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

6698 KİŞİSEL VERİLERİN KORUNMASI KANUNU VE 5237 SAYILI TÜRK CEZA KANUNU KAPSAMINDA KİŞİSEL VERİLERİN KORUNMASI

Sinem GÖÇMEN UYARER
12511152

TEZ DANIŞMANI
Doç. Dr. Vesile SONAY EVİK

İSTANBUL – 2019

ÖNSÖZ

Tezime ilişkin olarak kişisel verilerin korunması konusunu seçmemin nedeni, başta Avrupa Birliği ülkeleri ve Amerika olmak üzere genel olarak bireylerin temel hak ve özgürlükleriyle doğrudan ilgili bir alan olmasıdır. Günümüzde, kişisel verilerin korunması hakkının, hem kişisel verileri yeni bir tür sermaye olarak gören özel sektöre karşı hem de bireylerin gözetlenmesi ve kayıt altına alınmak suretiyle fişlenmesi ihtimaline karşı kamu sektörüne karşı korunmasının oldukça önemli olduğu tartışmasız bir gerçektir. Ülkemizde de uzun yıllar bu konunun ihmal edilmiş olması bireylerin hem özel sektöre hem de devlete karşı gerçek bir korumadan mahrum kalmasına sebep olmuştur. 6698 sayılı Kişisel Verilerin Korunması Kanunu ile birlikte görece bir önem kazandığını düşündüğüm bu alanda alınacak daha çok yol olduğu açıktır.

Tezimi yazarken, her ne kadar uluslararası alanda sayısız kaynak olsa da ülkemizde bu alanda henüz yeteri kadar güncel kaynak bulunmaması, Kişisel Verilerin Korunması Kanunu'nun henüz yeni bir kanun olması ve dolayısıyla bireylerin bu kanuna başvuru hususundaki pratiğinin eksik olması sebebiyle uygulamaya yönelik bilgilerin azlığı tezimi yazarken bir anlamda zorluk yaşamama sebep oldu. Bu noktada yakın zamanda yayınlanan bazı kitaplardan ve sıklıkla güncel makalelerden yararlandığımı belirtirken, özellikle konuya ilişkin oldukça faydalı akademik makaleleri ile hem kişisel verilerin korunması hukukuna hem de tezimi yazarken yoluma ışık tutan Doç. Dr. Murat Volkan Dülger'e teşekkürü bir borç bilirim.

Hayatımın her alanında olduğu gibi tezimi yazdığım bu oldukça uzun süreçte de desteğini benden hiç esirgemeyen sevgili eşim Bahadır Cem UYARER'e ve ben tez yazarken hep masamın bir kenarında benimle birlikte oturan kedimiz Nasip'e, bu tezi tamamlayabilmem için İstanbul kütüphanelerinden Berlin'e kitaplar, makaleler gönderen ve aynı mesleği paylaşmaktan büyük mutluluk duyduğum Zeynep Ece

UYARER'e, bütün bu süreçte bitmek bilmeyen sorularımı cevaplayan ve desteğini hiç esirgemeyen değerli arkadaşım Av. Hanife Emine KARA'ya, tüm aileme ve elbette Berlin'de olmama rağmen kilometrelerce öteden tezime danışmanlık yapan, çalışmamın daha iyi bir noktaya gelmesi için değerli görüşlerini her daim paylaşan, bu süreçte bana destek olan ve yol gösteren değerli hocam Doç Dr. Vesile Sonay EVİK'e en içten teşekkürlerimi sunarım.

Sinem Göçmen UYARER
Berlin - 2019

İÇİNDEKİLER

KISALTMALAR

a.g.e: Adı geçen eser

a.g.m: Adı geçen makale

AAD: Avrupa Adalet Divanı

AB: Avrupa Birliği

ABD: Amerika Birleşik Devletleri

AHİM: Avrupa İnsan Hakları Mahkemesi

AHİS: Avrupa İnsan Hakları Sözleşmesi

AK: Avrupa Konseyi

AYMK: Anayasa Mahkemesi Kararı

B.N: Başvuru no

C.: Cilt

CMK: Ceza Muhakemesi Kanunu

KVKK: Kişisel Verilerin Korunması Kanunu

Çev.: Çeviren

d.n.: Dipnot

E.: Esas sayısı

f.: fıkra

haz.: Hazırlayan

SS: İnternet Servis Sağlayıcı

K.: Karar sayısı

k.t.: Karar tarihi

m.: Madde

MERNIS: Merkezi Nüfus dairesi Sistemi

OECD: Organisation for Economic Co-operation and Development Ekonomik Birliği ve Kalkınma Teşkilatı)

para: Paragraf

paras: paragraflar

R.G.: Resmî Gazete

s.: Sayfa

S.: Sayı

t.: tarih

TCK: Türk Ceza Kanunu

Vd: ve devamı

Yay: Yayınları ya da Yayınevi

TABLO LİSTESİ

Sayfa No

Université : **Université Galatasaray**

Institut : **Institut des Sciences Sociales**

Département : **Département de droit public**

Programme : **Programme de maîtrise en droit public avec thèse**

Directeur de recherche : **Doç. Dr. Vesile Sonay Evik**

Diplôme sollicité- Date : **DEA –Avril 2019**

RESUME

Dans le cadre de ce travail, ce dont il s'agit est un sujet qui était ignoré depuis des années en Turquie : la protection des données personnelles qui s'est fait une place dans les agendas de certaines institutions et surtout des entreprises qui s'occupent de traiter des données personnelles, avec la publication de la loi n* 6698 y relative, et l'entrée en vigueur du règlement général sur la protection des données.

Dans cet ouvrage, ce sujet s'examine en trois parties. La première partie dans laquelle l'approche consacré à la protection des données personnelles consiste à la considérer à la fois comme droit économique et dans le cadre des droits de l'homme, fait place aussi aux règlements juridiques, relatifs au sujet, faits par OCDE, le Conseil de l'Europe et l'Union européenne, et à des exemples de Turquie et des autres pays. Dans la deuxième partie, le même sujet se trouve être traitée dans le cadre de la loi n* 6698 sur la protection des données personnelles. Dernièrement, dans la troisième partie nous avons examiné les différents types d'actes criminels qui se définissent dans les limites du code pénal turc (la loi n*5237).

Avec ce travail, nous espérons de contribuer au droit à propos de la protection des données personnelles, qui était ignorée en Turquie malgré sa popularité à l'échelle mondiale.

Mots clés : Données personnelles, Protection des données personnelle, Loi sur (relative à) la protection des données personnelles, Code pénal turc

University : **Galatasaray University**

Institute : **Institute for Social Sciences**

Department : **Public Law Department**

Program : **Public Law Master Program**

Thesis Supervisor : **Assoc. Prof. Vesile Sonay Evik**

Type and Date of Thesis : **Master - April 2019**

ABSTRACT

This study examines and analyzes the subject of data protection which has been omitted for a very long time. Subsequent to Data Protection Code no.6698 and General Data Protection Regulation entered into force, data protection issue has been included by the agendas of both private and public entities which processing personal data within the scope of their services in our country.

In the context of this study, we examine data protection matter in three sections. At first, the approach to data protection is examined by referring to the economic approach and the human rights approach then, we review the legal instruments prepared by OECD, European Council and European Union and finally, we examine some examples of data protection law belongs to foreign jurisdictions and also our own jurisdiction. Secondly, data protection matter is examined within the scope of Data Protection Code no 6698 and the third and final section of the study, we review and discuss the criminal provisions related to data protection in the Turkish Criminal Code no.5237. As the matter is being examined, the Data Protection Code is also taken into consideration because the Data Protection Code refers to the criminal provisions of the Turkish Criminal Code.

We expect that our study will be helpful for data protection law issues which are completely new to Turkish Law whereas they have been discussed on a very long time over the World.

Key Words **:Personal Data, Protection of Personal Data, Data Protection Code, Turkish Criminal Code**

Üniversite : **Galatasaray Üniversitesi**

Enstitü : **Sosyal Bilimler Enstitüsü**

Anabilim Dalı : **Kamu Hukuku Anabilim Dalı**

Program : **Kamu Hukuku Tezli Yüksek Lisans Programı**

Tez Danışmanı : **Doç. Dr. Vesile Sonay Evik**

Tez Türü ve Tarihi : **Yüksek Lisans-Nisan 2019**

ÖZET

Çalışmamız kapsamında Türkiye'de uzun yıllardır ihmal edilmiş bir konu, kişisel verilerin korunması işlenmektedir. Kişisel verilerin korunması, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun ve Avrupa Birliği Genel Veri Koruma Tüzüğü'nün yürürlüğe girmesi ile birlikte ülkemizde son dönemde başta faaliyetleri kapsamında kişisel veri işleyen şirketler olmak üzere pek çok kurum ve kuruluşun gündemine yerleşmiştir.

Bu çalışma kapsamında kişisel verilerin korunması konusu üç bölümde ele alınmıştır. Buna göre birinci bölümde kişisel verilerin korunması hakkında yaklaşım hem ekonomik hak yaklaşımı hem de insan hakları bağlamında ele alınmış, devamında ise kişisel verilerin korunmasına ilişkin olarak OECD, Avrupa Konseyi ve Avrupa Birliği tarafından yapılan hukuki düzenlemelerden bahsedilmiş.ve hem ülkemizde hem de yabancı ülke hukuklarındaki örneklere yer verilmiştir. Çalışmamızın ikinci bölümünde ise 6698 sayılı Kişisel Verileri Koruma Kanunu kapsamında kişisel verilerin korunması konusu incelenmiştir. Çalışmamızın üçüncü ve son bölümünde ise kişisel verilerin korunmasına ilişkin 5237 sayılı Türk Ceza Kanunu kapsamındaki suç tipleri ele alınmıştır. Üçüncü bölümdeki değerlendirme yapılırken 2016 yılında yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu göz önünde bulundurulmuştur. Nitekim bu kanunda, kişisel verilerin korunmasına ilişkin işlenecek suçlarda Türk Ceza Kanunu'nun ilgili maddelerinin uygulanacağına dair atıf bulunmaktadır. Ayrıca bu kanun ile birlikte kişisel verilerin korunmasına ilişkin olarak uzun yıllardır tanımlanmamış pek çok kavram tanımlanmış, belirsizlikten kaynaklı

birçok tartışmaya son verilmiş ve hukukumuza pek çok yeni kavram ve kurum dahil edilmiştir.

Çalışmamızın tüm dünyada uzun yıllardır tartışılırken, Türkiye'de yeni yeni gündeme alınmaya başlanan kişisel verilerin korunması hukuku adına yararlı olması temennisindeyiz.

Anahtar kelimeler **:Kişisel Veriler, Kişisel Verilerin Korunması, Kişisel Verilerin Korunması Kanunu, Türk Ceza Kanunu**

GİRİŞ

Bilgi teknolojilerinin günden güne geliştiği, bireylerin artık çevrimiçi bir hayat sürdüğü günümüzde, kişisel veriler hem en büyük güç hem de en büyük sermaye olma noktasına gelmiştir. Bugün çağın yeni petrolü[1] olmakla tanımlanan verilerin geldiği nokta, özellikle son dönemde yaşanan pek çok veri güvenliği olayı da dikkate alındığında, artık varlığı ve önemi yadsınamaz bir gerçek haline gelmiştir. Bugün dünyanın her yerinden pek çok insan, faaliyetleri gereği ellerinde büyük veri tabanları bulunduran pek çok şirkete karşı hak mücadelesi vermektedir. Yerel mahkemelerden, Avrupa İnsan Hakları Mahkemesi ve Adalet Divanı'na kadar pek çok yargı merci bugün kişisel verilerin korunmasına ilişkin kararlar vermektedir. Özellikle Avrupa Birliği Genel Veri Koruma Tüzüğü'nün de yürürlüğe girmesi ile birlikte, başta veri işleyen şirketler olmak üzere pek çok kurum ve kuruluş, cezaların büyüklüğü karşısında bu konuda önlemlerini arttırmak, bütün veri politikalarını değiştirerek eskisinden de büyük bir titizlik göstermek mecburiyetinde bırakılmışlardır. Bu konudaki yaptırımların arttırılması, düzenlemelerin daha geniş kapsamlı ve bağlayıcı hale getirilmesinde, son yıllarda yaşanan veri güvenliği skandallarının etkisi büyüktür. Elbette her uluslararası adımda olduğu üzere bu alanda atılan adımlarda da ekonominin etkisini yadsımak imkansızdır. Nitekim veri güvenliği ihlalleri ve skandallar, özellikle elektronik ticaretin bu derece aktif ve önemli olduğu bir çağda, bireylere güvenlik kaygısı ile geri adım attırmaktadır. Dolayısıyla alınan bu hukuki önemlerin bir yüzü de her zaman olduğu gibi ekonomiktir.

Çalışmamızın birinci bölümde, kişisel verilerin korunması hakkına getirilen hukuki yaklaşımlar incelenmiş ve yukarda bahsetmiş olduğumuz üzere, bu hakkın hem insan hakları ile hem de ekonomi ile olan ilişkisi üzerine yapılan tartışmalara yer verilmiştir. Bu tartışmalar teorik tartışmalar olsa da esasen kişisel verilere yaklaşım konusunda ülkelerin tutumlarını yansıtmakta olduğundan oldukça önemlidir. Nitekim ilgili bölümde de yer verildiği üzere örneğin veri güvenliği ihlallerinin en ağır biçimde yaşandığı ülkelerden biri olan, kişisel verilerin korunması gibi pek çok ülkede anayasal hak olarak ilan edilmiş bir hakkı, sektörel bazlı bazı vasat düzenlemeler ile koruma

[1] İlgili haber için bakınız. https://www.forbes.com/sites/bernardmarr/2018/03/05/heres-why-data-is-not-the-new-oil/#4d8cd3573aa9 Erişim Tarihi: 10.02.2019

çabasında olan Amerika'da bu hakka yaklaşım, ağırlıklı olarak ekonomik hak yaklaşımı üzerindendir.

Çalışmamızın ikinci bölümünde ise kişisel verilerin korunması hakkını bir insan hak ve özgürlüğü olarak benimseyen ve insanların bu haklarını korumak suretiyle veri işleyen kurum ve kuruluşlara güvenlerini artırarak globalleşen dünyada ekonominin geliştirilmesi amaçlayan Avrupa Birliği, Avrupa Konseyi, OECD gibi oluşumların uluslararası düzenlemelerine ve bazı Avrupa Ülkeleri ile Amerika'nın da içinde bulunduğu yabancı ülke hukuklarına da yer verilmiştir. Bu düzenlemelerin bilinmesi, genel olarak ulusal hukukumuzdaki düzenlemeleri değerlendirebilmek ve eksikleri tespit edebilmek açısından önemlidir. Ayrıca yine bu bölümde ülkemizde yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun getirdiği yeniliklere de yer verilmiştir.

Çalışmamızın üçüncü bölümünde ise ülkemizde 2016 yılında yürürlüğe giren Kişisel Verilerin Korunması Kanunu ışığında, Türk Ceza Kanunu'ndaki kişisel verilerin korunmasına ilişkin suç tipleri incelenmiştir. Bu bölümde, bu iki kanunun birlikte uygulanması neticesinde ortaya çıkabilecek uyuşmazlıklar ve birbirlerini tamamlayan noktaları ele alınmaya çalışılmıştır. Bu değerlendirme yapılırken, Yargıtay kararları ve Kişisel Verileri Koruma Kurulu kararları ile doktrinde konuya ilişkin yapılan tartışma ve eleştiriler de dikkate alınmış ve ayrıntılı olarak açıklanmaya çalışılmıştır.

BİRİNCİ BÖLÜM

KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN GENEL BİLGİLER

I. KİŞİSEL VERİLERİN KORUNMASI HAKKININ NİTELİĞİ ÜZERİNE YAKLAŞIMLAR

A. KİŞİSEL VERİLERİN KORUNMASI HAKKI

Kişisel verilerin korunması hakkı, geçmişten günümüze pek çok temel hak ve özgürlük kapsamında değerlendirilmiş ve doktrinde bu hakkın hangi hak kapsamında korunması gerektiği, hangi hakla birlikte değerlendirilmesi gerektiğine ilişkin pek çok tartışma yapılmıştır. Genel kabul gören görüşe göre, kişisel verilerin korunması hakkı insan hakları zemininde özel hayatın gizliliği kapsamında korunmalıdır. Ancak kişisel verilerin günümüzde yeni bir değer haline gelmesi sonucunda bu hakkın, özellikle Amerika doktrininde, mülkiyet hakkı ya da fikri mülkiyet hakkı kapsamında korunması gerektiği yönünde de görüşler bulunmakta ve tartışılmaktadır. Aşağıda bu kapsamda, kişisel verilerin korunması hakkı, ekonomik hak yaklaşımı ve insan hakları yaklaşımı ile bağlantılı olarak açıklanmıştır.

1. Ekonomik Hak Yaklaşımı

Ekonomik hak yaklaşımı, kişisel verinin yeni bir değer olarak kabul edildiği, pek çok kurum ve kuruluşun sermayesinin veri olmaya başladığı bir çağda, veri güvenliğinin, kişisel verilerin korunması hakkının ekonomik olarak analizinden doğan bir hak yaklaşımıdır. Ekonomik hak yaklaşımı, kişisel verilerin korunması hakkını insan hakları bağlamından uzaklaştıran, kişisel verileri bireylerin mülkiyetinde kabul eden ve bunlardan ekonomik olarak yararlanılmasını hedef alan bir yaklaşımdır. Bu yaklaşım daha ziyade veri güvenliğinin çok yüksek olmadığı Amerika gibi ülkelerde benimsenmekte ve tartışılmaktadır. Ekonomik hak yaklaşımı içinde kişisel verilerin

korunması hakkı, mülkiyet hakkı ve fikri mülkiyet hakkı kapsamında değerlendirilmektedir.

a. Mülkiyet Hakkı Teorisi

Kişisel verilerin hukuktaki yeri konusunda yapılan tartışmalarda en çok eleştirilen görüşlerden biri bu hakkın mülkiyet hakkı kapsamında olması gerektiği ve kişilerin üzerinde serbestçe tasarrufta bulunabileceği, alıp, satabileceği, kiralayabileceği[2] bir hak olması gerektiği yönündeki görüşlerdir. Kişisel verilerin mülkiyet hakkı kapsamında değerlendirilmesi gerektiği görüşünde olan yazarlar bu konuyu farklı perspektifler üzerinden savunmaktadırlar. Buna göre bazı yazarlar kişisel verilerin mülkiyet hakkı kapsamında değerlendirilmesinin bireylere kişisel verileri üzerinde kaybettikleri hakları yeniden verebilecek ya da bireyler ile verileri arasındaki doğal bağın onaylanmasını sağlayacaktır.[3] Bazı yazarlar ise Amerika hukuku ve politik sistemin doğal kısıtlama ve limitlerinin üstesinden gelmenin tek yolunun veriler üzerinde mülkiyet hakkına sahip olmak olduğunu ifade ederken, bütün bu görüşlerin içinde en çok tartışılan görüş ise kişisel verilerin mülkiyet kapsamında değerlendirilmesi yaklaşımının hukukun ekonomik analizine dayandığı görüşüdür. [4] Esasen bu konuda hukukun ekonomik analizi kişisel verilerin yeni bir güç odağı haline gelmesi ile yakında ilgilidir. Hatta kişisel veriler yeni çağın petrolü[5] olarak betimlenmektedir.

Günümüzde özellikle büyük şirketler başta olmak üzere pek çok kurum ve kuruluşun hem en büyük sermayelerinden biri hem de en büyük güçlerinden biri müşterilerinden ya da kullanıcılarından topladıkları verilerdir. Öyle ki artık veri toplama ve işlemenin maliyeti karşısında, halihazırda veri bankası olan kurum ve kuruluşlardan bu veriler satın alınmaya başlanmıştır.[6] Yani elinde büyük veri tabanları

---

[2] Ibrahim Korkmaz, **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, Ankara: Seçkin Yayıncılık, Mayıs 2017, s. 78.

[3] Purtova Nadezhda, "Property Rights in Personal Data: Learning from the American Discourse" **Computer Law & Security Review**, Vol. 25, No. 6, February 2009, S. 507-521, s. 507 https://ssrn.com/abstract=1554341 Erişim Tarihi: 05.02.2019

[4] ibid.

[5] Kişisel verilerin yeni çağın petrolü olduğuna ilişkin haber için bakınız. https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data. 05.02.2019

[6] Nadezhda, **Property Rights in Personal Data: Learning from the American Discourse**, s. 509

bulunduran şirketler yalnızca faaliyet gösterdikleri ticari alandan değil, sahip oldukları verilerden de aynı oranda ve hatta çoğu zaman daha fazla kar elde etmedirler.

Kişisel verilerin korunması hakkının mülkiyet teorisi ile açıklandığı görüşlere göre, kişisel veriler 2000'li yıllarda artık neredeyse yeni bir değer, yeni bir para birimi[7] olarak görülmekte ve özellikle Amerika tarafından bu hızla büyüyen ve gelişen yeni para biriminin trendinden kar elde edilmeye çalışılmaktadır.[8] Kişisel verilerin korunması konusuna ilişkin olarak Amerika ile Avrupa Birliği ülkeleri arasında derin bir farklılık olduğu aşikardır.[9] Amerika'da kişisel verilerin yeteri kadar korunmadığı, veri güvenliğinin sıklıkla ihlal edildiği, Avrupa Birliği Adalet Divanı tarafından da kabul edilmektedir.[10] Nitekim kişisel verilerin korunması hakkı Amerika'da anayasal bir hak olmayıp[11], bu hak bir temel hak ve hürriyet olarak korunmamakta ve bu konuda sektörel yaklaşımlar[12] aracılığı ile veri güvenliği sağlanmaya çalışılmaktadır. Örneğin Amerika'da özellikle finans ve sağlık sektöründe çok fazla kişisel veri işlendiğinden bu sektörler için düzenlenen kanunlarda veri güvenliğine ilişkin bazı hükümler yer almaktadır.[13] Elbette bu hükümler genel veri koruma sistematiğinden uzak ve kapsamlı bir koruma içermediğinden yeterli olduklarını söylemek mümkün değildir. Avrupa Birliği ülkelerinde ve genel olarak Kıta Avrupa hukukun hâkim olduğu ülkelerde ise kişisel verilerin korunması, temel hak ve özgürlükler kapsamında

---

[7] Kişisel verilerin yeni çağın maddi bir değeri olduğuna ilişkin haber için bakınız. Çevrimiçi https://medium.com/hub-of-all-things/personal-data-as-currency-ab1590163ad6. (Erişim Tarihi 05.02.2019)

[8] Paul M. Schwartz, "Property, Privacy and Personal Data", **Harvard Law Review**, Vol. 117, 2004, s. 2056. Schwartz, Amerika'da kişisel verilerin metalaştırılmasına ilişkin güçlü bir konseptin doğduğunu ve Amerikalıların da kişisel verilerinin metalaştırılma sürecine katılmaya başladığını belirtmiştir.

[9] Elif Mendos Kuşkonmaz, **Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması**, Yüksek Lisans Tezi, İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü, 2013, s. 19

[10] Çalışmamızın ikinci bölümünde açıklandığı üzere Avrupa Birliği tarafından kişisel verilerin korunmasına ilişkin olarak yapılan düzenlemelerin pek çoğunda, veri güvenliğinin yeteri kadar sağlanmadığı ülkelere Avrupa birliği ülkelerinden veri transferi yasaklanmaktadır ve Amerika da bu ülkelerden biridir. Nitekim Amerika ile ticaretin tüm dünya için önemli olması ve dünyanın ileri gelen elektronik ticaret şirketlerinin Amerika menşeli olması noktasında, Amerika ile veri transferine ilişkin özel olarak imzalanan Safe Harbour sözleşmesi de Avrupa Birliği Adalet Divanınca verilmiş olan bir karar geçersiz kılınmıştır. Bu kararın ayrıntılı incelemesine ikinci bölümde yer verildiğinden tekrar olmaması açısından burada yalnızca atıf yapmakla yetinilmiştir.

[11] Murat Volkan Dülger, "İnsan Hakları ve Temel Hak ve Özgürlükler Bağlamında Kişisel Verilerin Korunması", **İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi**, C. 5 (1), Bahar 2018, s. 76. Ayrıca bakınız. Viktor Mayer-Schonberger, "Beyond Privacy, Beyond Rights- Toward a Systems Theory of Information Governance", **California Law Review,** Vol. 98, 2010, s. 1857

[12] Atul Singh, "Protecting Personal Data as a Property Right ", **ILI Law Review**, Winter Issue 2016, S.123-139, s. 126. Ayrıca bakınız. Pamela Samuelson, Privacy as Intellectual Property, **Stanford Law Review**, Vol. 52, 1999, s. 2.

