T.C.

ATILIM ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

KAMU HUKUKU ANABİLİM DALI

KAMU HUKUKU YÜKSEK LİSANS PROGRAMI

5237 SAYILI TÜRK CEZA KANUNU KAPSAMINDA KİŞİSEL VERİLERİN KORUNMASINA YÖNELİK SUÇLAR

Yüksek Lisans Tezi

Hasan Çağrı Şaşmaz

Ankara 2021

T.C.

ATILIM ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

KAMU HUKUKU ANABİLİM DALI

KAMU HUKUKU YÜKSEK LİSANS PROGRAMI

5237 SAYILI TÜRK CEZA KANUNU KAPSAMINDA KİŞİSEL VERİLERİN KORUNMASINA YÖNELİK SUÇLAR

Yüksek Lisans Tezi

Hasan Çağrı Şaşmaz

Tez Danışmanı

Dr. Öğretim Üyesi Ali Tanju Sarıgül

Ankara 2021

KABUL VE ONAY

Hasan Çağrı ŞAŞMAZ tarafından hazırlanan "5237 Sayılı Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunmasına Yönelik Suçlar" başlıklı bu çalışma, 23/09/2021 tarihinde yapılan savunma sınavı sonucunda başarılı bulunarak jürimiz tarafından Kamu Hukuku Anabilim Dalında Yüksek Lisans Tezi olarak oy birliği ile kabul edilmiştir.

Doç. Dr. Ahmet BOZDAĞ (Başkan)

Dr. Öğr. Üyesi Ali Tanju SARIGÜL (Danışman)

Dr. Öğr. Üyesi. Altın Aslı ŞİMŞEK ÖNER (Üye)

Prof. Dr. Dilaver TENGİLİMOĞLU

Enstitü Müdürü

ETİK BEYAN

Atılım Üniversitesi Sosyal Bilimler Enstitüsü Tez Yazım Yönergesi'ne uygun olarak hazırladığım bu tez çalışmasını;

- Akademik ve etik kurallar çerçevesinde hazırladığımı,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmasında yararlandığım eserlerin tümüne atıfta bulunarak kaynak gösterdiğimi,
- Bu tezde sunduğum çalışmanın özgün olduğunu bildirir,

Aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

[13/10/2021]

Hasan Çağrı ŞAŞMAZ

ÖZ

ŞAŞMAZ, Hasan Çağrı. 5237 Sayılı Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunmasına Yönelik Suçlar, Yüksek Lisans Tezi, Ankara, 2021.

20. yüzyılın son çeyreğinden itibaren bilgisayar teknolojisinin gelişmesi ve internet ağının dünya genelinde çok hızlı bir şekilde yayılması, birey ve kurumları, sahip oldukları bilgi ve verileri kaydetme, koruma ve saklama konusunda tedbirler almaya sevk etmiştir. Kişisel verilerin korunması, sadece tek bir devletin gayret ve çabası ile mümkün olamayacağı anlaşılınca bu korumanın uluslararası düzeyde yapılması gereği ortaya çıkmış ve bu anlamda birçok tartışma ve çalışmalar yapılmıştır. Bu çalışmalarda kişisel verilerin korunması, özel hayatın gizliliği hakkı çerçevesinde koruma altına alınmıştır. Fakat teknolojik gelişmelere paralel olarak kişisel verilerin korunması hakkı da o denli önemli hale gelmiştir. Dolayısıyla kişisel verilerin korunması hakkının temel hak ve özgürlükler içinde dolaylı korumadan çıkarılarak kendi adıyla doğrudan bir koruma sağlanması çalışmaları hız kazanmıştır.

Kişisel veriler, bağımsız bir kanun çıkarılmadan önce uluslararası ve ulusal alanda çeşitli hukuki metinlerle koruma altına alınmıştır. Ülkemizde kişisel veriler, 2016 yılında mevzuatımıza dâhil edilen 6698 sayılı Kişisel Verilerin Korunması Kanunu ile koruma altına alınmıştır. Bu Kanun, kişisel verilerin korunmasıyla ilgili temel kaynaktır. Bu Kanun, kişisel verilerle ilgili suçlara ilişkin olarak "5237 sayılı Türk Ceza Kanunu"na atıf yapmaktadır.

Bu çalışma kapsamında, yargı kararları ve uluslararası düzenlemelerden de yararlanarak, kişisel veri kavramını açıklamak, korunmasının önemini ortaya koymak ve ülkemizdeki kişisel verilerin korunmasına yönelik ceza kanununda belirlenen adli ceza içeren düzenlemelerin incelenmesi sırasında tespit edilen eksiklik veya çelişkilerin giderilmesi için çözüm önerileri sunulmaktadır.

Anahtar Sözcükler: Kişisel Veri, Özel Hayatın Gizliliğinin Korunması Hakkı, Ceza Hukuku, Türk Ceza Kanunu

ABSTRACT

ŞAŞMAZ, Hasan Çağrı. Crimes Committed Against The Protection Against The Protection Of Personal Data Under The Turkish Criminal Law No 5237. Master Thesis, Ankara, 2021.

Since the last quarter of the 20th century, the development on computer technology and the rapid spread of the internet network around the world have prompted individuals and institutions to take measures for recording, protecting and storing their information and data. When it was understood that the protection of personal data could not be possible with the effort of only single state, it was revealed that this protection should be done at an international level and many discussions and studies in this regard were carried out. In these works, the protection of personal data is mostly made within the framework of the right to privacy. However, the right to protect personal data in parallel with technological developments has become more important. Therefore, the right to protect personal data under the umbrella of fundamental rights and freedoms has been transformed into protection under its own name.

Before a special law regarding the protection of personal data was enacted, they were protected by various legal texts both in the international arena and in our country. Personal data in our country are protected by the Personal Data Protection Law No.6698, which was included in our legislation in 2016. This Law is the main source for the protection of personal data. This Law has made reference to the Turkish Penal Code No.5237 in terms of crimes related to personal data.

The purpose of this study is to explain the concept of personal data, to reveal the importance of protection of personal data, by making use of comparative law, judicial decisions and international regulations, and to offer solutions to eliminate the deficiencies or contradictions wstablished during the examination of the regulations

containing judicial punishment determined in the penal code for the protection of personal data in our country.

Keywords: Personal Data, Right to Privacy, Criminal Law, Turkish Penal Code.

İÇİNDEKİLER

İKİNCİ BÖLÜM

KİŞİSEL VERİLERİN KORUNMASINA YÖNELİK ULUSLARARASI VE ULUSAL DÜZENLEMELER

ÜÇÜNCÜ BÖLÜM

TÜRK CEZA KANUNU'NDA KİŞİSEL VERİLERİN KORUNMASINA YÖNELİK SUÇLAR

KISALTMALAR

age : Adı geçen eser

agm : Adı geçen makale

agt : Adı geçen tez

AB : Avrupa Birliği

ABAD : Avrupa Birliği Adalet Divanı

ABD : Amerika Birleşik Devletleri

ABTHŞ : Avrupa Birliği Temel Haklar Şartı

AİHM : Avrupa İnsan Hakları Mahkemesi

AİHS : Avrupa İnsan Hakları Sözleşmesi

AK : Avrupa Konseyi

APEC : Asya Pasifik Ekonomik İşbirliği

AT : Avrupa Topluluğu

AYM : Anayasa Mahkemesi

B : Baskı

BDSG : Alman Veri Koruma Kanunu

Bkz : Bakınız

BM : Birleşmiş Milletler

C : Cilt

CD : Ceza Dairesi

CHD : Ceza Hukuk Dairesi

CMK : Ceza Muhakemesi Kanunu

İDDK : İdari Dava Daireleri Kurulu

EHK : Elektronik Haberleşme Kanunu

E.T : Erişim Tarihi

E : Esas

HGK : Hukuk Genel Kurulu

K : Karar

KVKK : Kişisel Verileri Koruma Kanunu

LDP : Verilerin Korunmasına İlişkin Federal Kanun

M : Madde

MERNİS : Merkezi Nüfus İdaresi Sistemi

OECD : Ekonomik İşbirliği ve Kalkınma Teşkilatı

PVSK : Polis Vazife ve Salahiyet Kanunu

RG : Resmi Gazete

s : sayfa

S : Sayı

T : Tarih

TBK : Türk Borçlar Kanunu

TCK : Türk Ceza Kanunu

TDK : Türk Dil Kurumu

TMK : Türk Medeni Kanunu

vd : ve devamı

ÖNSÖZ

20. Yüzyılın son çeyreğinden itibaren bilgisayar teknolojisinin gelişmesi ve internet ağının dünya genelinde çok hızlı bir şekilde yayılması, birey ya da kurumları, sahip oldukları bilgi ve verileri koruma ve saklama konusunda tedbirler almaya sevk etmiştir. Kişisel verilerin korunması, sadece tek bir devletin gayret ve çabası ile mümkün olamayacağı anlaşılınca bu korumanın uluslararası düzeyde yapılması gereği ortaya çıkmıştır. Bu çalışma ile Kişisel Verilerin Korunmasına yönelik dünya genelindeki hukuki düzenlemelere ek olarak ülkemizde yapılan çalışmalar da incelenmiştir. Ülkemizde yapılan düzenlemeler genelde Avrupa Birliğine uyum çerçevesinde yapılmış, bu alanda önemli bir mesafe kat edilmiştir. Bu çalışma ile 5237 sayılı Türk Ceza Kanunu kapsamında kişisel verileri korumaya yönelik suçlar ortaya konmaya çalışılmıştır.

Bu vesile ile öncelikle danışmanım olmayı kabul eden ve daha sonra tez konusunun belirlenmesinden sonuçlanmasına kadar geçen süreç boyunca her aşamada yardım ve desteğini esirgemeyen, çalışmanın tamamını okuyarak yaptığı eleştirilerle tezin bu hale gelmesini sağlayan danışman hocam Sayın Dr. Öğr. Üyesi Ali Tanju Sarıgül'e teşekkür ediyorum.

Ayrıca bu günlere gelmem için maddi ve manevi olarak çabalarını hiçbir zaman esirgemeyen başta babam Prof. Dr. Musa Şaşmaz olmak üzere annem Funda ve ablam Dr. Kübra Şaşmaz'a, çalışmayı hazırlarken desteğini her zaman hissettiren, yorulduğumda beni motive etmekten usanmayan değerli meslektaşım Av. Su Sümeyra Yılmaz'a sevgi ve şükranlarımı sunuyorum.

Hasan Çağrı ŞAŞMAZ

Niğde-2021

GİRİŞ

Eski dönemlerde daktilo veya elle kâğıda aktarılarak kaydedilen veriler, günümüz teknolojisiyle birlikte gerek cep telefonları, gerek bilgisayarlar vasıtasıyla depolanabilir, hatta saniyeler içerisinde kıtalararası bile paylaşılabilir hale gelmiştir. Bu durum her ne kadar kişilerin hayat standartlarını artırıyor olsa da, veri sahibi kişinin rızası olmaksızın paylaşılması ile sonuçlanabilmektedir. Bu durum kişiyi topluma karşı korumasız hale getirmekte, temel hak ve özgürlüklerinin ihlaline yol açabilmektedir. Örneğin bir iş başvurusu için bırakılan özgeçmişte veya siparişin ulaştırılması için paylaşılan adres bilgisinde olduğu gibi hayatın birçok alanında önümüze çıkan kişisel verilerin, ekonomik kazanç veya kişiye zarar verme gibi çeşitli amaçlarla kaydedilmesi veya üçüncü kişilerin erişimine açılması mümkündür. Bu durumda kişinin özel hayatının gizlilik alanı daralacak, hak ve menfaatleri zarara uğrayacaktır.

Kişisel verilerin öneminin evrensel olarak artmasıyla birlikte bu alanın uluslararası ve ulusal düzenlemelerle korunması gerekliliği doğmuştur. Ülkemiz bu alana ilişkin düzenlemelerde Avrupa devletlerine nazaran geç kalmakla birlikte, 12 Eylül 2010 tarihinde yapılan referandumla Anayasa'nın 20. maddesine eklenen 3. fıkrayla[1] birlikte kişisel veriler Anayasal olarak güvence altına alınmıştır. 24 Mart 2016 tarihinde kabul edilen 6698 sayılı Kişisel Verilerin Korunması Kanunu[2] kişisel verilerin korunması hakkına ilişkin özel bir kanuni düzenleme olarak yürürlüğe

[1] "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 islenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."

[2] Resmî Gazete Tarihi: 07.04.2016, Sayı: 29677. Bundan sonraki bölümlerde KVKK olarak adlandırılacaktır.

girmiştir. KVKK, "Suçlar ve Kabahatler" bölümünde kişisel verilerle ilgili bir ihlal durumunda adli[3], idari[4] ve disiplin[5] cezalarına ilişkin hükümlere yer vermiştir.

Bu tezin amacı, yargı kararları ve uluslararası düzenlemelerden de yararlanarak, kişisel veri kavramını açıklamak, korunmasının önemini ortaya koymak ve ülkemizdeki kişisel verilerin korunmasına yönelik Türk Ceza Kanunu'nda belirlenen adli ceza içeren düzenlemelerin incelenmesi sırasında tespit edilen eksiklik veya çelişkilerin giderilmesi için çözüm önerileri sunmaktır.

Bu amaca yönelik olarak ve tümdengelim yöntemi esas alınarak, öncelikle kişisel veri kavramı ve hukuki niteliği incelendikten sonra, belirtilen adli ceza içeren hükümlerin altyapısını oluşturan uluslararası düzenlemelerin incelemesi yapıldıktan sonra suç tiplerine dair açıklamalara yer verilecektir.

Yapılan açıklamalar ışığında çalışmamızın birinci bölümünde, tezin kavramsal temelini oluşturması sebebiyle, kişisel veri ve tanımı üzerinde durularak, kişisel veriyle ilgili kavramlar, kişisel verilerin korunması hakkının ne olduğu, neden ihtiyaç duyulduğu, bu ihtiyacın tarihsel gelişimi ve hukuki niteliği, kişisel verilerin korunması ve işlenmesine yönelik ilkeler konuları incelenmiştir.

Çalışmamızın ikinci bölümünde, kişisel verilerin korunması hakkı ve bu hakla ilişkili olan özel hayatın gizliliği hakkı ile ilgili uluslararası düzenlemeler incelenmiştir. Bu kapsamda OECD, Birleşmiş Milletler, Avrupa Konseyi ve Avrupa

---

[3] KVKK madde 17 "(1) Kişisel verilere ilişkin suçlar bakımından 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununun 135 ila 140 ıncı madde hükümleri uygulanır.
(2) Bu Kanunun 7 nci maddesi hükmüne aykırı olarak; kişisel verileri silmeyen veya anonim hâle getirmeyenler 5237 sayılı Kanunun 138 inci maddesine göre cezalandırılır."

[4] KVKK madde 18/1 "Bu Kanunun;
a) 10 uncu maddesinde öngörülen aydınlatma yükümlülüğünü yerine getirmeyenler hakkında 5.000 Türk lirasından 100.000 Türk lirasına kadar,
b) 12 nci maddesinde öngörülen veri güvenliğine ilişkin yükümlülükleri yerine getirmeyenler hakkında 15.000 Türk lirasından 1.000.000 Türk lirasına kadar,
c) 15 inci maddesi uyarınca Kurul tarafından verilen kararları yerine getirmeyenler hakkında 25.000 Türk lirasından 1.000.000 Türk lirasına kadar,
ç) 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, idari para cezası verilir."

[5] KVKK madde 18/3 "Birinci fıkrada sayılan eylemlerin kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları bünyesinde işlenmesi hâlinde, Kurulun yapacağı bildirim üzerine, ilgili kamu kurum ve kuruluşunda görev yapan memurlar ve diğer kamu görevlileri ile kamu kurumu niteliğindeki meslek kuruluşlarında görev yapanlar hakkında disiplin hükümlerine göre işlem yapılır ve sonucu Kurula bildirilir."

Birliği gibi ulus üstü örgütlerin kişisel verilerle ilgili düzenlemeleri değerlendirilmiştir. Buna ek olarak ulusal mevzuatımızda kişisel verilere ilişkin düzenleme yapılmış kanunlar incelenmiştir.

Çalışmamızın üçüncü bölümünde ise, Türk Ceza Kanunu kapsamında kişisel verileri korumaya yönelik olarak düzenlenen "kişisel verilerin kaydedilmesi", "verileri hukuka aykırı olarak verme veya ele geçirme", "verileri yok etmeme" suçları Anayasa Mahkemesi ve Yargıtay kararlarına ek olarak öğretideki görüşlerden de yararlanılarak teorik ve pratik açıdan değerlendirilmiştir.

BİRİNCİ BÖLÜM

KİŞİSEL VERİLERİN KORUNMASINA YÖNELİK KAVRAMLAR VE İLKELER

1.1.Kişisel Verilerin Korunmasına Yönelik Kavramlar

1.1.1.Kişisel veri kavramı

Kişisel veri kavramının açıklanabilmesi için öncelikli olarak "kişisel" ve "veri" kavramlarının ne anlama geldiği hakkında bilgi vermek gerekmektedir. "Türk Dil Kurumu"nun sitesinde kişisel kavramı "*Kişi ile ilgili, kişiye ilişkin, kişinin kendi malı olan, şahsi, zati*" şeklinde tanımlanmaktadır.[6] "Kişisel" kavramından çok "veri" kavramı çok karmaşık ve tartışmalıdır. TDK "veri" kavramını "bilgi" (information) ile aynı anlama geldiğini iddia etse de, bu iki kavram arasında epey bir anlam farkı olduğu açıktır. Ancak uygulamada, öğreti ve bu konudaki hukuki düzenlemelerde bahsi geçen iki kavram aynı şekilde değerlendirilmektedir. Kişisel veri kavramının İngilizcesi "personal data"dır. Dolayısıyla kişisel verideki veri kavramı, "bilgi (information)" kelimesinden ziyade "veri (data)" kelimesiyle daha çok örtüşmektedir. Aslında verinin sadece sonuç çıkarabilecek olgu, bilgi ve sayılardan ibaret olduğu, bilgisayar ortamında işlenebilen ham materyali nitelendirmekte kullanıldığı beyan edilmektedir.[7]

Genel olarak kişisel veri "kişiyi kişi yapan" her türlü bilgi olarak tarif edilebilir.[8] Diğer bir ifadeyle insanın insan olarak evrendeki yerini alması ve toplumdaki konumu, insana bağlı değerleri kişisel veri haline getirir; örneğin kişinin ismi, adresi, sağlık durumu, cinsel eğilimleri gibi özellikler o kişinin kişisel verisini oluşturmaktadır. Fakat 20. yüzyılın sonu ve 21. yüzyılın başında bilim ve teknolojide meydana gelen gelişmeler topluma ve toplumu oluşturan bireylere yeni bilgiler

---

[6]Türk Dil Kurumu (TDK), Güncel Türkçe Sözlük, (https://sozluk.gov.tr), Erişim Tarihi (E.T.) 08.01.2021.

[7]Elif Küzeci, **Kişisel Verilerin Korunması**, 4. Baskı, On İki Levha Yayıncılık, İstanbul, 2020, s. 10-11.

[8]Selami Hatipoğlu, "Kişisel Verilerin Korunması ve İdarenin Sorumluluğu", Trakya Üniversitesi Sosyal Bilimler Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, Edirne, 2019, s. 6-8, Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin Korunması Kanunu ve Getirdikleri**, Yayın No: 26, s. 2 ve Kişisel Verileri Koruma Kurumu, **6698 Sayılı Kanunda Yer Alan Temel Kavramlar**, s. 9-10. www.kvkk.gov.tr. E.T. 12.01.2021.

yüklemiştir. Bu bilgiler de kişilere yeni kişisel veriler olarak eklenmiştir. Bu verilere bireysel cep telefonu numarası, e-mail adresi, vatandaşlık numarası gibi örnekler verilebilmektedir. Yukarıda verilen bilgiler doğrultusunda kişisel veriler iki sınıfa ayrılabilmektedir. Bunlardan ilki insanın varoluşundan kaynaklı kişiliğine dair bilgiler, diğeri ise modern toplumun insanda bulunmasını gerektiren ya da çeşitli hizmetlere ulaşımına imkân veren bireysel bilgilerdir. Bu ikili ayrımdan birinin diğerine karşı bir üstünlüğü veya önceliği yoktur. Kişisel veri olarak her ikisi de aynı önemde değere sahiptir.[9]

Kişisel veri; uluslararası belgelerde veya ülkelerin ulusal mevzuatlarında ve "Türk Ceza Kanunu"nun 135. maddesinde düzenlenen "kişisel verilerin kaydedilmesi suçu"nun gerekçesinde, "*belirli ya da belirlenebilir nitelikteki bir kişiye ilişkin her türlü bilgi"* şeklinde tanımlanmıştır. Teoride bu anlama gelse de pratikte kişisel veri kavramının sınırlarını tespit etmek o kadar da kolay değildir. Ulusal mevzuatımıza dâhil olan "6698 sayılı Kişisel Verilerin Korunması Kanunu" ise kişisel veriyi "*kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi*" olarak tanımlamıştır. Bu tanıma ek olarak "Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD)"nın "Mahremiyetin ve Kişisel Verilerin Sınırlararası Aktarımının Korunması Hususunda Rehber İlkeleri"nin 1. maddesinde ve "108 sayılı Kişisel Verilerin Otomatik İşlenmesine İlişkin Olarak Bireylerin Korunması Hakkındaki Avrupa Konseyi Sözleşmesi"nin 2/a maddesinde "tanımlanmış veya tanımlanabilir gerçek bir kişiyle ilgili herhangi bir bilgi" şeklinde yapılmıştır. "*Belirlenebilir bir kişi, özellikle fiziksel, zihinsel, fizyolojik, ekonomik, sosyal ve kültürel kimliğine özgü bir kimlik numarası ile veya bir ya da daha fazla faktör referans alınarak doğrudan veya dolaylı şekilde tanımlanabilen kişi"*dir.[10] Kişisel verilerin korunması amacına yönelik yapılan yasal düzenlemelerin birçoğunun temeli olan 1995 tarihli ve "95/46/AT sayılı Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Hakkındaki Avrupa Birliği Konseyi ve Avrupa Parlamentosu Direktifi"nde ise kişisel veri, "belirlenmiş veya belirlenebilir gerçek kişiye ilişkin

[9] Murat Volkan Dülger, **Kişisel Verilerin Korunması Hukuku**, 3. Baskı, Hukuk Akademisi Yayınları, İstanbul, 2020, s. 61 ve Hayrunnisa Özdemir, **Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması**, 1. Baskı, Seçkin Yayıncılık, Ankara, 2019, s.123-126.
[10] Şeyma Sert, **Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması**, 1. Baskı, Seçkin Yayıncılık, Ankara, 2019, s. 21-22.

bütün bilgileri ifade eder" denilmektedir[11] ve yukarıda 108 sayılı Avrupa Sözleşmesi'ndeki tanımın hemen aynısı tekrar edilmiştir.

Avrupa Birliği (AB) düzenlemelerinden olan ve Kişisel Verileri Koruma Kanunu'na esas teşkil eden, 25 Mayıs 2018 tarihli, "Avrupa Veri Koruma Tüzüğü", 1995 tarihli AB 95/46/EC Sayılı Direktifi'nin yerini almış en temel ve güncel metinleri kapsamaktadır. Bu ve "Genel Veri Koruma Tüzüğü"nde kişisel verinin tanımı paralellik göstermektedir. Bu tanıma nelerin kişisel veri olarak gireceği hususu örneklerle açıklanmıştır.[12] Bunu açıklamak gerekirse, kişinin belirlenebilir kılınması, verilerin doğrudan ya da dolaylı olarak bir gerçek kişiyle ilişkilendirilmesi suretiyle kişinin tanımlanabilmesi, diğer bir ifade ile kişinin o kişi olduğunun ortaya çıkarılabilmesi özelliğini ifade etmektedir. Örneğin kişinin psişik, psikolojik, fiziksel, ekonomik, kültürel veya sosyal kimliğini ifade eden öğeleri, bir kimsenin kimliği, sağlık durumu, eğitim durumu, dini tercihi, etnik kökeni, ikametgâh adresi, bilgilerinin bir ya da birden fazla unsuruna dayanarak tanımlanabilen gerçek kişilere ilişkin herhangi bir bilgi, kişisel veri kapsamına dâhil edilebilmektedir. Başka bir ifade ile isim, telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, ses, parmak izleri ve genetik bilgiler gibi kişiye özgü spesifik bilgiler ile doğrudan değil ama dolaylı olarak kişiyi belirlenebilir kılan yaş, meslek, medeni durum, adres vb. nitelemeler kişisel veri olarak ele alınmaktadır.[13] Teknolojik gelişmelerin de etkisiyle bir süre sonra bu tanıma konum verileri, genetik bilgi ve çevrimiçi kimlik tanımlayıcıları da dâhil edilmiştir.

---

[11] Özdemir, age, s. 150.

[12] Oğulcan Özkan, **Kişisel Verilerin Korunması**, Yetkin Yayınları, Ankara, 2020, s. 6-7; Sert, age, s. 22 ve A. Çiğdem Ayözger Öngün, **Kişisel Verilerin Korunması Hukuku, Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dâhil**, Genişletilmiş 2. Baskı, Beta Yayıncılık, İstanbul, 2019, s. 5.

[13] Nilgün Başalp, **Kişisel Verilerin Korunması ve Saklanması**, Yetkin Yayınları, Ankara, 2004, s. 22 ve 33-34; Dülger, age, s. 63 ve 158; Alaattin Bük, **Bilişim Alanında Kişisel Verilerin Korunması**, 1. Baskı, Seçkin Akademik ve Mesleki Yayınları, Ankara, 2018, s. 33-34; Murat Uygun, "Avrupa Birliği'nin 95/46 Sayılı Veri Koruma Yönergesi Işığında Kişisel Verilerin Korunması", Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, Ankara, 2010, s. 43; Metin Çokmutlu, "Türk Ceza Hukukunda Kişisel Verilerin Korunması", Kocaeli Üniversitesi, Sosyal Bilimler Enstitüsü, Yayımlanmamış Doktora Tezi, Kocaeli, 2014, s. 27-28 ve İbrahim Korkmaz, **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, 2. Baskı, Seçkin Akademik ve Mesleki Yayınları, Ankara, 2019, s. 25-30.

Bilgisayar ve internetin icat edilmesi ve dünya genelinde her yerde kullanılır hale gelmesiyle, bilgisayarlarda bulunan bilgi ve verilerin korunması ve başkalarının bu verilere ulaşımının engellenmesi gereğini ortaya çıkarmıştır. Üstelik bu bilgilere ulaşımın kolay ve mümkün olması, kendisi lehine çıkar sağlamak isteyen kötü niyetli insanların iştahını kabartmıştır. Bu durum kişisel verilerin etkin olarak korunması ihtiyacını doğurmuştur.[14] Eğitim, öğretim, ticaret, iletişim, sağlık gibi birçok alan, internete bağlı olarak sürdürülmektedir. Üstelik 2020 ve 2021 yıllarındaki salgın döneminde insanlar her faaliyetini mecburen internet vasıtasıyla yerine getirmektedir. Web sitelerine kayıtlar, tıklama akışlı veriler, casus yazılımlar ve arama motorları vasıtasıyla kişisel veriler bir yerlerde birikmekte ve başkalarının kullanımına fırsat vermektedir. Bu şekilde oluşan kişisel verilerin kötüye kullanımının önüne geçmek ve bunu belirli bir kurallara bağlamak amacıyla hukuk alanında çeşitli adımlar atılması zarureti ortaya çıkmıştır. Kişisel veri tanımının genişliği ve belirsizliği her bir devleti kendi iç hukuku içinde farklı şekilde kapsamını belirlemeye sevk etmiştir. Bu nedenle kişisel verinin kapsam ve genişliği konusunda ulusal mevzuat ve uygulamalarda ülkeler arasında farklılıklar bulunabilmektedir.[15]

1.1.1.1.Kişisel veri kavramının unsurları

Kişisel veri kavramının Kişisel Verileri Koruma Kanunu'nda ve "95/46/AT sayılı Veri Koruma Direktifi"nde düzenlenen ve benimsenen tanımı gereğince "veri" ve "kimliği belirli veya belirlenebilir bir kişi" olmak şeklinde iki unsuru olduğu belirtilmektedir.[16] Ancak farklı birçok görüşe göre de kişisel veri kavramının üç unsurunun bulunduğu ileri sürülmektedir. Bunlar "bilgi", "kimliği belirli veya belirlenebilir kişi" ile "bilginin kişiye ilişkin olması" şeklinde sıralanmaktadır. Bu üç unsura ek "gerçek kişi" olarak dördüncü bir unsurun varlığını savunan öğreti görüşü de mevcuttur. Sözü edilen unsurlar bir arada bulunması şartıyla bir bilgi, kişisel veri olarak kabul görecek veya değerlendirilecektir. Bu çalışmada aşağıda da başlıkları

---

[14] Habip Oğuz, "Elektronik Ortamda Kişisel Verilerin Korunması, Bazı Ülke Uygulamaları ve Ülkemizdeki Durum", **Uyuşmazlık Mahkemesi Dergisi**, Haziran 2014, Sayı:3, s. 3-4.
[15] Zeynel T. Kangal, **Kişisel Verilerin Ceza ve Kabahatler Hukukunda Korunması**, 1. Baskı, On İki Levha Yayıncılık, İstanbul, 2019, s. 20-21.
[16] Sert, age, s. 25 ve Özkan, age, s. 8-9.

görüldüğü üzere üç temel unsur üzerinde durulacak ve bunlarla ilgili ayrıntılar ortaya konacaktır.

1.1.1.1.1.Kişi ile ilgili bir bilginin bulunması

Kişisel veri kavramının ulusal ve birçok uluslararası metinde "*kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi*" şeklinde açıklandığı yukarıda belirtilmiştir. Veri ve bilgi kavramları birbirinin yerine kullanılsa da gerçekte birbirinden farklı anlam taşımaktadırlar. "Türk Dil Kurumu"nun sitesinde yer alan "Güncel Türkçe Sözlüğü"nde veri "*olgu, kavram ya da komutların, iletişim, yorum ve işlem için elverişli biçimli gösterimi*", bilgi ise "*işlemde kullanılan uzlaşımsal kurallardan yararlanarak kişinin veriye yönelttiği anlam veya insan zekâsının çalışması sonucu ortaya çıkan düşünce ürünü, malumat, vukuf*" olarak açıklanmaktadır.[17] İki kavram arasındaki farklarla ilgili ayrıntıya girilmeyecek ve bu iki kavramın başka bir ifadeyle veri ve bilginin, hatta enformasyon kavramının da aynı anlama geldiği[18] farz edilerek konu ortaya konacaktır. Bu tanımdan yola çıkılarak veriyi "her türlü bilgi olarak" ifade etmek mümkün olacaktır. "Her türlü bilgi" kavramının kapsamı oldukça geniştir.[19] Sınırlarının belirlenmesi de oldukça zordur. Bu nedenle kanun koyucu karmaşaya neden olmamak için kişisel verilerin nelerden ibaret olduğunu maddeler halinde saymak yerine, kavramın kapsamının belirlenmesi işini uygulamaya bırakma yolunu seçmiştir.[20]

Kişinin özel hayatı, iş ilişkileri, aile hayatı, sosyal ve ekonomik yaşamına ait bilgiler kişisel veri kapsamına girmektedir. Kişinin telefon, bilgisayar ya da e-mail adresi ve buralarda kullandığı bilgiler kişisel veri niteliğindedir. Bu bilgilerin gizli veya açık, nesnel veya öznel olması kişisel veri olmasında fark yaratmaz. Hatta bizzat kendisi tarafından açığa vurulan bilgilere başkaları tarafından ulaşılsa bile yine de kişisel veri özelliğini korur. Herkesin ulaşabileceği bilgiler de kişisel veri olarak değerlendirilir. Kişinin ortalama gelirinin ne olduğu, hangi saç rengine veya mesleğe

---

[17] https://sozluk.gov.tr/(E.T. 09.01.2021.

[18] Küzeci, age, s. 12-13. Veri, bilgi ve enformasyon arasındaki anlam farklılığı üzerine tartışma ve ayrıntılar için bkz, Dülger, age, s. 152-155.

[19] Gizem Büşra Titrek, "Türk Ceza Hukukunda Kişisel Verilerin Korunmasına Yönelik Suçlar", Bursa Uludağ Üniversitesi, Sosyal Bilimler Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, Bursa, 2020, s. 5 ve Hatipoğlu, age, s. 8-10.

[20] Kangal, age, s. 21 ve Çokmutlu, agt, s. 24-25.

sahip bulunduğu, yardımsever ya da hırslı olup olmadığı gibi kişiden kişiye göre değişen bilgiler kişisel veri olarak algılanmaktadır. Bu verilerin kâğıt üzerinde veya ses, görüntü formunda olması farklılık yaratmamaktadır. Diğer bir ifade ile bilginin nerede ve ne formda olduğunun önemi yoktur. Bunların tamamı kişisel veri olarak muamele görmektedir. Bilgilerin doğru ya da yanlış olması kişisel veri olmasına engel değildir. Üstelik sadece doğru veriler değil, yanlış veriler bile koruma altına alınmıştır.[21]

1.1.1.1.2.Kişinin gerçek kişi olması

Kişisel verinin diğer unsuru verinin gerçek bir kişiye ait olmasıdır. Kişi, "Türk Dil Kurumu Sözlüğü"nde "*şahıs, zat, nefer*", "*kişi ile ilgili, kişiye ilişkin şahsi*" şeklinde tanımlanmaktadır.[22] Hukukta kişi ise "*haklara sahip olma ve borç altına girme ehliyeti bulunan varlık veya fiziki bir varlığı, bilinci ve iradesi olup, irade beyanı ile hukuki sonuç doğurabilen varlıklar*"[23] anlamına gelmektedir. Kişi bir başka yerde ise "hak ehliyeti olan varlık" olarak tarif edilmektedir. Hak ehliyeti ise "hak sahibi olabilme ve borç altına girebilme ehliyeti" olarak tanımlanmıştır. Dolayısıyla hak ehliyeti ile kişinin birbiriyle örtüştüğü görülmektedir.[24] Hukuk düzeninde gerçek ve tüzel olarak ikiye ayrılan kişi olmakla birlikte burada gerçek kişiden anlaşılması gereken insandır. Modern hukuk düzenlemelerinin hemen tamamında tüm insanlar gerçek kişi olarak kabul edilmektedir.[25] Verilerin de bu gerçek kişilere ait olması gerektiği tüm hukuk sistemlerince desteklenmektedir. Bunun nedeni ise kişisel verilerin, bir parçasını oluşturduğu özel yaşamın gizliliği ilkesinin yalnız gerçek kişilere özgü olmasıdır.[26] Dolayısıyla kişisel verilerin korunması sadece gerçek kişilerle sınırlı tutulmuştur. Ancak tüzel kişiler genel olarak koruma dışında tutulmuş olsa bile, bazı hukuk sistemleri tüzel kişiye ait verinin olabileceğini kabul etmektedir.

---

[21] Dülger, age, s. 155-157; Titrek, agt, s. 6-7 ve Korkmaz, age, s. 30-32.
[22] TDK, https://sozluk.gov.tr), (E.T.) 08.01.2021.
[23] Engin Dinç, "Kişisel Verilerin Korunmasında Uluslararası Düzenlemeler ve Türkiye'nin Durumu", Diyarbakır Dicle Üniversitesi, Sosyal Bilimler Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, 2006, s. 14.
[24] Turgut Akıntürk/Derya Ateş, **Medeni Hukuk**, 25. Baskı, Beta Yayınevi, İstanbul, 2019, s. 107.
[25] Serap Helvacı, **Gerçek Kişiler**, 6. Basım, Legal Yayıncılık, İstanbul, 2016, s. 20.
[26] "KVKK'nın 1. Maddesinde bu kanunun amacının kişilerin hak ve hürriyetlerinin korunması olduğu belirtilmektedir. Korunacak hak ve özgürlüklerin başında ise özel yaşamın gizliliği olduğu kanunda açıkça ifade edilmektedir. Bu durumda koruma kapsamına tüzel kişileri almak bu amaca uygun olmayacağı gibi, gerçek kişilere yönelik korumanın zayıflamasına da sebep olacağı ileri sürülmüştür."

Bir başka ifade ile tüzel kişiye ait bir veri gerçek kişileri belirlenebilir kılmaktaysa, gerçek kişilerin verilerinin korunması bağlamında korunması mümkün olarak görülmektedir.[27]

Gerçek kişilerin verilerinin koruma altına alındığı açık olmakla birlikte tüzel kişilerin verilerine dair koruma alanı tartışmalıdır. Bu çerçevede "6698 sayılı Kişisel Verileri Koruma Kanunu"nda tanımı yapılan kişisel verinin yalnız gerçek kişilerden söz etmekte olduğu görülmektedir. Bu kanuna esas oluşturan "OECD Rehber İlkeleri", "Avrupa Konseyi 108 nolu Sözleşme", "Genel Veri Koruma Tüzüğü" ve "Avrupa Birliği Direktifi" gibi uluslararası düzenlemelerde de veri korumasının mevzuatımızda olduğu gibi gerçek kişilere has olduğu vurgusunu yapmaktadırlar. Bu durumda tüzel kişi, koruma alanı dışında kalmaktadır. Ancak yukarıda temas edildiği üzere doğrudan olmasa da dolaylı olarak koruma altına alınabileceği ifade edilmektedir. [28]

Ancak AB tarafından 2002 yılında çıkarılan "2002/58/EC sayılı Elektronik Haberleşme Sektöründe Kişisel Bilgilerin İşlenmesi ve Korunması Direktifi"nde farklı olarak tüzel ve gerçek kişiler korunmaktadır. Diğer bir deyişle elektronik haberleşme sektörüyle ilgili işlenen bir verinin sahibinin gerçek veya tüzel olduğuna bakılmaksızın kişisel veri kapsamında değerlendirileceği hükmedilmiştir. 2016 yılında kanunlaşan 6698 sayılı KVKK, sadece gerçek kişilerin verilerini koruma altına almakta, tüzel kişileri bu korumanın dışında tutmaktadır. [29]

Burada tartışılması gereken bir diğer husus da ölü veya ceninin kişisel veri korumasından faydalanıp faydalanamayacağı sorusudur. TMK 28. maddesince "*kişilik tam ve sağ doğmakla kazanılmakta ve ölümle sona ermektedir*." hükmü yer almaktadır. Dolayısıyla bir kişinin, kişisel verinin koruma alanı tam ve sağ doğumla dâhil olup, ölümle bu korumanın son bulacağı ifade edilmektedir.[30] Kişisel veri kavramının ölmüş kişilerle ilgili nasıl değerlendirileceğine dair farklı düzenlemeler söz konusudur. Öldükten sonra kişilerin tıbbi verilerinin saklanacağına ve korumanın devam

[27] Sedat Erdem Aydın, **AİHM İçtihatları Bağlamında Kişisel Verilerin Kaydedilmesi Suçu**, İstanbul, 2015, s. 9; Kangal, age, s. 28.
[28] Özkan, age, s. 12.
[29] Başalp, age, s. 27-35 ve Kader Sarıusta, "Kişisel Verilerin Ceza Hukuku Yoluyla Korunması", Gaziantep Üniversitesi, Sosyal Bilimler Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, Gaziantep, 2018, s. 9.
[30] Özkan, age, s. 13-14.

edeceğine dair düzenlemeler olsa da bunun uygulanması ülkeden ülkeye değişmektedir. Nitekim İngiltere'de yalnızca yaşayan kişilere ilişkin kişisel veriler korunurken, Kanada'da kişinin ölümünü takip eden yirmi yıl boyunca verilerinin açıklanamayacağına dair hüküm getirilmiştir. Ölen kişinin verilerinin açıklanması, gelişen tıp teknolojileri ile ölen kişiye ek olarak soyunda da olabilecek bir hastalığı hakkında bilgi sahibi olunmasına yol açılabileceği, dolayısıyla bu durumun tehlikeli olabileceğinin değerlendirilmesi sonucu bu hususa ilişkin düzenlemeye yer verilmiştir.[31]

1.1.1.1.3.Kişinin kimliği belirli veya belirlenebilir olması

"Kişinin belirlenebilir olması", gerçek kişiyle veri arasında doğrudan veya dolaylı bağ kurulabilmesini, ilgili verinin ilgili gerçek kişiye ilişkin olduğunun ortaya çıkarılmasını ifade eder.[32] Bir başka ifadeyle kişinin belirli olması, kişinin adı, soyadı, kimlik numarası gibi verilerle kişinin kimliğinin doğrudan ortaya çıkarılması demektir. Karışık işlemlere gerek duymadan doğrudan bir kişi ile bağlantı kurmayı mümkün kılan veriler belirli kişilere ilişkindir.[33]

Kişiyi belirli kılan en önemli unsur hiç kuşkusuz adıdır. Bunun yanında çok sayıda unsur da kişiyi belirleyebilir veya belirlenebilir kılabilir. Örneğin verilerin kimlik numarası ile ilişkilendirilmesi veya veri kavramı başlığı altında sıraladığımız kişinin psikolojik, ekonomik, fiziksel kimliği gibi kişiye özel bir içerik taşıması kişiyi belirli bir hale getirebilir ya da onun belirlenmesini sağlayabilir. Bir kimsenin kimliği, sağlık durumu, eğitim durumu, genetiği, dini tercihi, siyasi parti üyeliği, dernek üyeliği gibi bilgiler, kişinin kimliğini belirli hale getirebilir veya onun belirlenebilir olmasını sağlayabilir.[34]

Bir kişinin belirli ya da belirlenebilir kılınmasında belirliliği sağlayacak unsurların neler olduğuna ilişkin kesin bir liste çıkarılması mümkün değildir. Genel

---

[31] Sabire Sanem Yılmaz, "Tıp Alanında Kişisel Verilerin Hukuka Aykırı Olarak Verilmesinin Ceza Hukuku Açısından Değerlendirilmesi (Sır Saklama Yükümlülüğü Kapsamında)", Bahçeşehir Üniversitesi, Sosyal Bilimler Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, İstanbul, 2014, s. 24.
[32] Dülger, age, s. 157-158; Bük, age, s. 34 ve Başalp, age, s. 16.
[33] Oğuz Şimşek, **Anayasa Hukukunda Kişisel Verilerin Korunması**, Beta Yayınları, Ankara, 2008, s. 122 ve Hatipoğlu, age, s. 10-11.
[34] Başalp, age, s. 33-34; Dülger, age, s. 157-158 ve Çokmutlu, agt, s. 27-28.

Veri Koruma Tüzüğü (GVKT), kişiyi belirli kılabilecek temel unsurları, isim, kimlik numarası, konum bilgisi, çevrimiçi unsurlar örnek olarak sayılmış olmakla birlikte, bunlar sınırlı sayıda değildir. Kişi ile alakalı doğrudan ve ekstra bir çaba sarf etmeden o kişiyi belirlemeye yarayan bazı unsurlar olabilir. Bunlar doğrudan ve dolaylı belirleyici unsurlar olarak ikiye ayrılabilir. Doğrudan belirleyici unsurların başında şüphesiz ki kişinin ismi gelir. Ancak bunun dışındaki bazı unsurlar da doğrudan belirleyici görevi görebilirler. Burada önemli olan kişinin başka bir bilgiyle birlikte değerlendirme yapmak zorunda kalmaksızın belirlenmesi diğer bir deyişle diğerlerinden ayırt edilmesidir. Dolaylı belirleyici unsurlar ise gerçek kişinin doğrudan kim olduğunu ortaya çıkarmasa da başka verilerle birleşerek, verinin kime ait olduğunun anlaşılmasına neden olabilen unsurlardır. Bu kriteri sağlayan her türlü veri kişiyi doğrudan belirli ya da belirlenebilir kılmış olur. Kişinin doğrudan belirleyici olmayan veriyle dolaylı olarak belirlenmesinde eldeki verinin başka verilerle eşleştirilmesi ya da tamamlanması gerekmektedir. Burada farklı bilgiler bir arada kullanılarak kişi belirli hale getirilebilir.[35]

1.1.1.2.Hassas veri

Hassas veri de, aslında bir kişisel veridir, ancak bunların bazen "özel koruma gerektiren veri" veya "özel tür veri" şeklinde sınıflandırıldığı görülmektedir. Bu tür kişisel veriler, diğer verilerle mukayese yapıldığında korunması ve muhafaza edilmesi daha önemli olan veriler olarak değerlendirilmektedir. Başka bir deyişle, belirli sosyal ve politik sorunlar nedeniyle, yasa koyucular bu tür veriler üzerinde etkiye sahiptir. Konusunun bireylerin temel hakları, özgürlükleri ve mahremiyetleri ile ilgili olduğu düşünüldüğünde, diğer kişisel verilerden farklı olarak daha katı korumalara tabidirler.[36] Hassas olan verilerin açıklanması halinde söz konusu kişinin toplumda ayrımcılığa uğrayacağı veya ötekileştirileceğinden kaygı duyulmuştur. Hassas veri olarak değerlendirilen verilerin ortak özelliği, açıklanması durumunda hassas veriyi taşıyan kişinin bulunduğu toplumda ayrımcılığa maruz kalacağı endişe ve korkusudur. Üstelik bu tür verilerin olumsuz etkisinin sadece kendisine değil, çevresine de sirayet edeceği, etkisinin de kısa değil uzun süreli ve geri döndürülemez nitelikte olacağından

[35] Dülger, age, s.159.
[36] Korkmaz, age, s. 50-53; Özdemir, age, s. 126 ve Hatipoğlu, age, s. 79-80.

endişe edilmiştir. Bu nedenle hangi tür verilerin bu kategoriye gireceği liste şeklinde sayılmıştır.[37]

Bu kategoriye giren veriler, Avrupa Hukuk Mevzuatında "95/46/AT sayılı AB Yönergesi"nin 8. maddesi, 108 sayılı AK Sözleşmesi'nin 6. maddesi, Birleşmiş Milletler Rehber İlkeleri 5. İlkesi tarafından belirli bir güvence ve koruma sağlamıştır. Buna karşılık OECD Rehber İlkeleri'nin 5. İlkesi ve APEC (Asya Pasifik Ekonomik İşbirliği)'in Çerçeve Belgesi özel bir koruma getirmemektedir. Türk Hukuk Sisteminde ise KVKK'nın 6. maddesi, TCK'nın 135. maddesi, maddeler halinde sıralanmıştır. Dolayısıyla "*ırk ve etnik köken, ahlaki yönelim, siyasi görüş, dini ve felsefi inanç, sendika veya vakıf üyeliği, sağlık veya cinsel tercihle ilgili verilerin*" hassas veri olduğu ve yüksek koruma gerektirdiği öngörülmektedir.[38]

"108 Sayılı Avrupa Konseyi Sözleşmesi"nin "Özel Veri Kategorileri" başlıklı 6. maddesinde, iç hukuk gerekli koruma önlemleri sağlamadıkça, etnik köken, siyasi görüşler, din veya diğer inançlar, sağlık veya cinsel yaşam ve adli sicil kayıtlarına ilişkin kişisel verilerin işlenemeyeceğine karar verilmiştir. "95/46/AT Sayılı Avrupa Birliği Yönergesi"nin "Özel Kategorideki Verilerin İşlenmesi" başlıklı 8. maddesi 1. fıkrasında da "ırksal veya etnik köken, politik düşünceler, dini veya felsefi inançlar, sendika üyelikleri, sağlık ve cinsel yaşamları ile ilgili kişisel verilerin işlenmesinin yasaklandığı"na karar verilmiştir. Veri koruma kanunlarına sahip olan ülkeler bu verileri hassas veri olarak kabul etmiş ancak hassas verinin kapsamı ülkelere göre değişiklik göstermiştir.[39]

"Kişisel Verileri Koruma Kanunu"nun 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 tedbirleri ile ilgili verileri ile biyometrik ve genetik verileri" "hassas veri" olarak tahdidi sayılmıştır. Burada sayılmayan herhangi bir veri, özel nitelikli olmayan bir başka deyişle genel nitelikli veri olarak kabul edilecektir. TCK'nın 135. maddesindeki hassas verilerin "*Kişilerin, siyasi, felsefi veya dini görüşlerine, ırki*

[37] Hüseyin Can Aksoy, **Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması**, Ankara, 2010, s. 30-32; Sarıusta, agt, s. 14 ve Özdemir, age, s. 126-127.
[38] Küzeci, age, s. 277-278; Bük, age, s. 38-40; Hale Akdağ, T**ürk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması**, Adalet Yayınevi, Ankara, 2013, s. 29-34 ve Sert, age, s. 42-44.
[39] Korkmaz, age, s. 52-53.

kökenlerine, hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin belgeler" şeklinde belirtilmektedir. TCK'daki düzenlemeler ile uluslararası düzenlemeler farklılık göstermektedir. Uluslararası mevzuatta "108 sayılı Avrupa Konseyi Sözleşmesi" hariç etnik köken hassas veri kapsamına dâhil edilmiştir. Buna karşılık TCK'da etnik kökene yer verilmemiş, bunun yerine ahlaki eğilimleri hassas veri olarak düzenlenmiştir.[40]

Hassas verilerin işlenmesi yasağının bazı istisnaları bulunmaktadır. Bunlar genel olarak ilgilinin kendi rızasıyla veya kendisinin hassas verilerini bizzat kamuya açıklaması, ya da hayati çıkarların korunması, kamuya yararlı kurum kuruluşlar tarafından işlenme ve yargılama nedeniyle işlenebilmektedir. KVKK'nın "Hassas Kişisel Verilerin İşlenme Şartları" başlıklı 6. maddede hassas verilerin işlenmesini belirleyen şartlar düzenlenmektedir. Bu maddenin 3. fıkrasına göre "*sağlık ve cinsel hayat dışındaki ırk, etnik köken, siyasi düşünce, felsefi inanç, din, mezhep ya da diğer inançlar, kılık ve kıyafet, dernek, vakıf veya sendika üyeliği, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili veriler ile biyometrik ve genetik veriler; kişilerin açık rızası aranmaksızın kanunlarda öngörülen hallerde işlenebilir*" denmektedir.[41]

1.1.1.3.Diğer kavramlar

Yukarıda açıklanan kavramlara ilave olarak kişisel verilerin korunması hakkındaki konunun daha iyi anlaşılabilmesi için aşağıdaki kavramların da açıklanması gerekli görülmüştür. Bu kavramlardan ilki "anonim veri"dir. Anonim veri, kişisel veri tanımının tersinden yola çıkarak verinin bir kişi ile ilişkilendirilmesi veya bu veriden yola çıkarak bir kişiye ulaşılamayan veya kaynağının belirlenememesi veya belirlenemez hale getirilmesi sonucunda oluşan bilgiye denmektedir.[42]

İstatistik, araştırma ve planlama amacıyla tutulan veriler, büyük miktarda bilgi olarak toplanır, bu nedenle ilgili kişilerle ilişkilendirilemediği için kişisel veri olarak

---

[40] Özkan, age, s. 18-19 ve Korkmaz, age, s. 53 ve Özdemir, age, s. 126-127.

[41] Aydın Akgül, **Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması**, 2. Baskı, Beta Yayıncılık, İstanbul, 2016, s. 26-31. "Hassas verilerin dışında bir de hassas olmayan veriler vardır. Bu veriler aslında hassas veriler kadar önemli olmakla birlikte işlendiklerinde Anayasa'da ve TMK'nin 24. Maddesinde yer alan kişilik haklarının ihlali söz konusu olmaktadır. Bu verilerin dışında kalan, ilgili oldukları kişilerin özelliklerini ortaya koyan hatta onların tanınmasına yardımcı olan bilgilerdir. Bunlara hassas olmayan kişisel veriler denilmektedir. İki çeşit veri arasındaki fark kendi korunma konusunda göstermektedir." Özdemir, age, s. 134-135.

[42] Uğur Ersoy, "Bir İnsan Hakları Kavramı Olarak Kişisel Verilerin Korunması", Gazi Üniversitesi, Sosyal Bilimler Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, Ankara, 2009, s. 17 ve Bük, age, s. 40.

kabul edilmez. Veri sahibi ile veri arasındaki nedensel ilişkisi kesintiye uğradığından, ilgili veriler hakkında gerçekleştirilen işlemler insan hak ve özgürlüklerinin ihlaliyle sonuçlanmayacaktır.[43] Bu kavramla ilgili olarak anonim hale getirme, "Kişisel Verileri Koruma Kanunu (KVKK)"nun 3. maddesinde "*kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi*" şeklinde açıklanmaktadır. Dolayısıyla istatistik veya araştırma gibi amaçlarla kaydedilen, ancak "*kimliği belirli ya da belirlenebilir bir kişi ile ilişkilendirilmesi mümkün olmayacak bir hale getirilen*" bilgiler anonim veri olarak nitelendirilmektedir. Bu tür verilerin bir kişi ile ilişkilendirilmesi mümkün olmadığından kişisel veri olarak işlem görmesi ve bu nedenle de koruma altına alınmasının söz konusu olmadığı beyan edilmektedir.[44]

Bu anlamda burada açıklanması gereken diğer bir kavram olan "veri işlenmesi" ise KVKK'nın 3. maddesinde, "*Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem*" şeklinde tanımlanmıştır.[45] Bu kanuna göre "veri işleyen" ise, "*veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi*" olduğu belirtilmiştir. Buradan veri sorumlusunun, kişisel verinin işlenmesiyle alakalı her türlü kararı verme ve sorumluluğuna sahipken, veri işleyen ise onun verdiği talimatlar doğrultusunda hareket eden, ondan bağımsız ve ayrı bir gerçek veya tüzel kişidir. Burada en temel kriterlerden birisi veri sorumlusu adına hareket etmektir.[46]

Bir başka kavram olarak "veri sorumlusu" ise KVKK'nın 12. maddesinde "*kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi*" şeklinde

[43] Başalp, age, s. 16 ve Ersoy, agt, s. 17.
[44] Titrek, agt, s. 12. Kişisel verilerin anonim hale getirilmesi yöntemleri ile ilgili bkz, Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi,** , s. 16-20. www.kvkk.gov.tr. E.T. 12.01.2021.
[45] Dülger, age, s. 183.
[46] Dülger, age, s. 208-209 ve Korkmaz, age, s. 62-64 ve Ezgi Çırak, "Dijital Çağda Sonsuza Kadar Hatırlamaya Karşı: Unutulma Hakkı", **CHD**, 2018, sayı 36, s. 161-189, özellikle s.163.

tanımlanmaktadır. Dikkat edilmesi gereken nokta ilgili kişi sadece gerçek kişi olabilir. Veri sorumlusu ise gerçek kişiler dışında kamu kurumu, şirket, dernek veya vakıf gibi tüzel kişiler de olabilir.[47]

Bu çerçevede burada verilmesi gereken son kavram ise "veri kayıt sistemi"dir. "Kişisel Verileri Koruma Kanunu" kapsamında veri kayıt sistemi, "*kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi*" olarak tanımlanmıştır. Kanunun gerekçesinde belirtildiği üzere veri kayıt sistemleri elektronik veya fiziki ortamlarda oluşturulabilmektedir. "95/46/AT sayılı AB Direktifi"nde, "kişisel veri dosyalama sistemi" terimi veri kayıt sisteminin yerini almaktadır. Bu direktifte, bir kişisel veri dosyalama sistemi, belirli koşullar altında erişilebilen bir dizi kişisel veri olarak tanımlanmaktadır.

