri ihlal bildirimine ilişkin detayları Kişisel Veri İhlali Bildirim Usul ve Esaslarına İlişkin kararı[202] ile somutlaştırmıştır. İlgili karardan "en kısa sürede" ifadesinden anlaşılması gereken sürenin 72 saat olduğunu, ihlalden etkilenen kişiler ulaşılabiliyorsa doğrudan iletişime geçerek bu mümkün değilse internet sitesi üzerinden duyurulması gerektiğini, Kurula bildirim yapmak için Kişisel Veri İhlal Bildirim Formu[203] doldurulmasının uygun olacağını, ihlale ilişkin tüm bilgilere 72 saatlik süre içinde erişilemiyorsa aşamalı olarak bildirim yapılabileceğini anlamaktayız.

Ayrıca veri işleyen bünyesinde ihlal gerçekleşmişse veri sorumlusuna bildirim yapılması gerektiği, yurtdışında yerleşik veri sorumlularının Türkiye'de yerleşik ilgili kişileri etkilemesi durumunda aynı esasların uygulanacağı, veri sorumlusu tarafından veri ihlali müdahale planı hazırlanması gerektiği ifade edilmiştir.[204]

Veri sorumlusunun ilgili kişiye yapması gereken veri ihlal bildiriminde; İhlalinin hangi tarihte gerçekleştiği, kategori bazında ihlale konu kişisel verilerin neler olduğu[205], ihlalden etkilenen kişisel verilerin neler olduğu ve veri ihlalinin olası sonuçları, ihlalinin olumsuz sonuçlarının azaltılması için alınan tedbirler, irtibat

---

[199] KVKK m. 12 hükmünün ihlal edilmesi sebebiyle m. 18/1-b kapsamında 450.000 TL idari para cezası uygulanması gerektiğine karar vermiştir.
[200] KVKK m. 12/5.
[201] **Dülger**, Murat Volkan: Kişisel Verileri Koruma Kurulunun "Kurula Şikâyette Bulunma Süresi" ile "Veri İhlali Bildirimi"ne İlişkin Kamuoyu Duyuruları Hakkında Değerlendirme, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3792293, s. 4, Erişim Tarihi: 11.02.2023.
[202] 24.01.2019 tarih ve 2019/10 sayılı Kurul kararı.
[203] https://ihlalbildirim.kvkk.gov.tr/ Erişim Tarihi:11.02.2023.
[204] https://www.kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirimi Erişim Tarihi: 11.02.2023.
[205] Kişisel veri/özel nitelikli kişisel veri ayrımı da dikkate alınarak yapılmalıdır.

kişilerinin isim ve iletişim bilgileri veya veri sorumlusuna ait internet sayfasının url adresi, çağrı merkezi ve buna benzeyen iletişim kanalları dahil olmak asgari gerekleri içermeli ve anlaşılır bir dille yazılmalıdır.[206]

Veri ihlal bildirimlerinde amaçlanan ilgili kişinin bir an evvel ihlalden haberdar olması ve olası doğabilecek zararların en aza indirilmesidir. Kurula yapılan veri ihlal bildirimleri Kurum'a ait internet sitesinde yayınlanmakta ve ilgili kişilerin bilgi edinmesi amaçlanmaktadır.[207]

2.2.2.2.2. Bildirim Yükümlülüğüne İlişkin Kurul Kararları

İhlal bildirimi yapılmaması nedeniyle Kurul idari para cezası uyguladığı çok sayıda karar mevcuttur. Bu kararlarda 72 saatlik süre içerisinde bildirimde bulunulmaması ve ihlale ilişkin hiç bir bildirim yapılmaması hususlarının kararların çoğunluğunu oluşturduğu görülmektedir.

İhlal bildiriminden beklenen fayda kullanıcıların bir an önce kişisel verilerinin kullanılmasını engellemek amacıyla adli ve idari mercilere başvurmak da dahil olmak üzere mağdur olmalarını engelleyebilecek tedbirleri alabilmeleri için zaman kazandırmaktır. Örneğin kredi kartı bilgileri çalınan bir ilgili kişi kredi kartıyla harcama yapılmasını engellemek maksadıyla kartını kullanıma kapatma imkanına sahip olacaktır.

Veri ihlal bildirim yükümlülüğüne aykırılık sebebiyle hükmedilen idari para cezalarından nispeten yüksek olanlar Facebook hakkında 450.000 TL[208] ve 550.000 TL[209], Marriott hakkında ise 350.000 TL[210] uygulanan kararlardır.

2.2.3. Kurul Kararının Yerine Getirilmemesi

Veri ihlalinin Kurul tarafından tespit edilmesinin ardından, tespit edilen hukuka aykırılıklar giderilmesi amacıyla veri sorumlusuna tebliğ edilir. Veri sorumlusu tebliğden itibaren otuz gün içerisinde kendisine kararı yerine getirmekle yükümlüdür.

---

[206] **Alımcı**, Ezgi: "Kişisel Verilerin Korunması Hukuku ve Bankaların Güven Kuruluşu Olarak Kabul Edilmesi Kapsamında Banka Bünyesinde Gerçekleşen Veri İhlalinin Değerlendirilmesi", Ankara Barosu Dergisi, C. 80 S.1, 2021, s. 57.
[207] https://www.kvkk.gov.tr/veri-ihlali-bildirimi/ Erişim Tarihi:11.02.2023.
[208] Kurul'un 18.09.2019 tarih ve 2019/269 sayılı kararı.
[209] Kurul'un 11.04.2019 tarih ve 2019/104 sayılı kararı.
[210] Kurul'un 16.05.2019 tarih ve 2019/143 sayılı kararı.

KVKK'nın m. 18/1-c hükmünde "*Kurul tarafından verilen kararları yerine getirmeyenler hakkında 25.000 Türk lirasından 1.000.000 Türk lirasına kadar*" idari para cezası uygulanacağı hükmü yer almaktadır. İlgili hüküm Kurul kararlarının gücünü ve etkisini artırmak için mevzuata eklenmiş bir düzenlemedir.

Kurul tarafından tebliği edilen kararlar hakkında 30 gün içerisinde işlem yapılmaması durumunda Kurul KVKK m. 18/1-ç hükmünü uygulayabilmektedir. Nitekim Kurul'un şikayet üzerine aldığı 16.10.2018 tarihli ve 2018/118 sayılı Kurul kararında bu husus görülmektedir.

Kurul 02.07.2018 tarihinde veri sorumlusuna Veri Silme Yönetmeliğinin m.11/1 hükmü kapsamında yapması gereken veri silme işlemlerinin detayları hakkında şikâyetçiye bilgi vermesi ve ilgili kişisel verilerin saklama maksadı harici işlenmemesi hususlarında veri sorumlusunun talimatlandırılmasına hükmetmiş ancak karar 30 gün içerisinde uygulanmamıştır. Kararda veri sorumlusunun 30 gün içerisinde şikâyetçiye bilgi verdiği ancak veri silme ve saklama işlemlerine değinmediği dolayısıyla Kurul kararının yerine getirilmediği ifade edilmektedir.

Veri sorumlusu bankanın Kurul kararında[211] yer alan talimatları yerine getirmemesi nedeniyle verilen kararda[212] da KVKK m. 18/1-ç hükmü uygulanmıştır. Kurul kararının yerine getirilmemesine ilişkin kararda, aydınlatma metninin Aydınlatma Tebliği'ne uygun biçimde hazırlanamadığı, aydınlatmanın kişisel veri işleme faaliyeti kapsamında her bir veri işleme kapsamında ayrı ayrı yapılması gerektiği ancak güncellenen aydınlatma metninin faaliyet bazlı olarak özgülenmediği[213] tespit edilmiştir.

Bir kargo firmasının internet sitesinin kargo takibi amacıyla oluşturulan sayfasında kargo sorgu numarasının son iki hanesi değiştirilerek başka kargoları alan ve gönderen kişilerin verilerine erişilebildiği ve gönderiyi sorgulayan kişilerin IMEI bilgilerine erişilebildiği tespit edilmiş ve bu güvenlik açığının düzeltilmesi için

[211] 06.02.2020 tarih ve 2020/98 sayılı Kurul kararı.
[212] 08.10.2020 Tarihli ve 2020/766 sayılı Kurul kararı.
[213] Konut kredisi başvurusu yapılmak istendiğinde işleme özgü aydınlatma metni ile karşılaşıldığı ancak kredi kartı başvurusu yapılmak istendiğinde genel nitelikli bir aydınlatma metnine yönlendirildiği görülmektedir.

ilgili firma talimatlandırılmıştır. Ancak 30 günlük süre içerisinde ilgili açığın giderilememesi nedeniyle KVKK m. 18/1-ç hükmü uygulanmıştır.[214]

Kurul kararları incelendiğinde KVKK m. 18/1-ç hükmünün uygulanabilmesi için iki şart arandığı anlaşılmaktadır. Öncelikle veri koruma mevzuatına aykırı bir hususun Kurul kararı ile tespit edilmesi akabinde bu kararın kendisine tebliğ edilmesi gerekmektedir.

2.2.4. VERBİS'e İlişkin Yükümlülükler

Veri Sorumluları Sicili oluşturulmasının amacı ilgili kişilerin şeffaf biçimde veri işleme amacı, kapsamı, işlenene verini içeriği, saklama süresi gibi konularda bilgi alabilmesidir. Bu kapsamda KVKK m. 16'da düzenlenen VERBİS'e kayıt yükümlülüğünün yerine getirilmemesi m. 18/1-ç'de kabahat olarak düzenlenmiştir.[215]

Kurul VERBİS kaydı için belirlediği son tarihi veri sorumlularının hazır olmaması nedeniyle defaten ertelemiş ve aldığı güncel kararla[216]bir kere daha ertelemiştir. VERBİS kayıt yükümlülüğünü yerine getirmeyen teşebbüslere idari para cezası uygulanacağı ve her bir veri işleme faaliyeti için bu idari para cezasının ayrı ayrı tespit edileceği hususları net olmakla birlikte Kurul son kayıt tarihini çeşitli sebeplerle erteleyerek[217] ve bu hususta esneklik tanımıştır. Ayrıca ciro ve çalışan sayısı gibi eşikler belirleyerek her veri sorumlusunu bu kayıt külfeti altına sokmamıştır.[218]

2.2.5. Kişisel Verilerin İhlaline İlişkin Suçlar

Konusu suç oluşturan ve ceza uygulanmasını gerektiren eylemler aynı zamanda haksız fiil niteliği taşımaktadır. Haksız fiiller sebebiyle tazminat sorumluluğu TBK m. 41 ve devamı hükümlerinde düzenlenmiştir. Bu nedenle suç olarak düzenlenen eylemler ceza yargılaması haricinde özel hukuk sorumluluğuna da

---

[214] **Kaya**, Mehmet Bedii/**Taştan**, Furkan Güven: Kişisel Veri Koruma Hukuku – Mevzuat & İçtihat, XII Levha Yayınları, İstanbul, 2019.
[215] KVKK m. 18/1-ç hükmü "*16 ncı maddesinde öngörülen Veri Sorumluları Siciline kayıt ve bildirim yükümlülüğüne aykırı hareket edenler hakkında 20.000 Türk lirasından 1.000.000 Türk lirasına kadar...*" şeklinde düzenlenmiştir.
[216] 23/06/2020 Tarihli ve 2020/482 sayılı karar.
[217] 17/12/2019 Tarihli ve 2019/387 Sayılı kararı
[218] **Kaya/Taştan**, s. 1257.

konu olacak ve suç oluşturan eylemler haksız fiil sorumluluğu kapsamında da değerlendirilmektedir.

Bu kapsamda öncelikle kişisel verileri korumayı amaçlayan TCK hükümleri incelenecek üçüncü bölümde ise bu suçlardan doğan tazminat sorumluluğuna yer verilecektir.

KVKK'nın suçlar başlıklı m. 17 hükmünde TCK'nın 135-140. maddelerine açıkça atıf yapılmaktadır. TCK'nın ilgili hükümleri incelendiğinde Kişisel Verilerin Kaydedilmesi Suçu, Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme Suçu, Verileri Yok Etmeme olmak üzere üç farklı suç tanımlandığı görülmektedir. Kişisel verilerin ihlaline ilişkin olarak hangi eylemlerin suç olarak düzenlendiğini bu başlıkta altında değerlendireceğiz.

2.2.5.1. Kişisel Verilerin Kaydedilmesi

Kişisel verilerin korunmasını talep edebilmek 2010 yılında açık biçimde anayasal hak olarak kabul edilmiştir. Anayasal bir hakkı ihlal etmenin caydırıcı bir yaptırımı olmalıdır. Bu nedenle kişisel verilerin kaydedilmesi suç olarak tanımlanmıştır.

İlgili kanun hükmü ile korunması amaçlanan değer özel hayatın gizliliği değil kişisel verilerin korunması hakkıdır.[219] Kişisel verilerin korunmasını hedefleyen suçların bu doğrultuda yorumlanması gerekmektedir.

Kişisel verilerin kaydedilmesi suçunu düzenleyen TCK m. 135 hükmü aşağıda yer verildiği gibidir:

" *(1) Hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir.*

(2) Kişisel verinin, kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması durumunda birinci fıkra uyarınca verilecek ceza yarı oranında artırılır."

Bir suçu değerlendirirken fail, mağdur, suçun konusu, eylem, sonuç açısından bakmak suçun analizin kolaylaştırmaktadır. Fail açısından herhangi bir özel

[219] **Dülger**, Veri Koruma Hukuku, s. 538. Daha evvel Anayasada düzenlemenin yer aldığı başlık nedeniyle farklı bir yorumun da yapıldığını ancak aslında özel hayatın gizliliğinden bağımsız bir hak olduğunu belirtmiştik.

nitelik aranmadığından her gerçek kişinin[220] bu suçun faili olabileceği anlaşılmaktadır.[221]Dolayısıyla VERBİS kaydı olmayan veya veri işlediğini açıkça duyurup herhangi bir resmi sıfat taşımayan biri de suçun faili olabilecektir.

Mağdur açısından değerlendirildiğinde ise kişisel veri sahipleri yalnızca gerçek kişilerdir ve kişisel verileri korumayı amaçlayan suçun mağduru da yalnızca gerçek kişiler olabilir.[222] Mağdur veri sahibi ilgili kişidir ve mağdur olmak için aranan şartlar kişisel verinin kaydedildiği alanın[223] ilgili kişiye ait olmaması ve ilgili kişinin rızasının bulunmamasıdır.

Suçun konusu hukuka aykırı biçimde kaydedilen kişisel veridir. Suçun konusunu özel nitelikli kişisel verilerin oluşturması ise kanun koyucu tarafından nitelikli hal olarak kabul edilmiştir. Ayrıca suçun konusunu oluşturan verinin gizli olması veya herkesçe erişebilir olmaması gibi bir kural mevcut değildir. Ancak herkesçe bilinen kişisel verilerin bu suçun konusunu oluşturamayacağı, suçun kapsamını bu denli genişletmemek gerektiği yönünde görüş de mevcuttur.

Yargıtay içtihadına bakıldığında[224] "...*yetkisiz üçüncü kişilerin bilgisine sunmadığı, istediğinde başka kişilere açıklayarak ancak sınırlı bir çevre ile paylaştığı, herkes tarafından bilinmeyen ve/veya kolaylıkla ulaşılması ve bilinmesi mümkün olmayan*...." kriterinin kullanıldığı anlaşılmaktadır. Yargıtay kararlarından[225] hareketle Yargıtay'ın kişisel veriyi belirlerken gizli tutmak gibi bir şart aramadığı ancak herkesin bildiği veya bilebileceği bir veriyi de kişisel veri olarak korumadığı anlaşılmaktadır. Ancak Yargıtay'ın diğer kararlarının aksine Yargıtay Ceza Genel Kurulu'nun (CGK) bu konudaki kararı[226] TCK m. 135 ve 136 hükümlerinin sadece gizlilik arz eden yani sır niteliğindeki verilerin korunacağına ilişkin bir şartı içermediği, aksine TCK m. 135. hükmünün gerekçesinde gerçek

---

[220] **Koca**, Mahmut/**Üzülmez**, İlhan: "Kişisel Verilerin Kaydedilmesi Suçu (TCK m. 135)", Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, Prof. Dr. Durmuş TEZCAN'a Armağan, C.21, 2019, s. 75.

[221] TCK m. 137/1 "*Kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle*" gerçekleşmesi ağırlaştırıcı neden olarak düzenlenmiştir.

[222] **Sınar**, Hasan: "Kişisel Verileri Hukuka Aykırı Olarak Verme, Yayma Veya Ele Geçirme Suçu (TCK m. 136)", Kişisel Verileri Koruma Dergisi, C.2, S.1, 2020, 33-62, s. 40.

[223] Fiziki veya dijital alan olması arasında bir fark bulunmamaktadır.

[224] Yargıtay 12. CD, 2.10.2012, 2012/20543, 2012/20422.

[225] Yargıtay 12. CD, 10.6.2013, 2013/9656, 2013/15773 ve 2014/3760 sayılı kararlar.

[226] Yargıtay CGK'nın 17.6.2014 tarihli ve 12-1510/331 sayılı kararı.

kişiyle ilgili tüm bilgilerin kişisel veri olarak kabul edilmesi gerektiği tespiti yer almaktadır.[227]

Ancak Yargıtay'ın sonraki tarihli kararlarında "*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*" gerektiği ifade edilerek her kişisel verinin işlenmesinin ilgili suçun oluşturmayacağı ifade edilmiştir. Literatürde bu görüşten ayrılan ve herhangi bir kişisel verinin kaydedilmesinin bu suçu oluşturacağını, verileri sınırlamanın suçta ve cezada kanunilik ilkesi olarak değerlendirilen alt ilkesi olan belirlilik ilkesine aykırı olduğunu düşünen yazarlar mevcuttur.[228] Yargıtay kararlarını ve literatürdeki görüşleri birlikte incelediğimizde somut olayın incelenmesi ve o olaya özgü özellikler dikkate alınarak değerlendirme yapılması gerektiği anlaşılmaktadır.

Suçu meydana getiren fiil kişisel verilerin hukuka aykırı biçimde bilişim sistemine veya fiziki olarak yazılı kayıtlara geçirilmesidir.[229] Madde gerekçesinde açıkça belirtildiği üzere bilgisayardaki bir dosyaya kaydedilmesi, taşınabilir bir belleğe kopyalanma veya kalem, daktilo gibi araçlarla kağıda yazılması arasında bir fark mevcut değildir. Ancak kişisel veriyi ezberlemek kaydetme eylemi oluşturmayacağı için ilgili suç kapsamında değerlendirilmeyecektir.[230]

Kişisel verilerin kaydedilmesi suçu neticeli bir suçtur.[231] Kaydedilme eylemi gerçekleştiği anda suç tamamlanmaktadır. Bilişim sistemleri için bir yazı dosyasına kaydetme anında, taşınabilir bellekte kopyalama anında fiziki dosyalarda ise kalemle veya daktilo ile yazma işleminin tamamlandığı anda netice gerçekleşmektedir.

---

[227] **Koca/Üzülmez**, s. 23.
[228] **Dülger**, s. 544.
[229] **Karagülmez**, Ali: Bilişim suçları, Seçkin Yayınları, Ankara, 2014, s. 448, **Koca/Üzülmez**, s. 79.
[230] **Aydın**, Kişisel Verilerin Kaydedilmesi Suçu, s. 131.
[231] **Yaşar**, Osman/ **Gökcan**, Hasan Tahsin/ **Artuç**, Mustafa: Türk Ceza Kanunu, Adalet Yayınevi, C. 3, S. 2, s. 438.

2.2.5.2. Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme

TCK m. 136 kapsamında kişisel verilerin yetkisiz kişilerce ele geçirilmesi veya ilgili kişinin rızasıyla verdiği bir bilginin izin alınmadan üçüncü kişilerle paylaşılması suç olarak düzenlenmiştir.

" *(1) Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır…*"

Kısaca verileri verme veya ele geçirme suçu olarak da ifade edebileceğimiz ilgili suçun kanuni tanımından da anlaşıldığı üzere herhangi biri tarafından işlenebilen suçlar yani genel suçlar arasındadır.

Mağdur açısından bakıldığında ise suç ile zarar verilen varlık yahut değerin sahibi, somut olayda ilgili kişi suçun mağduru konumundadır. Tüzel kişiler, kişisel veri sahibi olamayacağı için suçun mağduru yalnızca gerçek kişilerdir. Nitekim bu husus Yargıtay kararlarında[232] da "*Verileri hukuka aykırı olarak verme veya ele geçirme suçunun maddi konusunu oluşturan "kişisel veri" kavramından gerçek kişiye ait her türlü bilginin anlaşılması gerektiği nazara alındığında … şikayetçi… A.Ş.nin, sanığa yüklenen verileri hukuka aykırı olarak verme veya ele geçirme suçunun mağduru olmadığı…*" şeklinde yer bulmuştur.

Hareket unsuru açısından ele alındığında ise suçun oluşması açısından herhangi bir sonuç oluşması beklenmediğinden verileri hukuka aykırı olarak verme veya ele geçirme bir salt hareket suçudur. İlgili suçun kanuni tanımından hareketle "bir başkasına vermek", "yaymak" ve "ele geçirmek" şeklinde eylemlerin birinin gerçekleşmesiyle suçun oluşabilmektedir. Dolayısıyla seçimlik hareketli bir suç olduğu anlaşılmaktadır.

Yargı kararları ışığında ilgili suçun bu hareketlerle nasıl ortaya çıkabileceğini incelemek kişisel veri ihlalinin nasıl gerçekleşeceğini anlamak açısından uygun olacaktır.

Uygulamada oldukça sık karşılaşılan bir kişisel veri ihlali bir kişiye ait kişisel verinin üçüncü bir kişiye verilmesidir. Böylelikle kişisel verilerin başkasına verilmesi yoluyla TCK 136 m. hükmü ihlal edilmiş olacaktır. Nitekim ilgili Yargıtay

[232] Yargıtay 12. CD, E. 2017/1636, K. 2018/3978.

kararında[233] bu husus şu şekilde ifade edilmiştir: "*Sanık ...'in, kişisel veri niteliğindeki katılana ait cep telefonu numarasını kaydedilmiş haliyle ve hukuka uygunluk nedenlerinin bulunmaması nedeniyle hukuka aykırı olduğunda tereddüt bulunmayan bir yöntemle arkadaşına vermesi şeklinde sübut bulan eyleminden dolayı TCK'nın 136/1. madde ve fıkrasında tanımlanan verileri hukuka aykırı olarak verme veya ele geçirme suçundan mahkumiyetine...*".

Kişisel verinin üçüncü bir kişi tarafından öğrenilebilir konuma gelmesiyle suç tamamlanmakta ve bu eylemin sonucunda bir neticenin gerçekleşmesi beklenmemektedir. Bir diğer Yargıtay kararında[234] ise "...*eski eşi Ş. arasında gerçekleşen arama kaydı dökümlerini katılanın akrabalarına göndermesi eyleminde, arama kaydı dökümlerini, katılanın ve dava dışı Ş.'nin yaptıkları aramalarla kendilerini arayan numaralara dair tarih, saat ve süre bilgilerini içermesi ve bu iki kişi arasında gerçekleşen konuşma veya mesajlaşma içeriklerine dair bilgi bulunmaması karşısında, sanığın eyleminin haberleşmenin gizliliğini ihlal suçunu değil, T.C.K.nın 136/1. maddesinde düzenlenen, verileri hukuka aykırı olarak verme veya ele geçirme suçunu oluşturduğu...*"

Kişisel verilerin üçüncü kişilere verilmesi ve kişisel verilerin yayılması arasındaki sınırı somut olayda tespit etmek zor değildir. Aynı kişisel verinin yalnızca bir başka kişiye erişmesi amacıyla çevrim içi mesajlaşma uygulaması aracılığıyla gönderilmesi ile herkesin erişebileceği bir sosyal medya hesabında paylaşmak sırasıyla kişisel verilerin üçüncü kişilere verilmesi ve kişisel verilerin yayılması fiillerini oluşturmaktadır.[235] Neticeli bir suç olmadığı için her ikisinde de aynı sonuç ortaya çıkacaktır.