[13] Atul Singh, **Protecting Personal Data as a Property Right**, s. 126

korunmakta ve bu bakış açısıyla kişisel veriler ticareti yapılamaz ve devredilemez nitelikte görülmektedirler.[14]

Diğer yandan kişisel veriler üzerinde mülkiyet hakkını savunan yazarlar ise, Avrupa Birliği ülkelerinde ve Avrupa Birliği tarafından düzenlenen sözleşmeler kapsamında dahi, kişisel verilerin korunması hakkının bir temel hak ve özgürlük olmadığını, Avrupa İnsan Hakları Mahkemesi kararlarına göre dahi kişisel verilerin korunması hakkının Sözleşmesi'nin 8. Maddesi yani özel hayata ve aile hayatına saygı hakkı kapsamında korunmakta olduğunu ifade etmektedirler.[15] Ayrıca bu yazarlar, Mahkeme tarafından kişisel verilerin korunması hakkının başlı başına bir temel hak ve özgürlük olduğuna dair, hem özel hem de kamu sektörünü kapsayan, bir ifade kullanılmadığını ve bunda Avrupa İnsan Hakları Sözleşmesi'nin sadece imzacılarına yani devletlere yükümlülük yükleyen bir sözleşme niteliğinde olmasının etkisi olduğunu belirtmektedirler.[16] Bu noktada bu yazarlar sözleşme serbestisinin bu konuda da geçerli olması gerektiğini ve taraflar arasında yapılacak bir sözleşme ile bireylerin kişisel verilerinin korunması hakkından feragat edebilmeleri gerektiğini savunmaktadırlar. Bu görüşte olan yazarlar, özel sektörde halihazırda kişisel veriler bir şekilde işlenmekte olduğundan, bireylerin kişisel verileri üzerinde mülkiyet hakkına sahip olması, aynı zamanda bireyler tarafından bu verilerin değerinin belirlenmesi ile satılabileceğini, böylece bireylerin de bundan bir çıkar sağlayabileceğini, kişisel verileri işleyebilmek için belli bir bedel ödemek mecburiyetinde kalan şirketlerin ise bu konuda otomatik olarak daha dikkatli olacaklarını belirtmektedirler.[17]

---

[14] Federico Ferretti, **EU Competition Law, the Consumer Interest and Data Protection – The Exchange of Consumer Information in the Retail Financial Sector**, Springer International Publishing, 2014, s.116

[15] Nadezhda, **Property Rights in Personal Data: Learning from the American Discourse**.,s.520-521

[16] Nadezhda, **Property Rights in Personal Data: Learning from the American Discourse**.,s.520-521 Aksi yönde AİHM kararı için bakınız. 17 Ekim 1985 tarihli ve no. 10126/82 no.lu Ärzte für das Leben v. Austria kararı. Bu kararda bireylerin 8. Madde kapsamındaki haklarına özel kişilerden gelecek müdahalelerden devletin sorumlu olduğu yönündedir. Yani AİHM her ne kadar devletleri bağlasa da AİHM bireylerin özel kişilerden ya da kuruluşlardan korunması için devlete pek çok yükümlülük yüklemektedir. A. Şeref Gözübüyük ve Feyyaz Gölcüklü, **Avrupa İnsan Hakları Sözleşmesi ve Uygulaması**, Ankara, Turhan Kitabevi, 2009, s. 333.

[17] Samuelson, **Privacy as Intellectual Property**, s.7. Ayrıca bakınız. Hüseyin Can Aksoy**, Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması**, 1 Bası, Ankara, Çakmak Yayınevi, Mart 2010, s.58-59. Ayrıca bakınız. Corien Prins, Property and Privacy: European Perspectives and the Commodification of Our Identity, **Information Law Series**, Vol. 16, pp. 223-257, 2006, s.232

Yukarıda belirtmiş olduğumuz görüşler birlikte değerlendirildiğinde, kişisel verilerin korunmasının mülkiyet hakkı kapsamında değerlendirilmesinin yerinde olmadığı ve bu görüşün sadece devlet ile özel sektör sermayesine hizmet edeceği aşikardır. Elbette kişisel verilerin günümüzde ekonomik bir yönü olduğu tartışmasızdır. Bu veriler özellikle elektronik ticaretin ve sosyal medyanın gelişmesiyle beraber şirketler için vazgeçilmez bir ekonomik sermaye haline gelmiştir. Zira örneğin elektronik ticaret yapan bir şirket müşterilerin kullanıcı alışkanlıklarını belirleyerek satışlarını artırmakta ya da sosyal medya sitesindeki kullanıcı verileri kullanılarak bireylerin siyasi görüşleri ya da eğilimleri hakkında bilgi sahibi olunmakta ve hatta yönlendirilmektedir.[18] Kişisel verinin özellikle son yirmi yılda tüm dünya üzerindeki öneminin giderek arttığı ve artık değerinin petrol ile kıyaslanmaya başlandığı dikkate alındığında, bireylerin hem devlet otoriteleri karşısında hem de sermaye karşısında eskisinden de fazla korunması gerektiği açıktır. Elbette bireylerin kişisel verileri üzerinde söz sahibi ve kendi kişisel verilerinin kaderinin tayininde belirleyici olmaları[19] gerektiğini kabul etmekteyiz. Ancak bireyler kendi verileri üstünde söz sahibi olurken bu veriler devlet tarafından da koruma altında olmalıdır. Aksi takdirde bireylerin karşısında kendilerinden çok daha güçlü konumda olan sermaye, özel sektör ve kamu otoriteleri olacaktır.[20] Böyle bir durumda ise, bireylerin gerçek anlamda özgür bir iradeye sahip olduğundan bahsetmenin mümkün olmayacağı kanaatindeyiz.

b. Fikri Mülkiyet Hakkı Teorisi

Yukarıda da belirttiğimiz üzere Avrupa'da uzun yıllar önce veri koruma güvenliğine ilişkin pek çok mevzuat düzenlemesi yapılmışken, Amerika'da daha ziyade sektörel bazlı çözümler üretilmeye çalışılmaktadır. Bu sebeple çeşitli yazarlar tarafından kişisel verilerin hangi kapsamda korunacağı konusunda farklı görüşler dile

---

[18] Bu konunun ne derece önemli olduğu Amerika'da yapılan son seçimlerde belli olmuştur. 2018 yılı Nisan ayında Cambridge Analytica isimli politik danışmanlık ve strateji firması tarafından, Facebook kullanıcılarının yüklediği bir uygulama aracılığı ile profil bilgilerine, kullanıcı geçmişine ve bu kişilerin arkadaş listesinde olan diğer kişilerin de aynı bilgilerine ulaşıldığı, bu şekilde Facebook'un toplamda seksen yedi milyon kullanıcısının kişisel verilerine sahip olunduğu ve firmanın bu verileri 2016 tarihli Amerikan Başkanlık seçiminde Donald Trump lehine kullandığı iddiaları hem Facebook hem de bahsi geçen firma adına soruşturma açılmasına sebebiyet vermiştir. Daha ayrıntılı bilgi için bakınız. https://www.techrepublic.com/article/facebook-data-privacy-scandal-a-cheat-sheet/. 15.12.2018

[19] Schwarz, **Property, Privacy and Personal Data**, s.2087

[20] Kuşkonmaz, **Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması**, s. 21. Ayrıca bakınız Elif Küzeci, **Kişisel Verilerin Korunması**, Kişisel Verilerin Korunması, Turhan Kitapevi, Ankara, 2018, s. s. 65

getirilmiştir. Bunlardan birincisi kişisel verilerin mülkiyet hakkı kapsamında korunmasıydı ve bu konuyu yukarda işlemiştik. Bazı diğer görüşler ise kişisel verilerin taraflar arasında yapılacak genel bir sözleşmeye konu olmasını ya da mümkünse tarafların tam bilgilendirilmesi ile özel bir gizlilik anlaşmasına konu edilmesini desteklemektedir.[21] Bu görüşün hukuki temelinde ise, fikri mülkiyet hakkı kapsamında, tıpkı eser sahibi gibi, kişisel verilerin genel ya da özel nitelikli bir sözleşmeye konu edilerek kullanım haklarının karşı tarafa verilmesi yatmaktadır.

Bazı yazarlar ise bu başlık altında inceleneceği üzere kişisel verilerin fikri mülkiyet kapsamında korunmasını desteklemektedir. Dolayısıyla kişisel verilerin fikri mülkiyet hakkı kapsamında korunması görüşü de Amerikan doktrini tarafından ileri sürülen ve desteklenen bir nitelik taşımaktadır.

Bu görüş kişisel verilerin mülkiyet hakkı kapsamında korunmasına benzer bir nitelik taşımaktadır. Bu görüş çerçevesinde telif hakkı ile kişisel verilerin korunması arasında bağlantı kurulmaktadır. Doktrinde bu bağlantının, telif hakkı kapsamında ürünün sahibine ait olmaya devam ederken denetiminin devrinin söz konusu olması[22] ya da bir eserin üzerinde telif hakkı sahibinin manevi hakkının bulunması gibi[23], bireyinde kendisine ait veriler üzerinde manevi hakkı bulunduğu belirtilmektedir. Ancak bu görüş çerçevesinde kişisel verilerin korunabilmesi için fikri mülkiyet hukukunun klasik temellerinden uzaklaşarak, kişisel verilerin korunmasına ilişkin yeni ve farklı bir fikri mülkiyet görüşünün yaratılması gerektiği ifade edilmiştir.[24] Yani bu yazarlara göre, ilk bakışta bu iki alan birbirinden ne kadar uzak görünse de, fikri mülkiyet bireylere bir mülkiyet hakkı tanırken, kişisel verilerin korunması ise bireylerin verilerine yetkisiz erişimi engellemektedir ve bu iki hukuk alanı, birlikte yeni bir alan oluşturabilmek için ortak zeminlere sahiptir.[25] Bu bakış açısını eleştiren yazarlar ise kişisel verilerin fikri mülkiyet kapsamında korunması için genişletilmeye çalışılmasının hukuk ve kişisel verilerin korunması hakkının mantığı arasında zoraki bir bağ kurma çabası olduğunu ifade etmektedirler.[26]

---

[21] Samuelson, **Privacy as Intellectual Property**, s. 2
[22] Küzeci, **Kişisel Verilerin Korunması**, 2018, s. 66
[23] Dülger, **İnsan Hakları ve Temel Hak ve Özgürlükler Bağlamında Kişisel Verilerin Korunması**,s.77
[24] Samuelson, **Privacy as Intellectual Property**, s. 3
[25] Viktor Mayer-Schonberger, **Beyond Privacy, Beyond Rights**, s. 1855
[26] Samuelson, **Privacy as Intellectual Property**, s. 14

Yukarıda yer alan bilgiler ışığında kişisel verilerin korunması hukuku ile fikri mülkiyet hukuku birlikte değerlendirildiğinde, bu iki alanın hem amaç hem de kapsam itibariyle birbirlerinden farklı nitelikler taşıdığı ortadadır. Nitekim fikri mülkiyet hukuku eser sahiplerinin eserleri üzerindeki haklarını korurken ve sanatçıların, bilim insanlarının ve sair eser üreticilerinin üretimini desteklemek amacındayken, kişisel verilerin korunması alanı bireylerin kişisel verileri üzerindeki haklarını koruyabilmek ve bu verilere yetkisiz erişimleri ya da bu hakkın her türlü ihlalini önlemek amacındadır. Kaldı fikri mülkiyet alanında eser sahiplerinin eserleri üzerinde hem manevi hem de maddi hakları bulunmakta, yani üreticiler eserlerini satabilmekte, kiralayabilmekte, kullanım hakkı verebilmekte kısaca eserlerinden maddi gelir elde etmektedirler. Oysa kişisel verilerin korunması kapsamında bireylerin, tıpkı mülkiyet hakkı görüşünde belirttiğimiz üzere, kişisel verileri üzerinde bir satma, kiralama ya da bundan maddi bir çıkar elde etme gibi bir amaç yoktur. Bu bakımdan kişisel verilerin fikri mülkiyet kapsamında korunması görüşünün de doğru bir yaklaşım olmadığı kanaatindeyiz.[27]

2. İnsan Hakları Bağlamında Kişisel Verilerin Korunması

Kişisel verilerin insan hakları bağlamında korunması yaklaşımı, Avrupa Birliği ülkeleri ve Kıta Avrupa hukukunun uygulandığı ülkeler tarafından uzun yıllardır benimsenmektedir. Çalışmamızın ikinci bölümünde ayrıntılı olarak bahsedileceği üzere Avrupa Birliği ve Avrupa Konseyi tarafından, bireylerin kişisel verilerinin korunması için hukuki düzenlemeler yapılmakta, sözleşmeler hazırlanmakta ve bu konu üzerinde çalışmalar yürütülmektedir. Kişisel verinin her geçen gün önem kazanması ve ekonomik bir değer taşımaya başlaması kişisel veriler üzerine yapılan bu çalışmaları da artırmıştır. Avrupa İnsan Hakları Sözleşmesi'nde yer alan ve özel hayata ve aile hayatına saygı başlığını taşıyan 8.maddesi kapsamında kişisel verilerin korunması hakkı korunmaktadır. Avrupa İnsan Hakları Mahkemesi tarafından kişisel verilerin 8.madde kapsamında korunmasına ilişkin verilmiş pek çok karar vardır. Diğer yandan kişisel verilerin korunması sadece özel hayatın gizliliği değil, ifade özgürlüğü, unutulma hakkı gibi pek çok insan hak ve özgürlüğü ile de yakından

[27] Küzeci, **Kişisel Verilerin Korunması**, 2018, s.65. Ayrıca bakınız. Kuşkonmaz, **Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması**, s.23

ilgilidir. Aşağıda bu konu farklı insan hakları bağlamlarında ayrıntılı olarak incelenmiştir.

a. Özel Hayatın Korunması Hakkı Kapsamında Kişisel Verilerin Korunması

Kişisel verilerin korunması hakkının bir insan hakkı olarak korunduğu ülkelerde, kişisel veriler uzun yıllardır, kişisel verilerin kişinin özel alanına ait bulunduğu gerekçesiyle özel hayatın korunması hakkı kapsamında değerlendirilmektedir. Ancak gelişen teknolojinin kişisel veriyi başka bir noktaya taşıması, kişisel verinin günümüzde neredeyse ekonomik bir değer olarak görülmeye başlanması, kişisel verilerin korunması hakkına yönelik tehditleri artırmış ve kişisel verilerin bağımsız bir hak olarak korunması ihtiyacını doğurmuştur.[28] Zira özel hayatın gizliliğinin korunmasına ilişkin düzenlemeler ve ilkeler artık kişisel verilerin korunması bakımından yeterli gelmemekte ve esasen bireylerin veri güvenliği alanında ihtiyaçlarını karşılayamamaktadır.[29] Bu bakımdan günümüzde kişisel verilerin korunması hakkının, özel hayatın gizliliği hakkından ayrı bir noktada durduğunu[30] ve bu haktan bağımsız olarak değerlendirildiğini söyleyebiliriz.[31] Yine de kişisel verilerin korunması hakkı bugün hala Avrupa İnsan Hakları Sözleşmesi'nde yer alan ve özel hayata ve aile hayatına saygı başlıklı 8.madde kapsamında korunduğundan, özel hayat kavramı ve özel hayatın korunması ile kişisel verilerin korunması arasındaki bağlantının tartışmasız olduğu açıktır.

Bu noktada özel hayat kavramının ne olduğu üzerine bir değerlendirme yapacak olursak, öncelikle bu kavramın açıklanmasının karmaşık ve zor olduğunu belirtmek isteriz. Nitekim Avrupa İnsan Hakları Mahkemesinin bir kararında[32] da belirtildiği üzere neyin özel hayat kavramının içinde değerlendirilmesi gerektiğine ilişkin kazuistik bir metot kullanılmakta ve her olay içinde kendi içinde ayrı ayrı değerlendirmektedir. [33]

---

[28] Schwarz, **Property, Privacy and Personal Data**, s. 2072
[29] Kuşkonmaz, **Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması,** s. 25
[30] Dülger, **İnsan Hakları ve Temel Hak ve Özgürlükler Bağlamında Kişisel Verilerin Korunması**, s. 78
[31] Küzeci, **Kişisel Verilerin Korunması**, 2018, s. 73
[32] Avrupa İnsan Hakları Mahkemesi tarafından verilen Costello-Roberts, Birleşik Krallık'a karşı kararında, tıpkı Niemietz Almanya'ya karşı kararında olduğu üzere özel hayat kavramının geniş bir şekilde tanımlanmaya elverişli olmadığını belirtmiştir.
[33] Gözübüyük – Gölcüklü, **Avrupa İnsan Hakları Sözleşmesi ve Uygulaması**., s. 334. Doktrinde bazı yazarlar özel hayat kavramını bireylerin aleni olmayan ve başkalarının önünde yaşamaktan imtina

Avrupa İnsan Hakları Mahkemesi tarafından konuyla ilgili verilen kararlar değerlendirildiğinde, özel hayat kavramının tanımı yapılamasa da her olay kapsamında nelerin özel hayat kapsamına girebileceğine dair değerlendirmeler yapılmıştır. Buna göre kişinin kimliği ile ilgili bilgiler, kişinin cinsel yaşamına ilişkin bilgiler, kişinin adı, fotoğrafı, telefon konuşmaları, yazışmaları özel hayat kapsamında sayılabilecek bilgilerdendir. [34] Ancak Avrupa İnsan Hakları Mahkemesi özel hayat kavramını bu bilgiler ışığında değerlendirmekten öte bir bakış açısına sahiptir. Örneğin mahkeme *Von Hannover v. Germany*[35] kararında özel hayat kavramından anlaşılması gerekenin mutlaka kişinin gizli alanına ilişkin bir alan olmadığına aksine kişinin diğer insanlar ile kamuya açık alanlardaki ilişkilerinde de somut olayın koşullarına göre kişinin özel hayatı kapsamında değerlendirilebileceğini, sözleşmenin 8. Maddesi kapsamında bireyleri diğer bireyler ile ilişkilerinin geliştirilmesinin de korunduğunu belirtmiştir. Mahkeme benzer yönde *Rotaru v. Romania*[36] kararında ise kamuya mal olmuş bir bilginin, bu bilginin otoriteler tarafından sistematik olarak toplandığı ve depolandığı bir örnekte kişinin özel hayatı kapsamında sayılabileceğini ifade etmiştir. Mahkemenin bir diğer önemli *Satakunnan Markkinapörssi Oy ve Satamedia Oy v. Finland* kararında ise, mahkeme kişisel verilerin korunmasının, bireylerin sözleşmenin 8. Maddesi ile korunan özel hayata ve aile hayatına saygı hakkına sahip olmaları bakımından temel öneme sahip olduğunu ve ulusal hukuklarda alınacak uygun önlemlerle herhangi bir kişisel verinin sözleşmenin işbu 8. Maddesine uygun olmayan şekilde kullanılmasının engellenmesi gerektiğini ifade etmektedir. Ayrıca mahkeme aynı kararında bireylerin sözleşmenin bu maddesine güvenerek kendi bilgilerinin kaderini tayin hakkına da kullandıklarını eklemiştir. [37]

Görüldüğü üzere bu bilgilerin bir kısmı kişinin kişisel verileri olmakla beraber bir kısmı ise kişinin özel hayatının gizli alanına ilişkin bilgilerdir. Bu sebepledir ki,

---

ettikleri hayatları olarak tanımlamaktadır. Bakınız Zeki Hafızoğulları- Muharrem Özen, "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar", **Ankara Barosu Dergisi**, 2009, S.9-22, s. 18

[34] Gözübüyük – Gölcüklü, **Avrupa İnsan Hakları Sözleşmesi ve Uygulaması**. s.335

[35] Von Hannover v. Germany, 40660/08 - 60641/08 07 no, 07 Şubat 2012 tarih, par. 95. AİHM'nin ilgili karar metni için bakınız https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-109029%22]}. 05.02.2019

[36] Rotaru v. Romania, 28341/95 no, 04 Mayıs 2000 tarih, par. 43. AİHM'nin ilgili karar metni için bakınız. https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-58586%22]}. 05.02.2019

[37] Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland, 931/13 no., 27 Haziran 2017 tarih, par. 137.AİHM'nin ilgili karar metni için bkz. https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-175121%22]}. 05.02.2019

kişisel veriler özel hayatın gizliği kapsamında korunsa da kişinin özel hayatına ilişkin her bilgi kişisel veri olmadığı gibi, her kişisel veri de gizli bilgi değildir.[38] Örneğin kişinin adı kişisel veri kapsamındayken, bu bilgi kişinin özel hayatına konu gizli bir bilgi niteliğinde değildir. Diğer yandan örneğin kişinin aile hayatına ilişkin görüntüler kişinin özel hayatının korunması kapsamındayken, kişisel veri değildir. Bu bakımdan kişisel verilerin korunması hakkının, özel hayatın korunması hakkı kapsamında değerlendirilmesi anlaşılabilir olsa da, her iki hakkın birbirinden farklı noktaları olduğu aşikardır.

Bu noktada ulusal hukukumuza baktığımızda da kişisel verilerin korunması hakkının, Anayasa'nın "*özel hayatın gizliliği ve korunması*" başlıklı 20. Maddesi'ne 2010'da eklenen fıkra ile korunduğu görülecektir. Anayasanın 20.maddesine ek fıkra şu şekildedir. "*Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir*. ". Anayasa'ya 2010 yılında eklenen bu fıkradan yedi yıl sonra ise, 6698 sayılı Kişisel Verilerin Korunması Kanunu yürürlüğe girmiş ve bahsi geçen fıkranın gereği yerine getirilmiştir.

Görüldüğü üzere kişisel verilerin korunması hakkı bugün hala genel olarak hem uluslararası hukukta hem de ulusal hukukta özel hayatın gizliliği hakkı kapsamında korunmakta olup, bir yandan da teknolojinin gelişmesi ile beraber bu haktan bağımsız bir hak olarak ifade edilmeye ve kabul edilmeye başlanmıştır. Bugün Avrupa'nın pek çok ülkesinde ve Türkiye'de kişisel verilerin korunması hakkı bu hakka özgü kanunlar çerçevesinde korunmaktadır. Bu değişim de bu hakkın başlı başına bir hak olarak ele alınmaya başladığının en büyük göstergelerinden biridir.

[38] Dülger, **İnsan Hakları ve Temel Hak ve Özgürlükler Bağlamında Kişisel Verilerin Korunması**, s. 79

b. İfade Özgürlüğü ve Kişisel Verilerin Korunması

Avrupa İnsan Hakları Sözleşmenin ifade özgürlüğü başlıklı 10. Maddesinde güvence altına alınmıştır. Bu madde kapsamında herkesin hiçbir müdahale ve sınırlamaya tabi olmaksızın görüşlerini ortaya koyabilme hakkı korunmuştur. Aynı şekilde 1982 anayasasının düşünceyi açıklama ve yayma özgürlüğü başlıklı 26. Maddesinde de bu hak korunmuş ve bu madde kapsamında da Sözleşmenin 10. Maddesine uygun şekilde bireylerin resim, söz ya da sair yollarla düşüncelerini ortaya koyma hakları koruma altına alınmıştır. Ayrıca her iki maddenin önemli bir ortak noktası da Avrupa İnsan Hakları Mahkemesi kararlarında da sık sık yer verilen bireylerin haber alma özgürlüğünün de ifade özgürlüğü kapsamında koruma altına alınmış olmasıdır.

Kişisel verilerin korunması konusu ile ifade özgürlüğü arasında ciddi bir bağlantı vardır.[39] Bir birey kişisel verilerinin korunmasını, bu verilerin kime, nasıl ve nerede açıklanabileceğini belirleme hakkına sahiptir. İşte bu noktada düşünce özgürlüğü ve kişisel verilerin korunması hakkı arasındaki denge ortaya çıkmaktadır. Özellikle internet ortamındaki kişisel verilerimiz ve bunların kullanılması ya da basın[40] tarafından kişisel verilerin kamuya açıklanması durumlarında bu iki hak arasındaki dengenin korunması oldukça önemlidir. Örneğin çalışmamızın diğer bölümlerinde de atıf yapmış olduğumuz Google v. İspanya Kararında da Avrupa Adalet Divanı başvurucu tarafından kendisine ait kişisel verilerin Google'dan ve İspanya'nın ulusal bir gazetesinden çıkarılmasını istemiş ancak Divan bahsi geçen bilgilerin gazetede yayınlanmasının ifade özgürlüğü kapsamında olduğunu belirterek gazete bakımından başvuruyu reddetmiştir. Zira bu noktada bireyin kişisel verilerinin ve mahremiyet hakkının korunması ile ifade özgürlüğü arasında bir çatışma doğmuş ve ifade özgürlüğünden yana karar verilmiştir. Nitekim bazı verilerin aleni hale getirilmesi, ifade özgürlüğü kapsamında değerlendirilir ya da bu verilerin işlenmesi ya da açıklanması hukuki zorunluluk olur veya bunda kamu yararının bulunursa, bu halde

[39]Ayözger, **Kişisel Verilerin Korunması- Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil**, Beta, İstanbul, 2016, s. 42
[40] Küzeci, **Kişisel Verilerin Korunması**, s. 297

kişisel veri sahibinin bazı haklarına ifade özgürlüğü lehine kısıtlama getirilebilecektir.[41]

Doktrinde ifade özgürlüğünün kısıtlanmasının, ifade özgürlüğünün değil bilginin satışının kısıtlandığı şeklindeki bir gerekçeye dayanarak kısıtlanamayacağı belirtilmektedir.[42] Bu görüşe göre örneğin bir gazete ifade özgürlüğünün en büyük ürünlerinden biridir ve para karşılığında satılmaktadır. Keza reklamlar da ifade özgürlüğünün bir ürünü ancak ticari bir faaliyet kapsamında yapılmaktadır.[43] Bu görüşte olan yazarlar tarafından kişisel verilerin korunması ve bilgi güvenliği için alınacak önlemlerin ifade özgürlüğünün kısıtlanması için meşru bir sebep olarak kullanılması çoğu zaman kabul görmemekte ve bu önlemler ifade özgürlüğünün kısıtlanması olarak yorumlanmaktadır. Doktrinde bazı görüşler ise, bu yazarları veri gizliliği konusunu yeterince dikkate almadıklarını belirterek eleştirmektedirler. [44]

Özellikle son dönemde yapılan ve kişisel verilerin daha üstün bir korumaya sahip olması yönündeki yeni düzenlemeler çerçevesinde basında ifade özgürlüğüne ilişkin tartışmalar hız kazanmıştır. Bu tartışmalarda kişisel verilerin korunmasına ilişkin getirilen prosedürler bakımından basına ayrı bir alan açılması gerektiği zira basının temel amacının bireylere bilgi ulaştırmak olduğu, bu bilgileri ulaştırırken her şeyin önceden planlı olmasının mümkün olmadığı, olayların çoğu zaman ani geliştiği ve veri koruma prosedürlerini harfiyen uygulamanın basının işini yapmasını zorlaştıracağı ifade edilmektedir. [45]

Avrupa İnsan Hakları Mahkemesi tarafından verilen kararlarda da ifade özgürlüğü ile kişilerin özel hayatının gizliliğinin korunması hakkı arasında bir denge değerlendirmesi yapmaktadır. Avrupa İnsan Hakları Mahkemesi tarafından verilen *M.L. ve W.W. v. Germany* kararında mahkeme, medya tarafından ulaşılabilir hale

---

[41] Aydın Akgül, "Kişisel Verilerin Korunmasında Yeni Bir Hak: Unutulma Hakkı ve AB Adalet Divanının Google Kararı", **TBB Dergisi**, 2016, S. 12-38, s. 18

[42] Eugene Volokh, "Personalization and Privacy - Does personalization jeopardize our privacy? If so, what should the law do about it?" **Communication of the ACM**, Vol. 43, August 2000/ No. 8, s. 87

[43] Ibid.