"95/46/AT sayılı Avrupa Birliği Direktif"nde veri kayıt sistemi yerine kişisel veri dosyalama sistemi terimi kullanılmıştır. Direktifte ise kişisel veri dosyalama sistemi, belirli bir ölçüte göre erişebilecek şekilde yapılandırılmış kişisel veri kümesi olarak tanımlanmıştır.[48]

"Unutulma hakkı" da bu çerçevede açıklanması gereken bir başka kavramdır. Unutulma hakkı, en basit şekliyle bireyin internette bulunan kendisine ait bilginin erişiminden kaldırılması talebi veya bireyin geçmişinin gündeme getirilmemesi hakkı olarak tanımlanmaktadır. Başka bir deyişle, bireyler internette yer alan rahatsız edici içerikleri veya haklarına sahip oldukları kişisel verileri silme ve yayılmasını önleme hakkına sahiptir.Kişinin kendisiyle ilgili bir bilginin artık ilişkilendirilmeme hakkıdır. Kişiye ait bilgi alenileştiğinde hukuka aykırı bir bilgi halini alır. Bilgi yayıldığı ilk anda kişi buna rıza göstermiştir. Ancak aradan zaman geçmesiyle birlikte kişinin durumunda veya rızasında meydana gelen değişim unutulma hakkının ileri sürülmesine neden olmaktadır. Diğer bir ifade ile kişisel bilginin yayılması başta hukuka uygun iken, zamanın aşındırıcı etkisi ile kişisel menfaat toplumsal menfaate ağır basmaya başlamakta, bireyin özel hayatına ilişkin menfaati toplumun bilgilenme ve haber almaya ilişkin menfaatinin önüne geçmektedir. Bu sebeple unutulma hakkı,

---

[47] Kişisel Verileri Koruma Kurumu, **Veri Sorumlusu ve Veri İşleyen**, s. 2 ve Kişisel Verileri Koruma Kurumu, **6698 Sayılı Kanunda Yer Alan Temel Kavramlar**, s. 21.25. www.kvkk.gov.tr. E.T. 12.01.2021.

[48] Korkmaz, age, s. 63-64.

"*bireyin geçmişte hukuka uygun olarak yayılmış ve doğru nitelikteki bilgilerinin, zamanın geçmesine bağlı olarak erişimden kaldırılmasını ya da gündeme getirilmemesini talep edebilmesi*" şeklinde tanımlanmaktadır.[49]

Unutulma hakkının kapsamına yönelik olarak, sadece internet ortamındaki kişisel verilere ilişkin olduğu görüşünün aksine internet ortamında olmayan kişisel verilere yönelik olarak da tanınması gerektiğine ilişkin görüşler vardır.[50]

Unutulma hakkı, Anayasa Mahkemesi tarafından 2016 yılında yapılan bir bireysel başvuru sonucunda tanınmıştır.[51] Anayasa Mahkemesi'nin yanı sıra, Yargıtay Hukuk Genel Kurulu'nun da unutulma hakkını aldığı bir kararla[52] kabul ettiği görülmektedir.

---

[49] Eren Sözüer, **Unutulma Hakkı, İnsan Hakları Hukuku Perspektifinden Bir İnceleme**, İstanbul, 2017, s. 8, 55-56 ve 205.

[50] Titrek, agt, s. 12-13 ve Kangal, age, s. 1-2.

[51] "*Unutulma hakkı Anayasa'mızda açıkça düzenlenmemiştir. Bununla birlikte Anayasa'nın Devletin temel amaç ve ödevleri başlığında düzenlenen 5. maddesinde insanın maddi ve manevi varlığının gelişmesi için gerekli şartları hazırlamaya çalışmak ifadesi ile devlete pozitif bir yükümlülük yüklenmiştir. Bu yükümlülük bağlamında Anayasa'nın 17. maddesinde düzenlenen kişinin manevi bütünlüğü bağlamında şeref ve itibarının korunması hakkı ve Anayasa'nın 20. maddesinin üçüncü fıkrasında güvence altına alınan kişisel verilerin korunmasını isteme hakkı ile birlikte düşünüldüğünde, devletin bireye geçmişte yaşadıklarının başkaları tarafından öğrenilmesi engellenerek yeni bir sayfa açma olanağı verme hususunda bir sorumluluğu olduğu açıktır. Özellikle kişisel verilerin korunması hakkı kapsamında kişisel verilerin silinmesini talep edebilme hakkı, kişilerin geçmişlerinde yaşadıkları olumsuzlukların unutulmasına imkân tanımayı kapsamaktadır. Dolayısıyla Anayasa'da açıkça düzenlenmeyen unutulma hakkı, İnternet vasıtasıyla ulaşılması kolay olan ve dijital hafızada bulunan haberlere erişiminin engellenmesi için Anayasa'nın 5., 17. ve 20. maddelerinin doğal bir sonucu olarak karşımıza çıkmaktadır. Diğer taraftan unutulma hakkının kabul edilmemesi, İnternet vasıtasıyla kolayca ulaşılabilir ve uzun süre muhafaza edilebilir kişisel veriler nedeniyle başkaları tarafından kişiler hakkında ön yargı oluşturabilmesi nedeniyle manevi varlığının geliştirilmesi için gerekli onurlu bir yaşam sürdürmesine ve manevi bağımsızlığına müdahaleyi sürekli kılmaktadır. // Anayasa Mahkemesinin ifade ve basın özgürlükleri ile şeref ve itibarın korunması hakkı arasındaki dengelemeye ilişkin kararlarında Anayasa'nın 17. Maddesinin birinci fıkrası temelinde değerlendirme yaptığı gözetilerek unutulma hakkına ilişkin iddiaların İnternet ortamındaki haberlerin kişisel veriler ile arasındaki ilişki dikkate alınarak Anayasa'nın 17. Maddesinin birinci fıkrası kapsamında inceleme yapılması gerekmektedir*". (AYM, 03.03.2016, N.B.B., B. No: 2013/5653, RG. 24.08.2016

[52] "*Ayrıca şunun da ifade edilmesi gereklidir ki; unutulma hakkı tanımlarına bakıldığında her ne kadar dijital veriler için düzenlenmiş ise de, bu hakkın özellikleri ve bu hakkın insan haklarıyla arasındaki ilişkisi dikkate alındığında; yalnızca dijital ortamdaki kişisel veriler için değil, kamunun kolayca ulaşabileceği yerde tutulan kişisel verilere yönelik olarak da kabul edilmesi gerektiği açıktır. Davacı, geçmişte yaşadığı kötü bir olayın toplum hafızasından silinmesini istemektedir. Unutulma hakkı ile geçmişindeki yaşanan talihsiz bir olayın unutularak geleceğini serbestçe şekillendirmek, diğer bir deyişle hayatında, yeni bir sayfa açma olanağı istemektedir. Kaldı ki, davacı da yargılama sırasında verdiği dilekçelerinde bu istem üzerinde ısrarla durmuştur. Davacı unutulma hakkı ile özel yaşamına ilişkin kişisel verilerinin üçüncü kişiler tarafından bilinmemesini, aradan geçen süre nedeniyle toplum hafızasından silinmesini istemektedir. Bu bağlamda değerlendirildiğinde; 4 yıl önce gerçekleşen bir olayın mağduru olan kişinin adının açık bir şekilde yazılarak kitapta yer alması halinde unutulma hakkının bunun sonucunda da davacının özel yaşamının gizliliğinin ihlal edildiği kabul edilmelidir. Avrupa Birliği Adalet Divanı'nın Google Kararı'nda açıkladığı gibi ilgili verinin kamu hayatında*

1.1.2.Kişisel verilerin korunması hakkı

1.1.2.1.Tarihsel gelişimi

Bireylere ait veriler, tarih boyunca farklı gerekçelerle kişiler, modern topluluk ve kuruluşlar tarafından büyük ölçüde bilme ve öğrenme isteği duyulan bilgiler olarak değerlendirilmişlerdir. Bu isteğin en önemli nedeni her insanın doğasında bulunan merak duygusuyla ilgili olsa da, zamanla kişisel verilerin bilinme isteği ve ihtiyacının başta ekonomik, sosyolojik, siyasal ve teknolojik olmak üzere pek çok farklı alanlarda ilişkisi ortaya çıkmıştır.[53]

Bilişim teknolojisinin gelişmesi ve kullanımının yaygınlaşmasıyla o zamanlar tartışılmayan ve hukuksal korumadan faydalandırılmaya gerek duyulmayan kişisel veriler ilk olarak ABD ve Avrupa ülkelerinde olmak üzere zamanla tüm dünya ülkelerinde korunması gereken bir alan olarak görülmeye başlanmıştır. Tarihin çok eski yıllarından beri kişisel verilerin öğrenilmesine yönelik istek teknolojik gelişmelerle tartışmaya açık bir konu haline gelmiştir. Bunun nedeniyse verilerin teknolojik araçların sağladığı imkânlar sayesinde kolaylıkla elde edilmesi, saklanması ve işlenmesidir. Dolayısıyla insanların kayıt altına alınması ve gözetlenmesi esasen teknolojik gelişmelerle mümkün olmuş ve tehlike arz etmeye başlamıştır.[54]

Bu alanın günümüzde çok popüler olduğu ve ülkelerin elli yıldır veri koruma konusunda büyük çaba göstermeye çalıştıkları söylenebilir. Endüstriyel bir toplumdan bilgi toplumuna geçiş sırasında, bireylerin zarar verme korkusu, ülkeleri ve uluslararası kuruluşları veri koruma alanında düzenlemeler yapmaya itmiştir.

---

*oynadığı önemli rol ve halkın ilgili veriye yönelik yoğun ilgisi şeklinde, üstün bir kamu yararını ortaya koyan özel sebepler bulunmadığına göre bilimsel esere alınan kararda kişisel veriler açık bir şekilde yer almamalıdır. Görüşmeler sırasında azınlıkta kalan üyeler mahkeme kararlarında yer alan isimlerin rumuzlanmasına gerek olmadığını, yargılamanın istisnalar haricinde açık bir şekilde yapıldığını hükmün alenen tefhim edildiğini, bu nedenle özel hayatın gizliliğinin ihlal edilmediğini savunmuşlar ise bu görüş sorunun mahkeme kararlarında isimlerin rumuzlanmadan yer alması değil, kararların kitaba alınması sırasında rumuzlanması gerekip gerekmediği sorunu olduğu gerekçesi ile kurul çoğunluğu tarafından kabul edilmemiştir. 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 zorunludu*r". (HGK, 17.6.2015, E. 2014/4-56, K. 2015/1679,. E.T. 12.01.2021.

[53] Küzeci, age, s. 19-20.

[54] Dülger, age, s. 66-67.

1970'lerde, çeşitli AB ülkeleri kişisel verilerin otomatik olarak işlenmesine ilişkin düzenlemeler oluşturmaya başladı.[55]

Kişisel verilerin korumasına ilişkin ilk yasal düzenleme, 1970 yılında Almanya'nın Hessen eyaletinde yapılmıştır. Bu yasanın kabulüne neden olan en önemli dinamiğin, "Hessen Planı" olarak adlandırılan bir program içerisinde 1960'lı yılların sonunda, özel yaşamın gizliliği hakkı üzerindeki olası olumsuz sonuçlar doğurabilecek olan federe düzeyde merkezi bir veri bankasının kurulmasına ilişkin kanun tasarısı olduğu söylenmiştir.[56]

Hessen eyaletinin verilerin korunmasına ilişkin yaptığı düzenleme ve sonrasında konuyla ilgili ortaya çıkan tartışmalar, Almanya'da federal düzeyde bir koruma öngörülmesini de sağlamıştır. Bu doğrultuda 1977 yılında Federal Almanya Veri Koruma Kanunu kabul edilmiştir. Ancak bu Kanun, kişisel verilerin korunması görevini, aynı zamanda milli istihbarat ve polis teşkilatından da sorumlu olan İçişleri Bakanlığına bırakması nedeniyle oldukça eleştirilmiştir.[57]

Kişisel veriye ilişkin ilk kanun "1973 tarihli İsveç Veri Koruma Kanunu"dur. Daha sonra Hessen Eyaleti'nde veri korumayla ilgili çıkan tartışmalar, eyalet sınırlarını aşarak Almanya'da federal düzeyde 28 Ocak 1977 tarihinde "Alman Federal Veri Koruma Kanunu"nun çıkmasına vesile olmuştur. Bu kanunda eksiklikler olmasına rağmen ilk adım olması bakımından büyük önem arz etmektedir. 1970 ile 1980 yılları arasında veri koruma kanunu çıkarma furyasına 1978 yılında Fransa da katılmış ve "6 Ocak 1978 tarihli Veri İşleme ve Hürriyetler Kanunu" vesilesi ile kişisel veriler yasal olarak güvence altına alınmıştır. Bu tarihten sonra AB ülkelerinden bazıları veri korumaya yönelik kanun çıkarma yoluna giderken, bazıları da anayasalarına kişisel veri ile ilgili maddeler koyma yolunu seçmişlerdir. Bu ülkelere Portekiz, Avusturya ve İspanya örnek verilebilir. Avusturya'da 18 Ekim 1978 tarihli Federal Kişisel Verilerin Korunması Kanunu 1 Ocak 1980 tarihinde yürürlüğe girmiştir. İsviçre'de 19 Haziran 1992 tarihinde Federal Veri Koruma Kanunu, İngiltere'de ise "1998 yılında Veri Koruma Kanunu" yürürlüğe girmiştir. Ülkeler

[55] Türkay Henkoğlu, **Bilgi Güvenliği ve Kişisel Verilerin Korunması**, Ankara, 2015, s. 29.
[56] Kuşkonmaz, agt, s. 41.
[57] Özkan, age, s. 32-33.

yanında uluslararası kuruluşlar, insanların giderek daha fazla veri işleme ile karşı karşıya kaldıklarından endişelenmeye başlamış ve bu çerçevede, açık ve etkili koruma sağlamak için düzenlemelere gitmişlerdir.[58] İlerideki bölümlerde ayrıntılı olarak açıklanacağı üzere, OECD, AB, Avrupa Topluluğu ve Birleşmiş Milletler gibi kuruluşlar, bu konunun gelişmesine ve kişisel verilerin anayasal zeminde tanınmasına katkıda bulunan veri koruma ile ilgili çeşitli düzenlemeler oluşturmuştur.

1.1.2.2.Kişisel verilerin hukuki niteliği

1.1.2.2.1.Genel olarak

Ülkemizde kişisel verilerin korunması hakkı Anayasada temel bir hak olarak yer almamaktaydı. 12 Eylül 2010 tarihinde yapılan halk oylaması ile yürürlüğe giren 5982 sayılı kanunla 1982 Anayasası'nın "Özel hayatın gizliliği" başlıklı 20. maddesine eklenen üçüncü fıkra ile kişisel verilerin korunması temel bir hak olarak Anayasada yerini almıştır. Değişiklikten önce öğreti, Anayasa'daki diğer temel hak ve özgürlükler kapsamında kişisel verilerin korunması hakkını açıklamaya çalışmaktaydı.[59] Kişisel verilerin hukuki dayanağının esas olarak Anayasa'nın bireylerin maddi, manevi varlığını diğer bir deyişle kişiliğini özgürce geliştirme hakkını düzenleyen 17. maddesinde düzenlendiği ifade edilmiştir.[60] Anayasanın 20. maddesindeki özel yaşamın gizliliği hakkının da kendi koruma alanları içerisinde kişisel verilerin korunması hakkında bazı garantiler getirdiği belirtilmiştir.[61]

Kişisel verilerin korunması hakkı, demokratik ve özgür bir toplumda yaşayan ve kendi özgür iradeleriyle hayatlarına karar verme yeteneğine sahip kişilerin kişisel verilerinin korunmasıdır. Bu nedenle modern toplumlarda veri işleme faaliyetlerinin riskleri karşısında bireyin korunabilmesi için her şeyden önce bireyin kendisine ait verileri üzerindeki belirleme hakkının diğer bir ifadeyle bireyin kişisel verileri üzerinde karar verme özgürlüğünün güvence altına alınmasını sağlamaktadır. Eğer birey kişisel verilerinin kimler tarafından hangi oranda bilindiği hakkında tam bir bilgiye sahip değilse bu konuda özgürce karar verebilmesi beklenemez. Bu konuda

---

[58] Özkan, age, s. 33-34 ve Mesut Serdar Çekin, **Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku**, 3. Baskı, On İki Levha Yayıncılık, İstanbul, 2020, s. 5-6.
[59] Şimşek, age, s. 111; Aksoy, age, s. 71; Özdemir, age, s. 80-81 ve Çokmutlu, agt, s. 45-46.
[60] Şimşek, age, s. 112.
[61] Dülger, age, s. 71.

bireyin tam bir özgürlüğünün sağlanabilmesi için kişisel verilerinin toplanması, saklanması, kullanımı ve başkalarına aktarımı konusunda söz sahibi olması gerekir. Teknolojinin gelişmesine paralel olarak artan veri işleme faaliyetleri karşısında bireyler kişisel verilerinin kolayca elde edilmesi, toplanması, kullanılması ve başkalarına aktarılması ile karşı karşıya kalmışlardır. Bireyin bu durumda korunmasını amaçlayan ve bireye kendi verileri üzerinde belirleme hakkını veren kişisel verilerin korunması hakkı, öncelikli olarak Anayasanın 17. maddesindeki insan onuru diğer bir ifadeyle kişilik hakkı ile temellendirilmektedir. Sürekli gözetlenen, özel hayatına ait tüm kişisel verileri kapsamlı bir kayda alınan ve özel hayatın gizliliği ortadan kaldırılan, kişisel verileri üzerinde hiçbir hakkı olmayan birinin kişiliğini serbestçe geliştirmesi beklenemez. Nitekim normal hayatta bu şekilde özel hayatı kayda alınan ve özel yaşamın gizliliği ortadan kaldırılan bir kişi, kendi bireysel özgür iradesi gereği gibi değil, kendisinden istenilen davranış şekliyle hareket edecektir.[62]

Demokratik bir toplumda bir kişinin düşünce ve ifade özgürlüğü gibi temel hak ve özgürlüklere sahip olabilmesi için bunun devlet veya üçüncü bir kişi tarafından izlenip kontrol edilmemesi ve kamuya açıklanmaması gerekir. Ancak bireyler kendi verileri üzerinde tam kontrole sahip olduklarında bireysel özerklik ve demokratik yasal düzen gerçekleşmiş olur.[63]

Kısaca belirtmek gerekirse, "kişisel verilerin korunması hakkı", birçok temel hak ve özgürlük kapsamında değerlendirilmiş, öğretide bu hakkın hangi hak kapsamında korunması ve hangi hakla birlikte değerlendirilmesi gerektiğine ilişkin pek çok tartışma yapılmıştır. Genel kabul gören görüşe göre, bu hakkın insan hakları zemininde özel hayatın gizliliği kapsamında olması şeklinde olmuştur. Fakat Avrupa ve ABD'de kişisel verilerin korunması hakkının, daha çok mülkiyet hakkı ya da fikri mülkiyet hakkı kapsamında korunmasının daha uygun olacağı şeklinde tartışmalar da bulunmaktadır. [64]

Kişisel verilerin korunması hakkının hukuki niteliği incelenirken, genelde iki çeşit yaklaşım tarzı vardır. Bu iki yaklaşım tarzı, Avrupa ile ABD arasındaki

---

[62] Şimşek, age, s. 112 ve Çokmutlu, agt, s. 46-47.
[63] Dülger, age, s. 77.
[64] Sinem Göçmen Uyarer, **Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması**, 2. Baskı, Seçkin Yayınevi, Ankara, 2020, s. 23.

farklılardan kaynaklanmaktadır. Avrupa yaklaşımı sosyal değeri esas alıyorken, ABD daha çok işin ekonomik tarafına ağırlık vermekte ve olayları da bu şekilde ele almaktadır.[65] Örneğin Avrupa'da "bilgi toplumu", ABD'de ise "bilgi ekonomisi" ön plandadır ya da tartışılmaktadır. İki kıta arasındaki bakış açısı bu alanda da kendini göstermiştir. Böylece iki temel yaklaşım tarzı ortaya çıkmıştır. Bunların ilki "ekonomik hak yaklaşımı", diğeri de "insan hakkı yaklaşımı" şeklindedir. Ekonomik hak yaklaşımı daha çok ABD tarafından, insan hakkı yaklaşımı da Avrupa tarafından kabul görmekteydi. Bu iki tarz görüşten en çok kabul göreni, kişisel verilerin korunması hakkının insan hakları zemininde özel hayatın gizliliği kapsamında korunmasını savunanlardan meydana gelmekteydi. İkincisi ise daha çok ABD'de kabul gören ve kişisel verilerin korunmasını hakkını mülkiyet hakkı ya da fikri mülkiyet hakkı kapsamında korunması gerektiğine inananların görüşü şeklinde ortaya konmaktadır.[66] Ekonomik hak yaklaşımı altında mülkiyet hakkı ve fikri mülkiyet hakkı incelenecek ve daha sonra insan hakları bağlamında kişisel verilerin korunması maddelerine geçilecektir.

1.1.2.2.2.Mülkiyet hakkı

Kişisel verilerin mülkiyet kapsamında korunması gerektiği iddia edilmektedir. Kişisel veriler, yalnızca kişiliğin bir parçası değil, buna ek olarak kişilik ürünü olarak kabul edilmektedir. Bu görüş, verilere sahip olan herkesin kendileriyle ilgili kişisel verilerin sahibi olarak değerlendirileceği, bu veriler üzerinde tam kontrole sahip olacağı ve mülk sahibinin kapsamlı yasal korumasından yararlanacağı görüşüne dayanmaktadır. Bu görüşte kişisel verilerin ticari değeri ön plana çıkarılmaktadır. Bilginin güç ile eşdeğer olduğu ve verilerin de ticari değer kazandığı düşünüldüğünde, bireylerin sahip oldukları kişisel verileri başkaları tarafından kullanılması karşılığında para kazanacaklarını savunmuşlardır.[67] Teşebbüsler topladıkları kişisel verilerden faydalanarak müşterilerine sundukları hizmet kalitesini artıracaklar, iç pazar stratejilerinin belirlenmesinde kullanacaklar, ayrıca üçüncü kişilere devrederek ticari kazanç sağlayacaklardır. Hatta başka şirketlere satabileceklerdir. Verilerin satılması durumunda teşebbüsler kar elde ederken, verileri satılan kişilerin menfaatleri zarara

[65] Elif Mendos Kuşkonmaz, "Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması", İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, İstanbul, 2013, s. 19.
[66] Küzeci, age, s. 66-67 ve Korkmaz, age, s. 84-85.
[67] Küzeci, age, s. 68-69; Aksoy, age, s.57-58 ve Çokmutlu, agt, s. 49.

uğrayacaktır.[68] Bu görüşe göre ilgili kişi kişisel verilerinin kötüye kullanılması halinde doğrudan dava açma veya zararının giderilmesi için istemde bulunma hakkına sahip olacaktır.[69] Ancak kişisel verileri sahibinin rızası dâhilinde satan kimse, bu verileri istediği şekilde üçüncü kişilerle paylaşacaktır. Bu durum asıl veri sahibinin kişisel verisi üzerindeki hâkimiyetini kaybetmesine yol açacaktır.[70]

Kişisel verilerin korunması konusunda ABD ile AB ülkeleri arasında önemli fikir ayrılıklarının olduğu açıktır. Avrupa Adalet Divanı, ABD'de kişisel verilerin yeteri kadar korunmadığı ve veri emniyetinin sıklıkla ihlal edildiği görüşünü dile getirmektedir. ABD'de kişisel verilerin korunması hakkı, anayasal veya temel hak ve hürriyet olarak korunmamakta, bu konunun sadece sektörel yaklaşımlar aracılığıyla veri güvenliğinin sağlandığı bilinmektedir. Bu tarz bir korumanın Amerika kıtası dışında yeterli görülmeyeceği aşikârdır. Avrupa kıtasında kişisel veriler, temel hak ve özgürlükler kapsamında korunmaktadır. Bu nedenle verilerin ticaretinin yapılması ya da devredilmesi meşru görülmemektedir.[71]

Tüm bunlar topluca değerlendirildiğinde kişisel verilerin korunması hakkının mülkiyet hakkı kapsamında değerlendirilmesinin yerinde olmadığı, sadece güçlü devlet veya özel sektör sermayelerine hizmet edeceği açıktır. Bu verilerin kullanılması elbette sermaye sınıfına hizmet edeceği, ancak daha az varlıklı olan bireyin sahip olduğu kişisel verileri koruma konusunda zayıf ve yalnız bırakacağı, bu ortamda da kişinin özgür iradesinden söz edilemeyeceği aşikârdır.

1.1.2.2.3.Fikri mülkiyet hakkı

ABD'de diğer bir yaygın görüş, kişisel verileri fikri mülkiyet haklarıyla ilişkilendirerek kişisel verileri korumak için telif hakkı benzeri yöntemlerin kullanılması gerektiğidir. Bu açıdan bakıldığında, fikri mülkiyet hakları ile kişisel verilerin korunması arasında benzerlikler olduğu görülebilmekte ve kişisel verilerin korunması için telif hakkı benzeri bir yöntem önerilmektedir.[72] Burada, ikisi arasında amaca yönelik bir benzerlik vardır. Çünkü kişisel verileri ve fikri mülkiyeti korumanın

[68] Çokmutlu, agt, s. 48-50 ve Kuşkonmaz, agt, s. 21-22.
[69] Akgül, age, s. 76.
[70] Aksoy, age, s. 64-65; Ayözger, age, s. 16-17 ve Özkan, age, s. 23.
[71] Korkmaz, age, s. 85-87; Ayözger, age, s. 16-17; Uyarer, age, s. 25; Akgül, age, s. 73; Hatipoğlu, age, s. 31-32 ve Dülger, age, s. 78-79.
[72] Küzeci, age, s. 71 ve Kuşkonmaz, agt, s. 21-23

temel amacı, bilgiyi ve açıklamayı korumaktır. Bu görüşü savunanlar, kişisel veri sahiplerinin yararlandıkları hakların, fikri mülkiyet hukukunda yazarların manevi haklarına benzediğine işaret etmektedir. Ancak fikri mülkiyeti oluşturan değerler, kişinin bilinçli olarak gösterdiği çaba ve gücün ürünü olmasına rağmen, kişisel verilerin böyle bir tarafı bulunmamaktadır. Kişisel veriler, tamamen kişinin yaşamını sürdürmesi sonucunda tabi olarak meydana gelen veriler olarak görülmüştür. Fikri mülkiyet hukukunda ekonomik kaygılar ve kamusal yararla ilgili sorunların üstesinden gelme amaçları söz konusuyken, kişisel verilerin korunmasında ekonomik amaçlar değil, kişinin bilgilerinin izinsiz toplanılmaması, kullanılmaması ve yayılmaması amaçları önceliklidir.[73]

Kişisel verilerin fikri mülkiyet hakkı şeklinde korunması ile ilgili getirilen bir diğer eleştiri, her iki hakkın korunmasının doğuracağı sonuçlara ilişkindir. Kişisel verilerin korunmaması, veri sahipleri üzerinde, fikri mülkiyet hakkının korunmamasına oranla çok daha büyük zararlara yol açacaktır. Fikri mülkiyet hakkının korunamaması daha çok kişiyi maddi anlamda zarara uğratırken, kişisel verilerin korunmaması durumunda kişinin mesleğini kaybetmesi, toplumda aşağılanması, dışlanması gibi ağır insan hakları ihlalleri ile karşı karşıya kalması söz konusudur. [74]

1.1.2.2.4.Enformasyonel self determinasyon hakkı

Enformasyonel self determinasyon hakkı, bireylerin kendilerine ait kişisel verilerinden hangilerinin, kimler tarafından ve ne tür şartlarda işlenebileceğine karar verme hakkı olarak ifade edilmiştir. Enformasyonel self determinasyon hakkı, Alman Anayasa Mahkemesi tarafından verilen "Nüfus Sayımı"[75] kararıyla ortaya çıkmıştır. Alman Anayasa Mahkemesi 1980'lerin başında verdiği bir kararla kişisel verilerin korunmasındaki temel ilkeleri belirlemiştir. Bu karar Almanya'daki Nüfus Kanunu aleyhine yapılan şikâyetler sonucunda verilmiştir. Alman Nüfus Sayımı Kanunu'na göre 1983 yılında nüfus sayımı yapılması öngörülmekteydi. Bu kanun, vatandaşlara istatistiki amaçlarda kullanılmak üzere çok kapsamlı ve ayrıntılı bilgileri açıklama

[73] Ayözger, age, s. 17-18; Çokmutlu, agt, s. 52 Akgül, age, s. 74 ve Aksoy, age, s. 66.
[74] Çokmutlu, agt, s. 52-53; Hatipoğlu, age, s. 32-33, Aksoy, age, s. 84 ve Korkmaz, age, s. 87-89.
[75] Bkz. BVerfGE 65 1, 41. Alman Anayasa Mahkemesinin Nüfus Sayımı Hakkındaki Kararından. Aktaran: Özdemir, age, s. 8.

yükümlülüğü getirmekteydi. Bu yükümlülüğü yerine getirmeyenlere ise yaptırım öngörülmekteydi.[76]

Mahkemenin kararında ön plana üç ana unsur çıkmaktadır. Bunlardan ilki, kişisel verilerin belirsiz bir şekilde kaydedilemeyeceği ve kaydedilme amacının gerçekleşmesinden sonra en kısa sürede silinmesinin gerektiğidir. İkincisi, kişisel verilerin sadece belirli amaçlar için toplanması, bu amaçlar doğrultusunda kullanılması ve gelecekte belirli olmayan amaçlar için kullanılmamasıdır. Üçüncüsü ise çeşitli kurum ve kuruluşlar tarafından kişisel verileri tutulan kişiye, daha sonraki veri aktarmaları hususunda danışılması veya en azından böyle bir durum ortaya çıktığında kişinin bilgilendirilmesidir. Kısaca belirtmek gerekirse enformasyonel self determinasyon hakkı, kişilik hakkıyla ilgili her türlü kişisel verinin, yaşam alanlarından hangisine dâhil olduğuna ve gizli olup olmadığına bakılmaksızın korunmasını sağlamaktır.[77]

"Alman Anayasa Mahkemesi" nüfus sayımı kararında; devletin ortaya sürdüğü gerekçeleri insan onurunun korunması ve kişiliğin korunması hakkındaki maddeleri birlikte değerlendirerek, "bilgilerin geleceğini belirleme hakkı"nı türetmiştir. Mahkemeye göre anayasal düzenin merkezinde toplumun özgür bir üyesi olarak kişinin onuru bulunmaktadır. Teknik gelişmelerin etkisiyle çıkan yeni tehlikeler karşısında kişiliğin korunmasının önemli olduğu belirtilmiştir. Kendisi hakkında toplanılan bilgilerin neler olduğu ve kimler tarafından hangi amaçlarla kullanılacağını bilmeyen bireyin kendi kararlarını verme özgürlüğünün önemli ölçüde zarar göreceği beyan edilmiştir. Rıza ya da açık bir yasal temel olmaksızın, ilgilinin kişisel verilerinin sınırsız bir biçimde toplanması, kaydedilmesi, kullanılması ve devredilmesi nedeniyle bireyler devlet karşısında korunmak zorundadır. Üstelik bu bilgilerin her zaman açık ve ulaşılabilir olması dikkate alındığında kişinin üzerinde psikolojik baskı oluşması ve bunun kamusal yaşama katılımını etkilemesi muhtemel görülmüştür.[78]

[76] Şimşek, age, s. 114-119 ve Küzeci, age, s. 75.
[77] Şimşek, age, s.116-117; Aksoy, age, s. 71-72 ve Küzeci, age, s. 75-76.
[78] Aktaran Küzeci, age, s. 76-77.

1.1.2.2.5.Kişilik hakkı

Yukarıda izah edilen ekonomik gerekçelere dayanan mülkiyet ve fikri mülkiyet haklarına yapılan en önemli itiraz temel hak ve özgürlüklerle bağdaşmamasıdır.

Kişilik hakkı, kişinin kişiliğini oluşturan, kişiyi insan kılan tüm maddi ve manevi değerler, özel olarak hayat, beden bütünlüğü, sağlık, onur, saygınlık, özel yaşamın gizliliği, söz, resim, ad, eser, özgürlük ve ekonomik serbestlik konusundaki hakkıdır. Kişilik hakkının korunmasıyla insana manevi ve sosyal bir değer verilmesi, saygı gösterilmesi sağlanır. Kişilik hakkı, bilimsel ve teknik gelişmelerin, değişen yaşam ilişkilerinin meydana getirebileceği yeni tehlikelere karşı da kişiye koruma sağlamalıdır.[79] Kişilik hakkı kişiye, içinde gözetlenmeksizin yalnız kalabileceği, sadece kendisinin özel güvenine sahip kişilerle iletişimde bulunabileceği ve kendisini geliştirebileceği özel bir alan olarak tanımlanabilmekte ve bu konuda da kişiye garanti vermektedir. Kişilik hakkı, kişinin kendisini içine çekebileceği, yalnız kalabileceği, dar yaşam alanını da korumakta ve kişiye sosyal alanda koruma getirmektedir. Kişilik hakkı, kişinin kendisini dış dünyada ifade edebilme özgürlüğünü kapsayıp, resmi ve söylediği sözler üzerindeki hakkını da korumaktadır. Bütün bunlar bireyin kamuoyunda yanlış ve istemediği bir şekilde tasvir edilmesi karşısında korunmasını da kapsamaktadır. [80]

Kişilik hakkı herkese karşı ileri sürülebilen mutlak bir haktır. Bu hak doğrultusunda herkes başkalarının kişiliğine saygı göstermesi gerekmektedir. Bu hak, kişilik hakkı sahibine hakkın korunması yetkisini vermektedir. Aynı zamanda başkalarına da kişinin bu hakkına saygı duyma zorunluluğu yüklemektedir. Kişilik hakkı, malvarlığı haklarına değil, şahıs varlığı haklarına dâhildir. Çünkü kişilik hakkına konu değerler para ile ölçülemez. Kişilik hakkı, kişiye sıkı sıkıya bağlı bir haktır ve bu hakkı da yalnızca hakkın sahibi kullanabilir. Bu haklardan ne vazgeçilebilir, ne de bir başkasına devredilebilir. Bu hak ancak kişinin ölümü ile sonlanır ve kişinin malları gibi varislerine intikal etmez. Kişilik hakkı zaman aşımına uğramaz.[81]

---

[79] Sert, age, s.53-54.
[80] Şimşek, age, s. 133.
[81] Özkan, age, s. 27.

Kıta Avrupası'ndaki hâkim görüş kişisel verileri kişilik hakkının bir parçası olarak kabul etmektedir. Kişisel verilerin korunmasının dayanağını kişilik hakkı çerçevesinde savunanlar, bu görüşlerini özellikle özel hayatın gizliliği ve mahremiyet kavramlarına dayandırmaktadır.[82]

1.1.2.2.6.Özel hayatın gizliliği hakkı

Teknolojideki gelişmeler sonucunda kişisel verilerin sadece özel hayatın gizliliği hakkı kapsamında benimsenen ilkelerle korunmasının yetersiz kalmasıyla kişisel verilerin korunması bağımsız bir hak alanı olarak kabul görmeye başlamıştır.[83]

Özel hayat, geniş ve karmaşık yapısı sebebiyle tanımlanması güç bir kavramdır. Bu kavramın sınırının belli olmaması nedeni, özel hayat ile ilgili temel hakların iç içe geçmesinden ve "*özel hayatın gizliliği hakkı ile korunmak istenen hukuki değerin*" belirginleştirilememesinden kaynaklanmaktadır. Bu kavramın içini doldurmak için pek çok teori üretilmiştir. Bu kavramın net açıklanması için Türk hukukunda da kabul gören "Üç Alan" teorisi kullanılmaktadır. Buna göre hayat üç farklı alan olarak düşünülmüştür. Bunlar "kamuya açık alan", "özel alan" ve "sır alanı" şeklindedir.[84] Kamuya açık alan, kişinin genel yaşam alanıdır. Burasını herkesle paylaşmaktadır. Burası genel hayatı ifade edip, herkesçe bilinebilen bir alandır. Kişinin kamuya açık alana girmesi, yürümesi ve alışveriş yapması, kültürel faaliyetlerde bulunması, toplu taşıt araçlarına binmesi gibi faaliyetler, bu alan içine girmektedir. Özel alan, kişinin ancak yakın çevresince bilinebilen hayatıdır. Bu alan kişinin evinin bahçesi ya da arabasındaki alan gibi kısmen dışa açık bir alanlardaki aktivitelerini kapsamaktadır. Sır alan ise genel kişilik hakkının özü olması sebebiyle kamusal müdahaleye kapalı, dokunulmaz, çekirdek bir alandır.[85] Bireyin küçük dünyası olarak da isimlendirilebilecek sır alanda, kişinin mahremiyetinin korunması, onun kişiliğinin özgürce gelişimi açısından zorunludur. Kişinin aile hayatı, ikili ilişkileri, duygusal ve cinsel yaşamı sır alanının kapsamı içine girmektedir.[86]

---

[82] Korkmaz, age, s. 89-93 ve Aksoy, age, s. 47

[83] Yeşim Çelik, "Özel Hayatın Gizliliğinin Yansıması Olarak Kişisel Verilerin Korunması ve Bu Bağlamda Unutulma Hakkı", **Türkiye Adalet Akademisi Dergisi**, Yıl:8, Sayı:32, Ekim 2017, s. 391.

[84] Kuşkonmaz, agt, s. 25-26; Çokmutlu, agt, s. 56-58 ve Korkmaz, age, s. 99.

[85] Şimşek, age, s. 140 ve Çokmutlu, agt, s. 56-58

[86] Durmuş Tezcan, "Özel Hayat Açısından Kişisel Verilerin Korunması", **İstanbul Kültür Üniversitesi Hukuk Fakültesi Dergisi**, 16(1), 2017, 17-25, özellikle s. 21-22.

"Özel hayatın gizliliği hakkı", mutlak bir hak olmamakla birlikte, ulusal ve uluslararası düzenlemelerle sınırları belirlenmiştir. Fakat özel hayatın gizliliği hakkına karşı, son yıllarda özellikle 11 Eylül 2001 yılında yapılan saldırı sonrasında baskılar artmaya başlamıştır. ABD başta olmak üzere birçok ülkede yapılan düzenlemeler özel hayatın alanlarını daraltması ile sonuçlanmıştır. Toplanan kişisel veriler güvenlik kaygıları ile toplanma amaçlarının dışında kullanılmıştır.[87] Bu konu, Anayasanın 20. maddesinde bir hak olarak düzenlenmiştir. Kişisel verilerin korunması hakkı ise 12 Eylül 2010 tarihli referandumdan sonra çıkarılan "5982 sayılı TC Anayasasının Bazı Maddelerinde Değişiklik Yapılması Hakkında Kanun" ile Anayasanın 20. maddesine getirilen ek fıkra ile açıkça anayasal güvenceye kavuşturulmuştur. Bu kanundan önce kişisel veriler insan onuru ve genel kişilik hakkı çerçevesinde korunmaktaydı.[88] "Avrupa İnsan Hakları Sözleşmesi"nin 8. maddesinde "özel hayatın gizliliği"nin niteliği hakkında getirilen korumanın konut dokunulmazlığı hakkı da özel hayatı mekânsal olarak ve kişinin rahatsız edilmeden konutu içinde özel hayatını düzenlemesine imkân vermektir. Bu çerçevede konutların hukuka aykırı olarak ses veya görüntü kaydeden cihazlarla dinlenmesi veya gözlenmesi ve bunların kaydedilmesi, konut dokunulmazlığının, diğer bir ifadeyle özel hayat hakkının ihlali olarak değerlendirilmektedir. Bu müdahale, yasal bir zemine dayanmadığı ve bireyin rızası olmadığı sürece kişisel verilerin korunmasının ihlali olarak sayılacaktır.[89]

Kişisel verilerin hukuki niteliğine dair tüm görüşler incelendiğinde yalnızca kişilik hakkının bir değeri olan özel hayat ile ilişkilendirmek yerine, kendine münhasır ayrı bir değer olarak değerlendirilmesi daha isabetli ve uygun olacaktır. Diğer bir ifade ile "kişisel verilerin geleceğini belirleme hakkı" kişilik hakkının bir parçası olmakla birlikte sadece özel hayata indirgenmemelidir. Çünkü "kişisel verilerin geleceğini belirleme hakkı" kişilerin verilerinin bir kısmını değil, tamamını koruma altına almaktadır. Yine buna paralel olarak kişisel verilerin kamuya açık alanda korunmaması tehdidinden bahsedilmeyecektir. Buna ek olarak kişisel verilerin serbest dolaşımı da sağlanmış olacaktır. Yukarıda belirtilen bu nedenlerden dolayı kişisel

[87] Korkmaz, age, s. 101-102.
[88] Sert, age, s. 55; Korkmaz, age, s. 99-100.
[89] Şimşek, age, s. 140 ve Akgül, age, s. 142.

verilerin hukuki niteliğine dair görüşler arasında en uygun ve isabetli görüş, "bireyin verilerinin geleceğini belirleme hakkına dayanan görüş" şeklinde görülmektedir.[90]

Kişisel verilerin korunmasının, insan hakları bağlamında sadece "özel hayatın gizliliği" hakkından ibaret olmayıp, ifade özgürlüğü, unutulma hakkı, insan onuru ve bilgi edinme hakkı gibi pek çok insan hak ve özgürlüğü ile de yakından ilgilidir. Ancak bu maddelere ilişkin bu çalışmada konunun kapsamının genişliği dikkate alınarak bilgi verilmeyecektir.

1.1.3.Kişisel verilerin işlenmesi kavramı

Veri öznesi, sorumlusu ve işlemecisinin dâhilinde gerçekleştirilen veri işleme; "Avrupa Birliği Veri Koruma Direktifi"nde ve "Genel Veri Koruma Tüzüğü"nde "*otomatik veya otomatik olmayan vasıtalarla, kişisel veriler ve verilere dâhil unsurlar üzerinde gerçekleştirilen her türlü işlem*" olarak tanımlanmaktadır. Diğer bir ifadeyle; kişisel verilerin korunması alanı içerisinde bir veya birden fazla kişi veya kuruluşun müdahil olduğu sürece ilişkin tüm işlemlere genel olarak kişisel verilerin işlenmesi denilebilmektedir.[91]

Kişisel verilerin işlenmesi kavramı, nitelik olarak geniş bir içeriğe sahiptir. Burada süreç kişisel verilerin toplanması ile başlar silinmesine kadar devam eder. Kişisel verilerin işlenmesi, "Telekomünikasyon Sektöründe Kişisel Verilerin Korunması Yönetmeliği"nin[92] 4. maddesinde "*Otomatik olsun veya olmasın, toplama, kaydetme, hazırlama, yükleme, uyarlama, değiştirme, geri çağırma, danışma, kullanma, aktarma yoluyla açığa vurma, yayma ya da bunların dışında erişilebilir hale getirme, düzenleme, birleştirme, engelleme, silme gibi yollardan, kişisel bilgiler üzerinden yürütülmekte olan herhangi bir işlem ya da işlemler bütünü"* olarak tanımlanmaktadır. Bu tanımdan da anlaşıldığı üzere, kişisel verilerin toplanması, depolanması, değiştirilmesi ve silinmesi işleme kavramı içinde yer almaktadır. [93] Kişisel verilerin toplanması, değiştirilmesi, depolanması ve silinmesi işleme süreci içinde birbirini takip eden ayrı birer safha oluşturmaktadırlar.

---

[90] Özkan, age, s. 30.
[91] Sarıusta, agt, s. 25.
[92] 25365 sayılı ve 6 Şubat 2004 tarihli Resmi Gazete, https://www.resmigazete.gov.tr/eskiler/2020/12/20201204-13.htm, 09.07.2021.
[93] Özdemir, age, s. 135.

Kişisel verilerin toplanması, çeşitli kişisel bilgilerin herhangi bir şekilde elde edilmesi ve tedariki anlamına gelir. Hatta tedarik amacı olmayan, sadece deneme amaçlı edinilen bu tür bilgiler dahi kişisel verilerin toplanması faaliyetine dâhildir. Ayrıca, kişisel verilerin toplanması, mutlaka kanunda sayılan hallerden ibaret olmayıp, elektronik haberleşme araçlarından yararlanılarak ilgili kişilerin izlenmeleri, dinlenilmeleri, fotoğraflarının yayınlanmaları vb. durumlarında da söz konusudur. Şu halde, kişisel verilerin toplanması, ilgili kişiler hakkındaki bütün bilgilerin temin edilmesi ve bir araya getirilmesi demektir.[94] Kişisel verilerin temini ile onların toplanma amacı arasında doğrudan bir ilgi mevcut değildir. Toplanan kişisel veriler değişik amaçlarla kullanılabilirler. Toplama için kullanılacak metot, kullanma amacı için önem arz etmez. Kişisel verilerin toplanması için, ilgili kişilerin izlenmesi, resminin çekimi, sesinin kaydı, vücut ölçülerinin tespiti gibi değişik yöntemler kullanılmaktadır. Aynı şekilde, toplama yazılı veya sözlü de olabilir. İşletmeci, veri toplama yöntemi olarak daha çok kişilerin beyanlarına başvurmaktadır. Kişisel verilerin toplanmasında ve ilgililerin rızalarının alınmasında hep yazılılık esası geçerlidir. Elektronik haberleşme alanında kişisel verilerin toplanması; ilgililerin kişisel ilişkilerinin izlenmesi, eğer ilgili kişi belirlenebilir durumda ise, ona götürülecek ipuçlarının elde edilmesi, telefonların dinlenmesi, ilgililerin seslerinin kaydı ve haberleşmeyi sağlayan trafik verilerinin gösterimi vb. hususlar, çeşitli yöntemlerle kişisel veriler işletmeci tarafından toplanabilmektedirler.[95]

Kişisel verilerin depolanması, veri taşıyıcısına yapılacak kayıt ile koruma altına alınması anlamına gelir. Kayıt, depolama işleminin yazı ile gerçekleşen kısmıdır. Koruma altına alma ise, değişik koruma yöntemleri kullanılarak verilerin biriktirilmesi ve depolanmasıdır. Meselâ, ses, video ve film kayıtlarında durum böyledir. Kişisel veriler, veri taşıyıcılarına da kaydedilmektedirler. Veri taşıyıcısının tanımı kanunda tam olarak yer almamıştır. Ancak bundan her türlü veri kaydedilebilen taşıyıcılar anlaşabilir.[96] Meselâ, USB bellek, CD, CD-ROM, MP3, IP, DVD vb. bunlardan bazılarıdır.

---

[94] Üniversitelerde kişisel verilerin toplanması, düzenlenmesi ve saklanması ile ilgili ayrıntılar için bkz, Henkoğlu, age, s. 134-143.
[95] Özdemir, age, s. 135-136.
[96] Özdemir, age, s. 136.

Kişisel verilerin değiştirilmesi, çeşitli neden ve amaçlarla toplanan ve saklanan kişisel verilerin içeriğini değiştirmektir. Değiştirme, toplanıp depolanan kişisel verilerin diğer toplanan kişisel veriler ile irtibatlandırılmasıdır. Her içerik değiştirme, kişisel verilerin korunması açısından birer koruma tedbiridir. Ayrıca değiştirme işlemi gerçekleşirken, söz konusu kişisel verilerin diğer verilerle bağlantıları sağlanmaktadır. Verilerin diğer verilerle bağlantısının sağlanmasında aslında herhangi bir değişiklik söz konusu olmayıp, kişisel verilerin o ana kadar sadece sahip oldukları içerik değişikliğe uğramakta ve bilgilerin saklanma şekilleri de değiştirilmektedir. Meselâ, kişisel veriler, değiştirme işlemleri sonrası şifrelenerek, kriptografi tekniklerinden yararlanarak saklanabilmektedirler. Kişisel verilerin kısaltılmasında da herhangi bir içerik değişikliği söz konusu olmaz. Meselâ, "Doğum Tarihi 38" ifadesinde, aslında bunun açık hali "1938"dir. Kısaltmaların yanı sıra, bazı kişisel verilerin benzerlerinin yazılmasında içerik değişikliği söz konusu değildir. Buna karşılık, doğum tarihinin yanına, ilgili kişinin ölümünün işlenmesinde bir değişiklik söz konusu olur. Çünkü bu son halde ilgili kişinin mevcut kişisel durumu değişmiştir. İşletmeciler de, bu tür değişikliklere dikkat etmelidirler. Öyle ki, abonenin son ev adresinin rehbere veya faturalara işlenmemesi durumunda, abonenin faturaları geç ödemesinden kaynaklanan zararlar için işletmecinin sorumluluğuna gidilebilir.[97]

"Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik"in 8. maddesinde, "*Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.*" şeklinde tanımlanmaktadır.[98] Veri sorumlusu, ilgili kullanıcıların silinen kişisel verilere erişmesini ve bunları kullanmasını engellemek için gerekli her tedbiri almakla yükümlüdür. Silinmenin yöntemi hakkında bilgi verilmemiştir. Ancak bunun veri sorumlusunun görevi olduğu bildirilmiştir. Silme işlemi ile kişisel verilerin tüm kullanım ve erişim alanlarından çıkarılma kastedilmektedir.[99] Diğer bir deyişle silme, bilgisayar ortamında depolanan bilgiler silinerek yapılabileceği gibi, üstünü tamamen karalama gibi kişisel verinin okunmasına engel olabilecek faaliyetlerle de yapılabilir.

---

[97] Özdemir, age, s. 136-137.
[98] Kişisel Verilerin Korunması Kurulu, **Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik,** Ankara, 2017, s. 8-9 ve **Resmi Gazete**, Tarih: 28.10.2017 ve Sayı 30224.
[99] Dülger, age, s. 255-256.

Yazının üzerinde kırmızı kalemle geçme silme eylemi olarak görülmemektedir. Çünkü silme ile esas olan kişisel verinin ortadan kaldırılması veya tamamen okunamaz hale getirilmesidir.[100]

"Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik" kişisel verilerin yok edilmesini, "*Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Veri sorumlusu, kişisel verilerin yok edilmesiyle ilgili gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür*." şeklinde tanımlamaktadır.[101] Görüldüğü üzere tanım sadece sonuç odaklı olarak yapılmaktadır. Kişisel verilerin yok edilmesi, silmeden farklı olarak, "*verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz*" duruma getirilmesidir. İşlem sonucunda ilgili veriye hiçbir surette ulaşılamamaktadır.[102] Yok etme işleminin ne şekilde gerçekleşmesi gerektiği konusunda yol gösterici bilgi Kişisel Verilerin Korunması Kurulu tarafından 2017 yılında yayınlanan "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik"e göre yapılmaktadır.[103]

İlgili Yönetmelik'in 10. maddesinde "K*işisel verilerin anonim hale getirilmesi, kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir*." şeklinde tanımlanmaktadır. Anonim hale getirilme, kişisel verilerin hiçbir yöntemle yeniden bir kişi ile bağlantı kurulamayacak hale getirilmesi işlemidir. Burada önemli bir husus, kişisel verilerin başka veriler ile bir araya getirildiğinde de kimliği belirli ya da belirlenebilir bir kişiyi işaret etmiş olmaması gerekliliğidir. Kişisel verilerin anonim hale getirilmiş sayılması için; kişisel verilerin, geri döndürme de dâhil olmak üzere, başka verilerle eşleştirilme gibi uygun tekniklerin kullanılması yoluyla dahi bir gerçek kişiyle ilişkilendirilemez hale getirilmesi gerekmektedir.[104]

---

[100] Özdemir, age, s. 137.
[101] Kişisel Verilerin Korunması Kurulu, **Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik,** s. 9-12 ve **Resmi Gazete**, Tarih: 28.10.2017 ve Sayı 30224.
[102] Dülger, age, s. 256-257.
[103] Kişisel Verilerin Korunması Kurulu, **Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik,** Ankara, 2017, s. 9-12
[104] Kişisel Verilerin Korunması Kurulu, **Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik,** s.12.