Yargıtay'ın kişisel verileri yayılması yoluyla TCK m. 136'da düzenlenen suçun işlendiğine hükmettiği kararları mevcuttur. İlgili kararda[236] "*Sanıkların sahibi olduğu özel hastanede hastane müdürü ve başhekim olarak görev yapan, hastanenin aynı zamanda ortağı olan ortopedi doktoru katılan ...'in, anılan hastaneden ve ortaklıktan ayrılmasına rağmen hastaneye ait internet sitesinde yer alan reklam filmlerinde, hastanenin başhekimi ve ortopedi uzmanı olduğuna*

[233] Yargıtay 12. CD., E. 2018/8466, K. 2019/9054, T. 18.09.2019.
[234] Yargıtay 12. CD, E. 2014/22994, K. 2015/2630, T. 16.02.2015.
[235] **İtişgen**, Rezzan: "Türk Ceza Hukukunda Kişisel Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme Suçu", Türkiye Adalet Akademisi Dergisi, S. 23, 2015, 179-202.
[236] Yargıtay 12. CD, E. 2018/8144, K. 2019/8317, T. 10.07.2019.

dair açıklamalarla beraber rızası olmaksızın görüntülerinin yayımlanmaya devam ettiği iddia ve kabulüne konu olayda; Katılan tarafından kaldırılması istenilmesine ve bu konuda daha önce şikayette bulunulmasına rağmen reklam filmlerini aynı şekilde yayımlamaya devam ederek, katılanın kişisel veri niteliğindeki görüntüsünü hukuka uygunluk nedenlerinin bulunmaması nedeniyle hukuka aykırı olduğunda tereddüt bulunmayan bir yöntemle başkalarının görgüsüne sunmaya devam eden sanıkların sübut bulan eylemlerinden dolayı TCK'nın 136/1. madde ve fıkrasındaki verileri hukuka aykırı olarak verme veya ele geçirme suçundan mahkumiyet kararı verilmesi gerektiği" ifade edilmektedir. İlgili karardan anlaşılacağı üzere rızaya veya geçerli bir hukuki sebebe dayanmaksızın bir kişinin kişisel verilerini ticari amaçlarla herkesin görebildiği mecralarda kullanmak TCK 136/1 kapsamında suç teşkil etmektedir.

Yargıtay'ın bir diğer kararında ise sanığın, mağdurun sıradan günlük kıyafetleriyle poz verdiği resimlerini, mağdur adına açtığı sahte bir Facebook hesabında yayımladığı olayda; mağdura ait resimlerin kişisel veri niteliğinde olduğuna, hukuka uygunluk nedenlerinin bulunmaması sebebiyle hukuka aykırı bir yolla Facebook üzerinden yayımladığına ve ilgili eyleminin TCK'nın m. 136/1'de tanımlanan verileri hukuka aykırı olarak verme veya ele geçirme suçunu oluşturduğuna karar verilmiştir. İlgili karardan günlük kıyafetlerle alelade biçimde çekilen fotoğrafın kişisel veri olarak niteleneceği ve herkese açık bir sosyal paylaşım sitesinde herkesin görebileceği ayarlarla sunulması nedeniyle yayma eylemi teşkil edeceği açık biçimde anlaşılmaktadır.

Kişisel verilerin ele geçirilmesi TCK m. 136 hükmünün uygulanması için bir diğer seçimlik harekettir. Uygulamada sıklıkla karşılaşılan görünümlerinden biri ise kişinin hesap şifrelerinin ele geçirilmesi ve üçüncü kişilerle paylaşılmasıdır. Konuya ilişkin Yargıtay kararında[237] "*Sanığın, katılana ait Facebook hesabının şifresini, onun bilgisi ve rızası dışında ele geçirip, hesabın ismi ile birlikte değiştirerek, katılanın bilişim sistemindeki hesabına erişimini engellemesi biçiminde sübutu kabul edilen eylemlerinin, TCK'nın 136/1. madde ve fıkrasındaki verileri hukuka aykırı olarak verme veya ele geçirme ve aynı Kanunun 244/2. madde ve fıkrasındaki sistemi engelleme, bozma, verileri yok etme veya*

[237] Yargıtay 12. CD, E. 2022/5072 , K. 2022/6245, T. 15.06.2022

değiştirme suçlarını oluşturduğu gözetilmeksizin, yalnızca verileri hukuka aykırı olarak verme veya ele geçirme suçundan mahkumiyet hükmü kurulması, bozma nedenidir." tespiti yer almaktadır.

Aynı olayda birden fazla seçimlik hareket bir arada gerçekleşerek tek veri ihlali oluşturan fiilin birden fazla faili de olabilir. Nitekim Yargıtay'ın bir diğer kararında[238] trafikte tartışma yaşadığı kişinin araç plaka bilgilerini trafik şube müdürlüğünde çalışan polis memuru tanıdığı vasıtasıyla trafik sisteminden sorgulatarak araç sahibinin kimlik bilgilerini öğrenen failin bu davranışın, kişisel verilerin hukuka aykırı olarak ele geçirilmesi teşkil ederken, polis memurunun fiili ise kişisel verilerin hukuka aykırı olarak verilmesidir.[239]

Yargıtay CGK'nın konuyla ilgili kararında[240] ele geçirme fiili ilgili "*Kişisel verilerin ele geçirilmesi" seçimlik hareketi ise; kişisel verilerin kayıtlı olduğu belgelerin alınması ya da kayıtlı olduğu bilişim sisteminden ele geçirilmesi vb... şekillerde gerçekleştirilebilecektir. Ele geçirme fiili, başkasının hakimiyeti altında bulunan bir kişisel verinin, failin hakimiyeti altına girmesi ile gerçekleşmiş olacaktır…*" ifadeleri yer almaktadır. İlgili karardan da anlaşılacağı üzere ele geçirme suçunun konusunu oluşturan kişisel verinin fiziki veya dijital bir ortamda kaydedilmiş olması açısından bir fark mevcut değildir.

Veri sorumlularının kişisel verilere hukuka aykırı biçimde erişimi önlemek ve kişisel verileri korumak amacıyla gerekli güvenlik düzeyini sağlamaya yönelik gerekli her türlü teknik ve idari tedbirleri alma yükümlüğü ve TCK m. 136'nın uygulama alanı arasında örtüşme mevcuttur. KVKK m. 12 hükmü kapsamında veri güvenliği ile ilgili teknik ve idari tedbirleri almakla yükümlendirilirken TCK m. 136 kapsamında ilgili kişisel veriye erişim yetkisi olmayan kişilere ise ele geçirmeme yükümlülüğü yüklenmiştir.

Kurul'un veri sorumluları ve veri işleyenlerin, veri toplama amacına aykırı biçimde ilgili kişilerin e-posta adreslerine veya cep telefonlarına reklam yönlendirilmesinin önüne geçilmesini amaçlayan ilke kararında[241] da bu hususa değinilmiş veri

---

[238] Yargıtay 12. CD, E. 2018/636, K. 2018/6140, T. 30.5.2018.
[239] **Yaşar**, Osman/**Gökcan**, Hasan Tahsin/**Artuç**, Mustafa: Yorumlu-Uygulamalı Türk Ceza Kanunu (III), Yetkin Yayıncılık, Ankara, 2014.
[240] Yargıtay CGK, E. 2012/12-1514, K. 2014/312, T. 10.6.2014.
[241] Kurulun 21/12/2017 Tarihli ve 2017/61 Sayılı İlke Kararı.

sorumlusunun KVKK m. 12'ye aykırı davranması durumunda Kurul'un m. 18/1-b hükmüne göre idari para cezası uygulayacağı, TCK m. 136 kapsamında üçüncü kişilerin veriye erişmesi kapsamında ise Cumhuriyet Başsavcılığı'na durumun bildirileceği ifade edilmiştir. İlgili iki hüküm birlikte değerlendirildiğinde kişisel veri güvenliğini sağlamak amacıyla birbirini tamamlayan TCK'da bir suç ve KVKK'da bir kabahat hükmü konulduğu anlaşılmaktadır.

2.2.5.3. Verileri Yok Etmeme Suçu

KVKK'ya göre işlenmiş kişisel verilerin bir süre sonra silinmesi, yok edilmesi veya anonim hale getirilmesi gerekmektedir. Bu husus m. 7'de düzenlenmiş olup ilgili madde hükmü aşağıdaki gibidir.

" *(1) Bu Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir.*

(2) Kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesine ilişkin diğer kanunlarda yer alan hükümler saklıdır."

KVKK m. 7 hükmünün uygulanmaması durumunda uygulanacak yaptırım ise m. 17'de düzenlenmiştir. İlgili hükme göre "... *(2) Bu Kanunun 7 nci maddesi hükmüne aykırı olarak; kişisel verileri silmeyen veya anonim hâle getirmeyenler 5237 sayılı Kanunun 138 inci maddesine göre cezalandırılır*.". İşlenmiş kişisel verileri silmemek veya anonim hâle getirmemek TCK 138 kapsamında suç olarak düzenlenmiş olup ilgili hükme KVKK'da da atıf yapılmıştır.

TCK m. 138 hükmü "*(1) Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde altı aydan bir yıla kadar hapis cezası verilir. (2) Suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması hâlinde verilecek ceza bir kat artırılır.*" şeklindedir.

TCK 138. madde hükmün yerine getirilmesi esnasında uyulacak usule ilişkin kurallar ise Veri Silme Yönetmeliğinin kapsamında düzenlenmiştir. Ancak TCK yalnızca kişisel verilerin yok edilmesi olarak düzenlerken Veri Silme

Yönetmeliğine göre yok etme işlemi birden fazla yöntemle yapılabilmektedir. İlgili yönetmeliği m. 8 hükmünde kişisel verilerin yok edilmesi, m. 9 hükmünde kişisel verilerin anonim hale getirilmesi ve m. 10 hükmünde ise kişisel verilerin anonim hale getirilmesi yöntemleri düzenlenmiştir.

Bu yöntemlere göre yok etme işleminin: *"Kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi suretiyle silinerek"* m. 9 kapsamında " *kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi suretiyle yok edilerek* " veya m. 10 kapsamında "*kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi suretiyle anonim hale getirilerek* " yapılacağı anlaşılmaktadır. TCK m. 138 ve KVKK m. 7 ve 17 hükümleri birlikte yorumlandığında her ne kadar TCK m. 138'de yalnızca yok etme kavramı kullanılsa da madde lafızlarından Veri Silme Yönetmeliğinde sunulan üç yöntemden elverişli olanın kullanılması gerektiği anlaşılmaktadır.[242]

Verileri yok etmeme suçu diğer iki suçtan farklı olarak ihmali olarak da işlenebilen bir suçtur.[243] Diğer bir deyişle KVKK kapsamında bir yükümlülük getirilmiş ve yükümlülüğün yerine getirilmemesi TCK kapsamında suç olarak düzenlenmiştir. Kişisel verilerin işlenmesi belirli şartlar altında izin verilen istisnai bir durum olup ilgili şartlar ortadan kalktığında verinin yok edilmesini veya ilgili kişiyle olan tüm bağlantılarının ortadan kaldırılmasını gerektirmektedir. Bu gerekliliğin yerine getirilmemesi verileri yok etmeme suçunun tamamlanması için yeterlidir.

Verileri yok etmeme suçunun faili her bir veri işleme faaliyeti kapsamında verileri yok etmekle görevlendirilen kişidir. Örnek olarak şüpheli hakkında kovuşturma yapılmasına yer olmadığı kararı verilmişse yahut iletişimin tespiti, dinlenmesi ve kayda alınması konusunda hâkim onayının alınamaması halinde, tüm kayıtlarının en geç on gün içerisinde yok edilmesi gerektiği Ceza Muhakemesi Kanunu'nun[244] (CMK) 137/ 3. maddesi kapsamında düzenlenmiştir. CMK'da düzenlenen olan bu on günlük süre bitmeden iletişimin tespitine ilişkin verilerin yok edilmemesi

[242] Bu noktada belirli bir mevzuat kapsamında veri işleme yapılıyor ve bu kanunda özellikle bu veri imha yollarından birine işaret edilmişse bu durumda üç yöntemden diğer ikisinin uygulanması mümkün olmayacaktır.
[243] **Kart/Ketizmen**, s. 24.
[244] 5271 sayılı ve 17.12.2004 tarihli Ceza Muhakemesi Kanunu.

halinde TCK'nin 138. maddesinde düzenlenen verileri yok etmeme suçu gerçekleşecektir. Bu olayda suçun faili verilerin yok edilmesiyle görevlendirilen kamu görevlisidir.

Mağdur açısından bakıldığında ise suçun mağduru kişisel verinin sahibi yani ilgili kişidir. Bu noktada diğer kişisel verilere ilişkin suçlarda olduğu gibi verilerin yok edilmemesi suçunun mağduru yine yalnızca gerçek kişi olabilecektir. Suçun konusu veri işleme faaliyeti kapsamında işlenen ve yok edilmesi gereken kişisel veridir.[245] Verileri yok etmeme neticeli bir suç değildir ve soyut bir tehlike suçudur. Dolayısıyla ilgili başlık altında değinileceği üzere bu suç dolayısıyla bir tazminat sorumluluğuna gidilmesi için herhangi bir zararın ortaya konulması arayışına da girilmeyecektir.

[245] **Dülger**, Kişisel Verilerin Korunması, s. 125.

3. BÖLÜM: KİŞİSEL VERİLERİN KORUNMASI YÜKÜMLÜLÜĞÜNÜN İHLALİNDEN DOĞAN HUKUKİ SORUMLULUK

Hukuka aykırı veri işleyen kişi hakkında idari sürece başvurulması ve idari para cezası veya hapis cezası gibi yaptırımlar uygulanması elbette mümkündür. Ancak üçüncü bölümün konusu olan hukuki sorumluluk noktasında Kurul'un veya ceza yargılamasının herhangi bir rolü bulunmamaktadır.

Bu bölümde genel hükümler ve KVKK'da yer alan hükümler çerçevesinde hukuki sorumluluk incelenecektir. Sorumluluğun şartları ve niteliği, başvurulabilecek diğer hukuki yollar değerlendirilecektir. Bu bölümde tespit edilen eksiklikler ve öneriler sonuç başlığı altında ifade edilecektir.

3.1. KİŞİSEL VERİLERİN KORUNMASI YÜKÜMLÜLÜĞÜNÜN İHLALİNDEN GENEL HÜKÜMLER KAPSAMINDA SORUMLULUK

3.1.1. Kişisel Verilerin Korunması Yükümlülüğünün İhlalinde Haksız Fiil Sorumluluğu

3.1.1.1. Haksız Fiil Sorumluluğuna İlişkin Genel Olarak

TBK m. 49-64 hükümleri haksız fiilden doğan kusura dayalı sorumluluğu, m. 65-71 hükümleri ise kusursuz sorumluluk hallerini düzenlemektedir. Haksız fiile ilişkin sorumluluğu düzenleyen genel hüküm şu şekildedir:

"*Madde 49 - Kusurlu ve hukuka aykırı bir fiile başkasına zarar veren, bu zararı gidermekle yükümlüdür*."

Kusura dayanan sorumluluğun ilgili madde lafzından da anlaşıldığı üzere fiil, kusur, hukuka aykırılık, zarar, nedensellik bağı olmak üzere 5 unsuru olduğu anlaşılmaktadır.[246] Bu beş unsuru temel biçimde açıklamak kişisel verilerin haksız fiil olarak değerlendirilip değerlendirilmeyeceği hususunu anlamak açısından uygun olacaktır.

TBK'da borç kaynaklarından biri olarak düzenlenen haksız fiil sorumluluğunun doğması için öncelikle bir fiilin işlenmesi gerekmektedir. Bir davranışın iradi olarak isteyerek yapılması fiil olarak değerlendirilecektir. Haksız fiil oluşturan eylem somut olayda yapma ya da yapmama şeklinde ortaya çıkabilir[247] ancak yapmama eyleminin haksız fiil kapsamında değerlendirilebilmesi için açıkça düzenlenmiş bir yapma yükümlülüğü bulunmalıdır.[248]

Haksız fiil sorumluluğu için gerekli bir diğer unsur ise hukuka aykırılıktır. TBK'da açık biçimde tanımlanmamakla birlikte hukuk kurallarının yasakladığı bir davranışta bulunmak olarak yorumlanmaktadır. Hukuk kuralları arasında herhangi bir ayrım yapılmamış olup hukuk kuralları ile korunan bir mutlak hak

---

[246] **Nomer**, Haluk Nami: Borçlar Hukuku Genel Hükümler, Beta Yayınevi, İstanbul, 2015, s. 114, Eren Fikret, Borçlar Hukuku Genel Hükümler, Ankara, 2021, s. 516. Ancak doktrinde haksız fiilin hukuka aykırılık ve fiil unsurlarını ayrıca vurgulamayan ve toplamda üç unsuru olduğunu ifade eden görüşler de mevcuttur. **Oğuzman**, Kemal/ **Öz**, Turgut: Borçlar Hukuku Genel Hükümler, Vedat Kitapçılık, İstanbul, 2016, s. 12.

[247] **Oğuzman**/**Turgut**, s. 13; **Ayan**, Mehmet: Borçlar Hukuku Genel Hükümler, Adalet Yayınevi, Ankara 2020, s. 288;

[248] **Tekinay**/**Akman**/**Burcuoğlu**/**Altop**: Borçlar Hukuku Genel Hükümler, Filiz Kitabevi, İstanbul, 1993, s. 484; **Ayan**, s. 288; **Hatemi**/**Gökyayla**, s. 117. KVKK'da düzenlenen veri sorumlusu yükümlülüklerine ilişkin sorumluluğun haksız fiil sorumluluğu kapsamında değerlendirilmesi bu bölüm içerisinde ilerleyen sayfalarda yapılacaktır.

ihlali veya diğer bir menfaatin veya özel bir alanı korumayı amaçlayan hukuk kurallarının ihlali de olabilir.[249]

TBK m. 49/2'de "*Zarar verici fiili yasaklayan bir hukuk kuralı bulunmasa bile, ahlaka aykırı bir fiille başkasına kasten zarar veren de, bu zararı gidermekle yükümlüdür.*" hükmü mevcuttur. Dolayısıyla kasıtlı biçimde işlendiği durumda bir hukuk kuralını ihlal etmeden dahi hukuka aykırılık şartı gerçekleşmektedir. Daha açık bir ifadeyle kasıtlı ve ahlaka aykırı davranış hukuka aykırılığı oluşturacaktır. Ancak ihmali bir davranışla hukuka aykırılık oluşması için mutlaka açık bir yükümlülük gerekmektedir.[250]

Tazminat borcunun doğması için gerekli şartlardan bir diğeri de zarar unsurudur. Zarar kendi içinde maddi ve manevi zarar olmak üzere ikili bir ayrıma tabidir. Maddi zarar haksız fiil mağdurunun malvarlığında rıza dışı oluşan zarar olarak tanımlanmaktadır. Manevi zarar ise eylemden mağdur olanın kişilik hakkına yönelen saldırıdan duyulan elem ve üzüntü olarak tanımlanmaktadır.[251]

Manevi zarara ilişkin üç farklı teori mevcuttur.[252] Bunlardan ilki sübjektif görüştür. Bu görüşe göre fizik bir acı, ruhsal çöküntü, yaşama arzusunun yitirilmesi manevi zararın varlığına işaret eder. Sübjektif görüş zararın kesin tespitini zorlaştıran bir görüş olması gerekçesiyle eleştiriye maruz kalmıştır. İkinci görüş objektif görüştür. Objektif görüş zararın giderimini hedeflemekle birlikte herhangi bir sonuç doğması şartını aramamıştır. Kişinin manevi olarak üzülmesi sonucunda psikolojik olarak hastalık oluşması veya zararın tam ispatı gibi hususların aranmaması gerektiği ifade edilmiştir.

Üçüncü görüş ise karma görüş olarak ifade edilmektedir. Buna göre kişiliğe yönelik nitelikli bir saldırı durumu söz konusu olmalıdır. Bu saldırı sübjektif unsur

---

[249] Hukuka aykırılık açıkça tanımlanmamış olup bu konuyu açıklayan iki teoriyi açıklamak gerekmektedir. Bunlar objektif hukuka aykırılık ve sübjektif hukuk aykırılık teorileridir. Objektif teoriye göre, başka kişilere zarar vermeyi yasaklayan genel davranış kuralının ihlali şeklinde açıklamaktadır. **Abik**, Yıldız: "Normun Koruma Amacı Teorisi", AUHFD, C. 59, S. 3, 2010, s. 371.

[250] TBK m. 63/2'de sayılan hukuka uygunluk hallerinden biri mevcutsa hukuka aykırılık ortadan kalkacaktır. Bu haller: "*Zarar görenin rızası, daha üstün nitelikte özel veya kamusal yarar, zarar verenin davranışının haklı savunma niteliği taşıması, yetkili kamu makamlarının müdahalesinin zamanında sağlanamayacak olması durumunda kişinin hakkını kendi gücüyle koruması veya zorunluluk hâllerinde de fiil, hukuka aykırı sayılmaz.*"

[251] **Oral**, Tuğçe: Tüzel Kişilerin Manevi Zararı, XII Levha Yayınları, Ankara 2018, s. 42; **Eren**, s. 802; **Tandoğan**, Mes'uliyet, s. 330; **Tekinay**/**Akman**/**Burcuoğlu**/**Altop**, s.655.

[252] **Antalya, Gökhan**: Manevi Zarar, Cevdet Yavuz'a Armağan, C.1, 2016, s. 226.

olarak, kişinin içsel yönünde etki doğurmalı daha açık bir ifadeyle kişinin psikolojik üzerinde etkili olmalıdır. Ayrıca dışsal yönüyle de kişinin ekonomik ve sosyal hayatında olumsuz sonuçlar doğurmalıdır.

Manevi zarar tanımında olduğu gibi zarar kavramına ilişkin olarak da birden fazla görüş olmakla birlikte daha fazla kabul gördüğü için geniş anlamda zarar kavramını kabul edeceğiz. Buna göre malvarlığı veya şahıs varlığındaki eksilme zarar için yeterlidir. [253]

Haksız fiil sorumluluğunu açıklayabilmek için zarar hususunu da açıklamak gerekmektedir. Zarara sebep olan eylem ve ortaya çıkan zarar arasındaki neden sonuç ilişkisi bulunması nedensellik bağı olarak ifade edilir.[254] Nedensellik bağına ilişkin objektif ve somut her bir olayda uygulanabilir kriterler koymak oldukça zordur.[255] Ayrıca yasalarda nedensellik bağına ilişkin açık bir tanımlama yapılmamış[256] ancak uygulamada yargı kararlarıyla bazı kıstaslar konulduğu anlaşılmaktadır. Hayat tecrübeleri olayların normal akışı dikkate alındığında ortaya çıkan zararı meydana getirmeye elverişli bir sebebin olup olmadığı dikkate alınmaktadır.[257]

İlliyet bağı hususunda birden fazla teori mevcut olmakla birlikte hukukumuzda uygun illiyet bağı teorisi kabul edilmektedir.

---

[253] Zarar ifadesi ile geniş anlamda zarar kavramı kast edilmekte olup detaylar için bkz. **Ayan**, s. 320, **Eren**, s. 599, **Tandoğan**, Mesuliyet, s. 63; **Antalya**, Borçlar Hukuku Genel Hükümler, Legal Yayıncılık, İstanbul 2018, s. 81.

[254] **Kılıçoğlu**, Ahmet: Borçlar Hukuku Genel Hükümler, Turhan Kitabevi, Ankara 2012, s. 669.

[255] **Yıldız**, Kübra: "Haksız Fiil Hukukunda Nedensellik Bağının Belirlenmesi", Selçuk Üniversitesi Hukuk Fakültesi Dergisi, C. 30, S. 3, 2022, s. 1117.