[44] Paul M. Schwartz, "Symposium: Cyberspace and Privacy: A New Legal Paradigm? " **Stanford Law Review**, Vol. 52, No. 5, May, 2000, pp. 1559-1572. s. 1561

[45] İlgili haber için bkz. https://www.theguardian.com/commentisfree/2018/jun/10/data-protection-press-freedom. Ayrıca İngiliz mahkemesi de vermiş olduğu *Stunt v Associated Press* kararında Veri Koruma Kanun'da basın özgürlüğü istisnasına atıf yapmış ve veri sorumlusunun kamu yararı olduğunu düşündüğü olaylarda gazetecilik amacıyla kişisel verilerin işlenebileceğini ifade etmiştir. https://www.michalsons.com/blog/freedom-expression-news-data-protection-balancing-act/30035

getirilen bilgilerin internet arama motorları sayesinde kullanıcılar tarafından kolaylıkla ulaşılabilir hale geldiğini, ancak burada başvurucular tarafından şikayete konu edilen durumun arama motorlarından değil, medyanın kendi internet sitesinde bu materyali yayınlamasından kaynaklanmakta olduğunu, federal mahkemenin başvuruculara artık geçmişte kalan bu mahkumiyetler ile yüzleşmek zorunda kalmamak açısından bir yararları olsa da, kamunun da bu tip olaylar hakkında bilgi sahibi olabilmesi ve geçmiş hakkında araştırma yapabilmesi bakımından gözetilmesi gereken bir yararının olduğunu vurguladığını, ayrıca yine federal mahkemenin medyanın geçmiş olaylara yönelik haberleri ve bilgileri arşivinde bulundurarak demokrasiye katkıda bulunmak gibi bir görevinin olduğunu da vurguladığını belirttikten sonra, bu tip durumlarda haberlerden bu tip bilgilerin çıkarılmasını talep edilebileceği yönünde hak tanıyan bir kararın verilmesi halinde bunun basın ve ifade özgürlüğünü engelleme ve ket vurma gibi etkilerinin olacağını belirmiştir. Ayrıca mahkeme çok önemli bir değerlendirme daha yaparak, başvuruların isimlerinin çıkarılması değil anonimleştirilmesi talebini de her ne kadar bu talep isimlerin doğrudan çıkarılmasına yönelik olarak daha az kısıtlayıcı bir önlem olsa bile, Avrupa İnsan Hakları Sözleşmesi'nin 10. Maddesinde düzenlenen ifade özgürlüğü hakkının, neyin yayınlanıp neyin yayınlanmayacağı konusundaki kararı gazetecilere ve onların etik ve deontolojik normlarına bıraktığını yani böyle bir kararın da gazetecilere ait olması gerektiğini ifade ederek bu olayda sözleşmenin 8. Maddesinin ihlali olmadığını ifade etmiştir. [46] Bu karar aşağıda yer alan başlık altında ayrıntılı olarak incelenen unutulma hakkı bakımından da son derece önemlidir. Nitekim mahkeme her ne kadar bireylerin kişisel verilerinin kaderini tayin hakkı olduğunu kabul etse de bu karar ile bu hakkın da sınırları olduğunu ve ifade özgürlüğü noktasında mutlaka titizlikle değerlendirilmesi gerektiğine dikkat çekmiştir.

Görüldüğü üzere ifade özgürlüğü ve kişisel verilerin korunması hakkı arasındaki dengenin daima korunması ve bu dengede çok dikkatli olunması gerekmektedir. Zira her iki hak da bireyler açısından oldukça hassas olan haklar olup, her somut olayın koşullarında hassas ve dikkatli değerlendirmeler yapılmalıdır.

[46] Avrupa İnsan Hakları Mahkemesi'nin 26 Haziran 2018 tarihli ve 60798/10 ve 65599/10 sayılı kararı için bakınız. https://hudoc.echr.coe.int/eng/?i=001-184438

c. Unutulma Hakkı ve Kişisel Verilerin Korunması

İnternetin hayatın vazgeçilmez bir parçası olması, artık pek çok kişisel verimizin internet üzerinden ulaşılabilir hale gelmesi ve bu verilerin kayıt altına alınması ile birlikte, internet üzerinde tüm bireylere dair neredeyse bir arşiv çalışması yapılabilir hale gelmiştir. Üstelik internet kayıtlarının süreklilik arz etmesi ve yıllar öncesine ilişkin kayıtlara dahi kolaylıkla ulaşılabilmesi ise bazı durumlarda bireylerin hayatını zorlaştırabilmektedir. Bunun yanında ise bugün pek çok kurum ve kuruluş bireylerin kişisel verilerini işlemektedir. Sonuç olarak bireylerin bazen kendi iradeleriyle bazen de başka sebeplerle[47] bir şekilde işlenen verileri, işlendikten sonraki süreçte de dijital ortamda kalmaya devam etmektedir. İşte bu gibi durumlar için bireylere verilerinin silinmesini talep etme hakkı yani unutulma hakkı tanınmaktadır.

Unutulma hakkının doğuşunda İsviçre Federal Mahkemesi'nin vermiş olduğu kararların etkisi büyüktür. [48] İsviçre Federal Mahkemesi tarafından verilen bir kararda, bireyin 10 yıl önce işlemiş olduğu bir suçtan ötürü, bu suçun cezasını çektiği, adli sicilinden dahi suçun silindiği ve kişinin tanınmış bir kişi olmadığı ve bu suçun bilinmesinin toplum için bir yararının da olmadığı dikkate alındığında, bu kişinin söz konusu suçuyla ilgili olarak yazı yazılmasını ve kişisel verilerinin ifşa edilmesinin doğru olmadığını ifade etmiştir.[49]

Avrupa Adalet Divanı tarafından verilen 13 Mayıs 2014 tarihli Google-İspanya[50] kararı ise unutulma hakkı bakımından verilmiş ilke niteliğinde bir karardır. Ayrıca bu karar Divan tarafından verilen ve kişisel verilerin korunması kapsamında unutulma hakkına ilişkin verilmiş en önemli kararlardan biridir.

Şikâyet, İspanya vatandaşı Costeja González tarafından İspanya'nın yüksek tiraja sahip günlük bir gazetesi ve Google İspanya'ya yönelik olarak yapılmıştır. Başvurucu, adı Google arama motoruna yazıldığında kendisi hakkında yılları önce sonuçlanmış ve artık bir geçerliliği kalmayan sosyal güvenlik borçlarının tahsiline

---

[47] Ayözger, **Kişisel Verilerin Korunması Hukuku**, s. 39
[48] Nilgün BAŞALP, "Avrupa Birliği Veri Koruması Genel Regülasyonunun Temel Yenilikleri", **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, C. 21, 2015, S.1, s.95-96
[49] ibid.
[50] İlgili karar için bakınız.
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131

ilişkin haciz davaları ile bağlantılı bir gayrimenkul açık artırması ilanının yer aldığı bahsi geçen gazeteye ait 1998 tarihli sayfalara ulaşıldığını ve oldukça eski tarihli olan bu bilgilerin artık Google'da yer almasını istemediğini beyan etmiş ve bunun için sayfaların kaldırılması veya düzenlenmesini ya da verileri korumak için arama motorlarının sunduğu belirli araçların kullanılmasını talep etmiştir. İspanya Veri Koruma Kurumu, gazete hakkında yapılan şikâyeti, gazetenin bu yayını mevzuat gereğince yaptığı ve bu bakımdan hukuka uygun olduğu gerekçesi ile reddetmiş ancak Google ile ilgili şikâyeti onaylamıştır. Google şirketinin davayı ulusal yüksek mahkemeye taşıması üzerine, yüksek mahkeme konunun 95/46EC sayılı Veri Koruma Direktifinin yürürlüğe girmesinden sonra yaşanan teknolojik gelişmelerin değerlendirilmesi açısından bazı soruların sorulması gerektiğini belirterek, konuyu Avrupa Birliği Adalet Divanı'na yönlendirmiş ve Divan kararını bekletici mesele haline getirmiştir.

Divan bu inceleme neticesinde ilke niteliğinde sonuçlara ulaşmıştır. Divan, kişisel veri olarak kabul edilebilecek nitelikteki bilgileri içermesi durumunda, bir arama motoru faaliyetinin, kişisel verilerin işlenmesi faaliyeti olarak ve arama motoru operatörünün, 2'nci maddenin (d) bendi anlamında, bu işlemeye ilişkin olarak 'kontrolör' olarak değerlendirilmesi gerektiğini, direktifin ilgili maddelerine uyumlu olabilmek için bir arama motoru operatörünün, üçüncü taraflarca yayınlanan ve bir kişiye ilişkin bilgi içeren internet sitesi linklerini bu kişinin ismine dayanılarak yapılan bir arama sonrasında gösterilen sonuçlar listesinden kaldırmak zorunda olduğu şeklinde yorumlanması gerektiğini, veri sahibinin ilgili bilginin artık kamuya sunulmamasını talep etme hakkının olduğunu ve bu hakkın hem arama motoru operatörünün ekonomik menfaatine hem de kamunun bu bilgiye erişimine ilişkin menfaatine de üstün geleceğini belirtmiştir. Bu noktada bu kararın hala Google'a ilişkin farklı davalarda tartışıldığını ve bazı savunucuların bu karar ışığında Avrupa veri koruma mevzuatı değerlendirildiğinde unutulma hakkının yalnızca Avrupa'da etkili olabileceği ve global bir etkisinin olmasının mümkün olmadığını ifade ettiklerini de belirtmek isteriz.[51]

[51] Konuyla ilgili ayrıntılı bilgi için bkz. https://www.theguardian.com/technology/2019/jan/10/right-to-be-forgotten-by-google-should-apply-only-in-eu-says-court

Divan tarafından verilen bu kararı ise, yine unutulma hakkına ilişkin olarak Alman Mahkemesi tarafından 2009 yılında verilen ve kendilerine verilen cezayı çektikten sonra hala internette suçlarına dair bilgilerine ulaşılan iki cinayet zanlısı hakkında verilen karar takip etmiştir. [52]

Bu kararlar unutulma hakkı üzerine dikkatleri çekmiş ve bu hak üzerinde yapılan çalışma ve düzenlemelere hız verilmiştir. 1995 tarihli Veri Koruma Direktifinde veri sahiplerine tanınan verilerin silinmesi ve yok edilmesini talep etme hakkı, Avrupa Birliği Veri Koruma Tüzüğü'nün 17. Maddesinde veri sahibinin, veri sorumlusundan verilerinin silinmesini talep etme hakkı şeklinde düzenlemiştir. Bu maddeye göre veri sahibinin rızasına dayalı olarak verinin işlenmesi halinde rızanın geri alınması ve verinin işlenmesi için başka bir hukuki dayanak olmaması, veri sahibinin verilerin işlenmesine itiraz etmiş olması, bu verilerin hukuka aykırı olarak işlenmiş olması, verilerin bir hukuki yükümlülükten kaynaklı olarak silinmesi gerekmesi gibi durumlarda veri sahibinin verilerinin silinmesini talep hakkı bulunmaktadır. Esasen tüzüğün tasarısında bu haktan unutulma hakkı olarak bahsedilmiş olmasına rağmen, tüzüğün yürürlüğe giren halinde bu hak verilerin silinmesini talep etme hakkı olarak tanımlanmış ancak parantez içerisinde unutulma hakkı olarak da eklenmiştir. Ancak Avrupa'da ve kıta Avrupası hukukunun uygulandığı ülkelerde oldukça rağbet gören unutulma hakkı Amerika doktrini tarafından ise eleştirilmektedir. Amerika ve Avrupa'nın kişisel verilerin güvenliğine ilişkin konulardaki tutumunun ne denli farklı olduğuna yukarıdaki bölümlerde ayrıntılı olarak yer verilmiştir. Bu konuda da Amerikan doktrininde bazı görüşler, unutulma hakkını tanıyan Avrupa ülkelerinin doğru ve net şekilde düşünemediklerini, bu hakkı kabul etmekle Avrupa'nın kişisel verinin mülkiyet hakkı kapsamındaki yerini kabul ettiğini, bu hakkın kabulünün bürokratik bir kaostan başka bir şey üretmeyeceğini ifade ederken, daha yumuşak yaklaşımlar da ise bu hakkın en azından çocuklar ve gençler için kabul edilebileceğini ifade etmektedirler. [53]

---

[52] Steven C. Bennett, "the "Right to Be Forgotten": Reconciling EU and US Perspectives", **30 Berkeley Journal of International Law**, 161, 2012, s.164.
Wolfgang Werlé ve Manfred Lauber kararın geçmişi ve süreç içerisinde verilen kararlar için bakınız, https://en.wikipedia.org/wiki/Wolfgang_Werl%C3%A9_and_Manfred_Lauber

[53] Ibid, s. 165-167

Ülkemize baktığımızda da unutulma hakkının Yargıtay tarafından kabul edildiğini ve uygulandığını görmekteyiz. Yargıtay Hukuk Genel Kurulu tarafından verilen emsal niteliğindeki bir karara göre unutulma hakkı bakımından kamu yararı, hakkın sınırı olarak kabul edilmek suretiyle, internet ortamında yer alan ve kişinin artık başkaları tarafından ulaşılmasını istemediği birtakım bilgilerinin ortadan kaldırılması ve bu bilgilere başkaları tarafından erişiminin engellenmesi şeklinde tanımlanmıştır. [54]

Yukarıda yer vermiş olduğumuz bilgiler ışında unutulma hakkının oldukça önemli bir hak olduğu aşikâr olsa da bu hakkın mutlaka ifade özgürlüğü, veri koruma hakkı ve bireylerin bilgiye erişim hakkı gibi diğer temel haklar karşısında dengelenerek uygulanması gerekmektedir. Aksi takdirde bireylere unutulma hakkının kullandırılması sürecinde diğer bireylerin pek çok temel hak ve özgürlüğünün ihlal edilme ihtimali doğacaktır.

d. İnsan Onuru ve Kişisel Verilerin Korunması

Dünya tarihinde yaşanan ve insanlığa zarar veren her olayın, her acının arkasından insan haklarına ilişkin adımlar atılmıştır. Zira insanlık onuru, bu tip olaylarda öylesine büyük darbeler almıştır ki, her olayda temel hak ve özgürlüklere ilişkin bir adım atılmıştır. Örneğin yukarıda da belirttiğimiz üzere Avrupa İnsan Hakları Sözleşmesi'nin ortaya çıkışında ikinci dünya savaşında yaşanan insanlık onuruna yakışmayan olaylar etkili olmuştur. Kişisel verilerin korunması hakkı da aslında aynı şekilde, teknolojinin gelişmesi ile birlikte bu alanda insan onuruna yakışmayacak olayların yaşanması ile birlikte her geçen gün daha da önemli hale gelmiş ve bu konuda hukuki ve siyasi adımlar atılmıştır. Kendi yakın siyasi tarihimize

---

[54] Dülger, **İnsan Hakları ve Temel Hak ve Özgürlükler Bağlamında Kişisel Verilerin Korunması**, s.94. Yargıtay Hukuk Genel Kurulu da vermiş olduğu bir kararında unutulma hakkının bireylerin kişisel verilerinin korunması hakkı ile yakından bağlantılı olduğunu, bireylerin kişisel verileri üzerinde tasarrufta bulunma hakkı bulunduğunu ve verileri üzerinde hak sahibi olan bireyin bu verilerin geleceğini belirleyerek geçmiş ile bağlarını koparark esasen kendi geleceğine yön verdiğini ifade etmiştir. Bu bakımdan Yargıtay aynı kararında unutulma hakkı ile birlikte bireyin artık hayatının bir parçası olarak taşımak istemediği kişisel verilerinin silinmesini talep edebileceğini ve bu verileri bulunduran kişilerin de bu verilerin sair kişiler tarafından kullanılmasını engellemekle yükümlü olduğunu belirtmiştir. Yargıtay kararının devamında bireylerin unutulma hakkını örneklendirerek, bireylerin artık erişilmesini istemediği fotoğrafları ya da geçmişe dair cezalarıyla ilgili bilgilerin yok edilmesinden bahsetmiş ve bu konuda önlemler alınmasının talep edebilmenin de bu hak kapsamında değerlendirildiğinden bahsetmiştir. Yargıtay Hukuk Genel Kurulu'nun 2014/4-56 E. ile 2015/1679 K. Sayılı ve 17.06.2015 Tarihli Kararı

de baktığımızda, bu verilerin korunması yönünde atılmayan adımlar sonucunda, siyasi olarak çalkantılı dönemlerde insanların nasıl fişlendiğini ve bu fişlemeler yüzünden yaşanan acıları görüyoruz. Zira kişisel veri yalnızca bir bireyin adı, soy adı ya da biyometrik verilerini değil, aynı zamanda bireyler için oldukça hassas olan ırk, dini inanç, siyasi görüş, felsefi düşünce, cinsel yönelim, sağlık bilgileri gibi bilgileri de kapsamaktadır. Bu bilgilerin bireyin bilgisi dışında, hukuki dayanak olmaksızın ve bireye bu bilgilerin korunmasına ilişkin haklar verilmeden işlenmesinin, toplumu ayrıştıracağı, adeta bir gözetim toplumu oluşturacağı ve insanlık onuruna yakışmayacağı tartışmasızdır. Bireylerin kişisel verilerinin korunmadığı böyle bir toplum tıpkı George Orwell'ın 1984 isimli kitabında olduğu üzere bir denetim ve baskı toplumundan başka bir şey olmayacaktır. [55]

Bugün kişisel verilerin korunmasına ilişkin yapılan hukuki metinlere genel olarak baktığımızda bu verilerin korunmasına ilişkin bazı ortak düzenlemelerin olduğunu görüyoruz. Buna göre kişisel veriler bireylerin rızası dahilinde işlenmeli, eğer bireylerin rızasının alınmasına gerek olmayan haller söz konusu edilecekse bu haller mutlaka kanunlarla belirlenmeli, kişisel veriler amacına uygun, yeterli şekilde toplanmalı, verinin tutulması için artık yeterli bir sebep kalmamışsa veriler yok edilmeli, bireylere verilerine erişim, düzeltme ya da silme talep hakkı gibi haklar bireylere tanınmalıdır.

Bireylerin özellikle verinin yeni bir sermaye haline geldiği günümüzde, Facebook, Google, Amazon gibi elinde global anlamda büyük veri bulunduran şirketlere ve devlet otoritelerine karşı korunmaları gerekmektedir. Zira özellikle son dönemde bu tip şirketlerin veri güvenliğine ilişkin ihlallerinin ne derece büyük olduğuna ilişkin pek çok skandal ortaya çıkmakta ve yargılamalar yapılmaktadır. Yakın zamanda yukarıda ayrıntılı olarak bahsettiğimiz Facebook skandalı[56], Google tarafından pek çok şirkete Gmail hesaplarına erişim yetkisi verildiğinin[57] ortaya

[55] Gözde Dedeoğlu, Gözetleme, Mahremiyet ve İnsan Onuru, **TBB Bilişim Dergisi**, 19 Nisan 2004, S. 153, s. 3

[56] İlgili haber için bakınız https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election. 02.02.2019

[57] İlgili haber için bakınız. https://www.independent.co.uk/life-style/gadgets-and-tech/news/google-gmail-data-sharing-email-inbox-privacy-scandal-a8548941.html. 02.02.2019

çıkması ve bunun gibi binlerce olay gibi dikkate alındığında, kişisel verinin önemi ve insanlık onuru ile bağlantısı açıkça görülecektir.

Kişisel verilerin korunması insanlık onurunun korunmasında vazgeçilmez bir parçadır. Bireylerin kişisel verileri üzerinde hak ve denetim sahibi olmaları, günümüzde eskisinden de önemli hale gelmiştir. Bu konuda veri güvenliğiyle ilgili olarak giderek artan hukuki çalışmaların, bireylerin büyük sermayelere ve devlet otoritelerine karşı korunmasında oldukça etkili olduğu ve olmaya da devam edeceği kanaatindeyiz.

e. Bilgi Edinme Hakkı

Kişisel verilerin korunması hakkı ile bilgi edinme hakkı arasındaki ilişki, ifade özgürlüğü ile kişisel verilerin korunması arasındaki ilişki hassasiyetindedir. Zira bir hakkın lehine karar verilirken diğer hakkın zarar görmesi ya da ihlal edilmesi ihtimali söz konusu olabilecektir.

Avrupa İnsan Hakları Mahkemesi, bilgiye ulaşım hakkını devletlerin bireylerin bilgi alma hakkını kısıtlamalarının yasaklanması şeklinde tanımlamış ve bu hakkın devletlere bilgi toplaması yönünde bir pozitif yükümlülük yüklediği şeklinde yorumlanamayacağını ifade etmiştir.[58]

Nitekim yukarıda atıf yapmış olduğumuz Avrupa İnsan Hakları Mahkemesi kararında *M.L. ve W.W. v. Germany* kararında da belirtildiği üzere, kişisel verilerin korunması kapsamında unutulma hakkının incelendiği kararda, ifade özgürlüğü ile birlikte bireylerin bilgiye erişim hakkının da dikkate alınarak değerlendirilmesi gerektiği ifade edilmiştir. Ayrıca mahkeme *Magyar Helsinki Bizottság v. Hungary*[59] kararında, başvurucu sivil toplum kuruluşunun kamu savunması sistemine dair olarak yapmış olduğu çalışma için devlet yetkililerinden talep ettiği bazı bilgilerin, bu bilgilerin içerisinde bir takım kişisel verilerin de bulunduğu gerekçesiyle reddedilmesi konusunda, sözleşmenin 10. Maddesinde düzenlenen ifade özgürlüğü hakkının aynı

---

[58] Hermann Josef Blanke - Ricardo Perlingeiro, **The Right of Access to Public Information – An International Comparative Legal Survey**, Springer, 2018, s. 147

[59] Mahkemenin ilgili kararı için bakınız. https://hudoc.echr.coe.int/eng-press#{%22itemid%22:[%22003-5539963-6976296%22]}

zamanda bilgiye erişim, bilgi edinme hakkını da kapsadığı ve neticesinde kamu yararı bulunan bir çalışma için bu verilere ulaşımın talep edilmesi halinde bu kuruluşun ifade özgürlüğü ve bilgiye erişim hakkının korunması gerektiğini belirterek, bu olayda sözleşmenin 10. Maddesinin ihlal edildiği sonucuna varmıştır.

Anayasa Mahkemesi ise 2014 yılında vermiş olduğu çok önemli Twitter[60] kararında, başvurucular Telekomünikasyon İletişim Başkanlığı tarafından 'twitter' isimli sosyal medya sitesine erişimin engellenmesine yönelik kararın uygulanması neticesinde, bu siteye erişimin tamamen engellendiği oysaki uygulanan mahkeme kararlarında tüm siteye erişime yönelik karar verilmediğini dolayısıyla söz konusu uygulamanın hukuka ve söz konusu mahkeme kararına uygun olmadığını, bu hukuka aykırı uygulama ile bireylerin bilgiye erişim haklarının engellendiği ve bu hali ile de Avrupa İnsan Hakları Sözleşmesi'nin 10. Maddesinde düzenlenen ifade özgürlüğünü ihlal ettiğini ileri sürmüşlerdir.

Anayasa Mahkemesi bu konuda vermiş olduğu kararında, TİB'in bahsi geçen uygulamasına dayanak kararlarda yalnızca belirli URL'lere yönelik erişimin engellenmesi yönünde kararların olduğunu oysa TİB'in uygulamasında tüm twitter'a erişimi engelleyerek bireylerin ifade özgürlüğüne yönelik ağır bir müdahalede bulunduğunu ve bu müdahalenin hukuken dayanaksız olduğunu, bu sebeple başvurucuların Anayasa'nın 26. Maddesinde düzenlenen ifade özgürlüğü hakkının ihlal edildiği şeklinde görüş ifade ederek başvurunun kabulüne karar vermiştir.