Kanunda kişisel veri, "*kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi*" olarak tanımlanmıştır. Bu nedenle bilginin bir gerçek kişiye belirlemesi veya belirlenebilir olmasını sağlaması ihtimalinin ortadan kaldırılması halinde anonimleştirilme söz konusu olacaktır. Kanuna bağlı kalınarak Yönetmeliğin 10. maddesinde bu esastan hareketle anonimleştirme düzenlenmiştir. Bu iş öyle yapılmalı ki, kişisel veriler başka verilerle eşleştirilse, aralarında bir bağ kurulsa dahi hiçbir surette ait olduğu gerçek kişiyi belirlenebilir bir hale getirmemelidir. Anonimleştirme öyle yapılmalı ki, bunu yapan dahi sonradan geri dönüp ilgili kişiyi belirleyememelidir.[105]

1.1.4.Kişisel verileri işlemenin kapsamı

Veriler üzerinde hangi işlemlerin hangi yollarla gerçekleştirileceğinin sınırlarının belirlenmesi, veri işlemenin kapsamını oluşturmaktadır. Veri işleme genel olarak otomatik veya otomatik olmayan iki yolla gerçekleştirilebilir. Burada kast olunan bir otomasyon sistemi tarafından kullanılan yöntemlerle verilerin işlenmesidir. Örneğin bir işyerinde çalışan işçilerin verilerinin bilgisayar sistemi üzerinde işlenmesi ya da bir üniversitenin, öğrencilerinin not veya öğrenim durumlarına ilişkin bilgilerini bir sistem üzerinde tutması verilerin otomatik yollarla işlenmesidir.[106] Verilerin otomatik veya otomatik olmayan yollarla işlenmiş olması, verilerin korunmasının kapsamına dair genel anlamda bir değişiklik meydana getirmemektedir. Kişisel verinin kâğıt üzerinde veya bilgisayarda tutulması arasında kişisel verinin kabulü açısından da herhangi bir fark bulunmamaktadır.[107] Ancak kâğıt üzerinde diğer bir deyişle otomatik olmayan yollarla veri işlemenin, ancak kaydedilme biçimi itibarıyla işleyene bu veriye erişim açısından belli bir kolaylık sağlaması, bir dosyalama sisteminin parçası olarak veya olması niyetiyle işlenmiş olması gerekmektedir. Ayrıca gerçek kişilerin, şahsi amaçlarla ve sadece kişisel veya ailevi ilişkilerine ilişkin olarak otomatik veya otomatik olmayan yollarla yaptığı veri işleme faaliyetleri koruma kapsamının dışındadır. Örneğin kişinin kendi bilgisayarında tuttuğu annesine ait TC kimlik numarası gibi özel kayıtlar koruma kapsamı dışında tutulmuştur. Zaten bu tür işlemelerde KVKK'nın "*İstisnalar*" başlığı altında madde 28/1 bendine göre kanun

[105] Dülger, age, s. 257-258.
[106] Başalp, age, s. 33.
[107] Aksoy, age, s. 17.

hükümlerinin uygulanmayacağı belirtilmiştir. Yine KVKK'nın "*Kişisel Verilerin İşlenme Şartları*" başlıklı 5. maddesinde ise kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği bildirilmektedir. Bu maddenin ikinci fıkrasında da kişinin açık rızası aranmaksızın kişisel verilerin işlenebileceği haller düzenlenmiştir.[108] Avrupa Konseyi 108 Sayılı Sözleşmesi gibi uluslararası bazı sözleşmeler ve ulusal düzenlemelerle de verilerin yalnızca belli surette işlenmesi korunabilmektedir. Ancak Sözleşme'nin de öngördüğü gibi sadece otomatik yollarla veri işleme faaliyetlerini korumakta olan düzenlemelerde, devletlere koruma kapsamını genişletebilme inisiyatifi de bırakılmıştır.[109]

Otomatik ya da olmayan metotlara dayalı olarak yapılan her türlü toplama, kayıt altına alma, organize etme, depolama, değiştirme veya uyarlama, geri alma/kurtarma, sorma, kullanma, transfer yoluyla açığa çıkarma, yayımlama veya yayımlamaya uygun hale getirme, ilişkilendirilme veya kombinasyon kurma, bloke etme, silme, tahrip etme fiillerinin gerçekleştirilmesi veri işlemesinin kapsamındadır. Direktif'in belirlediği bu fiillere ek olarak düzenlemenin 4. maddesinde yapılandırma ve kısıtlama fiillerinin de işleme kapsamında olduğu kabul edilmiştir. Ulusal veri koruma mevzuatımıza göre de veri işlemenin kapsamı; KVKK madde 3/1/e bendinde "*Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem*" şeklinde belirlenmiştir.[110]

---

[108] Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür: "a) Kanunlarda açıkça öngörülmesi. b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması. c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması. ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması. d) İlgili kişinin kendisi tarafından alenileştirilmiş olması. e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması. f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması."

[109] Sarıusta, agt, s.26.

[110] Sarıusta, agt, s. 27; Şimşek, age, s. 94-96; Küzeci, age, s. 228-230.

Kişisel verilerin, özellikle istatistiksel veya kamusal ihtiyaçların belirlenmesi gibi amaçlarla işlenmesine gerek duyulması durumlarında çoğunlukla verilerin ilişkin olduğu kişilerin kim olduklarının bilinmesine ihtiyaç duyulmamaktadır. Bu gibi durumlarda imkân oranında verilerin anonim olarak ya da takma adlaştırma veya şifrelenme gibi usullerle işlenmesi, veri öznesinin kişisel verilerinin korunması hakkının daha az zarar görmesini veya hiç zarar görmemesini ayrıca kişilerin ifade özgürlüğünü daha serbest şekilde kullanabilmesini sağlayacaktır. Veri öznesinin kimliğine erişimi dolaylı kılan tedbirler olarak; anonimleştirme veya takma adlaştırma yoluyla kişisel verilerin toplanması, tutulması veya benzer şekilde işlenmesi en sık kullanılan yöntemlerdendir. Verilerin anonimleştirilerek veya takma adlaştırılarak işlenmesi, verilerin korunması amacının sağlanmasına ve *"işlemenin asgariliği"* gibi temel veri koruma ilkelerinin önemli ölçüde gerçekleştirilmesine imkân sağlamaktadır. [111]

Yukarıda görüldüğü üzere, KVKK'da baştan sona tüm süreci kapsayan düzenleme yoluna gidilmiştir. Dolayısıyla bu sürecin her aşamasını detaylı olarak incelemek gerekmektedir. Hükümde "*gibi veriler üzerinde gerçekleştirilen her türlü işlem*" ifadesinden işlenmenin kapsamının hükümde yer verilen işlemlerle sınırlı olmadığı anlaşılmaktadır.[112] Hükümde yer verilenler örnekleme niteliğindedir. Zira hükümde yer almasa dahi veriler üstünde gerçekleşen bütün işlemler kişisel verilerin işlenmesi kapsamında değerlendirilecektir.

1.2.Kişisel Verilerin Korunması ve İşlenmesine Yönelik Temel İlkeler

Kişisel verilerin korunması ve işlenmesi konusunda ilkeler belirlenirken, ulusal düzeyde bakılması gereken ilk düzenleme KVKK'dır. KVKK'nın "Genel İlkeler" başlıklı 4. maddesinde kişisel verilerin işlenmesinde uyulacak usul ve esaslar belirtilmiştir. Bunlar daha önce uluslararası düzeyde "108 sayılı Sözleşme" ve "95/46/EC sayılı Avrupa Birliği Direktifi"ne uygun şekilde düzenlenmiştir. Direktif'in 6. maddesinde bu ilkeler beş ayrı madde halinde düzenlenmiştir. Bunlar; "Hukuka ve dürüstlük kurallarına uygun olma", "Doğru ve gerektiğinde güncel olma", "Belirli, açık ve meşru amaçlar için işlenme", "İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü

[111] Sarıusta, agt, s. 27-28.
[112] Özkan, age, s. 83.

olma", "İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme" olarak sıralanmışlardır.[113] Kişisel veri işleme ilkeleri, tüm kişisel veri işleme faaliyetlerinin özü olmalı ve tüm kişisel veri işleme faaliyetleri bu ilkelere uygun olarak yürütülmelidir.

1.2.1.Hukuka ve dürüstlük kurallarına uygun olma

Hukuka ve dürüstlük kuralına uygun olma, kişisel verilerin işlenmesinde kanunlarla ve diğer hukuksal düzenlemelerle getirilen ilkelere uygun hareket edilmesi zorunluluğunu ifade etmektedir.[114] Bu ilke aslında kişisel verilerin işlenmesi sürecinin başından sonuna kadar var olması gereken bir ilkedir. Kişisel verinin işlenmesi, kural olarak, dürüstlük kurallarına uygun olmalıdır. Bu durum özellikle verilerin işlenmesinin saydamlığı açısından önem arz etmektedir.[115]

Hukuka uygun olma ilkesi, KVKK'nın m. 4/2-a bendinde; *"Hukuka ve dürüstlük kurallarına uygun olma"* şeklinde dürüstlük kuralıyla birlikte düzenlenmiştir. İlke, "108 sayılı Avrupa Konseyi Sözleşmesi" 5. maddesinin "a" bendinde kişisel verilerin yasal olarak elde edilip işlenebileceği şeklinde düzenlenmiştir. Nitekim "2016/679 sayılı Genel Veri Koruma Tüzüğü"nün 5. maddesinde düzenlenen ilk temel ilke, kanunilik, dürüstlük ve şeffaflıktır.[116]

Hukuka uygun olma gerekliliği kendi kendini açıklar niteliktedir. Kolaylıkla anlaşılacağı üzere bu gereklilik, kişisel verilerin işlenmesinde yasalarla ve diğer hukuksal düzenlemelerle getirilen ilkelere uygun hareket edilmesi zorunluluğunu ifade eder. Hukuka uygunluk, kanunlar ve tüm hukuki düzenlemelere uyulması gerektiği anlamına gelmektedir. Hatta hukuka uygunluk, sadece mevzuata uygunluğu değil, daha geniş bir anlamı ifade etmektedir. Hukuka uygun olan kanuna da uygundur. Ancak kanuna uygunluk her zaman hukuka uygun anlamına gelmez. Veri işleme sürecinin tamamında hukuka uygun hareket edilmesi gerekir. Zaten aşağıda belirtilen ilkeler de hukuka uygun hareket etme ilkesinin doğal bileşenlerini oluşturacaklardır.

---

[113] Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi**, Ankara, Aralık 2019, s. 63.
[114] Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi**, s. 64-66.
[115] Özdemir, age, s. 137
[116] Sert, age, s. 75-76.

Veri işlemenin KVKK ve diğer tüm hukuk kurallarına uygun olması yeterli değildir. Ayrıca dürüstlük kuralına da uygun olarak yapılması gerekir. Dürüstlük ilkesi de verilerin işlenmesine ilişkin her türlü eylemde dürüstlük[117] ilkesine uyulmasını gerekli kılar. Burada temel sorun "dürüstlük", sınırları belli olan bir kavram değildir ve zaman içinde de değişikliğe uğrayabilir. Bu ilkede dürüstlükten kastedilen veri sorumlusunun veri işlemedeki hedeflerine ulaşmaya çalışırken, ilgili kişilerin çıkarlarını ve makul beklentilerini dikkate alması olarak anlaşılmalıdır.[118]

Veri işleme hukuk ve dürüstlük ilkesine uygun yapılmış olsa bile, bu kendi başına yeterli değildir. Şeffaf olmayan bir işlemenin hukuka ve adalete uygun olarak yapılıp yapılmadığının tespit edilebilmesi oldukça zordur. Bu nedenle hukuk ve adalete uygun olup olmadığından önce, işlemenin şeffaf olarak yapılıp, yapılmadığı çok önemlidir. Şeffaf olmayan hiçbir işlemin hukuk ve dürüstlük ilkelerine uygun olup olmadığının anlaşılabilmesi çok zordur. Ayrıca şeffaflık ilkesi uyarınca ilgili kişiye, veri toplama ve işleme faaliyetleri hususunda gerekli, yeterli ve belirli bilgilerin verilmesi gereklidir.[119]

1.2.2.Doğru ve gerektiğinde güncel olma ilkesi

Kişisel verilerin işlenmesine ilişkin olarak uyulması gereken ikinci ilke, "doğru ve gerektiğinde güncel olma ilkesi"dir. Bu ilke, işlenen kişisel verilerin doğru işlenmesi ve gerektiğinde ya da talep edilmesi halinde güncellenmesine ilişkindir.[120] Aslında bu ilke "*ilgili kişinin verilerinin düzeltilmesini isteme hakkı*"na ilişkindir. 11/1/d bendine göre "*İlgili kişi, verilerin eksik veya yanlış işlenmiş olması halinde bunların düzeltilmesi hakkına sahiptir*." denmektedir. Eğer veriler doğru ve güncel olarak tutulmazsa, bu hüküm ile ilgili kişinin düzeltme hakkı doğacaktır.[121]

Verilerin doğruluğu, bunların işlenme sürecinin sonuna kadar devam etmelidir. Ayrıca veri sahipleri kendilerine ait bilgilerin doğruluklarını zaman zaman kontrol etme hakkına sahiptir. Verilerin, işlenme ile ulaşılmak istenilen amaç için güncel ve doğru kalmaları gerekmektedir. Verilerin doğruluklarının kaybolması durumunda,

---

[117] Dürüstlük TMK 2. Madde.
[118] Küzeci, age, s. 228-230 ve Özkan, age, s. 85-86.
[119] Dülger, age, s. 271-272.
[120] Uyarer, age, s. 125.
[121] Özkan, age, s. 87.

veri sahipleri tarafından bunların kaldırılmaları veya düzeltilmeleri istenebilir. Kullanıcı veya abonelere ait kişisel verilerin yanlış işlenmesi, onların yanlış tanınmalarına ve anılmalarına neden olması halinde hukuka aykırılık gerçekleşir.[122] Yanlış işleme, her türlü gerçek dışı, eksik veya işleme tarzının gereğine aykırı olması durumlarında söz konusu olur. Yanlışlık kişilerden kaynaklanabileceği gibi, bilgisayar veya teknik donanım kaynaklı da olabilir. Veri Koruma Direktifi madde 6/1'e göre "*İşlenecek veriler, güncel, tam ve işlenme amacıyla ilişkili olmalıdır.*" denilmektedir. Örneğin, işletmeci kendi abonelerine ait rehberi belli aralıklarla gözden geçirmeli, bu suretle abonelere ait kişisel verilerin doğruluğu ve güncelliği sağlanmalıdır. Kişisel verilerin güncelliği için verilerin toplanma, işlenme ve saklanmasında her zaman doğru olup olmadığı gözden geçirilmelidir.[123]

1.2.3.Belirli, açık ve meşru amaçlar için işlenme ilkesi

Kısaca "amaca bağlılık ilkesi" olarak da adlandırılan bu ilke kapsamında kişisel verilerin işlenmesi, verilerin işlenme amacının belirli olması ve kişisel verilerin meşru amaçlarla işlenmesi anlamına gelmektedir. Kişisel veriler işlenirken, bu veriler ya bireylerin açık rızası dâhilinde işlenebilecek ya da kanunda belirtilen istisna durumlarda açık rıza aranmaksızın işlenebilecektir. Bu nedenle kişisel verilerin bireylerin açık rızasına dayalı olarak işlenmesi halinde bu açık rızanın hukuka uygun olabilmesi için bireylerin verilerin işleme amaçları konusunda doğru şekilde bilgilendirilmesi gerekmektedir. Burada bireylere açıklanan kişisel verilerin işleme amaçları belirli ve açık olmalıdır. Kişisel verilerin hangi amaç, kapsam, sınır ve süre dâhilinde işleneceği bireylere açık ve net olarak bildirilmelidir.[124]

Bu ilke incelenirken verilerin toplanma amacının belirli ve açık olması, toplanma amacının meşru olması ve işlenme amaçlarının toplanma amacı ile uyumlu olması şeklinde üç alt başlık altında ele alınıp incelenmiştir. Veri sorumlusu veri toplarken amacını net bir şekilde ortaya koymalı, belirlediği amaçla işlediği amaç bağdaşmalı ve son olarak da toplanan ve işlenen verilerin toplanma ve işlenme

---

[122] Özdemir, age, s. 138 ve Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi**, s. 66-67.
[123] Özdemir, age, s. 168. Bu ilkenin AB Veri Koruma Yönergesi ile AK Sözleşmesi'nde yer alışı ile ilgili bkz, Küzeci, age, s. 243-244.
[124] Uyarer, age, s. 125-126 ve Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi**, s. 67-68.

amacına uygun ve uyumlu olarak kullanmalıdır. Veri sorumlusu topladığı kişisel bilgileri ileride işe yarar düşüncesi ile saklamamalıdır. Çünkü böyle bir durum bu ilkenin ihlali anlamına gelmektedir.[125]

1.2.4.İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma

Amaca bağlılık ilkesi, KVKK 4. maddesinde "*Kişisel verilerin, işlendikleri amaçlarla bağlantılı, sınırlı ve ölçülü olması ilkesi, işlenen verilerin belirlenen amaçların gerçekleştirilebilmesine elverişli olmasını, amacın gerçekleştirilmesiyle ilgili olmayan veya ihtiyaç duyulmayan kişisel verilerin işlenmesinden kaçınılmasını gerektirmektedir. Ayrıca işlenen veri, sadece amacın gerçekleştirilmesi için gerekli olanla sınırlı tutulacaktır*." şeklinde açıklanmaktadır.

Bu ilke ile kişisel verilerin niteliği, verilerin işlenme amacı ile uyumlu olmalı, amaç için gerekli olmayan hiçbir kişisel veri işlenmemeli, hangi kişisel verilerin işlenmesi gerekiyorsa sadece onlar işlenmelidir. Bu ilke ile incelenmesi gereken bir başka konu da kişisel verilerin toplanma amaçlarının sınırlandırılmasıdır. Örneğin, birisi bir dergiye abone olmak için cep telefonu numarasını girmiş, ancak kişi daha sonra aranmış ve başka bir şirketin reklamı yapılmıştır. Kişisel verilerin işlenmesinin başlangıç amacı ile bir sonraki kullanım amacı arasında bir fark olduğu görülmektedir. Amaçtaki bu değişiklik, "amaçla sınırlılık" ilkesiyle çelişmektedir. Başka bir deyişle, belirli bir amaç için toplanan veriler yeni veya diğer amaçları kapsamamalıdır.

Burada belirtilmesi gereken bir başka ilke de ölçülülük ilkesidir. Bu ilke ile işlenecek kişisel veri ile işleme amacının arasındaki denge ölçülü olmalıdır. Örneğin, bir spor müsabakasına seyirci olarak gidecek bir kişinin üyelik başvurusunda kişinin aylık geliriyle ilgili bir verinin istenmesi, orantılılık ilkesine aykırı olacaktır.[126]

Danıştay'ın buna yönelik olarak değerlendirdiği bir olayda, çalışma saatlerinin takibi için çalışanın biyometrik verisinin kullanılması işleminde hukuka aykırılık tespit etmiştir.[127]

---

[125] Dülger, age, s. 272-278, Küzeci, age, s. 230-236; Şimşek, age, s. 83 ve Kuşkonmaz, agt, s. 89-92.
[126] Özkan, age, s. 90-92 ve Şimşek, age, s. 98.
[127] " İlgililerden kişisel veri alınması niteliğinde olan, parmak izi taramasının, özel hayatın gizliliği ilkesi kapsamında bulunması karşısında Anayasal ilkeler ve uluslararası sözleşme kuralları ile bağdaşmayan parmak izi sistemiyle yürütülen mesai takibi uygulamasına ilişkin işlemde hukuka uygunluk

1.2.5.İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme

Kişisel verilerin işlenmesine ilişkin son ilke "İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkesi"dir. Bu ilkeyle amaçlanan, hukuka uygun işlenen kişisel verinin, veri sorumlusunca sonsuza kadar tutulmasının engellenmesidir. Ayrıca ilgili ilke, kişisel verilerin korunması ile de ilgilidir. Bu ilkenin olmadığı durumlarda haklı gerekçelerle de olsa, bir kez kişisel verileri elde eden kişi, bunları hayatı boyunca bir yerlerde kullanılmak üzere tutmayı sürdüreceğini ve yeri geldiği zaman da kullanacağını düşüneceğini, bunun da veri sahibinin bireysel özerklik, özel yaşamının gizliliği gibi değerlere zarar verebileceği endişesi dile getirilmiştir.[128]

Kişisel verilerin amaç açısından gereksiz duruma gelmesi, diğer bir ifadeyle hedeflenen amacın ortadan kalkması, amaca ulaşmak için kişisel verilerin işlenmesinin gereksiz olduğunun düşünülmesi ve amaca ulaşıldığı için artık kişisel verinin tutulmasına gerek duyulmaması durumunda kişisel verinin tutulma gerekliliği ortadan kalkabileceği düşünülmüştür. Bunun tam zamanını kestirmek pek de kolay değildir.[129]

bulunmadığı kararı verilmiştir." Danıştay İDDK., 09.12.2015 T., 2014/2242 E., 2015/4991 K. (Kazancı, E.T.: 21.01.2021).

[128] Hatipoğlu, age, s. 91-92.

[129] Küzeci, age, s. 244-246; Şimşek, age, s. 85 ve Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi**, s. 69-70.

İKİNCİ BÖLÜM

KİŞİSEL VERİLERİN KORUNMASINA YÖNELİK ULUSLARARASI VE ULUSAL DÜZENLEMELER

Çalışmamızın birinci bölümünde kavramsal incelemesi yapılan kişisel verilerin korunmasına yönelik detaylı açıklamaların yanı sıra üçüncü bölümde inceleyeceğimiz suç tiplerinin oluşmasına zemin hazırlayan ulusal ve uluslararası düzenlemelere bu bölümde yer verilecektir.

2.1.Kişisel Verilerin Korunmasına Yönelik Uluslararası Düzenlemeler

1980'li yıllarda teknoloji dünyasındaki hızlı gelişmeler ile bilgisayar sistemleri internet ile birbirine bağlanmış, her geçen yıl kullanım ağının da genişlemesi ile kişisel verilere erişimi sadece ulusal değil, uluslararası düzeyde daha mümkün ve açık hale getirmiştir. Bu da kişisel verilerin sadece ulusal düzeyde alınan tedbirlerle korunamayacağı gerçeğini ortaya çıkarmıştır. Ayrıca ulusal düzeyde depolanan verilerin ülkeler arasında aktarılmaya başlanması, kişisel verilerin korunması sorununa uluslararası bir boyut kazandırmış, böylece uluslararası veri bankalarında tutulan kişisel verilerin uluslararası boyutta korunması, toplanması, işlenmesi ve yayılmasına ilişkin düzenlemelerin uygulanmasında işbirliğini ve devletlerin ortak hukuki zeminde buluşmasını zorunlu hale getirmiştir. Dolayısıyla birçok devlet ve uluslararası kuruluş, kişisel verilerin korunmasıyla ilgili daha etkin politikalar belirlemek ve düzenlemeler yapmak amacıyla çalışmalar yapmışlardır.[130]

Kişisel verilerin korunmasının, ilk etapta kişisel verilerin korunması ile değil de bununla yakın ilişkili olduğu düşünülen özel yaşamın gizliliği hakkı şeklinde, pek çok insan hakları belgesinde güvence altına alındığı görülmektedir. "Birleşmiş Milletler (BM) İnsan Hakları Evrensel Bildirisi", "BM Medeni ve Siyasi Haklara İlişkin Uluslararası Sözleşme", "Avrupa İnsan Hakları Sözleşmesi" ve "Amerikalılar Arası İnsan Hakları Sözleşmesi" gibi düzenlemeler bunlara örnek gösterilebilir.

[130] Kuşkonmaz, agt, s. 37; Korkmaz, age, s. 155 ve Ceren Yakışır, **Türk Ceza Kanunu'nda Kişisel Verilerin Basın Yoluyla Açıklanması Suçu**, 1. Baskı, On İki Levha Yayıncılık, İstanbul, 2019, s. 44.

Bunları, doğrudan kişisel verilerin korunmasına yönelik adımların atıldığı düzenlemeler takip etmiştir.[131] Bu düzenlemeler "Ekonomik İşbirliği ve Kalkınma Örgütü (OECD)", "Birleşmiş Milletler (BM)", "Avrupa Konseyi (AK)", "Avrupa Birliği (AB)" gibi kuruluşlar tarafından yapılmıştır.

2.1.1.Ekonomik İşbirliği ve Kalkınma Örgütü (OECD) düzenlemelerinde kişisel verilerin korunması

Uluslararası düzeyde kişisel verilerin korunmasına ilişkin ilk adım, 1947 tarihli "Avrupa Ekonomik İşbirliği Örgütü" olarak kurulan ve 1961 tarihinde daha birçok üyenin katılımı ile ismi değiştirilen OECD[132] tarafından atılmıştır. OECD'nin temel amacı üye ülkelerde demokrasi, insan ve vatandaşlık haklarının geliştirilmesi ile halkın yaşam standardının, ekonomisinin iyileştirilmesi, işsizliğin ortadan kaldırılması, dünya ticaretinin geliştirilmesinin desteklenmesidir.[133] Bu örgütün kişisel verilerle ilgili düzenleme yapma ihtiyacı daha çok üye devletlerin ekonomik anlamda geliştirilmesi amacından kaynaklanmıştır.

Kişisel verilerin ülkeler arasında değişimini gerçekleştirmek üzere OECD bünyesinde 1978 yılında bir grup kurulmuş ve bu grup kişisel verilerin değişimi için gerekli olan tedbirlerin hazırlanmasına yönelik olarak çalışmıştır. Daha sonraları OECD veri bankalarının her alanda kullanılmasıyla birlikte, kişisel verilerin toplanması ve transferi, eskiye oranla kolaylaştığı görülmüştür. Ancak bu kolaylıklar özel hayata karşı yapılan saldırıları da beraberinde getirmiştir. Bu durum karşısında OECD kişisel verileri korumak ve veri aktarımına bir düzen getirmek amacıyla 23 Eylül 1980 tarihinde "*Mahremiyetin Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeleri*" adıyla bir düzenlemeyi kabul etmiştir.[134]

"OECD Rehber İlkeleri" bağlayıcı olmamakla birlikte konuyu uluslararası ölçekte ele alan ilk düzenlemedir. Ulusal ve uluslararası düzeyde sonraki düzenlemelere de temel olmuştur.[135] Bu belge kişisel verilerin toplanması, yönetilmesi

---

[131] Küzeci, age, s.127.
[132] https://www.oecd.org/about/ E.T: 20.02.2021.
[133] Türkiye bu örgüte 1961 yılında üye olmuştur. Örgütün aldığı kararlar tavsiye niteliğindedir ve bağlayıcılığı bulunmamaktadır. Dülger, age, s. 86; Küzeci, age, s.129-130; Korkmaz, age, s. 155-156 ve Yakışır, age, s. 50.
[134] http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm E.T: 20.02.2021.
[135] Sarıusta, agt, s. 57-58.

ve korunması ile sınır ötesi paylaşımında temel ilkelerin belirlenmesi amacıyla hükümetlerin, sivil toplum örgütleri ve iş dünyasının katılımı ile kabul edilmiştir. Bu Rehber İlkeleri ile üye ülkelerde moral ve fikri altyapının kurulması yanında otomatik veri işleme yöntemlerinin geliştirilmesi amaçlanmıştır. Büyük miktardaki verilerin kısa sürede sınır ötesine iletilmesi mümkün olabilmektedir. Bu nedenle kişisel verilerle ilgili gizliliğin korunmasına yönelik ilkelerin belirlenmesine ihtiyaç duyulduğu, ayrıca kişisel verilerin yasal olmayan yollarla kaydedilmesi, depolanması veya bunların yetkisiz olarak açıklanması ve suiistimalinin insan haklarına aykırı olacağı, gittikçe artan veri aktarımı üzerine bazı sınırlamalara gidilmesinin gerektiği belirtilmiştir.[136]

OECD Rehber İlkeleri, kişisel verilerin korunmasında üye ülkelerin iç hukuklarında uygulanması gerekli asgari şartları ortaya koymuştur. Bu ilkeler gereğince kişisel veriler hukuk ve dürüstlük kuralları çerçevesinde, kişisel veri sahibinin bilgilendirilmesi ve rızası dâhilinde sınırlı şekilde toplanmalıdır. [137] Kişisel veriler toplanma amaçlarına uygun olarak kullanılmalı ve bu amaçların gereklilikleri kapsamında doğru, tam ve güncel olmalıdır. [138] Kişisel verilerin toplanmasına ilişkin amaçlar en geç kişisel verilerin toplanması sırasında belirli olmalıdır. Bundan sonrasında gerçekleşecek tüm kullanımlar, bu amaçlarla bağdaşmalı bunun yanında bu amaçların değişmesi durumunda bildirilmelidir.[139] Kişisel veriler, ilgilinin rızası veya hukukun gereklilikleri hariç olmak üzere, açıklanmamalı, ulaşılabilir hale getirilmemeli veya belirlenen amaçlar dışında kullanılmamalıdır. Kişisel veriler, olası bir kaybolma veya yetkisiz erişim, yok etme, kullanma, modifiye etme veya açıklanma risklerine karşı makul güvenlik önlemleriyle korunmalıdır.[140] Kişisel verilere ilişkin olarak genel bir aleniyet politikası olmalıdır. Dolayısıyla kişisel verilerin mevcudiyetine ilişkin araçlar, kullanıma ilişkin amaçlar, kişisel veri sorumlusunun kimliği ve adresiyle birlikte hazır edilmelidir.[141] Bireylerin veri sorumlusundan bireyin kendisine ait bir veri bulundurup bulundurmadığına ilişkin bilgi veya onay alma hakkı

[136] Ayözger, age, s. 68.
[137] Nil Melek Gültekin, "Kişisel Verilerin Ceza Hukuku Yönünden Korunması", Galatasaray Üniversitesi, Sosyal Bilimler Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, İstanbul, Mayıs 2012, s. 13-14.
[138] Çokmutlu, agt, s. 74-75.
[139] Kuşkonmaz, agt, s.40-41.
[140] Şimşek, age, s.15-16.
[141] Akgül, age, s. 171.

olmalıdır. Bireyin bu noktada veri sorumlusuyla iletişim kurarak kendisiyle ilgili bilgilere ilişkin gerekliyse makul bir ücret karşılığında, usulüne uygun bir şekilde ve kendisinin anlayabileceği bir biçimde bilgi alma hakkı olmalıdır. Bu talebin reddedilmesi halinde itiraz etme hakkı, kabul edilmesi durumunda ise verilerinin silinmesi veya değiştirilmesi hakkı bireye verilmelidir. Veri sorumlusu bahsedilen bu durumlara ilişkin tedbir almak ve hesap verme yükümlülüğüne uymak durumundadır.[142]

Açıklanan bu ilkeler kendi türünde ilk örnek olması yanında, Asya, Amerika ve Avrupa kıtalarındaki değişik kültür ve yönetim biçimine sahip ülkeler kişisel verilerin korunması hakkında yukarıda belirtilen sekiz ilke üzerine uzlaşmışlardır. Bu ilkelerin üye ülkeler bakımından bağlayıcılığı olmasa bile, üye ülkelerin bu ilkeleri esas aldığı söylenebilir. Ayrıca bu ilkeler birçok ulusal ve uluslararası metinlere temel olmuş içeriklerine doğrudan etkili olmuştur. Türkiye'de de KVKK'nın gerekçesinde OECD Rehber İlkeleri'ne atıfta bulunulması bu etkinin hala devam ettiğinin bir göstergesidir.[143] OECD, 1980 yılında Rehber İlkeleri yayınladıktan sonra bünyesinde kurulan grup tarafından çalışmalara devam edilmiş ve spam ile mücadeleye dair yayınlar dışında birçok yayın yapılmıştır.[144]

OECD Rehber İlkeleri ile ilgili getirilen eleştiriler ise, yukarıda belirtildiği gibi, ülkeler için bağlayıcı olmamaları, ilkelerin uygulanmasına dair yol gösterici belgelere çok az yer verilmesi ve yeterli açık ifadelerden uzak olmaları[145] şeklinde sıralanmıştır. OECD'nin ekonomik ağırlıklı bir teşkilat olması ve amacının da üyelerinin ekonomik gelişmelerini desteklemek olması nedeniyle, kişisel verilerin korunması hususunu insan hakları kapsamında değerlendirme eğilimi yerine ulusal ve uluslararası düzeyde ticaretin konusu olan önemli meta olarak değerlendirilmesi sonucunu doğurmuştur. Dolayısıyla OECD Rehber İlkeler'de mevcut sekiz ilkeyi daha çok ekonomik öncelik

[142] Uyarer, age, s. 44.
[143] Kuşkonmaz, agt, s. 42 ve Korkmaz, age, s.157-158.
[144] Küzeci, age, s. 131-132 ve Dülger, age, s. 86-87.
[145] Özdemir, age, s. 19-20 ve Korkmaz, age, s. 157.

ve kaygılarla çıkarmıştır. Verilerin korunması yoluyla özel hayatın gizliliğinin korunması OECD için ikinci konumda kalmıştır.[146]

2.1.2.Birleşmiş Milletler düzenlemelerinde kişisel verilerin korunması

II. Dünya Savaşı'nın yıkıcı etkilerini ortadan kaldırmak, uluslararası barış ve güvenliği sağlamak, böyle yıkıcı bir savaşın tekrar etmesine engel olmak üzere 24 Ekim 1945 tarihinde Türkiye dâhil 51 üye devletin katılımı ile Birleşmiş Milletler kurulmuştur. BM'nin günümüzdeki üye sayısı da 193'e ulaşmıştır.[147]

BM'nin kuruluşundan kısa bir süre sonra 10 Aralık 1948 tarihinde "*İnsan Hakları Evrensel Bildirisi*" kabul edilmiştir. Bu Bildiri insan haklarının korunması alanında dünya ölçeğinde standart belirleme sürecinin ilk adımıdır. Bu Bildiri'nin 12. maddesinde "*Hiç kimsenin özel ve aile hayatı, konutu veya haberleşmesi keyfi olarak müdahaleye; şerefi ve itibarı saldırıya maruz bırakılamaz. Herkes bu tür müdahalelere veya saldırılara karşı hukuk tarafından korunma hakkına sahiptir."* düzenlemesi ile özel hayatın gizliliğine verdiği değeri ortaya koymaktadır.

1976 yılında yürürlüğe giren "*Birleşmiş Milletler Medeni ve Siyasal Haklara İlişkin Uluslararası Sözleşme*"nin[148] "*Mahremiyet Hakkı*" başlıklı 17. maddesinde de yukarıda 12. maddede belirtilen ifadelerle paralellik göstermektedir.

---

[146] İkbal Gür, "Kişisel Verilerin Korunması Hususunda AB ile ABD Arasında Çıkan Uyuşmazlıklar ve Çözüm Yolları", Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, Ankara, 2009, s. 12-15.

[147] https://www.un.org/en/about-us/ E.T: 21.02.2021.

[148] "BM Medeni ve Siyasal Haklara İlişkin Sözleşme 19.06.1966 tarihinde kabul edilmiş ve 23.03.1976'da yürürlüğe girmiştir. Türkiye Sözleşmeyi 15.8.2000'de imzalamıştır. BM Medeni ve Siyasal Haklara İlişkin Sözleşme'nin Uygun Bulunduğuna Dair 4868 sayılı Kanun, 18.6.2003 tarih ve 25142 sayılı Resmi Gazetede ve BM Medeni ve Siyasal Haklara İlişkin Sözleşme İlişik Beyanlar ve Çekince ile Onaylanmasına Dair Karar ise 21.07.2003, 25175 Resmi Gazetede yayınlanmıştır. Türkiye 23.09.2003 tarihinde Sözleşme'nin tarafı olmuştur." Sözleşme'nin Türkçe metni için bkz; http://www.tbmm.gov.tr/komisyon/insanhaklari/pdf01/53-73.pdf, E.T: 09.07.2021.

"BM İnsan Hakları Komitesi", 16. Genel Yorumu'nda[149], kişisel verilerin korunmasının "BM Medeni ve Siyasal Haklara İlişkin Sözleşme"nin 17. maddesi[150] kapsamında olduğu, kişisel verilerin toplanması ve saklanmasının hukuki düzenlemeye tabi olması gerektiği belirtilmiştir. Ayrıca Komite, devletlerin, kişisel verilerin Sözleşme'nin amacına aykırı olarak kullanılması ve yetkisiz kişilerin eline geçmesini engelleyici tedbirler alması gerektiğini belirtmiştir. Komiteye göre, bireyler, özel hayatlarının güvence altına alınabilmesini sağlamak için kendileri hakkında tutulan verilerin içeriklerini ve saklama amaçlarını öğrenebilmeli, ayrıca kendileri hakkında tutulan yanlış verilerin düzeltilmesini veya kaldırılmasını da isteyebilmelidirler.[151]

BM'nin kişisel verilerin korunması ile ilgili yaptığı doğrudan çalışma, 1990 yılında kabul edilen ve tavsiye niteliğinde olan "Bilgisayara Geçirilmiş Kişisel Veri Dosyalarının Düzenlenmesine İlişkin Rehber İlkeler"dir.[152] Başlığından da anlaşılacağı üzere, kişisel verilerin korunmasına ilişkin getirilen bu düzenleme Birleşmiş Milletlere dâhil devletler için bağlayıcı olmayıp yalnızca yol gösterici niteliktedir ve kişisel verilerin korunması için yetkili ve bağımsız koruma organlarının kurulması gerekliliğini ifade eden uluslararası hukuk bağlamındaki ilk belgedir.[153] Bu belgede belirtilen ilkeler "Meşruluk ve dürüstlük, doğruluk, amacın belirliliği, ilgili

---

[149] "Kamu otoritelerinin, özel kişi ve kurumların bilgisayarlarda, veri bankalarında veya benzeri cihazlarda kişisel bilgileri toplaması veya saklaması hukuki düzenlemeye tabi olmalıdır. Devletler, bir kimsenin özel hayatına dair bilgilerin hukuken bu bilgilere sahip olma ve kullanma yetkisine sahip olmayanların eline geçmesini ve bu bilgilerin Sözleşme'nin amaçlarına aykırılık teşkil edecek şekilde kullanılmasını engellemek için etkili tedbirler almalıdır. Özel hayatın gizliliğinin en etkili şekilde korunabilmesi için, her birey kişisel dosyalarda veya veri tabanlarında kendisiyle ilgili bilgiler saklanmışsa bu bilgilerin ne tür bilgiler olduğunu ve ne amaçla saklandığını öğrenme hakkına sahiptir. Ayrıca, her birey hangi kamu otoritelerinin, özel kişileri veya kurumların bu dosyaları kontrol altında tuttuğunu veya tutabileceğini öğrenebilmelidir. Söz konusu dosyaların, yanlış kişisel bilgilere yer vermesi hâlinde veya bu bilgilerin hukuka aykırı şekilde toplanması veya kullanılması hâlinde her birey düzeltme veya bilgilerin ortadan kaldırılmasını talep etme hakkına sahiptir." (BM İnsan Hakları Komitesi, 32. Oturum, Genel Yorum No:16, Y.1988, Madde 17: Özel Yaşamın Gizliliği, par.7, 10, B); Aktaran Yılmaz, agt, s. 126.

[150] Birleşmiş Milletler Medeni ve Siyasal Haklara İlişkin Uluslararası Sözleşme'nin 17. Maddesinde "(1) Hiç kimsenin özel ve aile yaşamına, konutuna veya haberleşmesine keyfi veya hukuka aykırı olarak müdahale edilemez; onuru veya itibarı hukuka aykırı saldırılara maruz bırakılamaz. (2) Herkesin, bu gibi müdahalelere ya da tecavüzlere karşı yasalarca korunma hakkı vardır." denilerek kişinin özel hayatı ve mahremiyet hakkı korunmuştur.

[151] Aktaran Küzeci, s.122-123; Bygrave, Lee A., Data Protection Pursuant to the Right to Privacy in Human Rights Treaties, International Journal of Law and Information Technology, C.6, S. 3, 1998, s. 253; KUŞKONMAZ, s. 44.

[152] Genel Kurul tarafından 14 Aralık 1990 tarihinde kabul edilmiştir. Metnin tamamı için bkz. http://www.unhcr.org/refworld/pdfid/3ddcafaac.pdf, E.T: 28.07.2021.

[153] Şimşek, age, s. 16.

kişinin erişimi, ayrımcılık yasağı, veri güvenliği, denetim ve yaptırım, sınır ötesi veri akışı" şeklinde sıralanmıştır.[154]

2.1.3.Avrupa Konseyi düzenlemelerinde kişisel verilerin korunması

2.1.3.1.Genel olarak

Kişisel verilerin korunması konusunda önemli çalışmalar yürüten uluslararası kuruluşlardan biri de "Avrupa Konseyi"dir. Avrupa Konseyi, 5 Mayıs 1949 tarihinde 10 Avrupa ülkesi tarafından kurulmuştur. İkinci Dünya savaşı sonrası kalıcı barışı sağlamak ve tahribatları gidermek için kurulan Avrupa Konseyi'nin temel amacı da insan hakları, demokrasi ve hukuk devleti ilkesi kavramlarını korumak ve bu kavramların üye ülkelerde uyum içinde gelişmesini sağlamaktır.[155] Kişisel verilerin korunmasına yönelik çalışmalar yapmıştır. Bunlardan ilki, 1970'li yıllarda bilişim alanındaki gelişmeler karşısında özel hayatın ve kişisel verilerin korunmasında yetersiz kalınması nedeniyle özel hayatın korunması için gerekli ilkeleri belirlemek üzere 1973 ve 1974 yıllarında iki tavsiye kararı almıştır. Bu tavsiye kararları birçok batı Avrupa ülkesinde kişisel verileri korumağa yönelik kanunlar çıkarılmasına neden olmuştur.[156] Son olarak da 28 Ocak 1981 tarihinde kişisel verilerin korunması alanında "Avrupa Konseyi" 108 no'lu *"Kişisel Verilerin, Otomatik İşlenmesinde Gerçek Kişilerin Korunmasına"* ilişkin sözleşmeyi kabul etmiştir.

Avrupa Konseyi'nin kabul etmiş olduğu sözleşmeler, OECD ve Birleşmiş Milletlerin kabul etmiş oldukları direktiflerden farklı olarak AB'ye üye ülkeler için bağlayıcı durumdadır. İmzalandığı dönemde Avrupa ve milletlerarası hukuku etkilemiştir.

2.1.3.2.108 Sayılı Sözleşme

"Avrupa Konseyi", 28 Ocak 1981 tarihinde "*108 Nolu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi*"ni imzaya açmıştır. Sözleşmenin üye devletler tarafından imzalanarak yürürlüğe girmesi ancak 1 Ekim 1985 tarihinde gerçekleşmiştir. Türkiye bu Sözleşmeyi diğer ülkelerle beraber 1981 yılında imzalamış, ancak uygulamaya koyan son ülke olmuştur.

---

[154] Bu ilkelerle ilgili ayrıntılar için bkz, Ayözger, age, s. 70-71 ve Gültekin, age, s. 28-29.
[155] Çokmutlu, agt, s. 15-16, Özdemir, age, s. 20 ve Küzeci, age, s. 138-139.
[156] Korkmaz, age, s.161-162 ve Dülger, age, s. 90.

Sözleşme, 17 Mart 2016 tarihinde de Resmi Gazetede[157] yayınlanarak Türkiye açısından bağlayıcı duruma gelmiştir.

Bu Sözleşme, kişisel verilerin korunması açısından önemli bir yere sahiptir. Bunun nedeni de kendisinden sonra gelen ve bu alanda yapılan her türlü hukuki düzenlemeye kaynaklık etmiş ve yol göstermiştir. Sözleşme'nin bir diğer önemi de yalnız Avrupa Konseyi'ne üye ülkeler değil, üye olmayan ülkelerin imzasına da açılmasıdır. Çünkü kişisel verilerin korunması ve aktarımında karşılaşılan sorunlar sadece bazı ülkelerin değil, tüm dünyanın sorunu olarak algılanmış ve bu çerçevede çözüm üretilmeye girişilmiştir. Bu sebepten Sözleşme, yalnız Avrupa Konseyi üyelerinin değil, diğer tüm devletlerin imza ve onayına açılmıştır.[158] Sözleşme, kişisel verilerin korunması alanında bağlayıcı olan tek uluslararası metindir.

Sözleşme, kişisel verilerin korunması alanında uluslararası bir standardın gerçekleştirilmesine ve iç hukukta veri korumasının güçlendirilmesine katkı yapmıştır. Taraf devletler Sözleşme'de bulunan ilkeleri kendi iç hukuklarının bir parçası haline getireceklerdir. Sözleşme, üye ülkeler için bir öneriden çok yükümlülük olarak değerlendirilmiştir. Sözleşme'nin amacı üye devletlerde bireyin temel hak ve özgürlüklerini, bu bağlamda özellikle kişisel verilerin otomatik bilgi işleme tabi tutulması karşısında özel yaşamın gizliliği hakkını güvence altına almaktır.[159] Buradan otomatik yollarla işleme tabi tutulmayan diğer bir deyişle elle tutulan veriler, bu Sözleşmeye göre koruma kalkanı altında bulunmayacaklardır. Ancak Sözleşme'ye göre "*otomatik işlem*"den kasıt, sürecin tamamında değil de bir kısmı otomatik işlenen veriler olsa bile koruma güvencesinin geçerli olacağı belirtilmiştir.

Sözleşme'de sektörel ayrım yapılmamış; Sözleşme ilkelerinin özel ve kamu sektöründe bulunan veriler için uygulanabileceği ve her iki tür veri için koruma sağlayacağı ifade edilmiştir. Ayrıca taraf devletlere önemli seçenekler verilmiş, istemeleri durumunda bu ilkeleri sadece gerçek kişileri değil de tüzel kişileri, hatta

[157] RG., T: 17.03.2016, S: 29656.
[158] Uyarer, age, s. 48-50 ve Kuşkonmaz, agt, s. 48-50,
[159] Henkoğlu, age, s. 55.

otomatik olmayan verileri de kapsayacak şekilde genişletebilecekleri beyan edilmiştir.[160]

Sözleşme'de kişisel verilerin işlenmesi konusunda uyulması gereken ilkeler de düzenlenmiştir. Buna göre kişisel veriler hukuka uygun olarak toplanmalı, amacına uygun olarak ve yine bu amaçlar için yeterli şekilde işlenmelidir. Bunun yanında verilerin doğru olması ve güncellenmesi, toplanma amacının gerektirdiği süreyi geçmeyecek şekilde saklanması öngörülmüştür. Hassas kişisel verilerin özel olarak korunması talep edilmektedir. Hassas veri olarak da insanların ırk, din ve inançları yanında, cinsel yaşam ve sağlıklarına ait her türlü kişisel veriler kastedilmiştir. Verilerin işlenmesi sonrasında korunması için alınması gerekli tedbirler, diğer bir ifade ile verilerin değiştirilmesi ya da ortadan kaldırılmasına yönelik önlemler düzenlenmiştir. Ayrıca veri sahibine sağlanan haklar, verinin işlenip işlenmediğini öğrenme, hukuka aykırı işlenmişse sildirtme, yanlış verileri düzeltme, bu hakları kullandırılmadığı durumda itiraz hakkı düzenlenmiştir. Yukarıda sayılan hakların kullanımına hangi durumlarda sınırlama getirileceği belirtilmiştir. Fakat bu sınırlamanın sınırları da aşağıda belirtilen konularla sınırlandırılmıştır. Buna göre sınırlamaların, ancak yasa ile devletin ve kamu güvenliğinin tehlikeye girmesi, kamu menfaatlerinin korunması, suçlarla mücadele, ilgili kişi veya başkalarının hak ve özgürlüklerinin korunması gibi durumlarda getirilebileceği belirtilmiştir.

Sözleşme ile Sözleşmede yer alan hükümleri yorumlamak ve uygulamaları geliştirmekten sorumlu bir Danışma Komitesi kurulmuştur. Bu Komitenin diğer bir görevi de kişisel verilerin korunması hakkında raporlar hazırlamak ve rehber ilkeleri geliştirmektir.[161] Bu Komite, Sözleşme'ye ek bir protokol hazırlamış ve bu ek Protokol 8 Kasım 2001 tarihinde imzalanmış, ancak 1 Temmuz 2004 tarihinde yürürlüğe girmiştir. Ek Protokol, iki kısımdan meydana gelmektedir. İlk kısımda ulusal kontrol sisteminin oluşturulması, kontrolün tamamen sözleşmeye taraf ülkelerin kabul edecekleri yasalar çerçevesinde düzenlenmesine vurgu yapılmıştır. Protokolde ayrıca verilerin korunması ile ilgili denetim ve kontrolü yapacak bir denetim mekanizmasının kurulması tavsiye edilmiştir. Diğer kısımda ise kişisel verilerin 3. ülkelere transferine

[160] Songül Atak, "Avrupa Konseyi'nin Kişisel Veriler Açısından Sağladığı Temel Güvenceler", **Türkiye Barolar Birliği Dergisi**, Sayı 87, 2010, s. 90.
[161] Küzeci, age, s. 147-148; Gültekin, age, s. 18 ve Kuşkonmaz, agt, s. 51.

yönelik düzenlemelere yer verilmiştir. Kişisel verilerin gönderileceği ülke ya da kuruluşun, transferin gerçekleştirilebilmesi için uygun veri koruma seviyesini göstermesi zorunlu kılınmıştır. Böyle bir seviye ya da güvence veremezse, verilerin gönderilmesinin mümkün olmayacağı belirtilmiştir. Bu da, 3. ülkeleri Sözleşme ve Ek Protokolü imzalamak zorunda bırakmıştır. Kamu yararı veya güvenlik söz konusu olduğunda uygunluk şartı gerekli görülmemiştir.[162]

Avrupa Konseyi'nin kabul etmiş olduğu 108 sayılı Sözleşme ile Ek Protokol, AB'ye üye ülkeler arasındaki işbirliğini geliştirmesine katkı sağlamıştır. Fakat sözleşmelerde yer alan ilkeleri gerçekleştirecek yaptırım ve mekanizmalara sahip olmaması, eksiklik ve zaaf olarak değerlendirilmiştir. Ayrıca üye devletlerde kişisel verilerin korunmasına dair uyum çalışmalarında yetersiz kaldığı yönünde eleştiriler de yapılmıştır.[163] Tüm bu olumsuzluklar bir yana, 108 sayılı Sözleşme ve Ek Protokol, uluslararası hukuk anlamında bağlayıcılığı ve kişisel verilerin korunması konusunda yaptığı büyük etki nedeniyle büyük bir boşluğu doldurmuştur.

Ek Protokol ile ilgili ise bunun kendi başına bağımsız bir veri koruma organı olmak için yeterli olmadığı, AB tarafından çıkarılan ve ileride ayrıntılı olarak incelenecek olan 95/46/AT sayılı koruma yönergesinin bir benzeri olmaktan öteye gidemediği şeklinde eleştirilmiştir.[164]

2.1.3.3.AİHS 8. madde

"Avrupa Konseyi" tarafından kişisel verilerin korunmasına yönelik dikkate değer metinlerden biri de "*Avupa İnsan Hakları Sözleşmesi*"dir.[165] AİHS imzaya açıldığı günden beri insan hakları alanında en önemli kaynaklardan biri olma özelliğini korumuştur. Ancak AİHS'de kişisel verilerin korunması, bağımsız bir hak alanı olarak

---

[162] Özdemir, age, s. 22-23; Şimşek, age, s. 27-29 ve Kılınç, agm, s. 1116-1117.
[163] Özdemir, age, s. 23 ve Kuşkonmaz, agt, s. 52.
[164] Dülger, age, s. 98.
[165]"Avrupa İnsan Hakları Sözleşmesi, tam adıyla *İnsan Hakları ve Temel Özgürlüklerin Korunması Sözleşmesi* 4 Kasım 1950 tarihinde Roma'da imzalanmış, 3 Eylül 1953 tarihinde 10 devletin onaylaması ile işlerlik kazanmıştır. Türkiye AİHS'nin onaylama sürecini 18 Mayıs 1954 tarihinde tamamlamıştır. 28 Ocak 1987 tarihinde Avrupa İnsan Hakları Komisyonu'na, 22 Ocak 1990 tarihinde ise Avrupa İnsan Hakları Divanı'na bireysel başvuru hakkının tanınması ile Sözleşme'nin Türkiye açısından asıl önemi ortaya çıkmıştır. AİHS'nin asıl önemi ortak güvence sistemine dayanan uluslararası bir yargısal denetim mekanizması kurması ve bireye sağlanan güvenceyi yaptırıma bağlamasıdır. Böylece Sözleşme, insan haklarının korunması sorununu ulusal düzeyden uluslararası düzeye taşımış, birey uluslararası hukukun süjesi haline gelmiştir." A. Şeref Gözübüyük-Feyyaz Gölcüklü, **Avrupa İnsan Hakları Sözleşmesi ve Uygulaması**, Turhan Kitapevi, Ankara, 2009, s. 11.

yer almamakta, AİHS'nin 8. maddesi çerçevesinde koruma altına alınmaktadır. AİHS'nin "*Özel ve aile hayatına saygı*" başlıklı 8. maddesinde "*(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 emniyeti, ülkenin ekonomik refahı, dirlik ve düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için, demokratik bir toplumda zorunlu olan ölçüde ve hukuka uygun olmak şartıyla söz konusu olabilir"* hükümleriyle özel ve aile yaşamı koruma altına alınmıştır.

AİHS'nin 8. maddesinin ilk bölümünde bireye dört alanda koruma sunulmaktadır. Bunlar kişinin özel yaşamı, aile yaşamı, evi ve haberleşmesi şeklindedir. İkinci fıkrasında ise birinci fıkrada koruma altına alınan temel haklara yönelik müdahalelerin hangi durumlarda yasal kabul edileceği ile ilgili durumlara yer verilmiştir.[166] Özel yaşamın korunması hakkı yukarıda sayılanlar arasında en geniş alanı kapsayandır. Bu alana kişisel verilerin korunması konusunun girip girmeyeceği ise Avrupa İnsan Hakları Mahkemesi'nin kararlarına başvurmakla açıklığa kavuşturulabilir. Nitekim AİHM, 8. maddenin veri koruma alanında uygulanıp uygulanmayacağı konusunda tereddüde düşmüş ve çekingen davranmıştır. Mesela 1930'lı yıllarda Hitler döneminde Almanya'da tutuklanan bir gazetecinin kişisel verileri kaydedilmiştir. Savaş sonrası verilerin silinmesi istenince, ilgili kişinin şüpheli halinin sürdüğü ve ilgilinin kişisel verilerinin tutulmasının devletin korunması için gerekli olduğu, bu yüzden verilerin toplanma, işlenme ve tutulmasının hukuka uygun olduğu beyanla dava reddedilmiştir.[167]

Ancak ilerleyen dönemde veri korunması ile ilgili kabul edilen kararlar da olmuştur. Kişisel verilerin korunması hakkında AİHM'in ilk kabul ettiği karar Leander/İsveç kararıdır. Bu kararda, "*Askeri alanda yer alan bir müzede teknisyen olarak çalışan Leander'in özel eşyalarının iş girişinde kontrol amacıyla terk etmesi gerektiği kendisine bildirilmiştir. Buna gerekçe olarak da, devlet güvenliği gösterilmiştir. Leander, bunun devlet güvenliği ile ilgili olmadığını, ayrıca ilgili*

---

[166] Sarıusta, agt, s. 63-64; Küzeci, age, s. 152-153 ve Kuşkonmaz, agt, s. 53-54.