[256] Yargıtay HGK, E. 1985/854, K. 1987/140, T. 6.3.1987: *...öğreti ve uygulamada geliştirilen görüş ve düşüncelerle; illiyet bağı sorunu, toplumun beklentilerine ve adalete uygun bir düzeye getirilmiştir. Bilindiği gibi illiyet bağı, özel hukuk alanında sorumluluğun önemli bir unsurudur: özellikle objektif sorumluluklarda (tehlike sorumlulukları) illiyet bağının önemi daha belirginleşir."*

[257] Yargıtay HGK T. 19.2.2019, E. 2017/2008, K. 2019/172: "*Hukuka aykırı bir fiil işleyen kimse ancak bu fiilinin sebep olduğu zararları tazminle yükümlüdür. Bir kimseden fiilinin sebep olmadığı bir zararın tazmininin istenememesi mantık icabıdır. Şu hâlde zarar ile fiil arasında mantıki illiyet bulunmayan bir zararın tazmini istenemez. Fakat fiille mantıki illiyet bağı bulunan bütün zararlardan faili sorumlu tutmak da adil olmayabilir. Hayat tecrübelerine göre, bir fiilin, olayların normal akışında meydana getirebileceği zararlarla olan mantıki illiyet bağına uygun illiyet bağı denilmektedir. Mantıki illiyet zinciri içinde bir sebebin zararı meydana getirmeye uygun bir sebep olup olmadığı araştırılacaktır.*"

Uygun illiyet bağı teorisi kapsamında bir olay, hayatın normal akışına ve evvelki tecrübelere göre ortaya çıkan zarar türünden bir sonucu doğurmaya elverişli ise, o olay gerçekleşen sonucun sebebi olarak değerlendirilir.[258]

Haksız fiilin son unsuru olan kusurun tanımına ilişkin TBK'da bir hüküm bulunmamaktadır.[259] Literatürde kusur, hukuk düzenine uygun olmayan ve ahlâk tarafından kınanabilir bir davranış biçimi olarak tanımlanmaktadır.[260] Buna göre kusur, hukuka aykırı bir fiili işleyen failin belirli bir düşünce veya ruh hâlini ifade eder. Kişi eğer hukuka uygun davranma olanağı bulunduğu hâlde kendisinden beklenen hareket biçimine aykırı davranarak hukuk kuralını ihlâl etmişse kusurludur.

TBK'da kusurun tanımı bulunmamakla birlikte "*Kusurlu ve hukuka aykırı bir fiille başkasına zarar veren, bu zararı gidermekle yükümlüdür.*" ifadesi kusurun kast veya ihmalle gerçekleşebileceğini ortaya koymaktadır.[261] Ayrıca fail her tür kusurundan doğan zarardan sorumludur.[262] Dolayısıyla haksız fiil sorumluluğu için kişinin gerekli dikkat ve özeni göstermesi yeterlidir.

Ayırt etme gücüne sahip olmayan kişiler fiil ehliyetine sahip olmamaları nedeniyle hukuka aykırı eylemlerinden dolayı sorumlu tutulmazlar. Geçici olarak ayırt etme gücünü kaybeden kişi ayırt etme gücünü kaybetme noktasında kusuru olmadığını ispatlarsa sorumluluktan kurtulacaktır. Ancak somut olayda hakkaniyet ilkesine göre eylemlerinden doğan zararın kısmen veya tamamen karşılanmasına hükmedilebilir.

Bu noktada hukuki sorumluluğun genişlemesini sağlayan kusursuz sorumluluk konusunu açıklamak uygun olacaktır. Kusursuz sorumluluk özünde istisnai bir durum olup fiilden mağdur olan kişinin imkanlarını genişleten bir hukuki olanaktır.

---

[258] **Erişgin**, Nuri: "Tehlike Bağı", AÜHFD, C. 49, S. 1, 2000, s. 139.

[259] Yargı kararlarında ise kusur tanımı yer almakta olup bu tanım şu şekildedir: "*…kusur, hukuk düzenince kınanabilen davranıştır. Kınamanın nedeni, başka türlü davranma olanağı varken ve zorunlu iken, bu şekilde davranılmayarak, bu tarzdan sapılmış olmasıdır. Kısacası; kusur, genel tanımıyla, hukuk düzeni tarafından bir davranış tarzının kınanması olup; bu kınama, o davranışın belirli koşullar altında bireylerden beklenen ortalama hareket tarzından sapmış olmasından kaynaklanır."* Yargıtay HGK'nın E. 2014/77, K.2015/1712, T. 19.06.2015 kararı.

[260] **Eren**, 653; **Tunçomağ**, s. 439; **Antalya**, Borçlar Genel, s. 416, **Tekinay**/**Akman**/**Burcuoğlu**/**Altop**, s. 492.

[261] **Ayan**, s. 315.

[262] **Tunçomağ**, Kenan: Türk Borçlar Hukuku Genel Hükümler, İstanbul, 1976, s. 441, **İnan**, Ali Naim: Borçlar Hukuku Genel Hükümler, AÜHF Yayınları, Ankara 1984, s. 265; **Eren**, 574, **Ayan**, s. 315, **Tekinay**/**Akman**/**Burcuoğlu**/**Altop**, s. 495.

Kusursuz sorumluluğunun şartları açısından bakıldığında ise kusura dayanan haksız fiilin şartlarından yalnızca kusur aranmaması yönüyle farklılaşmakta olup diğer şartlar olan fiil, hukuka aykırılık, zarar, nedensellik bağı açısından bir fark bulunmamaktadır. TBK'da kullanılan sistematiğe göre kusursuz sorumluluk kendi içinde hakkaniyet sorumluluğu, özen sorumluluğu ve tehlike sorumluluğu olmak üzere üçe ayrılmaktadır.[263]

Sorumluluk hukukunda kural olarak kişinin kusurlu davranışı sonucunda zararlı sonuç doğarken kusursuz sorumluluk hallerinde ise sorumluluk, kusurlu bir fiile değil açık bir kanun hükmünün öngördüğü açık bir olguya bağlanmıştır.[264] Kusursuz sorumluluk fikrinin ortaya çıkışına ve bir zararın kusursuz sorumluluk kapsamına bağlanma sebeplerine bakmak kusursuz sorumluluğu anlamak açısından uygun olacaktır.

Kusursuz sorumluluk kurumunun ortaya çıkmasına yol açan sebeplere bakacak olursak teknik gelişmeler ve kusur sorumluluğunun yetersizliği olduğu görülmektedir.

Teknik gelişmelere açısından bakıldığında endüstri devriminin tamamlanması ile birlikte makineleşme artmış ve gelişmiş toplum yapısına geçilmiştir. Kusur sorumluluğu ise küçük sanayi ve tarım üretimine dayanan bireyci toplumlarda yeterli olurken daha karmaşık ilişkilerin bulunduğu modern toplumlar için yetersiz kalmaya başlamıştır. Liberal devlet yapısından adalete ve hakkaniyete dayanan sosyal devlet yapısına evrilmeye başlamasıyla birlikte kusursuz sorumluluk ortaya çıkmıştır.[265]

Diğer taraftan gelişmiş makinelerin, ulaşım ve iletişim sistemlerinin, gelişmiş enerji tesislerinin kurulmasıyla birlikte yalnızca kusura dayalı sorumluluk bu yapılardan doğan zararı karşılamak ve somut olayda hakkaniyeti sağlamak için yetersiz kalmaya başlamıştır. Tehlikeli araç gereçler, iş yerleri, mekanik cihazlar gerekli tüm tedbirler alınsa ve tüm sorumluları dikkatli olsa dahi zararı önlemeye yetmeyebileceği gibi bireysel kusurun her bir olayda tespit edilmesi de mümkün

---

[263] **Eren**, s. 702; **Tekinay**/**Akman**/**Burcuoğlu**/**Altop**, s. 500; **Tandoğan**, Mesuliyet, s. 58; **Oğuzman**/**Öz**, Borçlar Hukuku Genel Hükümler, s. 188.
[264] **Yavuz**, Cevdet: Kusursuz Sorumluluk, MÜHF-HAD, C.14, S.4, Y.2008, s. 29-61, s.35.
[265] **Yavuz**, Kusursuz Sorumluluk, s. 36 vd.

olmamaktadır. Sosyal adaletin tesis edilebilmesi için kusursuz sorumluluk ilkesinin kabul edilmesi gerektiği anlaşılmaktadır.

Kusursuz sorumluluğu gerektiren hukuki ilkelerin hangileri olduğu konusunda ise genel olarak üç ilkenin öne sürüldüğü görülmektedir.[266] Bunlar sırasıyla hakkaniyet, tehlike ve hakimiyet ilkeleridir. Hakkaniyet ilkesine göre zarar veren ve zarar gören kişilerin ekonomik durumları birbirleriyle mukayese edilerek zarar verene kıyasla ekonomik olarak daha güçsüz durumdaki kişiyi korumayı amaçlamaktadır.

Tehlike ilkesi açısından bakıldığında ise yüksek risk arz eden bir faaliyete girişen veya bir işletmeyi çalıştıran kişi ilgili faaliyet veya işletmeden doğan karakteristik riskin gerçekleşmesinden dolayı kusuru olmasa dahi sorumludur. Tehlike ilkesinin amacı yüksek risk arz eden işlerden fayda elde eden kişinin ortaya çıkabilecek zarardan da sorumlu olması gerektiği fikridir.

Hakimiyet ilkesi açısından ise kişi kendi hakimiyeti içerisinde kalan bir faaliyet, işletme veya insan bir başkası kişilere zarar vermişse sorumluluğun hakimiyet sahibi kişiye ait olması uygun olacaktır. Hakimiyet sahibinin kendi hakimiyet alanında bulunan ve tehlike arz eden konuda denetim ve gözetleme olanağına sahiptir. Diğer bir ifadeyle hakimiyet alanı içinde kalmayan bir sebepten dolayı kusursuz sorumluluk yoluna başvurulması olanaksızdır. Dolayısıyla kusursuz sorumluluktan bahsedebilmek için hakimiyet sınırları içinde olmak gerekli bir kriterdir.

Kusursuz sorumluluk yolunu açan ilkeler yukarıda açıklanmıştır. Bu açıklamalar doğrultusunda bir faaliyetin kusursuz sorumluluk gerektirip gerektirmediği değerlendirilmektedir.[267]

3.1.1.2. Kişisel Verilerin Korunması Yükümlülüğü Kapsamında Haksız Fiil Sorumluluğu

İlgili başlıkta haksız fiilin şartlarını sayarak ve genel bilgiler vererek açıklamıştık. Bu başlıkta ise somut olarak bir veri ihlalini gerçekleşmesi durumunda haksız fiil

[266] **Yavuz**, Kusursuz Sorumluluk, s. 38.
[267] Kusursuz sorumluluk tartışmaları KVKK'daki 11. madde çerçevesinde bu bölümde incelenecektir.

sorumluluğuna başvurmak ve zararını tazmin edebilmek için gerekli şartların neler olduğu incelenecektir.

İlgili başlık altında veri ihllalerini kabahatler ve suçlar olmak üzere iki başlık halinde inceleyerek veri ihlallerinin neler olduğunu izah etmiştik. Bu veri ihlallerinden aynı zamanda haksız fiil teşkil edenlerin hangileri olduğunu inceleyeceğiz.

Konusu suç teşkil eden fiillerin aynı zamanda haksız fiil olarak değerlendirilmesi beklenir. Daha açık bir ifadeyle suçların kanunilik ilkesine tabi olması nedeniyle haksız fiil tanımında aranan hukuka aykırılık koşulunun doğrudan sağlandığını kabul edebiliriz. Konusu suç olan bir fiili işleyen kişi bir hukuk kuralını ihlal etmiştir. Ancak suç olarak düzenlenen bir davranışın sonucunda zarar ortaya çıkmaması ihtimal dahilindedir. Bu suç türleri[268] özel hukuk anlamında haksız fiil olarak değerlendirilmeyecektir.[269]

Yukarıda yer verdiğimiz veri ihlallerini inceleyecek olursak TCK'da düzenlenen kişisel verilerin kaydedilmesi, verileri hukuka aykırı olarak verme veya ele geçirme, verileri yok etmeme suçları sebebiyle maddi veya manevi bir zarar doğmuşsa haksız fiil hükümlerine dayanarak tazminat talep edilmesi mümkündür.

Kişisel verilerin kaydedilmesi işlemi eğer bir sözleşme veya yasal izin olmaksızın yapılıyorsa, üçüncü bölümde yer verilen tanım ve kriterler kapsamında haksız fiil oluşturacaktır. Kişisel verileri kaydedilen ilgili kişi aynı zamanda haksız fiilden zarar gören kişidir. Kişisel verilerin kaydedilmesi sebebiyle ilgili kişinin zararı maddi veya manevi zarar olarak ortaya çıkabilir.

Kişinin bir dönem yaşadığı veya halen devam bir hastalığa ilişkin sağlık verisinin, yetkisiz kişilerce kaydedilmesi sonucu hissettiği manevi zarar, şahıs varlığına ilişkin bir zarardır. Ancak kişinin bu veri ihlali sonucunda toplumdan dışlanarak

---

[268] Somut bir örnek vermek gerekirse 6136 sayılı Ateşli Silahlar Kanunu m. 13/1'de "*Bu Kanun hükümlerine aykırı olarak ateşli silahlarla bunlara ait mermileri satın alan veya taşıyanlar veya bulunduranlar hakkında bir yıldan üç yıla kadar hapis ve otuz günden yüz güne kadar adlî para cezasına hükmolunur.*" düzenlemesi mevcuttur. Herhangi bir somut zararın meydana gelmesi ilgili suçun oluşması için şart koşulmamıştır. Dolayısıyla ilgili suçun haksız fiil oluşturduğunu söylemek mümkün olmayacaktır.

[269] **Kılıçoğlu**, Ahmet: "Haksız Fiillerden Sorumlulukta Ceza Hukuku İle Medenî Hukuk İlişkisi", AÜHFD, C. 29, S. 3, 1973, s. 186.

veya sosyal çevresini kaybederek bozulan ruh sağlığının tedavisi amacıyla yapılan harcamalar mal varlığı zararı olarak değerlendirilebilir.

Aynı zamanda verileri hukuka aykırı olarak verme veya ele geçirme suçunda da, ilgili kişi bu davranıştan eğer maddi veya manevi bir zarar görmüşse diğer bir deyişle yukarıda yer verilen haksız fiil şartları somut olayda gerçekleşmişse haksız fiilden doğan sorumluluğa başvurulması gerekmektedir.

Nitekim Yargıtay 4. HD kişisel verilerin ele geçirilmesi nedeniyle uğranan zarara ilişkin kararında[270] "...*davacının kimlik bilgilerinin rızası dışında kullanılması sebebiyle davacının kişisel verilerinin haksız olarak ele geçirildiği ve kullanıldığı sabit olup davalının eyleminin davacının kişilik haklarına saldırı teşkil ettiği dikkate alınarak uygun bir miktar manevi tazminata hükmedilmesi gerekirken tümden reddine karar verilmiş olması doğru olmamış kararın bu sebeple de bozulması gerekmiştir.*" şeklinde hüküm kurmuştur. İlgili kararda kişisel verilerin ele geçirilmesi haksız fiil[271] olarak nitelendirilmiştir.

Diğer taraftan Yargıtay HGK'nin ilgili kararında[272] hükme bağlanan olayda cinsel istismar mağduru kişinin kişisel bilgileri bir ceza hukuku kitabında açıkça yer almaktadır. Kişi isim bilgilerinin kişisel veri olduğunu ve bir kitapta açık biçimde yer almasının kişisel verileri rıza dışında yayma olarak değerlendirilmesi yanlış olmayacaktır.[273]Kararda defaten kişisel verilerin korunmasının önemine değinilse de o dönemde KVKK'nın yürürlükte olmaması, veri ihlallerine ilişkin suçların uygulama alanının bugünkü kadar anlaşılmaması ve özel hayatın gizliliği ile kişisel verilerin korunması arasındaki ayrımın açıkça bilinmemesi gibi sebeplerle özel hayatın gizliliğinin ihlal edildiği gerekçesiyle manevi tazminat ödenmesi gerektiğine hükmedilmiştir.[274]

---

[270] Yargıtay E. 2019/979 , K. 2019/2679, T. 08/05/2019.

[271] "*Davalı tarafından davacının kimlik bilgilerinin kullanılması suretiyle hat çıkarılması işleminde bayi olarak gereken dikkat ve özeni göstermeyen davalı … haksız fiil faili ile birlikte zarardan sorumlu olduğu halde adı geçen davalı bakımından yazılı gerekçe ile davanın reddine karar verilmiş olması da yerinde değildir."*

[272] Yargıtay HGK E. 2014/4-56 K. 2015/1679 T. 17.6.2015.

[273] Davacı talebini unutulma hakkı ve özel hayatın gizliliği üzerinden gerekçelendirmeyi seçmiştir. Ancak mahkeme kararında yer almasa dahi ilgili suçun şartlarının somut olayda gerçekleştiği anlaşılmaktadır.

[274] "*O halde davacının isminin rumuzlanmadan kitapta yer almasının unutulma hakkını ve bunun neticesinde özel hayatın gizliliğini ihlal ettiği dikkate alındığında davacı lehine manevi tazminat koşullarının gerçekleştiğinin kabulü zorunludur."*

Yargıtay 4. HD kararında[275] ise davalının, mağdurun kimlik bilgilerini kullanarak davacı adına mobil telefon hattı çıkardığı, bu hatta ait faturayı ödememesi sebebiyle davacı aleyhine icra takibi yapıldığı anlaşılmaktadır. İlgili kararda, mağdurun kişisel verilerinin haksız biçimde ele geçirilerek kimlik bilgilerinin rızası dışında kullanılması gerekçesiyle mağdurun kişilik haklarına saldırıldığına ve manevi tazminata hükmedilmesi gerektiğine karar verilmiştir.

Değindiğimiz bilgiler, kararlar ve içtihat ışığında kabahat veya suç olarak düzenlenen veri ihlalleri sonucunda bir zarar doğmuşsa haksız fiil sorumluluğu yoluna başvurulması mümkün görünmektedir.

3.1.2. Kişisel Verilerin Korunması Yükümlülüğünün İhlalinde Sözleşme Sorumluluğu

3.1.2.1. Sözleşme Sorumluluğuna İlişkin Genel Olarak

TBK m. 1-48 arasında sözleşmeden doğan borç ilişkileri düzenlenmiştir. Bu bölümde sözleşmenin geçerli ve sağlıklı bir biçimde kurulması için gereli şartlar ve tarafların iradeleriyle kararlaştırılabileceği hususlar, sözleşmenin sağlıklı kurulmasını engelleyen haller düzenlenmiştir.

Sözleşmeye aykırılık sebebine dayanarak borçlunun sorumluluğuna gidilmek isteniyorsa öncelikle sözleşmenin geçerli bir biçimde kurulması gerekmektedir. Bunun için ise tarafların iradeleri karşılıklı ve birbiriyle uygun biçimde açıklanmasının yanı sıra tarafların sözleşme ehliyetine sahip olması, sözleşme konusunun emredici hukuk kurallarına, genel ahlâka, kamu düzenine ve kişilik haklarına uygun olması, sözleşme konusunun imkânsız olmaması ve irade beyanlarının hata, hile, korkutma sebepleriyle sakat olmaması şartları aranmaktadır.[276] Sağlıklı ve geçerli bir biçimde kurulmayan sözleşmeye göre ise tarafların sözleşme hükümlerine dayanarak talepte bulunması mümkün olmayacaktır.

Sözleşmeden doğan sorumluluktan bahsedebilmek için gerekli şartların borca aykırı davranış, ihlal, zarar, nedensellik bağı ve kusur olduğu kabul edilmektedir.[277]

---

[275] Yargıtay 4. HD, E. 2019/979 K. 2019/2679 T. 8.5.2019.
[276] **Eren**, s. 436; **Tunçomağ**, s. 332.
[277] **Eren**, s. 1172, **Kılıçoğlu**, Borçlar Genel, s. 669.

TBK'da sözleşmeden doğan borçlara aykırılık durumunda ne yapılması gerektiğine ilişkin m. 112 hükmü mevcut olup bu hükme göre "*Borç hiç veya gereği gibi ifa edilmezse borçlu, kendisine hiçbir kusurun yüklenemeyeceğini ispat etmedikçe, alacaklının bundan doğan zararını gidermekle yükümlüdür.*"

İlgili hükümden açıkça anlaşıldığı üzere borca aykırı davranan kişinin kusurlu olduğu varsayılmakta olup alacaklının yalnızca zararı ispatlaması gerekmektedir. Buradaki zarar alacaklının hukuk tarafından korunan değerlerinde iradesi dışındaki azalma olarak anlaşılmalıdır. Sözleşmeye aykırılık neticesinde maddi veya manevi zarar doğabilir ancak borçludan talep edilebilmesi için sözleşmenin ihlali ile nedensellik bağı içerisinde olmalıdır.

Maddi zarar ile kast edilen alacaklının malvarlığının bugünkü durumu ile gerektiği gibi ifa gerçekleşseydi malvarlığının bulunacağı durum arasındaki farktır.[278] Maddi zarar fiili zarar ve yoksun kalınan kar olarak iki türe ayrılmaktadır. Somut olayda TBK 112 hükmüne zararın tespitine ilgili başlık altında değinilecek olmakla birlikte ekonomik değer içermeyen menfaatlerin tazminata yol açmayacağını belirtmek gerekir.

Sözleşmeden doğan sorumluluk, sözleşmenin taraflarından birinin sözleşmede kararlaştırılan yükümlülüklerini ifa etmemesi durumunda ortaya çıkmaktadır.[279] Sözleşmeye aykırı davranan tarafın tazminat sorumluluğu gündeme gelecektir.

3.1.2.2. Kişisel Veri İşleme Sözleşmesi ve Bu Sözleşmeden Doğan Sorumluluk

3.1.2.2.1. Kişisel Veri İşleme Sözleşmesine İlişkin Genel Olarak

Mevzuatta kişisel verilerin işleme sözleşmesi isminde bir sözleşme düzenlenmemiştir. Ancak hukukumuzda geçerli olan prensip sözleşme tip serbestisi olduğundan taraflar aralarında anlaşarak kanunda yer almayan bir sözleşmeyi kurabilmektedir.[280] Taraflar aralarında bir sözleşme kurarak ana edim olarak kişisel verilerin işlenmesini kararlaştırabilir. Bu durumda sözleşmenin asli edim yükümlülüğü olan veri işleme faaliyeti sözleşmeye adını verecektir.[281]

---

[278] **Tekinay**, Sulhi/**Akman**, Sermet/**Burcuoğlu**, Haluk/**Altop**, Atilla: Borçlar Hukuku Genel Hükümler, Filiz Kitabevi, İstanbul, 1993, s. 855.
[279] **Eren**, 1190; **Tandoğan**, Mesuliyet, 415.
[280] **Gümüş**, Mustafa Alper: Borçlar Hukuku Özel Hükümler, Vedat Kitapçılık, İstanbul 2012, s. 4.
[281] **Oğuzman/Öz**, C. 1, s. 73, **Eren**, Borçlar Genel, s. 249.

Kanunda düzenlenmeyen bir sözleşmeyi akdetmek isteyen taraflar konusunu, hükümlerini ve sonuçlarını aralarında gibi kararlaştırabilecektir. Kanunda düzenlenmeyen ancak tarafların kendi iradeleriyle sözleşme özgürlüğü kapsamında akdettikeleri bu tür sözleşmeler isimsiz sözleşme olarak sınıflandırılmaktadır. Kişisel verilerin işlenmesi sözleşmesi, taraf iradesine dayalı olması nedeniyle her bir örnekte değişmekle birlikte, genellikle vekâlet ve eser sözleşmelerine özgü edimleri barındırmaktadır.[282]

Taraflardan biri hukuka uygun biçimde veri işleme edimini taahhüt ederken diğer taraf hizmet sunma veya ücret ödeme gibi buna denk bir edimi taahhüt etmektedir. Kişisel veri işleme sözleşmesi, kanunda düzenlenen birden çok sözleşme türüne ait edimlerin, kanunda düzenlenenden farklı bir biçimde bir araya getirilmesiyle kurulmaktadır. Dolayısıyla kişisel verilerin işlenmesi sözleşmesi, türü itibariyle kombine tipli karma sözleşme olarak değerlendirilmelidir.[283]

Kişisel verilerin işlenmesine ilişkin sözleşmeler, taraflarına göre üçe ayrılarak incelenebilir. Bu ayrıma göre veri sorumlusu ve ilgili kişi arasındaki sözleşme, veri işleyen ve veri sorumlusu arasındaki sözleşme[284], iki veri sorumlusu arasındaki sözleşmedir[285]. Ancak çalışmanın konusunu oluşturan ilgili kişiyle veri sorumlusu arasında akdedilen ve veri işlemeyi konu edinen sözleşmedir.