Anayasa'nın dilekçe, bilgi edinme ve kamu denetçisine başvurma hakkı başlıklı 74. Maddesinde [61] bireylerin bilgi edinme hakkı düzenlenmiştir. Ayrıca yine Bilgi Edinme Kanunu'nun özel hayatın gizliliği başlıklı 21. Maddesinde kişisel verilerin korunmasına ilişkin önemli bir düzenleme yapılmıştır. Buna göre kişinin rızası olan haller haricinde, bilgi edinme kapsamında kişinin özel ve aile hayatı, sağlık, şeref ve onuru ile mesleki ve ekonomik değerlerine ilişkin bilgilere ilişkin bilgi ve belgelerin açıklanması söz konusu edilmeyecektir. Bu madde ile kişisel veriler 3. Kişilere karşı

[60]Anayasa Mahkemesinin Twitter kararı için bakınız.
http://www.kararlaryeni.anayasa.gov.tr/BireyselKarar/Content/472bbf6e-ce2c-4c83-a402-6bdd44702537?wordsOnly=False

[61] Anayasanın ilgili maddesinde vatandaşların ve Türkiye'de yerleşik yabancıların (karşılılık ilkesine dayanarak) devletin yetkili makamlarına başvurarak dilek ve şikayetlerini iletebileceklerini ifade edilmiştir.

korunmak istenmiştir. Her ne kadar bilgiye ulaşım hakkı şeffaf idarenin bir görünümü olsa da[62] bunun sınırı olarak bireylerin özel hayatı ve kişisel verileri olarak çizilmiştir. Maddenin ikinci fıkrasında ise kamu yararının olduğu durumlarda bireyin önceden rızası alınmak şartıyla verilerin açıklanabileceği düzenlenmiştir. [63]

Ayrıca bilgi edinme hakkı, kişisel verilerin korunması kapsamında bireylerin hangi bilgilerinin işlendiği, ne kadar süreyle tutulacağı, 3. Kişilere aktarılıp aktarılmayacağı gibi konularda bilgi almalarını da ifade etmektedir. Zira veri güvenliğine ilişkin hukuki metinlerin hemen hepsinde bu haklar bireylere tanınmakta ve uluslararası metinlerde de bu hakların bireylere tanınması imzacı devlet otoritelerine bir görev olarak yüklenmektedir. Bu bakımdan da bireylerin bilgiye erişim hakkı oldukça önemlidir ve hem ifade özgürlüğü kapsamında hem de kişisel verilerin korunması hakkı kapsamında korunması gerekmektedir.

II. KİŞİSEL VERİLERİN KORUNMASI HAKKINA İLİŞKİN HUKUKİ DÜZENLEMELER

A. ULUSLARARASI DÜZENLEMELER

Uluslararası hukuka baktığımızda, kişisel verilerin korunmasına konusunda pek çok hukuki düzenleme bulunmaktadır. Hem Avrupa Konseyi ve OECD hem de Avrupa Birliği tarafından yapılan bu hukuki düzenlemeler hem Avrupa Birliği ülkelerinde hem de bu birlik ülkesi olmayan ülkeler üzerinde etkili olmuştur.

Nitekim globalleşen dünyada artık tüm dünya ülkelerinin birbirileriyle ekonomik bağları bulunmakta ve teknolojinin gelişmesi ile birlikte artık ekonomi klasik alım satım ticaretinden uzaklaşmakta, ekonomi internet üzerinden yapılan elektronik ticarete dönmektedir. Bunun yanı sıra ise Facebook, Google, Instagram gibi sosyal medya sitelerinin artık insanların hayatının vazgeçilmez bir parçası haline gelmesi, bireylerin neredeyse tüm kişisel verilerini artık bu sosyal mecralarda bulundurması ve bu ve bunları gibi pek çok şirketin sahip oldukları kişisel veri sermayesi ile tüm dünyada bir güç odağı haline gelmeleri de, bu konuda yaşanan

[62] Küzeci, **Kişisel Verilerin Korunması**, 2018, s.97
[63] Ayözger, **Kişisel Verilerin Korunması Hukuku**, s. 45

tartışmaların artmasına sebep olarak veri güvenliği konusundaki hukuki düzenlemelere hız verilmesine sebep olmuştur. Bu sebeplerle aşağıda kişisel veri hususunun tartışılmaya başlandığı ilk günden bu yana bu konuya yön veren tüm hukuki düzenlemeler ayrıntılı olarak incelenmiştir.

1. OECD Tarafından Kişisel Verilerin Korunmasına İlişkin Hazırlanan Hukuki Düzenlemeler

Kişisel verilerin korunmasına ilişkin uluslararası düzenlemelere baktığımızda, bu konudaki ilk girişimlerin Ekonomik İşbirliği ve Kalkınma Örgütü (bundan sonra OECD olarak anılacaktır) aracılığı ile ortaya çıktığı görülmektedir.

Teknolojinin gelişiminin ekonomiye yansıması ve kişisel verilerin sınırlar ötesi paylaşılmaya başlamasıyla birlikte OECD, kişisel verilerin işlenmesi, korunması ve aktarımı gibi kişisel verilere ilişkin düzenlemeler yapma girişiminde bulunarak 1980 yılında "Mahremiyetin Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeleri" kabul etmiştir. Toplam 8 ilkeden oluşan bu ilkeler veri toplamanın sınırlı şekilde olması, verinin tam ve güncel olması, veri toplama amacının belirlenmiş olması, kullanımın belirli sınırlar içinde olması, veri güvenliğinin sağlanması, şeffaf olunması ilkesi, bireyin müdahale edebilmesi ve veri sorumlularının veri sahiplerine karşı sorumluluğu ilkesi olarak sıralanabilir.[64]

– Veri Toplanmanın Sınırlı Olması İlkesi (Madde-7) – Bu maddeye göre kişisel veriler hukuk ve dürüstlük çerçevesinde, kişisel veri sahibinin bilgilendirilmesi ve onayı[65] ile sınırlı olmak üzere toplanmalıdır.

– Veri Kalitesi, Amacın Belirli Olması İlkesi (Madde 8) – Kişisel veriler, toplanma amaçlarına uygun olarak kullanılmalı ve bu amaçların gereklilikleri kapsamında doğru, tam ve güncel olmalıdır.

---

[64] http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[65] Els De Busser, **Data Protection in EU and US Criminal Cooperation**, Antwerpen – Apeldoorn - Portland, Maklu Publishers, 2009. Busser tarafından "*OECD ilkeleri kapsamında, kişisel verilerin toplanması, özellikle kişisel verilerin toplanmasına ilişkin limitler, kişisel veri sahibinin onayına bağlamıştır"* şeklinde ifade edilmiştir.

– Kullanma Amacının Belirli Olması İlkesi (Madde 9) – Kişisel verilerin toplanmasına ilişkin amaçlar en geç kişisel verilerin toplanması sırasında belirli olmalı ve bundan sonrasında gerçekleşecek tüm kullanımlar bu amaçlar veya bu amaçlar ile bağdaşması ve bu amaçların her değişiminin bildirilmesi şartıyla sınırlıdır.

– Kullanımın Sınırlı Olması İlkesi (Madde 10) – Kişisel veriler, ilgilinin rızası veya hukukun gereklilikleri hariç olmak üzere, açıklanmamalı, ulaşılabilir hale getirilmemeli veya 9. maddeye uygun olarak belirlenen amaçlar dışında kullanılmamalıdır.

– Veri Güvenliği İlkesi (Madde 11) – Kişisel veriler, olası bir kaybolma veya yetkisiz erişim, yok etme, kullanma, modifiye etme veya açıklanma risklerine karşı makul güvenlik önlemleri ile korunmalıdır.

– Aleniyet İlkesi (Madde 12) – Kişisel verilere ilişkin olarak genel bir aleniyet politikası olmalıdır. Kişisel verilerin mevcudiyetine ilişkin araçlar ile kullanıma ilişkin amaçlar ve kişisel veri sorumlusunun kimliği ve adresi ile birlikte hazır edilmelidir.

– Bireysel Katılım İlkesi (Madde 13) – Bireylerin veri sorumlusundan bireyin kendisine ait bir veri bulundurup bulundurmadığına ilişkin bilgi veya onay alma hakkı olmalıdır. Bireyin bu noktada veri sorumlusu ile iletişim kurarak kendisiyle ilgili bilgilere ilişkin gerekliyse makul bir ücret karşılığında, usulüne uygun bir şekilde ve kendisinin anlayabileceği biçimde bilgi alma hakkı olmalıdır. Ayrıca bireyin bu talebi reddedilirse, bireyin buna itiraz etmek hakkı, itirazının kabul edilmesi halinde ise kendisine ilişkin verilerin silinmesi, tadil edilmesi, düzenlenmesi veya tamamlanması hakları da bireye verilmelidir.

– Hesap Verebilirlik İlkesi (Madde 12) – Veri Sorumlusu, yukarıda belirtilen prensipleri hayata geçirecek tedbirlere uymak konusunda sorumlu/hesap verebilir olmalıdır.

Bu noktada belirtmek isteriz ki, gelişen teknolojinin kişisel veriler üzerindeki etkisi ile birlikte söz konusu ilkelerin dönemin şartları ile uyumlu hale gelmesi ve

geliştirilmesi için çeşitli çalışmalar yapılmaya başlanmıştır. Zira 1980 yılına ait bu ilkeler, veri kullanımı ve işlemesi konusunda daha az karmaşık, organizasyonların kişilerin verilerini yalnızca belli ve sınırlı amaçlar için topladığı ve kullandığı bir dönem içerisinde düzenlenmişti.[66] Bu kapsamda örneğin 16-17 Şubat 1998 tarihinde "Global Toplumda Gizliliğin Korunması" başlıklı bir workshop düzenlenmiş ve bu workshopta, global ağlar kapsamında OECD ilkelerinin nasıl ve ne şekilde tadil edilebileceği, OECD üyesi ülkeler tarafından geliştirilen özel hayatın korunmasına ilişkin farklı yaklaşımlar arasında bir köprü kurmada etkili olabilecek mekanizmalar ve teknolojik araçlar ve özel sektörün kişisel verilerin korunmasına ilişkin kayda değer bir koruma sağlaması hususlarında tartışılmıştır.[67]

OECD ilkelerinin güncellendiği 2013 yılına kadar, özel hayatın gizliliği ve kişisel verilerin korunmasına ilişkin çeşitli çalışmalar yapılmış, bu alandaki mevcut düzenlemelere ilişkin çeşitli görüşler ve eleştiriler dile getirilmiştir. Örneğin 1 Aralık 2009 yılında Avrupa Birliği Kişisel Verilerin Korunması Çalışma Grubu, kişisel verilerin korunması konusunda rıza kavramını değerlendirmiş ve özellikle kişisel veriyi işleyen ve kişisel verisi işlenen taraflar arasında statü farklılığı bulunması durumunda kişinin rızasının sağlıklı bir rıza olarak dikkate alınamayacağı ifade edilmiştir.[68]

OECD, 2010-2011 yılı döneminde 30. yılı kapsamında mevcut ilkelerin güncellenmesi için bir uzman grubu oluşturmuş ve gruptan bu ilkelerin yeniden incelenmesini istemiş ve bu paralelde Microsoft şirketi de benzer bir çalışmaya başlamıştır.[69] Bu çalışmalar neticesinde OECD 2013 yılında bu ilkeleri güncellemiş ve temel ilkeleri korumak suretiyle yeni düzenlemeler eklemiştir. OECD tarafından 2013 yılında güncellenen bu tavsiye niteliğindeki ilkelerde kişisel veri ihlallerinde bildirim yükümlülüğü, rıza kavramı, veri sorumlusu ve özellikle kişisel verileri kontrolü altında bulunduran kurumların, lokasyon bağımsız olarak, kişisel verilerin

---

[66] Fred H. Cate, Peter Cullen, Viktor Mayer-Schönberger, "Data Protection Principles for the 21st Century Revising the 1980 OECD Guidelines", **Oxford Internet Institute**, Mart 2014, s. 2.
[67] OECD**,** "**Privacy Online - OECD Guidance on Policy and Practice**" 2003, s.48
[68] Cate, Cullen, Schönberger, **Data Protection Principles for the 21st Century Revising the 1980 OECD Guidelines**, s. 9
[69] OECD (2013), "Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines", **OECD Digital Economy Papers**, No. 229, OECD Publishing, Paris, s.4. İlgili rapor için bakınız. http://dx.doi.org/10.1787/5k3xz5zmj2mx-en

sınırlar arası veri akışı bağlamında, sorumlu tutulmalarına yönelik[70] gibi hususlar üzerinde çalışılmıştır.

Yukarıda ayrıntılı olarak verilen bu ilkeler incelendiğinde, her ne kadar bu ilkeler tavsiye niteliğinde olsalar da bu ilkelerin kendinden sonra gelen ve başta Avrupa Birliği[71] olmak üzere uluslararası düzenlemelere ve bunun yanında ulusal düzenlemelere kaynak teşkil ettiği açıkça görülecektir.

2. Birleşmiş Milletler Tarafından Kişisel Verilerin Korunmasına İlişkin Hazırlanan Hukuki Düzenlemeler

Birleşmiş Milletler kişisel verilerin korunması konusunda" Bilgisayarla İşlenen Kişisel Veri Dosyalarına İlişkin Rehber İlkeler" isimli belgeyi 14 Ocak 1990 tarihinde kabul etmiştir. Bu belgede de tıpkı OECD tavsiye niteliğindeki ilkelerinde olduğu gibi, hukuki bir bağlayıcılığı olmayan tavsiye niteliğindeki ilkelerden oluşmaktadır. Söz konusu ilkeler aşağıdaki gibi sıralanabilecektir.[72] Ayrıca Birleşmiş Milletler tarafından aşağıda yer alan ilkelerin üye devletler tarafından uygulanabilmesi için bir denetim mekanizması oluşturulmuş olup bu anlamda kişisel verilere ilişkin bir otoritenin kurulmuş olması bakımından öncü niteliktedir. [73] Söz konusu ilkeler şu şekilde sıralanabilecektir:

- Hukuk ve Adalet Prensibi: Kişisel veriler hukuki ya da adil olmayan yöntemlerle toplanmama ve ayrıca Birleşmiş Milletler Sözleşmesi amaç ve prensiplerine aykırı olarak kullanılmamalıdır.

- Doğruluk Prensibi: Kişisel Verileri tutmakla yükümlü olan kişiler, düzenli olarak bu verilerin doğruluğunu kontrol etmek, herhangi bir ihmali hata oluşmaması için bu verilerin tam olduğundan emin olmak ve işlendikleri süre boyunca güncel tutmak sorumluluğundadırlar.

---

[70] Margaret Byrne Sedgewick, "Transborder Data Privacy as Trade", **California Law Review**, Vol. 105 **,** 1513, 2017, s.1527

[71] Cristina Blasi Casagran, **Global Data Protection in the Field of Law Enforcement - An EU Perspective**, Routledge, 2017, New York, s. 148

[72] Birleşmiş Milletler ilkeleri için bakınız. https://www.refworld.org/pdfid/3ddcafaac.pdf. 20.12.2018

[73] Ayözger, **Kişisel Verilerin Korunması- Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil**, s. 64

- Amacın Belirli Olması Prensibi: Kişisel verinin işlenmesine konu amaç belirli ve hukuka uygun olmalı ve amaçlar ilgili kişilere aleni bir şekilde bildirilmelidir.

- İlgili Kişi Tarafından Erişim Prensibi: Kişisel verisi işlenen kişinin, kimliğini ispatlaması halinde, veri işleyene ulaşma, verisi hakkında bilgi alma, gerektiğinde bu verilerin silinmesini ya da yok edilmesini talep etme hakkı olmalıdır.

- Ayrımcılık Yapmama Prensibi: Aksi hukuki mevzuat kapsamında belirtilmedikçe, ayrımcılığa sebebiyet verebilecek nitelikteki verilerin, kişinin ırki, etnik köken, cinsel hayat, politik görüş, dini görüş, felsefi ya da sair görüşleri ya da sendika üyeliği gibi verilerine ilişkin bilgiler toplanmamalıdır.

- İstisna Düzenleme Yapabilme Prensibi: Milli güvenlik, kamu güvenliği ve ahlakı ile ilgili olarak, kişisel veri sahibinin haklarına ilişkin olarak kanun koyucu tarafından istisna düzenlemeler yapılabileceğini ilişkin bir prensiptir.

- Güvenlik Prensibi: Kişisel veri dosyalarını hem kazayla kayıp ya da yok etme gibi olası tehlikelere karşı hem de yetkisiz erişim, bilgisayar virüsü gibi kasti tehlikelere karşı güvenlik önlemleri alınmalıdır.

- Denetim ve Yaptırım Prensibi: Kişisel verilerin korunması için, getirilen düzenlemelerin denetlenmesi ve gerekirse yaptırımların uygulanabilmesi için gerekli önlemleri alabilecek kurum ve kuruluş oluşturulmalıdır.

- Sınırötesi Veri Akışı Prensibi: İki veya daha fazla ülke arasında bir veri akışının olabilmesi için, bu ülkeler arasında veri koruma güvenliğine ilişkin denk düzeyde düzenlemeler bulunmalıdır.

Görüldüğü üzere bahsi geçen ilkeler, bugün kişisel verilerin korunması hukukuna yön veren temel oluşturan ilkelerdir.

3. Avrupa Konseyi Tarafından Kişisel Verilerin Korunması İlişkin Hazırlanan Hukuki Düzenlemeler

Bilindiği üzere Avrupa Konseyi'nin temel hak ve özgürlüklerin korunması alanındaki çalışmalarının en önemli adımı 4 Kasım 1950 yılında kabul ettiği Avrupa İnsan Hakları Sözleşmesi'dir. Bu sözleşme kapsamında bireylerin temel hak ve özgürlükleri korunmakta olup, bu konudaki en ünlü[74] yargı oranı ise Avrupa İnsan Hakları Mahkemesi olmuştur. Ancak Avrupa insan Hakları Sözleşmesi'nin hazırlandığı tarih itibariyle bu sözleşmeye kişisel verilerin korunmasına ilişkin herhangi bir madde konulması ihtiyacı söz konusu olmadığından, zaman içerisinde yaşanan teknolojik gelişmeler ve bireylerin kişisel verilerinin korunmasını talep etme hakkının artık temel bir insan hakkı statüne gelmesi üzerine, kişisel verilerinin korunması hakkı sözleşmenin 8.maddesi kapsamında değerlendirilmeye başlanmıştır.

Avrupa Konseyi ise kişisel verilerin dünya üzerindeki öneminin artması ve artık verinin yeni bir güç odağı haline gelmesi üzerine, doğrudan kişisel verilerin korunması üzerine bir sözleşme hazırlamıştır. 108 Sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi, 28 Ocak 1981 tarihinde imzaya açılarak, 01 Ekim 1985 tarihinde yürürlüğe girmiştir. Kişisel verilerin korunması adına Avrupa Konseyi tarafından hazırlanan ve bu alanda adeta bir dönüm noktası olan bu hukuki metni Türkiye 28 Ocak 1981 tarihinde imzalamıştır.

Çalışmamızın bundan sonraki kısmında kişisel verilerin korunması hususu, hem Avrupa İnsan Hakları Sözleşmesi bağlamında hem de 108 sayılı Kişisel Verilerin Otomatik Olarak İşlenmesi Sırasında Gerçek Kişilerin Korunmasın ilişkin Sözleşme. kapsamında ayrıntılı olarak değerlendirilmiştir.

a. Kişisel Verilerin Otomatik Olarak İşlenmesi Sırasında Gerçek Kişilerin Korunmasın ilişkin 108 Sayılı Sözleşme

108 sayılı Kişisel Verilerin Otomatik Olarak İşlenmesi Sırasında Gerçek Kişilerin Korunmasın ilişkin 108 Sayılı Sözleşme kişisel verilerin korunması açısından

---

[74] Ayözger, **Kişisel Verilerin Korunması- Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil**, s. 65

çok önemli bir yere sahiptir. Zira bu sözleşme kendisinden sonra gelen ve bu alanda düzenlenen her türlü hukuki metine kaynaklık etmiş ve yol gösterici olmuştur. [75]

Sözleşmeyi önemli kılan bir diğer özelliği ise bu sözleşme sadece konsey ülkelerine değil, konseyi ülkeleri dışında tüm 3. ülkelerin imzasına da açılmıştır.[76] Kişisel verilerin korunmasının yalnızca belirli ülkelerin değil, teknolojinin gelişmesiyle birlikte bu verilerin transferindeki kolaylık sebebiyle aslında global bir problem olduğunun kabulünün bu duruma sebebiyet verdiğini düşünmekteyiz.[77] Bu noktada belirtmek isteriz ki Türkiye sözleşmeyi 1981 yılında imzalamış olmasına rağmen, uygulama kanunu 2016 yılında çıkarmıştır. Nitekim sözleşme çerçeve niteliğinde olduğunda sözleşmenin uygulanması için ulusal hukuklarda onay kanunu çıkarılması gerekmektedir.[78] Bu sözleşme çalışmamızın 3. Bölümde incelenen 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun kaleme alınmasında oldukça etkili olmuştur. [79]

108 sayılı sözleşmenin 1. maddesinde kişisel verilerin yalnızca otomatik yollarla işlenenlerinin bu sözleşme kapsamındaki korumadan yararlanacağı ifade edilmiştir. Bu demektir ki, bir veri kayıt sisteminin parçası olsa bile otomatik yollarla işleme tabi tutulmayan veriler bu sözleşme kapsamında koruma alanı bulamayacaktır. Ancak doktrindeki bir görüşe göre, sözleşmenin tanımlar başlıklı 2. Maddesinde yer alan otomatik yöntemler kavramının tanımına göre, bu otomatik işlem kısmen ya da tamamen olabilecek olup, bu durum 1. Maddedeki ifadeyi yumuşatmaktadır. [80]

Sözleşmenin 3. Maddesinde ise bu sözleşmenin özel sektörde ve kamu sektöründe yer alan tüm veriler için uygulanabileceği ifade edilmiştir. Ayrıca aynı maddede taraf devletlere önemli opsiyonlar verilmiş ve eğer isterlerse kendi ülkelerindeki uygulama bakımından, bu sözleşmeyi, sadece gerçek kişileri değil tüzel

---

[75] Küzeci, **Kişisel Verilerin Korunması**, 2018, s. 133
[76] **İbid.**
[77] **İbid.**
[78] Ayözger, **Kişisel Verilerin Korunması Hukuku**, s. 68
[79] Murat Volkan Dülger, **İnsan Hakları ve Temel Hak ve Özgürlükler Bağlamında Kişisel Verilerin Korunması**, s.87. Dülger konuyu şöyle ifade etmektedir. "*Sözleşmenin Kanun'a neden ihtiyaç duyulduğunun detaylı olarak sayıldığı genel gerekçesinde 108 sayılı Sözleşmeye de atıf yapılmış ve Sözleşmenin Türkiye tarafından imzalandığının altı çizilmiştir.* "
[80] Küzeci, **Kişisel Verilerin Korunması**, 2018, s.134

kişileri de kapsayacak şekilde uygulayabileceklerini ve aynı zamanda otomatik olmayan veriler için de genişletebileceklerini ifade etmiştir.

Sözleşmenin 5. Maddesinde ise kişisel verilerin işlenmesine konusunda uyulması gereken ilkeler düzenlenmiştir. Bu maddeye göre kişisel veriler hukuka uygun şekilde toplanmalı, toplanan veriler toplanma amacına uygun şekilde ve yine bu amaçlar için yeterli şekilde işlenmeli, verilerin doğru olması ve gerekirse güncellenmesi ve toplanma amacının gerektirdiği süreyi aşmayacak biçimde veri sahibini belirlenebilir kılan şekilde saklanmalıdır.

Sözleşmenin 6.maddesinde ise hassas verilere ilişkin önemli bir düzenleme getirilmiştir. Bu düzenlemeye göre hassas verilerin otomatik olarak işlenmesi için gerekli önlemler alınmadıkça hassas verilerin otomatik yollar ile işlenmesi mümkün olmayacaktır. Sözleşmede hassas veri olarak kişilerin ırki, dini veya diğer inançlarına ilişkin her türlü kişisel verileri ile cinsel hayatına veya sağlığına ilişkin kişisel verileri sayılmıştır. Sözleşmenin 7.maddesinde ise kişisel verilerin işlenmesinden sonra bu verilerin korunması için alınması gereken önlemlere yer verilmiştir. Bu maddeye göre veriler herhangi bir yetkisiz erişime ya da yanlışlıkla kaybolmaya karşı mutlaka korunmalıdır.

Sözleşmenin 8.maddesinde kişisel veri sahibine tanınan haklar düzenlenmiş ve bu haklar kapsamında verilerinin işlenip işlenmediğini öğrenme, veri sorumlusu hakkında bilgi alma, verilerini düzeltme ya da sildirme ve bu hakları kullandırılmadığı takdirde bir başvuru yolundan yararlanma yani itiraz hakkı sıralanabilecektir.

Sözleşmenin 9. Maddesinde ise, bu sözleşme kapsamında düzenlenen 5,6 ve 8 yani verilerin niteliği, özel veri kategorileri ve kişilere tanınan güvencelere ilişkin maddelerine, ulusal güvenlik, kamu güvenli ve sağlığı, ulusal mali menfaatler veya suçun önlenebilmesi, bir kişinin veya sair kişilerin haklarının ve özgürlüklerinin korunması amacıyla bazı sınırlamalar getirilebileceği düzenlenmiştir.