[167] X/Almanya, 4 Ekim 1962, Yearbook 5, s. 230 vd. https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-104610&filename=G.%20W.%20v.%20THE%20FEDERAL%20REPUBLIC%20OF%20GERMANY.pdf E.T: 03.06.2021; aktaran. Özdemir, age, s. 30.

kişilerin de kontrol yapmaya yetkili olmadıklarını belirtmiştir. Avrupa İnsan Hakları Mahkemesi, kişiye ait verilerin toplanıp işlenmesi ve iletilmesinin AİHS. m. 8/II anlamında kişisel hayatı ihlâl ettiğini ilk kez bu olayda kabul ederek tazminata" hükmetmiştir.[168]

AİHM özel hayat alanının sınırlarını önündeki her dosyanın kendine has özelliklere göre belirlemektedir. Örneğin AİHM, Z./Finlandiya Davası'nda verdiği kararda özel hayat kavramını "*kişilerin mahrem alanı ile sınırlı görmemekte, kişilerin özel hayatlarının iç çemberi dışında kalan ve başkalarıyla ilişki kurdukları alanı da kapsayacak şekilde*" değerlendirmektedir. İlgili değerlendirme kişisel verileri korumaya yönelik olarak önem teşkil etmektedir. Buna göre özel hayat; mahrem alan ile sınırlı görülmeyecektir. Dolayısıyla bu çerçevede kişinin sadece ev telefonu değil iş telefonunun dinlenmesinin de koruma altına alındığı söylenebilecektir.[169]

AİHM, Rotaru/Romanya Davası[170] kamusal nitelikteki verilerin sistematik olarak toplanıp kaydedilmesi, ilgili kişinin verilerin içeriğine ulaşımı ve yanlış bilgilerin düzeltilmesini isteme hakkı ile ilgilidir. Başvuran, Romanya Gizli Servisi'nin kendisiyle ilgili bir dosya tutması ve kendisine bu dosyaya erişim ve düzeltme olanağının verilmemesinin Sözleşme'nin 8. maddesini ihlal ettiği ve kendisi hakkındaki yanlış bilgilerin düzeltilmesi veya yok edilmesi talebiyle dava açmıştır. AİHM, verilerin toplanıp kullanılması ve ilgili kişiye düzeltme imkânının verilmemesinin 8. madde kapsamında "*aile hayatına saygı hakkı*" ile ilgili olduğuna hükmetmiştir. [171]

AİHM, MGN Limited/Birleşik Krallık Davası'nın[172] konusunu oluşturan olayda, modellik yapan Naomi Campell'ın katıldığı uyuşturucu tedavisiyle ilgili olarak düzenlenen toplantı sonrasında fotoğrafları gizlice bir paparazzi tarafından çekilmiş ve "*Naomi: Ben bir uyuşturucu bağımlısıyım*" başlıklı bir haber yapılarak

[168] Leander/İsveç, B.No: 9248/81, 26.03.1987, para 48; aktaran. Kuşkonmaz, agt, s. 56-58.
[169] Z./Finlandiya, B.No: 22009/93, 25.02.1997 para.71; Aktaran Korkmaz, age, s. 182.
[170] "Başvurucu kendisi hakkında Romanya İstihbarat Servisi (RİS) tarafından tutulan dosyada bulunan bilgilerin gerçek olmadığını ispatlamanın mümkün olmadığından şikâyetçi olmuştur."
[171] Rotaru/Romanya, B.No:28341/95, 04.05.2000 para 57-60; Aktaran Berrak Yılmaz, "Türk Anayasa Mahkemesi ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması", Hacettepe Üniversitesi, Sosyal Bilimler Enstitüsü, Yayımlanmamış Doktora Tezi, Ankara, 2019, s. 144.
[172] MGN Limited/Birleşik Krallık, B.No:39401/04, 18.01.2011 para 72-76; Aktaran Aydın, agm, s. 116.

basında kullanılmıştır. AİHM, kararında söz konusu eylemin AİHS 8. maddesini ihlal ettiğini belirtmiştir.[173]

AİHM, Khadija Ismayilova/Azerbaycan Davası'na konu olayda, gazetecilik mesleğini icra eden başvurucu, mesleğini bırakmaması durumunda kamu tarafından aşağılanacağını belirten bir tehdit mektubuna itibar etmemesi üzerine bilgisi olmadan kaydedilen cinsel görüntülerinin internette paylaşıldığını belirtmiştir. Bu durum üzerine şikâyetçi, başlatılan soruşturmanın da etkisiz kaldığından itibarla makamı şikâyet ettiğinde ise özel hayatına ilişkin unsurların yer aldığı bir durum raporuyla karşılaşmıştır. AİHM olayla ilgili verdiği kararda başvurucunun insanlık onuruna müdahale edildiği ve bu müdahalenin devlet nezdinde etkili bir şekilde soruşturulmasının gerekliliği ortaya koyulmuştur. Buna ek olarak mahkeme devlet nezdince yapılan soruşturmanın gecikmesi ve yayınlanan başvurucunun özel hayatına dair bilgiler içeren soruşturma raporunun gazetelerde yayınlandığını belirterek 8. maddenin ihlal edildiği sonucuna varmıştır.[174]

AİHM kişisel verilerin korunmasıyla ilgili ilk kararlarında ifade ettiği kişisel verilerin korunmasının kişilerin özel hayatına saygı hakkından yararlanabilmesi için temel önemde olduğu anlayışı benimsenmiştir. Fakat zaman içinde bu fikrin değiştiği ve AİHM'in kişisel verilerin korunması hakkının kapsamını belirginleştirmeye başladığı ve AİHS'in 8. maddesinin sınırlarını genişleterek ilk bakışta özel hayat alanına dâhil olmayan verileri de bu kapsamda değerlendirmektedir.[175] Ayrıca AİHM'in kişisel verilerin korunması hakkına ilişkin olarak AİHS'in 8. maddesi kapsamında daha fazla değerlendirmeler yapmaya ve ilkeler belirlemeye istekli olduğu söylenebilir.[176]

---

[173] "Naomi Campbell/MGN davasında mahkeme, Bayan Campbell'in fotoğraflarının onun ten rengini ortaya çıkardığı için ırksal kökeni ile ilgili bilgileri açıkladığına ancak veri sahibinin tanınmış, Afrika kökenli olmaktan gurur duyan birisi olması nedeniyle, olayda fotoğrafların hassas veri olarak kabul edilemeyeceğine karar vermiştir. Bununla birlikte aynı davada mahkeme, uyuşturucu bağımlılığı ile ilgili the Narcotics Anonymous isimli merkezde alınan tedavinin niteliği ve detayları ile ilgili bilgileri, fiziksel ve zihinsel sağlıkla ilgili bilgiler olarak görmüş ve bu nedenle açıkça hassas veri kapsamında olduğuna karar vermiştir."

[174] Khadija Ismayilova/Azerbaycan, B.No:65286/13, 10.01.2019, para 105-114, Aktaran Yılmaz, agt, s. 146.

[175] Yılmaz, agt, s. 147.

[176] Küzeci, age, s. 150.

2.1.4.Avrupa Birliği düzenlemelerinde kişisel verilerin korunması

II. Dünya Savaşı'ndan sonra Avrupa'da husumete son vermek, savaşın yıkıcı etkilerini azaltmak, birlik ve dostluğu pekiştirmek amacıyla 1951 yılında Avrupa Kömür ve Çelik Topluluğu kurulmuş, bu topluluk daha sonra 1957 yılında Avrupa Ekonomik Topluluğu olarak değiştirilmiştir. Son olarak da 7 Şubat 1992 tarihli Avrupa Birliği Antlaşması ile 1 Ocak 1993 tarihinden itibaren geçerli olmak üzere "Avrupa Birliği" kurulmuştur. Bu Birliğin temel amacı barışın teşvik edilmesi, hürriyet, emniyet ve adaletin koruma altına alınması, sosyal ve ekonomik gelişmenin desteklenmesi, halkın refah ve değerlerinin korunması şeklindedir.[177] AB, temel hak ve özgürlüklerin korunması, eşitlik, insan hakları, demokratik kurumların varlığı, hukukun üstünlüğü ve şeffaflığın sağlanması gibi genel anlamda kabul görmüş ortak evrensel değerler üzerine bina edilmiştir. Kişilerin, malların, hizmetlerin, sermayenin ve bilginin serbestçe dolaşabilmesi için iç hukuklarda çalışmalar yapan AB'nde, kişisel verilerin de belli güvenceler sağlanması koşuluyla serbest dolaşımı hedeflenmiştir.[178]

AB, devletler üstü (supranational) bir yapıya sahip olmakla birlikte, devletlerin yerine geçemediğinden tali, ikincil yetkilerle donatılan bir örgüttür. Birlik, yetki alanına giren konularda, gerektiğinde üye devletlerin ulusal mevzuatlarının yerine geçecek şekilde ayrıntılı düzenlemeler yapabilme yetkisine sahiptir. Buna karşın AB, ölçülülük ilkesi çerçevesinde, gerekli olmayan durumlarda üye ülkelerin mevzuatını da göz önüne almakla yükümlüdür.[179] AB bünyesinde kişisel verilerin korunması ile yasama çalışmalarının 1970'li yıllardan sonra başladığı görülmektedir. Nitekim bazı ülkeler bu konuda çeşitli kanunları parlamentolarından geçirdikleri görülmektedir. Bu çerçevede ilk olarak İsveç 1973 yılında Veri Kanunu'nu kabul ile dünya çapında ilk veri koruma kanunu çıkaran ülke olmuştur. Bu ülkeyi Fransa, Batı Almanya, Norveç, Danimarka ve Lüksemburg gibi ülkeler takip etmiştir.

AB'nin idari organı olan "Avrupa Birliği Komisyonu" kişisel verilerin korunmasında önemli bir rol üstlenmiştir. Komisyon hukuki düzenleme yapılmasını önermek, uygulanmasını takip etmek ve uygulamada çıkan sorunlarla ilgili

---

[177] Dülger, age, s. 94.
[178] Kılınç, agm, s. 1117. Avrupa Birliği'nin kuruluşuyla ilgili tarihsel süreç için bkz, Gültekin, age, s. 29-30.
[179] Akgül, age, s. 135.

müdahalede bulunma yetki ve sorumluluğa sahipti. Nitekim bu Komisyonca önerilen "*Veri Koruma Paketi*" Avrupa Parlamentosu'nda kabul edilmiştir. Yayın organı olan Avrupa Birliği Adalet Divanı (ABAD) kişisel verilerin korunması konusunda verdiği kararlarla önemli rol oynamıştır. AB bünyesinde yukarıda sayılan kurum ve organlar dışında sadece kişisel verilerin korunması ile kurulmuş birimler "Avrupa Veri Koruma Kurumu, 29. madde Çalışma Grubu ve 31. madde Komitesi"[180] de vardır.

AB düzeyinde kişisel verilerin korunması ile ilgili yapılan çalışmalardan ilki AB Temel Haklar Şartı'dır. Daha sonra 24 Ekim 1995 tarihinde "Kişisel Verilerin İşlenmesi Sırasında Gerçek Kişilerin Korunması ve Serbest Veri Trafiğine İlişkin Yönergesi (95/46/AT) kabul edilmiş ve Yönerge 1998 yılında yürürlüğe girmiştir. "95/46/AT"nin yetersiz ve eksik kaldığı özellikle telekomünikasyon alanında Avrupa Parlamentosu ve Avrupa Konseyi 15 Aralık 1997 tarihinde "1997/66/AT sayılı Telekomünikasyon Alanında Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Yönergesi"ni yürürlüğe koymuştur. Bunu, 12 Temmuz 2002 tarihinde 95/46/AT'yi tamamlayan "2002/58/AT sayılı Elektronik Haberleşme Alanında Kişisel Özel Alanın Korunması ve Kişisel Verilerin İşlenmesi Yönergesi" takip etti ve "1997/66/AT sayılı Yönerge"yi de yürürlükten kaldırdı. 15 Mart 2006 tarihli "2006/24/AT sayılı Kamuya Açık Haberleşme Hizmetleri veya Kamu Haberleşme Şebekesi ile Bağlantılı Olarak Üretilen veya İşlenen Verilerin Saklanmasına İlişkin Yönerge (Veri Saklama Yönergesi)" hazırlanmıştır. Bu çerçevede hala yürürlükte olan "Avrupa Birliği Temel Haklar Şartı", "2002/58/AT sayılı Direktif", "2016/679 sayılı Direktif" ve "2016/800 sayılı Direktif"e ek olarak yürürlükten kaldırılmış olmasına rağmen KVKK'daki birçok ilkeye rehberlik etmesi sebebiyle "95/46/AT Sayılı Direktif" çalışmamızın bu bölümünde incelenecektir.

2.1.4.1.Avrupa Birliği Temel Haklar Şartı

1992 yılında imzalanan Avrupa Birliği Antlaşması ile AB'nin insan hakları ve temel özgürlüklerin korunması hakkında Avrupa Sözleşmesi ile güvence altına alınan temel haklara, hukuk genel ilkeleri gibi saygı göstereceği hükme bağlanmıştır. 1999 yılında Köln Zirvesi'nin sonuç bildirgesinde temel hakların tek bir kalemde toplanması gerekliliği ortaya çıkmış ve daha sonra yapılan çalışmalar sonucunda 7

[180] Korkmaz, age, s. 205-206.

Aralık 2000 tarihinde Nice'de imzalanan AB Temel Haklar Şartı (ABTHŞ) imzalanmıştır. Böylece AB bünyesinde yaşayan bütün insanların bireysel, siyasal ve ekonomik hakları tek bir metinde toplanmıştır.[181] ABTHŞ, 1 Aralık 2009 tarihinde Lizbon Antlaşması'nın kabulü ile AB içinde tam anlamıyla bağlayıcı bir metin haline gelmiştir.[182]

ABTHŞ, hakları 6 bölümde ele almıştır. Bunlar saygınlık, özgürlükler, eşitlik, dayanışma, yurttaş hakları ve adalettir. Genel özgürlük haklarından olan ve tarihsel süreç içerisinde kişisel verilerin korunmasına dair güvenceleri barındıran "özel yaşamın gizliliğine saygı hakkı ikinci bölümde "Özgürlükler" başlığı altında 7. maddede "*Herkes, özel ve aile yaşamına, konutuna ve haberleşmesine saygı gösterilmesini isteme hakkına sahiptir*" denilerek ortaya konmuştur. ABTHŞ, AİHS'nin 8. maddesi, AB üyesi devletlerin anayasaları, "AK Sosyal Şartı", "AB İşçilerin Temel Sosyal Hakları Şartı" ve üye ülkelerin taraf oldukları uluslararası sözleşmeler temel alınarak hazırlanmıştır. Nitekim Şart'ın giriş bölümünde "*Anayasal teamüller, üye ülkelere ortak uluslararası yükümlülükler, AİHS ve Avrupa İnsan Hakları Mahkemesi (AİHM)'nin içtihat hukukuna saygı gösterdiği"* vurgulanmaktadır.[183] Kullanılan dilde de farklılıklar vardır. AİHS'de haberleşme anlamında *correspondence* kavramı kullanılırken, burada iletişim anlamında *communication* kavramına yer verilmiştir. İletişim kavramının kullanılmasının asıl sebebinin ise gelişen teknolojinin etkisiyle ortaya çıkan ve kullanımı artan teknolojik aygıtların da bu kapsama dâhil edilme isteğidir. Buradan da teknolojik gelişmelerin takip edildiği, bu çerçevede hukuki düzenlemelerin güncelleştirildiği ve kapsamının genişletildiği anlaşılmaktadır.[184]

Kişisel verilerin korunması konusu, "Temel Haklar Şartı" 8. maddesine göre; "*(1)Herkes, kendisini ilgilendiren kişisel verilerin korunması hakkına sahiptir. (2)Bu veriler, adil bir şekilde, belirli amaçlar için ve ilgili kişinin rızasına veya yasa ile öngörülmüş diğer meşru bir temele dayanarak tutulur (3)Herkes, kendisi hakkında*

---

[181] ABTHŞ'nin Türkçe metni hakkında bkz, https://www.avrupa.info.tr/tr/avrupa-birligi-temel-haklar-bildirgesi-708. (E.T. 01.02.2021)
[182] Korkmaz, age, s.207-208.
[183] Kuşkonmaz, agt, s. 67-68 ve Yüksel Metin, "Avrupa Birliği Temel Haklar Şartı", **Ankara Üniversitesi Sosyal Bilimler Fakültesi Dergisi**, C.57, S.4, 2002, s. 35-63, özellikle s. 47.
[184] Gültekin, agt, s. 32.

toplanmış verilere erişme ve bunları düzelttirme hakkına sahiptir. Bu kurallara uyulması, bağımsız bir makam tarafından denetlenir".

"AB Temel Haklar Şartı"na kaynaklık eden "95/46/AT sayılı Yönerge" göz önüne alındığında koruma alanı yalnızca gerçek kişilere yöneliktir. Madde hükmündeki "*herkes*" deyimi tüzel kişileri değil, sadece gerçek kişileri kastetmektedir.[185]

"Avrupa Birliği Temel Haklar Şartı" 8. maddesiyle kişisel verilerle ve korunmasıyla ilgili açık hüküm öngörmekle; Sözleşme'den bağımsız olarak "*kişisel verilerin korunmasını*" ayrı bağımsız bir hak olarak ele almıştır. Böylece AİHS'nin 8. maddesinde yazılı "*özel yaşamın gizliliği hakkının*" İnsan Hakları Mahkemesi içtihatlarıyla doldurulmaya çalışılan bölümünü yasa metni haline getirerek, pek çok hukuki sorunun çözümüne yardımcı olmuştur. ABTHŞ'nin, hukuki anlamda AB üyesi ülkelerde ve kurumlarda bağlayıcılık kazanmasıyla, üye vatandaşları bu Şartın hükümlerine dayanarak kişisel verilerini koruma konusunda dava açma hakkı elde etmişlerdir.

2.1.4.2.95/46/AT Sayılı Avrupa Birliği Veri Koruma Direktifi

Avrupa Komisyonu 1990 yılında "*Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Direktif*" taslağını hazırlayarak Avrupa Parlamentosu'na sunmuştur. Komisyonlar taslak üzerinde 5 yıl kadar çalışmış ve gerekli gördükleri değişiklikleri yaptıktan sonra ancak 24 Ekim 1995 tarihinde kabul edilebilmiştir.[186] Direktif amacını 1. maddede kişisel verilerin işlenmesine dair başta kişisel mahremiyet hakkı olmak üzere gerçek kişilerin temel haklarını ve özgürlüklerini koruma olarak açıklamaktadır. Maddenin devamında üye devletlerin sağlanan korumayla bağlantılı nedenlerle üye devletlerarasında kişisel verilerin akışını yasaklamayacağı ya da engelleyemeyeceği ifade edilmiştir. Böylece kişisel verilerin korunması ile bu verilere ulaşım arasındaki denge oluşturulmaya çalışılmıştır.

---

[185] Şimşek, age, s. 73.

[186] Direktifin içeriği ile ilgili ayrıntılar için bkz, Metin Turan, **Karşılaştırma Hukukta Kişisel Verilerin Korunması**, 3. Baskı, Seçkin Yayınevi, Ankara, 2020, s. 159vd; Küzeci, age, s. 183vd; Dülger, age, s. 95vd; Korkmaz, age, s. 209vd; Kuşkonmaz, agt, s. 70vd; Şimşek, age, s. 45vd; Akgül, age, s. 214vd ve Ayözger, age, s. 78vd.

Direktifin kapsamı 3. maddede açıklanmıştır. Buna göre otomatik yollarla ya da bu yollarla olmasa bile veri kayıt sisteminin parçası olarak işlenen ve gerçek kişilere ait verilerin, kişisel verilerin korunması başlığı altında değerlendirileceği belirtilmiştir.[187] Bu anlamda Direktif' ile 108 sayılı Sözleşme karşılaştırıldığında Direktif'in kişisel veri kavramını sadece gerçek kişilerle sınırladığını ve bu konuda çok net bir çizgi çizdiği söylenebilir.

Direktifte veri kalitesine ilişkin prensiplere yer verilmiştir. Bu prensipler; kişisel verilerin adil ve yasal olarak işlenmesi, meşru amaçlar için toplanmış olması, toplanma amacıyla ilgisiz ve gereğinden fazla bilgi toplanmaması, doğru ve güncel olması, toplanma amacına uygun süre boyunca tutulması ve üye ülkelerin bu şartların yerine getirilmesi için gerekli tedbirleri almalarıdır. Gerekli tedbirlerin alınması durumunda tarihsel, istatistiksel ya da bilimsel amaçlar için kişisel verilerin ayrıntılı olarak işlenmesi veya daha uzun süre depolanmasının veri koruma direktifine aykırı olmayacağı belirtilmiştir.[188]

8. maddede hassas verilere ayrılmış ve bunların üst seviyede koruma gerektirdiği, veri sahiplerinin toplum içinde ayrımcılığa uğramamaları için üye devletler tarafından bu kapsamdaki kişisel verilerin işlenmesinin yasaklanması öngörülmüştür. Bu konudaki istisnalar ise aynı maddenin ikinci bendinde açıklanmıştır.

Direktifin en önemli maddelerinden biri de, kişisel verilerin yeterli derecede korumasının bulunmadığı AB'ye üye olan veya dışında kalan ülkelere transferi yasaklayan 25. maddesidir. Bu madde ile genel bir düzenleme getirilmiş ve uyulacak kuralları ayrıntılı olarak ortaya koymuştur.[189] Veri koruması konusunda güvenli

---

[187] Uyarer, age, s. 59.
[188] Henkoğlu, age, s. 59 vd.
[189] *"(1) Üye Devletler, bu Direktifin diğer hükümleri uyarınca benimsenen ulusal hükümlere uyuma zarar vermeksizin, yalnızca söz konusu üçüncü ülke yeterli koruma seviyesi sağlarsa, transfer sonrası işleme için istenen veya işlemeye tabi olan kişisel verilerin bir üçüncü ülkeye transferinin gerçekleşebilmesini sağlayacaktır. (2) Bir üçüncü ülke tarafından sağlanan koruma seviyesinin yeterliliği, veri transfer faaliyetlerinin dizisinin veya bir veri transfer faaliyetini çevreleyen tüm koşulların ışığında değerlendirilecektir. O ülkeyle uyumlu meslek kuralları ve güvenlik tedbirleri ve söz konusu üçüncü ülkedeki yürürlükte olan hem genel hem sektörel yasa hükümleri, son varış ülkesi ve menşe ülke, önerilen faaliyet veya faaliyetlerin süresi ve amacı, verilerin yapısına özel önem verilecektir. (3) Üye Devletler ve Komisyon, 2. Paragrafın anlamı dâhilinde yeterli koruma seviyesini bir üçüncü ülkenin sağlamadığını düşündükleri durumlarda birbirlerini bilgilendireceklerdir. (4) Komisyon, bu maddenin 2. paragrafının anlamında, bir üçüncü ülkenin yeterli koruma seviyesini*

olmayan ülkelere karşı tüm birlik ülkeleri gerekli tedbirleri almakla yükümlü tutulmuştur. ABD'de henüz AB'nin aradığı tarzda koruma düzeyi mevcut olmadığından artan e-ticaret ilişkileri nedeniyle ortaya çıkan kişisel verilerin korunması alanında problemleri gidermek amacıyla Safe Harbor Anlaşması imzalanmıştır.[190]

Direktifin 26. maddesinde ise serbest dolaşım ile ilgili getirilen istisnalar veya uygulama dışı durumlara yer verilmiştir. Yeterli koruma seviyesini sağlamayan üçüncü bir ülkeye kişisel verilerin transferinin hangi durumlarda gerçekleşeceğini maddeler halinde sıralamıştır.[191]

95/46/AT sayılı Direktif, AB bünyesinde kişisel verilerin korumasına yer veren düzenlemeler arasında, AB hukukuna veri koruma ilkelerini getirmesi ve AB'de kişisel verilerin korunmasının temel ölçütlerini belirlemesi itibarıyla en önemli olanıdır.

Direktif bir bütün olarak değerlendirildiğinde kişisel verilerin korunması açısından kendisinden sonra gelen pek çok ulusal ve uluslararası düzenlemeye kaynaklık ettiği görülmektedir. Zira Direktifte yer alan pek çok prensip ve düzenleme,

---

sağlamadığını madde 31 (2) kapsamında sağlanan prosedüre göre tespit ederse, Üye Devletler, söz konusu üçüncü ülkeye aynı tipte verilerin herhangi bir transferini önlemek için gerekli önlemleri alacaklardır. (5) Komisyon, uygun bir zamanda, paragraf 4 uyarınca sağlanan bulgudan kaynaklanan durumu çözmek amacıyla müzakerelere başlayacaktır. (6) Komisyon, madde 31 (2)'de atıfta bulunulan prosedüre uygun olarak; bireylerin temel haklarının ve özel yaşamlarının korunması için, özellikle paragraf 5'te atıfta bulunulan müzakerelerin sonuçlanması üzerine, giriştiği uluslararası taahhütler veya kendi yerel yasası nedeniyle, bu maddenin 2. paragrafı anlamı dâhilinde üçüncü bir ülkenin yeterli bir koruma seviyesini temin etmesini isteyebilir. Üye Devletler, Komisyonun kararıyla uyum sağlamak için gerekli tedbirleri alacaktır."

[190] Özdemir, age, s. 31; Aksoy, age, s. 105; Akgül, age, s. 194 ve Henkoğlu, age, s. 61. Safe Harbor Antlaşması ile detaylar için bkz, Gür, agt, s. 119-136.

[191] "*(a) Veri öznesi önerilen transfer için açık şekilde rızasını vermişse veya (b) Veri öznesinin talebine yanıt olarak alınan ön sözleşme tedbirlerinin uygulanması veya denetleyici ve veri öznesi arasındaki bir sözleşmenin yerine getirilmesi için transfer gerekliyse veya (c) Üçüncü bir şahıs ve denetleyici arasında veri öznesinin menfaatine sonuçlanan bir sözleşmenin yerine getirilmesi veya sonuçlandırılması için transfer gerekliyse veya (d) Transfer; kanuni hakların tesisi, işletilmesi veya savunulması için veya önemli kamu menfaati zemininde yasal olarak gerekliyse veya zorunluysa veya (e) Veri öznesinin hayati menfaatlerinin korunması için transfer gerekirse veya (f) Özel durumda yapılan görüş alışverişi için kanunda öngörülen koşullar ölçüsünde, bir meşru menfaat gösteren herhangi bir kişi tarafından veya genel olarak kamu tarafından danışmaya açık olan ve kamuya bilgi" "sağlamak amaçlı kanunlar veya yönetmeliklere göre transfer bir kayıttan sağlanırsa. (2) Paragraf 1'e zarar vermeksizin, bir Üye Devlet, ilgili hakların işletilmesine dair ve bireylerin temel hak ve özgürlükleri ve kişisel mahremiyet hakkının korunmasına ilişkin anlam dâhilinde, yeterli koruma seviyesini sağlamayan üçüncü bir ülkeye kişisel veri transferler dizisine veya bir transferine izin verebilir, bu tür korunma önlemleri özellikle uygun sözleşme maddelerinden kaynaklanabilir…"*

bugün bu Direktifin yerini alan "Avrupa Birliği Genel Veri Koruma Tüzüğü"nde de hala geçerliliğini korumaktadır.

Direktif'in kişisel verilerin korunmasıyla ilgili yeterli koruma düzeyi olmayan üçüncü ülkelere veri aktarımını yasaklayan hükmü, bu ülkelerde kişisel verilerin korunması ile ilgili düzenlemelerin yapılmasına yol açması sebebiyle Direktifin etkisini AB dışına taşımıştır. Diğer bir etki de AB üyesi ülkeler arasında kişisel veri koruma hukukunun uyumlu hale gelmesini sağlamıştır.

Türkiye açısından önemli olan kısmı ise "6698 sayılı Kişisel Verilerin Korunması Kanunu"nun hazırlanmasında büyük ölçüde örnek alınmış olması ile kanunun bu Direktifle önemli miktarda benzerlik ve paralellik göstermesidir. Mevcut hukukumuza uyup uymadığına bakılmaksızın çoğu noktada benzerlik olması eleştirilse de bundan aslında Avrupa düzenlemeleri ile uyumlu olunmaya çalışıldığı anlaşılmaktadır.[192]

2.1.4.3.2002/58/AT Sayılı Özel Yaşamın ve Elektronik İletişimin Korunması Direktifi

Yukarıda ayrıntıları verilen "95/46/AT sayılı AB Veri Koruma Direktifi" kişisel verilerin korunması hakkında genel ve kapsayıcı hükümlere sahip olsa da değişen şartlar ve gelişen teknoloji karşısında yeni düzenlemeler yapılması gereği ortaya çıkmıştır. Özellikle telekomünikasyon sektörünün kendine has niteliğini dikkate alan ve bu konuda AB Veri Koruma Direktifi'ni tamamlayan bir düzenleme yapılması gereksinimi 1997 yılında 97/66/AT sayılı Telekomünikasyonun Gizliliği Direktifi'nin kabul edilmesinde etkili olmuştur. Bu Direktif, telefon, dijital televizyon, mobil ağalar ve diğer telekomünikasyon sistemlerini kapsayan özel hükümler içermektedir. Telekomünikasyon Gizlilik Yönergesi kullanıcının iletişiminin gizliliğini sağlamak için kullanıcı ve taşıyıcılara geniş kapsamlı yükümlülükler getirmiştir. Bu şekliyle Direktif daha önce veri koruma hukukunda mevcut boşlukları doldurmuştur. [193]

97/66/AT sayılı Direktifin zamanla mevcut pazar ve gelişen teknoloji karşısında yetersiz kalması ve 11 Eylül saldırısının yarattığı ortam ile üye ülkelerin

[192] Dülger, age, s. 96.
[193] Küzeci, age, s. 210 ve Başalp, age, s. 87-90.

baskısı 1997 yılında bu Direktifin yerine, "2002/58/AT sayılı Elektronik Haberleşme Sektöründe Özel Alanın Korunması ve Kişisel Bilgilerin İşlenmesi Direktifi (Elektronik Veri Koruma Direktifi)" kabul edilmiştir.[194] 97/66/AT sayılı Telekomünikasyonun Gizliliği Direktifi 30 Ekim 2003 tarihinde yürüklükten kaldırılmıştır. 2002/58/AT sayılı Elektronik Veri Koruma Direktifi, aslında 95/46/AT sayılı Direktifin elektronik haberleşme sektörü için hazırlanmış daha özel bir versiyonu şeklindedir. "2002/58/AT sayılı Direktif" elektronik haberleşme yönünden eksiklikleri tamamlamakta ve verilerin telekomünikasyon ve hizmetler alanında korunmasını amaçlamaktadır.[195]

2002/58/AT sayılı Elektronik Veri Koruma Direktifi'nde birçok yerde 95/46/AT sayılı Direktife atıf yapılmakta ve 2002/58/AT sayılı Direktifte bahsedilmeyen veri koruma konuları için 95/46/AT sayılı yönergenin geçerli olacağı bildirilmektedir.[196]

"2002/58/AT sayılı Elektronik Veri Koruma Direktifi"nin amacı, "*Üye ülkelerin, elektronik haberleşme sektöründe kişisel bilgilerin işlenmesine ilişkin olarak temel hak ve özgürlüklerin, özellikle de gizlilik hakkının eşit ölçüde korunmasını ve Birlik içinde bu tür veriler ile elektronik haberleşme ekipmanı ve hizmetlerinin serbest bir şekilde dolaşmasını sağlamasını gerektiren hükümlerini uyumlaştırmaktadır"* şeklinde belirtilmiştir. Bu anlamda "95/46/AT sayılı Direktif"ten farkı, gerçek kişilere ek olarak tüzel kişileri de kapsam alanına almasıdır.

"2002/58/AT sayılı Elektronik Veri Koruma Direktifi"nde özel hayatın gizliliği ve kişisel verilerin korunması haklarına saygı gösterilmesi gerektiğine, uluslararası sözleşmelere ve AİHS'nde düzenlenen haberleşme gizliliği hakkının önemine de özel olarak işaret edilmiştir. Bu Direktifte üzerinde durulan konular; güvenlik, iletişimin gizliliği, veri işlemenin sınırlandırılması, istenmeyen iletiler

---

[194] Uyarer, age, s. 61.
[195] Nilgün Başalp, **Kişisel Verilerin Korunması ve İnternet, İnternet ve Hukuk,** Derleyen Yeşim M. Atamer, İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2004, s. 13; Korkmaz, age, s. 227 ve Şimşek, age, s. 57.
[196] Özdemir, age, s. 36; Küzeci, age, s. 213 ve Şimşek, age, s. 58.

(spam), çerezlerin (cookies) ve casus yazılımların (spyware) kullanımı, yer bilgileri ve verilerin saklanması ile bilgiler hakkındadır.[197]

Özetle 2002/58/AT sayılı Elektronik Veri Koruma Direktifi son yıllarda meydana gelen teknolojik gelişmeler ile kamusal iletişim ağlarında, özellikle internet ve elektronik mesaj aktarımında, kişilerin özel yaşamının korunması konusunda AB bünyesinde birtakım kurallar koymakta ve garantiler getirmektedir. Bu Direktif yetersiz kaldığı durumlarda "95/46/AT sayılı AB Veri Koruma Direktifi"ne yollama yapılmaktaydı.

Değişim ve dönüşümün çok hızla olması sebebiyle bu Direktiflerin yetersiz olduğu düşünülmüş olsa gerek ki AB 25 Mayıs 2018 tarihinde "Genel Veri Koruma Tüzüğü"nü yürürlüğe koymuş, dolayısıyla 1995 tarihli 95/46/AT sayılı direktifi ortadan kaldırmıştır. İnsan hak ve özgürlükleri bağlamında veri korumanın çağın ihtiyaçlarına uygun hale getirilmesi, elektronik haberleşme sektöründeki 2002/58/AT sayılı direktif için de uzun süredir aynı taleplerin dile getirilmesine neden olmuştur. Nitekim AB 10 Temmuz 2018 tarihinde "*Gizlilik ve Elektronik İletişim Tüzüğü*" adıyla yeni bir elektronik veri koruma düzenlemesini taslak olarak hazırlayıp yayınlamıştır.

2.1.4.4.2016/679 Sayılı Avrupa Birliği Veri Koruma Tüzüğü

1995 yılında kabul edilen "95/46/AT sayılı AB Veri Koruma Direktifi", internetin Avrupa'da bireysel yaşamın bir parçası haline gelmesi, hızla artan teknolojik gelişmeler ve küreselleşmenin kişisel verilerin toplanması, erişimi ve kullanılmasında önemli değişiklikler meydana getirmesiyle, 2000'li yıllarda duyulan ihtiyaca cevap vermekte artık yetersiz kalmaktaydı.[198] Bu yüzden bu Direktifte benimsenen ilkelerin modernize edilmesi ve gelecekte vatandaşların kişisel haklarının günümüz şartlarına uygun bir biçimde güvence altına alınması amacıyla, kapsamlı bir yeniliğe gidilmesi ihtiyacı ortaya çıkmıştır. Özellikle teknolojik gelişmelerle beraber kişisel verilere erişim, kişisel verilerin toplanması ve başka yerlere aktarılması yöntemlerinin çeşitlilik göstermesiyle, gelişen teknolojiye uyum sağlayan yeni bir düzenleme şart

[197] Küzeci, age, s. 214-215 ve Sarıusta, agt, s. 70-71.
[198] Küzeci, age, s. 221.

olmuştur. Ayrıca AB Veri Koruma Direktifi'nin AB'de üye ülkeler arasında farklı biçimlerde uygulanması yeni bir düzenlemeyi zorunlu hale getirmiştir.[199]

AB bünyesinde ilk taslak çalışmaları 2009 yılına kadar uzanmaktadır. 2012 yılında başlayan tüzük çalışması, "Avrupa Parlamentosu", "Avrupa Konseyi" ve "Avrupa Komisyonu" tarafından 24 Mayıs 2016 tarihinde kabul edilmiş ve 25 Mayıs 2018 tarihinde de AB Genel Veri Koruma Tüzüğü adını almıştır. İki yıllık süre içinde birlik ülkeleri ulusal düzenlemelerini bu Tüzüğe uyumlu hale getireceklerdir. Bu Tüzüğün yürürlüğe girmesi ile "95/46/EC sayılı AB Veri Koruma Direktifi" ilga edilmiştir. "2016/679 sayılı Genel Veri Koruma Tüzüğü"nün 94. maddesinde "*(95/46/EC sayılı Direktif'in 25 Mayıs 2018 tarihinden itibaren geçerli olmak üzere yürürlükten kaldırılması, yürürlükten kaldırılan Direktif'e yapılan atıfların bu Tüzüğe yapılmış sayılacağı, 95/46/EC sayılı Direktif'in 29. maddesi ile kurulan kişisel verilerin işlenmesiyle ilgili olarak bireylerin korunması hakkında çalışma grubuna yapılan atıflar bu Tüzük'le kurulan Avrupa Veri Koruma Tüzüğü'ne (GVTK) yapılmış sayılır.*" hükmü ile Tüzük'ün AB'ye bağlı tüm üye ülkeler için bağlayıcı olması sağlanmıştır.[200]

"2016/679 sayılı Genel Veri Koruma Tüzüğü", AB tarihinde kişisel verilerin korunması hakkındaki geniş ve kapsamlı bir konuyu tek bir bağlayıcı metinle ele alan metin olmuştur. AB, Tüzüğün kapsamını üye ülkelerden daha geniş tutmaktadır. Üye ülkelerde ikamet eden, ürün, hizmet veya denetim gibi herhangi bir nedenle Birliğe üye ülkelerden geçen kişisel verilerin Birliğe üye olmayan ülkelerle temas içerisinde olması durumunda, Tüzük o ülkeler için de bağlayıcı nitelikte olacağı belirtilmiştir. Böylece AB ile ilişkili verilerin, kişisel veri korumasının olmadığı ya da eksik koruma sağlandığı ülkeler açısından da güvence altına alınması amaçlanmıştır.[201] Örneğin AB dışında faaliyet gösteren Google, Facebook gibi şirketlerin AB sınırları içindeki veri sahibinin kendilerinden mal veya hizmet sağlamaları durumunda, bu şirketler AB içindeki şirketler gibi aynı kurallara bağlı olacakları belirtilmiştir. Yine Almanya ile ticari ilişki içinde olan bir şirketin merkezi Türkiye'de olsa bile kişisel verilerin

[199] Dülger, age, s. 102-103.
[200] Hatipoğlu, age, s. 58 ve Ayözger, age, s. 88.
[201] Dülger, age, s. 105vd.

toplanması, işlenmesi ve muhafazası konusunda aynen AB üyesi ülkelerdeki şirketler gibi muamele görecek ve sorumlu tutulacaktır.

Tüzük ilkelerine uyulmaması halinde, yükümlülüklerini yerine getirmeyenlere veya ihlal edenlere önemli cezalar verme yetkisi, ilgili ülkelerin veri koruma otoritelerine tanınmıştır. İhlal yapan kuruluşa üst sınır, ceza yıllık cirosunun %4'ü veya 20 milyon Euro para cezası olarak belirlenmiştir.

AB, vatandaşlarını ve üye ülkelerle ilişki içinde olan kişileri 1995 yılından beri artan veri ihlallerinden korumak için AB Veri Koruma Tüzüğü ile getirilen temel değişiklik ve yenilikler; AB dışındaki ülkelere de uygulanabilir hale getirecek şekilde bölgesel kapsamının genişletilmesi, Tüzük ile getirilen ilkelerini ihlal edilmesi halinde parasal ceza yaptırımı öngörülmesi, kişisel verisi işlenecek olan kişiden alınması gereken rıza için öngörülen şartların kuvvetlendirilmiş olması şeklindedir.

İlgili kişinin temel hakları açısından yapılan temel değişikler ise ihlal bildirimi, erişim hakkı, silme/unutulma hakkı, veri taşınabilirliği, tasarımdan itibaren veri mahremiyeti ve veri koruma görevlileri başlıkları ile ortaya konmuştur.

Gelişen ve artan ihtiyaçları daha iyi karşılamak için düzenlenmiş bulunan AB Veri Koruma Tüzüğü, henüz daha yeni uygulamaya konmuş olmakla birlikte beklentileri oldukça yükseltmiştir. Çünkü bu Tüzük kişisel verilerin korunması alanında son 20 yıl içinde yapılmış en önemli ve köklü değişiklik olduğu ifade edilmektedir.

AB Veri Koruma Tüzüğü ile gelişen teknoloji ve küreselleşen dünyanın gereklerine uygun olarak tüm AB ülkelerinde daha etkin bir veri koruma standardı oluşturulmaya çalışılmıştır. Özellikle internet çağının getirdiği yenilikler doğrultusunda oluşan dijital ekonominin ve elektronik ticaretin tarafları arasında güvenin oluşturulması açısından böyle bir veri koruma standardının kabulü gerçekten önemli bir adım olarak görülmüştür.

2.1.4.5.2016/680 Sayılı Kişisel Verilerin Cezai Prosedür Gereği İşlenmesi Karşısında Gerçek Kişilerin Korunması Direktifi

"Veri Koruma Tüzüğü (2016/679)" ile aynı zamanda 2016/680 sayılı "*Ceza Gerektiren Suçların Önlenmesi, Soruşturulması, Tespiti Veya Kovuşturulması Veya*

Cezai Yaptırımların İnfaz Edilmesi Amacıyla Yetkili Makamlarca Kişisel Verilerin İşlenmesine İlişkin Gerçek Kişilerin Korunmasına Dair Direktif" de 27 Nisan 2016 tarihinde yayınlanmıştır.[202] Direktifin amacı kamu güvenliğine yönelik tehditlerin korunması ve önlenmesi dâhil olmak üzere, cezai suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması veya cezai yaptırımların infaz edilmesi amacıyla yetkili makamlarca kişisel verilerin işlenmesine ilişkin gerçek kişilerin korunmasıdır. Üye devletlerin, kişisel verilerin işlenmesiyle ilgili olarak yetkili mercilerce, ilgili kişilerin hak ve özgürlüklerinin korunmasına yönelik Direktifte yer alanlardan daha yüksek güvenceler sağlayabileceğini öngörmektedir.[203]

Direktif üye devletlerin kişisel verilerin silinmesi veya saklama sürelerinin periyodik kontrolü için süreleri belirlemelerini öngörmektedir.[204] Bu düzenleme mülga edilen "95/46/AT sayılı Direktif"de bulunmayıp, "2016/679 sayılı Tüzük"e paralel olarak yapılmıştır.[205]

Direktif ilgili kişiler arasında sınıflandırma yapmaktadır. Direktif'e göre şüpheliler, hükümlüler, mağdurlar gibi suçla doğrudan ilgili kişilere ait kişisel veriler ile tanıklar gibi suçta dolaylı olarak ilişkili kişilerin kişisel verileri ayrıma tabi tutulmuştur. Bu hüküm de 96/46/AT sayılı mülga direktifte bulunmayan bir düzenlemedir. Bu konuda Çalışma Grubu da, şüpheli olmayan kişilerin kişisel verilerinin işlenmesinde dikkatli olunması ve suça karışmayan kişilerin kişisel verilerin haksız muameleye maruz kalmaması için özel önlemler alınmasını tavsiye etmektedir.[206]

2016/680 sayılı Direktif olaylardan elde edilen kişisel veriler ile kişisel değerlendirmelerden elde edilen kişisel veriler arasında ayrım yapılmaması gerektiğini öngörmektedir. Kişisel değerlendirmelerden elde edilen kişisel verilerin, olaylardan elde edilenlere oranla doğruluklarının az olması ihtimali değerlendirildiğinde, bu

---

[202] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L0680&qid=1612356536930 E.T. 03.02.2021

[203] 2016/680 sayılı Direktifin 1. maddesi.

[204] 2016/680 sayılı Direktifin 5. maddesi.

[205] Korkmaz, age, s. 243.

[206] Working Party on Police and Justice, The Future of Privacy: Joint contribition to the Consultation of the European Commision on the legal framework for the fundamental right to protection of personal data, s. 29. https://www.garanteprivacy.it/documents/10160/10704/WP168++The+Future+of+PrivacY E.T: 03.06.2021.

düzenleme yerinde olmuştur. Ayrıca yanlış verilerin aktarıldığı durumlarda, alan veri sorumlusu bu verinin yanlışlığı konusunda bilgilendirilmeli ve bu kişisel veri düzeltilmeli, silinmeli veya işlenmesi kısıtlanmalıdır.[207]

2016/680 sayılı Direktif ayrıca üye devletlerin yetkili makamlarının kişisel verileri sadece "*suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması veya cezai yaptırımların uygulanması amacıyla yürütülen görevler*" esnasında gerekli olduğunda işleyebileceklerini düzenlemektedir.[208]

Direktif'te üye devletler; başta kişisel verilerin korunması olmak üzere gerçek kişilerin temel hak ve özgürlüklerini korumakla yükümlü kılınmışlardır. Ayrıca gizli istihbarat teşkilatlarının ve AB kurumlarının veri işleme etkinlikleri kapsam dışı bırakılmıştır. "2016/679 sayılı AB Veri Koruma Tüzüğü" ile "2016/680 sayılı Direktif" arasında bir çelişki olup olmayacağı ise zamanla uygulama ile ortaya çıkacağı belirtilmiştir. 2016/680 sayılı Direktifin kolluk güçlerinin etkinlikleri ile bireysel haklar arasında dengeyi kurma ve bireyin haklarını güçlendirme açısından önemli bir adım olduğu, kişisel verilerin korunması alanında pek çok yenilik getirdiği, etkilerinin de yakında AB sınırları dışında bile hissedileceği ifade edilmiştir.

2.2. Kişisel Verilerin Korunmasına Yönelik Ulusal Düzenlemeler

Günümüzde teknolojideki gelişmelere paralel bir yandan kişisel verilere daha yüksek oranda ihtiyaç duyulurken, diğer yandan kişilerin temel haklarına ve verilere yönelen saldırılar da hızla artmış ve bu durum hukuksal düzenlemeler yapılması gereğini beraberinde getirmiştir. Türkiye dışında BM, OECD, AK ve AB gibi kuruluşlar kişisel verilerin korunması konusunda çalışırken, AB'ye girme yolunda adımlar atan Türkiye, önüne koyulan kriterleri aşabilmek için birçok alanda AB'de yapılan düzenlemelere ayak uydurmak için reformlar yapmıştır. Türkiye kişisel verilerin korunması ile ilgili ilk adımını "Avrupa Konseyi 1981 tarihli 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi"ni 28 Ocak 1981 günü imza atmış, ancak onaylamasını yapmamıştır.[209] Zamanla bireylerin temel hak ve özgürlükleri tehlike altına girmesi, kişisel verilerin

[207] 2016/680 sayılı Direktifin 7. maddesi
[208] 2016/680 sayılı Direktifin 8. maddesi
[209] Çokmutlu, agt, s. 118.

korunması ihtiyacı ve Avrupa ile olan ilişkilerin güçlenmesi bu alanda düzenleme yapmayı zorunlu hale getirmiştir.

Yukarıda detaylı olarak açıklandığı üzere Avrupa'da kişisel verilerin korunması ile ilgili uluslararası kuruluşlar vasıtasıyla yoğun çalışmalar yapılırken, Türkiye bunları yıllarca sadece takip etmekle geçirmiştir. Kişisel verilerin korunmasına yönelik 2016 yılında çıkarılan "Kişisel Verileri Koruma Kanunu"na kadar, Türkiye'de kişisel verilerin doğrudan değil de dolaylı olarak korunması hususunu düzenleyen pek çok kanun ve yönetmelik vardır. Bunlardan biri Türk Ceza Kanunu'dur. Ancak bu Kanun, ayrı bir bölümde inceleneceğinden burada yer verilmeyecektir. Bunun haricinde diğer temel kanunlara değinilerek bu kanunlarda kişisel verilerin nasıl işlendiği ve koruma altına alındığı ile ilgili bilgiler verilecektir.

2.2.1.Anayasa

Türkiye Cumhuriyeti'nin 1982 tarihli Anayasası'nda kişisel verilerin kullanılması ile ilgili 2010 yılına kadar özel bir düzenleme olmadığından, bu hakkın korunması Anayasa'da yer alan diğer maddelerle sağlanmaktaydı. Bu maddeler aşağıdaki şekilde yer almıştır.

1982 Anayasası'nda[210] düzenlenen "Kişinin Dokunulmazlığı, Maddi ve Manevi Varlığı"[211], "Özel Hayatın Gizliliği ve Korunması"[212], "Konut Dokunulmazlığı"[213], "Haberleşme Özgürlüğü"[214], "Din ve Vicdan Hürriyeti"[215] ve "Düşünce ve Kanaat Hürriyeti"[216] ile kişisel verilerin dolaylı olarak korunmaktaydı.

---

[210] 1982 Anayasası'nın maddeleri için bkz, https://www.mevzuat.gov.tr/MevzuatMetin/1.5.2709-19821018.pdf. (E.T.06.02.2021)

[211] Anayasa 17. madde: "Herkes, yaşama, maddi ve manevi varlığını koruma ve geliştirme hakkına sahiptir."

[212] Anayasa 20. madde: "Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz. Adli soruşturma ve kovuşturmanın gerektirdiği istisnalar saklıdır. Kanunun açıkça gösterdiği hallerde, usulüne göre verilmiş hâkim kararı olmadıkça; gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınan merciin emri bulunmadıkça, kimsenin üstü, özel kâğıtları ve eşyası aranamaz ve bunlara el konulamaz."

[213] Anayasa 21. madde: "Kimsenin konutuna dokunulamaz. Kanunun açıkça gösterdiği hallerde, usulüne göre verilmiş hâkim kararı olmadıkça; gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınan merciin emri bulunmadıkça, kimsenin konutuna girilemez, arama yapılamaz ve buradaki eşyaya el konulamaz."

[214] Anayasa 22. madde: "Herkes, haberleşme hürriyetine sahiptir. Haberleşmenin gizliliği esastır."

[215] Anayasa 24. madde: "Herkes, vicdan, dini inanç ve kanaat hürriyetine sahiptir"

[216] Anayasa 25. madde: "Herkes, düşünce ve kanaat hürriyetine sahiptir."

Bu maddeler içinde kişisel veriler 20. madde kapsamında özel olarak koruma alanı bulmuştur.

Kişisel verileri doğrudan korumaya yönelik olarak 2010 anayasa değişikliğiyle "Özel Hayatın Gizliliği" başlığı ile 20 maddeye ek 2. fıkra olarak girmiş bulunmaktadır. Bu ek fıkra uyarınca, "*Herkes, kendisi ile ilgili kişisel verilerin korunması hakkında sahiptir; Bu hak kişinin kendisi ile ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını da kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir*" denilmektedir.[217] Bu metnin Anayasaya eklenmesiyle kişisel verilerin hangi hallerde korunacağı ve sınırlanabileceğine dair dayanak maddesi Anayasal bir şekle dönüşmüştür.[218] Buna göre herkes kendi kişisel verilerinin korunmasını, bilgilere erişme, veriler hakkında bilgilendirilme, verilerinin düzeltilmesi veya silinmesini, amaçları doğrultusunda kullanıp kullanılmadığını isteme ve öğrenme hakkı kapsamına alınmıştır. Bu konuda ayrıntıların kanunla düzenleneceği maddeye eklenmiştir.

Ek fıkranın madde gerekçesinde; "*Anayasada kişisel verilerin korunmasına yönelik dolaylı hükümler bulunmakla birlikte yeterli değildir. Mukayeseli hukukta ve tarafı olduğumuz uluslararası belgelerde de kişisel verilerin korunması önemle vurgulanmaktadır*"[219]

Normlar hiyerarşisi göz önünde bulundurulduğunda tüm hukuki normlar Anayasa tarafından bağlayıcıdır. Mevzuatımızdaki hiçbir norm Anayasa kapsamında düzenlenmiş hususlara aykırılık teşkil edemez. Bu yüzden Anayasa'da güvence sağlanan temel hak ve özgürlüklerin ihlali durumunda ağır sonuçlar ortaya çıkacaktır. Kişisel verilerin korunması maddesi Anayasal bir zırha bürünmekle, bu konunun Anayasal olarak korunan temel hak ve özgürlükler gibi, üst bir korumaya alındığı ve

[217] Türkiye Cumhuriyeti Anayasası ve 20. Maddesinin tam metni ile 12.09.2010 tarih ve 5982 sayılı Kanun/2 ek fıkra için bkz, www.tbmm.gov.tr/anayasa/anayasa_2018.pdf. (E.T.06.02.2021).
[218] Kılınç, agm, s. 1132.
[219] Ek fıkra gerekçesi için bkz, https://www.tbmm.gov.tr/sirasayi/donem23/yil01/ss497.pdf. (E.T. 07.02.2021)

önem verildiğini göstermektedir. Diğer bir ifade ile kişisel verilerin korunması anayasal bir güvenceye kavuşturulmuştur.

Bu düzenleme ile ilişkili getirilen eleştiri ise kişisel verilerin elbette özel hayatın gizliliğiyle bağlantılı olmasına rağmen ayrı bir bentte temel hak olarak özel korumaya alınmış olması kişisel verilere verilen önem bakımından sevindirici bulunmuştur.

2.2.2.Türk Medeni Kanunu ve Borçlar Hukuku

Kişisel verilerin korunması, Anayasada "özel hayatın gizliliği hakkı"nın bulunduğu "kişinin hak ve görevleri" bölümünde düzenlenmiştir. Bu nedenle kişisel veriler Türk Medeni Kanunu'nun[220] (TMK) kişiliği koruyan hükümleri uyarınca korunabilecektir. Hukuka aykırı işlenen kişisel veri olması durumunda, bireyler TMK'nın 24. ve 25. maddeleri çerçevesinde kişilik haklarının saldırıya maruz kaldığını iddia ederek korunmasını talep edebileceklerdir. TMK'da 24. maddede[221] "kişiliğe yönelik saldırılara karşı temel ilkeler", 25. maddede[222] ise "başvurulabilecek hukuksal yollar" gösterilmiştir.[223]

Bireyler kişilik haklarına karşı bir saldırı olması veya olma tehlikesinin baş göstermesi halinde 25. madde hükmünce dava açma hakkına sahiptir.[224] Bu itibarla, kişisel verilerine karşı hukuka aykırı bir saldırıda bulunulan, bulunulması tehlikesi olan veya bulunulmuşsa olumsuz etkilerine maruz kalmaya devam eden kişinin, kişilik

---

[220] Türk Medeni Kanunu için bkz, https://www.mevzuat.gov.tr/MevzuatMetin/1.5.4721.pdf. (E.T. 07.02.2021).

[221] TMK 24. Madde: "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."