Veri sorumlusu ve veri işleyen arasında yapılan kişisel veri işleme sözleşmesi kapsamında veri sorumlusu veri işleme borcu altına girmektedir. Kişisel veri işleme kavramı daha evvel de belirttiğimiz üzere kişisel verilerin toplanmasının ardından mevzuatta belirtilen yöntemlere uygun olarak silme, yok etme veya anonim hale getirme işlemlerinden biri yapılana kadar geçen zamanda yapılan her tür eylem kişisel verilerin işlenmesi olarak adlandırılmaktadır. Sözleşmenin diğer tarafı ise sözleşmenin konusuna uygun olarak karşı bir edimi yerine getirme

---

[282] **Zevkliler**, Aydın/**Gökyayla** Emre: Borçlar Hukuku- Özel Borç İlişkileri, Vedat Kitapçılık, İstanbul, 2013, s. 470.
[283] **Özer Deniz**, s. 203.
[284] Veri işleyen ve veri sorumlusu kavramları ikinci bölümde anlatılmış, somut olayda bu iki statünün farkının nasıl ayırt edileceğine ve sorumluluklarına değinilmiştir. Çalışma kapsamında veri sorumlusu kararı doğrultusunda veri işleyenden yardım alması sorumluluğu açısından değişiklik yaratmayacaktır. KVKK'ya göre veri işleyen ve veri sorumlusu müteselsil sorumludur dolayısıyla aralarındaki sözleşme yalnızca rücu ilişkisi için değer taşımaktadır.
[285] İki veri sorumlusu arasındaki sözleşme yalnızca rücu ilişkisi açısından önem taşımaktadır. İki veri sorumlusu da veri işleme faaliyeti kapsamında müteselsil sorumludur.

borcu altına girecektir. Uygulamada genelde kişisel veri işleme sözleşmesi bir başka sözleşmenin devamı esnasında yapılmaktadır. İlgili sözleşmenin ifası için kişisel verilerin işlenmesi gerekebilir ve veri sorumlusu burada kişisel veri işleme yükümlülüğünü bir yan yükümlülük olarak üstlenmektedir.

Bir hukuki işlemin kurulabilmesi ve kendisinden beklenen sonuçları doğurabilmesi için kişisel verilerin işlenmesi zorunlu olabilir. Kişisel verileri korumayı hedefleyen mevzuat sıklıkla kurulan borç ilişkilerini ve ticaret hayatının gereklerini göz önüne alarak verilerin, bir sözleşme kapsamında işlenmesini hukuka uygun veri işleme yollarından biri olarak kabul etmiştir. Gerek KVKK'da gerekse Tüzük'te açıkça kişisel verilerin bir sözleşme çerçevesinde işlenmesinin mümkün olduğuna dair açık hüküm mevcuttur.[286]

Veri sorumlusu ve ilgili kişi arasında yapılan ve veri işleme gerekçesi olan sözleşme aradaki ilişkinin türüne göre değişmektedir. İş sözleşmeleri, sigorta sözleşmeleri, abonelik sözleşmeleri, tedavi sözleşmeleri, mesafeli satış sözleşmeleri uygulamada sıklıkla veri işlemeye ilişkin hükümleri de içeren anlaşmalardır. Bu sözleşmelerde taraflar asıl edimlerini üstlenirken aynı zamanda bu hizmeti sunmak için gerekli kişisel verileri işlemek ve bu verileri korumak edimlerini de taahhüt etmektedir.

Somut olarak örnek vermek gerekirse iş sözleşmesi kapsamında işçi bir hizmet sunma borcunu, işveren ise ücret ödeme borcunu ifa etmektedir. Ancak bu edimler iş sözleşmesinin asli edimleri olarak nitelendirilmektedir. Diğer taraftan yine iş sözleşmesi kapsamında işçinin sadakat yükümlülüğü ise yan edim olarak değerlendirilmektedir. İş verenin ise bu hizmet sözleşmesi kapsamında işçiye ait kimlik numarası, telefon numarası, medeni hali benzeri bilgiler iş veren tarafından kaydedilmektedir.

Benzer biçimde abonelik sözleşmesi kapsamında hizmet sunan teşebbüs kesintisiz biçimde elektrik, su, doğalgaz veya internet gibi bir hizmeti sunma edimini asli edim olarak yüklenirken abonelik alan taraf ise ücret ödemeyi taahhüt

[286] KVKK m. 5/2-c'de ve Tüzük m. 6/1-b'de sözleşmenin kurulması ve ifasıyla doğrudan ilgili olma koşuluyla kişisel veri işlemek için açık rıza aranmamaktadır. KVKK m. 5/2-c, "*Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.*"

etmektedir. Ancak aynı sözleşme ile hizmet sunan taraf hizmeti sunması için gerekli olan isim, adres ve ödeme bilgileri benzeri bilgileri işlemektedir.

Kredi kullanmak isteyen gerçek kişiden, banka tarafından, istenen icra ve iflas kayıtları, tapu bilgileri[287], banka hesap bilgileri, daha evvelki kredilerine ilişkin bilgiler doğrudan kredi sözleşmesinin kurulmasıyla ilgili olup banka bu bilgileri kredi sözleşmesi çerçevesinde işlemektedir. Kredi kullandırılmasına ilişkin kararın banka tarafından sağlıklı biçimde alınabilmesi için gerekli risk analizleri ancak bu bilgilerle yapılabilmektedir.

Sözleşme kapsamında kişisel veri işlemek için, ilgili kişisel verilerin sözleşmede yer alanlarla sınırlı olması gibi bir koşul mevcut mu diğer bir ifadeyle sözleşme kapsamında yer almamış kişisel veriler KVKK 5-2/c kapsamında işlenemez mi hususu tartışma konusu olabilecek bir diğer husustur. Ancak sözleşmede kişisel verilerin işlenmesine ilişkin açık bir hüküm bulunmasa dahi KVKK'da yer alan ilgili hüküm lafzından veri işlemenin önünde bir engel bulunmadığı anlaşılmaktadır. Sözleşmenin ifası için zorunlu olsun veya olması sözleşme kapsamında taraflardan biri kişisel verilerin işlenmesine ilişkin yükümlülük altına girdiğinde sözleşmeden doğan sorumluluk açısından fark oluşmayacaktır.

Taraflar arasında kişisel veri işleme sözleşmesi mevcutsa tarafların hak ve borçlarını incelemek uygun olacaktır. Kişisel veri işleme sözleşmesi kapsamında veri sorumlusunun kişisel verileri işleme yükümlülüğü mevcuttur. Sözleşmeye ismini veren ve ana edim olarak sözleşmenin konusunu oluşturmaktadır.

Kişisel verileri işleme sözleşmesi, vekalet sözleşmesine ait özellikleri taşımaktadır. Vekalet sözleşmesinin gereği olarak veri sorumlusunun sözleşmenin kurulması aşamasından başlayarak sözleşme sona erene kadar tüm aşamalarda özen gösterme borcu bulunmaktadır.[288] Sır saklama, sadakat ve aydınlatma yükümlülükleri özen gösterme borcu kapsamında değerlendirilebilir.[289]

Sır saklama ve sadakat, veri sorumlusunun sözleşme kurulmadan evvel başlayan ve sözleşme sona erene kadar devam eden bir borçtur. Kaynağını sözleşmenin

---

[287] KVKK m. 5'in gerekçesinde açıkça örneklendirilmiştir.
[288] TBK'da özen gösterme ile ilgili olarak somut bir tanım bulunmamaktadır.
[289] **Özer Deniz**, s. 218.

güven ilişkisine dayanmasından almaktadır.[290] Veri sorumlusunun bilgilendirme, aydınlatma yükümlülüğü, veri işleyeni seçimesi ve talimat vermesi sadakat borcu kapsamındadır.[291] Diğer taraftan herhangi bir meslek veya faaliyet kapsamında sır saklama yükümlülüğüne tabi olmasa dahi ilgili veri işleme faaliyeti esnasında edindiği kişisel bilgileri paylaşmamalıdır.[292]

Sözleşme kapsamında veri sorumlusunun borçlarına karşılık ilgili kişinin de borçları de borçları bulunmaktadır. İlgili kişinin borcu kişisel veri işleme faaliyetinin sebebine göre değişiklik göstermektedir.

Eğer ilgili kişinin talebi üzerine kişisel verilerinin işlendiği bir sözleşmede ilgili kişinin ücret ödeme yükümlülüğü de doğacaktır. Kişinin talebiyle kişisel veri işlenen sözleşmelere tipik örnek olarak kordon kanı saklama sözleşmeleri gösterilmektedir.[293] Kordon kanı saklama hizmeti sunan tıbbi kuruluşlar çeşitli isimler altında ücret talep etmektedir.[294]

Ancak kişinin talebi olmaksızın kişisel veri işlenen sözleşmeler de mevcuttur. Örneğin bir borcu ifa edebilmek için veri işlemek gerekiyorsa bu amaçla yapılan sözleşme kapsamında ilgili kişinin ücret ödeme borcu doğmayacaktır. İlgili kişinin ücret ödeme borcu oldukça istisnai bir durumdur ve aslolan ücret ödeme yükümlülüğü olmamasıdır.

3.1.2.2.2. Kişisel Veri İşleme Sözleşmesinden Doğan Sorumluluk

Kişisel veri işleme sözleşmesinin (KVİS) ihlal edilmesinden doğan doğan zararların tazminine ilişkin olarak KVKK'da m. 11/ğ ve m. 14 hükümlerinde TBK m. 112 ve devamına atıf yapan düzenlemeler mevcuttur. TBK m. 114 düzenlemesinden de anlaşılacağı üzere haksız fiil hükümleri sözleşmeden doğan zararlara kıyasen uygulanacaktır.[295]

---

[290] **Yavuz**: Borçlar Özel Hükümler, Seçkin Yayınları, Ankara 2018, s. 655; **Eren**, Fikret: Borçlar Hukuku Özel Hükümler, Yetkin Yayınları, Ankara 2017, s. 728; **Donay**, Süheyl: "Vekilin Talimata Uyma ve Dürüstlükle Hareket Etme Borcu", BATİDER, C. 5, S. 4,1970, s. 739; **Gökyayla**, Emre: Eser Sözleşmesinde Müteahhidin Sadakat ve Özen Borcull, GSÜHFD, Prof. Dr. Kemal Oğuzman'a Armağan, S. 1, 2002, s. 786.

[291] Veri işleyen, vekalet sözleşmesine göre alt vekil olarak değerlendirilmektedir. **Özer Deniz**, s. 219; **Yavuz**: Borçlar Özel, s. 660; **Akipek**, Şebnem: Alt Vekâlet, Yetkin Yayınları, Ankara 2014, s. 58.

[292] KVKK m. 12/4'de bu yasak açıkça düzenlenmektedir.

[293] RG 05.07.2005 ve No: 25866.

[294] Kordon kanı saklama ücreti ve yıllık aidat talep edilmektedir.

[295] **Eren**, s. 1052; **Kılıçoğlu**, Borçlar Genel, s. 667; **Oğuzman/Öz**, s. 385.

KVİS'den kapsamında veri sorumlusunun hukuki sorumluluğunun doğması için, veri sorumlusunun sözleşmeye aykırı davranması, ilgili davranışın kişiye zarar vermesi, veri sorumlusunun davranışı ve zarar arasında uygun illiyet bağı bulunmalıdır.

Sözleşmeden doğan sorumluluktan kurtulmak elbette mümkündür. Ancak illiyet bağının kesildiği durumlarda sözleşmeden doğan sorumluluktan kurtulmak mümkün olacaktır. Mücbir sebep illiyet bağını ortadan kaldırmaya yeten sebeplerden biridir ayrıca üçüncü kişinin ağır kusuru veya ihlalden zarar görenin ağır kusuru da sorumluluğun ortadan kalkması için yeterlidir.[296] Bu noktadan haksız fiil sorumluluğu ve sözleşmeden doğan sorumluluk için tazminat hususu tekrara düşmemek amacıyla aynı başlıkta anlatılacaktır.

3.1.3. Kişisel Verilerin Korunması Yükümlülüğünün İhlalinde Vekaletsiz İş Görmeden Doğan Sorumluluk

TBK m. 526-531 hükümlerinde vekaletsiz iş görme hükümleri yer almaktadır. Buna göre vekâletsiz iş görme iş sahibinin menfaatine uygun olup olmamasına göre kendi içerisinde gerçek vekâletsiz iş görme ve gerçek olmayan vekâletsiz iş görme olmak üzere ikiye ayrılmaktadır.[297]

Çalışma kapsamında konumuzu oluşturan gerçek olmayan iş görmedir. İş sahibinin izni veya yasal yükümlülüğü olmaksızın, iş görenin kendi veya üçüncü kişi faydasına bir işi görmesi durumu gerçek olmayan vekaletsiz iş görme olarak ifade edilmektedir.

Gerçek olmayan vekaletsiz iş görme kapsamında, iş sahibi TMK m. 25/3 hükmüne dayanarak elde edilmiş olan kazancın kendisine verilmesini talep edebilir.[298] Ancak iş sahibinin elde etmek istediği veya elde edebileceği kazançlar varsa, bu beklenti mahrum kalınan kar olarak nitelendirilecek ve maddi tazminat kapsamında tazmin edilebilecektir. Daha açık bir ifadeyle iş sahibinin kazanç elde etme amacının varlığı, vekâletsiz iş görme sebebiyle açılan davayla yoksun kalınan kar talep edilen maddi tazminat davasını birbirinden ayırmaktadır.

---

[296] **Ayan**, s. 332.
[297] **Kılıçoğlu**, Medeni Hukuk, s. 395.
[298] **Orak**, Beşir; Kişisel Sağlık Verilerinin Korunması, Yetkin, Ankara, 2020, s. 91.

Aynı olayda TMK m. 25 hükmü gereği kazancın iadesi, maddi ve manevi tazminat taleplerinin birlikte yapılmasının önünde bir engel yoktur.[299] Eğer maddi ve manevi tazminat ve kazanç iadesi taleplerinin tüm koşulları aynı olayda gerçekleşmişse birlikte talep edilebilecektir. Ancak iş görenin kazancı aynı zamanda ilgili kişi açısından fiilî zarar oluşturuyorsa maddi tazminat talebi ve gerçek olmayan vekâletsiz iş görmeden doğan dava birlikte açılamaz. Aynı olayda iş sahibinin kazançtan yoksun kalması ve elde edemeyeceği kazancın iş gören tarafından elde edilmesi mümkündür. Bu şartlarda iş sahibi zararı maddi tazminat davası ile talep ederken maddi zararı aşan kazancı da, vekâletsiz iş görme gerekçesiyle talep edilecektir.[300]

Kazancın iadesini talep eden davada hâkim kazancın miktarını TBK m. 50 uyarınca tespit edecek olup bu dava için zamanaşımı süresi TBK m. 72 hükmüne göre belirlenecektir.[301] Kazancın iadesi talebinin kabulü için kişilik hakkı ihlalinin hukuka aykırı olması yeterlidir. Ayrıca iş görenin kusurlu olması şartı aranmamaktadır. Aynı zamanda vekâletsiz iş görme sebebiyle talep edilen kazanç ve iş arasında illiyet bağı olmalıdır.[302]

Somut örneklerle kişisel veri ihlalleri ile bağlantılı olarak gerçek olmayan vekâletsiz iş görmeden doğan talepleri incelemek uygun olacaktır. Çevrim içi bir platformdan ürün satın alan kullanıcının mesafeli satış sözleşmesi kapsamında ürün teslimi için gerekli kişisel verileri işlenecektir. Veri sorumlusu işlediği verileri amacı dışında kullanarak gelir elde ettiği takdirde hem sözleşme hükümlerine aykırılık sebebiyle hem de gerçek olmayan vekâletsiz iş görme hükümleri kapsamında sorumlu olacaktır.

---

[299] Bu konuda literatürde birden fazla görüş vardır. Manevi tazminat ve gerçek olmayan vekâletsiz iş görme davalarının aynı zamanda açılamayacağını kabul eden bir görüş mevcut olup Bkz.: **Arpacı**, Abdülkadir: Kişiler Hukuku, İstanbul, Beta Yayınevi, 2000, s. 162. Diğer görüşe ise gerçek olmayan vekâletsiz iş görme ve maddi tazminat davası birlikte açılamazken manevi tazminat davası ile açılabilir demektedir. **Hatemi/Gökyayla**, Borçlar Hukuku, s. 303-304; **Hatemi**, Kişiler Hukuku s. 79.

[300] **İmançlı**, s. 198.

[301] **Özdemir**, Kişisel Veri, s. 204; **Helvacı**, Serap: Gerçek Kişiler, Legal Yayınları, İstanbul 2017, s. 168-169.

[302] **Tandoğan**, Haluk: Mukayeseli Hukuk, İstanbul 1957, s. 143; **Kılıçoğlu**, Medeni Hukuk, s. 395.

Bir diğer örnekte ise hukuka aykırı biçimde reklam şirketlerine ilgili kişinin kişisel verilerini[303] satan bir veri sorumlusu elde ettiği gelir sebebiyle gerçek olmayan vekaletsiz iş görme hükümleri kapsamında sorumlu tutulacaktır.

3.1.4. Kişisel Verilerin Korunması Yükümlülüğünün İhlalinde Dürüstlük Kuralına Dayanan Sorumluluk

Sözleşme kurulması durumunda sözleşme hükümlerine göre tarafların sorumlulukları mevcuttur. Ancak taraflar sözleşme yapmak maksadıyla istişarelere başlarsa ve beklenen sözleşme kurulmazsa sözleşme hükümlerine dayanmak mümkün olmayacaktır. Ancak bu durumda dürüstlük kuralından hareketle yine tarafların sorumlulukları mevcuttur. Öncelikle sözleşme görüşmeleri sürecinde tarafların dürüstlük kuralına aykırı davranması hususuna değineceğiz.

Sözleşme görüşmeleri esnasında görüşenlerin dürüstlük kuralarına aykırı biçimde hareket etmesinden doğan zararın tazmini *culpa in contrahendo* (sözleşme görüşmelerinde kusurlu davranmak) olarak ifade edilmektedir.[304]

TMK m. 2'de düzenlenen dürüstlük kuralı hükümlerine göre sözleşme kurmak amacıyla görüşme yapmaya başlayan taraflar, karşılıklı dürüst davranma ve sözleşme koşullarını etkileyecek konularda birbirlerine doğru bilgi vermekle yükümlüdür. Sözleşme öncesi süreçte yapılması planlanan sözleşmeye göre değişmekle birlikte taraflar birbiriyle çok sayıda kişisel bilgiyi paylaşabilmektedir.

Örneğin taraflar konusu eğitim olan bir vekâlet sözleşmesi yapmak için bir araya geldiklerinde eğitim verecek kişi isim, tecrübe ve nitelikleri hakkında kişisel bilgileri de içeren bir takım bilgileri verirken diğer taraf da kendisine ait isim, yaş ve önceki deneyimlerini de içeren bilgileri karşı tarafa sunacaktır. Yapılmak istenen sözleşmenin amacı değiştiğinde paylaşılan kişisel bilgilerin niteliği de değişebilmektedir.

İş başvurusu yapan biri kişisel bilgilerini ihtiva eden bilgileri paylaşmaktadır. Bu başvurularda adli sicil kaydında yer alan kişinin özel nitelikli verileri de

---

[303] Veri sorumlusu, ilgili kişinin iletişim bilgilerini satarak reklama maruz kalmasına yol açabilir veya görsel vb. reklamda kullanılabilecek kişisel verileri satarak gelir elde edebilir.
[304] **Hatemi**, Hüseyin: Medeni Hukuk, XII Levha Yayınlar, İstanbul 2020, s. 195.

paylaşılmaktadır. İşveren kişiyle iş sözleşmesi yapmasa dahi bu sözleşme öncesi görüşmelerde bilgilere erişebilmektedir.

Sözleşme görüşmelerinden doğan sorumluluğun haksız fiil hükümleri mi uygulanır borca aykırılık hükümleri mi uygulanır konusu literatürde kesin değildir.[305] İlk görüş tarafların karşılıklı olarak duydukları güvene dayandığı ve dürüstlük kuralı kapsamında sözleşme benzeri bir borç ilişkisi teşkil ettiği görüşüdür.[306] İkinci görüş ise görüşme taraflarının arasında bir sözleşme kurulmadığı için sözleşme hükümlerinin uygulanamayacağı haksız fiil hükümlerinin uygulanması gerektiği görüşüdür.[307] Üçüncü görüş ise, *culpa in contrahendo* sorumluluğun özgün bir yapısı olması nedeniyle somut olayda hangi hükümlerin uygulanacağının değerlendirilmesinin uygun olacağı yönündedir.[308]

Bu görüşler arasında sözleşme görüşmeleri esnasında tarafların karşılıklı güvene dayalı olarak dürüstlük kuralına dayanan sözleşme benzeri borç ilişkisi kurulduğunu savunan görüş kişisel veri ihlallerinden doğan sorumluluk açısından daha makuldür. KVKK'den doğan haksız fiil sorumluluğu kusura dayanmadığından sözleşmeden doğan sorumluluk hükümlerine dayanılması daha makul görünmektedir. [309]

Diğer taraftan sözleşme sağlıklı bir şekilde kurulduktan sonra sona ermesi de mümkündür. Herhangi bir sebeple sona eren bir sözleşme sonrası taraflar güven ilişkisi nedeniyle birbirine zarar vermemekle yükümlüdür. Bu duruma sözleşmenin art etkisi ismi verilmektedir.[310]

Sözleşmenin art etkisinin dayanağı dürüstlük kuralıdır. Sözleşme sona erse dahi tarafların karşılıklı borçlarının tamamıyla sona ermediği dolayısıyla sözleşme kapsamında işlenen verilerin eğer derhal imhası mümkün değilse veya mevzuat kapsamındaki bir yükümlülük vb. sebepler mevcutsa veri sorumlusunun yükümlülükleri devam edecektir. Sözleşme sona erse dahi devam eden bu

---

[305] **Eren**, Borçlar Hukuku Genel Hükümler, s. 1159; **Nomer**, s. 410; **Oğuzman/Öz**, Borçlar Hukuku, s. 480.
[306] **Zor**, s. 163.
[307] **Kılıçoğlu**, Borçlar Genel, s. 124; **Antalya**, Borçlar Genel, İstanbul 2015, s. 195.
[308] **Oğuzman/Öz**, Borçlar Hukuku, s. 480; **Eren**, s. 1160; **Antalya**, Borçlar Genel, s. 196.
[309] **İmançlı**, s. 163.
[310] **Serozan**, s. 263, **Oğuzman/Öz**, s. 38.

yükümlülükler ihlal edilirse sözleşmenin art etkisi nedeniyle sözleşmeye aykırılık hükümlerine gidilecektir.[311]

Sözleşmenin art etkisine benzer bir hüküm KVKK'da m. 12/4'de yer almaktadır. İlgili madde hükmü "*Veri sorumluları ile veri işleyen kişiler, öğrendikleri kişisel verileri bu Kanun hükümlerine aykırı olarak başkasına açıklayamaz ve işleme amacı dışında kullanamazlar.*" şeklindedir. Sözleşme sonrası devam eden yükümlülüklere örnek olarak sır saklama ve sadakat yükümlülükleri verilmektedir. KVKK m. 12/4 hükmüne bakıldığında veri sorumlusu veya veri işleyenin bu görevi bittikten sonraki sorumluluğunun sözleşmenin art etkisinden kaynaklandığı anlaşılmaktadır.[312]

Dolayısıyla sözleşme öncesi süreçte ve sözleşmenin sona ermesiyle başlayan süreçte de veri sorumlusunun yükümlülükleri mevcuttur. Yukarıda bahsedildiği üzere veri sorumlusu ve ilgili kişi arasında sözleşme kurulmazsa dahi bu süreçte edindiği bilgileri paylaşmamakla yükümlüdür. Diğer taraftan sözleşme kurulup bağlayıcı hale geldikten sonra da sona erebilir. Bu durumda da yukarıda açıklandığı üzere veri sorumlusunun elde ettiği bilgilerle ilgili yükümlülükleri sona ermemektedir. Dürüstlük kuralı ve KVKK 12/4 hükmü gereği başka bir yerde bu bilgiler kullanılamaz.[313]

3.2. KİŞİSEL VERİLERİN KORUNMASI YÜKÜMLÜLÜĞÜNÜN İHLALİNDE KVKK KAPSAMINDA SORUMLULUK

KVKK m. 11/1-ğ hükmünde herkesin "*Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme*" hakkı olduğu açıkça düzenlenmiştir. Veri koruma hukuku ülkemizde yeni gelişmekte olan bir hukuk alanı olup uygulamaları tam anlamıyla oturmamıştır. Buna paralel biçimde veri ihlallerinden doğan özel hukuk sorumluluğuna ilişkin uygulamanın netleşmesi de zaman almaktadır.