Sözleşmenin en önemli maddelerinden biri ise kişisel verilerin sınır ötesi akışını düzenleyen 12. maddesidir. Bu maddeye göre özel hayatın korunması hakkına dayanarak veri transferi önlenemeyecek olsa da transfere konu ülkede transferi

gerçekleştirecek ülkede yer alan veri güvenliğine eş değer bir güvenlik yoksa ya da bu transfer taraf olmayan bir devlete yapılmak üzere bir taraf devlet üzerinden, mevzuat boşluklarından yararlanmak üzere yapılıyorsa bu durumda veri transferine sınırlamalar getirilebilecektir. Bu noktada 108 sayılı sözleşmeye ek 181 sayılı protokol ile veri transferi konusunda aranan eş değerlik kriterinin yeterlilik olarak ifade edildiğini de belirtmek isteriz.[81]

Zaman içerisinde teknolojinin gelişmesi ile kişisel verilerin güvenliği konusu çok daha önemli bir hal almaya başladığından ve bu konuda ihtiyaçlar değişerek arttığından, bu sözleşmeye ek 181 no.lu protokol düzenlenmiştir. Bu protokol ile sınır ötesi veri akışı ve denetim mekanizmaları kapsamında ek düzenlemeler getirilmiştir.[82]

Görüldüğü üzere 108 sayılı sözleşme her yönüyle, kendinde sonra gelen uluslararası ve ulusla veri koruma metinlerine öncülük etmiştir. Nitekim yukarıda incelediğimiz tüm ilkeler ve düzenlemeler bazı minör farklılıklarla da olsa bugün hala geçerliliğini korumaktadır. Bu bakımdan 108 sayılı sözleşmenin veri koruma hukuk bakımından ayrı bir öneminin olduğunu belirtmek yanlış olmayacaktır.

b. Avrupa İnsan Hakları Sözleşmesi

04 Kasım 1950 tarihinde kabul edilen Avrupa İnsan Hakları Sözleşmesi, 3 Eylül 1953 tarihinde yürürlüğe girmiş olup, esas amacı kişilerin kültürel, ekonomik, sosyal haklarından önce temel olarak sivil ve politik haklarının korunması olan bir sözleşmedir.[83]

Avrupa İnsan Hakları Sözleşmesi, ikinci dünya savaşı boyunca tüm dünyanın gözü önünde gerçekleştirilen insanlık suçları sonucunda, özellikle bireylerin devlete karşı daha fazla koruma altında olması, gerektiğinde devlete karşı hak arama olanaklarının artırılması ve insan hakları, demokrasi ve hukukun üstünlüğünü destekleyerek Avrupa'da sosyal, kültürel ve politik hayatın artırılması ihtiyacı ile

---

[81] Margaret Allars, **Perspectives on Privacy. Increasing Regulation in the USA, Canada, Australia and European Countries,** Dieter Dörr ve Russell L. Weaver, Berlin, Boston: De Gruyter, 2014, s. 108
[82] Ayözger, **Kişisel Verilerin Korunması Hukuku**, s.66
[83] Philipp Leach, "Taking a Case to the European Court of Human Rights", **Oxford University Press**, 2011, United Kingdom, s. 5

Avrupa Konseyi tarafından hazırlanmıştır. Türkiye bu sözleşmeyi 18 Mayıs 1954'te onaylanmış olmasına rağmen Avrupa İnsan Hakları Mahkemesi'nin yargı yetkisini bu tarihten çok sonra, 28 Ocak 1990 tarihinde kabul etmiştir.

Avrupa İnsan Hakları Sözleşmesi 59 madde ve ek protokollerden oluşmakta olup, çalışmamıza konu kişisel verilerin korunması hakkı Avrupa İnsan Hakları Sözleşme'nde bağımsız olarak yer almamıştır.[84] Avrupa İnsan Hakları Mahkemesi, bu hakkı 8. Maddesinde yer verilen özel hayat ve aile hayatına saygı hakkı altında değerlendirmektedir.

aa. AİHS madde 8 Kapsamında Kişisel Verilerin Korunması ve Müdahalenin Meşruluğu

Avrupa İnsan Hakları Sözleşmesi'ne baktığımızda kişisel verilerin korunması konusunda Sözleşme içerisinde direk bir madde bulunmadığını görmekteyiz. Ancak özellikle son 20 yılda teknolojinin gelişmesi ile beraber bireylerin kişisel verilerinin korunmasını talep etme hakkı öylesine önem kazanmış ve bu hakka yönelik müdahaleler bireylerin özel hayatını öylesine etkilemiştir ki, Avrupa İnsan Hakları Mahkemesi kişisel verilerin korunması hakkını, söz konusu sözleşmenin özel ve aile hayatına saygı başlıklı 8. Maddesi[85] kapsamında değerlendirmeye başlamıştır. Nitekim Avrupa İnsan Hakları Mahkemesinin kararlarında pek çok kez değindiği üzere, sözleşme yaşayan, canlı bir belge niteliğindedir.[86] Yani mahkeme, kararlarını verirken mutlaka günün koşullarını dikkate almakta ve değerlendirmelerini ve yorumlamalarını buna göre yapmaktadır.[87]

Mahkeme S. ve Marper v UK kararında[88], kişisel verilerin korunması konusunun, kişinin özel hayatı ve aile hayatının korunmasına saygı hakkı bakımından

---

[84] Küzeci, **Kişisel Verilerin Korunması**, 2018, s.138.

[85] Bu maddeye göre her bir bireyin özel hayatı ile aile yaşamına, ikamet ettiği konutuna, özel hayatı kapsamındaki yazışmalarına saygı gösterilmesini talep etme hakkı bulunmaktadır. Ayrıca maddenin ikinci fıkrasında ise bu hakka müdahale hususu düzenlenmiş ve bu müdahalenin şartlarından bahsedilmiştir. Buna göre bu hakka yalnızca kamu güvenliğinin söz konusu olması, ulusal güvenlik, suç işlemenin önlenmesi, hak ve özgürlüklerin korunması gibi sebeplerle kısıtlanabilecektir.

[86] Franziska Boehm, **Information Sharing and Data Protection in the Area of Freedom, Security and Justice**, Springer-Verlag Berlin Heidelberg, 2012, s.23

[87] George Letsas, **Constituting Europe: The European Court of Human Rights in a National, European and Global Context**, A. Føllesdal, B. Peters, & G. Ulfstein, Cambridge University Press, 2013, pp. 106-141, s. 2

[88] S. Marper vs UK kararında https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-90051%22]} Mahkeme söz konusu kararında, başvurucunun bir cezai yargılama kapsamında alınan parmak izi, hücre örneği ve DNA profilinin, ceza yargılaması başvurucu beraatı ile sonuçlanmış olmasına rağmen,

temel bir öneme sahip olduğunu ve sözleşmenin 8. Maddesi kapsamında garanti altında olduğunu belirtmiştir. Mahkeme bu kararında ayrıca kişisel verilerin sözleşmenin bu maddesine aykırı olacak şekilde kullanımı engellemek için ulusal hukuk kapsamında tüm uygun önlemlerin alınmasının zorunlu olduğunu da ifade etmiştir.

Avrupa İnsan Hakları Mahkemesi 8. madde kapsamında dört alanı korumaktadır. Bunlar özel hayat, aile hayatı, kişinin ev yaşamı ve yazışmaları olarak sıralanabilecektir.[89] Ayrıca devletin bu hak kapsamında hem negatif hem de pozitif yükümlülüğü bulunmaktadır. Bu noktada devletin negatif yükümlülüğü, kişilerin özel hayatına, aile hayatına, yazışmalarına ve ev hayatına müdahale etmemek, pozitif yükümlülüğü ise bireylerin işbu haklarına hem devlet hem de diğer bireyler ve özel teşebbüsler tarafından müdahale edilmesini önleyerek gerekli güvenlik önlemlerini almaktır.[90]

Sözleşmenin işbu 8.maddesi incelendiğinde görüleceği üzere maddenin birinci fıkrasında bireylerin özel hayatı kapsamında bireylerin özel ve aile hayatı, konutu ve yazışmaları sayılmıştır.

Maddenin ikinci fıkrasında ise bahsi geçen hakka müdahalenin sınırları çizilmiştir. Görüldüğü üzere sözleşme kapsamında bireylerin hakkı korunmakla beraber, kamu otoritelerinin fıkrada sayılan haller kapsamında bu hakka müdahale edebileceklerine ilişkin istisna getirilmiştir. Buna göre bahsi geçen hakka müdahale, bu müdahalenin yasayla düzenlenmiş olmasına bağlı olarak, yalnızca kamu güvenliği, ahlakı, kamu sağlığı veya hak ve özgürlüklerinin korunması için kamuyu ilgilendiren hayati haller doğmuşsa söz konusu olabilecektir.

---

tutulmaya devam edilmesini başvurucunun 8. Madde kapsamındaki özel hayat ve aile hayatına saygı hakkını ihlal ettiğini ve ceza yargılamalarında yeni teknolojilere öncülük eden her devletin bu teknolojilerin kullanımı konusunda doğru dengeyi sağlamak adına özel bir sorumluluk taşıdığını ifade etmiştir.

[89] Leach, **Taking a Case to the European Court of Human Rights**, s. 314. Ayrıca bakınız Murat Volkan Dülger, **İnsan Hakları ve Temel Hak ve Özgürlükler Bağlamında Kişisel Verilerin Korunması**, s.88

[90] **Ibid**.

bb. Avrupa İnsan Hakları Sözleşmesinin 8. Maddesi Kapsamında Verilmiş Kararlar

Mahkemenin Uzun Almanya'ya[91] karşı kararında, başvurucu, aşırı sol örgütlenmesi içinde bir bombalı saldırıya karışma şüphesi ile devlet tarafından GPS ile takip edilmesinin ve GPS ile elde edilen delillerin ceza yargılamasında delil olarak kullanılmasının özel hayatına müdahale olduğunu iddia etmiştir. Mahkeme ise bu kararında, elbette kişinin GPS ile izlenmesinin bu izleme sonucu kişiye ait kişisel verilerin elde edilmesinin kişinin özel hayatına bir müdahale olduğunu ancak bu müdahalenin ulusal güvenliğin korunması, kamu güvenliği ve suç önleme gibi hukuki amaçlar dahilinde yapıldığını belirterek bu olayda sözleşmenin 8. Maddesinin ihlal edilmediğini ifade etmiştir. Mahkeme aynı kararda, GPS ile izlemenin de orantılı bir müdahale olup olmadığını incelemiş ve başvurucunun diğer yöntemlerin yetersiz kalması sonucunda, üç ay gibi kısa bir süreliğine ve yalnızca aracıyla seyahat ederken izlendiğini, dolayısıyla başvurucun bütün ve kapsamlı bir izlemeye tabi tutulmadığını bu bakımdan şüphe konusu suçun son derece ciddi ve tehlikeli bir suç olduğu da göz önünde bulundurulduğunda demokratik bir toplumda başvurucunun GPS ile takip edilmesinin orantılı bir müdahale olduğunu ifade etmiştir. Mahkeme bahsi geçen kararında olayı 8. Maddenin 2. Fıkrası kapsamında değerlendirmiş ve ulusal güvenlik, kamu güvenliği gibi hususlar söz konusu olduğunda yasayla belirlenen sınırlara uygun olarak kişinin özel hayatına müdahale edilebileceğini vurgulamıştır. [92]

Mahkemenin Faiza Fransa'ya karşı kararında ise, başvurucu, yer tespiti için kendisine ait araca GPS yerleştirilmesini ve mahkeme kararı ile telefonlarının dinlenmesini sözleşmenin 8. Maddesi kapsamında özel hayatına müdahale olduğunu iddia etmiştir. Mahkeme bu olayda başvurucunun GPS ile izlenmesi sürecinde Fransa Hukuku'nda başvurucunun izlenme kapsamını, görevlilerin bu yetkilerini nasıl

---

[91] Uzun vs Almanya kararı için bakınız.https://hudoc.echr.coe.int/eng-press#{%22itemid%22:[%22003-3241790-3612154%22]}

[92] Mahkemenin ulusal güvenlik söz konusu olduğunda kamu otoritelerine müdahale alanı tanınması hususunda pek çok kararı bulunmaktadır. Bu kararlardan birinde mahkeme, karara konu devletin müdahalenin gerekli olup olmadığı, ulusal güvenliğin sağlanması için kullanılacak aracın belirlenmesi gibi hususlarda geniş bir takdir yetkisi tanıdığını ifade etmiş ve sözleşmeci devletlerin ulusal güvenliğin korunması amacıyla kişisel verilerin kaydı ve bu verilerin işe alım süreçlerinde değerlendirme için kullanılması konusunda kamu otoritelerine yetki tanıyabileceğini belirtmiştir. İlgili karar için bkz. Mahkemenin 26 Mart 1987 tarihli Leander v İsveç kararı. Ayrıca bakınız. Pieter van Dijk, Fried van Hoof, Arjen van Rijn, Leo Zwaak, **Theory and Practice of the European Convention on Human Rights**, Intersentia, Fourth Edition, C.2, 2006, Antwerpen – Oxford.

kullanacaklarına ilişkin bir kanun düzenlemesinin ya da yol gösterici bir mahkeme kararının olmadığını, bu bakımından başvurucunun demokratik bir toplumda sahip olması gereken minimum korumaya sahip olmadığını bu durumun ise sözleşmenin 8. Maddesinin ihlali olduğunu ifade etmiştir. Diğer yandan mahkeme başvurucunun telefonlarının dinlenmesini ve kaydedilmesini ise, organize bir çete tarafından uyuşturucu trafiğinin izlenmesi gibi ciddi bir suçunun önlenmesi amacını taşıdığı ve yasal dayanağı olan bir tedbir aracılığı ile başvurucunun da korunduğunu ve demokratik bir toplumda bu tedbirin orantılı olduğu gerekçeleriyle 8.maddenin ihlalinin söz konusu olmadığını ifade etmiştir.[93]

Görüldüğü üzere mahkeme her ne kadar olay bakımından devlet tarafından alınan tedbirler ve kullanılan yöntemler orantılı olsa da bu yöntemlerin yasal dayanağının bulunmaması halinde de 8. Maddenin ihlali yönünde karar vermektedir. Nitekim Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesinin 2. fıkrasında da kamu güvenliği, milli güvenlik ve sağlık gibi amaçlar dahilinde yapılacak müdahalelerin mutlaka yasal bir dayanağının olması gerektiği belirtilmiştir. Kaldı ki yukarıda da belirttiğimiz üzere mahkemenin 8. Madde kapsamında hem negatif hem de pozitif yükümlülükleri vardır. Bireylerin keyfi müdahalelere karşı korunması için gerekli hukuki düzenlemelerin yapılması da devletin pozitif yükümlülüklerinden biridir.

Mahkemenin Mustafa Sezgin Tanrıkulu Türkiye'ye[94] karşı kararında, başvurucu, kendisi ile beraber Türkiye'de bulunan herkesin, 2005 yılında verilen bir ulusal mahkeme kararına dayanarak bir buçuk ay boyunca iletişimin denetlenmesine tabi tutulduğunu, bu durumun ulusal mevzuatın ihlali olduğunu ve aynı zamanda devlet otoritelerinin kendisi tarafından yapılan hukuki başvuruyu reddetmeleri sebebiyle hukuki olarak bir çareye de başvuramadığını ileri sürmüştür. Mahkeme bu kararında denetlemeye ilişkin verilen yerel mahkeme kararının hukuka uygun olmadığını, başvurucunun 8. Madde kapsamındaki hakkının ihlal edildiğini ve aynı zamanda başvurucunun 13. Madde kapsamındaki hak arama özgürlüğünün de ihlal edildiğine karar vermiştir.

---

[93] Mahkemenin Faiza vs Fransa kararı için bakınız. https://hudoc.echr.coe.int/eng-press#{%22itemid%22:[%22003-5999245-7685292%22]}

[94] Mustafa Sezgin Tanrıkulu vs Türkiye kararı için bakınız. https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-175464%22]}

Mahkeme L.H Litvanya'ya[95] karşı kararında, başvurucu kendisine ait sağlık verilerinin rızası olmaksızın bir devlet kurumu tarafından toplanmasının özel hayatına hukuksuz bir müdahale olduğunu ve 8. Madde kapsamındaki hakkının ihlal edildiğini iddia etmiştir. Mahkeme bu kararında özel hayatın korunması hakkı kapsamında kişinin sağlık verilerinin korunmasının önemini hatırlattıktan sonra, Litvanya hukukunun, sorumluların yetkilerinin sınırları ve tedbirlerin uygulama şekli bakımından yeterli netliğe ve açıklığa sahip olmadığını ve özellikle Litvanya hukukunun söz konusu devlet kurumu tarafından toplanan sağlık verilerine ilişkin hiçbir sınırlama getirmediğini ve bu durumun başvurucunun sağlık verilerinin, ne amaçla olursa olsun, önceden bir değerlendirme yapılmaksızın periyodik olarak 7 yıldan beri toplanmasına sebebiyet verdiğini ifade ederek, 8.maddenin ihlal edildiğine kanaat getirmiştir. Mahkeme bu kararında, tüm ulusal ve uluslararası düzenlemeler kapsamında hassas veriler olarak kabul edilen sağlık verileri konusunda gösterilmesi gereken hassasiyeti bir kez daha vurgulamış ve özellikle hassas verilerin toplanması konusunda, veri sorumlusu bir devlet kurumu olsa dahi, bir sınırlama ve değerlendirmeye tabi tutulması gerektiğini ifade etmiştir.

Mahkemenin Barbulesco Romanya'ya karşı kararında, başvurucu, işverenin işten çıkarma kararının kendisinin özel hayatının ihlal edilmesi sonucunda verildiğini ve ulusal mahkemenin başvurucunun özel hayatının korunmasına yönelik hakkını korumadığını ileri sürmüştür. Mahkemeye göre, ulusal mahkeme başvurucunun işverenden iletişiminin denetlenme olasılığının bulunduğuna ya da bu denetlemenin kapsamına ya da bu denetlemenin seviyesine ilişkin olarak bir bilgilendirmede bulunup bulunmadığını değerlendirmeyerek hataya düşmüştür. Mahkeme ayrıca ulusal mahkemenin, işveren tarafından yapılan bu denetlemeyi meşru hale getiren sebeplerin olup olmadığını, işverenin başvurucunun özel hayatına daha az müdahale edebilecek yöntemleri kullanabilme ihtimalinin bulunup bulunmadığını da değerlendirmeyerek yine hataya düşmüştür. Bu bakımdan mahkemeye göre başvurucunun 8. Madde kapsamındaki hakkı ihlal edilmiştir.[96]

---

[95]Mahkemenin L.H Litvanya kararı için bakınız. https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22002-9365%22]}

[96] Mahkemenin Barbulesco vs Romanya kararı için bakınız. https://hudoc.echr.coe.int/eng-press#{%22itemid%22:[%22003-5825428-7419362%22]}

Görüldüğü üzere Mahkeme, bir çalışanın kişisel verilerinin denetlenebilmesi için işverenin daha önce çalışanı bu konuda bilgilendirmiş olmasını[97] ve söz konusu denetlemenin bu denetlemeyi gerektirecek makul sebepler bulunması halinde ve son çare olarak gerçekleştirilmesini aramıştır. Diğer yandan mahkeme işverene ait bilgisayar donanımında porno görüntüler bulunduran çalışanın işten çıkarılmasına yönelik vermiş olduğu bir kararında ise[98] işverenin çalışanın işyerine ait bilgisayarı sözleşmesel yükümlülüklerine ve mevzuata uygun kullanımını beklemek ve bunu garanti etmek gibi meşru bir amaca dayanarak bilgisayarı denetleme hakkına sahip olabileceğini belirtmiştir.

Mahkemenin özel hayatın ve aile hayatının korunması hakkı kapsamında kişisel verilerin korunması hakkı ile kamu güvenliği arasında kurmuş olduğu dengeye ilişkin B.B. v. France, Gardel v. France, M.B. v. France kararında[99] ise, başvurucu 15 yaşında bir çocuğa cinsel saldırı suçundan suçlu bulunarak cezalandırılmış ve bu sebeple devletin cinsel suçlular veri tabanına eklenmesine ilişkin olarak bu durumun sözleşmenin 8. Maddesini ihlal ettiğini iddia etmiştir. Mahkeme ise birey ve kamu yararı karşılaştırıldığında bu kişilerin devletin veri tabanına kaydedilmelerinin 8. Maddenin ihlali niteliği taşımadığını, ayrıca devletin bu kayıtları tutması bakımından özel bir süre öngörüldüğünü ve mahkeme tarafından orantılı bulunan bu sürenin sonunda başvurucunun bu verinin silinmesi hakkının devlet tarafından sağlandığını, ayrıca bu verilere yalnızca mahkeme, polis ve idari görevlilerin erişebildiğini de eklemiştir.

Mahkeme hassas verilerden olan kişinin politik görüşlerine ilişkin Catt United Kingdom'a karşı kararında[100] ise, başvurucunun polis kayıtlarında aşırı siyasi birey olarak kaydedilmiş olması ve başvurucu 94 yaşına gelmiş olmasına rağmen bu kaydın hala muhafaza edilmesine ilişkindir. Mahkeme başvurucunun politik görüşlerinin özel

---

[97] Hukukumuzda da mahkemenin bu kararına uygun bir uygulama yapılmakta olup, Yargıtay'da işçinin daha önce bilgilendirilmesi kaydıyla, işyerinde kullandığı bilgisayarının ve işyeri uzantılı e-mail adresinin işveren tarafından denetlenebileceğini belirmiştir. Ayrıntılı bilgi için bkz. Durmuş Tezcan, **"**Özel Hayatın Gizliliğini İhlal ve Kişisel Verilerin Kaydedilmesi Suçu ile İlgili Bazı Gözlemler", **İstanbul Üniversitesi Hukuk Fakültesi Dergisi**, C. LXXI, S. 1, 2013, s. 1159-1164,

[98] Mahkemenin Libert vs France kararı için bakınız. https://hudoc.echr.coe.int/eng-press#{%22itemid%22:[%22003-6014614-7713110%22]}

[99] Mahkemenin B.B. v. France, Gardel v. France, M.B. v. France kararları için bakınız https://hudoc.echr.coe.int/fre-press#{%22itemid%22:[%22003-4480954-5400075%22]}

[100] Mahkemenin Catt v. the United Kingdom kararı için bakınız. https://hudoc.echr.coe.int/fre-press#{%22itemid%22:[%22003-6308613-8238123%22]}

olarak korunması gereken verilerden olduğunu, başvurucunun daha önce bir şiddet eyleminin bulunmadığı ve yaşı sebebi ile bundan sonrasında da bulunamayacağını ve ayrıca her ne kadar başvurucunun kişisel verileri toplanırken bu durum meşru olarak gerekçelendirildiğini ancak aynı verilerin muhafaza edilmesinin ise meşru olarak gerekçelendirilmediğini de eklemiştir. Mahkeme sonuç olarak başvurucunun sözleşmenin 8.maddesi kapsamındaki hakkının ihlal edildiği kanaatine varmıştır.

Yukarıda yer alan kararlarda görüldüğü üzere Avrupa İnsan Hakları Mahkemesi, yaşayan hukuki metin olarak tasvir ettiği sözleşmenin 8.maddesinde yer alan Özel Hayat ve Aile Hayatına Saygı hakkı kapsamında, kişilerin özel hayatının da bir parçası olan kişisel verilerin korunması hakkını da korumakta ve bu konuya ilişkin başvuruları söz konusu madde çerçevesinde değerlendirmektedir.

4. Avrupa Birliği Nezdinde Kişisel Verilerin Korunması

a. Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Direktifi- 95/46/EC

24 Ekim 1995 tarihli Avrupa Birliği Kişisel Verilerin Korunması ve Verilerin Serbest Dolaşımına İlişkin Direktif olarak bilinen ve kısaca 95/46/EC sayılı Veri Koruma Direktifi olarak adlandırılan bu direktif, kişisel verilerin korunması için atılan adımlar arasında en önemlilerinden biri olup veri korumanın temellerinden[101] birini teşkil etmektedir. Zira bu direktif ile beraber hem birlik ülkelerine kişisel verilerin korunmasına ilişkin yüksek standartlar getirilirken hem de elektronik ticaretin ekonomide çok daha büyük bir yer kaplaması sebebiyle birlik ülkeleri içinde verilerin serbest dolaşıma ilişkin düzenlemeler yapılmıştır.[102]

Direktifin 1. Maddesinin birinci paragrafında, birlik ülkeleri özel hayatın korunması hakkı kapsamında bireylerin kişisel verilerini korumakla yükümlü

---

[101] Türkay Henkoğlu ve Bülent Yılmaz, "Avrupa Birliği (AB) Bilgi Güvenliği Politikaları", **Türk Kütüphaneciliği**, C. 27- 3, 2013, S. 451-471, s.460

[102] Paul M. Schwartz, "European Data Protection Law and Restrictions on International Data Flows", **80 Iowa Law Review**, 471, 1994, s.483. Ayrıca bkz. Hayrunnisa Özdemir, Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması, Ankara, Seçkin Yayınları, 2009'dan aktaran Ayözger, **Kişisel Verilerin Korunması Hukuku**, s. 74

tutulmuşlardır. Nitekim doktrinde de kişisel verilerin işlenmesi için atılacak her türlü adımın aslında bir anlamda özel hayata müdahale niteliği taşıdığı ifade edilmiştir. [103]

Maddenin ikinci paragrafında ise, birlik ülkelerinin, birinci paragrafta sağlanan korumayla bağlantılı nedenler için[104] birlik ülkeleri arasındaki veri akışını engellemeyecekleri ve yasaklamayacakları düzenlenmiştir. Maddenin ikinci paragrafı ile beraber, kişisel verilerin korunması ile bu verilere ulaşım arasındaki denge oluşturulmaya çalışılmıştır.[105] Direktif bu anlamda önemli bir yere sahiptir.