[222] TMK 25. Maddesi "Davacı, hâkimden saldırı tehlikesinin önlenmesini, sürmekte olan saldırıya son verilmesini, sona ermiş olsa bile etkileri devam eden saldırının hukuka aykırılığının tespitini isteyebilir. Davacı bunlarla birlikte, düzeltmenin veya kararın üçüncü kişilere bildirilmesi ya da yayımlanması isteminde de bulunabilir.
Davacının, maddî ve manevî tazminat istemleri ile hukuka aykırı saldırı dolayısıyla elde edilmiş olan kazancın vekâletsiz iş görme hükümlerine göre kendisine verilmesine ilişkin istemde bulunma hakkı saklıdır.
Manevî tazminat istemi, karşı tarafça kabul edilmiş olmadıkça devredilemez; miras bırakan tarafından ileri sürülmüş olmadıkça mirasçılara geçmez.
Davacı, kişilik haklarının korunması için kendi yerleşim yeri veya davalının yerleşim yeri mahkemesinde dava açabilir."

[223] Küzeci, age, s. 448.

[224] Başalp, age, s. 102 ve Gültekin, age, s. 70.

hakları saldırıya uğramış olacağından, bu kişi TMK'nın 25. maddesinde düzenlenmiş olan dava hakkını kullanabilecektir.[225]

Gerçekleşebilecek bir saldırının engellenmesi veya gerçekleşmeye devam eden bir saldırının sonlandırılmasına yönelik izlenebilecek usul 25. maddede belirlenmiştir. Fakat maddedeki gerçekleşebilecek bir saldırının engellenmesi bu durumun gerçekleşeceğine ilişkin açık bir emare bulunması hususunu aramaktadır. Dolayısıyla TMK'da bu düzenleme pratikte önleme işlevi açısından güçlü olmamakla beraber saldırının sonlandırılmasında etkili olacağı öngörülmektedir.[226]

TMK'daki bu maddeler ile kişilerin gizli ve özel yaşam alanı kapsamındaki verilere yönelik saldırı olması durumunda belli oranda bir koruma sağlamaktadır. Kişilerin gizli alan dâhilindeki sırlarının öğrenilmesi, teknolojik cihazlarla kaydedilmesi veya kopya edilmesi gibi saldırılar TMK 24-25. maddeleri ile koruma altına alınmaktadır. Ancak bu koruma yetersiz olup, sadece kişilik hakkına müdahale gerçekleştikten sonra yapılabilecek işlemleri kapsadığı görülmektedir. Önleyici nitelikte değildir. Kişisel verilerin hukuka uygun bir şekilde işlenmesini konu almamaktadır. Bu nedenle konunun her yönünü ele alan müstakil bir kanuna ihtiyaç duyulmuştur.[227] Diğer bir deyişle kişisel verisinin hukuka uygun olmadan kaydedildiğini veya kullanıldığı varsayımıyla kişi, TMK hükümlerince ilgili fiilin önlenmesini, durdurulmasını veya tespitini isteyebileceği gibi, bu ihlal nedeniyle bir zarara uğramış ise bu zararların da tazminini isteyebilecektir.

Aynı şekilde benzer bir koruma da "6098 sayılı Türk Borçlar Kanunu"nda (TBK)[228] yer almaktadır. TBK'nın 49. maddesine göre "*Kusurlu ve hukuka aykırı bir fiille başkasına zarar veren, bu zararı gidermekle yükümlüdür. Zarar verici fiili yasaklayan bir hukuk kuralı bulunmasa bile, ahlaka aykırı bir fiille başkasına kasten zarar veren de, bu zararı gidermekle yükümlüdür.*" denilmektedir.

---

[225] Kemal Atasoy, "Kişilik Hakkı Kapsamında Sosyal Medyada Kişisel Verilerin Korunması Ve Veri Sahibinin Rızası", **Marmara Üniversitesi Hukuk Araştırmaları Dergisi**, Cilt:22, Sayı:3, 2016, s.274.
[226] Henkoğlu, age, s. 81.
[227] Çokmutlu, agt, s. 125-127.
[228] Türk Borçlar Kanunu hakkında bkz, https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6098&MevzuatTur=1&MevzuatTertip=5. (E.T. 07.02.2021).

Hukuka aykırı olarak kişisel verileri ele geçirilmek, başkasına vermek, kaydetmek eylemleri suç oluşturmasının yanında aynı zamanda haksız fiil de oluşturmaktadır. Yapılan haksız fiilin sonucu olarak da kişinin maddi ve manevi tazminat hakkı ile ilgili düzenlemeler TBK'nın 51 ve 52. maddelerinde düzenlenmiş bulunmaktadır.[229]

Sonuç olarak TMK ile TBK hükümlerince kişilik hakkına yönelen ihlalin önlenmesinin yanında kişisel verinin korunmasına hukuki zemin hazırlamaktadır.[230] Ancak kendine has niteliği olan bu alan, genel hükümler çerçevesinde yeterli koruma bulamamaktadır.

2.2.3.İş Kanunu

Kişisel verilerin korunması konusunda yeterli olmasa da 4857 sayılı İş Kanunu'nda[231] da hukuki düzenlemeler bulunmaktadır. Bu düzenlemelerden en önemlisi 4857 sayılı Kanunun "İşçinin özlük dosyası" hakkındaki 75. maddesidir. Bu maddede "*İşveren çalıştırdığı her işçi için bir özlük dosyası düzenler. İşveren bu dosyada, işçinin kimlik bilgilerinin yanında, bu Kanun ve diğer kanunlar uyarınca düzenlemek zorunda olduğu her türlü belge ve kayıtları saklamak ve bunları istendiği zaman yetkili memur ve mercilere göstermek zorundadır.*

İşveren, işçi hakkında edindiği bilgileri dürüstlük kuralları ve hukuka uygun olarak kullanmak ve gizli kalmasında işçinin haklı çıkarı bulunan bilgileri açıklamamakla yükümlüdür" denilmektedir.

İşveren tarafından işçi hakkında kaydedilen veriler ister fiziki ortamlarda ister elektronik ortamlarda depolansın, tüm veriler Kanun'un 75. maddesi gereğince korumadan yararlanacaktır. İşverenin yapılan iş kapsamında, işçinin kişilik haklarına ve özel yaşamına aykırı bir durumun oluşmaması konusunda gerekli özeni göstermesi gerekmektedir. Aynı zamanda bunun "işverenin gözetme borcu"nun da bir gereği olduğu ifade edilmiştir. [232]

---

[229] Çokmutlu, agt, s. 127.
[230] Ayözger, age, s. 98.
[231] İş Kanunu hakkında bkz, https://www.mevzuat.gov.tr/MevzuatMetin/1.5.4857.pdf (E.T. 07.02.2021)
[232] Öner Eyrenci, Savaş Taşkent, Devrim Ulucan, **Bireysel İş Hukuku**, 8. Baskı, Beta Yayımcılık, 2017 İstanbul, s. 170.

İşçilerin kişisel verilerinin korunması açısından işverenlere Kanun'un 75. maddesi ile bazı yükümlülükler getirilmiştir. Bu çerçevede işveren işçilerin kişisel verilerini içerecek bir özlük dosyası tutmakla yükümlüdür. Dolayısıyla işçilerin bu dosya kapsamına alınan kişisel verileri işverenin bilgisi ve denetimi altında tutulmaktadır. Maddenin ikinci bendinde ise bu verileri hukuka aykırı olarak kullanmaması için işveren uyarılmıştır. Bu maddede eksik olan eğer işveren bu kişisel verileri hukuka aykırı şekilde kullanması durumunda nasıl bir yaptırıma maruz kalacağı konusudur ve bu konuda bu maddede herhangi bir bilgi verilmemiştir. Ancak Kanunun başka bir yerinde 107. maddesinde işverenin yükümlülüklerine uymaması durumunda haklarında idari para cezası yaptırımı uygulanacağı bildirilmektedir.[233] Aslında işçi-işveren arasındaki ilişki sona erse bile, işverenin, işçinin kişisel verisini saklama konusunda sorumluluğu devam edecektir.[234]

Bu alanda dikkat edilmesi gereken bir başka nokta, işçinin internet ve eposta kullanımına yönelik bir düzenleme bulunmamasıdır. Gerçekten de bu konuda iş hukukuna ilişkin mevzuatta açık hükümler bulunmamaktadır. Bu konuda çıkan veya çıkabilecek ihtilaflar, ancak, Anayasa çerçevesinde, TMK genel hükümlerince (m. 24, 25) ve TCK hükümlerine başvurularak çözülebilecektir.[235]

2.2.4.Nüfus Hizmetleri Kanunu

5490 sayılı Nüfus Hizmetleri Kanunu[236] bireylerin nüfus bilgilerinin, diğer bir ifadeyle kişisel verilerinin kaydedilmesi ve korunması ile ilgili hükümleri içermektedir. Gerçekten de nüfus ile ilgili veriler kişisel verilerin temellerini oluşturmaktadır. Bu kanunla kişilerin ismi, soy ismi, doğduğu yıl, doğduğu yer, anne adı, anne kızlık soyadı, ikametgâhı, fotoğrafı, medeni durumu ve hatta dini görüşü gibi hassas kişisel verileri kütüklere işlenmektedir. Bu nedenle aralarında hassas kişisel

---

[233] İlke Gürsel, "İşçinin Kişisel Verilerinin Korunması Hakkı", Dokuz Eylül Üniversitesi, Sosyal Bilimler Enstitüsü, Yayımlanmamış Doktora Tezi, İzmir, 2016, s. 157-159.

[234] A. Eda Manav, "İş İlişkisinde İşçinin Kişisel Verilerinin Korunması", **Gazi Üniversitesi Hukuk Fakültesi Dergisi**, C. XIX, Y. 2015, Sayı 2, s. 133.

[235] K. Ahmet Sevimli, **İşçinin Özel Yaşamına Müdahalenin Sınırları,** Legal Yayınevi, İstanbul, 2006, s. 118.

[236] 5490 sayılı Nüfus Hizmetleri Kanunu için bkz, https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5490.pdf.

verilerin yer aldığı bu kadar çok verinin işlenmesine imkân veren bir kanunun, bu verileri tutanlara gizlilikle ilgili birtakım yükümlülükler getirmesi de kaçınılmazdır.[237]

"5490 sayılı Nüfus Hizmetleri Kanunu"nun amacı "*Kişinin doğumundan ölümüne kadar kişisel ve medeni durumuna, uyrukluğuna ve bunlarda meydana gelebilecek değişikliklere ait doğal ve hukuki olayların belirlenip saptanması, bu amaçla düzenlenmiş kütüklere yazılması, elektronik ortamda ulusal adres veri tabanının oluşturulması, nüfus kayıtları ile adres bilgilerinin ilişkilendirilmesini sağlamak"* olarak belirtmiştir. Buna yönelik kişilerin kişisel veri nitelikli bilgileri nüfus kütüklerine kaydedilmiştir.

Bu Kanunun 7. maddesi çerçevesinde kütüklere kaydedilecek kişisel bilgilerin neler olduğu ile ilgili bilgiler verilmektedir. 7. maddede;

"*1-Türkiye Cumhuriyeti Kimlik Numarası,*

2-Kayıtlı bulunduğu il, ilçe, köy veya mahalle adı ile cilt, aile ve birey sıra numarası,

3-Kişinin adı ve soyadı, cinsiyeti, baba ve ana adı ile soyadları, evli kadınların anne kızlık soyadları,

4-Doğum yeri ile gün, ay ve yıl olarak doğum tarihi ve kütüğe kayıt tarihi,

5-Evlenme, boşanma, soybağının kurulması veya reddi, ölüm, vatandaşlığın kazanılması veya kaybedilmesi gibi kişisel durumda meydana gelen değişiklik veya yetkili makamlarca yapılan düzeltmeler,

6-Dini,

7-Medeni hali,

8-Yerleşim yeri adresi

9-Fotoğrafı" aile kütüğüne kaydedilmektedir.

[237] Gültekin, age, s. 75.

Bu kayıtlar kişisel verilerin ve özel hayatın korunması bağlamında gizli olması gerekmektedir. Nitekim bu Kanunun "*Gizlilik*" başlıklı 9. maddesinde[238] bu bilgilerin gizli olduğu belirtilmektedir. Bu maddenin ilk fıkrasında nüfus kayıtları ve bu kayıtların tutulmasına dayanak olan belgelerin gizli oldukları ve bunların, yetkili ve sorumlu memurlar ile teftiş ve denetim yetkisi olanlar dışında kimse tarafından görülüp incelenemeyeceği belirtilmiştir. İkinci fıkrada ise, nüfus kayıtlarına bu bilgileri işleyen memurlar ve "Kimlik Paylaşımı Sistemi" kapsamında nüfus kayıtlarından faydalanan diğer görevlilerin de bu gizliliğe uymak zorunda oldukları ve bu yükümlülüğün kamu görevlilerinin görevlerinden ayrılmalarından sonra da devam ettiği ifade edilmiştir.[239] Bu yükümlülüklere uymayanların TCK'nın ilgili maddelerine göre sorumlu tutularak cezalandırılacaktır.

İdare, görevi gereğince ilgili kişisel verileri toplama, kullanma, işleme ve bazı durumlarda üçüncü kişilere aktarımını sağlanmaktadır. İlgili işlemleri yaparken de bilişim teknolojisinin kullanımının arttığı gözlemlenmektedir. Bu kapsamda "Merkezi Nüfus İdaresi Sistemi (Mernis)", "Kimlik Paylaşım Sistemi" gibi sistemleri de kullanmaktadır. Nüfus Hizmetleri Kanunu'nun 45. maddesine[240] göre, "Kimlik Paylaşımı Sistemi" veri tabanında bulunan verilerin tamamı veya bir kısmı herhangi bir kurum veya üçüncü kişilerin erişimine açılmayacaktır. Kurum veya üçüncü kişiler

---

[238] "(1) Nüfus kayıtları ve bu kayıtların tutulmasına dayanak olan belgeler gizlidir. Bunlar, yetkili ve sorumlu memurlar ile teftiş ve denetim yetkisi olanlar dışında kimse tarafından görülüp incelenemez. Mahkemeler bu hükmün dışındadır.
(2) Nüfus kayıtlarına bu bilgileri işleyen memurlar ve Kimlik Paylaşımı Sistemi kapsamında nüfus kayıtlarından faydalanan diğer görevliler de bu gizliliğe uymak zorundadırlar. Bu yükümlülük, kamu görevlilerinin görevlerinden ayrılmalarından sonra da devam eder."

[239] Gültekin, age, s. 75.

[240] "Madde 45- (1) Bakanlık, Kimlik Paylaşımı Sistemi ve Adres Paylaşımı Sistemi veri tabanlarında tutulan bilgileri bu Kanunda belirtilen esas ve usuller çerçevesinde kurumlar ile diğer kişilerin hizmetine açabilir. Yerleşim yeri adresi bilgileri ancak kurumlar ile 5411 sayılı Bankacılık Kanunu çerçevesinde faaliyette bulunan bankaların ve 3/6/2007 tarihli ve 5684 sayılı Sigortacılık Kanunu çerçevesinde faaliyette bulunan sigorta ve emeklilik şirketleri ile Güvence Hesabının paylaşımına açılabilir.
(2) Kimlik Paylaşımı Sistemi veri tabanındaki bilgilerin tamamı veya bir kısmı toplu halde hiçbir kuruma veya diğer kişilere verilemez. Kurumlar ve diğer kişiler kendi iş ve işlemlerine esas olmak üzere sadece kayıtlarını tuttukları kişilerin bilgilerini alabilirler.
(3) Kurumlar aldıkları bilgileri tanımlanmış hizmetlerin yerine getirilmesi dışında başka hiçbir amaçla kullanamaz; ilgilisi veya bu Kanunun 44 üncü maddesinde belirtilenler dışında kimseye veremez. Sistemin bütün aşamalarında görev yapan yetkililer de bu kurallara uymakla yükümlüdür. Bu yükümlülük, kamu görevlilerinin görevlerinden ayrılmalarından sonra da devam eder.
(4) Genel Müdürlükten alınan bilgilerin iş ve işlemlerde kullanılmasının hukukî sonuçları bilgiyi alan kurumun sorumluluğundadır.
(5) Bu Kanun ile kurulacak veri tabanlarının istatistik amaçlı kullanımında 10/11/2005 tarihli ve 5429 sayılı Türkiye İstatistik Kanunu hükümleri uygulanır."

sadece görev alanı bünyesindeki kayıtları tutup, ilgililerin verilerini isteyebilirler. Bu hüküm önemlidir. Zira devletin birçok kurumu neredeyse kişilerin bütün bilgilerine ulaşmak istemektedirler. Bu hükme göre ise kurumlar ancak görev alanlarına giren konularda sadece ilgili kişilerin bilgilerini talep edebileceklerdir.[241]

2.2.5.Vergi Usul Kanunu

"213 sayılı Vergi Usul Kanunu"nda[242] kişisel verilerin toplanmasına ilişkin Maliye Bakanlığı mükellefler hakkında bilgi toplama ve saklama yetkisine dair özel düzenlemeler bulunmaktadır. 5. maddede vergi dairelerinin elde ettiği sır veya bilginin yalnız vergi kanununda yer alan amaçlarca kullanılabilmesine yönelik normdur.[243] 148. madde hükmünce, "kamu idare ve müesseseleri, mükellefler veya mükelleflerle muamelede bulunan diğer gerçek veya tüzel kişiler", Maliye Bakanlığınca vergi incelemesi yapma yetkisi verilen tarafından istenilen verileri sözlü veya yazılı olarak vermek zorundadırlar.[244] Sözlü istenen bilgilerin verilmemesi durumunda bir yazı yazılarak cevap verilmesi için uygun bir süre verilir. İlgilinin cevap vermemesi durumunda zor kullanılarak vergi dairesine getirilmesi mümkün değildir. Buna ek olarak vergi incelemelerinin hızla yapılabilmesi ve elde edilen bilgilerin saklanabilmesi amacıyla 152. madde gereğince istihbarat arşivi kurulmuş, arşivden kimlerin ne şekilde faydalanabileceğine Maliye Bakanlığı'nın karar vereceği hükme bağlanmıştır.[245] Bu arşivde saklanan verilerin amaç dışı kullanımı veya başkalarının eline geçmesi durumunda kişisel verilerin korunması hakkı ihlal olacağından, idarenin sorumluluğuna gidilebilecektir.

---

[241] Çokmutlu, agt, s. 130-131 ve Korkmaz, age, s. 361.

[242] 213 sayılı Vergi Kanunu için bkz, https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=213&MevzuatTur=1&MevzuatTertip=4.

[243] "Madde 5 – *Aşağıda yazılı kimseler görevleri dolayısıyla, mükellefin ve mükellefle ilgili kimselerin şahıslarına, muamele ve hesap durumlarına, işlerine, işletmelerine, servetlerine veya mesleklerine mütaallik olmak üzere öğrendikleri sırları veya gizli kalması lazım gelen diğer hususları ifşa edemezler ve kendilerinin veya üçüncü şahısların nef'ine kullanamazlar;*
1.Vergi muameleleri ve incelemeleri ile uğraşan memurlar; 2. Vergi mahkemeleri, bölge idare mahkemeleri ve Danıştayda görevli olanlar; 3. Vergi kanunlarına göre kurulan komisyonlara iştirak edenler; 4. Vergi işlerinde kullanılan bilirkişiler. Bu yasak, yukarıda yazılı kimseler, bu görevlerinden ayrılsalar dahi devam eder."

[244] Çetin Arslan, "Vergi Mahremiyetini İhlal Suçu (VUK md. 362)", **Hacettepe Hukuk Fakültesi Dergisi**, 3(2) 2013, s.16.

[245] Neslihan Karataş Durmuş, "Ticari Sırların Ve Kişisel Verilerin Korunması Kapsamında Vergi Mahremiyeti", TAAD, Yıl:8, Sayı:31, Temmuz 2017, s.375.

2.2.6.Polis Vazife ve Salahiyet Kanunu

"2559 sayılı Polis Vazife ve Salahiyet Kanunu (PVSK)"nda[246] çeşitli kamu hizmetlerinin verilmesi ve kamu güvenliğinin sağlanması ile suçun önlenmesi amaçları için bazı kişisel verilerin toplanabilmesine izin verilmektedir. PVSK'da kişisel veri niteliğinde olan kişilerin parmak izi ve fotoğrafların kayda alınması ile istihbarat amaçlı iletişimin tespiti konularında özel hükümler bulunmaktadır.[247]

PVSK'nın 5. maddesine[248] göre, "sisteme kaydedilen bilgiler, kimlik tespiti, suçun önlenmesi veya yürütülmekte olan soruşturma ve kovuşturma kapsamında maddî gerçeğin ortaya çıkarılması amacıyla mahkeme, hâkim, Cumhuriyet savcısı ve kolluk" tarafından kullanılabilir. Ayrıca sistemde kayıtlı bilgilerin hangi kamu görevlisi tarafından ve ne amaçla kullanıldığının denetlenebilmesine imkân tanıyan bir güvenlik sistemi kurulmasının gerekliliği kanunda düzenlenmiştir. PVSK'nın 5/9 maddesi hükmünce "*Sistemde yer alan kayıtlar gizlidir ve belirlenen amaçlar dışında kullanılamaz. Sisteme kayıtlı olan parmak izi ve fotoğraflar, kişinin ölümünden itibaren on yıl ve her halde kayıt tarihinden itibaren seksen yıl geçtikten sonra sistemden silinmesi gerekir.*" Kayıtları silmekle yükümlü kişi tarafından silinmemesi sonucu TCK'nın 138. maddesi gereğince sorumluluk doğacaktır.

Ayrıca PVSK'nın EK 7. maddesi uyarınca polisin istihbarat kapsamında bilgi toplama ve iletişimi denetleme yetkisi de bulunmaktadır. Polis, ülke ve milletin bütünlüğü, anayasa düzeni ve genel güvenlik için önleyici ve koruyucu tedbirleri uygulamada yasal dayanağını bu genel düzenlemeden alır. İstihbarat çalışmaları ise açık bilgi veya gizli bilgi üzerinden yapılır. Açık bilginin kişisel veri kapsamında olan kısmının depolanması ve bunların değerlendirilmesi kişilik hakları ile ilgili olduğundan yasa ile düzenlenmelidir. Gizli bilgilere erişilebilmesi için de yasal

---

[246]"2559 sayılı Polis Vazife ve Salahiyet Kanunu" için bkz, https://www.mevzuat.gov.tr/MevzuatMetin/1.3.2559.pdf.

[247] Çokmutlu, agt, s. 132-133 ve Korkmaz, age, s. 339-340.

[248] 2559 sayılı PVSK'nın 5. Maddesi "*Polis; her çeşit silah ruhsatı, sürücü belgesi, pasaport veya pasaport yerine geçen belge almak için başvuruda bulunan, başta polis olmak üzere, genel veya özel kolluk görevlisi ya da özel güvenlik görevlisi olarak istihdam edilen, Türk vatandaşlığına başvuruda bulunan, sığınma talebinde bulunan veya gerekli görülmesi halinde, ülkeye giriş yapan sair yabancı, gözaltına alınan kişilerin parmak izini alır. Birinci fıkraya göre alınan parmak izi, ait olduğu kişinin kimlik bilgileri ile birlikte, ne zaman ve kim tarafından alındığı belirtilmek suretiyle, bu amaca özgü sisteme kaydedilerek saklanır. Ancak, parmak izinin hangi sebeple alındığı sisteme kaydedilmez.*
Olay yerinden elde edilen ve kime ait olduğu henüz tespit edilemeyen parmak izleri, kime ait olduğu tespit edilinceye kadar, ilgili soruşturma dosya numarası ile birlikte sisteme kaydedilir."

düzenleme gerekmektedir. Yürürlükte olan istihbarat yasalarımız, hangi yetkinin kim tarafından, nasıl kullanılacağı ve nasıl denetleneceği konusunda detaylı düzenleme içermemektedir. Mevcut olan eksikliklerin tamamlanması gerekmektedir.[249]

İleride suç işlenmesini önlemek amacıyla polisin bilgi toplama yetkisini kullanabilmesi için "belli olayların" ortaya çıkması ve bu olaylarla ilgili şüphenin belli kişiler üzerinde yoğunlaşması şart olmalıdır. Aksi takdirde istihbarat yoluyla kişinin özel hayatına, kişisel verilerine, haberleşme özgürlüğüne müdahale söz konusu olacaktır. Söz konusu hakların, temel hak ve özgürlüklerden olması sebebiyle ancak Anayasa ve Uluslararası sözleşmelere uygun olarak kanuni düzenlemeler doğrultusunda müdahale edilebilir.[250]

2.2.7.Elektronik Haberleşme Kanunu

Elektronik Haberleşme Kanunu(EHK)[251], elektronik haberleşme sektörüne ilişkin kişisel verilerin korunmasıyla ilgili hükümler içermektedir. EHK 12/2(d) maddesinde işletmecilerin hak ve yükümlülükleri arasında kişisel veri ve gizliliğinin sağlaması açık bir yükümlülük olarak belirlenmiştir. EHK 12/2(g) maddesinde ise işletmecilerden kanunlarla yetkili kılınan kurumlar tarafından yasal dinleme ve iletişime müdahalenin yapılmasına teknik olanak sağlanmasını temin etmek bir yükümlülük olarak düzenlenmiştir.[252]

EHK'nın 55. maddesi, "Kurum tarafından izin verilmedikçe, abone kimlik ve iletişim bilgilerini taşıyan özel bilgiler veya cihazın teşhisine yarayan elektronik kimlik bilgileri yeniden oluşturulamaz, değiştirilemez, kopyalanarak çoğaltılamaz veya herhangi bir amaçla dağıtılamaz."

EHK'nın 56. maddesi ise, " *abone kimlik ve iletişim bilgilerini taşıyan özel bilgiler ile cihazların elektronik kimlik bilgilerini taşıyan her türlü yazılım, kart, araç veya gereç yetkisiz ve izinsiz olarak kopyalanamaz, muhafaza edilemez, dağıtılamaz,*

[249] Ramazan Karabulut, "Kişisel Verilerin Korunması ve Kolluk Hizmetleri", Dicle Üniversitesi, Sosyal Bilimler Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, Diyarbakır, 2014, s. 91.
[250] Zeynep Bayram, "Suç Öncesi ve Sonrası Kişisel Veri Toplama Yetkisi", Bahçeşehir Üniversitesi, Sosyal Bilimler Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, İstanbul, 2009, s. 12.
[251] 5 Kasım 2008 tarihli 5809 sayılı Elektronik Haberleşme Kanunu için bkz, RG, T. 10 Kasım 2008, S. 27050.
[252] Ayözger, age, s. 106.

kendisine veya başkasına yarar sağlamak maksadıyla kullanılamaz." hükümleriyle kişisel verilerin korunmasının önemi vurgulanmıştır.

EHK'nın 51. maddesinin eski hali[253], Anayasa Mahkemesi kararıyla iptal edilmiştir.[254] İptal kararında, anayasal bir hakkın sınırlandırılmasının ancak kanuni bir düzenlemeyle yapılabileceği belirtilmiştir. Dolayısıyla yürütme organı tarafından yapılacak bir sınırlandırmanın hukuka aykırılık oluşturacağı gerekçesiyle ilgili madde iptal edilmiştir. İlgili madde yeniden düzenlenmiş ve bugünkü halini almıştır. EHK kapsamında bir kişisel verinin işlenmesi ancak KVKK'nın 4. maddesinde düzenlenen temel ilkeler kapsamında yapılabilecektir. Yine bu kapsam çerçevesinde yapılan veri işlemelerinin amacı doğrultusunda kullanımının ve güvenliğinin temini işletmecilerin yükümlülüğü olarak belirtilmiştir.[255]

2.2.8.İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun

"5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadelesi Hakkında Kanun"[256] internet ortamındaki yayınları düzenlemek ve suç işlenmesiyle mücadele amaçlanmaktadır. Buna ek olarak kanun internet aktörlerini "*erişim sağlayıcı, yer sağlayıcı, içerik sağlayıcı, internet toplu kullanım sağlayıcı ve ticari amaçla internet toplu kullanım sağlayıcısı*" olarak belirtmiş ve yükümlülüklerini düzenlemiştir.[257]

Kanun 3. maddesiyle *"İçerik, yer ve erişim sağlayıcıları, yönetmelikle belirlenen esas ve usuller çerçevesinde tanıtıcı bilgilerini kendilerine ait internet ortamında kullanıcıların ulaşabileceği şekilde ve güncel olarak bulundurmakla*

---

[253] EHK iptal edilen 51. madde metni: "Bilgi Teknolojileri ve İletişim Kurumu elektronik haberleşme sektörüyle ilgili kişisel verilerin işlenmesi ve gizliliğinin korunmasına yönelik usul ve esasları belirlemeye yetkilidir."

[254] Anayasa Mahkemesi iptal gerekçesinde "*Yasama yetkisinin devredilmezliği ilkesi gereğince, Anayasa'nın açıkça kanunla düzenlenmesinin öngördüğü konularda yürütme organına doğrudan ve ilk elden düzenleyici işlem yapma yetkisi verilemez. Elektronik haberleşme sektörüyle ilgili kişisel verilerin işlenmesi ve gizliliğinin korunmasına yönelik usul ve esasları belirleme yetkisini Bilgi Teknolojileri ve İletişim Kurumuna veren itiraz konusu kural, Anayasa'nın 20. Maddesinde öngörülen kişisel verilerin korunmasına ilişkin usul ve esasların ancak kanunla düzenleneceğine ilişkin güvenceye aykırıdır*." AYM, E: 2013/122, K: 2014/74, T: 09.04.2014, RG, T. 26.07.2014, S. 29072.

[255] Küzeci, age, s. 522.

[256] 5651 sayılı Kanun için bkz, https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5651.pdf.

[257] Zeynep Yasaman, **İnternette Marka Hakkının İhlali**, 1. Baskı, On İki Levha Yayıncılık, İstanbul 2020, s. 562.

yükümlüdür." bilgilendirme yükümlülüğü düzenlenmiştir. Hükümle birlikte internet kullanıcıları aktörlere kolay bir şekilde ulaşabilecektir.

Kanun'un "Bilgilendirme yükümlülüğü" başlıklı 3. maddesinin dördüncü fıkrası, "6552 sayılı İş Kanunu ile Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılması ile Bazı Alacakların Yeniden Yapılandırılmasına Dair Kanun" ile değişikliğe uğramıştır. Buna göre ilgili fıkra "(4) Trafik Bilgisi Telekomünikasyon İletişim Başkanlığı tarafından ilgili işletmecilerden temin edilir ve hâkim tarafından karar verilmesi hâlinde ilgili mercilere verilir." şeklinde bir düzenlemeye gidilmiştir.[258] Söz konusu düzenleme ve Kanunla getirilen diğer bazı düzenlemeler hakkında Anayasa Mahkemesinde iptal davası açılmıştır. Anayasa Mahkemesi kararında, TİB tarafından trafik bilgileri temin edilecek olan ilgili işletmeciler ile trafik bilgileri kendilerine verilecek olan ilgili mercilerin hangileri olduğunun belirtilmediği, bunun sonucunda sınırları belirsiz bir durumun oluşması neticesinde, keyfi uygulamalara sebebiyet verilebileceği ve bunun Anayasa'nın 2. maddesinde bulunan "hukuk devleti" ilkesine aykırı olduğunu belirtmiştir. Mahkeme ayrıca söz konusu düzenlemeyle, TİB'e, trafik bilgilerinin ilgili işletmecilerden temini yetkisi tanındığı belirtilmektedir. Buna göre, TİB herhangi bir ihbar, iddia, şikâyet, talep ya da başvuru olmaksızın, kendi kendine trafik bilgilerini ilgili işletmecilerden isteyebilecektir. Kararda belirtildiği gibi, bu durum "hukuk devleti" ve "özel hayatın gizliliği" ilkeleriyle çelişmektedir. Mahkeme, söz konusu düzenlemenin, kişilerin açık rızası olmadan kişisel verisi olan trafik bilgilerine ulaşılabilmesine imkân tanıması nedeniyle, Anayasanın 20. maddesine aykırı olduğu sebebiyle iptaline hükmetmiştir.[259]

Buna ek olarak 9. madde hükmünce, bir içeriğin kişinin haklarını ihlal etmesi durumunda tazminini sağlama imkânı ortaya çıkmaktadır. İhlalin doğduğunu düşünen

---

[258] Korkmaz, age, 368. Dava konusu Kural'ın önceki düzenlemesi, "Trafik bilgisi ancak bir suç soruşturması ve/veya kovuşturması kapsamında mahkemelerce talep edilmesi hâlinde Başkanlık tarafından içerik sağlayıcı, yer sağlayıcı ve/veya erişim sağlayıcıdan alınarak verilir." şeklindeydi. Diğer bir deyişle, değişiklikten önce, trafik bilgisi ancak bir soruşturma kapsamında mahkemeler tarafından talep edilmesi halinde, ilgili yerlerden alınarak mahkemelere veriliyordu. Değişiklikle artık trafik bilgileri TİB tarafından ilgili işletmecilerden temin edildikten sonra hâkim tarafından karar verilmesi halinde (mahkemeler dışında) ilgili mercilere verilebilecektir.

[259] Şaban Cankat Taşkın, "İnternete Erişim Yasakları ve Hukuka Aykırılıklar", Kocaeli Üniversitesi, Sosyal Bilimler Enstitüsü, Yayımlanmamış Doktora Tezi, Kocaeli, 2015, s. 489-490, AYM, K: 2014/151, E: 2014/148, T: 02.10.2014. RG, T:01.01.2015, S: 29223.

kişi önce içerik sağlayıcısı cevap alamaması durumunda yer sağlayıcıya başvurarak kendisiyle ilgili ihlali oluşturan içeriğe ilişkin yayının kaldırılmasını ve kendisi tarafından hazırlanan cevabın bir hafta süre ile yayımlanarak yanlışlığın düzeltilmesini talep edebilir.[260]

2.2.9.Ceza Muhakemesi Kanunu

Ceza Muhakemesi Kanunu'nun (CMK)[261] 75 vd. maddelerinde kişisel verilerin işlenmesi düzenlenmiştir. Soy bağının tespiti veya suç mahallinde elde edilen delillerin, suç ile ilgili şüpheli veya sanığa ya da mağdura ait olup olmadığının araştırılması, zorunluluk halinde moleküler genetik incelemeler yapılması, şüpheli, sanık veya diğer kişilerin beden muayenesi ve vücudundan numune alınması, konuya ilişkin örnekler olarak gösterilebilir. Fiziki kimliğin tespitine yönelik olarak, şüpheli veya sanığın, kimliğinin teşhisine yönelik araştırmalarda, Cumhuriyet savcısının emriyle fotoğrafı, parmak ve avuç içi izi, beden ölçüleri, bedeninde bulunan ve teşhisine yardımcı olacak diğer özellikleri ile ses ve görüntülerin kaydedilmesine izin verilmektedir.[262] CMK'nın 75 vd. maddeleri uyarınca alınan örnekler üzerinde yapılan inceleme sonucu elde edilen bulgular CMK'nın 80. maddesi kapsamında kişisel veri niteliğinde olup, alınma amacı dışında başka bir amaçla kullanılamaz, dosya içeriğini öğrenme yetkisi bulunanlarca açıklanamaz, yayınlanamaz ve bir başkasına verilemez.[263]

CMK'nın 134 vd. maddelerinde ise; bilgisayar ortamında verilerin kopyalanması, telekomünikasyon yoluyla yapılan iletişimin denetlenmesi, gizli soruşturmacı ve teknik araçlarla izlemeyle ilgili önlemler ve bu önlemlerin denetlenmesine ilişkin hükümler düzenlenmektedir. Buna göre; 134. maddede "Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma" işlemlerine ilişkin düzenlemeler getirilmiştir. 135. maddeye göre ise; "Bir suç dolayısıyla yapılan soruşturma ve kovuşturmada, suç işlendiğine ilişkin kuvvetli

---

[260] Kılınç, agm, s. 1138.

[261] 5271 sayılı Ceza Muhakemeleri Kanunu için bkz, https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5271.pdf.

[262] Bahri Öztürk, Durmuş Tezcan, Mustafa Ruhan Erdem, Özge Sırma, Yasemin F. Saygılar ve Esra Alan, **Nazari ve Uygulamalı Ceza Muhakemesi Hukuku**, 11. Baskı, Seçkin Yayınevi, Ankara, 2017, s. 96 vd.

[263] Hakan Hakeri ve Yener Ünver, **Ceza Muhakemesi Hukuku**, 15. Baskı, Adalet Yayınevi, Ankara, 2019, s. 141 vd.

şüphe sebeplerinin varlığı ve başka suretle delil elde edilmesi imkânının bulunmaması durumunda, hâkim veya gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısının kararıyla şüpheli veya sanığın telekomünikasyon yoluyla iletişimi tespit edilebilir, dinlenebilir, kayda alınabilir ve sinyal bilgileri değerlendirilebilir." Görüldüğü üzere, kişinin iletişimine müdahale edilebilmesinin tek yolu ancak yargı kararıyla mümkündür.[264] Yine 140. maddede sayılan belli suçların işlendiğine dair güçlü şüphe bulunması ve başka bir şekilde delil elde edilmesinin mümkün olmaması hâlinde, şüpheli veya sanığın kamuya açık yerlerdeki eylemleri ile işyeri izlemeye uygun araçlarla izlenebilir, sesli ve görüntülü kaydı yapılabilir. Günümüzde, telekomünikasyon vasıtasıyla yapılan iletişimin son derece yaygınlaşması ve hayatın vazgeçilemez bir parçası haline gelmesi karşısında bu maddenin değerinin daha da arttığı söylenebilir. [265]

Yine kişisel verilerin gizliliğinin sağlanması açısından önemli bir düzenleme de "duruşmada okunması zorunlu belge ve tutanaklar" başlıklı CMK'nın 209. maddesidir. Maddenin ikinci fıkrası, "sanığa veya mağdura ilişkin kişisel verileri içeren belgelerin, açıkça istemeleri halinde kapalı duruşmada okunmasına karar verilebileceği" şeklindedir. Maddeyle ilgisiz kişilerin davanın taraflarına ait kişisel verileri öğrenmelerinin engellenmesi amaçlanmıştır. Ayrıca Anayasaya uygun olarak kişisel verilerin açıklanması kişinin rızasına bırakılmıştır.[266]

2.2.10.Hukuk Muhakemeleri Kanunu

Ceza Muhakemesi Kanunu'nda olduğu gibi Hukuk Muhakemeleri Kanunu'nda da duruşma yapılırken davanın taraflarının kişisel verilerinin korunmasına ilişkin hükümler bulunmaktadır. Bilindiği üzere açık yargılama ilkesinin bir gereği olarak duruşmalar alenidir. Davanın tarafları haricinde davayı izlemek isteyenler de duruşmalara katılabilmektedirler. Ancak Kanunda belirtilen bazı durumlar için duruşmaların gizli yapılmasına karar verilebilmektedir.[267] Bu durumu düzenleyen 6100 sayılı Kanunun 28. maddesinin ikinci fıkrası, "*Duruşmaların bir kısmının veya*

---

[264] Veli Özer Özbek, Koray Doğan, Pınar Bacaksız, İlker Tepe, **Ceza Muhakemesi Hukuku**, 8. Baskı, Seçkin Yayınevi, Ankara, 2016, s. 234 vd.
[265] Nur Centel, Hamide Zafer, **Ceza Muhakemesi Hukuku**, 13. Baskı, Beta Yayımcılık, İstanbul, 2016, s. 463.
[266] Güray Dağ, "Kişisel Verilerin Ceza Muhakemesi Hukukunda Delil Olarak Kullanılması", Marmara Üniversitesi Sosyal Bilimler Enstitüsü, Yayımlanmamış Doktora Tezi, İstanbul, 2011, s. 181.
[267] Çokmutlu, agt, s. 165.

tamamının gizli olarak yapılmasına ancak genel ahlâkın veya kamu güvenliğinin kesin olarak gerekli kıldığı hâllerde, taraflardan birinin talebi üzerine yahut resen mahkemece karar verilebilir." şeklindedir. Bu hükme göre taraflar duruşmanın gizli yapılmasını talep edebilmektedirler. Ancak bunun için genel ahlak veya kamu güvenliği sebebiyle gereklilik bulunması gerekmektedir.

Konuya kişisel verilerin korunması açısından bakılacak olursa, davanın tarafları, kendi özel hayatlarına ilişkin kişisel verilerin üçüncü kişilerce öğrenilmesini engel olmak için bu verilerin ifşasının genel ahlaka aykırı olacağı iddiasıyla duruşmanın gizli yapılmasını hâkimden isteyebileceklerdir.

Hukuk Usulü Muhakemeleri Kanununda kişisel verilerin korunmasına yönelik bir başka hükümde, 6100 sayılı Kanunun "Kayıt ve yayın yasağı" başlıklı 153. maddesidir. Maddenin birinci fıkrasına[268] göre, yargılamanın zorunlu kıldığı hallerde duruşma sırasında yapılan kayıtlar, bu kayılar taraflara ait kişisel verileri içereceğinden, mahkeme ve ilgili kişilerin izni olmadığı sürece yayınlanamayacaktır. Bu hükümde, Anayasal düzenleme gereği, kişisel verilerin işlenmesinde ilgili kişinin rızasının alınması gerekliliği kuralına uygun bir hükümdür. [269]

[268] "Duruşma sırasında fotoğraf çekilemez ve hiçbir şekilde ses ve görüntü kaydı yapılamaz. Ancak, dava dosyasında saklı kalmak kaydıyla, yargılamanın zorunlu kıldığı hâllerde, mahkemece çekim yapılabilir ve kayıt alınabilir. Bu şekilde yapılan çekim ve kayıtlar ile kişilik haklarını ilgilendiren konuları içeren dava dosyası içindeki her türlü belge ve tutanak, mahkemenin ve ilgili kişilerin açık izni olmadıkça hiçbir yerde yayımlanamaz."

[269] Çokmutlu, agt, s. 165-166.

ÜÇÜNCÜ BÖLÜM

TÜRK CEZA KANUNU'NDA KİŞİSEL VERİLERİN KORUNMASINA YÖNELİK SUÇLAR

TCK'da kişisel verilerin korunmasına yönelik olarak "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" başlıklı dokuzuncu bölümünde "Kişisel verilerin kaydedilmesi", "Verileri hukuka aykırı olarak verme veya ele geçirme", "Verileri yok etmeme" suçları, sırasıyla TCK'nın 135, 136 ve 138. maddelerinde düzenlenmiştir.

Kişisel veriyi korumaya yönelik cezai düzenlemelerin, Almanya gibi kişisel verilere ilişkin olarak düzenlenen kanunda ya da ülkemiz veya Fransa'da olduğu gibi ceza kanununda yer vererek yaptırıma bağlandığı görülmektedir.

TCK'da kişisel veriyi korumaya yönelik olarak düzenlenen suçların uygulanmasında kişisel veri ve işlenmesine ilişkin tanımların TCK'da düzenlenmemiş olması öğretide sıkça eleştirilmiş, kanunilik ve belirlilik ilkelerine aykırılık oluşturduğu görüşleri ortaya atılmıştır. [270]

[270] KVKK'nın yürürlüğe girmesinden önce öğretide TCK'da kişisel veri tanımının yapılmamasının, kanunilik ve belirlilik ilkesine aykırı olduğu yönünde görüşler mevcuttu. Küzeci, 286, Osman Yaşar, Hasan Tahsin Gökcan, Mustafa Artuç, **Yorumlu Uygulamalı Türk Ceza Kanunu** (Tamamen Gözden Geçirilmiş 2. Baskı), C: 3, Adalet Yayınevi, Ankara, 2014, s, 4432. Bunun yanısıra TCK'da yer alan suç tiplerinin uygulanmasının KVKK'nın yürürlüğe gireceği tarihe kadar ertelenmesi gerektiği belirtilmiştir. Diğer bir görüşe göre bu eksikliğin sebebi, madde kaynağını oluşturan Fransız Ceza Kanunu'nda da kişisel verinin tanımının yapılmayıp tanımın kişisel verilerin korunması için çıkarılmış özel kanunda yapılmış olmasıdır. Muammer Ketizmen, **Türk Ceza Hukuku'nda Bilişim Suçları**, Adalet Yayınevi, Ankara, 2008, s, 235. Başka bir görüşe göre ise KVKK'nın yürürlüğe girmesinden önce TCK'da yer alan kavramların anlamının kıyas yasağını ihlal etmeden yorum yoluyla değerlendirilmesinde sorun bulunmamaktadır. Asıl olan kıyas yasağıdır. Kanun koyucunun burada kavramın tanımlanmasını ve içeriğinin belirlenmesini öğreti ve uygulamaya bırakması doğaldır. Veli Özer Özbek, **TCK İzmir Şerhi, Yeni Türk Ceza Kanunun Anlamı Özel Hükümler**, C: 2, Seçkin Yayıncılık, Ankara, 2008, s. 948.

Nitekim bu aykırılık iddiası Anayasa Mahkemesi'ne taşınmış olmakla birlikte mahkeme "*kişisel veri kavramının teknolojik gelişmelere bağlı olarak çok farklı şekillerde ortaya çıkabileceğinden, bu kapsama giren tüm verilerin kanun koyucu tarafından önceden öngörülebilmesi ve tek tek sayılabilmesinin mümkün olmadığı*" gerekçesiyle itirazı reddetmiştir.[271]

KVKK'nın yürürlüğe girmesiyle bu tanımlar kanuni bir temele oturtulmuş olmakla birlikte, kanunilik ilkesi sağlanmış ve öğretideki bu konuyla ilgili tartışmaların bir önemi kalmamıştır.

Çalışmamızın bu bölümünde "Kişisel verilerin kaydedilmesi", "Verileri hukuka aykırı olarak verme veya ele geçirme", "Verileri yok etmeme" suçları sırasıyla incelenecek olup tekrara düşmemek adına bu suçlar bakımından ortak hükümler içeren özel görünüş şekillerine ayrıca değinilecektir.

3.1.Kişisel Verilerin Kaydedilmesi Suçu

TCK 135. maddesinde kişisel verinin amacının dışında kullanımını ve kaydedilmesini önlenmek amacıyla "kişisel verilerin hukuka aykırı olarak kaydedilmesi" suç olarak düzenlenmiştir.

"Kişisel verilerin hukuka aykırı olarak kaydedilmesi suçu" iki fıkra olarak düzenlenmiştir. İlk fıkrada suçun yaptırımı genel olarak hukuka aykırı olarak kaydedilme işlemiyle ilgiliyken, ikinci fıkrada "hassas veri"ye ilişkin bir kaydetme işlemi söz konusu olması durumunda cezanın artırılacağı düzenlenmiştir. TCK'nın 137. maddesinde[272] ise suçun nitelikli halleri düzenlenmiştir.

---

[271] "Kuralda yer alan kişisel veri kavramı teknolojik gelişmelere bağlı olarak çok farklı şekillerde ortaya çıkabileceğinden bu kapsama giren tüm verilerin kanun koyucu tarafından önceden öngörülebilmesi ve tek tek sayılabilmesi mümkün değildir. Bununla birlikte gerek ulusal ve uluslararası mevzuat gerekse yargı içtihatları çerçevesinde kişisel veri kavramının, belirli veya kimliği belirlenebilir olmak şartıyla, bir kişiye ilişkin bütün bilgileri ifade ettiği kabul edilmektedir kişisel veri kavramının bu çerçevede öğreti, uygulama ve yargı kararlarında belirlenerek anlam ve içeriğinin gelişip değişeceğinde kuşku yoktur. Dolayısıyla başvuru kararında her ne kadar ceza mevzuatında kişisel veri ile ilgili bir tanım ve sınırlandırmanın yapılmadığı, bu nedenle itiraz konusu kuralın belirsiz olduğu ileri sürülmüş ise de ulusal ve uluslararası mevzuat ile yargı içtihatları dikkate alındığında kuralın belirsiz olduğundan söz edilemeyeceği açıktır." Anayasa Mahkemesi, E. 2015/32, K. 2015/102, T. 12.11.2015.

[272] "Nitelikli haller: (1) Yukarıdaki maddelerde tanımlanan suçların; a) Kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle, b) Belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle, İşlenmesi halinde, verilecek ceza yarı oranında artırılır."

Bu fıkranın KVKK yürürlüğe girmeden önceki hali[273] öğreti ve uygulama açısından farklı yoruma sebep olmaktayken, madde değişikliğiyle birlikte düzenlenme şekli öğreti ve uygulama arasındaki kafa karışıklığını gidermek için uygun bir değişiklik olmuştur. Maddenin değişikliğe uğramadan önceki halinin ilk ve ikinci fıkralarında öngörülmüş fiiller ve aynı yaptırıma bağlanmış olması ile ikinci fıkrada suç oluşturan fiilerin işleniş şekliyle ilgili belirsizlik, öğretide tartışmalara konu olmuştur. Yazarların bir kısmı kişisel verilerin kaydedilmesi ile ikinci fıkrada tahdidi olarak sayılmış olan bilgilerin veri olarak kaydedilmesinin aynı anlama gelmediğini savunmuştur. Bu görüşe göre kanunun lafzından yola çıkılarak ilk fıkrada "kişisel verileri kayıt etme", ikinci fıkrada ise "tahdidi olarak sayılmış verilerin kişisel veri olduğunu bilerek kayıt etme"nin yasaklandığı benimsenmiştir.[274] Maddenin bu şekildeki lafzının ve yorumlanmasının kişisel verilerin korunması amacını tam olarak sağlamaya elverişli olmadığı ve konuya ilişkin düzenlemenin asıl amacının ikinci fıkrada sayılan hassas veri niteliğindeki verilere yönelik daha fazla koruma sağlanması olduğu kanaatindeki yazarların da katkısıyla düzenleme bugünkü şeklini almıştır.[275]

3.1.1.Suçla korunan hukuki değer

Suçla korunan hukuki değer, toplumsal düzenin devamı için bir ceza normuyla korunması gereken soyut, manevi, ideal değerlerdir.[276] "Kişisel verilerin kaydedilmesi suçu", "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" bölümünde düzenlenmiştir. TCK'nın sistematiğine bakıldığında suçla, özel hayatın koruma altına alınmaya çalışıldığı anlaşılmaktadır. Kişisel verilerin korunmasını isteme hakkının Anayasal ve AİHS 8. Madde kapsamında güvence altına alındığını çalışmamızın ikinci bölümünde detaylı olarak incelemiştik. Dolayısıyla ilgili suçta korunan hukuki değerin, Anayasa'da dayanağını bulan ve Anayasa Mahkemesi kararında[277] da bahsedildiği gibi "*kişinin insan onurunun korunmasının ve kişiliğini serbestçe*

[273]"Kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimse, yukarıdaki fıkra hükmüne göre cezalandırılır."
[274] Zeki Hafızoğulları, Muharrem Özen, **Türk Ceza Hukuku Özel Hükümler Kişilere Karşı Suçlar**, 5. Baskı, Usa Yayıncılık, Ankara, 2016, s. 289.
[275] V. Özer Özbek, Koray Doğan, Pınar Bacaksız, **Türk Ceza Hukuku Özel Hükümler**, 15.Baskı, Seçkin Yayıncılık, Ankara, 2020, s. 581.
[276] Mehmet Emin Artuk, Ahmet Gökcen, Mehmet Emin Alşahin, Kerim Çakır, **Ceza Hukuku Genel Hükümler**, 14. Baskı, Adalet Yayınevi, Ankara, 2021, s. 307.
[277] İçtihat detayı için bkz; AYM, E. 2013/122, S. 2014/74, T. 09.04.2014.

geliştirebilmesi hakkının özel bir biçimi" olarak kişisel verinin korunması hakkının olduğunu söyleyebiliriz.

Öğretide bazı yazarlar[278], kişisel verilerin kişinin manevi şahsiyetini korumayı amaçladığı, bu alanın da kişinin özel hayatının önemli bir kısmını oluşturduğunu ifade etseler de, genel kabul gören görüşe göre bu suç ile korunan hukuki değer kişisel verilerin korunması hakkıdır.[279]

3.1.2.Suçun unsurları

Suçun unsurları kapsamında maddi ve manevi unsura ilişkin incelemelerin yanı sıra hukuka aykırılık unsuruyla birlikte suçu hukuka uygun hale getiren eylemlerin ne olduğuna dair açıklamalar yapılacaktır.

3.1.2.1.Maddi unsur

3.1.2.1.1.Fail ve mağdur

"Kişisel verilerin kaydedilmesi suçu"nun faili herhangi bir kimse olabilir. Kanunda faillik açısından bir özellik aranmamıştır. İlgili suçun faili sadece gerçek kişiler olabilir.

Failin tüzel kişi olması mümkün değildir.[280] Kişisel verinin bir tüzel kişiliğin etkinliği çerçevesinde hukuka aykırı olarak kaydedilmesi halinde, suçun faili tipik hareketi bizzat gerçekleştiren gerçek kişi olabilecektir. [281] Bununla birlikte kişisel verilerin kaydedilmesi suçu yararına işlenen tüzel kişilerle ilgili TCK'nın 60. maddesi hükmünce güvenlik tedbirleri uygulanabilecektir.[282]

---

[278] Mustafa Albayrak, "Kişisel Verilerin Kaydedilmesi Suçu", **HUKAB Dergisi**, S. 5, Nisan- Haziran 2013, s. 12.

[279] Hafızoğulları/Özen, age, s. 290, Bazı yazarlar madde ile korunan değerin, özel hayatın gizliliği ve korunması hakkına yönelik hukuka aykırı müdahalelerin önlenmesi olarak tanımlamışlardır. Ali Parlar, Muzaffer Hatipoğlu, **Açıklamalı – Yeni İçtihatlarla 5237 Sayılı Türk Ceza Kanunu Yorumu**, 2. Cilt, 3. Baskı, Ankara, 2010, s. 2087.

[280] TCK m.20/2: "Tüzel kişiler hakkında ceza yaptırımı uygulanamaz. Ancak, suç dolayısıyla kanunda öngörülen güvenlik tedbiri niteliğindeki yaptırımlar saklıdır."

[281] Kangal, age, s. 61.

[282] "1) Bir kamu kurumunun verdiği izne dayalı olarak faaliyette bulunan özel hukuk tüzel kişisinin organ veya temsilcilerinin iştirakiyle ve bu iznin verdiği yetkinin kötüye kullanılması suretiyle tüzel kişi yararına işlenen kasıtlı suçlardan mahkûmiyet halinde, iznin iptaline karar verilir.
(2) Müsadere hükümleri, yararına işlenen suçlarda özel hukuk tüzel kişileri hakkında da uygulanır.
(3) Yukarıdaki fıkralar hükümlerinin uygulanmasının işlenen fiile nazaran daha ağır sonuçlar ortaya çıkarabileceği durumlarda, hâkim bu tedbirlere hükmetmeyebilir.
(4) Bu madde hükümleri kanunun ayrıca belirttiği hallerde uygulanır."