---

[311] **Zor**, s. 164.

[312] **Ayözger Öngün**, Çiğdem: Kişisel Verilerin Korunması Hukuku – Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil, 2. Baskı, İstanbul, Beta, 2019, s. 237.

[313] Veri Silme Yönetmeliği, sözleşme sonrası veri işleme için dayanağı kalmayan veri sorumlusunun verileri nasıl yok edeceği hususunu kapsamlı olarak düzenlemektedir. Bkz ilgili yönetmelik m. 7-12 hükümleri.

İlgili madde hükmünün bir kusur sorumluluğu mu yoksa kusursuz sorumluluk mu olduğu, kusursuz sorumluluksa alt türü, zararın nasıl hesaplanacağı ve kapsamının nelerden oluştuğu belirgin değildir.

Literatürde ilgili hükmün lafzından hareketle "kusur" ifadesinin madde hükmünde yer almadığını, veri sorumlusunun veriyi koruma yükümlülüğünün KVKK'da açıkça düzenlendiğini, veri sorumlusunun objektif özen yükümlülüğü bulunduğunu ifade eden bir görüş bulunmaktadır.[314] Bu görüş veri sorumlusunun KVKK kapsamındaki sorumluluğunu olağan sebep sorumluluğu olarak tanımlamaktadır.[315] KVKK'da düzenlenen sorumluluğun özen sorumluluğu olarak kabul edilmesi veri sorumlusunun, ilgili kişinin verilerinin korunması noktasında daha hassas davranmaya itecektir. Ayrıca ilgili kişi yalnızca fiilin hukuka aykırı olduğunu ve fiilden kaynaklanan zararı ispat etmelidir. Gerekli dikkat ve özeni gösterdiğini ispat yükü ise bu andan itibaren veri sorumlusuna aittir.

Veri sorumlusunun kurtuluş kanıtı getirdiği takdirde sorumluluktan kurtulmasına olanak tanıyan bu görüşe göre veri sorumlusu yalnızca özenli davrandığını[316] ispatladığı takdirde sorumluluktan kurtulacaktır.[317] Veri işleme faaliyetinin ağırlıklı olarak dijital sistemlerle gerçekleşmesi, her geçen gün daha karmaşık ve teknik bir hal alması ve bu faaliyete ilişkin veri sorumlusuna mevzuatla bir takım yükümlülükler yüklendiği dikkate alındığında ispat standardının sağlanması açısından kusursuz sorumluluk yolunun daha makul olduğu anlaşılmaktadır.[318] Aksi takdirde ilgili kişi erişimi ve denetimi olmayan bir sistemin yeterince özenli olup olmadığı konusunda ispat yükümlülüğünü sağlamakta zorlanacaktır.

Literatürde tartışılan bir diğer konu ise veri sorumlusunun yine kusursuz sorumluluğu bulunduğunu ancak bu sorumluluğun alt türünün tehlike

---

[314] **Çekin**, Mesut Serdar: Kişisel Verilerin Korunması, XII Levha Yayınları, İstanbul 2019, s. 139; **Korkmaz**, İbrahim: "Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme", TBB Dergisi S. 124, 2016, s. 134; **Zor**, s. 148.

[315] **Çekin**, Mesut Serdar: "6698 Sayılı Kişisel Verilerin Korunması Hakkında Kanun'un Big Data (Büyük Veri) ve İrade Serbestisi Açısından Değerlendirilmesi", İÜHFM, C. LXXIV, S. 2, 2016, s. 638.

[316] Özen kavramı soyut olmakla birlikte özen seviyesinin belirlenmesinde yalnızca veri koruma mevzuatında belirtilen önlemlerin artması yeterli olup olmadığı ve somut olayda başkaca kriterlerin aranması gerekip gerekmediği hususunda net bir mevcut değildir.

[317] **Çekin**, Kişisel Veri, s. 139. Kurtuluş kanıtına ilişkin olarak bkz. **Tekinay/ Akman/ Burcuoğlu/ Altop**, Borçlar Genel Hükümler, s. 497 vd.

[318] **Çekin**, Kişisel Verilerin Korunması, 139; **Gürpınar**, s. 694.

sorumluluğu olup olamayacağı hususudur.[319] Kişisel verileri işlemek için kullanılan dijital ortamların tüm önlemler alınsa dahi güvenliğinin tam anlamıyla sağlandığını garanti etmek mümkün değildir. Nitekim birçok büyük teknoloji teşebbüsü bu tür veri sızıntıları sebebiyle veri ihlalleri yaşamıştır. Dolaysıyla yapılan veri işleme faaliyeti kendi içerisinde her zaman veri ihlali riskini barındırmaktadır.

Dijital mecraların sağladığı olanaklarla büyük hacimli veriyi kolaylıkla işleyen veri sorumlularının, bu verileri dijital ortamda gerektiği gibi koruyamama riskini de üstlenmeleri hakkaniyet ilkesinin gereğidir.[320] Bu noktada hakkaniyet gereği tehlike sorumluluğunun varlığını kabul etmek makul olarak görülse de KVKK'da bu yönde açık bir hüküm olmaması[321] nedeniyle uygulamada bu mümkün görünmemektedir.[322] Diğer taraftan KVKK'da hüküm bulunmaması nedeniyle genel hükümlere bakıldığında TBK'nın tehlike sorumluluğu ve denkleştirme hususunu düzenleyen m. 71 hükmü mevcuttur.

Bu konudaki tartışmanın merkezinde veri sorumlularının veri işleme faaliyetlerinin TBK m. 71 kapsamında tipik bir tehlike olarak nitelendirilip nitelendirilemeyeceği hususu yer almaktadır. Eğer tipik veri işleme faaliyeti bir tehlike olarak tanımlanırsa herhangi bir kusur işletenin herhangi bir kusuru olmaksızın, özenli davranıp davranmadığı değerlendirilmeksizin, işletmenin organizasyonunda bir eksikliği olup olmadığına bakılmaksızın zararın tazminini sağlayacaktır.

Ancak veri ihlalleri doğrudan maddi veya manevi bir zararın doğması için yeterli değildir. Kişisel verilerin açığa çıkması, TBK'da zarar olarak sayılan ölüme veya bedensel bütünlüğün bozulmasına yahut başkaca bir kişisel değerin zedelenmesine veya malvarlığında bir eksilmeye neden olmayacaktır.[323]

---

[319] Bu başlık altında görüşlere detaylı yer verilecektir.
[320] **Gürpınar**, s. 691.
[321] **Yavuz**, Türk Borçlar Kanunu Tasarısı'na Göre 'Kusursuz Sorumluluk' Halleri ve İlkeleri, MÜHF-HAD, C.14, S.4, 2008, s. 43.
[322] Kusur sorumluluğunun kural kusursuz sorumluluğun da istisna olduğu hukukumuzda genel kabul edilen görüştür. TBK m. 66 hükmünde adam çalıştıranın sorumluluğu kusursuz sorumluluk hali olarak açıkça düzenlenmiş olup kanun koyucunun kusursuz sorumluluk gibi şartları ağır bir sorumluluk türünü oluşturmak istediği takdirde bunu açık biçimde yapmasını beklemek uygun olacaktır. Ayrıca TBK m. 56 ve m. 58 hükümlerinde "kusur" kelimesi geçmemektedir. Ancak bu hükümlerin uygulanması esnasında kusur aranmaktadır.
[323] **Gürpınar**, s. 692.

Somut bir örnek ile açıklamak gerekirse kişinin kimlik bilgilerinin veri sorumlusunun kusuru olmaksızın ifşa olunması durumunda doğrudan bir zarar oluşmayacaktır. Ancak burada ifşa edilen bilgiler kullanılarak ilgili kişi adına bir kimlik düzenlenir ve bu kimlikle kredi kullanılırsa bir maddi zarardan bahsedilebilir. Bir diğer örnek ise kişinin e posta adresi ve şifresinin ifşa edilmesi durumunda bu e postaya erişim sağlanarak üçüncü kişilere hakaret edilirse bu eylem sebebiyle ilgili kişiye uygulanacak adli para cezası bir zarar olarak değerlendirilebilir.

TBK m. 71'e dayanarak veri sorumlularının tehlike sorumluluğu bulunduğunu iddia etmek üçüncü kişinin sorumluluğu olmaksızın bir zarar doğmaması nedeniyle işlevsel olmayacaktır. Bu nedenle eğer tehlike sorumluluğuna gidilecekse özel bir düzenlemeye ihtiyaç duyulacaktır. Yapılacak olası bir düzenlemenin işlevsel olabilmesi için üçüncü kişinin ağır kusurunun nedensellik bağını kesmediğini açıkça belirtilmelidir.[324]

Bu noktada Kurul kararlarından hareketle Tüzük'te düzenlenen "*kabul edilen tasarımdan itibaren ve başlangıçtan itibaren veri koruma*" ilkesinin KVKK'ya eklenmesi gerektiği belirtilmektedir.[325] Birinci bölümde değindiğimiz bu iki veri koruma yöntemi KVKK'da açıkça düzenlenmediği gibi ikincil mevzuatla da buna yönelik bir kural getirilmemiştir.

Ancak Kurul'un verdiği bir karardan hareketle içtihat olarak risk sorumluluğunun benimsendiği ifade edilmiştir.[326] İlgili kararda[327] yer alan sistemsel veya yönetimsel hata ifadesine dayanarak bir risk sorumluluğuna işaret edildiği ifade edilmektedir. Risk sorumluluğu olarak isimlendirilen bu görüşe göre veri sorumlusuna, veri güvenliğine ve muhafazasına ilişkin yükümlülük getiren KVKK m. 12 hükmü sorumluluğunun dayanağını oluşturmaktadır. Bu noktada risk sorumluluğu kavramı ve tehlike sorumluluğu ile ilişkisine de değinmek uygun olacaktır.

---

[324] **Gürpınar**, s. 694.
[325] **Çekin**, Büyük Veri, s. 642.
[326] **Dülger**, Risk Sorumluluğu, s. 5.
[327] Kurul'un 26/07/2018 tarih ve 2018/91 sayılı veri sorumlusunun kişisel verilere hukuka aykırı biçimde erişilmesini önleme yükümlülüğünü yerine getirmemesi konulu kararı.

Risk sorumluluğu esasında idarenin sorumluluğunu genişletmek maksadıyla içtihat ile ortaya konan ve kamu hukuku alanında kullanılan bir sorumluluk türüdür. İdarenin her türlü tedbiri alsa dahi yine de zarar doğruma ihtimali olan hizmetlerin yüksek risk barındırdığı kabul edilmektedir.[328] Risk sorumluluğu, bu gibi hizmetlerden doğan zararla illiyet bağı mevcutsa ayrıca kusuru aramadan idarenin sorumluluğuna gitmeyi sağlamaktadır.[329]Risk sorumluluğunun temelinde yatan sebebin tehlike sorumluluğu olduğu kabul edilmektedir.[330]

Ancak risk sorumluluğu teşhisi yapabilmek için yalnızca Kurul kararında veri sorumlusunun yükümlülüklerinin geniş yorumlanmasının yeterli olmayacağı düşüncesindeyiz. Bu noktada tehlike sorumluluğu veya risk sorumluluğu hususunun söz konusu olmayacağını kabul ettikten sonra olağan sebep sorumluluğu olup olmadığı hususunu açıklamak uygun olacaktır.

Özen sorumluluğundan bahsedebilmek için bir kanun hükmüyle getirilmiş bir özen yükümlülüğüne ihtiyaç olduğu kabul edilmektedir. Bu kusursuz sorumluluk türünde kişi özen yükümlülüğünü yerine getirdiğini veya getirse de yine zararın doğacağını ispatlamakla yükümlüdür.[331]Bu sebeplerle veri sorumlusunun, KVKK m. 12 ile getirilen yükümlülüklere tabi olmasının kusursuz sorumluluktaki özen yükümlülüğüne denk geldiğini ifade eden görüşler mevcuttur.[332]

Bu görüşe destek olarak Kurul'un veri işleme ilkelerinden bir tanesi hakkında aldığı kararlar da veri sorumlusuna özen yükümlülüğüne benzer yükümlülükler getirmektedir. İkinci bölümde değindiğimiz üzere verilerin doğru ve güncel olması konusunda Kurul veri sorumlusundan aktif bir çaba beklediğini izah etmiştir. Yine kusursuz sorumluluk olduğunu savunanların bir diğer argümanı ise 95/46/AT sayılı Direktif'de yer alan veri sorumlusunun sorumluluğuna ilişkin düzenlemenin[333] kusursuz sorumluluğa işaret ettiğidir. İlgili hükümde veri

---

[328] Örneğin hızlı tren seferleri, uçuşlar, nükleer santraller gibi hizmetlerde idarenin risk sorumluluğuna gidilebilmektedir. AYİM 2. Dairesinin E.1995/532, K.1996/9 T. 10.01.1996 kararı.
[329] **Köksal**, Mustafa: "Risk İlkesinin İdareye Yüklediği Külfetler ve Güncel Yargı Kararları", TBB Dergisi, S. 85, 2009, s. 264.
[330] **Uzunkaya**, Mehmet Celal/**Avcı**, Mustafa: "Tehlike Sorumluluğunun Genelleşmesine Yönelik Düzenleme Tercihi", Antalya Bilim Üniversitesi Hukuk Fakültesi Dergisi, C.3 S.5, 2015, 41; **Günday**, Metin: İdare Hukuku, İmaj Yayıncılık, Ankara 2003, s. 330.
[331] **Oğuzman**/**Öz**, s. 139; Eren, Borçlar Hukuku Genel Hükümler, s. 705, **Kılıçoğlu**, Borçlar Genel, s. 203; **Antalya**, Borçlar Genel, s. 247
[332] **Zor**, s. 149; **Çekin**, Kişisel Veri, s. 146.
[333] İlgili Direktifin 23. maddesinde düzenlenmiştir.

sorumlusunun, zarara yol açan veri işlemeden sorumlu olmadığını kanıtlayarak tazminat ödemekten kaçınabileceği ifade edilmektedir.[334]

Ancak ilgili düzenlemelerin lafzından ve düzenlemelerin kapsamında anlaşılan bu sorumluluğun bir kusursuz sorumluk olmadığı kusur karinesine dayanan bir kusur sorumluğu olduğu anlaşılmaktadır. Ayrıca hukukumuzda kusur sorumluluğu esası benimsemiş olup kusursuz sorumluluk istisnadır.[335] Literatürdeki görüşlerin incelenmesi sonucunda oluşan kanaatimiz ise kusursuz sorumluluk olması için açık bir düzenlemenin varlığının gerektiği ve KVKK'da bu yönde bir açık düzenleme olmadığı için kusursuz sorumluluğa gidilemeyeceği yönündedir.[336]

3.3. KİŞİSEL VERİLERİN KORUNMASI YÜKÜMLÜLÜĞÜNÜN İHLALİ DURUMUNDA BAŞVURULACAK HUKUKİ YOLLAR

3.3.1. Tazminat Davaları

Kişilik haklarına saldırıda bulunulan kişiler saldırı sonucunda zararının giderilmesi veya eski hale getirilmesi amacıyla tazminat davası açabilir.[337] Kişisel verileri sözleşme ilişkisine dayanarak işlenen kişiler sözleşmeye aykırılık sebebiyle tazminat davası açabilmektedir. Ayrıca verileri tamamıyla rızası dışında işlenen kişiler de tazminat davası açabilir.

Verilerinin hukuksuz biçimde işlenmesi nedeniyle açılacak tazminat davasında özel kanun olarak ilk bakılacak mevzuat KVKK'dır. KVKK'nın m. 11/ğ ve 14 hükümleri genel hükümlere atıf yapmaktadır. Bu durumda tazminat davasının dayanağı TMK m. 23,24,25 ve TBK hükümleri olacaktır.

Tazminata ilişkin olarak Kurum'un herhangi bir yetkisinin olmadığı Kurulun 16/01/2020 tarihli ve 2020/41 sayılı kararı ile netleşmiştir. Kuruma 100 bin TL maddi tazminat talebiyle başvuran kişinin talebi KVKK m. 11 ve 14/3 hükümlerine dayanılarak reddedilmiş ve genel mahkemelerin görevli olduğu ifade edilmiştir.

---

[334] KVKK m. 11, 95/46/AT m. 23 ve Tüzük m. 82 hükümlerinde veri sorumlusuna ilişkin tazminat hususunda kusur kelimesine yer verilmemiştir.
[335] **Günay**, Cevdet İlhan: Borçlar Hukuku Genel Hükümler – Özel Borç İlişkileri, Yetkin Yayınları, Ankara 2016, s. 83.
[336] **Vuraloğlu**, s. 199; **Taştan**, s. 69.
[337] **Hatemi**/**Gökyayla**: s. 167; **Eren**, 873; **Tandoğan**, Mes'uliyet, s. 255; **Kılıçoğlu**, Basın Yoluyla Saldırı, s. 382.

3.3.1.1. Maddi Tazminat Davası

Kişinin rızası dışında mal varlığının aktiflerindeki azalma veya pasiflerindeki artış maddi zarar olarak ifade edilmektedir. İlgili zararın kişinin malvarlığının parasal olarak ölçülebilir kısmında olması gerekmektedir.

Tazminat davası talep edilen tazminat türüne göre maddi zarar ve manevi zarar olarak ikiye ayrılmaktadır. Bu kapsamda öncelikle maddi zarara ilişkin talepler incelenecektir.

Maddi tazminat davasında kusurun ve zararın ispatı gerekmektedir. Maddi zarar malvarlığının parayla ölçülebilen bölümündeki aktiflerin azalması veya pasiflerin artması şeklinde ortaya çıkabilir. Dava kapsamında kişisel verileri haksız işlenen kişi bu işlemden dolayı doğan maddi zararını ve veri işleyenin kusurlu olduğunu ispatlaması gerekir.

Maddi tazminat davasının TMK m. 25'de düzenlenen davalarla birlikte açılması da mümkündür. Saldırının tespiti, saldırıya son verilmesi, kazancın iadesi, mahkeme kararının yayınlanması ve manevi tazminat davaları maddi tazminat ile birlikte açılabilir. Diğer taraftan saldırının önlenmesi davası ve maddi tazminat davası saldırının önlenebileceği aşamada henüz saldırı kaynaklı bir zarar doğmadığı için birlikte açılamayacaktır.

Maddi tazminat talepli davayı incelerken dava taraflarını inceleyerek başlamak uygun olacaktır. Hukuka aykırı biçimde kişisel verilerin işlenmesinden kaynaklanan maddi tazminat davasında kişisel verisi işlenen ilgili kişi davacı tarafıdır.[338]

Kişisel verisi işlenen gerçek kişi, küçük veya ayırt etme gücünden yoksunsa yasal temsilcisi maddi tazminat davası açabilecektir. Birden fazla kişinin verisi aynı veri işleme faaliyeti kapsamında işlense dahi toplu dava benzeri bir uygulama hukukumuzda kabul edilmediği için her bir ilgili kişi ayrı ayrı dava açmalıdır.

Maddi tazminat davasında davalı hukuka aykırı biçimde kişisel veri işleyen gerçek veya tüzel kişidir. Eğer tarafların arasında bir sözleşme ilişkisi mevcutsa ve bu kapsamda veri işleme faaliyeti devam ediyorsa davalı veri sorumlusu olacaktır. Sözleşme ilişkisi kapsamında kişisel veri işleyen veri sorumlusu

[338] **Oğuzman/Seliçi/Özdemir**, Kişiler Hukuku, s. 227.

sözleşmeye aykırı biçimde veri işlemişse KVKK m. 11 hükmü kapsamında maddi tazminat ödemek zorunda kalabilir.[339] Daha açık bir ifadeyle ilgili kişi zararı ispatladığında kusuru ayrıca ispatlamak zorunda kalmadan maddi tazminat talebinde bulunabilecek veri sorumlusu ise kusurlu olmadığını ispatlamak durumda kalacaktır.

Birden fazla veri sorumlusunun mevcudiyeti durumunda TBK m. 61'de düzenlenen müteselsil sorumluluk hükümleri uygulama alanı bulacaktır. Aynı zamanda bir taraf veri işleyen diğeri veri sorumlusu ise KVKK m. 12 hükmü uygulama alanı bulacak olup yine müteselsil sorumluluk uygulanacaktır.[340]

Maddi tazminata hükmedilebilmesi için belirli şartlar aranmaktadır. Bu şartlar hukuka aykırı bir fiil, bu fiil sonucu doğan bir zarar ve bu ikisi arasında bir illiyet bağı olması gerekmektedir.[341] Bu unsurlar arasında tespiti en zoru maddi zararın kapsamı ve miktarıdır. Kişisel veri ihlalinin mağduru olan ilgili kişi maddi zararını ispatlamak zorundadır.

Maddi tazminatın kapsamının belirlenmesi ise TBK m. 51 hükmünde düzenlenmiştir. Buna göre hakim durumun gereğine ve kusurun ağırlığına göre tazminatın kapsamını ve ödeme yöntemini belirleyecektir. Ancak Türk hukukunda kabul edilen telafi edici görüş sebebiyle[342] hakim bu tazminat miktarını belirlerken zarar miktarını aşamaz.[343]

Kişisel veri ihlallerinden doğan tazminat kişilik haklarına ilişkin olup ilişkin olup maddi olarak değer biçilmesi kolay değildir. Günümüzde verinin ekonomik bir değeri olduğunu iddia etmek elbette mümkündür ancak veri ihlali sebebiyle doğrudan bir zarar oluşsa dahi bu zararı hesaplamak kolay olmayacaktır. Ayrıca kişisel veri ihlali nedeniyle doğrudan zarar ortaya çıkması olası görünmemektedir.[344]

---

[339] **Özer Deniz**, s. 280.
[340] **Tepe**, Esra; Özel Hukuk Açısından Avrupa İnsan Hakları Mahkemesi İçtihatları Işığında Kişisel Verilerin Korunması, Adalet, Ankara 2021, s. 78.
[341] **Eren**, s. 540, **Kılıçoğlu**, Medeni Hukuk, s. 401, **Tandoğan**, Mesuliyet Hukuku, s. 76.
[342] Tazminatın üst sınırı konusunda temelde iki görüş mevcuttur. Bunlardan ilki cezalandırıcı ikincisi ise telefi edici yaklaşımdır. Hukukumuzda ağırlıkla telafi edici yaklaşım kabul edilmekle birlikte 4054 sayılı Rekabetin Korunması Hakkında Kanun'un m. 58 hükmüne göre rekabet ihlallerinden doğan zararın üç katına kadar tazminata hükmedilmesi mümkündür.
[343] Yargıtay HGK. 17.03.2010, E. 2010/4.130, K. 2010/161. **Eren**, s. 214.
[344] **Özer Deniz**, s. 281.

Kişisel veri işleme faaliyeti nedeniyle kural olarak doğrudan bir zarar ortaya çıkmamakta dolaylı zarar doğma ihtimali ortaya çıkmaktadır. Örneğin kişinin, kişisel verilerinin işlenmesi sonucu işverenin iş sözleşmesini fesh etmesi buna örnek gösterilebilir. Eğer işlenen veri özel nitelikli kişisel veriyse maddi zararın miktarı artacaktır.[345]Aynı örnek üzerinden ilerleyecek olursak işçinin dini inancının işlenmesinden doğan tazminat miktarı diğer kişisel verilerin işlenmesine göre daha yüksek olacaktır.[346]

Özel nitelikli kişisel verilerin öğrenilmesi kişinin ayrımcılığa uğranılması açısından daha elverişlidir. Kişinin hastalıkları, suç geçmişi, siyasi görüşü, etnik kökeni gibi bilgilerin öğrenilmesi kişiye önyargı beslenmesi, bir grupla ilişkilendirilmesi veya sosyal açıdan tecrit edilmesi gibi olasılıkları artırmaktadır. Diğer kişisel veriler açısından bu tip risk yüksek görünmemektedir. Örneğin kişiye ait iletişim bilgilerinin işlenmesi benzeri bir riski yaratmayacaktır.