Direktifin bir diğer önemli maddesi ise, direktifin kapsamını düzenleyen 3.maddesidir. Nitekim bu madde kapsamında, otomatik yollarla ya da bu yollarla olmasa bile bir veri kayıt sisteminin parçası olarak işlenen ve gerçek kişilere ait verilerin, kişisel verilerin korunması başlığı altında değerlendirilebileceği belirtilmiştir. Bu bakımdan direktif ile yukarıda bahsedilen 108 sayılı Sözleşme karşılaştırıldığında, direktifin kişisel veri kavramını yalnızca gerçek kişiler ile sınırlandığı ve bu konuda çok daha net bir çizgi çektiğini söyleyebiliriz.[106] Direktif bu yönüyle kişisel verinin tanımına ilişkin hukukumuzda da yapılan pek çok tartışma açısından belirleyici olmuş ve kişisel verilerden anlaşılması gerekenin temel olarak gerçek kişilere ait veriler olduğunu ortaya koymuştur. [107]

Direktifin 6. Maddesinde ise kişisel veriler işlenirken dikkate alınması gereken temel prensiplere yer verilmiştir. Buna göre kişisel veriler adil şekilde işlenmeli, hukuka uygun şekilde işlenmeli, açık ve hukuken geçerliliği olan amaçlar ile işlenirken bu amaçlara da uygun şekilde toplanmalı, kişisel veriler tam ve eksiksiz şekilde bulundurulmalı ve yeri geldiğinde güncellenmeli[108], kişisel veriler söz konusu verilere uygulanan işlemin amacının gerektirdiği süre zarfında bulundurulmalıdır. Görüleceği

---

[103] Christian Koenig, Andreas Bartosch, Jens Daniel Braun, Marion Romes, **EC Competition and Telecommunications Law,** Second Edition, Kluwer Law International, 2009, UK, s. 519
[104] Ayözger, **Kişisel Verilerin Korunması Hukuku**, s. 74
[105] Henkoğlu- Yılmaz, **Avrupa Birliği (AB) Bilgi Güvenliği Politikaları**, s. 461
[106] G. González Fuster, **The Emergence of Personal Data Protection as a Fundamental Right of the EU**, Springer International Publishing, 2014, 274 pp, s. 136
[107] 2002/58/EC sayılı Elektronik Veri Koruma Direktifi kapsamında yalnızca gerçek kişileri değil tüzel kişileri de kapsamakta olup, bu konuya ilişkin ayrıntılı bilgi bu bölümde ayrıca inceleneceğinden tekrar olmaması adına bu başlıkta bahsedilmemiştir.
[108] Make Gilliot, Vashek Matyas and Sven Wohlgemuth, **Privacy and Identy, The Future of Identity in the Information Society- Challenges and Opportunities**, Kai Rannenberg, Denis Royer, André Deuker (Editors), Springer-Verlag Berlin Heidelberg, 2009, s.351

üzere bu prensipler bugün de geçerliliğini koruyan ve kişisel verilerin korunması alanına yön veren ilkeler arasındadır.

Direktifin 8. Maddesinde etnik ve ırki kökene, dini ve felsefi inanca, siyasi görüşe, sağlık ve cinsel hayata, sendika üyeliğine ilişkin verileri hassas veriler olarak tanımlamış ve işlenmeleri istisnai haller dışında yasaklanmıştır. Ancak hassas verilerin işlenmesini için istisnai hallerin düzenlenmiş olması, bu verilerin bu istisnai durumlarda direktifin koruması dışında kaldığı şekline yorumlanmamalıdır. Nitekim direktifte, hassas verilerin istisnai durumlarda işlenebilmesi için her türlü güvenlik önleminin alınması ve sürecin kontrol altında tutulması önemle vurgulanmıştır.[109]

Direktifin bir diğer kayda değer maddesi ise yeterli kişisel veri korumasının bulunmadığı ülkelere veri transferini yasaklayan 25. maddesidir. Bu anlamda komisyonun veri koruma konusunda güvenli olmadığını işaret ettiği ülkeler için tüm birlik ülkeleri gerekli tedbirleri almakla yükümlüdür.[110] Bu noktada Komisyonun ABD'ye ilişkin kararından ve Safe Harbour sözleşmesinden bahsetmek yerinde olacaktır. Direktifin 25. Maddesi çerçevesinde, her ne kadar Komisyon tarafından ABD'de veri güvenliği için yeterli tedbirin bulunmadığı işaret edilse de, elektronik ticaretin artması neticesinde ABD ile Safe Harbour anlaşması imzalanmış ve bu sözleşme kuralları sınırlarında AB ile ABD arasında veri akışı sağlanmıştır.[111] Ancak Avrupa Birliği Adalet Divanı tarafından 2015 yılında verilen '*Schrems*' kararı sonucunda söz konusu Safe Harbour anlaşması geçersiz kılınmıştır.[112] Bu karar veri koruması bakımından son derece önemli bir karar olup, bugün hala büyük şirketlerin veri transferiyle ilgili olarak yapılan şikayetler (elbette artık GDPR yani işbu direktifi mülga eden Avrupa Birliği Veri Koruma Tüzüğü'ne dayanarak) devam etmektedir.

---

[109] Cemil Kaya, "Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi", **İstanbul Üniversitesi Hukuk Fakültesi Dergisi,** 69 / 1-2, Aralık 2011, 317-334. s.324

[110] Henkoğlu- Yılmaz, **Avrupa Birliği (AB) Bilgi Güvenliği Politikaları,** s. 461

[111] Ayözger, **Kişisel Verilerin Korunması Hukuku**, s. 76

[112] Max Schrems, Facebook İrlanda Şirketi hakkında İrlanda Veri Koruma Komisyonuna bir şikâyette bulunmuştur. Söz konusu şikâyetin amacı, Facebook'un merkez ofislerinden birinin bulunduğu İrlanda'dan, Facebook'un, kod adı PRISM olarak bilinen ve ABD Ulusal Güvenlik Kurumu tarafından kişilerin internet kullanım ve iletişim verilerinin çeşitli şirketlerden kaydının toplandığı bir denetim programı kapsamında, ABD'ye kişilerin verilerini transfer etmesini engellemekti. Schrems bu şikayetinde direktifin yeterli veri korumasını sağmadığı sürece birlik üyesi olmayan ülkelere veri transferini yasaklayan 25. Maddesine dayanmıştır. Ulusal mahkemedeki süreç 2014 tarihinde Konunun Adalet Divanı'na taşınması amacı ile askıya alınmış ve divanın kararı beklenmiştir. 06 Ekim 2015 tarihinde Avrupa Adalet Divanı, Safe Harbour anlaşmasının geçersiz olduğuna karar vermiştir. Ayrıntılı bilgi için bkz. https://www.nytimes.com/2015/10/07/technology/european-union-us-data-collection.html

95/46/EC sayılı direktif ile veri sahiplerine getirilen haklar kapsamında, kişisel verinin işlenmesi ve bu verilerin kullanılmasına ilişkin olarak veri sahibinin bilgilendirilmesi, kişisel veri sahiplerinin verilerine ulaşma ve düzeltme hakkı gibi haklar sayılabilir. Direktifte ayrıca veri sahiplerinin başvurabileceği yargı yolları ve para cezaları ile devletlerin bu direktifin uygulanmasını denetlemeleri için bağımsız denetim organları kurmaları gereğini düzenlenmiştir.

Esasen direktif bir bütün olarak değerlendirildiğinde, kişisel verilerin korunması açısından kendisinden sonra gelen pek çok ulusal ve uluslararası düzenlemeye kaynaklık ettiği görülecektir. Zira direktifte yer alan pek çok prensip ve düzenleme, bugün bu direktifin yerini alan Avrupa Birliği Genel Veri Koruma Tüzüğü'nde de hala geçerliliği korumaktadır.

b. Elektronik Veri Koruma Direktifi – 2002/58/EC

95/46/EC sayılı Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Direktifinin 1995 yılında kabulünden sonra bu direktifin, elektronik haberleşme sektöründeki eksikliklerini kapatması ve bu alandaki boşluğu doldurması amacı ile 1997 tarihinde, 97/66/EC sayılı direktif kabul edilmiştir. Ancak bu direktifin zaman içerisinde mevcut pazara ve gelişen teknolojiye adapte edilememesi[113] ve 11 Eylül saldırılarının yarattığı ortam ile üye ülkelerin bu direktifin çıkarılması yönündeki artan baskıları[114] sebebiyle, 1997 tarihli bu direktifin yerine 2002/58/EC sayılı yeni bir direktif kabul edilmiştir. Esasen bu direktif, 95/46/EC sayılı Veri Koruma Direktifinin elektronik haberleşme sektörü için oluşturulmuş daha spesifik bir versiyonu niteliğindedir.[115] Öyle ki genel nitelikteki bazı veri koruma esasları için direktifin 14.maddesinde doğrudan 95/46/EC sayılı Veri Koruma

[113] Eloise Gratton, **Internet and Wireless Privacy - A Legal Guide to Global Business Practices**, CCH Canadian Limited, Kanada, 2003, s. 55
[114] Küzeci, **Kişisel Verilerin Korunması**, 2018, s. 190
[115] G. González Fuster, **The Emergence of Personal Data Protection as a Fundamental Right of the EU**, s.216

Direktifine atıf yapılmıştır. [116] Nitekim bu direktifte bahsedilmeyen ve veri koruma konularına ilişkin olarak 95/46/EC sayılı Veri Koruma Direktifi uygulanacaktır. [117]

Direktifin amacı özellikle başta telekomünikasyon sektöründe kişisel verilerin korunması olmak üzere temel hak ve özgürlüklerin korunmasında birlik ülkelerinde eş değer[118] bir koruma sağlamak ve söz konusu verilerin ve telekomünikasyon ekipmanları ve servislerinin serbest dolaşımını sağlamaktır.

Yukarıda da belirttiğimiz üzere bu direktif özel ve tamamlayıcı nitelikte bir direktif olduğundan, bu direktif yalnızca kamuya açık telekomünikasyon hizmetlerinin tarafı olan gerçek ya da tüzel kişiler için uygulama alanı bulacaktır. Direktif tüzel kişilerin verilerini koruması bakımından 1995 tarihli veri koruma direktifinden ayrılmaktadır.[119]

Ayrıca direktife göre elektronik iletişim ağları vasıtasıyla veri işlenmesi ya da kullanıcının terminal ekipmanında depolanan halihazırda verilere ulaşım sağlanabilmesi için, veri sahibinin veri işlemenin amaçları hakkında açık ve net bir şekilde bilgilendirilmesi ve bu müdahaleyi reddetme hakkının kendisine tanınmasını gerektirmektedir.[120] Görüldüğü üzere direktif, çerez olarak bilinen "cookies" ler ve benzer teknikler ile bireylerin mevcut verilerine erişimini ve bu verilerin takibini engellemek ve bu durumu yalnızca kullanıcıların ya da abonelerin rızasına bağlı olarak gerçekleştirilmesine izin vermek adına düzenleme yapmıştır.

Direktif kapsamında trafik bilgileri, lokasyon bilgileri gibi elektronik haberleşme ve telekomünikasyona konu ve veri koruma hukukunu yakından ilgilendiren konularda da bazı düzenlemeler yapılmıştır. Direktife göre birlik ülkeleri iletişimi ve trafik verilerinin gizliliğinin korunmasını temin etmekle ve bu iletişimlerin ve trafik datalarının dinlenmesini, takibe alınmasını ya da benzer yöntemlerle bu verilere müdahale edilmesini engellemekle yükümlüdürler.

---

[116] Elektronik Veri Koruma Direktifinin tam metni için bakınız. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31997L0066&from=EN

[117] European Commission, E-privacy Directive: **Assessment of Transposition, Effectiveness and Compatibility with Proposed Data Protection Regulation**, 2013, s.18

[118] ibid. s. 20

[119] Koenig, Bartosch, Braun, Romes, **EC Competition and Telecommunications Law**, s.521

[120] Gratton, **Internet and Wireless Privacy- A Legal Guide to Global Business Practices**, s. 55

Bunun yanında kullanıcılara ya da abonelere yönelik pazarlama mesajlarının iletilmesi konusunda da direktifte bir düzenleme yapılmış ve bu düzenlemeye göre kişilerin rızası olmaksızın bu kişilere fax, e-mail ve benzeri yollar ile ulaşılmasına izin verilmemesi gerektiği ifade edilmiştir.

Yukarıda da bu direktifin spesifik bir konu üzerine hazırlanmış olduğunu ve direktife göre bunun dışındaki veri koruma hususlarında 1995 tarihli Veri Koruma Direktifinin uygulanacağı belirtmiştik. Ancak aşağıda ayrıntılı olarak bahsedildiği üzere 25 Mayıs 2018 tarihinde Avrupa Birliği Genel Veri Koruma Tüzüğü yürürlüğe girmiş ve söz konusu direktifi mülga etmiştir. İnsan hak ve özgürlükleri bağlamında veri koruma konusunun çağın ihtiyaçlarına göre güncellenmesi, elektronik haberleşme sektöründeki 2002/58/EC sayılı direktif için de uzun süredir aynı taleplerin dile getirilmesine sebep olmuştur.[121] Avrupa Birliği yeni elektronik veri koruma regülasyonu için bir taslak metin hazırlayarak yayınlamıştır.[122] Önümüzdeki günlerde bu yeni düzenlemenin de yürürlüğe girmesi beklenmektedir.

c. Avrupa Birliği Vatandaşlık Hakkı Direktifi – 2009/136/EC

Avrupa Birliği Vatandaşlık Hakkı Direktifi olarak da bilinen 2009/136/EC sayılı direktif, 2002/58/EC sayılı Elektronik Veri Koruma Direktifini tadil eden bir direktif niteliğindedir. 2002/58/EC sayılı Elektronik Veri Koruma Direktifini genel olarak veri güvenliği ve ihlali konusundaki düzenlemeler daha ayrıntılı hale getirilmiştir.

Bu değişikliklerden birine örnek verecek olursak, 2002/58/EC sayılı Elektronik Veri Koruma Direktifinde *cookies* olarak da bilinen bilgisayar çerezleri aracılığı ile veri toplama işlemi yapılabilmesi için, kişinin daha önceden bilgilendirilmesi ve bu işlemi reddetme olanağının verilmesi gerektiği düzenlenmişti. 2009/136/EC sayılı direktif ile ise kişilerin bu işlemi reddetmesi değil yani negatif bir eylemsizliği değil, bu çerezler ile yapılan işlem hakkında bilgilendirildikten sonra onaylaması yani olumlu bir eylemi gerekmektedir. Bu tadil metni üzerinde çalışan Madde 29 Çalışma Grubu, bu konuyu tadil ederken, ortalama kullanıcıların çok büyük bir çoğunluğunun

---

[121] Küzeci, **Kişisel Verilerin Korunması**, 2018, s.193
[122] 10 Temmuz 2018 tarihli Gizlilik ve Elektronik İletişim Tüzüğü taslak metni için bakınız. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=consil:ST_10975_2018_INIT

çevrimiçi davranışlarının takibi konusunda farkındalık sahibi olmadıklarını ve bu yüzden bu konuda eylemsiz kalmalarının asıl iradelerini yansıtmayacağını tam tersi *opt-in* olarak da bilinen bir kabul iradesini açıkça ortaya koymaları gerektiğini ifade etmiştir.[123]

2002/58/EC sayılı Elektronik Veri Koruma Direktifinde 2009/136/EC sayılı direktif ile yapılan değişikliklerle beraber, hizmet sağlayıcılardan, kullanıcıların ya da abonelerin verilerini mevzuata uygun şekilde toplamaları ve muhafaza etmeleri, verileri erişimi yetkili kişiler ile sınırlı tutmaları, veri koruması için bu konuda kullanılabilecek teknolojik yöntemleri[124] kullanmaları beklenmektedir. Görüldüğü üzere bu direktif ile, 2002/58/EC sayılı Elektronik Veri Koruma Direktifinde yer alan bazı düzenlemeler gelişen teknolojiye ayak uydurmak ve bu teknoloji karşısında bireylerini veri güvenliğini artırmak amaçlanmıştır.

d. Avrupa Birliği Veri Saklama Direktifi – 2006/24/EC

Öncelikle bu direktifin Avrupa Birliği Adalet Divanı tarafından verilen 2014 tarihli karar ile geçersiz kılındığını belirtmek isteriz. Ancak bu direktifte 2014 yılına kadar veri koruma hukukunun bir parçası olduğundan, çalışmamız kapsamında bu direktife ve direktifin geçersiz sayılmasına sebebiyet veren hususlara yer verilmiştir.

Avrupa Birliği Adalet Divanı Nisan 2014'de vermiş olduğu bir karar ile 2006/24/EC sayılı Avrupa Birliği Veri Saklama Direktifini geçersiz kılmıştır. Divan bu kararında, söz konusu direktifin, Avrupa İnsan Hakları Sözleşmesi aracılığı ile bireylere verilen özel hayatın ve kişisel verilerin korunması haklarını önemli ölçüde ihlal ettiğini ayrıca ulusal yetkili otoritelerin verilere erişim konusundaki yetkilerini ve bunların sınırlarını belirlemediğini belirtmiş ve bu direktifi ulusal hukuklarına almış ülkeler için aksi yönde bir karar verilene kadar, bu direktifin geçersiz sayıldığı belirtmiştir. [125]

---

[123] Charles Wild, Stuart Weinstein, Neil MacEwan, Neal Geach, **Electronic and Mobile Commerce Law – An analysis of trade, finance, media and cybercrime in the digital age**, University of Hertfordshire Press, Great Britain, 2011, s.158

[124] George O.M. Yee, **Privacy Protection Measures and Technologies in Business Organizations-Aspects and Standarts**, IGI Global, USA, 2012, s. 333

[125] Theresa Papademetriou, "European Union: ECJ Invalidates Data Retention Directive", **Global Legal Research Center**, Haziran 2014, s. 1. İlgili rapor için bkz. https://www.loc.gov/law/help/eu-data-retention-directive/eu-data-retention-directive.pdf

Avrupa Birliği Veri Saklama Direktifi 2006 yılında birlik ülkelerinin terör olaylarından[126] duydukları kaygı neticesinde, Elektronik Veri Koruma Direktifi'nde kalan boşlukları doldurması amacıyla çıkarılmıştır. Zira bu direktifin giriş bölümüne bu direktifin düzenleme öngörmediği alanlarda Elektronik Veri Koruma Direktifinin ve Veri Koruma Direktifinin uygulanacağı belirtilmiştir.[127]

Bu direktifin 1. Maddesine göre direktifin amacı gerçek ya da tüzel kişi olabilecek tüm kullanıcıların ya da abonelerin trafik, lokasyon ve bu kişileri ya da kuruluşları belirlenebilir kılacak ilgili her türlü verinin muhafazası, veri türü, muhafaza süresi ve bu muhafazanın sair şartlarıdır.

Direktifin 4. Maddesinde, saklanan verilere erişimle ilgili olarak yalnızca ulusal otoritelerin, özel durumlarda ve ulusal hukuklarına uygun şekilde bu verilere erişebilecekleri, bu erişimin orantılılığı ve gerekliliği konusundaki düzenlemelerin her birlik ülkesi tarafından, Avrupa İnsan Hakları Sözleşmesi, Avrupa Birliği Hukuku ve uluslararası hukuk kuralları dikkate alınarak yapılacağı belirtilmiştir. Görüldüğü üzere bu maddede söz konusu verilere erişimle ilgili olarak direktif tarafından hiçbir sınırlama getirilmemiş ve bu konu tamam ülkelerin ve ulusal otoritelerin inisiyatifine bırakılmıştır. Nitekim 2014 yılında Avrupa Adalet Divanı tarafından verilen direktifi geçersizliğine ilişkin kararda bu maddenin de payı büyüktür.

Ancak direktifin geçersizlik kararından sonra Avrupa Birliğinde veri saklamaya ilişkin ek ya da yeni bir düzenlemenin gerekli olduğu konusunda bazı görüşler dile getirilmeye başlanmış ve hatta 15 Eylül 2017 tarihinde Avrupa Birliği Terörle Mücadele Koordinatörü veri saklama regülasyonu için çalışma raporunu sunmuştur.[128] Nitekim yukarıda da belirttiğimiz üzere bu direktifin çıkış noktası da esasen dünya üzerinde yaşanan terör olayları olduğundan, Avrupa Birliği nezdinde bu direktifin geçersizliğine ilişkin karardan sonra, aynı kaygılarla farklı bir düzenleme ihtiyacının yaşandığını görmekteyiz.

---

[126] Ayözger, **Kişisel Verilerin Korunması Hukuku**, s.78
[127] İlgili direktif metni için bkz.
https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF
[128] Söz konusu metin için bkz.
http://www.statewatch.org/news/2017/nov/eu-council-ctc-working-paper-data-retention-possibilities-wk-9699-17.pdf

e. Avrupa Birliği Genel Veri Koruma Tüzüğü

Günümüzde hızla artan teknolojik gelişmelerin ve globalleşmenin kişisel verilerin korunması bakımından yeni mücadele alanları yarattığı, ekonomik ve sosyal hayatı şekillendirdiği tartışmasızdır. Kişisel verilerin işlenmesi ve bu verilerin ulusal ve uluslararası olarak hem özel sektörde hem de kamu sektöründe kurum ve kuruluşlar arasında farklı amaçlarla paylaşımı dikkat çekici derece artmaktayken, Avrupa Birliği bu gelişmeler karşısında artık daha ayrıntılı, ihtiyaçlara cevap veren ve en önemlisi Avrupa Birliği ülkeleri arasındaki veri koruma esaslarında yeknesaklık oluşturabilecek yeni bir düzenleme için adımlar atmaya başladı. Her ne kadar 95/46/EC sayılı Veri Koruma Direktifi veri koruma hukuku bakımından son derece önemli bir adım olsa da artık güncellenmesi gerektiği uzun yıllardır dile getirilmekteydi. Bu ihtiyaçlar üzerine 24 Mayıs 2016 tarihinde Avrupa Birliği Genel Veri Koruma Tüzüğü yürürlüğe girmiş ve 1995 tarihli Veri Koruma Direktifini geçersiz kılmıştır. [129]

Avrupa Birliği Genel Veri Koruma Tüzüğü'nün amacı, birlik ülkeleri arasında ve/veya bu ülkelerden, birlik üyesi olmayan üçüncü ülkelere ve/veya uluslararası organizasyonlara veri transferini düzenlemek, veri güvenliği konusunda birlik oluşturarak veri korumasında tüm ülkelerde eşdeğer bir koruma sağlamak ve bu sayede veri sahiplerinin verilerinin korunduğuna ilişkin güvenlerini arttırarak elektronik ticaretin ve ekonominin gelişmesini sağlamaktır.[130]

Nitekim hem birlik ülkelerinde hem de bunlar dışındaki ülkelerde, veri koruma hukukuna ilişkin yeknesak ve eşdeğer bir korumanın olmayışı özellikle elektronik ticaret, internet üzerinden alışveriş gibi araçlarla hayatın çevrimiçi hale gelmeye başladığı bir dönemde, bireylerin verilerinin korunup korunmadığı ya da hangi kapsamda korunduğu ya da bu verilerin kimlerle ya da hangi kurum ve kuruluşlarla

---

[129] Birleşik Krallık'ın, Mart 2019 tarihli Brexit sonrası Avrupa Birliği üyesi ülkesi olmama ihtimali bulunduğundan, Avrupa Birliği Genel Veri Koruma Tüzüğü'nün uygulaması tartışma konusu olmuştur. Birleşik Krallık Mart 2019 tarihine kadar hala Avrupa Birliği üyesi olduğundan bu tarihe kadar Avrupa Birliği Genel Veri Koruma Tüzüğü ile bağlı olacaktır. Zira Avrupa Birliği Genel Veri Koruma Tüzüğü, 95/46/EC sayılı Direktiften farklı olarak, birlik üyesi ülkelerin herhangi bir onay kanunu çıkarmasına gerek olmaksızın doğrudan uygulanabilme bağlayıcılığına sahiptir. Ancak Birleşik Krallık, Brexit gerçekleşirse bundan sonrası için 1998 tarihli Veri Koruma Kanunu'nu mülga hale getiren bir kanun çıkarmıştır. Söz konusu kanunun genel olarak GDPR ile uyumlu olduğu söyleyebiliriz. (Bu tezin yazıldığı tarihte konuya ilişkin tartışmalar hala devam ettiğinden bu dipnot ihtimaller dahilinde yazılmıştır)

[130] Avrupa Birliği Genel Veri Koruma Tüzüğü'nün tam metni için bkz. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02016R0679-20160504&from=EN

paylaşıldığı yönünde soru işaretleri taşımalarına sebep olmuştur. Avrupa'da yapılan bir araştırma, Avrupa'da yaşayan insanların %67'sinin kişisel verilerinin korunması ile ilgili endişeleri olduğunu ve özellikle internet aracılığı ile paylaştıkları kişisel verileri üzerinde kontrol sahibi olmadıklarını düşündüklerini ortaya koymaktadır.[131]

Bu sebeplerle, 22 Haziran 2011 tarihinde Avrupa Veri Koruma Denetmeni, Konsey nezdinde mütalaasını sunmuş ve 25 Ocak 2012 tarihinde Avrupa Konseyi tarafından Avrupa dijital ekonomisinin desteklenmesi ve özel hayatın korunması hakkının güçlendirilmesi amacıyla teklif metni sunulmuştur. 07 Mart 2012 tarihinde Avrupa Konseyi tarafından sunulan teklif metnini içeren reform paketi Avrupa Veri Koruma Denetmeni tarafından kabul edilmiştir. Mevcut metin üzerine yapılan tartışmalar neticesinde Avrupa Konseyi, Avrupa Parlamentosu ve Avrupa Komisyonu tarafından 15 Aralık 2015 tarihinde tüzük metni üzerinde bir anlaşmaya varılmış ve üzerine anlaşmaya varılan metin Avrupa Parlamentosu tarafından 2016/679 sayı ile 27 Nisan 2016 tarihinde kabul edilmiş ve işbu düzenleme 25 Mayıs 2018 tarihinden itibaren uygulanmak üzere 24 Mayıs 2016 tarihinde yürürlüğe girmiştir.[132] Tüzük, hem 95/46/EC sayılı Veri Koruma Direktifinden farklı olarak pek çok yeni düzenlemeyi beraberinde getirmiş hem de bazı kavramların yeniden tanımlanmasına sebep olmuştur.