Suçun failinin "kamu görevlisi veya belli bir meslek ve sanat sahibi kişiler olması", diğer koşulların da mevcudiyeti halinde, nitelikli hal sayılmıştır. Dolayısıyla suçun nitelikli halinin belirli bir sıfata haiz kişiler tarafından işlenebileceğinden görünüşte özgü suçtur.[283]

Suçun mağduru da herhangi bir kimse olabilir. Suçun konusunu oluşturan ve kaydedilen kişisel verinin ilişkili olduğu gerçek kişi veya kişiler bu suçun mağdurudur. Tüzel kişilere ait veriler bu suçun konusunu oluşturamayacağı için, suçun mağduru olmaları mümkün değildir. Zira Yargıtay da ilgili bir kararında[284] tüzel kişilerin mağdur olamayacağından kanaatle davaya katılamayacağına hüküm vermiştir. Fakat suçun oluşması sebebiyle tüzel kişinin suçtan zarar gören olarak nitelendirilmesine bir engel bulunmamaktadır.

Suçun mağdurunun mutlaka kişisel verinin maliki veya zilyedi olması zorunlu değildir, önemli olan kaydedilen kişisel verinin bireyle ilgili olmasıdır. Esasen verilerin maliki her zaman ilgili olduğu bireydir. Bu noktada belirtilmek istenen verilerin tutulduğu, saklandığı veya kaydedildiği fiziksel veya otomatik alanın mutlaka ilgili kişiye ait olmaması gerektiğidir. Kişisel verilerin ilişkin olduğu her gerçek kişi suçun mağduru olabilir.[285]

Mağdurun belirli veya belirlenebilir bir kişi olması gerekir. Verinin kişiyle bağlantısı kesilmişken (anonim hale getirilmesi gibi) yapılan kaydedilme işleminde suç oluşmayacaktır.[286]

---

[283] Sert, age, s. 106-109.
[284] 12. CD., E: 2019/12443, K: 2019/11106, T: 27.11.2019.
[285] Dülger, age, s. 690-691. Tüzel kişilerin bu suçun mağduru olabileceğine dair görüş için bkz. Sacit Yılmaz, **Türk Ceza Hukuku Sisteminde Siber Suçlar**, Ankara, 2016, s. 257.
[286] Aydın, age, s. 139.

3.1.2.1.2.Suçun konusu

Bu suçun konusunu "kişisel veri" oluşturur.[287] Anayasa Mahkemesi[288] ve Yargıtay[289] kararlarında da suçun oluştuğuna kanaat getirdiği kişisel verinin ne olduğu açıklanmıştır. Bu bağlamda kişilerin kesin olarak belirlenmesini sağlayan adı, soyadı TC kimlik numarası, doğum tarihi ve doğum yeri gibi bilgiler yanında, kişinin fiziki, ailevi, ekonomik ve sosyal özelliklerine ilişkin bilgiler de kişisel veri olarak kabul edilmelidir. KVKK gerekçesinde, bir kişinin belirli veya belirlenebilir olması, "mevcut verilerin herhangi bir şekilde bir gerçek kişiyle ilişkilendirilmesi suretiyle, o kişinin tanımlanabilir hale getirilmesi" olarak tanımlanmıştır.[290] Kişisel verilere örnek olarak kişilerin adı, soyadı, adresi, resmi, telefon numarası, parmak izi, genetik bilgileri vb. verilebilir. Kişilerin yaptığı iş gereği müşterileriyle veya iş arkadaşlarıyla ilgili öğrendiği ve kaydettiği her türlü bilgiler de kişisel veri kapsamındadır.[291]

---

[287] Kişisel verinin tanımı ve unsurlarına çalışmamızın ilk bölümünde yer verdiğimiz için tekrara düşmemek adına bu kısımda tekrar yer verilmeyecektir.

[288] "Adı, soyadı, Tc kimlik numarası, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil, telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler, IP adresi, e-posta adresi, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler kişisel veri kapsamındadır." AYM, E: 2014/196, K: 2015/103, T: 12.11.2015

[289] "a- Yasam şekline ilişkin kişisel veriler: Kişilerin üçüncü kişiler tarafından ayırımcılığa uğramaması ve haysiyetinin korunmasıyla ilişkili olarak, dini inançları, cinsel tercihleri, etnik kökeni, suç geçmişi, politik eğilimleri ve kişisel özel aktivitelere ilişkin bilgiler bu bağlamda sayılabilecektir. b- Ekonomik ve finansal kişisel veriler: Suçlular tarafından suistimale ve kimlik hırsızlığına hedef olmamak için kişinin mali varlığı, sahip olduğu hisse ve hesaplar, borçları, yaptığı alış verişler, kredi kartlarına ilişkin veriler. Ayrıca sayılan bu bilgiler ile kişinin nerede ve kimlerle bulunduğuna, sağlık bilgilerine ilişkin bilgiler de ortaya çıkarabileceğinden ve varlık bilgisinin toplumsal açıdan da özel sayılmasından dolayı önemi artmaktadır. c- Bilişim alanına ilişkin kişisel veriler: e-postaların bizzat adresleri veya şifreleri, internet ortamında paylaşılan kişisel veriler mahrem olarak değerlendirilebilir. Bunun önemi şu bakımdan artmaktadır. İnternette gezinti yapan kişi birçok kişisel bilgileri paylaşmakta, bu bilgiler kayıt altına alınmakta, yine internet erişimine ilişkin iz kayıtlarının hizmet sağlayıcı ve sunucu sahipleri tarafından tutulabiliyor olması nedenleriyle artmaktadır. d- Sağlıkla ilgili kişisel veriler: Sağlık verileri kişilerin iş güvenliğini, toplum içindeki statüsünü ve sigorta kapsamını etkileyen hassas bilgilerdir. Ayrıca sağlık verileri kişilerin sosyal yaşantısı ve psikolojik durumları hakkında bilgi edinilmesine neden olabilir. Biyometrik (Kişinin kendine özgü fiziksel veya biyolojik niteliklerine dayalı olarak insanların kimliğini tespit için dijital teknolojiden faydalanma bilimi) veriler de kişisel veriler arasındadır. e- Politik kişisel veriler: Toplum içinde yasayan kişilerin siyasi tercihleri toplum katmanları arasında bilinme halinde ayırımcılığa maruz kalma ihtimali bulunduğundan bu bilgilerde kişisel veridir." Yargıtay CGK, E: 2012/12-1510, K: 2014/331, T: 17.06.2014

[290] Gerekçeye göre, "kişinin belirli veya belirlenebilir olması kavramında, orantılılık prensibine dikkat edilmelidir. Burada bir kişinin tespiti için orantısal olarak çok fazla zaman ve çaba gerekiyorsa bu durumda bu kişi belirlenebilir farz edilmemelidir. Bir kişinin kimliğinin belirlenebilir olup olmadığının tespitinde, başkaları tarafından kullanılabilecek makul yöntemler hesaba katılmalıdır."

[291] Bu kapsamda Yargıtay 11. CD 11.07.2006 tarih ve 5430/6541 Esas ve Karar sayılı kararında, şirkette satış müdürü olarak görev yapan sanığın, çalıştığı şirketin müşterilerine ait tüm verileri kendi şirketinde

Kişisel veriler çoğu zaman "sır" kavramı içinde değerlendirilebilmektedir. Sır, "*herkes tarafından bilinmeyen, sahibinin açıklanmamasını istediği ya da belirli kişilere açıkladığı ve açıklanmamasında menfaatinin bulunduğu gerçek nitelikteki her türlü gizli bilgidir*".[292] Ancak bilginin, kişisel veri olabilmesi için mutlaka sır niteliğine de sahip olması gerekmemektedir. Bununla birlikte, herkes tarafından bilinen veya bilinebilir veya erişilebilir olan bilgiler alenileşmiş olduğundan artık kişisel verilerin kaydedilmesi suçunun konusunu da oluşturmayacaktır.[293] Ayrıca önceden de bahsettiğimiz gibi kişinin kendisi tarafından KVKK m.5'e göre alenileştirdiği kişisel verisinin işlenmesi durumunda da bu suçun konusu oluşmayacaktır. Veri ile kişi arasındaki doğrudan veya dolaylı olarak bağlantının kurulması arandığından anonim veriler 135. maddede yer alan "kişisel verilerin hukuka aykırı olarak kaydedilmesi suçu"nun konusunu oluşturmayacaktır. TCK'nın 135. maddesinin gerekçesinde verilerin "*sanal ortamda ya da somut kâğıt üzerinde kayda alınması açısından fark gözetilmediği*" yer almaktadır. Buna göre yalnızca bilişim sistemlerinde yer alan kişisel veriler değil, örneğin kâğıda yazılmış, dosyalanmış kişisel veriler dahi bu suçun kapsamındadır.[294]

3.1.2.1.3.Fiil

"Kişisel verilerin kaydedilmesi suçu"nun hareket unsuru "kaydetmek" fiilinden oluşmaktadır. Kaydetmek TDK'da "*Yazmak, bazı önemli noktaları tespit etmek; herhangi bir şeyi bir yere mal etmek, bir şeyin tarih, numara veya adını bir deftere geçirmek; hatırlamak için yazmak, not etmek; belirtmek, söylemek; sesi veya resmi manyetik bant üzerine geçirmek; elektronik veya sayısal araçlarda bilgiyi korumaya almak*." ifadeleri ile tanımlanmıştır.[295] Kişisel verinin kaydedilmesinin tanımı TCK ve KVKK'da yapılmamıştır. Buna karşılık kişisel verinin işlenmesi kavramı, kaydedilmeyi de kapsayan geniş bir işlemdir. Kişisel verilerin işlenmesi "*Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi,*

kullanmak üzere aktarmasını TCK 136. maddenin ihlali olarak tanımlamış ve bu verilerin kişisel veri olduğunu belirtmiştir. Aktaran Gültekin, age, s.130.

[292] Kangal, age, s. 63.

[293] Aydın, age, s. 588.

[294] Kuşkonmaz, age, s. 137.

[295] Titrek, agt, s. 71.

açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem" olarak ifade edilmiştir. Dolayısıyla bir kişisel verinin kaydedilmesi işlemi için verinin, "*tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla*" kaydedilmelidir.

Fakat TCK'nın 135. maddesinin kapsamı bu kadar dar yorumlanmamalıdır. Kaydetmenin yapıldığı yerin, bir veri kayıt sisteminin parçası olmak zorunda olduğuna ilişkin herhangi bir düzenleme yoktur.[296] Dolayısıyla kaydetme fiili "kişisel verilerin herhangi bir yöntemle, daha sonra kullanılmak amacıyla hazır edilmesi, depolanması" olarak tanımlanabilir. Kaydetme, bir kâğıt parçasına yazarak olabileceği gibi bilgisayar ortamına kaydederek de gerçekleştirilebilir[297] Öğretide bir verinin ezberlenmesi veya kâğıda yazılmasını kaydetmek fiilinin bir parçası kabul edilmemesi gerektiğini savunan bir görüş mevcuttur.[298] Fakat kâğıda yazılan bir bilgi sonradan kullanılabileceğinden kaydetme fiilini oluşturması mümkündür. Ayrıca 135. maddenin gerekçesinde de "kişisel verilerin bilgisayar ortamında veya kâğıt üzerinde kayda alınması arasında bir ayrım" gözetilmemiştir.[299]

"Kişisel verilerin kaydedilmesi suçu" serbest hareketli suç tipidir. Dolayısıyla kaydedilme işleminin nasıl yapıldığına bakılmaksızın suç gerçekleşecektir.

3.1.2.2.Manevi unsur

Kanun koyucunun suçun işlenmesine yönelik özel kast aramaması, suç unsuru haline gelecek bir saik belirtmemesi nedeniyle, suçun genel kastla işlenebileceği söylenebilir. Kast, suçun unsurlarının bilerek ve istenerek gerçekleştirilmesidir. Kastın söz konusu olabilmesi için suçun tanımındaki bütün unsurların fail tarafından bilinmesi ve istenmesi gerekmektedir.[300] Bu suç açısından da failin, kişisel verileri

---

[296] Kangal, age, s. 65.
[297] Handan Yokuş Sevük, **Türk Ceza Hukuku Özel Hükümler**, 3. Baskı, Adalet Yayınevi, Ankara, 2020, s. 246.
[298] Özbek/Doğan/Bacaksız, age, s. 587.
[299] Ankara HBV Üniversitesi Türk Ceza Hukuku Uygulama ve Araştırma Merkezi, **Türk Ceza Hukuku Mevzuatı – Cilt 1 (Kanunlar)**, 23. Baskı, Seçkin Yayıncılık, Ankara: 2019, s. 340.
[300] "Örneğin aldığı eşyanın başkasına ait olduğunu bilmeyen failde hırsızlık (TCK m.141) kastı bulunmamaktadır." Kişisel verilerin kaydedilmesi suçunun kastla işlenmesi gerektiği hakkındaki bir Yargıtay Kararı için bkz. "Hukuka aykırı olarak kişisel verileri kaydetmek suçundan, sanığın beraatine ilişkin hüküm mahallin Cumhuriyet savcısı tarafından temyiz edilmekle, dosya incelenerek gereği

bilme ve isteme unsurlarıyla kaydetmesi durumunda suç oluşacaktır.[301] Ayrıca, kanunda suçun taksirle işlenebileceğine dair özel bir düzenleme bulunmamaktadır.[302] TCK'nın 22. maddesi[303] gereği, bir suçun taksirle işlenebilmesi için, kanunda açık bir düzenleme bulunması gerekmektedir. Dolayısıyla fail, kişisel verileri taksirli hareketiyle kaydederse suç oluşmayacağından sorumluk doğmayacaktır.

Genel kastla işlenebilen bir suç, kural olarak olası kastla da işlenebilir. Öğretide bazı yazarlar kişisel verilerin kaydedilmesi suçunun olası kastla da işlenebileceğini savunmaktadırlar.[304] Olası kastta ise, failde kastın bilme unsuru bulunmasına rağmen, sonucu isteme net bir şekilde bulunmamakta, daha çok sonucu umursamama, kabullenme hali bulunmaktadır.[305]

Suçun düzenlemesi açısından, ilk fıkrada ve ikinci fıkrada belirli veriler açısından "hukuka aykırı" [306] olarak kişisel verileri kaydetmeden bahsedilmektedir. Dolayısıyla kanun bu suç açısından özel bir hukuka aykırılık bilinci aramaktadır. Her ne kadar bu husus hukuka aykırılık başlığı altında incelenecek olsa da, 1. fıkradaki kişisel verileri "hukuka aykırı olarak" kaydetme açısından ve 2. fıkradaki "hukuka aykırı olarak" "*kişilerin ahlakî eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veriler*" açısından, bu suç ancak doğrudan kastla işlenebilecek; olası kastla işlenmesi söz konusu olamayacaktır. Ancak

düşünüldü: Olay günü Ören belediyesindeki işlerini halletmek için belediyeye giden sanığın, belediye başkanının belediyede bulunmaması nedeniyle Anamur'a dönmesi üzerine Ören Belediye Başkanına ait makam aracının mesai saatleri içinde bir kahvehanenin önünde park halinde olduğunu ve beyanına göre başkanın da kahvede oyum oynadığını görmesi üzerine, kahvehanenin önünde park etmiş halde bulunan Ören belediyesine ait aracın fotoğraflarını çekmek isterken belediyede çalıştığını ve başkanla gezdiğini beyan eden katılanın gelerek sanığı engellemeye çalışarak sanığın kolundan çekmesi üzerine, sanığın da kendisini engelleyen ve muhtemel şikâyet hakkını kullanmasına engel olan bu şahsın kim olduğunu öğrenmek amacıyla katılanın fotoğrafını çekmesi şeklinde gelişen olayla ilgili yapılan yargılama sonunda yüklenen suç açısından failin kastının bulunmadığı gerekçeleri gösterilerek mahkemece kabul ve takdir kılınmış olduğundan, mahalli Cumhuriyet savcısının yerinde görülmeyen temyiz itirazlarının reddiyle, sanığın beraatine ilişkin hükmün tebliğnamedeki isteme uygun olarak ONANMASINA." Yargıtay 12.CD, E: 2012/20111, K:2012/12850, T: 23.05.2012

[301] Hakan Hakeri, **Ceza Hukuku Genel Hükümler**, 24. Baskı, Adalet Yayınevi, Ankara, 2021, s. 190.

[302] Mahmut Koca, İlhan Üzülmez, **Türk Ceza Hukuku Özel Hükümler**, 7. Baskı, Adalet Yayınevi, Ankara, 2020, s. 562.

[303] TCK 22. madde: "(1) Taksirle işlenen fiiller, Kanun'un açıkça belirttiği hallerde cezalandırılır."

[304] Özbek/Doğan/Bacaksız, age, s. 579.

[305] Hakeri, age, s. 191.

[306]"Hukuka aykırılık, kanundaki tanıma uygun olarak işlenen fiilin hukuk düzeninde iyi karşılanmaması, yalnız ceza hukukunda değil, bütün hukuk düzeniyle çelişki ve çatışma içinde olması demektir." Mehmet Emin Artuk, Ahmet Gökcen, **Ceza Hukuku Özel Hükümler**, 19. Baskı, Adalet Yayınevi, Ankara, 2021, s. 53.

2. fıkranın ilk kısmında yer alan "*Kişilerin siyasî, felsefî veya dinî görüşlerine, ırkî kökenleri*" hakkındaki kişisel veriler açısından "hukuka aykırı olarak" kaydetme özel olarak aranmadığından, bu verileri kaydetme açısından suçu doğrudan kastla işlemek mümkün olacağı gibi olası kastla işlemek de mümkün olabilecektir.[307]

3.1.2.3.Hukuka aykırılık unsuru

Bu suçun oluşabilmesi için hukuka aykırı olarak bir kaydetme işlemi söz konusu olmalıdır. Suç maddesinde hukuka aykırılığın açıkça belirtildiği görülmektedir. Kişisel verinin kaydedilmesi esnasında, hukuka aykırılığı ortadan kaldıracak bir hukuka uygunluk sebebi bulunmaması halinde suç gerçekleşmiş olacaktır.[308]

Hukuka aykırılık unsuru, birinci ve ikinci fıkradaki çeşitli veri kategorileri yönünden farklı şekilde düzenlenmiştir. Maddenin birinci fıkrasında genel anlamda kişisel verilerin kaydedilmesi, ikinci fıkrada ise "ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına ya da sendikal bağlantılarına" ilişkin verilerin kaydedilmesinde özel aykırılık aranmıştır.[309] Bunun aksine maddenin ikinci fıkrasının ilk bölümünde ise "kişilerin siyasi, felsefi ya da dinî görüşleri ile ırki kökenlerine" ait bir verinin kaydedilmesi açısından özel hukuka aykırılık hali aranmamıştır.

Öğretide "hukuka aykırı olarak" ifadesinin bir suç metninde açıkça yer alması durumunda nasıl yorumlanması gerektiğine yönelik farklı iki görüşe değinmek gerekmektedir. İlk görüş, kanun maddesinde hukuka aykırılık ibaresinin bulunması durumunda, "hukuka aykırılığın tipikliğe ait bir unsur" hâline geldiği görüşüdür. İlgili görüşe göre, eğer suç tipinde, "hukuka aykırı olarak" ifadesi bulunuyorsa, hukuka aykırılık, tipikliğe ait bir unsur özelliği kazanır.[310] İkinci görüş, bu ve benzer kavramların suç tipinde kullanılmasının nedeninin, hukuka uygunluk sebebinin yokluğuna işaret etmek üzere gereksiz yazıldığı, özel bir anlamı olmadığı, hâkime uyarı anlamı içerdiği yönündedir. Bu görüşe göre, suç tipinde bu tarz ifadelerin kullanılması, kanun koyucunun hâkimlere, olayda hukuka uygunluk nedenlerinin

[307] Gültekin, agm, s. 137.
[308] Koca/Üzülmez, age, s. 562-563.
[309] Sert, age, s. 113.
[310] Artuk/Gökcen, age, s. 330, Özbek/Doğan/Bacaksız, age, 582. "Konuyla ilgili olarak işlenen eylemin ceza kanundaki suç tipine uygunluğu söz konusu olsa bile, suçun oluşması için hâkimin özel olarak hukuka aykırılık araması gerektiğini ifade etmişlerdir."

bulunup bulunmadığı üzerinde hassasiyetle durmaları için uyarı mahiyetindedir. Suçun unsurlarına dâhil olmayıp gereksiz yere kullanılmıştır.[311] Yargıtay'ın da bir kararında "*sanığın hukuka aykırılık bilinciyle hareket etmemesi durumunda suçun oluşmayacağı*" gerekçesiyle ilk görüşe uygun hüküm verdiğini belirtmemiz gerekir.[312]

TCK'nın 135. maddesinde, "kişilerin siyasi, felsefi, dini görüşleri ile ırki kökenlerine ilişkin" verilerinin kaydedilmesi yönünden özel hukuka aykırılık aranmamıştır.[313] Dolayısıyla fail buna ilişkin bir veriyi kaydettiğinde eğer herhangi bir hukuka uygunluk sebebi yoksa suç tamamlanmış olacaktır.

3.1.2.3.1.Hukuka uygunluk nedenleri

Bir fiilin suç olması için, tipe uygun olması yetmez. Fiilin aynı zamanda hukuka da aykırı olması gerekir. Bir fiil, bir ceza normu ile belirtilen emir veya yasağa aykırı olduğunda hukuka da aykırı olacaktır. Bu açıdan hukuka aykırılık, tipe uygun olarak gerçekleştirilen fiilin, hukuk düzenince caiz sayılmaması ve bu fiilin hukuk düzeni ile çelişki ve çatışma halinde bulunmasıdır.[314]

Hukuka uygunluk nedenleri, TCK'da "kanun hükmünü yerine getirme", "meşru müdafaa", "hakkın kullanılması", "ilgilinin rızası" olarak düzenlenmiştir. Kişisel verilerin korunmasına yönelik olarak düzenlenen suçlar bakımından incelenmesi gereken hukuka uygunluk nedenleri ise "kanun hükmünün yerine getirilmesi (TCK m. 24)", "hakkın kullanılması (TCK m. 26/1)" ve "ilgilinin rızası (TCK m. 26/2)"dır. TCK ve KVKK'da düzenlenmiş hukuka uygunluk sebepleri çalışmamızın bu bölümünde incelenecektir.

3.1.2.3.1.1.Kanun hükmünün ifası (TCK m. 24)

TCK'nın 24/1. maddesinde; "Kanun hükmünü yerine getiren kimseye ceza verilmez." hükmü geçmektedir. KVKK "kişisel verilerin işlenme şartları" başlıklı m.

---

[311] Dülger, age, s.704-705.

[312] "Sanık, katılanla yaptığı konuşma içeriğini kaydedip bu kaydı içeren CD'yi, görülmekte olan dava dosyasına delil olarak vermiştir. Kaydı üçüncü kişi ya da kişilerle paylaştığı ve/veya çoğaltarak dağıttığına ilişkin hakkında bir iddia ileri sürülmeyen sanık, eylemiyle resmi belgede sahtecilik iddiasını ispatlama amacını taşımaktadır. Hukuka aykırı hareket ettiği bilinciyle hareket etmediğinden, kişisel verilerin kaydedilmesi suçunun unsurları oluşmamıştır." Yargıtay 12.CD., E: 2014/17630, K: 2015/1672, T: 02.02.2015.

[313] Ketizmen, age, s. 235.

[314] Meral Ekici Şahin, **Ceza Hukukunda Rıza**, 1. Baskı, On İki Levha Yayıncılık, İstanbul, 2012, s. 96.

5/2-a bendine göre ise, kanunların açık olarak öngörmesi halinde, ilgilinin açık rızasına dayanılmaksızın işlenebileceği belirtilmiştir. Kanun "özel nitelikli kişisel verilerin işlenme şartları" başlıklı 6. maddesi üçüncü fıkrasına göre ise maddede sayılan "sağlık ve cinsel hayat dışındaki özel nitelikli veriler", kanunların öngördüğü durumlarda, ilgilinin açık rızası olmaksızın işlenebilecektir. Buna göre kişinin kişisel veriyi, kanun, tüzük, yönetmelik gibi bir düzenlemeden kaynaklanan yetkiye dayanarak kaydetmesi ve bu yetkinin sınırlarını içerisinde olması durumunda fiil hukuka uygun hale geleceğinden suç oluşmayacaktır.[315]

Örnek olarak çalışmamızın ikinci bölümünde detaylı olarak incelediğimiz PVSK'nın 5. maddesini gösterebiliriz. Hüküm gereğince polis tarafından alınan parmak izi ve fotoğrafların, bu amaca özgü sisteme kaydedilerek saklanması durumunda kişisel verilerin kaydedilmesi suçu oluşmayacaktır. Yalnız bu kaydetme işleminin suç sayılmaması için, kanunlar tarafından kaydeden makama verilmiş açık bir yetki bulunmalıdır.[316]

3.1.2.3.1.2.Bir hakkın kullanımı ve ilgilinin rızası (TCK m.26)

TCK'nın 26/1 maddesinde; "Hakkını kullanan kimseye ceza verilmez." hükmünden bahsetmektedir. Öncelikle kişiye hukuk düzenince tanınmış, kişi tarafından doğrudan kullanılabilen objektif bir hakkın bulunması gerekmektedir. Ayrıca kişi bu hakkını kullanırken ölçülü olmalı ve hakkın amacına uygun hareket etmiş olmalıdır. Örneğin birçok işletmede güvenlik nedeniyle yerleştirilmiş kamera sistemleri güvenlik için gerekli olan alandan çok daha geniş bir alanı kaydediyorsa bu durum, kişilerin özel hayatlarına haksız bir müdahale sayılacaktır. Burada hakkın kullanılmasından söz edilemez.[317]

Buna göre, kişisel verileri kaydederken bir hakkını kullanan kimsenin fiili, kişisel verilerin kaydedilmesi suçunu oluşturmayacaktır. Örneğin hekim veya avukatın mesleğin icrası kapsamında kayda aldığı veriler, mesleğin icrası bir hak teşkil ettiğinden suç oluşturmayacaktır.[318]

---

[315] Sert, age, s. 115.
[316] Yaşar/Gökcan/Artuç, age, s. 4436-4438.
[317] Aydın, age, s. 148.
[318] Ersan Şen, **Yeni Türk Ceza Kanunu Yorumu**, Cilt: I, Vedat Kitapçılık, İstanbul 2006, s. 602.

Rıza kişinin hukuken tanınan kendi geleceğini belirleme hakkına dayanarak, hukuksal değerine ilişkin hukuki korumadan somut olayda vazgeçmesi olduğuna göre, rıza menfaatlerin değerlendirilmesinde bir tür araçtır.[319] Hukuk düzeni kişiye kendisine ait hukuksal değerler üzerinde tasarruf etme yetkisi tanıdığına göre, bu tasarruf yetkisini kullanarak ve bu yetkinin sınırlarını aşmadan, hukuksal değerine ilişkin hukuki korumadan vazgeçmesi de hukuka aykırı olmayacaktır. Kişinin kendi geleceğini belirleme hakkını ve kendi hukuksal değerleri üzerindeki tasarruf yetkisini tanımıştır. Kişi yalnızca üzerinde mutlak surette tasarruf edebileceği hukuksal değerlere ilişkin hukuki korumadan vazgeçebilir.[320] Kişisel veriler, kişinin üzerinde mutlak surette tasarruf edebileceği haklarındandır.[321]

TCK'nın 135. maddesi gerekçesinde de "kişisel verilerin kaydedilmesi suçu"nun oluşabilmesi için, kişisel verilerin hukuka aykırı olarak kayda alınması gerektiği; kişinin rızasıyla kendisine ilişkin bilgilerin kayda alınmasının suç oluşturmayacağı belirtilmiştir.[322] Aynı şekilde KVKK'nın 5/1 maddesinde kişisel verilerin "*ilgili kişinin açık rızası olmaksızın*" işlenemeyeceği belirtilmiş, KVKK'nın 6/2 maddesinde ise "*özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın*" işlenmesinin yasak olduğu ifade edilmiştir. Benzer şekilde TCK'nın 135. maddesinin gerekçesinde de "kişinin rızası ile kendisiyle ilgili bilgilerin kayda alınmasının suç oluşturmayacağı" ifade edilmiştir. Bu durumda kişinin rızasının bu suç için hukuka uygunluk nedeni oluşturacağı açıktır. Ancak rızanın "açık rıza" olması önem

---

[319] Ekici Şahin, age, s. 100.
[320] Ekici Şahin, age, s. 48.
[321] "Sanık ... ile hakkındaki hükmün açıklanması geri bırakılan sanık ...'e ait ortak işyerinde, üçüncü kişilere ait çok sayıda nüfus cüzdanı fotokopisinin hukuka aykırı olarak saklandığı iddiasıyla ilgili olarak mahkemece kişisel verilerin hukuka aykırı olarak kaydedilmesi suçundan sanık ... hakkında mahkumiyet hükmü kurulmuş ise de; TCK'nın 135. maddesinde düzenlenen Kişisel Verilerin Kaydedilmesi suçunun konusunu oluşturan kişisel veri kavramından, kişinin, 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, kişinin kimliğini belirleyen veya belirlenebilir kılan, kişiyi toplumda yer alan diğer bireylerden ayıran ve onun niteliklerini ortaya koymaya elverişli, gerçek kişiye ait her türlü bilginin anlaşılması gerektiği, belirli veya belirlenebilir bir kişiye ait her türlü bilginin, hukuka aykırı olarak kaydedilmesi gerektiği gözetildiğinde; üçüncü kişilere ait nüfus cüzdanı fotokopilerinin, bu kişilerin rızaları dışında hukuka aykırı olarak ele geçirilip sanığın işyerinde bulundurulduğuna dair bir iddia bulunmadığı gibi, nüfus cüzdanı sahiplerinin ifadelerinde kendi rızaları ile birtakım hukuki işlemler nedeniyle nüfus cüzdanlarını verdiklerini beyan etmeleri karşısında sanık ...'in, unsurları oluşmayan hukuka aykırı olarak kişisel verileri kaydetmek suçundan beraati yerine mahkumiyetine karar verilmesi…" 5. CD., E. 2014/10479, K. 2018/4622, T. 21.06.2018.
[322] Sert, age, s. 119.

taşımaktadır. Açık rızanın "belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza" şeklinde tanımlandığını ve şartlarına ilişkin detaylı açıklamaya önceki bölümlerde yer verdiğimizden bu bölümde açık rızaya ilişkin kısa açıklamalarla yetinilecektir.

Veri sahibinin açık rızasının olduğunu kabul edebilmek için "rızanın belirli bir konuya ilişkin verilmesi", "rızanın bilgilendirmeye dayalı olması" ve "rızanın özgür iradeyle açıklanmış olması" gereklidir. Sayılan üç şartın dışında, rızanın yazılı şekilde alınması zorunlu değildir. Elektronik ortam ve çağrı merkezi gibi yöntemlerle de açık rızanın alınması mümkün olacaktır. Açık rıza alındığına dair ispat yükü veri sorumlusuna aittir.[323]

Rızanın geçerliliği, kural olarak şekil şartına bağlı değildir. Dolayısıyla karşı tarafta bir şüpheye mahal vermediği sürece, rızanın herhangi bir şekilde açıklanması mümkündür.[324] Her ne kadar KVKK'da açık rızadan bahsedilse de zımni rızanın da suç açısından hukuka uygunluk nedeni olarak kabul edilmesi isabetli olacaktır. Örneğin kişinin tanıdığı arkadaşından, tanıdığı başka bir arkadaşının telefon numarasını alması durumunda dahi numarayı alan ve numarayı veren verileri işlemiş olur. Numarayı alan veriyi ilk defa kaydeden olmadığı için kişisel verilerin kaydedilmesi suçundan sorunlu olmasa da; numarayı veren, "kişisel verileri hukuka aykırı olarak verme" suçunu işlemiş olur. Zımni rızanın kabul edilmesi gündelik hayatta sıkça karşılaşılan durumların suç teşkil etmesini ve bu suçların şikâyete bağlı olmaması nedeniyle soruşturma makamlarının bu tarz fiillerle ilgili soruşturma başlatması gibi pratikte imkânsız durumların ortaya çıkmasını engeller.[325]

İlgili kişinin verilerinin kaydedilmesine rıza göstermesi, verileri kaydeden kişinin bu verileri istediği gibi kullanabileceği ya da ifşa edebileceği anlamına da gelmez.[326]

---

[323] Titrek, agt, s. 79.
[324] Artuk/Gökcen, age, s. 480.
[325] Koca/Üzülmez, age, s. 577.
[326] "Mağdurun, herkes tarafından bilinmeyen veya kolaylıkla ulaşılması ve bilinmesi mümkün olmayan, ancak sınırlı bir çevre ile paylaştığı kişisel verilerini, kimliğini ortaya koyacak biçimde, … isimli internet sitesine, onun bilgisi ve rızası dışında, hukuka aykırı olarak kaydeden sanığın sübut bulan eyleminden dolayı TCK'nın 135/1. maddesindeki kişisel verilerin kaydedilmesi suçundan mahkumiyetine karar verilmesi gerekirken, kişisel verilerin hukuka aykırı olarak ele geçirilmediğinden bahisle ve salt TCK'nın 136/1. maddesi kapsamında değerlendirme yapılarak, dosya kapsamına uygun

3.1.2.3.1.3.KVKK'da öngörülen hukuka uygunluk nedenleri

KVKK'nın "kişisel verilerin işlenme şartlarını düzenleyen" 5/2-b bendine göre; "fiili imkânsızlık sebebiyle rızasını açıklayamayacak durumda bulunan ya da rızasına hukuki geçerlilik tanınmayan kişinin, kendisinin veya bir başkasının hayatı ya da beden bütünlüğünün korunması için zorunlu olması hâlinde", ilgilinin açık rızasının olup olmadığına bakılmaksızın kişisel verisi işlenebilir. Bu durumda kaydetme fiili, hukuka uygunluk sebebinin varlığı nedeniyle suç teşkil etmez. KVKK'nın gerekçesinde bu duruma örnek olarak, şuurunu kaybetmemiş ya da akıl hastalığı nedeniyle rıza beyanının geçerliliği olmayan kişinin verisinin hayatı söz konusu olduğunda müdahale sebebiyle işlenebileceği belirtilmiştir. Örneğin, yaralanan ve yanında kimsesi olmayan kişiye doktorun müdahale etmesi hâlinde üstün nitelikte özel yarar vardır.[327] Bu hâlde hastaya müdahale etmek için kişisel verilerin kaydedilmesinde hukuka aykırılık bulunmamaktadır.

KVKK'nın "kişisel verilerin işlenme şartlarını düzenleyen" 5/2-b bendine göre sözleşmenin ifası için gerekli olması halinde, kişinin açık rıza yokluğunda dahi kişisel veri işlenebilir. Düzenleme doğrudan uluslararası düzenlemelere paralel olarak mevzuatımıza eklenmiştir. Yapılan bir sözleşme gereği, o kişiye ait adı, soyadı ya da hesap numarası gibi verilerin işlenmesi[328] veya internetten yapılan bir alışverişin teslimi için adres bilgilerinin işlenmesi örnek olarak gösterilebilir.

KVKK'nın "kişisel verilerin işlenme şartlarını düzenleyen" 5/2-ç bendine göre, ilgilinin kişisel verileri, "Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması" durumunda açık rıza yokluğunda dahi işleme yapılabilir. KVKK'nın gerekçesinde bu durumla ilgili olarak çalışanın maaşının ödenmesi için banka bilgisi, medeni durumu, bakımıyla yükümlü olduğu kişiler, varsa eşin çalışma durumu gibi verilerini işlemesi, bu bendin verdiği yetki gereği hukuka uygun olacaktır.

KVKK'nın "kişisel verilerin işlenme şartlarını düzenleyen" 5/2-d bendinde, ilgilinin kişisel verileri, "İlgili kişinin kendisi tarafından alenileştirilmiş olması"

---

düşmeyen yetersiz gerekçelerle, sanık hakkında beraat hükmü kurulması kanuna aykırıdır." Yargıtay 12. CD., E: 2013/2773, K: 2013/26643, T: 25.11.2013

[327] Sert, age, s. 122.

[328] Korkmaz, age, s. 358.

durumunda, açık rızası aranmaksızın işlenebilir. Alenileştirme, kamuya açık hâle getirme anlamına gelir.

KVKK'nın gerekçesinde göre, ilgilisinin kendi rızasıyla kamuoyuyla paylaştığı kişisel verinin işlenebileceği belirtilmiştir. Burada ilgilinin alenileştirdiği ve böylece herkesin erişimine açıp bilgi sahibi olabileceği bir kişisel veriye dönüştürdüğünden, ilgili verinin korunmasında hukuki yarar olup olmadığına dair öğretide iki görüş mevcuttur.

Bir görüş kişisel verinin sahibi tarafından alenileştirilmesi halinde artık ilgili kişisel verinin artık başkaları tarafından kaydedilmesi gibi benzer fiilleri en baştan rıza gösterdiği anlamına geldiğini ve bu verilerin artık kişinin özel yaşam alanından çıkarak koruma kapsamı dışında kaldığını ifade etmektedirler.[329] Yargıtay bu hususa ilişkin bir kararında suça konu kişisel verilerin sır niteliğinde olması gerekmediği, herkes tarafından erişilmesi mümkün, aleni hale gelmiş olsa dahi kişisel veri niteliğinin korunmaya devam edeceğini, suçun oluşup oluşmadığına dair her olayda detaylı inceleme yapılması gerekliliğine vurgu yapmıştır.[330] Zira ilk görüşün doğrudan kabulü halinde, kişisel verisini paylaşan kişinin kişisel verisi üzerindeki hakkı herhalde ve her durumda son bulacaktır. Oysa kişisel verilerin korunması kapsamında bireyin kişisel verisi ile ilgili yapılacak olan her türlü işlemden haberdar olma, bu konuda aydınlatılma ve bunlara rıza gösterme veya göstermeme hakkı bulunmaktadır. Bu görüşün kabulü halinde ise bireyin söz konusu hakları elinden alınmış olacaktır.[331]

Yargıtay vermiş olduğu bir kararında açıkça, mağdur sıfatındaki şahsın kendi rızası ile çektirdiği ve kendi rızası ile sosyal medyaya koymuş olduğu kişisel verilerinin daha sonra rızası hilafına yayınlanmaya devam edilmesi üzerine, her ne kadar veriler şahsın kendi rızası ile alenileştirilmiş veriler olsa dahi artık mağdurun rızası dışında bir kullanım söz konusu olduğundan TCK çerçevesinde "kişisel verileri

---

[329] Bkz, Özbek/Doğan/Bacaksız.

[330] "TCK kapsamında düzenlenen 135. 136. Maddelerde kişisel verilere karşı işlenen suçlarla ilgili olarak, bu suçların işlenmesi için suça konu kişisel verilerin sır niteliğinde olması gerekmediğini, bu bakımdan herkes tarafından erişilmesi mümkün, aleni hale gelmiş verilerin de kişisel veri olarak kabul edildiğini ancak bu noktada her türlü kişisel veri bakımından bu suçun oluşmaması için, her olay için ayrıntılı inceleme yapılması gerektiğini, her olayda titizlikle durumun değerlendirilmesi gerektiğini, olayda bir hukuka uygunluk sebebi söz konusu olabilecekse bunların değerlendirilmesi gerektiğini ve sanığın da özel olarak hukuka aykırı hareket ettiğine ilişkin hukuka aykırılık bilincinin olması gerektiğini ifade etmiştir." Yargıtay 12. CD., E: 2017/2960, K: 2018/1541 T: 14.02.2018.

[331] Uyarer, age, s. 168.

hukuka aykırı olarak verme veya ele geçirme suçu"nun oluştuğunu gözetmiş ve ilgili yerel mahkeme kararını bozmuştur.[332]

KVKK'nın "kişisel verilerin işlenme şartlarını düzenleyen" 5/2-e bendine göre, ilgilinin kişisel verileri, *"Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması*" hâlinde, açık rıza yokluğunda dahi veri işleme yapılabilir. Başka bir ifadeyle bu demektir ki kişi eğer bir hukukun kendine tanıdığı bir hakkı kullanıyorsa örneğin dilekçe hakkı gibi bu durumda yine kişinin kişisel verilerinin işlenmesi açık rıza olmaksızın hukuka uygun hale gelecektir.[333]

KVKK'nın "kişisel verilerin işlenme şartlarını düzenleyen" 5/2-f bendi, ilgilinin kişisel verileri, "*İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması*" durumunda, açık rıza olmasa bile işleme yapılabilir. Diğer bir ifadeyle veri sorumlusu; meşru menfaati de olsa, ilgili kişinin; temel hak ve hürriyetlerinin zararına olmamak koşuluyla işleme yapılabilecektir.

KVKK'nın gerekçesinde bu duruma örnek olarak, çalışanların terfi, ikramiye gibi işlemlerinin kontrolünü sağlamak veya düzenlemek için veri sorumlusunun, ilgililerin temek hak ve hürriyetlerine zarar vermeden işleme yapması gösterilmiştir. Ancak burada, verilerin işlenmesinde veri korumayla ilgili temel ilkelere uygun ve veri sorumlusuyla ilgili kişinin menfaat dengesinin gözetilmesine dikkat edilmesi gerekir.

KVKK'nın "özel nitelikli kişisel verilerin işlenme şartlarını" düzenleyen 6/1. Fıkrasına göre, özel nitelikli kişisel veriler sayılmıştır. Maddenin ikinci fıkrasında ise özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesinin yasak olduğu düzenlenmiştir. Maddenin üçüncü fıkrasında ise, "*Sağlık ve cinsel hayata ilişkin kişisel verilerin ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî*

---

[332] "Sanığın, mağdur ile birlikte çektirmiş olduğu fotoğraflarının mağdur tarafından talep edilmesine rağmen kaldırılmaması, fotoğrafların sanık ile mağdur arasındaki ilişkinin varlığını gösteren fotoğraflar olmasına rağmen fotoğrafların sosyal medyada yayınlanmış olması karşısında bu fotoğrafların mağdurun kimsenin görmesini istemeyeceği nitelikteki özel hayatına ilişkin fotoğraflar olarak değerlendirilemeyeceği ve ancak sanığın mağdurun kişisel verilerinden olan fotoğraflarını mağdurun rızası hilafına yayınlamaya devam etmesinin Türk ceza Kanunu'nda düzenlenen ve 136. madde kapsamında yer verilen kişisel verileri hukuka aykırı olarak verme ve yayma suçunu teşkil edeceği gözetilmeden sanık hakkında verilen beraat kararının bozulmasına karar vermiştir." Yargıtay 12. CD., E:2017/150 K: 2017/6231

[333] Uyarer, age, s. 212.

teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir." şeklinde düzenleme bulunmaktadır.[334]

KVKK'nın "İstisnalar" başlıklı 28. maddesinde kişisel verilerin işlenmesinin ve kaydedilmesinin hukuka aykırı olmadığı, kanun kapsamı dışında tutulduğu hâller düzenlenmiştir. KVKK'nın gerekçesine göre 28/1'de tamamen kanun kapsamı dışında tutulan hâller düzenlenmiştir. Maddeye göre[335], belirtilen durumlarda KVKK hükümleri uygulanmayacaktır. Sayılan hallerde "kişisel verilerin kaydedilmesi", kişisel verilerin kaydedilmesi suçunu oluşturmayacaktır.

KVKK 28/2'de[336] ise kısmen KVKK kapsamı dışında tutulan hususlar düzenlenmiştir. Buna göre, kural olarak bu fıkrada sayılan durumlar KVKK hükümlerine tabi olmakla birlikte, yalnızca fıkrada belirtilen kanun maddelerinde düzenlenen hükümler bakımından bazı istisnalar bulunmaktadır. Bu çerçevede ikinci fıkrada, KVKK'nın temel ilkelerine ve amacına uygun ve orantılı olmak şartıyla, veri sorumlusunun aydınlatma yükümlülüğünün düzenlendiği 10. maddenin; zararın giderilmesini talep etme hakkı hariç, ilgili kişinin haklarını düzenleyen 11. maddenin

---

[334] Sert, age, s. 124.

[335] "a) Kişisel verilerin, üçüncü kişilere verilmemek ve veri güvenliğine ilişkin yükümlülüklere uyulmak kaydıyla gerçek kişiler tarafından tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında işlenmesi,
b) Kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi,
c) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi,
ç) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi,
d) Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi."

[336] "a) Kişisel veri işlemenin suç işlenmesinin önlenmesi ya da suç soruşturması için gerekli olması,
b) İlgili kişinin kendisi tarafından alenileştirilmiş kişisel verilerinin işlenmesi,
c) Kişisel veri işlemenin kanunun verdiği yetkiye dayanılarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olması,
ç) Kişisel veri işlemenin bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olması."

ve sicile kayıt yükümlülüğünü düzenleyen 16. maddenin uygulanmayacağı düzenlenmiştir.

Burada dikkat edilmesi gereken husus, maddenin birinci fıkrasında düzenlenen durumlarda KVKK bütün olarak uygulanmayacaktır. İkinci fıkrada düzenlenen durumlarda ise Kanun kısmen uygulanmayacaktır. Bu fıkrada belirtilen durumlarda genel olarak Kanun uygulanacak ancak bu durumlarda fıkrada sayılan kanun maddeleri uygulanmayacaktır.[337]

3.1.3.Suçun nitelikli halleri

3.1.3.1.Özel nitelikli kişisel verilerin kaydedilmesi

TCK'nın 135. maddesinin birinci fıkrasında hukuka aykırı olarak kişisel verilerin kaydedilmesi suçunun temel şekli belirlenmiştir. İkinci fıkrada ise "kişilerin siyasi, felsefi ya da dinî görüşlerine, ırki kökenlerine; cinsel yaşamlarına, hukuka aykırı olarak ahlaki eğilimlerine, sağlık durumlarına ya da sendikal bağlantılarına ilişkin" hassas verilerinin kaydı durumunda suçun cezasının yarı oranında artırılacağı belirtilerek, nitelikli hâl düzenlenmiştir. Hassas veriler, KVKK'da özel nitelikli veriler adıyla TCK'nın 135. maddesinin ikinci fıkrasındakilerden farklı olarak sayılmıştır. TCK'da ve KVKK'da "kişilerin siyasi, felsefi, dinî görüşleri, ırki kökenleri, cinsel yaşamları, sağlık durumları ve sendika üyelikleri" hassas veri olarak düzenlenmiştir. TCK'da, KVKK'da yer almayan "kişinin ahlaki eğilimlerine ilişkin veriler" hassas veri olarak düzenlenmiştir. Ancak KVKK'da bunlara ek olarak "etnik köken, mezheple ilgili ya da diğer inançlar, kılık kıyafet, dernek ve vakıf üyelikleri, ceza mahkûmiyeti, güvenlik tedbirleri, biyometrik ve genetikle ilgili veriler" de hassas veri olarak düzenlenmiştir. KVKK'da farklı olarak yer alan bu hassas veriler, TCK'da özel olarak sayılmadığından ek güvencelerle korunmamaktadır.[338] Dolayısıyla sadece TCK'nın 135/2'de yer alan hassas verilerin kaydı durumunda failin cezası ağırlaştırılacak; TCK'da yer almayıp da KVKK'da yer alan hassas verilerin kaydedilmesi durumunda fail, suçun temel hâli olan TCK'nın 135. maddesinin birinci fıkrasına göre cezalandırılacaktır.[339] Dolayısıyla iki kanun arasında yer alan bu uyumsuzluğun giderilmesi için, KVKK'da hassas veri olarak düzenlenen tüm veriler,

[337] Korkmaz, age, s. 326.
[338] Sert, age, s. 108.
[339] Korkmaz, age, s. 336.

TCK'nın 135. maddesinin ikinci fıkrası kapsamına alınması isabetli olur. Böylece bazı hassas verilerin ek güvencelerle korunup bazılarının korunmaması şeklindeki sorun giderilebilir.

TCK'nın 137. maddesinde ise "kişisel verilerin kaydedilmesi" ve "verileri hukuka aykırı olarak verme veya ele geçirme" suçları açısından ortak olan nitelikli hâller düzenlenmiştir. 137. maddede öngörülen ağırlaştırıcı sebepler, şahsa bağlı ağırlaştırıcı sebeplerdir. Bu nedenle TCK'nın 135-136. maddelerinde düzenlenmiş bu suçların, görünüşte özgü suç oldukları söylenebilir.

3.1.3.2.Kamu Görevlisi Tarafından ve Görevinin Verdiği Yetkiyi Kötüye Kullanmak Suretiyle Kaydedilmesi

Bu nitelikli hâlin uygulanabilmesi için, failin suçu işlediği anda kamu görevlisi olması gerekir. TCK'nın 6. maddesine göre kamu görevlisi; "*kamusal faaliyetin yürütülmesine atama ya da seçilme yoluyla veya herhangi bir surette sürekli, süreli veya geçici olarak katılan kişi*"dir. Bu nitelikli hâlin uygulanabilmesi için failin kamu görevlisi olması yeterli olmayıp, kamu görevinin verdiği yetkinin kötüye kullanılmasıyla suçun işlemesi de gerekir. Kamu görevlisinin aynı zamanda kişisel verileri kaydetme konusunda bir yetkisinin de bulunması gerekir.[340] Örneğin, bir polis memurunun, kanunda izin verilen hâller dışında karakola gelen kişilerden parmak izi alarak kaydetmesi durumunda, bir kamu görevlisinin yetkisini kötüye kullanarak bu suçun işlemesi söz konusu olur.[341] Bu nitelikli hâlin uygulanabilmesi için, suçun kamu görevi sırasında işlenmesi şart olmayıp suçun kamu görevi nedeniyle işlenmiş olması ve failin suç işlediği sırada kamu görevlisi olması yeterlidir. Yine kanuni tanımda bu nitelikli hâlin uygulama alanı bulması için herhangi bir zararın ortaya çıkması da şart

[340] Yargıtay, suçun görevin sağladığı kolaylıktan yararlanarak işlendiği bir olayda, sanık hakkında TCK m. 137/1-b'de düzenlenen nitelikli hâlin uygulanmamasının bozma nedeni olduğuna hükmetmiştir. Karara göre; "Dosya kapsamında incelenen görüntülerden 19.01.2009 tarihli bilirkişi tutanağında, silinen video görüntüsü 5 başlığı altındaki görüntüde bir kadının tuvalet kabininin içindeki görüntülerinin bulunduğu tespit edilmekle, sanığın eyleminin tamamlanmış olduğu gözetilmeksizin teşebbüs aşamasında kaldığı kabul edilerek eksik ceza tayini; katılanların görevli olduğu okulda hizmetli olarak çalışan sanığın bayan öğretmenlerin kullandığı tuvalete görevinin sağladığı kolaylıktan yararlanmak suretiyle gizli kamera yerleştirdiği anlaşılmasına rağmen, sanık hakkında TCK'nın 137/1-b maddesinin tatbik edilmemesi…" Yargıtay 12. CD., E: 2012/12221, K: 2012/12232, T: 16.05.2012.

[341] "TCK'nın 257. maddesinde düzenlenen görevi kötüye kullanma suçu genel nitelikte bir suç olduğundan, bu durumda TCK m. 135. maddesinde düzenlenen suç hükümleri uygulanacaktır." Yaşar/Gökcan/Artuç, age, s. 4439.

değildir.[342] İkinci olarak kamu görevlisinin görevinin gereklerine aykırı hareket ederek verileri hukuka aykırı bir şekilde kaydetmesi gerekir. Dolayısıyla kaydetme fiili, kamu görevlisinin görevine ilişkin olmalıdır. Kişisel verinin kaydedilmesi, kamu görevlisinin görevine girmediği takdirde, bu nitelikli hâl uygulama alanı bulmayacaktır. Ayrıca kişisel verilerin hukuka aykırı olarak kaydedilmesi fiili icrai hareketlerle işlenebileceği için, görevin gereklerini yapmakta ihmal ya da gecikme gösterilmesi, bu suçu oluşturmayacaktır.[343]

3.1.3.3.Belli Bir Meslek ve Sanatın Sağladığı Kolaylıktan Yararlanmak Suretiyle Kaydedilmesi

Meslek; "*Belli bir eğitim ile kazanılan sistemli bilgi ve becerilere dayalı, insanlara yararlı mal üretmek, hizmet vermek ve karşılığında para kazanmak için yapılan, kuralları belirlenmiş iş*", sanat ise; "*Bir şey yapmada gösterilen ustalık*" anlamına gelir.[344]

Nitelikli hâlin uygulanabilmesi için fail, meslek ve sanat olarak kabul edilecek herhangi bir işle iştigal etmeli ve bu meslek ve sanatla iştigal etme, kişisel verileri kaydettiği sırada ona kolaylık sağlamalıdır. Serbest şekilde çalışan bir doktorun, kendisine muayene için gelen ve tahlil yaptıran hastaların tahlil sonuçlarını ve genetik bilgilerini bilgisayarında hukuka aykırı bir şekilde depolaması, aynı şekilde banka memurunun sistemde kayıtlı müşteri bilgilerine ulaşıp bu verileri kendi bilgisayarına kolaylıkla kaydetmesinde de bu nitelikli hâl örnek verilebilir.[345]

3.1.4.Yaptırım ve yargılama usulü

"Kişisel verilerin kaydedilmesi suçu" ihlal eden kişi "*bir yıldan üç yıla kadar hapis cezası*" ile cezalandırılır. Suçun nitelikli halini oluşturan hassas verilerin kaydedilmesi halinde verilecek ceza yarı oranda artırılacaktır. Ayrıca 137. madde hükmünce, "kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle" veya "belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle" suçun işlenilmesi durumunda ceza yarı oranında artırılacaktır.

---

[342] Özbek/Doğan/Bacaksız, age, s.580.
[343] Özbek/Doğan/Bacaksız, age, s.581.
[344] TDK, "Güncel Türkçe Sözlük", http://www.tdk.gov.tr/ (Erişim Tarihi: 15.03.2021).
[345] Sert, age, s. 109.

Suç için "bir yıldan üç yıla kadar hapis cezası" öngörüldüğünden hapis cezasının ertelenmesi ya da hükmün açıklanması geriye bırakılabilir. TCK'nın 51. maddesi uyarınca, maddede aranan şartların varlığı halinde, "işlediği suçtan dolayı iki yıl veya daha az süreyle hapis cezasına mahkûm edilen kişinin cezası ertelenebilir". Ayrıca CMK m. 231 hükmünce kişiye verilecek ceza "*iki yıl veya daha az süreli hapis veya adlî para cezası ise; mahkemece, hükmün açıklanmasının geri bırakılmasına karar verilebilir*". Aynı maddede sayılan şartların da varlığı halinde bu karar verilebilecektir.