Burada iki hususu ve bu iki husus arasındaki ayrımı belirtmek uygun olacaktır. Bunlardan birincisi zararın denkleştirilmesi ikincisi ise tazminatın indirilmesidir.

Haksız fiil oluşturan bir kişisel veri ihlalinden doğan zarar miktarı belirlenirken bu fiilden kaynaklı elde edilen gelirler düşülür. Burada amaçlanan zarar görenin brüt zararından aynı olay sebebiyle elde ettiği faydaları düşerek net zararını tespit etmektir. Aksi takdirde tazminatın bir zenginleşme aracı olması söz konusu olacaktır ki bu yukarıda bahsettiğimiz üzere hukuka aykırıdır.

Zararın denkleştirilmesi için kümülatif olarak birden fazla şartın aynı anda gerçekleşmesi beklenmektedir. Bu şartlar zarar gören kişinin zararı doğuran olaydan maddi bir menfaat elde etmesi, zararı doğuran olay ve maddi menfaat arasında illiyet bağı olması ve taraf iradelerinin denkleştirme doğrultusunda olmasıdır.

Karşılıksız kazandırmaların zararın denkleştirilmesinde hesaba katılmayacağı TBK m. 55/1 hükmünden anlaşılırken karşılık arz eden kazanımlar hesaba katılacaktır. Örnek vererek somutlaştırmak gerekirse ses yarışmasına katılan ve daha evvel suç işlediği ve cezasını çektiği öğrenilen bir sanatçı bu nedenle yarışmayı kazandığı halde elenerek para ödülü verilmiyor. Ancak toplum

[345] **Özdemir**, Kişisel Veri, s. 209.
[346] **Özer Deniz**, s. 281.

sanatçıyı aynı sebepten destekliyor ve bağış toplamaya başlıyor. Diğer taraftan yine aynı sebeplerle daha fazla organizasyon ve konserde sahne aldığı için gelirlerinde de bir artış gerçekleşiyor.

Mevcut örnekte yarışma sonunda ödenmesi beklenen miktar brüt zarar olarak değerlendirilecek bu miktardan işlerinden kazandığı gelirinin artması nedeniyle elde ettiği miktar düşülüp net zarar elde edilecektir. Ancak sanatçı için toplanan bağışlar karşılıksız kazandırma olarak değerlendirilecek olup zarar denkleştirmesi kapsamında göz önüne alınmayacaktır.

Zararın denkleştirilmesi net zararın hesabıyla ilgili bir konudur. Ancak net zarar her zaman tazminat miktarıyla birebir uyuşmamaktadır. Tazminat belirlenirken net zarar miktarı üzerinden şartları mevcutsa indirim uygulanabilir. Dolayısıyla zarar miktarı yalnızca tazminatın üst sınırının tespiti açısından önemlidir. Üst sınır belirlendikten sonra hakkaniyet gereği bazı indirimlerin yapılması gerekmektedir. Bu indirim sebepleri TBK m. 51 ve TBK 52 hükümlerinde düzenlenmiştir.

Zarar gören kişisel veri özelinde ilgili kişi fiile rıza göstermişse, zararın doğmasında, artmasında etkisi varsa veya tazminat yükümlüsünün durumun ağırlaşmasına sebep olmuşsa hakimin tazminatı indirme veya tamamıyla kaldırma yetkisi vardır.[347] Ayrıca hâkimin, hafif kusuruyla zararın doğmasına yol açan tazminat yükümlüsünün yoksulluğa düşecek olması ve hakkaniyetin gerektirmesi durumunda tazminatı indirme yetkisi mevcuttur.[348]

TBK m. 51 hükmünde kusurun ağırlığının tazminatın belirlenmesinde esas alınacağı düzenlenmiştir. İlgili hüküm çerçevesinde kusurun ağırlığı takdiri bir indirim sebebi olarak değerlendirilmektedir.[349]Zarar verenin hafif kusurlu olması ve ağır kusurlu olması arasında tazminat hukuku açısından fark oluşması mümkündür. Somut olayda hakim öncelikle kusurun ağırlığını tespit edip akabinde tazminat sorumluluğunun kapsamını tespit edecektir. Dolayısıyla gerek gördüğü takdirde hafif kusurlu olan zarar verenin tazminatında indirime karar verebilir. Ortaya çıkan zarara kıyasla kusurun çok hafif olması durumunda hakim takdir yetkisini kullanabilir.

---

[347] TBK m. 52/1 hükmünde açıkça düzenlenmiştir.
[348] TBK m. 52/2 hükmünde açıkça düzenlenmiştir.
[349] TBK m. 114 hükmü gereği sözleşmesel sorumlulukta herhangi bir indirim söz konusu olmayacaktır. Borçlu tüm kusurundan sorumludur.

Dürüstlük kuralı kapsamında kişi kusuruyla doğmasına veya artmasına sebep olduğu zararın bir kısmına da olsa katlanmalıdır. Kişisel veri hukuku ile sorumlu olmaksızın kabul gören görüş tazminat takdirinde zarar görenin kusuru olması durumunda tazminat sorumluluğunun zarar veren ve zarar gören arasında bölüştürülmelidir.[350]

Zarar görenin kusurlu olup olmadığı dikkate alınırken objektifleştirilmiş kusur kavramı temel alınacaktır.[351] Dürüstlük kuralı kapsamında zarar görenden uğradığı zararı azaltacak veya daha fazla zarara uğramasını engelleyecek tedbirler alması beklenmektedir.[352] Bu kapsamda objektifleştirilmiş kusur kavramı esas alındığından dürüst ve makul bir insandan beklenen dikkat ve özenin gösterilmemesi durumunda zararın paylaşılması gerekmektedir.[353]

Objektifleştirilmiş kusur sorumluluğunun uygulanabilmesi için ayırt etme gücünün bulunması gerekmektedir. Ayırt etme gücünden yoksun birine kusur atfedilmesi mümkün değildir. Taraf fark etmeksizin zarar verenin de zarar görenin de kusuru tespit edilirken objektifleştirilmiş kusur sorumluluğu kriterleri uygulanacaktır. İlgili kriterler somut olayda kişinin yaşı, mesleki bilgisi, teknik konulara hakimiyeti, sosyal becerileri dikkate alınarak belirlenecektir.

Yukarıda açıklanan bilgileri kişisel veri hukuku özelinde örneklemek gerekirse ilgili kişinin ver ihlalinden doğan zararı azaltmak veya artmasını engellemek gibi bir yükümlülüğü mevcuttur. İlgili kişinin güçlü şifre belirleme, lisanslı yazılım kullanma, şifrelerini başkalarıyla paylaşmama gibi temel teknik tedbirleri almasının beklenmesi olağandır. Bu yönde gelişen bir somut olayda ilgili kişinin de sorumlu olduğu düşünülerek tazminat sorumluluğunun kusura orantılı bölüşülmesi uygun olacaktır.

Tazminattan bir diğer indirim sebebi ise zarar görenin rızasıdır. Zarar görenin rızası, rızanın verildiği zamana göre ikiye ayrılır. İlki zararı doğuran olaydan evvel verilen rızadır. Hukuka uygunluk sebebi olarak değerlendirilir ve tazminattan indirim sebebi oluşturmaz. İkincisi ise Yargıtay içtihadına göre zarar doğuran

---

[350] Yargıtay HGK T: 13.05.2015 E. 2013/2206 K. 2015/1324. **Gönül Koşar**, Günhan: Haksız Fiil Sorumluluğunda Kusur ve Etkisi, XII Levha Yayınları, İstanbul 2020, s. 214.
[351] **Gönül Koşar**, s. 79.
[352] **Eren**, s. 881, **Nomer**, s. 122.
[353] **Baysal**, Başak: Zarar Görenin Kusuru, XII Levha Yayınları, İstanbul 2012, s. 34.

olayın ardından verilen rızadır.[354] Zararı doğuran olayın ardından verilen rıza, tazminattan indirim sebebi veya zararın boyutuna göre tazminatı ortadan kaldıran sebep olarak değerlendirilir.[355]

Somut bir örnek vermek gerekirse kişisel veri politikası ve veri güvenliği açısından problemli olduğunu bilmesine rağmen bir sosyal medya platformuna kayıt olan kullanıcının ortak kusurlu olarak değerlendirilerek tazminattan indirim uygulanabilir.

Tazminattan indirim sebebi olarak değerlendirilebilecek bir diğer husus ise zarar veren ve zarar gören harici birinin kusuru ile zarara sebep olmasıdır. Üçüncü kişinin kusuru illiyet bağını kesecek kadar fazlaysa zarar verenin sorumluluğu kalkacaktır. Diğer taraftan üçüncü kişinin kusuru illiyet bağını koparacak boyutta değilse dahi tazminattan indirim sebebi olarak değerlendirilecektir.

Veri koruma hukuku alanında üçüncü kişinin kusur denilince ilk akla gelen siber saldırı sonucu ortaya çıkan veri sızıntılarıdır. Veri sorumlularının veri güvenliğini sağlamaya ilişkin yükümlülükleri olduğu ve bu yükümlülükleri yerine getirebilmek için yapması gerekenleri daha evvel açıklamıştık. Ancak siber saldırı sonucu veri ihlali ortaya çıkması durumunda saldırıyı yapan kişi üçüncü kişi, saldırı ise üçüncü kişinin kusuru olarak değerlendirilecektir.

Üçüncü kişinin kusuru veri koruma hukuku kapsamında illiyet bağını koparan bir unsur olarak kabul edilmemektedir. Ayrıca tazminat sorumluluğunu kaldıran veya azaltan bir sebep olarak değerlendirilmediği görülmektedir. Nitekim Kurum kararları incelendiğinde Clickbus Seyahat Hizmetleri AŞ kararında üçüncü kişi tarafından yapılan siber saldırının sonucunda kaynak koduna erişebildiği tespit edilmiş olup bu durumun veri sorumlusu şirketin veri güvenliğine ilişkin yükümlülüklerini yerine getirmemesinden kaynaklandığı gerekçesiyle idari para cezası uygulandığı anlaşılmaktadır.

Kurum siber saldırıları engelleme konusunda veri sorumlusunun yükümlülüğünü ağır biçimde uygulamakta ve siber saldırıları engelleme yükünün veri

---

[354] Yargıtay HGK E. 2003/4-161, K. 2003/201,T: 26.03.2003. **Kılıçoğlu**, Ahmet: Medeni Hukuk, Turhan Kitabevi, Ankara 2016, s. 411.
[355] **Eren**, Borçlar Genel, s. 787, **Özdemir**, s. 217.

sorumlusunda olduğu konusunda görüşü netleşmektedir. Bu durumun tazminat sorumluluğu açısında da aynı doğrultuda yorumlanması uygun olacaktır.[356]

3.3.1.2. Manevi Tazminat Davası

Kişilik haklarına yönelen bir saldırı sonucu kişinin hissettiği üzüntü, elem ve ızdırap manevi zarar olarak adlandırılmaktadır.[357] Kişilik hakkı ihlallerinden doğan manevi tazminat TMK 25/3 ve TBK 58/1 hükümlerinde düzenlenmiştir. Manevi tazminat talebinin amacı, kişilik hakkının ihlâli edilmesi sonucu hissedilen ızdırabın hafifletilmesi veya tamamıyla giderilmesidir. Manevi tazminatın zara görende huzuru doğurmayı sağlayacak bir işlevi olmalıdır.[358]

Manevi tazminat davasını, kişisel veri ihlalinin mağduru kişi açabilir. Eğer mağdur küçük veya kısıtlı olmakla birlikte ayırt etme gücüne sahip olduğu anlaşılıyorsa yasal temsilcisinin izni gerekmeksizin manevi tazminat davası açabilmektedir. TMK 25/4 hükmü gereği manevî tazminat talepleri, davanın karşı tarafı kabul etmedikçe devredilemez; sağken mirasbırakan tarafından talep edilmemişse mirasçılara geçmesi mümkün değildir.

Manevi zarar ve maddi zarar aynı olayda ortaya çıkabilir. Örnek vererek somutlaştırmak gerekirse kişinin eskiden suç işlediğine dair bir bilginin varlığı aynı olayda hem işinden olmasına hem de sosyal çevresini kaybetmesine yol açabilir. Bu örnekte kişi çalışamaması nedeniyle maddi zarara uğrarken sosyal açıdan dışlanması nedeniyle de manevi zarara uğrayacaktır. Kişi her iki zararı da talep edebilir ancak manevi zararın tespiti maddi zarar kadar kolay olmayacaktır.

Türk hukukunda cezalandırıcı değil telafi edici tazminat anlayışının hakim olduğunu belirtmiştik. Bu nedenle manevi tazminattan beklenen kişinin hissettiği üzüntü ve ızdırabı gidermesidir. Manevi zararın tam olarak belirlenebilmesi için kişinin yaşadığı üzüntüye ve ızdıraba maddi olarak değer biçilmesi gerekmektedir ki bu imkânsızdır. Dolayısıyla aslında manevi zarar tamı tamına hesaplanabilir bir şey değildir.

Ancak kişinin duyduğu elem ve üzüntünün telafi edilebilmesi maksadıyla belirli kriterler değerlendirilerek manevi zarar tespit edilmeye çalışılmaktadır. Bu tespit

---

[356] **Özer Deniz**, s. 293.
[357] Manevi zarara ilişkin görüşlere “zarar” başlığı altında değinilmiştir.
[358] **Günay**, s. 83.

yapılırken objektif ve somut bir sistem mevut değildir. Hakim her bir somut olayda hakkaniyete ve hukuka uygun biçimde tarafların sosyal ve ekonomik durumunu değerlendirecektir.

Her bir olayda somut olayın gerçekleşme biçimi, zarar doğuran olayın niteliği, mağdurun kişiliği, ülkenin ekonomik koşulları[359], mağdurun uğradığı zarar, mağdurun yaşı[360], manevi zararın ortadan kalkabilme durumu, zarar doğuran olayın devam ettiği süre, çalışma hayatına etkisi, zarar doğuran olayın öğrenilme hızı göz önüne alınarak hakkaniyete göre karar verilecektir[361]. Bu kriterler[362] yalnızca örnekleme yoluyla sayılmış olup sınırlı sayıda değildir.

Aynı olay karşısında iki kişinin hissedeceği elem ve üzüntü birebir aynı değildir. Dolayısıyla hakim somut olayda aynı olaydan mağdur olan kişiler için yukarıda yer verilen kriterlere göre bir birinden farklı miktarlarda tazminat ödenmesine karar verebilir. Hakim somut olayda manevi tazminata hükmederken emsal kararları dikkate almalı ve tarafların durumlarını göz önüne alarak karar vermelidir.

Hakim belirlediği manevi tazminat tutarını ve bu tutara ulaşırken yaptığı değerlendirmelerini gerekçelendirmelidir.[363] Miktarın belirlediği miktardan daha az veya fazla olmama sebebini de gerekçelendirmesi ve sağlıklı bir temele dayandırması hukuken daha sağlıklı olacaktır.[364]

Manevi tazminatın tam ve doğru biçimde tespiti için TBK m. 51-52 hükümlerinde yer alan indirim sebeplerinin de uygulanması gerekmektedir. Maddi tazminattan indirim sebepleri başlığında açıklanan zararın ağırlığı, zarar verenin ortak kusuru, zarar görenin rızası, zarar görenin ekonomik durumu, zarar verenin tazminat

---

[359] Yargıtay 21. HD E. 2015/20412 K. 2016/847 T. 01.02.2016, Yargıtay'ın 22.06.1966 gün 1966/7-7 sayılı İçtihadı Birleştirme Kararı.
[360] Yargıtay 17. HD E. 2015/3753 K. 2017/9582 T. 25.10.2017 "…olay tarihi, olayın meydana geliş şekli, mağdurun yaşı ve tarafların kusur durumu dikkate alındığında…"
[361] **Antalya**, Borçlar Genel, s. 177.
[362] Yargıtay HGK E. 2017/4-1340 K. 2018/1622 T. 6.11.2018 kararında manevi tazminata ilişkin kriterler sayılmıştır. "*Yargıç, manevi tazminatın tutarını belirlerken, saldırı oluşturan eylem ve olayın özelliği yanında tarafların kusur oranını, sıfatını, işgal ettikleri makamı ve diğer sosyal ve ekonomik durumlarını da dikkate almalıdır. Tutarın belirlenmesinde her olaya göre değişebilecek özel durum ve koşulların bulunacağı da gözetilerek takdir hakkını etkileyecek nedenleri karar yerinde nesnel (objektif) olarak göstermelidir."*
[363] Yargıtay 4. HD E. 2020/3757 K. 2022/978 T. 26.1.2022.
[364] **Özer Deniz**, s. 308.

sonrası yoksulluğa düşecek olması, beklenmedik olaylar ve üçüncü kişilerin sorumluluğa etkisi dikkate alınmalıdır.[365]

3.3.2. Kişisel Verilerin Korunması Yükümlülüğünün İhlalinde Başvurulabilecek Diğer Hukuki Yollar

Tazminat davaları haricinde başlama tehlikesi olan saldırıyı önleme, devam eden saldırıyı durdurma veya etkileri süren saldırıyı tespit amaçlı davaları da mevcuttur. Koruyucu davalar olarak isimlendirilen bu davaların açılması için kusur ve zarar şartları aranmamakta olup yalnızca hukuka aykırı bir saldırı olması yeterlidir.[366]

TMK'da koruyucu davalar ile ilgili bir zamanaşımı süresi düzenlenmemiştir. Ancak davaların amacı itibariyle açılabilecekleri süreler sınırlıdır. Aksi takdirde davadan elde edilmesi beklenen faydanın elde edilmesi imkânsız hale gelecektir. Daha açık bir ifadeyle saldırı tehlikesinin önlenmesi davası, saldırı olacağına dair ciddi ve yakın tehlike devam diyorsa; saldırıya son verme davası, hukuka aykırı saldırı devam ediyorsa; tespit davası ise, hukuka aykırı saldırının etkileri devam ediyorsa açılabilir.[367]

Kişisel verilerin korunması hukuku açısından bakacak olursak davacı kişisel verisi işlenen veya işlenme tehdidi altındaki gerçek kişidir. Davalı konumda ise veri sorumlusu ve varsa veri sorumlusundan aldığı yetkiye dayanarak hareket eden veri işleyen olacaktır. Koruyucu davalar için 6100 sayılı Hukuk Muhakemeleri Kanunu'nda (HMK) düzenlenen genel yetki kuralı haricinde TMK 25/5'te bir hüküm bulunmaktadır. Dolayısıyla, verisi hukuka aykırı biçimde işlenen kişi kendi yerleşim yerinde veya davalının yerleşim yerinde bahsi geçen davaları açabilmektedir.

Ancak TMK m. 25/5'te yer verilen hükmün kesin yetki kurallarından olmadığı dikkate alınmalıdır. Dolayısıyla kişilik haklarına yönelen saldırının sözleşmeden kaynaklanması durumunda HMK m. 10 hükmü kapsamında ifa yerinin olduğu yer mahkemesinde de açılabilir. Ayrıca davanın haksız fiilden kaynaklanması durumunda HMK m. 16 kapsamında haksız fiilin gerçekleştiği yahut zararın

---

[365] **Atlan**, Hülya: Manevi Zararı Tazmin Yolları, XII Levha Yayınları, İstanbul 2015, s. 209, **Eren**, s. 818.
[366] **Helvacı**, Koruyucu davalar, s. 86, **Kılıçoğlu**, Medeni Hukuk, s. 368.
[367] **Oğuzman/Seliçi/Oktay/Özdemir**, Kişiler Hukuku, s. 255.

oluştuğu ya da oluşma ihtimalinin bulunduğu yer mahkemeleri de yetkilidir. Görevli mahkeme açısından bakıldığında ise HMK m. 2/1 hükmü gereği şahıs varlığına ilişkin davalarda asliye hukuk mahkemesi görevlidir. Koruyucu davaların da şahıs varlığına ilişkin olması nedeniyle asliye hukuk görevli mahkemedir.[368]

Veri sorumlusunun kamu tüzel kişiliği olması durumda ise görevli ve yetkili mahkemeye ilişkin değerlendirmeler HMK hükümlerine göre değil İYUK hükümlerine göre yapılacaktır. Kamu kurumları tarafından yapılan hukuka aykırı veri işleme faaliyetlerine karşı iptal ve tam yargı davaları açılabilecek olup görevli mahkeme genel görevli mahkeme olan idare mahkemesidir. [369] İYUK m. 32/1 hükmü gereği yetkili idare mahkemesi kişisel veri sorumlusu kamu kurumunun bulunduğu yer idare mahkemesidir.

3.3.2.1. Saldırının Önlenmesi Davası

TMK m. 25/1'de düzenlenen saldırının önlenmesi veya saldırı tehlikesinin önlenmesi davasının şartları hukuk aykırı bir saldırı tehlikesinin olması ve bu saldırı tehlikesinin ciddi ve yakın olması gerekmektedir. Eğer saldırı başlamış ve hali hazırda devam ediyorsa veya tamamlanmışsa saldırının önlenmesi davasının konusunu oluşturmayacaktır.[370]

Diğer koruyucu davalar da olduğu gibi saldırının önlenmesi davasının açılabilmesi için de kusur ve zarar şartı aranmamakta olup hukuka aykırılık yeterlidir. Kişisel verilerin korunması hukuku kapsamında baktığımızda ise hukuka aykırı biçimde kişisel veri işlemeye yönelik ciddi ve yakın bir tehdit yeterli olacaktır.

Koruyucu davalar sonucunda tazminata hükmedilemeyeceğini daha evvel belirtmiştik. Dolayısıyla önleme davası sonucunda da veri sorumlusuna yönelik somut bir davranışta bulunmayı yasaklama şeklinde bir hüküm kurulması beklenmelidir.

---

[368] **Badur**, Emel/**Kurt Konca,** Nesibe: "Kişisel Verilerin Hukuka Aykırı İşlenmesinden Doğan Zararların Tazmini Ve Görevli Mahkeme", İnönü Üniversitesi Hukuk Fakültesi, C. 13 S. 2, s. 486.
[369] **Badur/ Kurt Konca**, s. 485.
[370] **Kılıçoğlu**: Medeni Hukuk, s. 374; **Serozan**, 476; **Tandoğan**, Mesuliyet, 247; **Akipek**/**Akıntürk**/**Ateş**: Kişiler, s. 395.

Saldırının önlenmesi davasında verilen karar İcra İflas Kanunu'nun m. 30 hükmü kapsamında gereği icra edilebilir bir hüküm olduğu için, saldırının önlenmesi davası nitelik itibariyle eda davasıdır.

Kişisel veri ihlalleri teknolojik imkanlar dikkate alındığında saniyeler içerisinde gerçekleşebilecek ihlaller olup saldırının önlenmesi davasının işlerliği sınırlıdır.[371] Ancak veri işleme sürecinin ne kadar hızlı olduğu dikkate alındığında gerçekleşmesi ciddi ve yakın bir hukuka aykırı veri işleme tehdidi oldukça nadir görülebilecek bir durumdur.[372]

3.3.2.2. Saldırıya Son Verilmesi Davası

Hukuka aykırı olarak kişilik haklarını hedef alan ve devam eden saldırılara karşı saldırıya son verilmesi davası açılır. İki farklı biçimde isimlendirilmekte olup bunlar saldırıya son verilmesi davası veya durdurma davası şeklindedir.

Saldırıya son verilmesi davası açılabilmesi için kişilik hakkında yönelen hukuka aykırı saldırının devam etmesi zorunludur. Dolayısıyla anlık olarak gerçekleşen bir saldırı için bu yola başvurulması olası değildir. Hukuka aykırı biçimde kişisel verilerin işlenmesi istisnalar haricinde anlık bir faaliyet değildir. Saldırının önlenmesi davasından farklı olarak kişisel verilerin korunması hukukunda uygulama imkanı sınırlı bir dava değildir.