Tüzükle ilgili çok önemli bir konu ise, Tüzüğün yalnızca Avrupa Birliği ülkelerini değil, pratik olarak bu ülkelerle özellikle ekonomik bağlarını devam ettirmek isteyen tüm dünya ülkelerini ilgilendiriyor oluşudur. Globalleşen dünyada artık neredeyse tüm dünyanın bir ticaret ilişkisi içinde olduğu düşünüldüğünde, bu Tüzüğe uygun adım atmak dışında bir çare olmadığı açıktır. Nitekim bu Tüzük tüm Avrupa Birliği vatandaşlarının kişisel verilerini korumakta olup, bu ülkelerle herhangi bir şekilde işbirliği içinde olan tüm ülkeleri bağlamaktadır.[133]

Ayrıca tüzük ile belirlenen cezaların çok yüksek meblağlar olduğunu, veri güvenliğinin korunması için oldukça caydırıcı olduğunu da belirtmek isteriz. Nitekim Fransa çok yakın zamanda Tüzük'e dayanarak Google'a tam 57 milyon dolar ceza

---

[131] İlgili haber için bakınız. https://britishlegalitforum.com/wp-content/uploads/2017/02/GDPR-Whitepaper-British-Legal-Technology-Forum-2017-Sponsor.pdf

[132] Avrupa Birliği Genel Veri Koruma Tüzüğü'nün tarihçesi için bakınız. https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

[133] Jan Philipp Albrecht, "How the GDPR Will Change the World" **European Data Protection Law Review**, Volume 2, Issue 3, 2016, S. 287 – 289, s. 287

vermiştir. Bu ceza Avrupa Birliği Genel Veri Koruma Tüzüğü yani GDPR kapsamında verilen ilk ceza olma niteliğini taşımaktadır. [134]

aa. Kişisel Veri Kavramının Yeniden Tanımlanması

Avrupa Birliği Genel Veri Koruma Tüzüğü ile beraber kişisel veri kavramı hem günümüzün gereklerine hem de AİHM kararlarına uygun şekilde genişletilmiştir.

95/46/EC sayılı Veri Koruma Direktifi kapsamında kişisel veri belirli bir kişi ya da kimliği belirlenebilir gerçek kişi ile arasında bağlantı kurulmasını sağlayan her türlü bilgi ya da bir kişinin tanınmasını sağlayabilecek bireyin vatandaşlık numarası, finansal kimliği, psikolojik ya duygusal durumu gibi bilgiler olarak ifade edilmiştir.

Avrupa Birliği Genel Veri Koruma Tüzüğü kapsamında ise bu tanım genişletilerek, IP adresi, parmak izi alma, retina taraması gibi yollarla elde edilen kişilerin biyolojik dataları, lokasyon bilgisi, kişilerin fiziksel, psikolojik, genetik, mental, ekonomik, kültürel veya sosyal kimliği gibi verilerin tamamı kişisel veri olarak kabul edilmiştir.[135]

bb. Veri Kontrolörü ve Veri İşleyicisi

95/46/EC sayılı Veri Koruma Direktifi kapsamında yer verilmiş olan kontrolörü ve veri işleyicisi kavramlarına, Avrupa Birliği Genel Veri Koruma Tüzüğü kapsamında da yer verilmiş ve bu iki kavram Tüzük ile beraber daha ayrıntılı olarak düzenlenmiştir.

Avrupa Birliği Genel Veri Koruma Tüzüğünün tanımlar başlıklı.4. maddesinde veri sorumlusu kişisel veri işlenme sürecindeki amaçlara ve araçlara karar veren gerçek veya tüzel bir kişi, kamusal bir otorite, temsilci ya da diğer bir kamusal organdan oluşan bir organ olarak tanımlanırken, veri işleyicisi ise gerçek bir kişi,

---

[134] Google'a verilen bu cezanın sebebi, None of your Business ve La Quadrature du Net isimli iki organizasyonun, Google'ın Android cihazlardaki kurulum aşamasında kullanıcıları ilerleyebilmek için verilerinin işlenmesi konusunda rıza vermeye zorladığı yönünde yapılan şikayettir. Google bu şikayet sebebi ile Fransız mahkemeleri tarafından 57 milyon dolar cezaya çarptırılmıştır. https://www.itpro.co.uk/general-data-protection-regulation-gdpr/32811/france-issues-google-with-the-heaviest-gdpr-fine-to. 10.02.2019

[135] Avrupa Birliği Veri Koruma Tüzüğü'nün kişisel verilerin tanımını genişlettiğine ilişkin yazı için bakınız. https://www.kefron.com/blog/will-term-personal-data-defined-within-gdpr/ 10.02.2019.

kamusal bir otorite, temsilci ya da diğer bir kamusal organdan oluşan ve veri sorumlusu yerine veriyi işleyen organ olarak tanımlanmıştır.

Tüzüğün 24.maddesine göre Veri Kontrolörü işleme faaliyetinin mahiyeti, kapsamı, bağlamı ve amaçlarının yanı sıra gerçek kişilerin hakları ve özgürlükleri açısından olası riskleri dikkate alarak, veri işleme faaliyetinin Tüzük'e uygun şekilde gerçekleştiğini garanti edebilmek ve bunu gösterebilir durumda olmak için Tüzük'e uygun teknik ve tedbirleri uygulamakla yükümlüdür. Yine Tüzük'e göre söz konusu tedbirler gerekli olduğunda gözden geçirilir veya güncellenir. Tüzüğün 25. maddesi kapsamında ise Veri Kontrolörü veri işleme için kullanılacak yöntemlere karar verme anında ve veri işleme süreci anında takma isim verme (*pseudonymization*)[136], yalnızca gerekli ve yeterli verinin toplanması (*data minimisation)* gibi Tüzük'e uygun teknik ve tedbirleri uygulamakla ve yalnızca her bir amaç için gerekli olan veriyi işlemekle yükümlü tutulmuştur. Yine ilgili maddede bu yükümlülüğün verinin miktarı, kapsamı, depolama süresi ve ulaşılabilirliğine de uygulanması gerektiği öngörülmüştür.

Tüzüğün 28.maddesinde ise Veri İşleyicisinin sorumluluklarına yer verilmiştir. Buna göre Veri Kontrolörü adına Veri İşleyicisinin işlemleri yürüttüğü durumlarda, Veri Kontrolörü Veri İşleyicisini yalnızca veri işleme sürecinin Tüzüğün gerekliliklerini karşılayacak ve veri öznesinin haklarını koruyacak şekilde, Veri İşleyicisinin Tüzük'e uygun teknik ve tedbirleri uygulayacağının yeterli derecede garanti edilmesi halinde kullanabilecektir. Bu noktada Veri İşleyicisi ile Veri Kontrolörü arasındaki ilişki, veri işleme konusunu, süresini, amacını, verinin türünü ve kategorisini, Veri Kontrolörünün hak ve yükümlülüklerini gösteren bir sözleşme ile kurulabileceği gibi, Birlik veya Birlik üyesi ülkenin bir hukuki işlemi çerçevesinde de kurulabilecek ve her türlü sözleşme veya hukuki işlem Veri İşleyicisi için bağlayıcı nitelikte olacaktır. Bu durum Veri İşleyicisinin Veri Kontrolörü ile birlikte sorumlu olmasından kaynaklanmaktadır.

---

[136] Kişisel verilerin anonim hale getirerek muhafaza edilmesine ilişkin yöntemler sıklıkla kullanılsa da bunların ne kadar güvenli olduğu tartışılmaktadır. Zira verilerin yok edilmesi aşamasında da bir yöntem olarak kullanılan anonim hale getirme işleminin o kadar da güvenli ve kesin bir yöntem olmadığı, bazı araştırmacılar tarafından tersine işlem ile anonim bilgilerin ait olduğu bireylerin tespit edilerek ortaya konmuştur. Netflix şirketinin kullanıcılarının kişisel verilerinin anonim hale getirildiği bir olayda, araştırmacılar basit bilgi parçaları ile bu verilerin sahiplerini yeniden bulmuşlardır. İlgili haber için bakınız.https://www.computerworld.com/article/2987050/data-privacy/are-datasets-truly-anonymized-two-well-suited-researchers-are-going-to-find-out.html. 10.02.2019

Bu noktada Tüzükteki bir diğer önemli düzenleme ise Veri Kontrolörü ve/veya Veri İşleyicisi ile çalışan ve verilere ulaşım imkânı bulunan kişilerin Kontrolörün talimatı olmaksızın, Birlik veya Birlik üyesi devlet hukukundan kaynaklı bir gereklilik olmadığı müddetçe, veri işleme yetkisinin bulunmamasıdır. Bu noktada açıkça görülmektedir ki Tüzük, veri işleme yetkisini sadece Veri Kontrolörüne ve Veri İşleyicisine tanımıştır. Görüldüğü üzere 95/46/EC sayılı Veri Koruma Direktifinden farklı olarak Tüzük kapsamında Veri İşleyicisi de Veri Kontrolörü ile birlikte hatalardan ve veri güvenliğinden sorumlu tutulacaktır.

Tüzük kapsamındaki bir diğer düzenleme ise Veri Koruma Yetkilisidir. Tüzük'e göre Veri Kontrolörü veya Veri İşleyicisinin temel faaliyetlerinin veri sahibinin düzenli ve sistematik olarak denetlenmesini içermesi halinde Veri Koruma Yetkilisi atanmak zorundadır. Veri Koruma Yetkilisi kurum veya kuruluşta çalışan herhangi bir kişi olabileceği gibi, veri toplama ve işleme süreçleri konusunda bilgi sahibi herhangi bir kişi de olabilir. Tüzük ile getirilen düzenlemeye göre iki yüz elli kişiden çok çalışanı olan kurum ve kuruluşların Veri Kontrolörü ve Veri İşleyicisi veri toplama ve işleme süreçlerine ilişkin tüm dokümanları muhafaza etmekle veri ihlali riskinin yüksek olduğu yerlerde ayrıntılı değerlendirmeler yapmakla yükümlüdürler.

Veri Kontrolörü ve Veri İşleyicisi veri işlemeden veri depolamaya tüm süreçlerde Denetim Otoritesini bilgilendirmekle yükümlüdürler. Denetim Otoritesi Tüzük kapsamında denetim yapmaya yetkili ve Birlik Üyesi Ülke tarafından kurulmuş bağımsız kamusal otoriteyi ifade etmektedir. Tüzüğün 33. maddesinde Veri Kontrolörü ve Veri İşleyicisinin, herhangi bir veri koruma ihlalinden haberdar olmalarından itibaren en geç yetmiş iki (72 saat) içinde Denetim Otoritesini bilgilendirmekle yükümlü oldukları ve bu bilgilendirmenin söz konusu süreyi geçtikten sonra yapılması halinde, bilgilendirmenin gecikmenin sebepleri ile birlikte sunulması gerektiği düzenlenmiştir. Tüzüğün 34.maddesinde ise ihlale konu verinin, gerçek kişinin hak ve özgürlüklerini yüksek derecede riske atması ile sonuçlanma ihtimali varsa, bu ihlalin en kısa zaman Veri Sahibine de bildirilmesi gerekmekte olduğu ve bu bilgilendirmenin Kontrolör tarafından yapılmaması halinde Denetim Otoritesinin de risk değerlendirmesi yaparak bu bilgilendirmeyi veri sahibine yapabileceği öngörülmüştür.

Görüldüğü üzere Tüzük kapsamında veri işleme süreçleri için yeni sorumlu pozisyonlar oluşturulmuştur. Avrupa Birliği ülkelerinde faaliyet gösteren veya bu ülkelerin dışında olan ancak Birlik ülkelerinde ikamet eden gerçek kişilerin verilerine sahip kurum ve kuruluşların 25 Mayıs 2018 tarihi sonrasında sıkça aşina olacakları bu sorumluluklar kanımca Tüzük ile getirilen yeni düzenlemelerin en önemlilerinden birini oluşturmaktadır.

cc. Verinin Olağan Korunması ve Özel Önlemler ile Korunması

Tüzüğün 25. Maddesi çerçevesinde kişisel verilerin korunmasına ilişkin olarak bu verilerin korunma yöntemleriyle ilgili bir ayrıma gidilmiş ve verilerin özel yöntemlerle ve olağan yöntemlerle korunması esaslarından bahsedilmiştir.

Bahsi geçen maddede *data protection by design* olarak ifade edilen özel veri koruma yöntemi ile, Kontrolörün hem veri işleme için kullanılacak yöntemlerin belirlenmesi aşamasında hem de verilerin işlendiği aşamada yalnızca gerekli ve yeterli verinin toplanması (*data minimisation*) gibi veri koruma ilkelerinin etkili bir şekilde uygulamasını ve bu Tüzüğün gerekliliklerinin yerine getirilmesine yönelik olarak gerekli güvencelerin entegre edilmesi amacı ile tasarlanan takma isim verme (*pseudonymisation*) gibi uygun teknik ve düzenlemeye ilişkin tedbirleri uygulanarak veri sahiplerinin haklarını koruması yükümlülüğü düzenlemiştir. Görüldüğü üzere Tüzüğün ilgili maddesinde, Kontrolörün veri sahiplerinin haklarını koruyabilmek için özel ve Kontrolörün ek faaliyetini gerektiren önlemler alması gerektiği düzenlenmiştir. Esasen Tüzükte *data protection by design olarak* ifade edilen ve takma isim verme olarak ifade edilebilecek *pseudonymisation* gibi yöntemlerin örnek olarak gösterildiği bu koruma şekli, Tüzüğün yürürlüğe girmesinden önce de veri koruma hukukun bir parçası olarak kullanılmaktaydı. [137] Tüzükle birlikte verilerin korunması için alınan ve Kontrolörün ek faaliyetini gerektiren bu tip önlemler *data protection by design* olarak ifade edilerek ilk kez hukuki olarak düzenlenmiştir. [138]

---

[137] Bu noktada *Pseudonymization* ve *Anonymization* yani takma isim verme ve anonim hale getirme gibi veri koruma dünyası bakımından sıkça karıştırılan iki kavramın birbirinden farklı olduğunu ve farklı amaçlara hizmet ettiğini hatırlatmanın faydalı olacağı görüşündeyim. *Pseudonymization* veri sahibinin kimliğinin yerine farklı/takma bir kimlik kullanılması ve gerçek kimliğin yeniden ortaya çıkması için ek bir bilgiye ihtiyaç duyulan bir veri depolama yöntemidir. *Anonymization* yani anonim hale getirme ise kişisel verinin silinmesi, yok edilmesi gündeme geldiğinde uygulanan ve söz konusu kişisel verinin, veri sahibi ile tamamen ve geri dönülemez şekilde ilişkilendirilmesini engelleyen bir kişisel veri yok etme yöntemidir. https://www.protegrity.com/pseudonymization-vs-anonymization-help-gdpr/

[138] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/

Tüzükte *data protection by default* olarak ifade edilen veri koruma yöntemi ise Kontrolörün her bir kişisel veri işleme amacı için yalnızca yeterli ve gerekli verinin toplanması için uygun teknik ve organizasyonel tedbirlerin almasını ve toplanılan kişisel verilerin topladığı kişisel verinin miktarı, işlenen verinin kapsamı, depolama süresi ve ulaşılabilirliği ile ilgili bir yöntemdir ve Tüzüğe göre özellikle bu tedbirlerin bireylerin açık müdahalesi olmaksızın kişisel verilerinin belirsiz sayıda kişi tarafından ulaşılabilir olmamasını da sağlaması gerekmektedir. Örnek vermek gerekirse, bir sosyal medya sitesine üyelik yapan bireyin, sosyal medya sitesine üyeliğinin ilk anında kişisel verileri kendiliğinden, Tüzüğün deyimi ile *default* olarak sitenin amacına uygun şekilde işleyebilmesi için yeterli olanı kadarıyla ve sınırlı olarak diğer kullanıcılarla paylaşılmalıdır. Yani kişinin adı soyadı gibi kişisel verileri kendiliğinden profilinde yer alabilecekse de, yaşı ve cep telefonu numarası gibi amacını aşan kişisel veriler ancak bireyin kendi arzusu ve müdahalesi ile sonradan paylaşılabilir hale getirilmelidir.[139]

dd. Veri Sahibinin Hakları

Tüzüğün 12. ve 23.maddeleri arasında Veri Sahibine tanınan haklar ayrıntılı olarak düzenlenmiştir. Buna göre Tüzük kapsamında veri sahibinin bilgilerine erişim hakkı, bilgilerin düzeltmesini talep etme hakkı, verilerin silinmesini talep etme hakkı, veri işlemeyi sınırlama hakkı verinin işlenmesine itiraz etme hakkı bulunmaktadır. Bu hakların bir yönüyle bir önceki Veri Koruma Direktifi'nde de yer verilmiş ancak tüzük kapsamında daha ayrıntılı olarak düzenlenen haklardır.

Tüzüğe göre, kişilerin verilerine erişim hakkını kullanabilmeleri için öncelikle veri kontrolörü tarafından bireylere verilerinin işlenmesi akabinde, veri kontrolörünün iletişim bilgileri, verilerinin hangi amaçla işlendiği, hangi veri kategorilerinin işlendiği, süresi, bu verilerin kimlere aktarılacağı gibi bilgilerin verilmesi gerekmektedir. Bu bilgiler verildikten sonra, veri sahibinin tüzük kapsamında kendisine tanınan erişim hakkını kullanması da mümkün olabilecektir.

Kişisel verilerin işlenmesinden sonra bireylerin, verilerine erişme hakkı bulunduğu için, bu bilgilerin yanlış ya da eksik olması halinde bireylerin bu verileri düzeltme hakkı da tüzük kapsamında bireylere tanınmıştır.

---

[139] https://www.ics.ie/news/what-is-privacy-by-design-a-default

Tüzüğün bireylere tanımış olduğu en önemli haklardan biri ise, bireylerin kişisel verilerinin silinmesini talep etme yani unutulma hakkıdır. Unutulma hakkına ilişkin olarak çalışmamızın ilk bölümünde ayrıntılı açıklamalar yapıldığından bu açıklamalar tekrar olmaması açısından yinelenmeyecektir. Ancak Tüzük taslak aşamasındayken bu hakkın unutulma hakkı olarak kaleme alındığını daha sonra ise kişisel verilerin silinmesini talep etme hakkı olarak değiştirildiğini de belirtmek isteriz. Esasen bu değişiklik kanımızca yerinde olmuştur. Zira veri kontrolörüne edilgen bir yükümlülük yükleyen unutulma hakkının yerine verilerin silinmesini talep etme hakkı ile veri sahibine etkin bir yükümlülük yüklenmesi uygulama açısından daha pratik bir yaklaşım olmuştur. [140]

Bunun dışında ise, veri sahibine Tüzükte belirlenen durumlarda veri kontrolörünün veri işleme faaliyetini kısıtlama hakkı verilmiştir. Bu haller kişisel verilerin doğruluğuna veri sahibi tarafından itiraz edilmesi, işleme faaliyetinin yasa dışı olması ve veri sahibinin kişisel verilerin silinmesine itiraz etmesi ve bunun yerine verilerin kullanımının kısıtlanmasını talep etmesi, kontrolörün işleme amaçlarına yönelik olarak artık kişisel verilere ihtiyaç duymaması, ancak veri sahibinin iddiaların karşısında söz konusu verilere ihtiyaç duyması; kontrolörün meşru gerekçelerinin veri sahibinin meşru gerekçelerine ağır basıp basmadığı doğrulanması olarak sayılabilecektir.

B. ULUSAL DÜZENLEMELER

1. Yabancı Ülke Hukuklarında Kişisel Verilerin Korunması

a. Fransa

Fransa'da kişisel verilerin korunması konusu Türkiye'de olduğu gibi hem Fransız Ceza Kanunu çerçevesinde hem de bu konuya özgü özel bir kanun kapsamında korunmaktadır. Bu konuya ilişkin olarak ilk olarak 1978 tarihli ve içerisinde kişisel verilerin korunmasına ilişkin maddeler içeren 6 Ocak 1978 tarihli Bilgi Teknolojisi, Veri Dosyaları ve Sivil Özgürlükler kanunu ile Avrupa Birliği Genel Veri Koruma Tüzüğü'nün yürürlüğe girmesi ile birlikte kabul edilen ve 1978 tarihli kanunu büyük ölçüde değiştirerek Tüzüğe uyumlu hale getiren 21 Haziran 2018 tarihli değişiklikleri ifade edip akabinde Fransız Ceza Kanunu'nda kişisel verilerin korunmasına ilişkin maddelerden bahsedeceğiz. Dolayısıyla bu noktada Fransa'da kişisel verilerin

[140] Ayözger, **Kişisel Verilerin Korunması Hukuku**, s.41

korunması hukuku kapsamında bir hukuka aykırılık söz konusu olduğunda bunun hem medeni hukuk bağlamında hem de ceza hukuku kapsamında yaptırımı olduğunu belirtmek gerekmektedir. [141]

Öncelikle Fransa'da kişisel verilerin korunmasına ilişkin olarak faaliyet gösteren CNIL (*Commission Nationale de l'informatique et des libertés)* yani Ulusal Veri Koruma Komisyonu, 6 Ocak 1978 tarihli Bilgi Teknolojisi, Veri Dosyaları ve Sivil Özgürlükler kanununa dayalı olarak kurulmuştur.[142] Esasen bu komisyonun kuruluşu da söz konusu kanunun çıkarılması da Fransa'da 1970'lerin ortasında yaşanan ve dönemin siyasilerinin istifa etmek zorunda kalmasına yol açan SAFARI programı skandalına dayanmaktadır. Bu olayın Fransa'da duyulması ile beraber Fransa halkı ayaklanmış ve verilerinin korunması konusunda önlem alınmasını ve hukuki koruma getirilmesini talep etmiştir. [143] İşte bunun sonucunda bahsi geçen kanun çıkarılmış ve veri korumaya ilişkin bağımsız bu otorite kurulmuştur.

Esasen 1978 tarihli kanunun gelişimine şöyle bir baktığımızda, bu kanunun öncelikle 2004 yılında bir değişikliğe uğradığını görüyoruz. Bu değişikliğin sebebi ise 1995 tarihli Avrupa Birliği Veri Koruma Direktifi ile Avrupa Birliği veri koruma hukukuna getirilen yeni düzenlemelerin, söz konusu kanuna yansıtılmasıdır. Görüldüğü üzere Fransa 1995 tarihli Veri Koruma Direktifini ulusal kanuna oldukça geç yansıtmıştır. Bu durumun ortaya çıkmasında Fransa'da kişisel verilerin uzun süre ağırlıklı olarak Fransız Ceza Kanunu kapsamında korunmaya çalışılmasının payı olduğunu ifade etmek yanlış olmayacaktır. Zira yukarıda da belirttiğimiz üzere ülkemizde de uzun yıllar aynı sistem benimsenmiştir. 2004 yılındaki bu değişikliğin akabinde ise kanun 2009, 2010, 2011, 2013 ve 2014 yıllarında pek çok kez değişikliğe maruz kalmış ve son olarak Avrupa Birliği Veri Koruma Tüzüğü'ne uyum sürecinde 20 Haziran 2018 tarihinde değiştirilmiştir. Bu kez değişiklik için uzun süre beklenmemesinin sebebinin ise Tüzüğün, 1995 tarihli Veri Koruma Direktifinden

---

[141] Thomas W. Golden, Steven L. Skalak, Mona M. Clayton, Jessica S. Pill, **A Guide to Forensic Accounting Investigation**, Second Edition, New Jersey, Wiley&Sons, Inc., s. 160

[142] Korkmaz, **Kişisel Verilerin Ceza Hukuku Kapsaminda Korunması**, s.218

[143] Le Monde gazetesinde yer alan bir haber neticesinde, Fransız halkı, devletin bireylerin kişisel verilerini topladığı merkezi bir veri tabanı oluşturduğunu, çeşitli devlet yetkilileri tarafından bireylerin sosyal güvenlik numaraları üzerinden bu veri tabanında kayıtlı tüm kişisel verilere ulaşıldığını ve bu sürecin SAFARI isimli program kapsamında yürütüldüğünü öğrenmişlerdir. Bunun sonucunda ise Fransa'da hem programa karşı hem de hükümete karşı eylemler başlamıştır. Bu eylemler Fransa'da veri korumaya ilişkin bir kanun çıkarılmasını ve bu kanuna dayanarak bir Ulusal Veri Koruma Komisyonunun kurulmasını sağlamıştır. Çevrimiçi https://www.dw.com/en/france-maintains-long-tradition-of-data-protection/a-14797711 Erişim Tarihi: 21.02.2019

farklı olarak ulusal hukukta uygulanmak üzere bir onay kanuna ihtiyaç duymaması yani doğrudan uygulanabilir nitelikte olması ve yaptırımların ağırlığı olduğunu düşünmekteyiz.