"Kişisel verilerin kaydedilmesi suçu", şikâyete bağlı bir suç olmadığından soruşturması Cumhuriyet savcısı tarafından re'sen yapılır. Kişisel verilerin kaydedilmesi suçu açısından görev, "5235 sayılı Adlî Yargı İlk Derece Mahkemeleri İle Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanun" 11. maddesi[346] hükmünce Asliye Ceza Mahkemesi bünyesindedir.

Kişisel verilerin kaydedilmesi suçu, soruşturması şikâyete bağlı olmadığı ve CMK'nın 253. maddesinde sayılan suçlar arasında yer almadığı için, uzlaşma hükümlerine tabi değildir.

Kişisel verilerin kaydedilmesi suçunun temel hâli ve cezayı ağırlaştıran nitelikli hâlinin cezası beş yıldan fazla hapis cezasını gerektirmediği için bu suç açısından dava zamanaşımı, TCK'nın 66/1-e fıkrası gereğince sekiz yıldır. Ceza zamanaşımı ise TCK'nın 68/1-e fıkrası gereğince suçun cezasının beş yılın altında hapis cezası olması nedeniyle on yıldır.[347]

[346] Madde 11- "Kanunların ayrıca görevli kıldığı hâller saklı kalmak üzere, sulh ceza hâkimliği ve ağır ceza mahkemelerinin görevleri dışında kalan dava ve işlere asliye ceza mahkemelerince bakılır."
[347] Sert, age, s. 135.

3.2. Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme Suçu

Kişisel verilerin, yetkisiz üçüncü kişilerin eline geçmesinin ve içeriklerinin öğrenilmesinin önlenmesi amacıyla, "verilerin hukuka aykırı olarak verilmesi, yayılması veya ele geçirilmesi", TCK'nın 136. maddesinde[348] suç olarak düzenlenmiştir.[349]

TCK 136. maddenin başlığında suçun ismi "verileri hukuka aykırı olarak verme veya ele geçirme" olarak ifade edilmiştir. Ancak "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" bölümünde düzenlenen maddede yer alan veri kavramıyla, her türlü veri değil, sadece kişisel veriler kast edilmektedir. Madde metninden de kast edilenin kişisel veriler olduğu anlaşılmaktadır.[350] Ayrıca başlıkta, madde metninde bulunan "yayma" fiili yer almamaktadır. Dolayısıyla madde başlığında sadece "veri" kavramının kullanılması ve "yayma" ibaresinin bulunmaması hatalı olduğundan, suçun, "kişisel verilerin hukuka aykırı olarak verilmesi, yayılması veya ele geçirilmesi" olarak isimlendirilmesi daha isabetli olacaktır. [351]

3.2.1.Suçla korunan hukuki değer

Bu suçla korunan hukuki değer, kişisel verilerin korunması hakkıdır. "Kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçu", "kişisel verilerin kaydedilmesi suçu" gibi, 2010 tarihli Anayasa Değişikliği ile ayrı bir hak alanı olarak anayasal temele kavuşan kişisel verilerin korunması hakkını korumaktadır.[352] Kişisel verilerin kaydedilmesi suçu incelenirken, bu suçla korunan hukuki değer konusunda ayrıntılı açıklama yapıldığından burada tekrar incelenmeyecektir.

---

[348] "Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır."
[349] Ketizmen, age, s. 239.
[350] Erdoğan, agm, s. 624.
[351] Hafızoğulları/Özen, age, s. 289.
[352] Özbek, age, s. 960.

3.2.2.Suçun unsurları

3.2.2.1.Maddi unsur

3.2.2.1.1.Fail, mağdur ve suçun konusu

TCK 136.maddesinde düzenlenen "Verileri hukuka aykırı olarak verme ve ele geçirme suçu"nun faili, kanunun metninden de anlaşılabileceği üzere herkes olabilecektir.[353] Nitekim bu madde kapsamında özel olarak bir fail tanımı yapılmamıştır. Öğretideki, bu suçun verme ve yayma fiili ile işlenmesi halinde, suçun failinin kişisel verilerin zilyedi ya da maliki olan kişi olacağı belirtilmiştir.[354]

Diğer yandan bu suçun failine ilişkin olarak TCK 137. maddesi de dikkate alınmalıdır. Buna göre "kişisel verileri hukuka aykırı olarak veren, yayan ya da ele geçiren kişi"nin "görevini kötüye kullanan bir kamu görevlisi olması" veya "belirli bir sanatın veya mesleği sağladığı kolaylıktan yararlanması" ile bu suçu işlemesi halinde faile uygulanacak yaptırım artırılacaktır.[355] Bu bakımdan verileri hukuka aykırı olarak verme ve ele geçirme suçunun 137. madde kapsamında değerlendirilebilmesi için bu suçun failinin yukarıda saydığımız kişilerden biri olması gerekecektir. Ancak kamu görevlisi ile ilgili olarak öğretide failin yalnızca kamu görevlisi olmasının bu suçun işlenmesi için yetmeyeceği, bu suçun aynı zamanda kamu görevlisinin görevini kötüye kullanmak suretiyle işlenmesi gerektiği özellikle belirtilmiştir. Kamu görevlisinin tanımı konusunda daha önceki bölümümüzde açıklama yapıldığından burada tekrar olmaması açısından bahsedilmeyecektir. [356]

"Kişisel verilerin hukuka aykırı olarak verilmesi, yayılması veya ele geçirilmesi suçu"nun mağduru, verileri verilen, yayılan veya ele geçirilen gerçek kişi veya kişiler olup tüzel kişiler suçtan zarar gören olabilir.[357] Yine aynı doğrultuda Yargıtay da bu görüşte karar vermiştir.[358] Çünkü kişisel veri, TCK'nın 135.

---

[353] Yaşar/Gökcan/Artuç, age, s.4444. Özbek, age, s.960. Hatipoğlu, age, s.2048. Korkmaz, age, s. 394. Dülger, age, s. 704. Özbek/Doğan/Bacaksız, age, s. 583.
[354] Korkmaz, age, s. 394.
[355] Yaşar/Gökcan/Artuç, age, s. 4445.
[356] Sert, age, s. 141
[357] Dülger, age, s. 732. Özbek/Doğan/Bacaksız, age, s. 583. Koca/Üzülmez, age, s. 575.
[358] "Şikâyetçi Türk Telekomünikasyon AŞ'nin, sanığa yüklenen verileri hukuka aykırı olarak verme veya ele geçirme suçunun mağduru olmadığı ve suçtan doğrudan zarar görmemesi nedeniyle davaya katılma hakkının bulunmadığı gözetilmeksizin davaya katılmasına karar verilip, kendisini vekil ile temsil ettiren şikâyetçi lehine vekâlet ücreti hükmedilmesi…" Yargıtay 12.CD., E: 2017/1636, K: 2018/3978, T: 04.04.2018

maddesinin gerekçesinde ve KVKK m. 3/1-d'de, "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi" olarak tanımlanmıştır. Tüzel kişiler, kişisel verilerin korunması kapsamına dâhil edilmemiştir.

"Kişisel verilerin hukuka aykırı olarak verilmesi, yayılması veya ele geçirilmesi suçu"nun konusu kişisel veridir.[359] Çalışmanın birinci bölümünde "kişisel veri" başlığı altında yapılan açıklamalar burası için de geçerlidir.

Yargıtay'ın da uygulamada verdiği kararlarda ad, soyad bilgisi gibi[360] en temel verilerden fotoğraf, ses, görüşme kayıtları gibi[361] bilgilere kadar geniş bir kişisel veri tanımını kabul ederek bu veriler üzerinden suçun oluştuğunu kabul etmiştir.[362]

3.2.2.1.2.Fiil

"Verileri hukuka aykırı olarak verme ve ele geçirme suçu"nda suç başlığından anlaşılabileceği üzere verilerin hukuka aykırı şekilde verilmesi ve ele geçirilmesi bu suçun işlenebileceği hareketleri oluşturmaktadır. Ancak daha evvel de bahsettiğimiz üzere kanun koyucu her ne kadar suç başlığında "Verileri hukuka aykırı olarak verme ve ele geçirme" olarak ifade etmiş olsa da suçun tanımını yaparken "verilerin hukuka aykırı olarak verilmesi, yayılması ve ele geçirilmesi"nden[363] bahsetmiştir. Görüldüğü üzere kanun koyucu suç tanımını yaparken bahsi geçen icrai hareketleri genişletmiş ve bu suçun işlenebilmesi için 'verme' ve 'ele geçirme' hareketlerinin yanı sıra kişisel verileri 'yayma' hareketini de suçun icrai hareketlerinden biri olarak saymıştır.[364] Bu suçun ortaya çıkması için bir zararın doğması da şart olmadığından, bu suç seçimlik hareketli bir soyut tehlike suçu[365] olup, verme, yayma ve ele geçirme hareketlerinden birinin gerçekleştirilmesi halinde bu suç tipi işlenmiş sayılacaktır.[366] Burada verme ve

---

[359] Dülger, age, s. 733.
[360] ".. kendisini mağdur Meryem'in adı ve soyadı ile tanıtıp, onlara, mağdurun babasının ismini, nüfusa kayıtlı olduğu ili ve ev adresini de açıklayıp, onları, tanışmak için mağdurun adresine yönlendirmesi biçiminde sübut bulan eyleminin.." Yargıtay 12. CD., E: 2018/8314, K:2019/7734, T: 26.06.2019
[361] "Katılanın kişisel veri niteliğindeki fotoğraflarını hukuka uygunluk nedenlerinin bulunmaması nedeniyle hukuka aykırı olduğundan tereddüt bulunmaya bir yöntemle başkalarının görgüsüne sunan sanığın…" Yargıtay 12.CD., E: 2018/8186, K: 2019/5456, T: 20.04.2019
[362] Dülger, age, s. 734.
[363] Koca/Üzülmez, age, s. 576.
[364] "Bu durumda vermenin yaymayı da kapsayacak şekilde düşünüldüğü ancak sonradan yaymanın da metin içine alınarak olası bir boşluğun engellenmeye çalışması şekilden yorumlanır" Özbek, **TCK İzmir Şerhi**, s. 961.
[365] Dülger, age, s. 735.
[366] Özbek/Doğan/Bacaksız, age, s. 598.

yayma kavramlarından ne anlaşılması gerektiği konusunda öğretide çeşitli görüşler ifade edilmiştir. Bu görüşlere göre verme ve yayma fiilleri arasındaki farklılık, kişisel verilerin ulaştığı kişi sayısı bakımından farklılık göstermektedir. Buna göre verme, kişisel veriyi bir kişiye iletme şeklinde ortaya çıkabilecekken[367], yayma fiili için ise verilerin birden fazla kişiye ulaşması aranmalıdır.[368] Diğer bir deyişle yayma, verme fiilinin daha geniş daha ileri seviyede bir halini ifade etmektedir. Öğretide yayma seçimlik hareketinden sadece kişisel verilerin doğrudan iletilmesinin anlaşılmaması gerektiği, kişisel verilerin çevrimiçi ortamda[369] ifşanın da bir çeşit yayma olduğu ifade edilmiştir. Diğer yandan bu fiiller konusunda kanunda özel bir yöntem belirtilmediğinden, kişisel verilerin her şekilde yetkisiz bir 3. kişiye verilmesi mümkündür.

Öğretide kişisel verilerin yalnızca bilişim sistemleri üzerinden ele geçirilmesi değil, otomatik olmayan yöntemlerle örneğin bir kâğıt üstüne kaydedilmiş kişisel verilerin de verilmesi, yayılması ve ele geçirilmesi halinde bu suçun oluşacağı ifade edilmiştir.[370] Dolayısıyla kişisel verilerin akılda tutulmak suretiyle kaydedilmesi ve akabinde başkasına yayılması ya da verilmesi halinde, söz konusu suçun oluşup oluşmayacağı konusunda suçun oluşmayacağı yönünde görüş belirtilmiştir.[371] Ayrıca öğretide bilgilerin kulaktan kulağa şekilde aktarılması da bu suçun oluşması için yeterli olmadığı ve mutlaka bir araç kullanılması gerektiği ifade edilmiştir.[372] Yargıtay kararları incelendiğinde de sadece elektronik ortamda değil fiziki ortamda muhafaza

---

[367] "Suça sürüklenen çocuğun, konuyu ve kimliği belirsiz şahsın kendisine yönelik tehdit iddialarını okul idaresine, kanuni temsilcilerine ya da yetkili makamlara anlatıp, kimliği belirsiz kişi hakkında adli soruşturma başlatılmasını sağlamak yerine, mağdura ait kişisel veri niteliğindeki cep telefonu numarasını, mağdurun cinsel amaçlı olarak rahatsız edileceğini bilerek ve mağdurun bilgisi dışında, kimliği belirsiz şahsa vermesi karşısında, verileri hukuka aykırı olarak verme veya ele geçirme suçunun sübut bulduğu gözetilmeksizin…bozma nedenidir" Yargıtay 12. CD., E: 2015/12823 K: 2017/873 T: 08.02.2017

[368] Yaşar/Gökcan/Artuç age, s. 4447.

[369] "Yargıtay da vermiş olduğu bir kararında, verileri hukuka aykırı olarak verme ve ele geçirme suçunun işlenmesiyle ilgili olarak, sanığın, katılana ait kişisel veri niteliğindeki fotoğrafını sosyal medya hesabı üzerinden yayınlaması ve böylece diğer insanlara sunması ile gerçekleşen olayda, hiçbir hukuka uygunluk nedeni tespit edilemeyen olayda sanık hakkında kişisel verileri hukuk aykırı olarak verme ve ele geçirme suçundan cezalandırılmasına ilişkin kararın yerinde olduğunu ifade etmiştir." Yargıtay 12. CD., E: 2015/13248 K: 2017/3108 T: 12.04.2017

[370] Korkmaz, age, s. 393.

[371] Dülger, age, s. 739.

[372] Özbek/Doğan/Bacaksız, age, s. 598.

edilen veriler de korunmaktadır.[373] Diğer yandan bu fiillerin ortak noktası ise ikisinin de verilerin aktarılması kavramını ifade etmesidir. Öğretide bu fiillerden ne anlaşılması gerektiğinin kanun maddesinde belirtilmemesinin, suçların ve cezaların belirliliği ilkesi kapsamında uygulamada şüpheye düşülmesine neden olacağı ifade edilmiştir.[374]

Ele geçirme kavramı ise açıkça hukuka aykırı şekilde kişisel verilerin tüm yöntemler ile[375] ele geçilmesini ifade etmekte olup sıklıkla bilişim ortamında işlenen suçların arasında yer almaktadır. Burada ele geçirme kavramı ile kaydetme kavramı arasındaki farka öğretide dikkat çekilmiştir. Kişisel verilerin kaydedilmesi ayrı bir suç olarak düzenlendiğinden, ele geçirmenin bu suç kapsamı dışında kalan fiillerden oluşması gerekmektedir.[376] Yargıtay vermiş olduğu bir kararında katılana ve eşine ait ve bu kişilerin özel hayatı içerisinde değerlendirilemeyecek nitelikteki bazı fotoğraflarının sosyal medyada paylaşılması neticesinde, sanıklar tarafından alınmasını ve başka hesaplarda yayınlanmasını ele geçirme fiili olarak değerlendirilmiştir.[377] Diğer bir önemli husus ise kişisel verilerin verildiği ya da yayıldığı yetkisiz kişi ya da kişilerin kim olacağı sorusudur. Kanun maddesine baktığımızda, kişisel verilerin hukuka aykırı şekilde verilmesi ya da yayılması halinde

---

[373] "Yargıtay vermiş olduğu bir kararında ele geçirme fiili ile ilgili olarak, ele geçirme kavramı kapsamında çeşitli yöntemlerin söz konusu olabileceğini, yalnızca elektronik ortamda muhafaza edilen verilerin değil, örneğin fiziksel ortamda kaydı tutulmuş bir takım kişisel verilerin yazılı bulunduğu defterin, dosyanın vs. yerinde alınmasının ya da başka bir ortama aktarılmasının ve böylece daha sonra istenildiği her an yeniden kullanılabilecek durumda bulundurulmasının da ele geçirme olduğunu ancak birinin yalnızca hafızasında bir bilgi olarak yer alan kişisel verinin başkasına anlatılması ya da kişisel verilerin yalnızca bulunduğu ortamda okunması yani öğrenilmesi durumunun ise ilgili suç kapsamında ele geçirme sayılmayacağını, bu eylemlerin en fazla özel hayatın gizliliğinin korunması kapsamında değerlendirebileceğini ifade etmiştir." Yargıtay 12. CD., E: 2017/12083, K: 2018/2539, T: 07.03.2018.

[374] Küzeci, age, s. 407. Nitekim Yargıtay'da vermiş olduğu bir kararında her olay için ayrıntılı değerlendirmeler yapılması gerektiği, her somut olayda her eylemin suç oluşturmaması, pratikte belirsizliklere neden olmamak için tüm ayrıntıların dikkatle değerlendirilmesi, olayda bir hukuka uygunluk sebebi olup olmadığının ayrıntılı olarak incelenmesi ve sanığın bir hukuka aykırılık bilinci içinde bu suçu işleyip işlemediğini ortaya koyması gerektiğini ifade ederek, evli olan sanığın, eşi ile mağdur arasında ilişki olduğunu öğrenmesi ve bunun üzerine mağdur adına bir sahte sosyal medya hesabı açıp bu hesapta da mağdura ait ve mağdurun özel hayatı kapsamında sayılmayacak günlük kıyafetleri ile yer aldığı bir fotoğrafı yayınlaması üzerine davaya konu olan olayda sanığın gerçekleştirdiği eylemin mağdurun kişisel verisi olan fotoğrafını başkalarının huzuruna sunması sebebiyle kişisel verilerin hukuka aykırı yayma ve ele geçirme suçunu teşkil ettiği ve sanığın eylemi bakımından da hiçbir hukuka uygunluk nedeni olmadığı dikkate alındığında sanık hakkında mahkûmiyet kararı verilirken beraat kararı verilmesini uygun bulmadığını açıklamıştır. Yargıtay 12. CD., E: 2015/4006, K: 2015/18748, T: 02.12.2015.

[375] Dülger, age, s. 740.

[376] Özbek, age, s. 961.

[377] Uyarer, age, s. 189.

suçun oluşacağı ifade edilmiş ancak bu verilerin kime verileceği hususunda özel bir düzenleme yapılmamıştır. Buna göre kişisel veriler hukuka aykırı olarak yetkisiz 3. gerçek kişi ya da kişilere verilebileceği/yayılabileceği gibi bu veriler tüzel kişilere de verilebilecek ve bu halde de suç oluşmuş sayılacaktır.[378]

3.2.2.2.Manevi unsur

"Verileri hukuka aykırı olarak verme ve ele geçirme suçu"nun tanımında bu suçun işlenebilmesi bakımından verilerin, hukuka aykırı şekilde verilmesi, yayılması ve ele geçirilmesi halinde bu suçun oluşacağı belirtilmiştir.

Bu halde söz konusu suçun işlenmiş sayılabilmesi için özel bir saikten bahsedilmediği için bu suçun kast ile işlenmesinin yeterli olduğunu söyleyebiliriz. Bu halde kast kavramının genel tanımında da yer aldığı üzere söz konusu fiillerin "bilerek" ve "isteyerek" işlenmesi halinde bu suçun manevi unsuru tamamlanmış olacaktır. TCK bir suçun taksirle işlenebilmesi için bunun açıkça belirtilmesi gerektiğinden ve söz konusu madde metninde ise böyle bir ifadeye yer verilmediğinden bu suçun taksirle işlenmesinin mümkün olmayacağını söylemek doğru olacaktır.[379]

3.2.2.3.Hukuka aykırılık unsuru

İlgili suçumuzda "hukuka aykırılık" tipiklikte açıkça yer aldığından, bu suç açısından failde özel hukuka aykırılık bilinci aranır. Bu suçta, hukuka aykırılığın özel olarak araştırılması ve failin kastının fiilin hukuka aykırılığını kapsaması gerekir. Yargıtay da ilgili kararıyla bu görüşü desteklemektedir.[380] Kişisel verilerin kaydedilmesi suçunun "hukuka aykırılık" başlığı altında, suç tipinde hukuka

---

[378] Sarıusta, agm, s. 166.

[379] Yaşar/Gökcan/Artuç, age, s. 4448.

[380] "Katılan tarafından bilgisayarın açık hâlde unutulması nedeniyle tesadüfen katılana ait Facebook mesajlarını gören sanığın, katılanın kendisine, annesine, personel amiri olan diğer sanığa ve bir başka iş yeri arkadaşına karşı haksız bir saldırıda bulunduğu düşüncesine kapılmasının ardından ve başkaca şekilde ispatlanması mümkün olmayan bir hâl içerisinde iken, kaybolma olasılığı bulunan delilleri muhafaza etme ve sanık ...'in de iş akdinin haklı nedenle feshedildiğini ispatlama amacını taşıyan eylemlerinde, hukuka aykırı hareket ettikleri bilinciyle davrandıkları kabul edilemeyeceğinden, sanıklara yüklenen fiillerin kanunda suç olarak tanımlanmamış olması nedeniyle, sanıkların CMK'nın 223/2-a maddesi gereğince beraatlerine karar verilmesi gerekirken, sanıklar hakkında verileri hukuka aykırı olarak verme veya ele geçirme suçundan dolayı CMK'nın 223/2-e maddesi gereğince beraat hükümleri kurulması, bozmayı gerektirir." Yargıtay 12. CD., E: 2015/12942, K: 2017/874, T: 8.2.2017.

aykırılığın özel olarak vurgulandığı hâllerde kastın hukuka aykırılığı kapsayıp kapsamadığıyla ilgili öğretide yer alan tartışmalar bu suç kapsamında da geçerlidir.

3.2.2.3.1.Hukuka uygunluk nedenleri

"Kişisel verilerin hukuka aykırı olarak verilmesi, yayılması veya ele geçirilmesi suçu"nda, TCK'da yer alan "kanun hükmünün icrası", "hakkın kullanılması" ve "ilgilinin rızası" hukuka uygunluk sebepleri uygulama alanı bulur.

Kişisel verilerin bir kanun hükmünün icrası çerçevesinde verilmesi, yayılması veya ele geçirilmesi hâlinde fiil hukuka uygun hâle gelir. Örneğin, Adlî Sicil Kanunu'nun 7. maddesinde, adlî sicil bilgilerinin ilgili kişiye veya vekâletnamede yer alması koşuluyla vekiline, kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarına verilebileceği düzenlenmiştir. Kişisel veri niteliğinde olan adlî sicil bilgilerinin, bu madde kapsamında verilmesi, yayılması veya ele geçirilmesi hâlinde, kanun hükmünün icrası hukuka uygunluk sebebinin varlığından dolayı suç oluşmayacaktır.[381]

Kişisel verilerin bir hakkın kullanılması çerçevesinde verilmesi, yayılması veya ele geçirilmesi hâlinde suç oluşmayacaktır. Örneğin, avukatın mesleği gereği müvekkilinin bilgilerini öğrenmesi ve mahkemeye vermesi hâlinde, mesleğin icrası bir hak teşkil ettiğinden suç oluşmayacaktır.[382]

İlgilinin, kişisel verilerinin verilmesi, yayılması veya ele geçirilmesine rıza göstermesi, fiilleri hukuka uygun hâle getirdiğinden suç oluşmayacaktır. Öğretide, suçun şikâyete bağlı olmaması nedeniyle bireyin değil kamunun menfaatinin ağır bastığı, dolayısıyla bu suç açısından rızanın fiili hukuka uygun hâle getirmeyeceği yönünde bir görüş bulunmaktadır[383]. Ancak, bireylerin kişisel verileri üzerinde kanunda düzenlenen hususlar dışında mutlak tasarruf hakları bulunduğu düşünüldüğünde, ilgili kişinin rızası bulunması halinde suç oluşmayacağı savunulmuştur.[384] Ayrıca, bu suçta uygulama alanı bulan, TCK'da yer alan hukuka uygunluk nedenleri ile KVKK'da özel olarak düzenlenen hukuka uygunluk nedenleri

[381] Sert, age, s. 146.
[382] Şen, age, s. 603.
[383] Özbek/Doğan/Bacaksız, age, s. 600.
[384] Gültekin, agm, s. 194.

hakkında, kişisel verilerin kaydedilmesi suçunda yapılan açıklamalar bu suç açısından da geçerlidir.

3.2.3.Suçun nitelikli halleri

TCK'nın 136. maddesinde suçun temel şekli düzenlenmiştir. 137. maddede ise suçun "kamu görevlisi tarafından görevinin verdiği yetki kötüye kullanılmak suretiyle" veya "belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenmesi" durumunda cezanın yarı oranda artırılması, suçun nitelikli hâlleri olarak düzenlenmiştir.[385] Örneğin, Tapu Müdürlüğü'nde çalışan bir memurun, sisteme kayıtlı verileri başkalarına vermesi durumunda cezasında artırım yapılacaktır. İlgili suçun nitelikli hâlleriyle kişisel verilerin kaydedilmesi suçunun nitelikli hâlleri aynı olduğundan, söz konusu suç tipinin incelendiği kısımda bu nitelikli hâllere ilişkin yapılan açıklamalar burası için de geçerlidir.

3.2.4.Yaptırım ve yargılama usulü

İlgili suçu işleyen kişi, "*iki yıldan dört yıla kadar hapis cezası*" ile cezalandırılır. Suçun nitelikli hâllerinin işlenmesi durumunda verilecek ceza yarı oranında artırılır.

TCK'nın 53. maddesinde kişinin kasten işlemiş olduğu suç sebebiyle hapis cezasına mahkûmiyeti sonucunda, belli haklardan yoksun bırakılabileceği düzenlenmiştir. Suç bakımından fail hakkında bu hak yoksunlukları uygulanabilir.

CMK'nın 231. maddesine göre, sanık hakkında verilen cezanın, iki yıl ya da daha az süreli hapis veya adlî para cezası olması hâlinde, maddede öngörülen şartlar sağlandığı takdirde, hükmün açıklanmasının geri bırakılmasına karar verilebilir. İlgili suç, iki yıldan dört yıla kadar hapis cezası öngörüldüğünden, CMK'nın 231. maddesindeki şartların varlığı hâlinde fail hakkında hükmün açıklanmasının geri bırakılmasına karar verilebilir.

---

[385] Örneğin, TCK m. 137/1-b kapsamında tıp mesleği mensuplarının, hastalarına ait kişisel verileri hukuka aykırı şekilde başkalarına verme ya da yayması hâlinde ceza artırılır. Ahmet Nezih Kök, "Bir Olgu Nedeniyle Tıp Uygulamalarında Mahremiyet İlkesi", Özel Yaşamın Gizliliği ve Kişisel Verilerin Kaydedilmesi, **Terazi Hukuk Dergisi**, C: 11, S: 119, 2016, 172. "Hekimler, diş hekimleri, eczacılar, ebeler ve bunların yardımcıları ve diğer tüm tıp meslek ya da sanatları mensupları bakımından" bu nitelikli hâl geçerlidir. Sevük, age, s. 795.

İlgili suç şikâyete bağlı suçlar arasında olmadığından, suç re'sen soruşturulur.[386] Görev, "5235 sayılı Adlî Yargı İlk Derece Mahkemeleri İle Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanun" 11. maddesi[387] hükmünce Asliye Ceza Mahkemesi bünyesindedir.

İlgili suç, soruşturması şikâyete bağlı olmadığı ve CMK'nın 253. maddesinde sayılan suçlar arasında yer almadığından, uzlaşma hükümlerine tâbi değildir.

İlgili suçun temel hâlinin cezası beş yıldan fazla hapis cezasını gerektirmediği için bu suç açısından dava zamanaşımı, TCK'nın 66/1-e fıkrası gereğince sekiz yıldır. TCK'nın 137. maddesinde düzenlenen cezayı ağırlaştıran nitelikli hâlin uygulama alanı bulduğu durumlarda, suçun cezası beş yıldan fazla hapsi gerektirdiğinden dava zamanaşımı, TCK'nın 66/1-d fıkrası gereğince on beş yıl olur. Ceza zamanaşımı ise TCK'nın 68/1-e fıkrası gereğince on yıldır.

3.3. Verileri Yok Etmeme Suçu

Bireysel veya toplumsal ihtiyaçlar nedeniyle işlenmesi meşru kabul edilen kişisel verilerin, bu ihtiyacın ortadan kalkması durumunda ilgisiz üçüncü kişilerin eline geçmesini engellemek amacıyla, kişisel verilerin yok edilmemesi bir suç olarak düzenlenmiştir.[388]

Suç, TCK'nın "Verileri yok etmeme" başlıklı 138. maddesinde[389] düzenlenmiştir. TCK 138. maddesinin madde başlığında suç, "verileri yok etmeme"

---

[386] Karara göre: "Sanığın, bir dönem duygusal boyutta arkadaşlık ilişkisi içerisinde olduğu mağdurenin, adı, soyadı, mezun olduğu okul bilgileri, ikamet ettiği eve ait adres bilgileri ile birlikte, mağdurenin günlük hayatta çekilmiş fotoğrafı ile oturduğu eve ait dış cepheden çekilmiş fotoğrafları, mağdure tarafından arkadaşlıklarına son verilmesine tepki olarak ve mağdurenin bilgisi ve rızası dışında, Facebook adlı sosyal paylaşım sitesinde yayınladığı olayla ilgili olarak, mağdurenin, aktif kullanımında olan, herkes tarafından bilinmeyen veya kolaylıkla ulaşılması ve bilinmesi mümkün olmayan, ancak sınırlı bir çevre ile paylaştığı adres bilgilerini, adı, soyadı, kendisine ve oturduğu eve ait fotoğrafı ile birlikte rızası dışında, başkalarının bilgisine sunan sanığın eyleminin Verileri hukuka aykırı olarak verme veya ele geçirme suçunu oluşturacağı, mahkemece suç vasfında yanılgıya düşülerek, sanığın özel hayatın gizliliğini ihlal suçundan mahkûmiyetine karar verilmiş ise de, sanığın sübut bulan eyleminin soruşturulmasının ve kovuşturulmasının şikâyete bağlı olmadığı, bu yönüyle sanık hakkında kurulan hükmün, usul ve yasaya uygun olduğu anlaşılmakla, sanığın eyleminin şikâyete tabi olduğu ve şikâyet yokluğu nedeniyle davanın düşürülmesi gerektiği gerekçesiyle, bu suç yönünden kurulan hükme ilişkin kanun yararına bozma talebinin reddine karar verilmiştir." Yargıtay 12. CD., E: 2013/30406, K: 2014/2980, T: 10.2.2014.

[387] Madde 11- "Kanunların ayrıca görevli kıldığı hâller saklı kalmak üzere, sulh ceza hâkimliği ve ağır ceza mahkemelerinin görevleri dışında kalan dava ve işlere asliye ceza mahkemelerince bakılır."

[388] Ketizmen, age, s. 240.

[389] "(1) Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde bir yıldan iki yıla kadar hapis cezası verilir.

şeklinde düzenlenmiştir. Ancak kişisel verilerin yok edilmemesi suçuyla aslında düzenlenmek istenen kişisel verilerin yok edilmemesidir. Çünkü "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" bölümünde düzenlenen maddede veri kavramıyla her türlü veri değil, sadece kişisel veriler kast edilmektedir.[390] Ayrıca maddenin lafzından, gerekçesinden ve düzenleniş amacından da madde ile kişisel verilerin yok edilmemesinin suç olarak düzenlendiği anlaşılmaktadır. Dolayısıyla madde başlığında sadece "veri" kavramının kullanılması hatalı olduğundan, suçun başlığının "Kişisel Verilerin Yok Edilmemesi" şeklinde değiştirilmesi daha doğru olacaktır.[391]

Kişisel verilerin yok edilmemesi suçu, KVKK'nın 17. maddesinin ikinci fıkrasında, Kanun'un 7. maddesindeki hükümlere aykırı olarak; kişisel verileri silmeyen ya da anonim hâle getirmeyenlerin TCK'nın 138. maddesine göre cezalandırılacağı şeklinde düzenlenmiştir.

3.3.1.Suçla korunan hukuki değer

Kişisel verilerin yok edilmemesi suçunun konusu kişisel veriler olan diğer suç tipleri gibi "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" başlıklı dokuzuncu bölümünde düzenlenmiştir. Buna göre ilgili suç tipiyle korunmak istenen hukuki yararın uluslararası düzenlemelere paralel şekilde genel olarak kişilerin özel hayatı ve hayatın gizli alanı[392], özel olarak ise kişisel verilerin korunması olduğu söylenebilir.[393]

Öğretide bu suçun kamusal yönü dikkate alınarak bu suç ile korunan hukuki değerin kamu idaresinin güvenirliği ve işleyişi olduğu ifade edilmiştir.[394] Ancak biz bu görüşe katılmamaktayız. Nitekim aşağıda ayrıntılı olarak işlendiği üzere bu suçun mağduru kişisel verileri yok edilmeyen gerçek kişiler olup, korunan hukuki değer de bu kişilerin kişisel verilerinin korunması hakkı olmalıdır. Ayrıca hukuka uygun olarak işlenen kişisel verilerin kanunda belirtilen süreler geçtikten sonra sistemden yok

(2) Suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması hâlinde verilecek ceza bir kat artırılır."

[390] Sert, age, s. 153.

[391] Yavuz Erdoğan, "Kişisel Verilerin Korunması Bakımından Türk Ceza Kanunu Hükümlerinin Değerlendirilmesi (Madde 135, 136, 137, 138)", **Erciyes Üniversitesi Hukuk Fakültesi Dergisi**, S: 2, 2013, s. 620.

[392] Yaşar/Gökcan/Artuç, age, s.4461. Özbek, age, s. 964. Özbek/Doğan/Bacaksız, age, s. 588.

[393] Kuşkonmaz, agt, s. 129, Dülger, age, s. 753, Korkmaz, age, s. 427.

[394] Dülger, age, s. 753.

edilmesi hususu ile bireyin özel hayatına keyfi müdahalelerin önlenmesi amaçlanmıştır. [395]

3.3.2.Suçun unsurları

3.3.2.1.Maddi unsur

3.3.2.1.1.Fail, mağdur ve suçun konusu

TCK'nın 138. maddesinde düzenlenmiş olan kişisel verilerin yok edilmemesi suçunun faili, kanun tarafından verileri sistem içinde yok etme yükümlülüğü getirilmiş kişilerdir. Dolayısıyla suç, söz konusu verileri yok etme yükümlülüğü altında bulunan kişilerce işlenebileceği için özgü bir suçtur. Bir kişinin suçun faili olabilmesi için, verileri sistem içinde yok etmekle yükümlü kılınması yeterlidir, kamu görevlisi olması gerekmez.[396]

Suçun faili açısından verileri sistem içinde yok etmekle yükümlü olan kişilerin tespiti önemlidir. KVKK'nın 7. maddesinde kişisel verilerin işlenmesini gerektiren sebeplerin ortadan kalkması durumunda, kişisel verilerin veri sorumlusu tarafından re'sen veya ilgilinin talebi üzerine silineceği, yok edileceği ya da anonim hâle getirileceği belirtilmiştir. Söz konusu maddenin üçüncü fıkrasına istinaden çıkarılan "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik"in, "Kişisel Verilerin Silinmesi" başlıklı 8. maddesi, "Kişisel Verilerin Yok Edilmesi" başlıklı 9. maddesi ve "Kişisel Verilerin Anonim Hâle Getirilmesi" başlıklı 10. maddesine göre kişisel verilerin silinmesi, yok edilmesi ve anonim hâle getirilmesi için her türlü teknik ve idari tedbirleri almakla yükümlü olan kişinin, veri sorumlusu olduğu belirtilmiştir. Dolayısıyla kişisel verilerin yok edilmemesi suçunun faili, KVKK'da ve çıkarılan Yönetmelik'te belirtildiği üzere kişisel verileri silmekle yükümlü olan veri sorumlusudur. Veri sorumlusunun tanımı KVKK'nın 3/1 maddesinde, "*kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi*"dir. "Veri Sorumluları Sicili Hakkında Yönetmelik"in 11. maddesine[397] göre; tüzel

[395] Uyarer, age, s. 237.
[396] Sevük, age, s. 259.
[397] "Tüzel kişilerde veri sorumlusu tüzel kişiliğin kendisidir. Türkiye'de yerleşik olan tüzel kişilerin Kanun kapsamındaki veri sorumlusu yükümlülükleri, ilgili mevzuat hükümlerine göre tüzel kişiliği temsil ve ilzama yetkili organ veya ilgili mevzuatta belirtilen kişi veya kişiler marifetiyle yerine getirilir. Tüzel kişiliği temsile yetkili organ, Kanunun uygulanması bakımından yerine getirilecek yükümlülükler

kişilerde veri sorumlusu, tüzel kişiliği temsile yetkili organ veya ilgili mevzuatında belirtilen kişi veya kişiler ya da tüzel kişiliği temsile yetkili organ tarafından görevlendirilen kişilerdir. Tüzel kişiliğin bünyesince verilen görev, Kanun gereği tüzel kişiliğin sorumluluğu ortadan kaldırmamakta, tüzel kişiliği temsile yetkili organ da bu kişilerle birlikte sorumlu olur. Veri Sorumluları Sicili Hakkında Yönetmelik'in 11/5 maddesi gereğince, kamu kurumlarında verilerle ilgili koordinasyonu sağlamakla yükümlü üst düzey bir yönetici, veri sorumlusu olarak belirlenir.[398]

Kişisel verilerin yok edilmemesi suçunun mağduru, sistemde kayıtlı kişisel verileri yok edilmeyen gerçek kişilerdir.[399]

Kişisel verilerin yok edilmemesi suçunun konusu, sistem içinde hukuka uygun olarak kayıtlı bulunan kişisel verilerdir.[400] Çalışmamızın birinci bölümünde "kişisel veri" hakkında yapılan açıklamalar burası için de geçerlidir.

3.3.2.1.2.Fiil

TCK'nın 138. maddesinin birinci fıkrasına göre kişisel verilerin yok edilmemesi suçunun fiili, yok etme görevini yerine getirmemektir. Suçun oluşması için kişisel verilerin; kanuna uygun olarak kaydedilmiş olması, kişisel verinin yok edilmesi için belirlenen sürenin geçmiş olması ve verileri sistem içinde yok etmekle yükümlü olanların bu yükümlülüğü yerine getirmemesi gerekmektedir.

Suçun fiil unsurunu oluşturan yok etmek[401] KVKK'da açıklanmıştır. Verinin yok edilmesi tamamen ortadan kaldırma şeklinde olabileceği gibi veriyle ilgili kişi arasındaki bağlantının ortadan kaldırılması şeklinde de gerçekleşebilir. Örneğin, verinin anonim hâle getirilmesi durumunda veriyle kişi arasındaki bağlantı kesilmektedir.[402] Örneğin, bilgisayar, telefon gibi teknolojik aletlerde saklanan bir

---

ile ilgili olarak bir veya birden fazla kişiyi görevlendirebilir. Bu görevlendirme Kanun hükümleri uyarınca tüzel kişiliğin sorumluluğunu ortadan kaldırmaz."

[398] Sert, age, s. 133.

[399] Timur Demirbaş, **Ceza Hukuku Genel Hükümler**, 12. Baskı, Seçkin Yayıncılık, Ankara, 2017, s. 556, Hafızoğulları/Özen, age, s. 292; Özbek/Doğan/Bacaksız, age, s. 603; Yaşar/Gökcan/Artuç, age, s. 4461. "Suçla korunan hukuki değerin, kamu idaresi ve işleyişine duyulan güven olduğunu belirten yazarlara göre ise bu suçun mağduru toplumdaki herkestir. Verileri sistemde kayıtlı olan kişiler ise suçtan zarar görendir."

[400] Dülger, age, s. 753.

[401] KVKK 7. Madde gerekçesi: "bir veri kayıt sisteminin parçası olan evrakı yok etmek, yakmak, veri saklamaya elverişli olan dosya, CD, hard disk gibi kayıt ortamlarından hiçbir şekilde tekrar kullanılamayacak ve geri dönüştürülemeyecek şekilde ortadan kaldırmaktır."

[402] Ketizmen, age, s. 241.

verinin silinmesi bile dönüşümü mümkündür. Dolayısıyla verinin üstüne veri yazılması veya format atılması gibi işlemler veriyi dönüştürülemez, tekrar kullanılamaz kılacaktır.

Kişisel verilerin yok edilmemesi suçunun oluşması için aranan ilk şart, kişisel verilerin kanuna uygun olarak kaydedilmiş olmasıdır. Eğer veri, kanuna aykırı olarak kaydedilmişse kişisel verilerin yok edilmemesi suçu değil, "kişisel verilerin hukuka aykırı olarak kaydedilmesi suçu" oluşur.[403]

Kişisel verilerin yok edilmemesi suçunun oluşması için ikinci şart, kişisel verinin yok edilmesi için belirlenen sürenin geçmiş olmasıdır. Kişisel verilerin yok edilmemesi suçunun madde metninde; "kanunların belirlediği süreler" şeklinde bir ifadeye yer verilmiştir. Bu maddedeki "kanun" ifadesinden ne anlaşılması gerektiği hususunda öğretide farklı görüşler bulunmaktadır. Bir görüş, sadece kanunda düzenlenen sürelerin bu suçun konusunu oluşturabileceğini kabul ederken[404] diğer bir görüş, kanun dışında kalan tüzük, yönetmelik gibi genel düzenleyici işlemlerdeki sürelerin de bu suçun konusunu oluşturabileceğini kabul etmektedir.[405] Suçta ve cezada kanunilik ilkesi gereğince verilerin silinmesi gereken sürenin kanunlar dışındaki genel düzenleyici işlemlerde belirlenmesi durumunda failin cezai sorumluluğuna gidilemeyeceğinden, sadece kanunda düzenlenen sürelerin bu suçun konusunu oluşturabileceği görüşüne katılıyoruz.[406]

Kişisel verilerin yok edilmesi gereken süreler, düzenlendiği kanunda açıkça belirtilmişse suçun oluşması için mutlaka bu sürenin geçmesi gerekmektedir.[407] Öğretide, kanunda belirtilen süreler dolmadan önce verileri silme yükümlülüğü altında bulunan görevlinin veriyi silmeyeceğini yahut amirinin veriyi silme yönündeki emrini yerine getirmeyeceğini açıkça beyan etmesi durumunda da kanundaki sürenin geçmesini bekleme gereği olmadan suçun oluşacağı belirtilmiştir. Ancak suçun

[403] Yılmaz, age, s. 212.
[404] Erdoğan, agm, s. 620; İsmail Dursun, "Türk Ceza Kanunu'nda Verileri Yok Etmeme Suçu", **Kocaeli Üniversitesi Hukuk Fakültesi Dergisi**, S: 10, Seçkin Yayıncılık, Ankara 2014, s. 22.
[405] Özbek/Doğan/Bacaksız, age, s. 604.
[406] Dülger, age, s. 758.
[407] Akdağ, age, s. 146.

gerçekleşebilmesi için kanun maddesinde açıkça belirlenen sürenin geçmesi şartı arandığından[408] bu görüşe katılmıyoruz.

Verilerin yok edileceği sürelerin düzenlendiği kanunlarda, sürenin somut bir şekilde belirtilmesi zorunluluğu bulunmaz. Bu gibi kanunda verilerin yok edilmesi için belli bir sürenin öngörülmediği, "*ihtiyaç duyulmaması hâlinde silineceği, makul süre içinde silineceği, derhal silineceği*" gibi ifadelere yer verildiği yahut bir kararın alınması şartına bağlandığı durumlarda kişisel verilerin silinmemesi suç teşkil eder. Kanunda açıkça verilerin silinmesini emreden herhangi bir emir normunun bulunmaması hâlinde ise verilerin yok edilmemesi suçu oluşmayacaktır.[409]

Kişisel verilerin yok edilmesi gereken sürenin ilgili kanunda açıkça belirtilmemesi hâlinde, suçun oluşacağı zamanı tespit problemi ortaya çıkar. Verileri yok etmekle yükümlü veri sorumluları, "Veri Sorumluları Sicili Hakkında Yönetmelik" m. 9/5'e göre, "*Kişisel verilerin işlendikleri amaç için gerekli olan azami sürenin belirlenmesi ve azami sürenin aşılıp aşılmadığının takibi için kişisel veri saklama ve imha politikası hazırlayarak, bu politikanın uygulanmasını temin ederler*." Dolayısıyla kişisel verilerin silinmesi gereken süreler ilgili kanunda açıkça belirlenmediyse, Veri Sorumluları Sicili'ne kayıt zorunluluğu bulunan veri sorumlularının kişisel veri saklama ve imha politikası hazırlaması ve orada, verilerin silinmesi gereken sıklığı belirlemesi gerekir. Bu sıklık, "Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmelik"in 11. maddesine göre, her hâlde altı ayı geçemez. KVKK'nın 28. maddesinde İstisnalar başlığında düzenlenen, Veri Sorumluları Sicili'ne kaydolmak zorunda olmayan ve veri saklama ve imha politikası hazırlama yükümlülüğü bulunmayan veri sorumlularının ise "*kişisel verileri silme yükümlülüğünün ortaya çıktığı tarihi takip eden üç ay içinde, kişisel verileri sileceği düzenlenmiştir. Dolayısıyla kişisel verileri sistem içinde yok etmekle yükümlü olan veri sorumlularının, bu 6 ve 3 aylık süreler sonunda verileri yok etmemesi hâlinde*" suç oluşur.

Kişisel verilerin yok edilmemesi suçunun oluşması için aranan üçüncü şart, verileri yok etmekle yükümlü kişinin veriyi yok etmemesidir. Suçun, kanunda

[408] Akdağ, age, s. 148.
[409] Yaşar/Gökcan/Artuç, age, s. 4463.

öngörülen "yok etme" emrinin ihlali şeklindeki ihmali hareketle işlenebildiğinden gerçek ihmali bir suçtur. İcrai hareketlerle bu suçun işlenebilmesi mümkün görünmemektedir.[410] Gerçek ihmali suçlarda netice olmadığından, verilerin yok edilmemesi suçu sırf hareket suçudur.[411] Suçun madde metninde, "*verileri sistem içinde yok etmek*" şeklinde bir ifade yer almaktadır. TCK'nın 2004 yılında kabul edildiği göz önüne alındığında, sistem ibaresi sadece otomatik sistemler olarak değil, kişisel verilerin kaydedildiği yer olarak anlaşılmalıdır. Örneğin iletişimin denetlenmesi tedbirinde, banda alınan iletişim kayıtlarının yazıldığı kâğıtlar veya gizli soruşturmacının elde ettiği deliller herhangi bir sisteme kaydedilmemektedir, ancak bu delillerden suçla bağlantılı olmayanlar derhal yok edilmelidir.[412]

3.3.2.2.Manevi Unsur

Suç kasten işlenebilir. Suç tipinde manevi unsur açısından özel bir amaç ve saik aranmamıştır. Dolayısıyla bu suç, genel kastla işlenebilir.[413] Bu suçun oluşabilmesi için fail, söz konusu verilerin kişisel veri niteliğinde olduğunu, bu verileri sistem içinde yok etmekle yükümlü olduğunu ve kanunda belirtilen sürelerin sonunda verileri yok etmediğinde suçun oluşacağını bilmeli ve iradesini suç işlemeye yönlendirmelidir.

Kural olarak doğrudan kastla işlenen suçlar, tipiklikte bilme unsurunun veya hukuka aykırılık bilincinin ya da failin belli bir amaç veya saikle hareket etmesinin arandığı suçlar haricinde, olası kastla da işlenebilirler. Bu sebeple kişisel verilerin yok edilmemesi suçunun olası kastla da işlenebilmesi mümkündür. Örneğin, fail kişisel verileri derhal yok etmesi gerektiğini öngörmesine rağmen süresi içinde yok etmemişse suç, olası kastla işlenmiş olur. Ancak kanunda verilerin yok edileceği süreler açıkça belirlenmişse ve fail, verileri bu süre içinde yok edeceğini öngörmesine rağmen hareketsiz kalmışsa, suçu kasten işlemiş olacaktır.

Kanun koyucu, suça vücut veren fiilin dikkat ve özen yükümlülüğüne aykırı olarak icrasını ayrıca suç olarak düzenlemediğinden, kişisel verilerin yok edilmemesi

---

[410] Hafızoğulları/Özen, age, s. 291, Ketizmen, age, s. 240.
[411] Artuk/Gökcan, age, s. 258.
[412] Sert, age, s. 158.
[413] Kangal, age, s. 170.

suçunun taksirli hali cezalandırılmaz. Failin kanunda belirtilen süreler içinde görevini kasten ihmal etmesi hâlinde suç gerçekleşmiş olacaktır.[414]

Suçun, fiilin bir zarara yol açması gibi daha ağır ya da başkaca neticeye yol açması ihtimaline yer verilmediğinden neticesi sebebiyle ağırlaşmış hâli suç olarak düzenlenmemiştir.

3.3.2.3.Hukuka Aykırılık Unsuru

Kişisel verilerin yok edilmemesi suçunda, TCK'nın 135. ve 136. maddelerinden farklı olarak failin hukuka aykırılık bilinci ile hareket etmesi aranmamıştır.[415]

Suç açısından kanunda herhangi bir hukuka uygunluk sebebi bulunmamaktadır. Meşru savunma, kanun hükmünün icrası ve hakkın kullanılması hukuka uygunluk sebeplerinin şartları, kişisel verilerin silinmesi suçu açısından uygulama alanı bulacak bir örneğe sahip değildir. Verilerin yok edileceği sürelerin belirlendiği kanunlarda, kişisel verilerin yok edilmesi yönünde emredici hüküm bulunması nedeniyle mağdurun verileri yok etmemeye rızası olsa dahi eylem hukuka uygun duruma gelmeyeceğinden, ilgilinin rızası bu suç açısından geçerli bir hukuka uygunluk sebebi teşkil etmez.[416]

3.3.3.Suçun nitelikli halleri

TCK'nın 138. maddesinin ikinci fıkrasında, "*Suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması hâlinde verilecek ceza bir kat artırılır.*" şeklindeki düzenlemeyle suçun cezasını artıran bir nitelikli hâle yer verilmiştir. Buna göre suçun konusunu oluşturan yok edilmesi gereken kişisel verinin CMK'nın çeşitli maddelerinde öngördüğü bir kişisel veri olması hâlinde failin cezası bir kat artırılır. Kişisel verilerin yok edilmemesi suçu sonucunda bir zararın ortaya çıkması hâlinde, bu durumun daha ağır cezayı gerektiren nitelikli hâl olarak düzenlenmesi isabetli olur. TCK'nın 98. maddesinde yer alan "Yardım veya bildirim yükümlülüğünün yerine getirilmemesi" suçu da sırf hareket suçu olmasına rağmen, yardım veya bildirim yükümlülüğünün

[414] Şen, age, s. 719.
[415] Erdoğan, agm, s. 625.
[416] Hafızoğulları/Özen, age, s. 293.

yerine getirilmemesi sonucunda kişinin ölmesi hâli, cezayı artıran nitelikli hâl olarak düzenlenmiştir. Kişisel verilerin yok edilmemesi suçunda da benzer şekilde düzenleme yapılabilir.

CMK'da kişisel verilerin kaydedildikten sonra yok edilmesine yönelik düzenlemeler bulunmaktadır. Konuya ilişkin olarak yapılan ilk düzenleme, CMK'nın "Genetik inceleme sonuçlarının gizliliği" başlıklı 80. maddesinde, CMK'nın 75, 76 ve 78. maddelerine göre alınan kan, tükürük, saç, deri, tırnak gibi örnekler üzerinde yapılacak inceleme sonucu elde edilen kişisel veri niteliğindeki bilgilerin, "kovuşturmaya yer olmadığı kararına itiraz süresinin dolması, itirazın reddi, beraat veya ceza verilmesine yer olmadığı kararı verilip kesinleşmesi hâllerinde Cumhuriyet savcısının huzurunda derhâl yok edileceği"ne yönelik düzenlemedir.

CMK'nın "Fizik kimliğin tespiti" başlıklı 81. maddesine göre, şüpheli veya sanığın beden ölçülerinin, fotoğraflarının, parmak ve avuç içi izlerinin, bedeninde yer alıp teşhisini kolaylaştıracak diğer özelliklerinin, ses ve görüntülerinin maddedeki şartların varlığı hâlinde kayda alınacağı ve bu verilerin, "*kovuşturmaya yer olmadığı kararına itiraz süresinin dolması, itirazın reddi, beraat veya ceza verilmesine yer olmadığı kararı verilip kesinleşmesi hâllerinde Cumhuriyet savcısının huzurunda derhâl yok edileceği*" düzenlenmiştir.

CMK'nın "İletişimin tespiti, dinlenmesi ve kayda alınması" başlıklı 135. maddesinin üçüncü fıkrasında; "*şüpheli ya da sanığın tanıklıktan çekinebilecek kişilerle arasındaki iletişimi kayda alınamaz*." şeklinde düzenleme yapılmıştır. Maddeye göre kayıt yapıldıktan sonra bu durum anlaşılırsa, alınan kayıtlar derhâl yok edilmelidir. CMK'nın 137/3. maddesi gereğince de 135. maddeye göre verilen iletişimin tespiti, dinlenmesi ve kayda alınması sırasında şüpheli hakkında kovuşturmaya yer olmadığı kararı verilmesi veya aynı maddenin birinci fıkrasına göre hâkim onayının alınmaması hâlinde, yapılan tespit ya da dinlemeyle ilgili kayıtlar, savcının denetimi altında en geç on gün içinde yok edilmelidir.

CMK'nın "Gizli soruşturmacı görevlendirilmesi" başlıklı 139. maddesinin altıncı fıkrasına göre, soruşturmacı görevlendirilmesi suretiyle elde edilen kişisel bilgilerden suçla bağlantılı olmayanlar, derhâl yok edilmelidir.

CMK'nın "Teknik araçlarla izleme" başlıklı 140. maddesinin ikinci fıkrasına göre, Cumhuriyet savcısı, şüpheli veya sanığın kamuya açık yerdeki faaliyetleriyle işyerinin teknik araçla izlenmesi için verdiği kararları yirmi dört saat içinde hâkimin onayına sunar ve hâkim, kararını en geç yirmi dört saat içinde verir. Sürenin dolması ya da hâkim tarafından aksine karar verilmesi hâlinde ise kayıtlar derhâl imha edilmelidir. Aynı maddenin dördüncü fıkrasında da teknik araçlarla izleme sonucunda elde edilen delillerin, ceza kovuşturması bakımından gerekli olmaması hâlinde Cumhuriyet savcısının gözetiminde derhâl yok edileceği düzenlenmiştir.