Somut olarak örneklemek gerekirse kişinin rızası dışında verileri kaydedilmiştir. Ayrıca açıkça talep etmesine rağmen silinmediği bilinmektedir. Gündelik hayatta sıklıkla rastlanabilecek bir olay olan bu örnek olayda saldırıya son verilmesi davası açılmasının önünde bir engel mevcut değildir. Böyle bir olayda kişi saldırıya son verilme davası sonucunda icrai bir hüküm elde edecektir. Diğer bir deyişle hakim bir hukuka aykırı olarak devam eden veri işlemenin kesilmesine karar verecektir. Saldırının önlenmesinde yaptığımız hükmün icrai bir hüküm olduğu ve davanın niteliği itibariyle eda davası olduğu yönündeki tespit burada da geçerlidir.[373]

---

[371] **Küzeci**, s. 387.
[372] **Özdemir**, Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması, s. 190.
[373] **Tandoğan**, Mes'uliyet, s. 245; **Serozan**, Kişiler, s. 476; **Kılıçoğlu**, Basın Yoluyla Saldırı, s. 335 **Dural/Öğüz**, s. 152.

3.3.2.3. Saldırının Hukuka Aykırılığını Tespit Davası

Kişilik haklarına yönelik bir saldırıya uğrayan ve saldırının etkileri hala devam eden kişi bu saldırının hukuka aykırı olduğunun tespitini TMK 25/1 kapsamında talep edebilir. Bu dava kapsamında yalnızca saldırının hukuka aykırı olduğu tespit edilir ve davanın açılabilmesi için saldırının nihayete ulaşmış olması ancak etkilerinin devam ediyor olması gerekir.

Saldırı ihtimalinde önleme davası, devam ederken ise durdurma davası açılabilmektedir. Bu davalar nitelik itibariyle eda davası olup eda davası açılabilen hallerde tespit davasının açılması mümkün değildir.[374] Saldırının önlenmesi veya durdurulması davalarının açılabildiği durumlarda saldırının hukuka aykırılığının tespiti davası açılamayacaktır.

Koruyucu davalardan bir tanesi olan saldırının hukuka aykırılığının tespiti, genel nitelikteki tespit davasının TMK'da düzenlenen özel bir görünümüdür[375].Kişisel verilerinin hukuka aykırı biçimde işlendiğini düşünen gerçek kişi bu yola başvurabilir. Ancak uygulamada daha pratik alternatifler olması nedeniyle sık rastlanan işlevsel bir yol değildir.[376]

KVKK m. 11 hükmünde ilgili kişiye veri sorumlusuna başvurmak suretiyle verilerinin işlenip işlenmediği, eğer işleniyorsa kapsamını, verilerinin işlenme amacını ve belirtilen amaca uygun kullanılıp kullanılmadığını, üçüncü kişilere aktarılıp aktarılmadığını ve aktarılıyorsa kimlere aktarıldığını öğrenme hakkında sahiptir. Bu hakkı kullanan gerçek kişinin ayrıca tespit davası açması ve hukuka aykırılığın tespitini talep etmesi işlevsel ve faydalı görünmemektedir.[377]

3.3.2.4. Kararın Yayımlanması veya Üçüncü Kişilere Bildirilmesi

Koruyucu davaların yanı sıra ilgili kişinin düzeltmeyi veya mahkeme kararını daha fazla kişiye duyurmayı isteyebilir. TMK m. 25/2'de yer alan hükme göre kişilik haklarına saldırının düzeltilmesi veya ilgili mahkeme kararının yayımlanmasını veya üçüncü kişilere başkaca yollarla duyurulmasını talep edebilmektedir.[378]

---

[374] Kişinin eda davası açması ihtimali mevcut olduğunda tespit davası açmasında hukuki fayda bulunmamaktadır. Eda davası hali hazırda ilgili tespit hükmünü de içerecek niteliktedir.
[375] **Helvacı**, Koruyucu Davalar, s. 134.
[376] **Zor**, s. 180.
[377] **Taştan**, s. 191.
[378] **Kılıçoğlu**, Medeni Hukuk, s. 388.

Koruyucu davalar kişi lehine sonuçlansa dahi kişilik haklarına yönelen saldırı sonucu kişi üçüncü kişiler nezdinde haksız durumda görünebilir. Bu durum toplum içindeki saygınlığını ve itibarını da olumsuz etkileyecektir. Özellikle saldırıdan başka kişilerin haberdar olması durumunda tercih edilmesi mümkündür.

İlgili kişi durdurma veya tespit davası açtığı takdirde aynı dava içerisinde kararın yayınlanması veya üçüncü kişilere bildirilmesi yönündeki talebini de iletebilir. Ancak bağımsız olarak dava ve talep edilebilen bir hak değildir.[379]

[379] **Özdemir**, Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması, s. 196.

SONUÇ

Dijital ekonominin giderek gelişmesi ve verinin ekonomik değerinin artmasıyla birlikte kişisel verilerin korunması ihtiyacı da artmıştır. Bu gelişmelerin sonrasında kişisel verilerin korunması, temel bir insan hakkı olarak değerlendirilmiştir. Yıllardır birçok ulusal ve uluslararası metin kapsamında korunan kişisel veriler, Türkiye'de ilk kez TCK m. 135-140 hükümleriyle koruma kapsamına alınmıştır. Ancak burada yer alan düzenlemeler oldukça kısıtlı bir koruma sağlamıştır. TCK'nın yürürlüğe girdiği tarihten KVKK'nın yürürlüğe girdiği tarihe kadar veri korumayı amaçlayan özel bir kanun olmaması ve idari bir merci bulunmaması bir eksiklik olarak göze çarpmaktadır.

Ardından 2010 yılına gelindiğinde Anayasa'nın "özel hayatın gizliliği" başlıklı m. 20 hükmüne eklenen düzenlemeyle birlikte verilerinin korunmasını istemek kişinin temel hakları arasında kabul edilmiş anayasal güvenceye kavuşmuştur. Ancak temel bir hak olduğu kabul edilmesine rağmen kişisel verilerin korunmasını detaylı düzenleyen, idari süreçleri belirleyen ve güvence altına alan bir mevzuat ve idari süreci yönetecek bir kurum kurulması uzun yıllar almıştır. Anayasa değişikliğinden yaklaşık 6 yıl sonra 7 Nisan 2016 tarihine gelindiğinde, KVKK yürürlüğe girmiş böylece ülkemizde kişisel verilerin korunması yönünde temel düzenleme yapılmıştır.

Kişisel verilerin korunması hukukunun amacı veri işleme faaliyetlerinin bir hukuki çerçeve içerisinde ilerlemesini sağlamak ve kişinin haklarını ve özgürlüklerini ihlal edilmesini engellemektir. Birçok beşeri faaliyetin devamı, insanların daha kaliteli hizmet alabilmesi, ihtiyaçların tespiti ve çözüm önerilerinin geliştirilmesi, hastalıkların tespiti ve tedavisi, insanlara hizmet etmeyi hedefleyen algoritmaların geliştirilmesi için kişisel verilerin işlenmesi zorunludur. Dolayısıyla kişisel verilerin korunması ve veri işlenme zorunluluğu arasında, hukuki bir menfaat dengesi sağlanması gerektiği anlaşılmaktadır.

Ülkemizde kişisel verilerin işlenmesine ilişkin temel kavramları, hakları ve yükümlülükleri düzenleyen temel mevzuat KVKK'dır. KVKK'da kişisel veri kavramının kapsamı, veri işleme sürecinin tarafları, veri sorumlusunun yükümlülükleri, ilgili kişinin hakları, veri ihlali oluştuğunda uygulanacak idari para cezaları, kişisel verilerin korunmasına ilişkin kabahatler düzenlenmiştir.

Çalışmamızın konusunu kişisel verilerin korunmasına ilişkin kamu hukuku süreçleri oluşturmamakla birlikte birinci bölümde Tüzük ile karşılaştırılarak eksik olduğunu düşündüğümüz hususlar belirtilmiştir. Bu noktada Tüzük'te düzenlenip KVKK'da düzenlenmeyen dizaynla koruma, varsayılan ayarlarla koruma teknolojik gibi karmaşık alanlarda kullanıcıyı koruyan hususların yeniden incelenip mevzuata eklenmesinin çağın gereklerini yakalamak açısından faydalı olacağını düşünmekteyiz.

Ayrıca unutulma hakkı ve çocukların kişisel verilerinin korunması hususlarının da mevzuatta açıkça düzenlenmemesi kanımızca bir eksikliktir. Yargı kararlarında unutulma hakkı sıklıkla geçmekte ve arama motorlarının bu hakkı kullanıcılarına tanıdığı bilinmekle birlikte mevzuatımızın bu alanda eksik olduğu görülmektedir.

KVKK, ikincil mevzuat ve idari süreçler çalışma kapsamında incelenmekle birlikte çalışmanın ele aldığı temel konu bu alan değildir. Çalışmamızın konusu kişisel verilerin korunması yükümlülüğünün ihlalinden doğan hukuki sorumluluk olup bu konuda KVKK'da sınırlı düzenleme mevcuttur. KVKK m. 11/1-ğ ve m. 14 incelediğinde hukuk aykırı biçimde veri işlenmesi durumunda hangi yollara başvurabileceğinin düzenlendiği görülmektedir.

Öncelikle 11/1-ğ hükmünde ilgili kişinin veri sorumlusuna başvurarak kanuna aykırı biçimde veri işlenmesi nedeniyle uğradığı zararı talep edebileceği belirtilmiştir. Bu noktada Kurumun zararın talep edilmesi veya tazminat talepleriyle ilgili olarak hiçbir yetkisi olmadığını ve AB örneklerinde de hiçbir veri koruma otoritesinin tazminat süreçlerinde karar verici olmadığını belirtmek uygun olacaktır. Bu husus Kurul tarafından verilen kararlarda da açıkça izah edilmiştir.

KVKK m. 11/1-ğ lafzı incelendiğinde kusur ifadesinin geçmediği görülmektedir. Buradan hareketle literatürde veri işleme faaliyetiyle ilişkili biçimde zararın doğmasının zararın tazmini için yeterli olduğu, bunun bir kusursuz sorumluluk haline işaret ettiği görüşü mevcuttur. Bu görüş kapsamında kanun koyucu m. 12 hükmünde sayılan verilerin hukuka aykırı işlenmesini ve erişilmesini önleme ve muhafazasını sağlama yükümlülüklerine aykırı davranan kişi kusuru olmasa dahi sorumludur. Ayrıca idari ve teknik tedbirleri alma yükümlülüğünün veri sorumlusunda olduğu hususu da yine bu madde hükmünde belirtilmiştir.

Kusursuz sorumluluk tespitini yapan görüş KVKK m. 11/1-ğ ve 12 birlikte değerlendirmektedir. Bu görüşe göre veri güvenliğini tam olarak sağlamak mümkün değildir. Ayrıca kullanılan yüksek teknoloji ve karmaşık sistemler sebebiyle kusuru mağdurun tespit etmesi kolay değildir. Yapısı itibariyle veri sorumlusunun kusursuz sorumluluğuna gidilmesinin daha uygun olduğunu ve kanun koyucunun da bunu dikkate alarak düzenleme yaptığını savunmaktadırlar.

Bu noktada kurulun veri işleme süreçlerindeki ilkelere ilişkin verdiği kararlara da bakmak gerekmektedir. KVKK m. 12 verileri hukuka uygun işlenmesi gerektiğini düzenlemiştir. KVKK m. 4 ise veri işleme sürecinde dikkate alınması gereken ilkeleri sıralamıştır. Bunlardan bir tanesi de doğru ve gerektiğinde güncel işlemedir. Bu ilkenin uygulanmasına ilişkin kararlara bakıldığında veri sorumlusundan "aktif özen yükümlülüğü" veya "veri doğruluğunun proaktif sağlanması" gibi bir çabanın beklendiği görülmektedir. Aktif özen yükümlülüğüne ilişkin net bir tanım yapılmamakla birlikte veri doğruluğu ve güncelliği ilkesinin uygulanmasında veri sorumlusunun sorumluluğunun genişletildiği açıktır.

Ancak kişisel verilerin işlenmesine ilişkin sorumluluğun kusur sorumluluğu olduğu yönünde argümanlar da mevcuttur. TBK m. 56'da düzenlenen "manevi tazminat" ve m. 58'de düzenlenen "kişilik hakkının zedelenmesi" hükümlerinde de kusur açık biçimde zikredilmemiştir. Ancak her iki hükmün uygulanması için de kusurun varlığı aranmaktadır.[380]

Ayrıca Kurul kararlarında yer verilen özen yükümlülüğüne ilişkin tespitler tek başına bir olağan sebep sorumluluğu yaratmak için elverişli değildir. Kurul bir yükümlülüğü geniş yorumlayabilir ancak idare bir işlemiyle kanun hükmünün kapsamını genişletemez. Kamu hukuku anlamında uygulanan yaptırım mahkeme açısından bağlayıcı değildir.

Bunların yanı sıra hukukumuzdaki genel kabule göre kusur sorumluluğu kural kusursuz sorumluluk ise istisnadır. Kanun koyucu eğer bir kusursuz sorumluluk getirmek ve veri sorumlusunun sorumluluğunu genişletmek isteseydi bunu oldukça açık biçimde yapabilirdi. Bu gerekçeler ışığında KVKK m. 11/1-ğ bir kusursuz sorumluluk hali olmadığı görüşünü kabul etmekteyiz.

---

[380] **Demir**, Kübra: "Manevi Tazminatın Belirlenmesine Genel Bir Bakış", Sakarya Üniversitesi Hukuk Fakültesi Dergisi, C. 8, S. 1-2, 2020, s. 82; **Eren**, s. 898 vd.

KVKK m. 14/3 hükmünde ise veri işleme faaliyeti nedeniyle kişilik hakları ihlal edilen gerçek kişilerin genel hükümler kapsamında tazminat talep edebileceği ifade edilmektedir. Kişisel verilerin korunması hakkının kişilik haklarının altında bağımsız bir hak olduğu görüşüne katıldığımızı ilgili başlık altında ifade etmiştik. Dolayısıyla hukuka aykırı bir veri işleme faaliyeti neticesinde kişilik hakkı ihlalinin doğması muhtemeldir.

Kişilik hakları ihlal edilen kişilerin tazminat hakkı olduğu genel hükümler çerçevesinde güvence altına alınmıştır. Ancak aynı veri ihlalinden binlerce hatta milyonlarca kişinin etkilenmesi mümkündür. Her bir mağdurun tek tek dava açması ve mağduriyetinin giderilmesini talep etmesi kolay olmadığı gibi usul ekonomisi açısından da pratik değildir. Mağdur olanların alabileceği bireysel tazminat miktarının yargılama giderlerine oranla çok düşük kalması ve gerekli hukuki bilgiden yoksun olmaları veri ihlallerinden doğan hukuki sorumluluk yollarına başvurmalarını engelleyebilmektedir. Bu durum hukukumuzda toplu davaların eksikliğinin bir sonucudur. Hukukumuzda toplu davalarla benzerlik taşıyan topluluk davaları mevcuttur. Ancak topluluk davaları yalnızca tüzel kişilere üyelerinin menfaatlerini korumak amacıyla dava açma imkânı sunmaktadır. Dolayısıyla kişisel veri ihlalleri sebebiyle oluşacak kişilik hakkı ihlallerinin giderilmesi açısından uygulanabilir değildir. Kanaatimizce toplu davalara benzer bir şekilde aynı sebepten mağdur olan kişilerin davaya katılarak haklarını alabilecekleri bir dava açma imkânı kişisel veri ihlalleri açısından caydırıcı olacağı gibi zararın tazminini de kolaylaştıracaktır.

Koruyucu davalar açısından baktığımızda ise saldırının önlenmesi, saldırının hukuka aykırılığının tespiti kişisel veri ihlallerinin oluşumu açısından uygulanmasına oldukça nadir rastlanan davalardır. Ancak teorik olarak veri ihlali nedeniyle bu davaların açılmasının önünde bir engel bulunmamaktadır. Ayrıca saldırıya son verilmesi ve kararın yayınlanması veya üçüncü kişilere bildirilmesi davaları da veri ihlallerinden kaynaklanan uyuşmazlıklarda uygulama alanı bulabilecek davalardır.

KAYNAKÇA

ABİK, Yıldız: “Normun Koruma Amacı Teorisi”, AÜHFD, C. 59, S. 3, 2010, s. 345-448.

ABİK, Yıldız: “Kişisel Sağlık Verilerinin Medeni Hukuk Bakımından Korunması”, II. Uluslararası Tıp Hukuku Kongresi Bildirileri Kitabı (Ed. Hakeri/Doğan), Ankara 2018, s. 537-613. (Kişisel Sağlık Verilerinin Korunması)

AGULLÓ, Diego: “Directive 2020/1828 On Representative Actions For The Protection Of The Collective İnterests Of Consumers: An Overview”, UNIO - EU Law Journal. C. 8, S. 1, 2022, s. 127-142.

AKİPEK, Jale**/AKINTÜRK,** Turgut**/ATEŞ,** Derya**:** Türk Medeni Hukuku Başlangıç Hükümleri Kişiler Hukuku, Yenilenmiş 16. Baskı, Beta Yayınları, İstanbul, Eylül 2020. (Kişiler)

AKİPEK, Şebnem: Alt Vekâlet, Yetkin Yayınları, Ankara 2014.

AKKURT, Sinan Sami: “Kişisel Veri Kavramının Hukuki Niteliğine İlişkin Yaklaşımlara Mukayeseli Bir Bakış”, Kişisel Verileri Koruma Dergisi, C. 2, S.1, 2020, s. 20-32.

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

AKSOY, Abdulkadir**/TÜRKÖLMEZ,** Onur: “Dijital Çağa Demokrasiyi Çağırmak: Cambridge Analytica Skandalı”, Journal of Political Administrative And Local Studies, C.3, S. 1, 2020, s. 41-59.

ALIMCI, Ezgi: “Kişisel Verilerin Korunması Hukuku ve Bankaların Güven Kuruluşu Olarak Kabul Edilmesi Kapsamında Banka Bünyesinde Gerçekleşen Veri İhlalinin Değerlendirilmesi”, Ankara Barosu Dergisi, C. 80 S.1, 2021, s. 47-76.

ANTALYA, Gökhan: “Manevi Zararın Belirlenmesi ve Manevi Tazminatın Hesaplanması, Türk Hukukuna Manevi Zararın İki Aşamalı Olarak Belirlenmesine İlişkin Bir Model Önerisi”, Cevdet Yavuz‘a Armağan, C.1, 2016, s. 221-250. (Manevi Zarar)

ANTALYA, Gökhan: Borçlar Hukuku Genel Hükümler, Legal Yayıncılık, İstanbul 2018. (Borçlar Genel**)**

ARPACI, Abdülkadir: Kişiler Hukuku (Gerçek Kişiler), 2. Bası, İstanbul, Beta Yayınevi, 2000.

ATLAN, Hülya: Manevi Zararı Tazmin Yolları, XII Levha Yayınları, İstanbul 2015.

AYÖZGER ÖNGÜN, Çiğdem: Kişisel Verilerin Korunması Hukuku – Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil, 2. Baskı, İstanbul, Beta, 2019.

ARINMIŞ UZUN, Sündüs: "Türkiye'de Kişisel Verilerin Korunması ve Vatandaş Algısının Ölçülmesi", Bilişim Teknolojileri Dergisi, C. 14, S. 3, 2021.

AYAN, Mehmet: Borçlar Hukuku Genel Hükümler, Adalet Yayınevi, Ankara 2020.

BADUR, Emel/**KURT KONCA,** Nesibe: "Kişisel Verilerin Hukuka Aykırı İşlenmesinden Doğan Zararların Tazmini ve Görevli Mahkeme", İnönü Üniversitesi Hukuk Fakültesi, C. 13 S. 2, 202, s. 476- 490.

BAŞALP, Nilgün: Kişisel Verilerin Korunması ve Saklanması, Yetkin Yayınları, Ankara, 2004.

BAŞAR, Cemal; Türk İdare Hukuku ve Avrupa Birliği Hukuku Işığında Kişisel Verilerin Korunması, XII Levha Yayınları, İzmir, Haziran 2020.

BAŞARA, Gamze Turan: "Kişisel Veri İşleme Sözleşmesi", Uyuşmazlık Mahkemesi Dergisi, S.16, 2020, s. 57 – 90.

BAŞBUĞ, Aydın: Hekimin Yükümlülükleri ve Hukuki Sorumluluğu, II. Sağlık Hukuku Sempozyumu, Kuzey Kıbrıs Türk Cumhuriyeti, Lefke Avrupa Üniversitesi, 17-18 Mayıs 2010.

BAYSAL, Başak: Zarar Görenin Kusuru, XII Levha Yayınları, İstanbul 2012.

BELLE, Ashwin/ **THİAGARAJAN,** Raghuram/ **SOROUSHMEHR,** Reza/ **NAVİDİ,** Fatemeh/ **BEARD,** Daniel/ **NAJARİAN,** Kayvan: Big Data Analytics In Healthcare, Biomed Research International, 2015.

BİLGİN, Metin/**ERKAN,** Sema/**ATASU,** İdil/**YILMAZ,** Enes: "Privacy Impact Assessment as a Tool for GDPR Compliance Preparation", Kişisel Verileri Koruma Dergisi, C. 1, S. 2, 2019.

BORAN GÜNEYSU, Nilüfer/**MEMİŞ,** Burak: Kişisel Verilerin Korunması Kanunu Kapsamında Avukatın Yükümlülük ve Sorumlulukları, Anadolu Üniversitesi Hukuk Fakültesi Dergisi, C. 5, S. 2, 2019.

CANBOLAT, Ferhat/**GÖNÜL KOŞAR,** Günhan: Basın Yoluyla Kişilik Hakkının İhlalinin Tespitinde Kullanılan Yargıtay ve Avrupa İnsan Hakları Mahkemesi Ölçütlerinin Değerlendirilmesi, TBB Dergisi, S. 151, 2020, s. 265.

BRAUN, Cihan Avcı: Kişisel Verilerin İşlenmesinde Rıza. Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, C.15 S.1, 2018, 13-35.

CHENG, Long/**LİU,** Fang/**YAO,** Dafeng: "Enterprise Data Breach: Causes, Challenges, Prevention, And Future Direction", Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, C. 7, S. 5, 2017.

ÇEKİN, Mesut Serdar: "6698 Sayılı Kişisel Verilerin Korunması Hakkında Kanun'un Big Data (Büyük Veri) ve İrade Serbestisi Açısından Değerlendirilmesi", İÜHFM, C. LXXIV, S. 2, 2016, s. 629-644. (Büyük Veri)

ÇEKİN, Mesut Serdar: Kişisel Verilerin Korunması, XII Levha Yayınları, İstanbul 2019. (Kişisel Veri)

ÇELİK, Yeşim: "Özel Hayatın Gizliliğinin Yansıması Olarak Kişisel Verilerin Korunması ve Bu Bağlamda Unutulma Hakkı", Türkiye Adalet Akademisi Dergisi, Sayı: 32, s. 391-410.

ÇİMEN BULUT, İpek: "Avrupa Birliği Genel Veri Koruma Tüzüğü Kapsamında Getirilen Yeni Teknik ve Yaptırım Mekanizmaları", Anadolu Üniversitesi Sosyal Bilimler Dergisi, C. 20 S. 2, 2020, s. 127-142.

DEMİR, Kübra: "Manevi Tazminatın Belirlenmesine Genel Bir Bakış", Sakarya Üniversitesi Hukuk Fakültesi Dergisi, C. 8, S. 1-2, 2020, s. 67-88.

DEVELİOĞLU, Murat: 6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku, XII Levha Yayıncılık, İstanbul 2017.

DONAY, Süheyl: “Vekilin Talimata Uyma ve Dürüstlükle Hareket Etme Borcu”, BATİDER, C. 5, S. 4, 1970, s. 728-749.

DUMAN, Berat: Anayasa Hukukunda Kişisel Verilerin Korunması, Doktora Tezi, Selçuk Üniversitesi, Konya, 2020.

DURAL, Mustafa/**ÖĞÜZ,** Tufan: Kişiler Hukuku, Filiz Kitabevi, İstanbul 2013.