Kişisel verilerin yok edilmemesi suçunun nitelikli hâlini teşkil eden bu düzenlemelerde, verilerin sistemin içinde yok edilmesiyle görevli kişi Cumhuriyet savcısı değil, veri sorumlusudur. Belirlenen bu veri sorumlusunun, kişisel verileri kanunda belirlenen süreler sonunda Cumhuriyet savcısı huzurunda yok etmemesi hâlinde ceza artırılarak verilir. CMK'daki düzenlemelerde yer alan derhal ifadesinden kasıt, yapılabilecek en kısa sürede ve gerekirse fazla mesai harcanarak verilerin silinmesidir. Makul süre ise kişisel verilerin silinebileceği ilk anda silinmesidir. Ancak bu düzenlemelerde yer alan suçla bağlantılı olmayan verilerin derhal veya makul süreler içinde silinmesi, hâkimin sonradan delilleri takdir edecek olması nedeniyle isabetli bir uygulama değildir. Suçla bağlantılı olmayan verilerin, en azından soruşturma konusu suçun yargılaması sonuna kadar saklanması gerekir.

3.3.4.Yaptırım ve yargılama usulü

TCK'nın 138. maddesine göre kanunlar tarafından belirlenen süreler geçmiş olmasına rağmen verileri sistem içinde yok etmekle yükümlü olan fail, görevini yerine getirmezse, bir yıldan iki yıla kadar hapis cezasıyla cezalandırılır. TCK'nın 138. maddesinin ikinci fıkrası gereğince kişisel verileri yok etmeme suçunun konusu, CMK hükümlerine göre ortadan kaldırılması ya da yok edilmesi gereken verilerden olursa suçun temel hâline göre belirlenecek somut ceza bir kat artırılacaktır.

Suçun cezasının alt sınırının 1 yıl olması sebebiyle failin cezası, hâkim tarafından TCK'nın 50. maddesinde düzenlenen seçenek yaptırımlara çevrilebilir. Kişisel verilerin yok edilmemesi suçunun temel hâlinin cezası bir yıldan iki yıla kadar hapis cezası olduğundan, TCK'nın 51. maddesine göre failin önceden kasıtlı bir suçtan dolayı üç aydan fazla hapis cezasına mahkûm edilmemiş olması ve suç işlendikten

sonra yargılama sürecinde gösterdiği pişmanlık dolayısıyla tekrar suç işlemeyeceği konusunda mahkemede bir kanaat oluşması hâlinde cezası ertelenebilir.

Kişisel verileri yok etmeme suçunun temel hâlinin cezası bir yıldan iki yıla kadar hapis cezası olduğu için, CMK'nın 231. maddesindeki şartların varlığı hâlinde hükmün açıklanmasının geri bırakılmasına karar verilebilir.

Verilerin yok edilmemesi suçu şikâyete bağlı suçlar arasında olmadığından, suçun soruşturulması Cumhuriyet savcısı tarafından re'sen yapılır. Kişisel verilerin yok edilmemesi suçu açısından görev, "5235 sayılı Adlî Yargı İlk Derece Mahkemeleri İle Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanun" 11. maddesi[417] hükmünce Asliye Ceza Mahkemesi bünyesindedir.

Kişisel verilerin yok edilmemesi suçu, soruşturması şikâyete bağlı olmadığı ve CMK'nın 253. maddesinde sayılan suçlar arasında yer almadığı için, uzlaşma hükümlerine tabi değildir.

Kişisel verileri yok etmeme suçunun hem temel hâli hem de cezayı ağırlaştıran nitelikli hâlinin cezası beş yıldan fazla hapis cezasını gerektirmediği için bu suç açısından dava zamanaşımı, TCK'nın 66/1-e maddesi gereğince sekiz yıldır. Bu süre en fazla 12 yıla kadar uzayabilir. Ceza zamanaşımı ise aynı madde gereğince suçun cezasının beş yılın altında hapis cezası olması nedeniyle on yıldır.[418]

[417] 11. madde: "Kanunların ayrıca görevli kıldığı hâller saklı kalmak üzere, sulh ceza hâkimliği ve ağır ceza mahkemelerinin görevleri dışında kalan dava ve işlere asliye ceza mahkemelerince bakılır."
[418] Artuk/Gökcen/Alşahin/Çakır, age, s. 1010.

3.4.Suçun Özel Görünüş Şekilleri

3.4.1.Teşebbüs

"Kişisel verilerin kaydedilmesi suçu"nun teşebbüs ile işlenip işlenemeyeceğiyle ilgili öğretide görüş ayrılığı mevcuttur. Bazı yazarlar[419] suçun harekete bitişik bir suç olduğundan varsayımla teşebbüsün mümkün olmayacağını, ele geçirilmiş fakat kaydedilememiş olması durumunda teşebbüsten ziyade "hukuka aykırı olarak ele geçirme" suçunun oluşacağını savunmaktadır. Bazı yazarlar[420] ise, icra hareketlerinin bölünebilir olması halinde teşebbüs ile suçun işlenebileceğini savunmaktadır. Örneğin (A), müşterilerin bir alışveriş internet sitesine kendi rızasıyla verdiği kişisel verileri, normal şartlarda veriler internet sitesinin kayıtlarında başkalarının erişimine kapalı olarak tutulduğundan dolayı göremez. Fakat (A), bir şekilde internet üzerinden bu alışveriş sitesinin müşteri kayıtlarına ulaşır ve onları kopyalayıp kendi bilgisayarına kaydederken herhangi bir nedenle kayıt işlemini kaydedemezse, kişisel verilerin kaydedilmesi suçu teşebbüs aşamasında kalmış olacaktır. Zira bu durumda (A) kişisel verileri kopyalamak suretiyle icra hareketlerine başlamış olacak, ancak verileri kendi bilgisayarına kaydederken kendi iradesi dışında kayıt işlemini gerçekleştiremediğinden icra hareketleri tamamlanamayacak ve suç oluşmamış olacaktır.[421] Kişisel verileri hukuka uygun olarak elinde bulunduran kişi bunları hukuka aykırı olarak kaydetmek üzereyken kendi rızası dışında tamamlayamamışsa yine suça teşebbüs mümkün olacaktır.[422] Örnek verecek olursak, failin başkasına ait bir bilgisayara taktığı USB belleğe kopyalama işlemini yaparken yakalanması durumunda suça teşebbüs söz konusu olacaktır.

"Kişisel verilerin hukuka aykırı olarak verme ve ele geçirme suçu" bakımından da icrai hareketlerin parçalara ayrılabilir olması durumunda, suç teşebbüs aşamasında kalabilecektir. Ancak suçun oluşması açısından ayrıca bir neticeye yer verilmediği için, bu suçun teşebbüs aşamasında kalmasına sıklıkla rastlanılmaz.[423] Örneğin Yargıtay'ın da bir kararına konu olan kart bilgilerinin kopyalanması için düzenlenen

---

[419] Özbek/Doğan/Bacaksız, age, s. 595, Özbek, **TCK İzmir Şerhi**, s. 963.
[420] Dülger, age, s. 728, Yaşar/Gökcan/Artuç, age, s. 4122, Sevük, age, s. 810, Erdoğan, agm, s. 602.
[421] Korkmaz, age, s. 423.
[422] Köse, age, s. 167.
[423] Dülger, age, s. 748.

bir sistem sonucu sanıklar hiçbir kart bilgisini elde edememiş olsalar dahi ele geçirmeye teşebbüsten suçun oluştuğuna kanaat getirilmiştir.[424]

Kişisel verilerin yok edilmemesi suçu, gerçek ihmali suç olduğundan suça teşebbüs mümkün değildir.[425] Kanunda belirtilen süreler içinde verileri yok etmekle yükümlü kimsenin bu yükümlülüğünü yerine getirmemesiyle suç tamamlanmış ve bitmiş olur.[426]

Kişisel verileri yok etmekle görevli kişi, kanunda belirtilen süreler geçtikten sonra ancak yetkili makamların bilgisi olmadan önce verileri yok etse dâhi, ceza hukuku kapsamında sorumluluğu oluşmaktadır.[427] Çünkü bu suç sürelerin geçmesi sonunda verilerin silinmemesiyle tamamlanmış olur ve suç bakımından etkin pişmanlık hükümleri de düzenlenmemiştir.[428]

3.4.2.İştirak

"Kişisel verilerin kaydedilmesi suçu" ile "Kişisel verilerin hukuka aykırı olarak verilmesi, yayılması veya ele geçirilmesi suçu" herkes tarafından işlenebilen suçlar olduğundan iştirak hükümleri bakımından özellik göstermez. TCK'da yer alan iştirakle ilgili hükümler uygulama alanı bulacaktır.[429]

Suçun birden fazla kişi tarafından müştereken ve fiil üzerinde ortak hâkimiyet kurmak suretiyle işlenmesi halinde, bu kişilerin her biri TCK'nın 37/1 maddesi uyarınca suçtan müşterek fail olarak sorumlu tutulacaklardır. Eğer suç, yaptığı fiilin hukuki anlam ve sonuçlarını veya suç olduğunu anlamayan bir kişi, örneğin bir çocuğun veya akıl hastasının araç olarak kullanılması suretiyle işlenmesi halinde, bu kişi veya kişileri araç olarak kullanan kişi veya kişiler, TCK'nın 37/2 maddesi gereği suçun işlenmesinden dolaylı fail olarak sorumlu olacaktır. Aklında suç işleme fikri olmayan bir kişi veya kişileri, kişisel verileri kaydetme suçunu işlemeye ikna eden kişi veya kişiler azmettiren (TCK m. 38), bu suçu işlemek isteyen kişi veya kişilerin suçu

[424] Yargıtay 12. CD., E: 2016/12565, K: 2017/12892, T: 20.11.2017
[425] Koca/Üzülmez, age, s. 597, Dülger, age, s. 762.
[426] Yaşar/Gökcan/Artuç, age, s. 4464; Dülger, age, s. 762; Özbek/Doğan/Bacaksız, age, s. 605.
[427] Yaşar/Gökcan/Artuç, age, s. 4465.
[428] Akdağ, age, s. 147.
[429] Özbek/Doğan/Bacaksız, age, s. 596, Dülger, age, s. 729.

işlemesini kolaylaştıran, yardım eden kişi veya kişiler, yardım eden (TCK m. 39) olarak sorumlu olacaklardır.[430]

TCK 137. madde kapsamında, iştirak edenlerin kamu görevlisi veya belli bir sanat veya meslek sahibi olmaları ve suçun kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle veya belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenmesi halinde, iştirak edenlere verilecek ceza daha ağır olacaktır. [431] Bu durumda görünüşte özgü suç söz konusu olacağından, suçun faili olabilmek için gerekli özelliğe haiz olmayan kişi veya kişiler, burada kamu görevlisi veya belli bir sanat veya meslek sahibi olmayan kişiler, suçun işlenmesinden müşterek fail olarak değil, azmettiren veya yardım eden olarak sorumlu olacaklardır.[432] Kamu görevlisi veya bir meslek veya sanat sahibi olmayan kişi veya kişiler, TCK'nın 135. maddesine göre, kamu görevlisi veya bir meslek veya sanat sahibi olan fail ve failler ise TCK'nın 137. maddesindeki nitelikli hale göre cezalandırılacaklardır.[433]

"Kişisel verilerin yok edilmemesi suçu" bakımından öğretide her türlü iştirakin gerçekleşebileceğine dair bir görüş[434] olsa da, hâkim görüşe göre sadece sistem içinde verileri yok etmekle yükümlü olan kişiler tarafından işlenebilen özgü bir suçtur.[435] Failinin ancak belli özellikler taşıyabilen kişiler olabileceği kabul edilen suç tipi özgü suç olarak tanımlanmaktadır. Bu özellikler; cinsiyet gibi doğal veya failin mesleği gibi hukuki nitelikler şeklinde iki kategori altında sınıflandırılabilirler.[436] Dolayısıyla TCK'nın 40/2 maddesi gereğince, bu suçun işlenişine iştirak eden diğer kişiler, suçun icrasına yaptıkları katkı ne olursa olsun suçun faili olamayacağından, azmettiren ya da yardım eden olarak sorumlu tutulur.[437]

---

[430] Sedat Bakıcı, **5237 Sayılı Yasa Kapsamında Ceza Hukuku Genel Hükümleri**, 2. Baskı, Adalet Yayınevi, Ankara, 2008, s. 333, Gültekin, age, s. 149, Korkmaz, age, s. 424.
[431] Kangal, age, s. 85.
[432] Artuk/Gökcen/Alşahin/Çakır, age, s.640, Koca/Üzülmez, age, s. 441.
[433] Gültekin, age, s. 150.
[434] Özbek, **TCK İzmir Şerhi**, s. 970, Özbek/Doğan/Bacaksız, age, s. 605.
[435] Parlar/Hatipoğlu, age, s. 2103, Hafızoğulları/Özen, age, s. 280, Dülger, age, s. 762, Koca/Üzülmez, age, s. 597.
[436] Demirbaş, age, s. 556.
[437] Dülger, age, s. 762, Yaşar/Gökcan/Artuç, age, s. 4136, Parlar/Hatipoğlu, age, s. 2103, Hamide Zafer **Ceza Hukuku Genel Hükümler**, Beta Yayımcılık, İstanbul, 2015, s. 403.

3.4.3.İçtima

Bu suçların, bir suç işleme kararı kapsamında aynı kişiye karşı birden fazla kez işlenmesi durumunda zincirleme suç hükümleri uygulanabilecektir.[438] "Kişisel verilerin kaydedilmesi", "kişisel verilerin verilmesi, yayılması ya da ele geçirilmesi" veya "kişisel verileri yok etmeme" suçlarının aynı kişiye ait kişisel verilere ilişkin olarak farklı zamanlarda birçok defa işlenmesi halinde faile tek ceza verilecektir. Bu durumda ceza TCK'nın 43/1 maddesine göre, dörtte birinden dörtte üçüne kadar artırılacaktır.[439] Ancak "kişisel verileri yok etmeme suçu" bakımından aynı kişiye ilişkin aynı olaydan elde edilmiş kişisel verilerin, sistemden uzun süre yok edilmemesi, tek suç oluşturacak ve bu durumda zincirleme suç hükümleri uygulanmayacaktır.[440]

Bunun yanında "kişisel verilerin kaydedilmesi", "kişisel verilerin verilmesi, yayılması ya da ele geçirilmesi" veya "kişisel verileri yok etmeme" suçları, fail tarafından, birden fazla kişiye ait kişisel verilere ilişkin olarak tek bir fiille de işlenebilir. Bu durumda aynı neviden fikri içtima söz konusu olacak ve ceza TCK'nın 43/2 maddesine göre belirlenecektir.[441]

Farklı neviden fikri içtima ile suçların işlenmesi de mümkündür. Örneğin kişisel verilerin herkesin ulaşabileceği internet sayfasına kaydedilmesi veya yayılması halinde 135. ve 136. madde kapsamında suç oluşacak, fikri içtima hükmü uyarınca daha ağır cezayı gerektiren TCK'nın 136. maddesi hükmü uygulanacaktır[442]. Ancak önce kişisel veriler kaydedilip daha sonra da yayılır ya da verilirse bu durumda iki ayrı hareket gerçekleştiğinden gerçek içtima hükümleri uygulanacaktır.[443] Kişisel verilerin verilmesi ya da yayılması fiilinin aynı zamanda TCK'nın 125. maddesinde yer alan

---

[438] "Sanığın aynı mağdurla ilgili fotoğrafı hem ... Dergisinde, hem ... Gazetesinde ve hem de internetteki … sitesinde hukuka aykırı olarak yayınlaması karşısında, TCK'nın 43/1. maddesine göre cezasının artırılması gerekeceği", Yargıtay 4.CD., E: 2011/11771, K: 2013/1376, T: 24.01.2013

[439] "Birbirine yakın zaman dilimi içerisinde ve bir suç işleme kararının icrası kapsamında, katılanın arama kayıtlarını, birden fazla kişiye veren sanık hakkında, zincirleme suç nedeniyle artırım yapılması gerekir." Yargıtay 12.CD., E: 2014/22994, K: 2015/2630, T: 16.02.2015, "Sanığın aynı mağdurla ilgili fotoğrafı hem ... Dergisinde, hem ... Gazetesinde ve hem de internetteki … sitesinde hukuka aykırı olarak yayınlaması karşısında, TCK'nın 43/1. maddesine göre cezasının artırılması gerekeceği", Yargıtay 4.CD., E: 2011/11771, K: 2013/1376, T: 24.01.2013.

[440] Özbek/Doğan/Bacaksız, age, s. 591; Yaşar/Gökcan/Artuç, age, s. 4466.

[441] Sarıusta, agt, s. 137, Korkmaz, age, s. 425, Koca/Üzülmez, age, s. 598.

[442] Özbek/Doğan/Bacaksız, age, s. 603.

[443] Kuşkonmaz, agt, s. 149, Sarıusta, agt, s. 138.

hakaret suçunu da mümkün kılabilecektir. Yine aynı hareketle birden fazla suç işlendiğinden farklı neviden fikri içtima söz konusu olacaktır[444]

Fail, kişisel verileri bulunduğu sistemden silip başka bir yere kopyalarsa, bu durumda kişisel verileri yok etmeme suçu ve kişisel verilerin hukuka aykırı olarak kaydedilmesi suçu oluşur.[445] Çünkü veriler, bulunduğu sistemden silinse de başka yere kaydedildiği için başkaları tarafından ulaşılabilir olduğundan, yok etme yükümlülüğü yerine gelmemiş olur. Başka yere kaydetme ise hukuka aykırı bir kaydetme olur. Bir bilişim sistemindeki kişisel verilerin silinmesi hâlinde, o verilere tekrar erişim mümkün olabileceğinden kişisel verilerin yok edilmemesi yükümlülüğü yerine getirilmemiş olacaktır. Suçun oluşmasının engellenmesi için, bu verilerin bilişim sistemlerinden geri döndürülemeyecek şekilde özel programlarla silinmesi gerekmektedir. Ancak verileri silmekle yükümlü olan kişinin, bu verilerin sonradan tekrar kullanılabileceğini bilmemesi hâlinde, suç taksirle işlenemeyeceğinden cezai sorumluluğu doğmayacaktır.

Fail, verileri sistemden silmemekle birlikte bu verileri bir başkasına verir ya da yayarsa bu durumda hem kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçu hem de verileri yok etmeme suçu oluşacaktır. Fail gerçek içtima hükümlerince iki suçtan da ayrı cezalandırılacaktır.[446]

"Verileri hukuka aykırı olarak verme, yayma veya ele geçirme suçu" birden fazla fiille işlenmesi durumunda gerçek içtima hükümleri uygulanacak ve fiil sayısı kadar suç oluştuğu kabul edilecektir. Fail bir kişiye cebir uygulayarak o kişinin kişisel verilerini ele geçirmişse hem cebir ilgili suçtan cezalandırılacaktır.[447]

Öğretide kişisel verilerin yok edilmemesi suçunun, "*ihmal suretiyle görevi kötüye kullanma*" suçunun özel bir tipini oluşturduğunu söyleyen görüşler bulunmaktadır.[448] Ancak görevi kötüye kullanma suçu, kamu görevlileri tarafından işlenebilen bir suçtur. Verileri yok etmeme suçu ise kamu görevlileri dışında verileri

---

[444] Sevük, age, s. 258.
[445] Aksi görüş için bkz. Erdoğan, agm, s. 626. Bu görüşe göre, veriler sistemden silindiği için verileri yok etmeme suçu oluşmaz.
[446] Yaşar/Gökcan/Artuç, age, s. 4466.
[447] Dülger, age, s. 749.
[448] Şen, age, s. 720.

sistem içinde yok etmekle görevlendirilen kişilerce de işlenebildiği için, bu görüşe katılmıyoruz.[449]

TCK'nın 133. maddesinde düzenlenen "kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması" suçunun 1. fıkrasında "*kişiler arasındaki aleni olmayan konuşmaları, taraflardan herhangi birinin rızası olmaksızın bir aletle dinleyen veya bunları bir ses alma cihazı ile kaydedilmesinden*", 3. fıkrasında ise ifşa edilmesinden bahsedilmektedir. İlgili suçta, "kişiler arasındaki aleni olmayan konuşmaların kaydedilmesinden veya ifşa edilmesinden" bahsedildiğinden, kişisel veri kavramının korunmasını amaçlayan TCK'nın 135. ve 136. maddelerindeki suçlara göre özel norm durumundadır. Bu suç işlenirken konuşmaların kaydedilmesiyle beraber kişisel verilerin de kaydedilmesi veya ifşa edilmesi durumunda, TCK'nın 133. maddesindeki düzenleme, TCK'nın 135. ve 136. maddesindeki düzenlemelere göre özel norm olduğundan, TCK'nın 133. maddesi hükmü uygulanacaktır.[450]

"Haberleşmenin gizliliğini ihlal" başlıklı TCK'nın 132. maddesinin 1. ve 2. fıkrasında ise "gizlilik ihlali haberleşme içeriklerinin kaydı veya ifşası" düzenlenmiştir. Düzenlenen suçlar işlenirken, kişisel veri niteliğine sahip verilerin de kaydedilmesi veya ifşa edilmesi durumunda, yukarıdaki açıklamalar ışığında, TCK'nın 132. maddesi yalnızca haberleşme içeriklerini kapsadığından, TCK'nın 135. ve 136. maddelerindeki suçlara göre özel normdur. Bu sebeple TCK'nın 132. maddesi uygulama alanı bulacaktır. Farklı neviden fikri içtima da bu suç için söz konusu olabilecektir.

TCK'nın 134. maddesinde yer alan "özel hayatın gizliliğini ihlal suçu" işlenirken, kişinin özel hayatı dışında kalan kişisel verilerinin kaydedilmesi durumunda, farklı neviden fikri içtima hükümleri uygulanacaktır.[451] TCK'nın 244. maddesinde yer alan "Sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu" işlenirken de kişisel veri niteliğine sahip bilgilerin kaydedilmesi durumunda da farklı neviden fikri içtima ortaya çıkacaktır.[452]

---

[449] Sarıusta, agt, s. 140.
[450] Gültekin, age, s. 153.
[451] Dülger, age, s. 729.
[452] Titrek, agt, s. 83.

TCK'nın 239. maddesinde yer alan "ticarî sır, bankacılık sırrı veya müşteri sırrı niteliğindeki bilgi veya belgelerin açıklanması suçu" ile "Kişisel verilerin kaydedilmesi" ve "Kişisel verileri hukuka aykırı olarak verme, yayma veya ele geçirme" suçları arasında da fikri içtima uygulanabilecektir. Müşteri sırrı niteliğindeki kişisel veriyi herkesin erişebileceği bir internet sitesine kaydeden fail aynı hareketle bir kişisel veriyi kaydetmiş ve müşteri sırrı niteliğindeki bilgiyi ifşa etmiş olacağından TCK'nın 239. maddesi ve TCK'nın 135. veya 136. maddeleri arasında farklı neviden fikri içtima hükümleri uygulanacaktır.[453]

Ayrıca şartlarının olması durumunda TCK 136. maddesinde yer alan "kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçu" ile 135. madde arasında da farklı neviden fikri içtima hükümlerinin uygulanması da mümkündür. Bu durumda TCK'nın 44. maddesine göre, fail, en ağır cezayı gerektiren suçtan dolayı cezalandırılacaktır.[454]

"Kişisel verilerin kaydedilmesi" ve "Kişisel verileri hukuka aykırı olarak verme, yayma veya ele geçirme" suçları bakımından gerçek içtima hükümleri uygulanabilecektir. Fail, cebir veya tehdit yoluyla kişisel verileri kaydetmeye mecbur bırakmış veya ele geçirmişse, bu durumda, kişisel verilere ilişkin suçlara ek olarak cebir (TCK m. 108) veya tehdit (TCK m. 106) suçlarından da ayrı ayrı cezalandırılacaktır.[455]

TCK'nın 244/2. maddesinde "*Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır*." demek suretiyle 136. maddede yer alan düzenlemeye benzer bir hüküm getirmiştir. Her iki düzenleme arasındaki farklar; 136. maddedeki düzenlemenin sadece kişisel verileri kapsarken, 244. maddedeki düzenlemenin tüm verileri kapsaması ve 136. maddedeki suç bilişim sistemleri yanında başka yollarla işlenebilirken, 244. maddedeki suçun ancak bilişim sistemleri vasıtasıyla işlenebilmesidir. 244. madde kapsamında işlenen suçta, başka bir yere gönderilen verilerin kişisel veri olması durumunda, hem 136.

[453] Kangal, age, s. 86.
[454] Korkmaz, age, s. 367.
[455] Özbek/Doğan/Bacaksız, age, s. 596.

maddede düzenlenmiş suç, hem de 244. maddede düzenlemiş suç oluşacaktır. Fail de, tek fiille Kanun'un iki ayrı hükmünü ihlal ettiğinden dolayı, hakkında farklı neviden fikri içtima hükümleri uygulanarak, en ağır olan suçun cezasıyla cezalandırılacaktır.[456]

TCK'nın 245/1. maddesi[457] hükmünce başkasına ait banka ya da kredi kartının ele geçirilmesi bu suçun bir unsuru olduğundan bileşik suç söz konusu olacaktır. TCK'nın 42. maddesi gereğince bileşik suç söz konusu olduğundan, suç tek fiil ile işlenmiş sayılacak ve bu suçlar arasında içtima hükümleri uygulanmayacaktır. Bu sebeple TCK'nın 245/1. maddesi kapsamında kendisine yarar sağlayan kimse sadece bu maddeden dolayı cezalandırılacak, TCK'nın 136. maddesinden ayrıca cezalandırılmayacaktır.[458] TCK'nın 243. maddesinde "bilişim sistemine girme suçu" düzenlenmiştir. Bu suç ile TCK'nın 136. maddesi arasında gerçek içtima hükümlerinin uygulanması mümkündür.

[456] Korkmaz, age, s. 496.

[457] "Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır."

[458] "Dosya kapsamına göre, sanık hakkında katılanlar ... ve ...'a karşı kişisel verileri hukuka aykırı ele geçirmek suçlarından kurulan hükümlerde, ele geçirilen katılanlara ait kart bilgilerini kullanarak alışveriş yapmak eylemlerinin kül halinde, mağdur sayısınca TCK'nın 245/1. maddesindeki suçu oluşturacağı gözetilmeden, aynı Kanun'un 136. maddesi uyarınca ayrıca mahkumiyet hükmü kurulmasında isabet görülmemiş olup…" Yargıtay 12. CD., E: 2017/11578, K: 2018/1164, T:07.02.2018.

SONUÇ

Teknolojinin gelişmesi ve dünya geneline yayılmasıyla birlikte "belirli veya belirlenebilir nitelikteki bir kişiye ilişkin her türlü bilgi" olarak tanımlanan kişisel verilerin kullanım alanı, gerek kamu kuruluşları gerekse özel teşebbüslerce duyulan ihtiyaç nedeniyle oldukça artmıştır. Eskiden daktiloyla veya kâğıt üzerine kaydedilen kişisel verilere ulaşım imkânı hesaba katıldığında günümüz teknolojisiyle bu verilere ulaşım cep telefonu, bilgisayar gibi aygıtlarla kolay bir hale gelmiştir. Üstelik kişisel verilerin kıtalararasında dahi hızlı bir şekilde aktarılabilir olması, veri sahibinin verisi üzerindeki kontrolünü zorlaştırmıştır. Dolayısıyla veri sahibinin özel yaşamının gizliliği ve hukuki güvenliğinin sağlanması için kişisel verilerin korunmasına ilişkin olarak hukuki düzenleme yapılması ihtiyacı artmıştır. Kişisel verilerin korunması hakkı, anayasal çerçevede, kişisel verilerin işlenmesi sebebiyle kişinin uğrayacağı tehlikelere karşı koruma sağlayan bir haktır. Bu hak, kişisel verilerin işlenmesi durumunda kişilerin özel yaşamının gizliliğini koruması yanı sıra, kişisel verilerin güvenle paylaşılabilmesini amaçlamaktadır. Böylece veri sahibi, verileri üzerinde özgürce tasarrufta bulunabilecek; temel hak ve özgürlükleri korunacaktır.

Kişisel verilerin korunması alanındaki ilk hukuki düzenlemeler, 1970'li yıllarda Avrupa'da ortaya çıkmıştır. Hızla gelişen teknolojiye karşı bireyin özel yaşamının korunması düşüncesinin etkili olduğu bu düzenlemelerde, ilk olarak bireyi devlete karşı koruma amaçlanmıştır. Bu çerçevede veri koruma kanununa ilişkin ilk çalışma 1970'de Almanya'nın Hessen eyaletinde yapılmıştır. Bu düzenlemeleri, Federal Almanya ve Fransa Veri Koruma Kanunları takip etmiştir. Bunun yanında uluslararası belgelerde de kişisel verilerin korunması garanti altına alınmaya başlamıştır. Temel hak ve özgürlüklerin sağlanmasını hedefleyen en temel uluslararası belgelerden biri olarak kabul gören "Avrupa İnsan Hakları Sözleşmesi"nde kişisel verilerin korunmasına yönelik özel bir hüküm bulunmamaktadır. Fakat Avrupa İnsan Hakları Mahkemesi, bu hususu özel hayatın ve aile hayatının gizliliğinin korunduğu Sözleşme'nin 8. maddesi kapsamında kabul ederek verdiği kararlarla kişisel verileri korumuştur. Bu konuda OECD Kılavuz İlkeleri, BM Rehber İlkeleri, 108 Sayılı Direktifi, 95/46/AT sayılı Direktif, 2002/58/AT sayılı Direktif, Genel Veri Koruma

Tüzüğü gibi uluslararası kaynaklar da kişisel verilerin korunmasında büyük rol oynamaktadır.

Türk hukukunda kişisel verilerin korunması hakkı, Anayasa'nın 20. maddesine 07.05.2010 tarihinde 5982 sayılı Kanun'la eklenen fıkrayla Anayasal güvence altına alınmıştır. Türkiye'de kişisel verilerin korunmasına yönelik özel bir kanuni düzenleme ise uzun yıllar yapılamamıştır. 07.04.2016 tarihinde KVKK'nın yürürlüğe girmesiyle Anayasa'nın 20. maddesindeki kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği hükmü ve 108 sayılı Avrupa Konseyi Sözleşmesi'nin 4. maddesinde belirtilen yükümlülük yerine getirilmiştir.

AB'de Almanya gibi bazı ülkelerde kişisel verilerin korunmasına ilişkin suçlar kişisel verilerin korunmasıyla ilgili özel kanunlarda yer alırken, Fransa gibi bazı ülkelerde ise bu suçlar genel ceza kanunlarında düzenlenmiştir. Ülkemizde de ikinci yol benimsenerek TCK'nın 135, 136 ve 138. maddelerinde kişisel verileri korunmaya yönelik suçlara yer verilmiştir. İlgili suç tipleri, kişisel verilerin kaydedilmesi, verilerin hukuka aykırı olarak verilmesi veya ele geçirilmesi, verilerin yok edilmemesi olarak sıralanabilecektir. Bu suç tipleri incelenirken, 2016 yılında yürürlüğe giren 6698 sayılı KVKK ile birlikte değerlendirilmesi gerektiğinden çalışmamız boyunca ilgili suç tipleri bu kanun kapsamında değerlendirilerek incelenmiştir. Nitekim 6698 sayılı KVKK da kişisel verilerin korunması hakkına karşı işlenecek suçlar bakımından TCK'yı işaret etmiştir.

TCK'da düzenlenen suç tipleriyle KVKK arasındaki uyumsuzluklarla ilgili doktrindeki eleştirilere çalışmamız boyunca yer verilmiştir. Buna ilişkin olarak kişisel verilerin korunmasına yönelik bir kanunun olmadığı 2004 yılında hazırlanan ve yürürlüğe giren TCK ile 2016 yılında yürürlüğe giren KVKK arasındaki farklılıklar doğal olmasına rağmen, bu farklılıkların giderilmesi gerekmektedir. Örnek olarak KVKK'nın 6. maddesi ile TCK'nın 135. maddesi arasında özel nitelikli veri kategorileri bakımından bazı farklılıklar olup, ayrıca hukuka aykırılık unsuru bakımından da farklı bir düzenleme mevcuttur.

Çalışmamız boyunca yapılan tüm bu eleştirilere ve düzeltilmesi gereken hususlara rağmen, ülkemizde KVKK'nın yürürlüğü girmesi kişisel verilerin korunmasına yönelik olarak büyük adım olarak görülmektedir. Ayrıca bu kanunun

uygulanmasına yönelik olarak çıkarılan yönetmeliklerin de kişisel verilerin korunmasına hizmet etmektedir. İlerleyen dönemlerde kanunun uygulanması ve toplum bilincinin artmasıyla ihtiyaçlara cevap veren kanuni düzenlemelerin yapılacağına inancımız tamdır.

KAYNAKÇA

Akdağ, Hale, Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması, Adalet Yayınevi, Ankara, 2013.

Akgül, Aydın, Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması, 2. Baskı, Beta Yayıncılık, İstanbul, 2016.

Akıntürk, Turgut / Ateş, Derya, Medeni Hukuk, 25. Baskı, Beta Yayınevi, İstanbul, 2019.

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

Albayrak, Mustafa, "Kişisel Verilerin Kaydedilmesi Suçu", *HUKAB Dergisi*, S. 5, Nisan- Haziran 2013, s. 9-23.

Ankara HBV Üniversitesi Türk Ceza Hukuku Uygulama ve Araştırma Merkezi, Türk Ceza Hukuku Mevzuatı – Cilt 1 (Kanunlar), 23. Baskı, Seçkin Yayıncılık, Ankara, 2019.

Arslan, Çetin. "Avrupa Birliği Hukukunda Kişisel Verilerin Üçüncü Ülkelere Aktarılması", *Galatasaray Üniversitesi Hukuk Fakültesi Dergisi: Prof. Dr. Köksal Bayraktar'a Armağan*, C.1, 2010, 454.

Arslan, Çetin. "Vergi Mahremiyetini İhlal Suçu (VUK md. 362)", *Hacettepe Hukuk Fakültesi Dergisi*, 3(2) 2013, 15-30.

Artuk, Mehmet Emin; Gökcen, Ahmet; Alşahin, Mehmet Emin; Çakır, Kerim, Ceza Hukuku Genel Hükümler, 14. Baskı, Adalet Yayınevi, Ankara, 2021.

Artuk, Mehmet Emin–Gökcen, Ahmet, Ceza Hukuku Özel Hükümler, 19. Baskı, Adalet Yayınevi, Ankara, 2021.

Atak, Songül. "Avrupa Konseyi'nin Kişisel Veriler Açısından Sağladığı Temel Güvenceler", *Türkiye Barolar Birliği Dergisi*, Sayı:87, 2010, 90-120.

Atasoy, Kemal. "Kişilik Hakkı Kapsamında Sosyal Medyada Kişisel Verilerin Korunması Ve Veri Sahibinin Rızası", *Marmara Üniversitesi Hukuk Araştırmaları Dergisi*, Cilt:22, Sayı:3, 2016, 269-301.

Aydın, Sedat Erdem, AİHM İçtihatları Bağlamında Kişisel Verilerin Kaydedilmesi Suçu, İstanbul, 2015.

Ayözger Öngün, A. Çiğdem, Kişisel Verilerin Korunması Hukuku, Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dâhil, Genişletilmiş 2. Baskı, Beta Yayıncılık, İstanbul, 2019.

Bakıcı, Sedat, 5237 Sayılı Yasa Kapsamında Ceza Hukuku Genel Hükümleri, 2. Baskı, Adalet Yayınevi, Ankara, 2008.

Başalp, Nilgün, Kişisel Verilerin Korunması ve İnternet, İnternet ve Hukuk, Derleyen Yeşim M. Atamer, İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2004.

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

Bayram, Zeynep, "Suç Öncesi ve Sonrası Kişisel Veri Toplama Yetkisi", Bahçeşehir Üniversitesi, Sosyal Bilimler Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, İstanbul, 2009.

Bük, Alaattin, Bilişim Alanında Kişisel Verilerin Korunması, 1. Baskı, Seçkin Akademik ve Mesleki Yayınları, Ankara, 2018.

Centel, Nur; Zafer, Hamide; Ceza Muhakemesi Hukuku, 13. Baskı, Beta Yayımcılık, İstanbul, 2016.

Çekin, Mesut Serdar, Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku, 3. Baskı, On İki Levha Yayıncılık, İstanbul, 2020.

Çelik, Yeşim. "Özel Hayatın Gizliliğinin Yansıması Olarak Kişisel Verilerin Korunması ve Bu Bağlamda Unutulma Hakkı", *Türkiye Adalet Akademisi Dergisi,* Yıl:8, Sayı:32, Ekim 2017, 387-406.

Çırak, Ezgi, "Dijital Çağda Sonsuza Kadar Hatırlamaya Karşı: Unutulma Hakkı", *CHD*, 2018, Sayı 36, s. 161-189.

Dağ, Güray, "Kişisel Verilerin Ceza Muhakemesi Hukukunda Delil Olarak Kullanılması", Marmara Üniversitesi Sosyal Bilimler Enstitüsü, Yayımlanmamış Doktora Tezi, İstanbul, 2011.

Demirbaş, Timur, Ceza Hukuku Genel Hükümler, 12. Baskı, Seçkin Yayıncılık, Ankara, 2017.

Çokmutlu, Metin, "Türk Ceza Hukukunda Kişisel Verilerin Korunması", Kocaeli Üniversitesi, Sosyal Bilimler Enstitüsü, Yayımlanmamış Doktora Tezi, Kocaeli, 2014.

Dinç, Engin, "Kişisel Verilerin Korunmasında Uluslararası Düzenlemeler ve Türkiye'nin Durumu", Diyarbakır Dicle Üniversitesi, Sosyal Bilimler Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, 2006.

Dursun, İsmail, "Türk Ceza Kanunu'nda Verileri Yok Etmeme Suçu", *Kocaeli Üniversitesi Hukuk Fakültesi Dergisi*, S: 10, Seçkin Yayıncılık, Ankara 2014, s. 9-37.

Dülger, Murat Volkan, Kişisel Verilerin Korunması Hukuku, 3. Baskı, Hukuk Akademisi Yayınları, İstanbul, 2020.

Ekici Şahin, Meral, Ceza Hukukunda Rıza, 1. Baskı, On İki Levha Yayıncılık, İstanbul, 2012, s. 96.

Erdoğan, Yavuz, "Kişisel Verilerin Korunması Bakımından Türk Ceza Kanunu Hükümlerinin Değerlendirilmesi (Madde 135, 136, 137, 138)", *Erciyes Üniversitesi Hukuk Fakültesi Dergisi*, S: 2, 2013, s. 569-632.

Ersoy, Uğur, "Bir İnsan Hakları Kavramı Olarak Kişisel Verilerin Korunması", Gazi Üniversitesi, Sosyal Bilimler Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, Ankara, 2009.

Eyrenci, Öner-Taşkent, Savaş- Ulucan, Devrim, Bireysel İş Hukuku, 8. Baskı, Beta Yayımcılık, İstanbul, 2017.

Gözübüyük, A. Şeref; Gölcüklü, Feyyaz, Avrupa İnsan Hakları Sözleşmesi ve Uygulaması, Turhan Kitapevi, Ankara, 2009.

Gültekin, Nil Melek, "Kişisel Verilerin Ceza Hukuku Yönünden Korunması", Galatasaray Üniversitesi, Sosyal Bilimler Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, İstanbul, 2012.

Gür, İkbal, "Kişisel Verilerin Korunması Hususunda AB ile ABD Arasında Çıkan Uyuşmazlıklar ve Çözüm Yolları", Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, Ankara, 2009.

Gürsel, İlke, "İşçinin Kişisel Verilerinin Korunması Hakkı", Dokuz Eylül Üniversitesi, Sosyal Bilimler Enstitüsü, Yayımlanmamış Doktora Tezi, İzmir, 2016.

Hafızoğulları, Zeki; Muharrem Özen, Türk Ceza Hukuku Özel Hükümler Kişilere Karşı Suçlar, 5. Baskı, Usa Yayıncılık, Ankara, 2016

Hakeri, Hakan, Ceza Hukuku Genel Hükümler, 24. Baskı, Adalet Yayınevi, Ankara, 2021.

Hakeri, Hakan ve Ünver, Yener; Ceza Muhakemesi Hukuku, 15. Baskı, Adalet Yayınevi, Ankara, 2019.

Hatipoğlu, Selami, "Kişisel Verilerin Korunması ve İdarenin Sorumluluğu", Trakya Üniversitesi Sosyal Bilimler Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, Edirne, 2019.

Helvacı, Serap, Gerçek Kişiler, 6. Basım, Legal Yayıncılık, İstanbul, 2016.

Henkoğlu, Türkay, Bilgi Güvenliği ve Kişisel Verilerin Korunması, Ankara, 2015.

Kangal, Zeynel T., Kişisel Verilerin Ceza ve Kabahatler Hukukunda Korunması, 1. Baskı, On İki Levha Yayıncılık, İstanbul, 2019.

Karabulut, Ramazan, "Kişisel Verilerin Korunması ve Kolluk Hizmetleri", Dicle Üniversitesi, Sosyal Bilimler Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, Diyarbakır, 2014.

Ketizmen, Muammer, Türk Ceza Hukuku'nda Bilişim Suçları, Adalet Yayınevi, Ankara, 2008.

Kılınç, Doğan, "Anayasal Bir Hak Olarak Kişisel Verilerin Korunması", *AÜHFD*, C. 61, S. 3, 2012, s.1089-1170.

Kişisel Verileri Koruma Kurumu, 6698 Sayılı Kanunda Yer Alan Temel Kavramlar. www.kvkk.gov.tr. (Erişim Tarihi: 23.01.2021)

Kişisel Verileri Koruma Kurumu, Kişisel Verilerin Korunması Kanunu ve Getirdikleri, Yayın No: 26.

Kişisel Verileri Koruma Kurumu, Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi.

Kişisel Verileri Koruma Kurumu, Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi, www.kvkk.gov.tr (Erişim Tarihi: 23.01.2021)

Kişisel Verileri Koruma Kurumu, Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik, Resmi Gazete, Tarih 28.10.2017 ve Sayı 30224.

Kişisel Verilerin Korunması Kurulu, Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik, Ankara, 2017.

Koca, Mahmut; İlhan Üzülmez, Türk Ceza Hukuku Özel Hükümler, 7. Baskı, Adalet Yayınevi, Ankara, 2020.

Korkmaz, İbrahim, Kişisel Verilerin Ceza Hukuku Kapsamında Korunması, 2. Baskı, Seçkin Akademik ve Mesleki Yayınları, Ankara, 2019.

Kök, Ahmet Nezih, "Bir Olgu Nedeniyle Tıp Uygulamalarında Mahremiyet İlkesi", Özel Yaşamın Gizliliği ve Kişisel Verilerin Kaydedilmesi, *Terazi Hukuk Dergisi*, C: 11, S: 119, 2016, s. 170-173.

Köse, Melike Aysun Kişisel Verilerin Kaydedilmesi Suçu (TCK m.135), 1. Baskı, Seçkin Yayıncılık, Ankara, 2018.

Kuşkonmaz, Elif Mendos, "Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması", İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, İstanbul, 2013.

Küzeci, Elif, Kişisel Verilerin Korunması, 4. Baskı, On İki Levha Yayıncılık, İstanbul, Mayıs 2020.

Manav, A. Eda. "İş İlişkisinde İşçinin Kişisel Verilerinin Korunması", *Gazi Üniversitesi Hukuk Fakültesi Dergisi*, C. 19, Y. 2015, Sayı 2, s. 130-142.

Metin, Yüksel "Avrupa Birliği Temel Haklar Şartı*", Ankara Üniversitesi Sosyal Bilimler Fakültesi Dergisi*, C.57, S.4, 2002, s. 35-63.

Oğuz, Habip. "Elektronik Ortamda Kişisel Verilerin Korunması, Bazı Ülke Uygulamaları Ve Ülkemizdeki Durum", *Uyuşmazlık Mahkemesi Dergisi*, Haziran 2014, Sayı:3, http://dergipark.gov.tr/download/article-file/155549 (Erişim Tarihi:15.08.2021).

Orta, Mesut, Elektronik İmza ve Uygulaması, Seçkin Yayıncılık, Ankara, 2005.

Özbek, Veli Özer; Doğan, Koray; Bacaksız, Pınar, Türk Ceza Hukuku Özel Hükümler, 15. Baskı, Seçkin Yayıncılık, Ankara, 2020.

Özbek, Veli Özer; Doğan, Koray; Bacaksız, Pınar; Tepe, İlker, Ceza Muhakemesi Hukuku, 8. Baskı, Seçkin Yayınevi, Ankara, 2016.

Özbek, Veli Özer, TCK İzmir Şerhi, Yeni Türk Ceza Kanunun Anlamı Özel Hükümler, C: 2, Seçkin Yayıncılık, Ankara, 2008.

Özdemir, Hayrunnisa, Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması, 1. Baskı, Seçkin Yayıncılık, Ankara, 2009.

Özkan, Oğulcan, Kişisel Verilerin Korunması, Yetkin Yayınları, Ankara, 2020.

Öztürk, Bahri; Tezcan, Durmuş; Erdem, Mustafa Ruhan; Sırma, Özge; Saygılar, Yasemin F. ve Alan, Esra; Nazari ve Uygulamalı Ceza Muhakemesi Hukuku, 11. Baskı, Seçkin Yayınevi, Ankara, 2017.

Parlar, Ali; Hatipoğlu, Muzaffer, Açıklamalı Yeni İçtihatlarla 5237 Sayılı Türk Ceza Kanunu Yorumu, 2. Cilt, 3. Baskı, Ankara, 2010.

Sarıusta, Kader, "Kişisel Verilerin Ceza Hukuku Yoluyla Korunması", Gaziantep Üniversitesi, Sosyal Bilimler Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, Gaziantep, 2018.

Sert, Şeyma, Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması, 1. Baskı, Seçkin Yayıncılık, Ankara, 2019.

Sevimli, K. Ahmet, İşçinin Özel Yaşamına Müdahalenin Sınırları, Legal Yayınevi, İstanbul, 2006.

Sevük, Handan Yokuş, Türk Ceza Hukuku Özel Hükümler, 3. Baskı, Adalet Yayınevi, Ankara: 2020.

Sözüer, Eren, Unutulma Hakkı, İnsan Hakları Hukuku Perspektifinden Bir İnceleme, İstanbul, 2017.

Şen, Ersan, Yeni Türk Ceza Kanunu Yorumu, Cilt: I, Vedat Kitapçılık, İstanbul, 2006.

Şimşek, Oğuz, Anayasa Hukukunda Kişisel Verilerin Korunması, Beta Yayınları, Ankara, 2008.

Taşkın, Şaban Cankat, "İnternete Erişim Yasakları ve Hukuka Aykırılıklar", Kocaeli Üniversitesi, Sosyal Bilimler Enstitüsü, Yayımlanmamış Doktora Tezi, Kocaeli, 2015.

Tezcan, Durmuş, "Özel Hayat Açısından Kişisel Verilerin Korunması", *İstanbul Kültür Üniversitesi Hukuk Fakültesi Dergisi*, 16(1), 2017, s.17-25.

Titrek, Gizem Büşra "Türk Ceza Hukukunda Kişisel Verilerin Korunmasına Yönelik Suçlar", Bursa Uludağ Üniversitesi, Sosyal Bilimler Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, Bursa, 2020.

Turan, Metin, Karşılaştırma Hukukta Kişisel Verilerin Korunması, 3. Baskı, Seçkin Yayınevi, Ankara, 2020.

Türk Dil Kurumu (TDK), Güncel Türkçe Sözlük, https://sozluk.gov.tr (Erişim Tarihi: 23.01.2021)

Uyarer, Sinem Göçmen, Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması, 2. Baskı, Seçkin Yayınevi, Ankara, 2020.

Uygun, Murat, "Avrupa Birliği'nin 95/46 Sayılı Veri Koruma Yönergesi Işığında Kişisel Verilerin Korunması", Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, Ankara, 2010.

Yakışır, Ceren, Türk Ceza Kanunu'nda Kişisel Verilerin Basın Yoluyla Açıklanması Suçu, 1. Baskı, On İki Levha Yayıncılık, İstanbul, 2019.

Yaşar, Osman; Hasan Tahsin Gökcan; Mustafa Artuç, Yorumlu Uygulamalı Türk Ceza Kanunu (Tamamen Gözden Geçirilmiş 2. Baskı), C: 3, Adalet Yayınevi, Ankara, 2014.

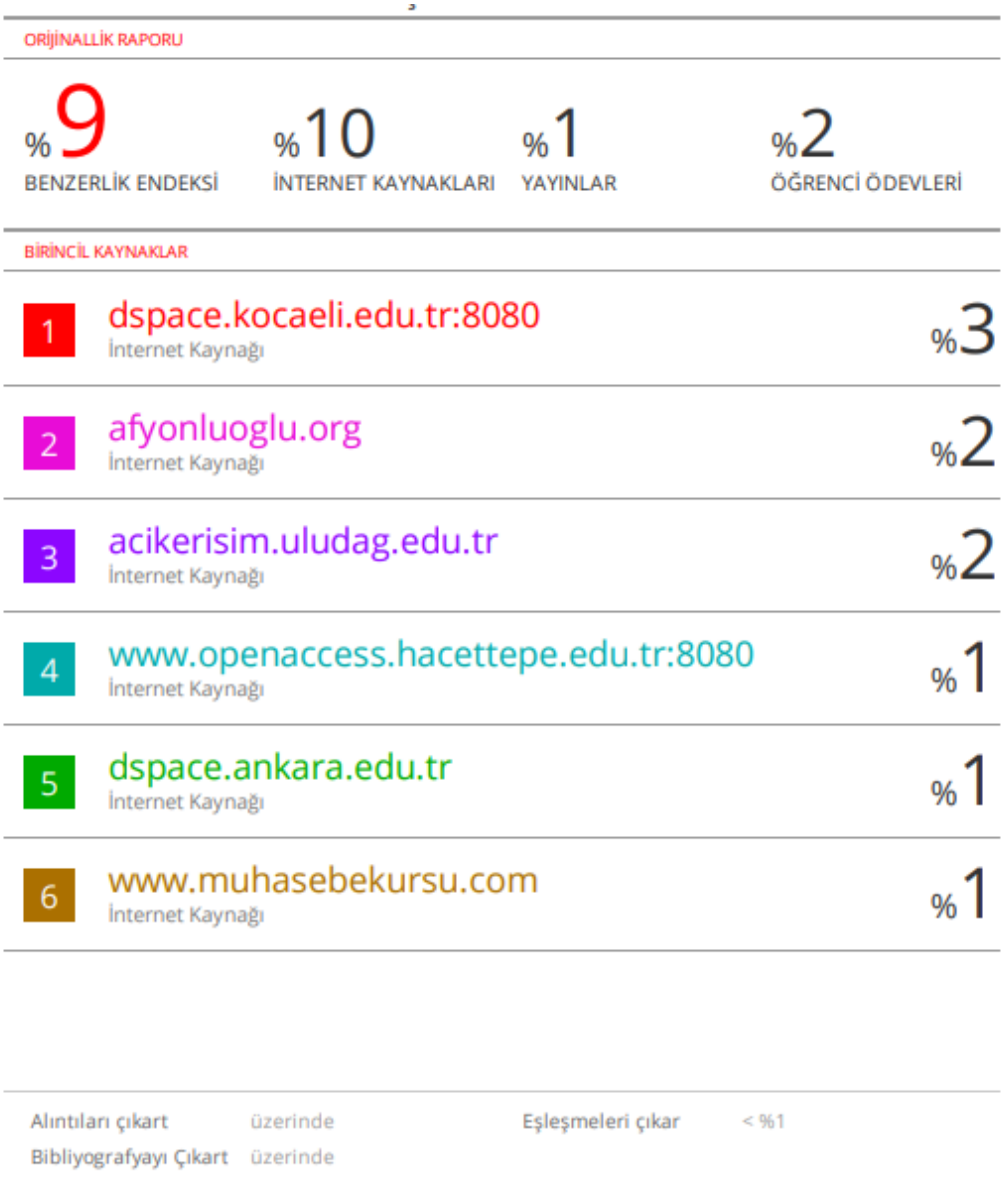
Yılmaz, Berrak, "Türk Anayasa Mahkemesi ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması", Hacettepe Üniversitesi, Sosyal Bilimler Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, Ankara, 2019.

Yılmaz, Sabire Sanem, "Tıp Alanında Kişisel Verilerin Hukuka Aykırı Olarak Verilmesinin Ceza Hukuku Açısından Değerlendirilmesi (Sır Saklama Yükümlülüğü Kapsamında)", Bahceşehir Üniversitesi, Sosyal Bilimler Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, İstanbul, 2014.

Yılmaz, Sacit, Türk Ceza Hukuku Sisteminde Siber Suçlar, Ankara, 2016.

Zafer, Hamide, Ceza Hukuku Genel Hükümler, Beta Yayımcılık, İstanbul 2015.

TURNITIN RAPORU



ORİJİNALLİK RAPORU

%9	%10	%1	%2
BENZERLİK ENDEKSİ	İNTERNET KAYNAKLARI	YAYINLAR	ÖĞRENCİ ÖDEVLERİ

BİRİNCİL KAYNAKLAR

1	dspace.kocaeli.edu.tr:8080 İnternet Kaynağı	%3
2	afyonluoglu.org İnternet Kaynağı	%2
3	acikerisim.uludag.edu.tr İnternet Kaynağı	%2
4	www.openaccess.hacettepe.edu.tr:8080 İnternet Kaynağı	%1
5	dspace.ankara.edu.tr İnternet Kaynağı	%1
6	www.muhasebekursu.com İnternet Kaynağı	%1

Alıntıları çıkart	üzerinde	Eşleşmeleri çıkar	< %1
Bibliyografyayı Çıkart	üzerinde		

ÖZGEÇMİŞ

Hasan Çağrı ŞAŞMAZ

Öğrenim Durumu:

Derece	**Alan**	**Üniversite**	**Yıl**
Lisans	Hukuk	Atılım Üniversitesi	2012-2017
Yüksek Lisans	Kamu Hukuku ABD	Atılım Üniversitesi	2018-2021

İş Deneyimi:

Çalıştığı Yer	**Görev**	**Yıl**
Ertul Hukuk Bürosu	Stajyer Avukat	2018-2019
Yılmaz & Şaşmaz Hukuk Bürosu	Avukat	2020-Halen

Yabancı Diller: İngilizce

Tarih: 08/10/2021