DÜLGER, Murat Volkan: Bilişim Suçları ve İnternet İletişim Hukuku, Seçkin Yayınevi, Ankara, 2014. (Bilişim Suçları)

DÜLGER, Murat Volkan: Kişisel Verilerin Korunması Hukuku: Veri Korumaya İlişkin Temel İlkeler, KVKK'da Kişisel Verilerin Korunması, Veri Korumaya İlişkin Suçlar Ve Kabahatler, Uyumluluk Süreci Ve Örneklerle Anlatımlı KVKK ve GDPR Karşılaştırmalı, Hukuk Akademisi, İstanbul, 2019. (Veri Koruma Hukuku)

DÜLGER, Murat Volkan: “Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması”, İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi C. 3 S. 2, 2016, s. 101-167. (Kişisel Verilerin Korunması)

DÜLGER, Murat Volkan: “Tasarlanmış Ve Önceden Tanımlanmış Veri Koruma İle Zarara Karşı Risk Sorumluluğu: Kişisel Verileri Koruma Kurulu’nun 18 Şubat 2019 Tarihinde Yayınlanan Kararları Ne Anlama Geliyor?”, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3792301 Erişim Tarihi: 11.03.2023. (Risk Sorumluluğu)

ELGESEM, Dag: “The Structure Of Rights İn Directive 95/46/EC On The Protection Of İndividuals With Regard To The Processing Of Personal Data And The Free Movement Of Such Data”, Ethics and Information Technology, S.1, 1999, s. 283-293.

EREN, Fikret: Borçlar Hukuku Genel Hükümler, Yetkin Yayınları, Ankara 2021.

ERİŞGİN, Nuri: “Tehlike Bağı”, AÜHFD, C. 49, S. 1, 2000, s. 137-154.

EVAN, Oddleifson: The Effects of Modern Data Analytics in Electoral Politics: Cambridge Analytica’s Suppression of Voter Agency and the Implications

for Global Politics, Political Science Undergraduate Review, C. 5, Winter 2020.

GÖÇMEN UYARER, Sinem: 6698 Sayılı Kişisel Verilerin Korunması Kanunu ve 5237 Sayılı Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması, Yüksek Lisans Tezi, Galatasaray Üniversitesi, İstanbul, 2019.

GÜNAY, Cevdet İlhan: Borçlar Hukuku Genel Hükümler – Özel Borç İlişkileri, Yetkin Yayınları, Ankara 2016.

GÜLTEKİN VÁRKONYİ, Gizem: "Avrupa Birliği Genel Veri Koruma Tüzüğü Kapsamında Gerçek Kişilerin Kişisel Sosyal Robot Kullanımından Doğabilecek Sorumlulukları", Kişisel Verileri Koruma Dergisi, C. 2 S. 2, s. 19-29.

GÜMÜŞ, Mustafa Alper: Borçlar Hukuku Özel Hükümler, Vedat Kitapçılık, İstanbul 2012.

GÜNDAY, Metin: İdare Hukuku, İmaj Yayıncılık, 7. Baskı, Ankara 2003.

GÜRPINAR, Damla: "Kişisel Verilerin Korunamamasından Doğan Hukuki Sorumluluk", Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, C. 19 S. 3, 2017.

HAMMOUCHİ, Hicaham/**CHERQİ,** Othmane/**MEZZOUR,** Ghita/**GHOGHO,** Mounir/**EL KOUTBİ,** Mohammed: Digging Deeper İnto Data Breaches: An Exploratory Data Analysis Of Hacking Breaches Over Time, Procedia Computer Science, 2019.

HATEMİ, Hüseyin: Kişiler Hukuku, 8. Bası, XII Levha Yayıncılık, İstanbul, Eylül 2020. (Kişiler Hukuku)

HATEMİ, Hüseyin: Medeni Hukuka Giriş, XII Levha Yayınlar, İstanbul 2020. (Medeni Hukuk)

HATEMİ, Hüseyin**/ GÖKYAYLA,** K. Emre: Borçlar Hukuku Genel Bölüm, 4. Bası, İstanbul, Vedat Kitapçılık, 2017. (Borçlar Hukuku)

HELVACI, Serap: Türk ve İsviçre Hukuklarında Kişilik Hakkını Koruyucu Davalar, İstanbul, Beta, 2001. (Koruyucu Davalar)

HELVACI, Serap: Gerçek Kişiler, Legal Yayınları, İstanbul 2017. (Gerçek Kişiler)

HORNUNG, Gerrit/**SCHNABEL,** Christoph: Data Protection in Germany I: The Population Census Decision and The Right To Informational Self Determination, Computer Law & Security Report, 2009, C. 25, S. 1, s. 84-88.

İNAN, Ali Naim: Borçlar Hukuku Genel Hükümler, AÜHF Yayınları, Ankara 1984

ISAAK, Jim/**HANNA,** J. Mina: "User Data Privacy: Facebook, Cambridge Analytica, And Privacy Protection", Computer, 2018, C. 51, S. 8.

İMANÇLI, Canan: Kişisel Sağlık Verilerinin Korunamamasından Doğan Özel Hukuk Sorumluluğu, On İki Levha Yayınları, İstanbul 2020.

İNCİROĞLU, Kübra/**ÖGE,** Ercan: "İnsan Kaynakları ve Bilgi İşlem Departmanlarının İşletmelerde Kişisel Verilerin Korunmasındaki Rolü: Farklı Sektörlerden Örnek Olay Çalışmaları", Journal of International Social Research, C. 12, S. 65, 2019, s. 1433-1454.

İTİŞGEN, Rezzan: "Türk Ceza Hukukunda Kişisel Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme Suçu", Türkiye Adalet Akademisi Dergisi, S. 23, 2015, 179-202.

KAYA, Kübra: "Özel Hayatın Gizliliği Hakkı ile Kişisel Verilerin Korunması Hakkı Bağlamında Ortaya Çıkan Bir Hak Olarak Unutulma Hakkının Değerlendirilmesi", Türkiye İnsan Hakları ve Eşitlik Kurumu Akademik Dergisi, C. 5 S. 8, 2022, s. 177-196.

KARAGÜLMEZ, Ali: Bilişim Suçları, Seçkin Yayınları, Ankara, 2014.

KARLIDAĞ, Serpil: "Ekonomi Politik Açıdan Kişisel Verilerin Korunması", Amme İdaresi Dergisi, C. 46 S.1, 2013, s. 127-152.

KART, Aslıhan/**KETİZMEN,** Muammer: "Kabahatler Kanunu'nun İçtima Hükümleri Açısından Kişisel Verilerin Korunmasına İlişkin Suç ve Kabahatler İle Kurul'un İdari Ceza Kararlarına İlişkin Bir Değerlendirme", Kişisel Verileri Koruma Dergisi, C.1 S. 2, 2019, 17-29. (Kişisel Verilerin Korunmasına İlişkin Suç ve Kabahatler)

KAYA, Mehmet Bedii/**TAŞTAN,** Furkan Güven: Kişisel Veri Koruma Hukuku – Mevzuat & İçtihat, XII Levha Yayınları, İstanbul, 2019.

KÜÇÜKGÜNGÖR, Erkan: Tıbbi Kayıtlarda Sır Saklama Yükümlülüğü, Ankara Barosu III. Sağlık Hukuku Kurultayı, 7-8 Mayıs, Ankara 2011, s. 554-577.

KÜZECİ, Elif: Kişisel Verilerin Korunması, XII Levha Yayınları, İstanbul, 2020.

GÖNÜL KOŞAR, Günhan: Haksız Fiil Sorumluluğunda Kusur ve Etkisi, XII Levha Yayınları, İstanbul, 2020.

KESKİNKILIÇ, Gamze Nur: Veri Koruma Görevlisi, Yüksek Lisans Tezi, İstanbul Medipol Üniversitesi, İstanbul, 2021.

KILIÇOĞLU, Ahmet: Şeref, Haysiyet ve Özel Yaşama Basın Yoluyla Saldırılardan Hukuksal Sorumluluk, 3. Bası, Ankara, Turhan Kitabevi, 2008. (Basın Yoluyla Saldırı).

KILIÇOĞLU, Ahmet: "Haksız Fiillerden Sorumlulukta Ceza Hukuku İle Medenî Hukuk İlişkisi", Ankara Üniversitesi Hukuk Fakültesi Dergisi, C. 29, S. 3, 1973, s. 185-222. (Haksız Fiillerden sorumluluk)

KILIÇOĞLU, Ahmet: Borçlar Hukuku Genel Hükümler, Turhan Kitabevi, Ankara 2012. (Borçlar Genel)

KILIÇOĞLU, Ahmet: Medeni Hukuk, Turhan Kitabevi, Ankara 2016. (Medeni Hukuk)

KILINÇ, Doğan: "Anayasal Bir Hak Olarak Kişisel Verilerin Korunması", AÜHFD, C. 61, S. 3, 2012, s. 1089-1172.

KOCA, Mahmut/**ÜZÜLMEZ,** İlhan: "Kişisel Verilerin Kaydedilmesi Suçu (TCK m. 135)", Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, Prof. Dr. Durmuş TEZCAN'a Armağan, C.21, 2019, s. 69-93.

KORKMAZ, İbrahim: "Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme", TBB Dergisi S. 124, 2016, s. 81-152.

KÖKSAL, Mustafa: "Risk İlkesinin İdareye Yüklediği Külfetler ve Güncel Yargı Kararları", TBB Dergisi, S. 85, 2009, s. 241-274.

LANEY, Doug: 3D Data Management: Controlling Data Volume, Velocity, and Variety, 2001.

LLOYD, Ian J: Information Technology Law, 6th Edition, Oxford University Press, Oxford, 2020.

MURRAY, Alan: Information Technology Law (The Law and Society), Oxford University Press, Oxford, 2019.

NALBANTOĞLU, Seray: "Bir Temel Hak Olarak Unutulma Hakkı", Türkiye Adalet Akademisi Dergisi, S. 35, 2018, s. 583-605.

NOMER, Haluk Nami: Borçlar Hukuku Genel Hükümler, Beta, 14. Baskı, İstanbul, 2015.

OĞUZMAN, Kemal/**ÖZ,** Turgut: Borçlar Hukuku Genel Hükümler, Vedat Kitapçılık, İstanbul, 2016.

ORAL, Tuğçe: Tüzel Kişilerin Manevi Zararı, XII Levha Yayınları, Ankara 2018.

ORAK, Beşir: Kişisel Sağlık Verilerinin Korunması, Yetkin, Ankara, 2020.

ÖZDEMİR, Hayrunnisa: Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması, Seçkin Yayıncılık, Ankara 2009. (Kişisel Veri)

ÖZKAN, Oğulcan: Kişisel Verilerin Korunması, Yüksek Lisans Tezi, Ankara Üniversitesi, Ankara 2020.

OĞUZMAN, Kemal/**ÖZ,** Turgut: Borçlar Hukuk Genel Hükümler, Vedat Kitapçılık, İstanbul 2018.

ÖZER DENİZ, Miray: Özel Nitelikli Kişisel Verilerin İşlenmesi ve Bundan Doğan Sorumluluk, XII Levha Yayınları, İstanbul 2022.

ÖZSUNAY, Ergun: Gerçek Kişilerin Hukuki Durumu, İstanbul Üniversitesi Yayınları, İstanbul, 1979.

PERSİLY, Nathaniel: "The 2016 US Election: Can Democracy Survive the Internet?", Journal of Democracy, C. 28, S. 2, 2017.

POLİTOU, Eugenia/**ALEPİS,** Efthimios**/PATSAKİS,** Constantinos: "Forgetting Personal Data And Revoking Consent Under The GDPR: Challenges And Proposed Solutions", Journal Of Cybersecurity, C. 4 S. 1, 2018, s. 1-20.

SEFER, Oğuz: "Kişisel Verilerin Korunması Hukukunun Genel İlkeleri", Bilgi Ekonomisi ve Yönetimi Dergisi, C.13 S. 2, 2018, s. 121-138.

SINAR, Hasan: "Kişisel Verileri Hukuka Aykırı Olarak Verme, Yayma Veya Ele Geçirme Suçu (TCK m. 136)", Kişisel Verileri Koruma Dergisi, C.2, S.1, 2020, s. 33-62.

SIRABAŞI, Volkan: İnternet ve Radyo- Televizyon Aracılığıyla Kişilik Haklarına Tecavüz, Adalet Yayınevi, Ankara, 2007.

ŞAHİN, Murat/**ÇELİK ŞAHİN,** Hande: "Toplu Hak Aramada Etkin Bir Yol Olarak Mukayeseli Hukukta ve Türk Hukukunda Sınıf Davaları", İstanbul Hukuk Mecmuası, C. 72, S. 1, 2014, s. 383-410.

TANDOĞAN, Haluk: Mukayeseli Hukuk ve Hususiyle Türk-İsviçre Hukuku Bakımından Vekâletsiz İş Görme, İstanbul, Fakülteler Matbaası, 1957. (Mukayeseli Hukuk)

TANDOĞAN, Haluk: Türk Mesuliyet Hukuku, Ankara Hukuk Fakültesi Yayınları, Ankara 1961. (Mesuliyet)

TANDOĞAN, Haluk: Şahsiyetin Akit Dışı İhlâllere Karşı Korunmasının İşleyiş Tarzı Ve Basın Yoluyla Olan İhlâllere Karşı Özel Hayatın Korunması, AÜHFD, C. 20, S.1, 1963. (Şahsiyetin Korunması)

TİKKİNEN-PİRİ Christina/**ROHUNEN,** Anna/**MARKULA,** Jouni: "EU General Data Protection Regulation: Changes And İmplications For Personal Data Collecting Companies", Computer Law & Security Review, C. 34, S. 1, 2017.

TUNÇOMAĞ, Kenan: Türk Borçlar Hukuku Genel Hükümler, İstanbul, 1976

ÜZELTÜRK, Hakan: Avrupa Birliği Genel Veri Koruma Düzenlemesi, Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, C.15, S. 2, 2018, s.161-179.

PAPAİOANNOU, Georgios/**SARAKİNOS,** Ioannis: The General Data Protection Regulation (GDPR, 2016/679/EE) and The (Big) Personal Data İn Cultural İnstitutions: Thoughts On The GDPR Compliance Process. In: ICADL 2018: Maturity and Innovation In Digital Libraries, Springer, Hamilton, 2018, s. 201-204.

SEROZAN, Rona: Kişiler Hukuku, 6. Bası, Vedat Kitapçılık, İstanbul 2015.

ŞEN, Ersan: Türk Ceza Kanunu Yorumu, Vedat Kitapçılık, İstanbul, 2006.

TAŞTAN, Furkan Güven: Türk Sözleşme Hukukunda Kişisel Verilerin Korunması, XII Levha Yayınları, İstanbul, 2017.

TAMÒ-LARRIEUX, Aurelia: Designing for Privacy and its Legal Framework: Data Protection by Design and Default for the Internet of Things, 2018 Heidelberg, Springer.

TEPE, Esra: Özel Hukuk Açısından Avrupa İnsan Hakları Mahkemesi İçtihatları Işığında Kişisel Verilerin Korunması, Adalet Yayınevi, Ankara 2021.

TEKİNAY, Sulhi/**AKMAN,** Sermet/**BURCUOĞLU,** Haluk/**ALTOP,** Atilla: Borçlar Hukuku Genel Hükümler, Filiz Kitabevi, İstanbul, 1993.

UZUNKAYA, Mehmet Celal**/AVCI,** Mustafa: "Tehlike Sorumluluğunun Genelleşmesine Yönelik Düzenleme Tercihi", Antalya Bilim Üniversitesi Hukuk Fakültesi Dergisi, C.3 S.5, 2015, s. 41-65.

YAŞAR, Osman/**GÖKCAN,** Hasan Tahsin**/ARTUÇ,** Mustafa: Yorumlu-Uygulamalı Türk Ceza Kanunu, 3. Cilt, Md. 86-140, 2. Baskı, Ankara 2014.

YAVUZ, Cevdet: "Türk Borçlar Kanunu Tasarısı'na Göre 'Kusursuz Sorumluluk' Halleri ve İlkeleri", MÜHF-HAD, C.14, S.4, 2008, s. 29-61. (Kusursuz Sorumluluk)

YAVUZ, Cevdet: Borçlar Hukuku Özel Hükümler, Seçkin Yayınları, Ankara 2018, (Borçlar Özel)

YILDIZ, Kübra: "Haksız Fiil Hukukunda Nedensellik Bağının Belirlenmesi", Selçuk Üniversitesi Hukuk Fakültesi Dergisi, C. 30, S. 3, 2022, S. 1115-1158.

YILMAZ, Süleyman/**ÇAVUŞOĞLU,** Gökçe Filiz: Kişisel Verileri Koruma Hukuku, Yetkin, Ankara 2020, s.59 vd.

VELİDEDEOĞLU, Hıfzı Veldet: Türk Medeni Hukuku, İstanbul, 1961.

VURALOĞLU, Mehmet Oğuz: "Kişisel Verilerin İşlenmesi Suretiyle Kişilik Hakkı İhlalinde Kazancın Devri Talebi", YÜHFD, C. XV S.1, 2020, s.181-203.

WARREN, D. Samuel/**BRANDEİS,** Louis: "The Rigth to Privacy", Harvard Law Review, C. 4, S. 5, 1890, s. 193-220.

WEBER, H. Rolf/**DOMİNİC,** Staiger: Transatlantic Data Protection in Practice Basel, Springer, Basel 2017.

ZEVKLİLER, Aydın/**GÖKYAYLA,** Emre: Borçlar Hukuku- Özel Borç İlişkileri, Vedat Kitapçılık, İstanbul Üniversitesi Yayınları, İstanbul, 2013.

ZOR, Abdülhamid: Veri Sorumlusunun Yükümlülükleri ve Bu Yükümlülükleri İhlalinden Doğan Özel Hukuk Sorumluluğu, XII Levha, İstanbul, 2020.

HACETTEPE ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
YÜKSEK LİSANS TEZ ÇALIŞMASI ORİJİNALLİK RAPORU

HACETTEPE ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
ÖZEL HUKUK ANABİLİM DALI BAŞKANLIĞI'NA

Tarih: 16/06/2023

Tez Başlığı : Kişisel Verilerin Korunması Yükümlülüğünün İhlalinden Doğan Sorumluluk

……

Yukarıda başlığı gösterilen tez çalışmamın a) Kapak sayfası, b) Giriş, c) Ana bölümler ve d) Sonuç kısımlarından oluşan toplam 120 sayfalık kısmına ilişkin, 16/06/2023 tarihinde şahsım/tez danışmanım tarafından Turnitin adlı intihal tespit programından aşağıda işaretlenmiş filtrelemeler uygulanarak alınmış olan orijinallik raporuna göre, tezimin benzerlik oranı % 23 'tür.

Uygulanan filtrelemeler:

1- X Kabul/Onay ve Bildirim sayfaları hariç
2- X Kaynakça hariç
3- ☐ Alıntılar hariç
4- X Alıntılar dâhil
5- X 5 kelimeden daha az örtüşme içeren metin kısımları hariç

Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü Tez Çalışması Orijinallik Raporu Alınması ve Kullanılması Uygulama Esasları'nı inceledim ve bu Uygulama Esasları'nda belirtilen azami benzerlik oranlarına göre tez çalışmamın herhangi bir intihal içermediğini; aksinin tespit edileceği muhtemel durumda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

Gereğini saygılarımla arz ederim.

Tarih ve İmza

Adı Soyadı:	Kemal KÜÇÜKKAVRUK
Öğrenci No:	N20231734
Anabilim Dalı:	Özel Hukuk
Programı:	Private Law

DANIŞMAN ONAYI

UYGUNDUR.

(Dr, Günhan GÖNÜL KOŞAR, İmza)

HACETTEPE UNIVERSITY
GRADUATE SCHOOL OF SOCIAL SCIENCES
MASTER'S THESIS ORIGINALITY REPORT

HACETTEPE UNIVERSITY
GRADUATE SCHOOL OF SOCIAL SCIENCES
…… DEPARTMENT

Date: 16/06/2023

Thesis Title : Legal Responsibilty Arising from Obligation to Protect Personel Data …….

……

According to the originality report obtained by myself/my thesis advisor by using the Turnitin plagiarism detection software and by applying the filtering options checked below on 16/06/2023 for the total of 120 pages including the a) Title Page, b) Introduction, c) Main Chapters, and d) Conclusion sections of my thesis entitled as above, the similarity index of my thesis is 23 %.

Filtering options applied:

1. X Approval and Decleration sections excluded
2. X Bibliography/Works Cited excluded
3. ☐ Quotes excluded
4. X Quotes included
5. X Match size up to 5 words excluded

I declare that I have carefully read Hacettepe University Graduate School of Social Sciences Guidelines for Obtaining and Using Thesis Originality Reports; that according to the maximum similarity index values specified in the Guidelines, my thesis does not include any form of plagiarism; that in any future detection of possible infringement of the regulations I accept all legal responsibility; and that all the information I have provided is correct to the best of my knowledge.

I respectfully submit this for approval.

Date and Signature

Name Surname:	Kemal KÜÇÜKKAVRUK
Student No:	N20231734
Department:	Private Law
Program:	Private Law Master's Degree

ADVISOR APPROVAL

APPROVED.

(Dr, Günhan GÖNÜL KOŞAR,
Signature)

HACETTEPE ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
TEZ ÇALIŞMASI ETİK KOMİSYON MUAFİYETİ FORMU

HACETTEPE ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
ÖZEL HUKUK ANABİLİM DALI BAŞKANLIĞI'NA

Tarih: 16/06/2023

Tez Başlığı: Kişisel Verilerin Korunması Yükümlülüğünün İhlalinden Doğan Hukuki Sorumluluk
……

Yukarıda başlığı gösterilen tez çalışmam:

1. İnsan ve hayvan üzerinde deney niteliği taşımamaktadır,
2. Biyolojik materyal (kan, idrar vb. biyolojik sıvılar ve numuneler) kullanılmasını gerektirmemektedir.
3. Beden bütünlüğüne müdahale içermemektedir.
4. Gözlemsel ve betimsel araştırma (anket, mülakat, ölçek/skala çalışmaları, dosya taramaları, veri kaynakları taraması, sistem-model geliştirme çalışmaları) niteliğinde değildir.

Hacettepe Üniversitesi Etik Kurullar ve Komisyonlarının Yönergelerini inceledim ve bunlara göre tez çalışmamın yürütülebilmesi için herhangi bir Etik Kurul/Komisyon'dan izin alınmasına gerek olmadığını; aksi durumda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

Gereğini saygılarımla arz ederim.

Tarih ve İmza

Adı Soyadı:	Kemal KÜÇÜKKAVRUK
Öğrenci No:	N20231734
Anabilim Dalı:	Özel Hukuk
Programı:	Özel Hukuk Tezli Yüksek Lisans
Statüsü:	X Yüksek Lisans ☐ Doktora ☐ Bütünleşik Doktora

DANIŞMAN GÖRÜŞÜ VE ONAYI

(Unvan, Ad Soyad, İmza)

Detaylı Bilgi: http://www.sosyalbilimler.hacettepe.edu.tr
Telefon: 0-312-2976860 **Faks:** 0-3122992147 E**-posta**: sosyalbilimler@hacettepe.edu.tr

HACETTEPE UNIVERSITY
GRADUATE SCHOOL OF SOCIAL SCIENCES
ETHICS COMMISSION FORM FOR THESIS

HACETTEPE UNIVERSITY
GRADUATE SCHOOL OF SOCIAL SCIENCES
PRİVATE LAW DEPARTMENT

Date: 16/03/2023

Thesis Title: Legal Responsibility Arising from Obligation to Protect Personal Data

……

My thesis work related to the title above:

1. Does not perform experimentation on animals or people.
2. Does not necessitate the use of biological material (blood, urine, biological fluids and samples, etc.).
3. Does not involve any interference of the body's integrity.
4. Is not based on observational and descriptive research (survey, interview, measures/scales, data scanning, system-model development).

I declare, I have carefully read Hacettepe University's Ethics Regulations and the Commission's Guidelines, and in order to proceed with my thesis according to these regulations I do not have to get permission from the Ethics Board/Commission for anything; in any infringement of the regulations I accept all legal responsibility and I declare that all the information I have provided is true.

I respectfully submit this for approval.

Date and Signature

Name Surname:	Kemal KÜÇÜKKAVRUK
Student No:	N20231734
Department:	Private Law
Program:	Private Law Master's Degree
Status:	☐ MA ☐ Ph.D. ☐ Combined MA/ Ph.D.

ADVISER COMMENTS AND APPROVAL

(Title, Name Surname, Signature)