Öncelikle bahsi geçen 1978 tarihli kanunu incelediğimizde, öncelikle bu kanunun 'Prensipler ve İlkeler' başlıklı birinci bölümünün 1. maddesine baktığımızda bilgi teknolojilerinin her vatandaşın hizmetinde olması gerektiği, bilgi teknolojilerinin gelişiminin uluslararası iş birliği açısından kurucu nitelikte olduğu ve ancak bireysel ve toplumsal hak ve özgürlükleri ve özel hayatı ihlal edemeyeceği ifade edilmiştir. Görüldüğü üzere Fransa'da 1978 yılından itibaren kişisel verilerin korunması hukuku açısından insan hakları yaklaşımı benimsenmiştir.

Aynı bölümün ikinci maddesinde ise kanun kapsamı, kişisel veri, kişisel veri işleme, veri kayıt sistemi, veri sahibi gibi kavramların tanımları yapılmıştır. Buna göre tüm bu kavramların uluslararası düzenlemelere paralel olduğunu söyleyebiliriz. Örneğin işbu madde çerçevesinde kişisel veri, "*…kişinin kimlik numarasına ya da bir veya birden fazla faktöre atıf yapmak aracılığı ile kimliği belirli ya da belirlenebilir gerçek kişiye ait tüm bilgiler…"* olarak tanımlanmıştır. Kanunun 3. Maddesinde ise Tüzük ile uyumlu olarak veri sorumlusu, kanunun 4. maddesinde kanun kapsamı dışında kalan hallere yer verilmiştir.

Kanunun ikinci bölümünde ise yine Tüzükle uyumlu olarak ilk olarak veri işlemenin genel ilkelerine yer verilmiştir. Nitekim kanunun 6. maddesinde kişisel verilerin, hukuka uygun şekilde; özelleştirilmiş, sınırlı ve hukuka uygun amaçlar için; amaçla bağlantılı ve yeteri kadar; doğru, tam ve gerekirse güncellenerek; yalnızca amacın gerektirdiği süreyle sınırlı olarak ve veri sahibinin belirlemeye izin verecek şekilde, işlenebileceği ifade edilmiştir. Kanununun 7. maddesinde ise kişisel verilerin yalnızca kişilerin açık rızası bulunması halinde ya da kanun kapsamında, kişinin hayatını korumak için gerekli olması, kamu hizmetinin yerine getirilmesi gibi sınırlı olarak sayılan sebepler ile işlenebileceği belirlenmiştir. Kanununun 8.maddesinde önemli bir düzenlemeye yer verilerek özel nitelikli hassas verilere ilişkin düzenleme yapılmıştır. Bu düzenlemeye göre kişilerin, ırk, etnik politik, felsefi, dini veya sendikal bilgileri ile sağlık ve cinsel hayatına ilişkin verileri özel nitelikli hassas veri kapsamında sayılmış ve kanunda sayılan belirli haller dışında bu verilerin işlenmesi yasaklanmıştır.

Kanunun 3. ve 4. bölümünde ise yukarıda da bahsettiğimiz üzere Fransa Ulusal Veri Koruma Komisyonunun kuruluşuna ilişkin bilgiler ve veri işleme sürecinde bu komisyona bildirilmesi gereken hususlar, Komisyon ile veri sorumluları arasındaki ilişkiler, veri sorumluların kaydı gibi konulara ayrıntılı olarak yer verilmiştir. Buna ek olarak kanunun 6. bölümünde ise veri işleme sürecinin denetimine ilişkin yine Veri Koruma Komisyonunun görevlerine ilişkin düzenlemelere yer verilmiştir.

Kanunun 5. bölümünde ise veri sorumlularının yükümlülükleri ile veri sahibinin hakları düzenlenmiştir. Bu bölümde kanunun 32 ve 38. maddeleri arasında veri sorumlularının yükümlülükleri sayılmıştır. Buna göre veri sorumluları öncelikle verileri işlenen veri sahiplerine kendileri ya da temsilcilerine ait isim, adres, telefon gibi tüm bilgileri vermekle, veri sahiplerinden elde ettikleri ve işledikleri verilerin güvenliğini sağlamakla yükümlüdürler. Diğer yandan veri sorumluları adına veri işleyen kişiler ise yine aynı bölümde, sadece veri sorumlularının talimatı ile veri işlemekle ve veri sorumlusuna verilerin güvenliğine ve gizliliğine ilişkin önlemleri aldığına ilişkin garanti vermekle yükümlüdür. Bu noktada belirtmek gerekir ki veri işleyicisinin bu garanti yükümlülüğü veri sorumlusunun veri işleyicisi tarafından alınan önlemleri denetim yükümlülüğünü ortadan kaldırmayacaktır. Veri Sahibinin hakları ise kanunun 38. ve 44. maddeleri arasında sayılmıştır. Buna göre veri sahibi, verisinin işlenmesine meşru bir sebeple itiraz etmek hakkı, veri sorumlusu ya da işleyicisinden verilerine ilişkin bilgi alma, verilerin silinmesini, değiştirilmesini ya da güncellenmesini talep etme gibi haklara sahiptir. Elbette bu haklara ilişkin bazı istisnalar ve özellikli durumlara da kanunda yer verilmiştir.

Kanunun 7. bölümünde, Ulusal Veri Koruma Komisyonu tarafından verilebilecek idari yaptırımlara ve para cezalarına yer verilmiştir. Bu noktada özellikle idari para cezalarına ilişkin olarak ilk hukuki ihlalde 150.000 Euro olmak üzere, beş yıl içinde yapılacak ikinci ihlalde 300.000 Euro'ya kadar çıkan yaptırımların yer aldığını ifade edebiliriz.

Kanunun 8. bölümünde ise kişisel verilerin korunmasına ilişkin işlenecek suçlarda, Fransız Ceza Kanunu'nun 226-16 / 226-24 arasındaki maddelerinin uygulanacağı belirtilerek bu kanuna ve maddelere atıf yapılmıştır. Bu noktada Ulusal Veri Koruma Komisyonu ile ceza makamlarının iş birliği içinde olduklarını da ve

kanuna göre bir veri sorumlusu hakkında soruşturma başlatılması halinde savcılık makamının bildirim yükümlülüğü olduğu düzenlenmiştir.

Bu noktada Fransız Ceza Kanunu'nun kişisel verilerin korunmasına ilişkin maddelerine baktığımızda ilk olarak, tıpkı Türk Ceza Kanunu'nda olduğu üzere bu konunun Fransız Ceza Kanunu'nda da 'Özel Hayata Karşı Suçlar' başlıklı birinci bölüm kapsamında incelendiğini görüyoruz. Kişisel verilere ilişkin suçlar ise aynı bölümün 'Kişilere Karşı İhlaller' başlıklı 6. kısmında yer almaktadır. Ceza Kanununda düzenlenen konuya ilişkin suç tiplerini aşağıda kısaca inceleyeceğiz. Buna göre;

Fransız Ceza Kanunu'nun 226-16 maddesinde kişisel verilerin usulüne aykırı işlenmesine ilişkin suç tipi düzenlenmiş ve gerçek bir kişiye ait kişisel verilerin işlenmesinden önce kanunda öngörülen prosedürlere uyulmaması halinde, bu suç taksir ile işlenmiş olsa dahi, kişi hakkında beş yıldan başlayan hapis cezası verilebilecek ve kişi 300.00 Euro tutarında para cezası ile cezalandırılabileceği ifade edilmiştir. [144]

Fransız Ceza Kanunu'nun kişisel verilerin işlenmesi için alınması zorunlu önlemler alınmaksızın işlenmesine ilişkin 226-17 maddesinde ise kişisel verilerin, 1978 tarihli kanunun 34. maddesinde yer alan önlemler alınmadan işlenmesi ya da işlenmesine sebebiyet verilmesi halinde kişi hakkında beş yıldan başlayan hapis cezası verilebilecek ve kişi 300.00 Euro tutarında para cezası ile cezalandırılabileceği düzenlemesi yapılmıştır.

Fransız Ceza Kanunu'nun kişisel verilerin yasal olmayan, haksız ve hileli yöntemler ile işlenmesini düzenleyen 226-18 maddesinde ise kişisel verilerin yasal olmayan, haksız ve hileli yöntemler ile işlenmesi halinde işleyen kişi hakkında, beş yıldan başlayan hapis cezası verilebilecek ve kişi 300.00 Euro tutarında para cezası ile cezalandırılabileceği düzenlemesi yapılmıştır.

Fransız Ceza Kanunu'nun özel nitelikli hassas verilere ilişkin 226-19 maddesinde ise kanunda öngörülmedikçe, taraflar arasında açık bir anlaşma olmaması halinde bireyin doğrudan ya da dolaylı olarak ırki, politik, felsefi, dini veya sendikal

---

[144] Kanunun İngilizce metni için bakınız.
(Çevrimiçi)https://www.legifrance.gouv.fr/...Downloads/Code_33.pdf (Erişim Tarihi: 01.03.2019)

bilgileri ile sağlık ve cinsel hayatına ilişkin verileri ortaya çıkaran kişi hakkında beş yıldan başlayan hapis cezası verilebilecek ve kişi 300.00 Euro tutarında para cezasına hükmedileceği ifade edilmiştir. Burada eleştirilebilecek husus, özel nitelikli olmayan verilerin hukuku aykırı şekilde işlenmesi ile, özel nitelikli hassas verilerin hukuka aykırı şekilde işlenmesi durumunda öngörülen ceza aynıdır. Oysaki özel nitelikli hassas verilerin hukuka aykırı işlenmesi durumunda verilecek cezanın daha ağır olması gerekirdi. [145]

Fransız Ceza Kanunu'nun 226-20 maddesinde ise kişisel verilerin hukukun gerektirmesi halinde tarihsel, istatiksel ya da bilimsel bir amaçla tutuluyor olmaları dışında, kanunlarda ya da yönetmeliklerde belirlenen sürelerin geçmesine ya da talep edilmesine rağmen kişisel verilerin saklanmaya devam edilmesi halinde kişi hakkında beş yıldan başlayan hapis cezası verilebilecek ve kişi 300.00 Euro tutarında para cezasına hükmedileceği ifade edilmiştir.

Fransız Ceza Kanunu'nun 226-21 maddesinde ise yasayla, yönetmelikle ya da öncesinde yapılan bir açıklamaya dayalı olarak kişisel verinin kaydedilmesi, sınıflandırılması, aktarılması veya her türlü işlenmesi sırasında, bu verileri elinde bulundurmak suretiyle verilerin yasanın, yönetmeliğin ya da söz konusu rıza beyanının amacından saptıran kişi hakkında beş yıldan başlayan hapis cezası verilebilecek ve kişi 300.00 Euro tutarında para cezasına hükmedileceği ifade edilmiştir.

Fransız Ceza Kanunu'nun 226-22 maddesinde ise kişisel verilerin kaydedilmesi, sınıflandırılması veya diğer her türlü şekilde işlenmesi esnasında ilgili kişinin önceden izni olmaksızın kişisel verinin yetkisiz 3. kişiye açıklanması suretiyle ilgili kişinin namına ya da özel hayatına zarar vermesi durumunda, eylemi gerçekleştiren kişi hakkında üç yıldan başlayan hapis cezası verilebilecek ve kişi 300.00 Euro tutarında para cezasına hükmedileceği ifade edilmiştir. Burada dikkat çeken bir husus ise maddenin devamında belirtildiği üzere bahsi geçen suçun şikâyete bağlı olmasıdır.

Görüldüğü üzere Fransa'da ceza kanunda kişisel verilere karşı işlenen suçlar bakımından oldukça büyük para cezaları ve hapis cezaları öngörülmüştür. Bu suçlar karşısındaki yaptırımların büyüklüğünün caydırıcı niteliğinin, üçüncü bölümde

[145] Korkmaz, **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, s.223

işlendiği üzere Türk Ceza Kanunu'ndaki konuya ilişkin suçlarda olmadığını görüyoruz. [146]

b. Almanya

Almanya'da kişisel verilerin korunması hukukuna baktığımızda ilk olarak 1978 yılında Almanya'nın Hessen eyaletinde kişisel verilerin korunmasına ilişkin bir yasanın geçtiği görülmektedir. Bu yasa aynı zamanda dünya üzerindeki ilk kişisel verilerin korunması yasası olarak da bilinmektedir. Bu tarihten sonra teknolojinin gelişmesiyle beraber Almanya'da ve tüm dünyada kişisel verilerin korunmasına ilişkin endişeler artarken, Almanya Anayasa Mahkemesi tarafından 15 Aralık 1983 tarihinde verilen bir kararla Almanya'da kişisel verilerin korunması hakkı ilk kez anayasal bir hak olarak tanınmış[147] ve böylelikle Almanya'da veri koruma hukukunun temelleri atılmıştır.[148] Bu kararla birlikte, kararda *informational self-determination* olarak tanımlanan ve bireylerin kişisel verileri üzerindeki yetkileri ve bu verilerinin kaderini tayin etme haklarını ifade eden kavrama da ilk kez yer verilmiştir.

Almanya'da nüfus sayımına ilişkin kanundan kaynaklı olarak kişisel verilerin ve özel hayatın gizliliğinin tartışılmaya başlanması ve akabinde Anayasa Mahkemesi tarafından verilen bu karardan sonra Almanya'da kişisel verilerin korunması bakımından toplumun talebi artmaya devam etmiş ve nihayetinde 1990 yılında ilk kez

---

[146] Korkmaz, **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, s. 222

[147] Max Schönfeld, "Big Data and Automotive-Legal Approach", Thomas Hoeren, Barbara Kolany-Raiser(Editors), **Big Data in Context Legal, Social and Technological Insights,** Almanya, Springer, 2015, s.57

[148] **Gerrit Hornung, Christoph Schnabel**, "Data protection in Germany I: The population census decision and the right to informational self-determination" , **Computer Law & Security Report**, Volume 25, Issue 1, 2009, S. 84-88, s.85-86. 1982 yılında Alman Federal Parlamentosunda genel nüfus sayımına ilişkin bir yasa geçirilmiş ve bu yasanın geçirilmesi sürecinde esasen ver korumaya ilişkin olarak parlamentoda hiçbir tartışma yapılmamasına rağmen, söz konusu yasa halk arasında tepki toplamış ve bireylerde genel bir denetime tabi tutulacakları yönünde bir korku ve özel hayatlarına müdahale edileceği şeklinde bir duygu oluşmuştur. Bu durum toplumda tartışmalara ve boykota sebep olmuş ancak bu konuda hükümet aksi yönde ikna edilememiştir. Bu süreçte nüfus sayımı sırasında kullanılması öngörülen formlar düzenlenmiş ve bu formlar aracılığı ile bireylerin kişisel verilerine ilişkin 160'a yakın soru da yöneltilmesine karar verilmiştir. Bu husus en nihayetinde Alman Anayasa Mahkemesi'nin önüne getirilmiş ve mahkeme nüfus sayımını genel olarak onaylamakla birlikte, bireylerin hak ve özgürlüklerinin korunması adına daha fazla prosedürel ve organizasyonel önlem alınması gerektiğini ifade etmiş ve ayrıca bireylerin kişisel verilerinin yerel yetkililere transferini anayasaya aykırı bularak bu durumun kişisel verilerin anonim istatistiksel amaçlarla toplanması ile kişisel verilerin yerel yetkililer tarafından işlenmesi arasındaki sınırı bulanıklaştırdığını ifade etmiştir. Bütün bu sürecin sonunda nüfus sayımına ilişkin yasa geçmiş ve Almanya'da bir nüfus sayımı yapılmış ancak bu karar ile birlikte *informational selfdetermination olarak da bilinen ve* bireylerin verilerinin kaderini tayin edebilmeleri, verileri üzerinde yetki sahibi olabilmeleri olarak da açıklanabilecek önemli bir hakka yer vererek Almanya'da veri korumaya ilişkin çok bir adım atmıştır.

Kişisel Verilerin Korunmasına ilişkin bir kanun kabul edilmiştir. Söz konusu kanun, gelişen teknoloji ve toplumun ihtiyaçları karşısında 2009 ve 2010 yıllarında değişliğe uğramış ve 1990 yıllardan bu yana Almanya'da veri koruma hukukuna yön vermiştir.

Ancak Avrupa Birliği Genel Veri Koruma Tüzüğü'nün yürürlüğe girmesi ile birlikte pek çok Avrupa ülkesinde olduğu üzere Almanya'da da yeni bir kanunun kabul edilmesi gereği hasıl olmuştur. Buna göre 30 Haziran 2017 tarihinde[149] yayınlanan yeni Alman Veri Koruma Kanunu 25 Mayıs 2018 tarihinde yani Avrupa Birliği Genel Veri Koruma Tüzüğü'nün yürürlüğe girdiği tarihte yürürlüğe girmiştir. Bahsi geçen kanun Tüzük'e uyumlu olması bakımından bir önceki Veri Koruma Kanuna göre pek çok farklılık barındırmaktadır.

Diğer yandan Almanya'da da tıpkı Fransa'da ve Türkiye'de olduğu üzere Alman Ceza Kanunu'nun özel hayatın gizliliğine karşı suçları düzenleyen 15. bölümünde kişisel verilerin korunmasına karşı işlenen suçlara yer verilmiştir. Görüldüğü üzere Almanya'da kişisel verilerin korunması hem Kişisel Verilerin Korunması Kanunu kapsamında hem de Alman Ceza Kanunu kapsamında korunmaktadır. Bu kapsamda ilk olarak 25.05.2018 tarihinde yürürlüğe giren Kişisel Verilerin Korunması Kanunu'nu inceleyeceğiz.

25.05.2018 tarihinde yürürlüğe Kişisel Verilerin Korunması Kanunu'nu 4 bölümden oluşmaktadır. Bu bölümler ortak hükümler, 2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü'nün 2. maddesine uygun olarak kişisel verilerin korunmasına ilişkin hükümlerin uygulaması, 2016/680 sayılı Kişisel Verilerin suçun engellenmesi, soruşturulması, tespiti amacıyla yetkili otoriteler tarafından kişisel verilerin işlenmesi veya cezai yaptırımların ifa edilmesi ve bu verilerin transferine ilişkin Avrupa Birliği Veri Koruma Direktifi'nin 1. maddesine uygun olarak kişisel verilerin korunmasına ilişkin hükümlerin uygulaması, 2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü ile 2016/680 sayılı Direktifin kapsamı dışında kalan aktivitelere konu işlemler için özel hükümler, olarak sıralanabilecektir.

---

[149] Kanunun İngilizce metni için bakınız. (Çevrimiçi) https://www.gesetze-im-internet.de/englisch_bdsg/ (Erişim tarihi: 01.03.2019)

Kanunun ‘Ortak Hükümler’ başlıklı ilk bölümüne baktığımızda, 1. bölümün ‘Kanunun Kapsamı’ başlıklı 1. maddesinde, bu kanunun kamu kuruluşları ve özel kuruluşlar tarafından işlenen verilere uygulanacağı ancak özel kuruluşlara bu kanunun uygulanabilmesi için özel kuruluşun veri sorumlusunun veya işleyicisinin Almanya’da ikamet etmesi gerektiği, veri sorumlusu veya işleyicisinin kuruluş aktiviteleri dahilinde veri sorumlusu ya da işleyicisinin Avrupa Birliği ülkelerinden birinde ya da Avrupa Ekonomik Bölgesi ülkelerinden birinde bulunmamasına rağmen Avrupa Genel Veri Koruma Tüzüğü’nün uygulama alanı kapsamına dahil olması gerektiği düzenlenmiştir. Ayrıca yine aynı maddede Almanya’daki diğer federal veri koruma mevzuatlarının bu genel Veri Koruma Kanunu karşısında öncelikli oldukları ve eğer bahsi geçen mevzuatlarda konuya ilişkin bir düzenleme yoksa söz konusu boşluğun bu genel kanun tarafından doldurulması gerektiği ifade edilmiştir.

Kanunun aynı bölümünün kamu kuruluşları tarafından kişisel verilerin işlenmesi başlıklı 3. maddesinde, kamu kuruluşlarının kişisel veri işleyebilmesi, veri sorumlusuna yüklenen resmi görevin yerine getirilebilmesi için kişisel veri işlemenin gerekli olması şartına bağlanmıştır.

Kişisel Verilerin Korunması Kanunu’nun kamusal alanlarda video gözetimi başlıklı 4. maddesinde ise farklı bir düzenlemeye yer verilmiştir. Bu maddeye göre kamusal alanlarda optik-elektronik araçlarla izleme yapılabilmesi için bu izleme, kamu kuruluşlarının görevlerini yerine getirebilmeleri, kimin erişime izinli ya da izinsiz olduğuna ilişkin tespit hakkının kullanılabilmesi ya da özel olarak belirlenmiş amaçlar için meşru menfaatleri teminat altına alınabilmesi için gerekli olmalıdır. Aynı maddede, spor tesisleri, toplanma alanları ve eğlence, alışveriş merkezleri, otoparklar veya tren, gemi veya otobüs gibi geniş kitlelerin erişimine açık araçlar gibi kamuya açık alanlarda, videolu izleme için hayatın, sağlığın ve özgürlüğün korunması önemli bir meşru menfaat olarak kabul edilebilecektir. Elbette bu durumda dahi madde metninde, bu izlemeyi yapabilmek için uygun önlemlerin alınması ve veri sorumlusunun isim ve iletişim bilgilerinin olabilecek en erken şekilde belirlenebilir olması yükümlülüğü düzenlenmiştir. Ayrıca yine madde de bu izlemenin spesifik bir kişiyi konu edinmesi halinde, bu kişinin Avrupa Birliği Veri Koruma Tüzüğü’nün 13 ve 14. maddelerine uygun olarak bilgilendirilmesi gerektiği de ifade edilmiştir.

Kanunun birinci bölümünün devam eden 5, 6 ve 7. maddelerinde ise kamu kuruluşları açısından veri sorumluları ve yetkililikleri hakkında düzenlemelere yer verilmiştir. Söz konusu maddelerde bu yetkililerin belirlenmesi, yetkililerin pozisyonları ile idari hiyerarşideki yerleri ve görevleri hakkında ayrıntılı olarak düzenlemeler yapılmıştır. Burada dikkat çeken husus, kamu görevlilerinin veri koruma konusundaki görevlerini yerine getirirken neredeyse bağımsız hale getirilmiş olmaları ve yalnızca ilgili kamu kuruluşunun en başındaki kişi ya da kişilere hesap vermekle yükümlü tutulmalıdır. Keza aynı şekilde bu görevlilerin görevlerini yerine getirmemesi sürecinde çalıştıkları kamu kuruluşu tarafından da işten çıkarılmaları veya cezalandırılmaları yasaklanmıştır. Kanuna göre bir veri koruma yetkilisinin işten çıkarılması, ancak Alman Medeni Kanunu'nun 626. maddesinde belirlenen prosedüre göre talep edilebilecektir. Ancak yukarıda da belirtiğimiz gibi ilgili kamu kuruluşunun bu yönde bir yetkisi bulunmamaktadır. Görüldüğü üzere Almanya'da veri koruma hukukuna ilişkin olarak faaliyet gösteren kamu görevlilerinin objektif şekilde görevlerini yerine getirebilmeleri ve görevlerini yerine getirdikleri için idari hiyerarşi içerisinde haksız yaptırımlara maruz bırakılmamaları adına koruma sağlanmıştır. Bu düzenlemenin oldukça önemli ve dikkat çekici bir düzenleme olduğunu düşünmekteyiz.

Kanunu'nun 8. ve 16. maddeleri arasında ise yine önemli bir düzenlemeye yer verilmiştir. Bu düzenleme de Almanya'da veri koruma hukuku alanında çalışan kamu görevliliklerinin bağımsızlığı ve denetimine ne denli önem verildiğini göstermektedir. Buna göre Almanya veri koruma ve bilginin serbestisini sağlaması için bir Federal Komiserlik düzenlemiştir. Federal Komiser, Almanya'daki kamu kuruluşlarını ve özel kuruluş olmakla birlikte çoğunluk sermayesini devletin elinde bulundurduğu kuruluşları denetlemekle görevli, bağımsız bir kimsedir. Kanun'da Komiser'in tam bağımsız olduğu ve ancak Federal Mahkeme tarafından denetlenebileceği ifade edilmiştir. Federal Komiser diğer görevlerinin yanı sıra, her sene Alman Meclisi'ne, o yıl tespit ettiği veri koruma ihlallerini, cezaları ve alınan önlemleri içeren bir rapor sunmakla görevlidir. Her yıl Komiser tarafından sunulan bu rapor Alman Meclis'i tarafından kamuya açık hale getirilerek halkın kamu kuruluşlarının veri koruma hukukuna yaklaşımları konusunda bilgi sahibi olmaları sağlanmaktadır. Bu yöntemin kamuda şeffaflık açısından oldukça önemli olduğunu düşünmekteyiz.

Kanunun 20. ve 21. maddesinde ise kamu kuruluşlarının veri koruma süreçlerine ilişkin faaliyetleri bakımından, gerçek kişilerin ve tüzel kişilerin bu kuruluşlara karşı başvurabilecekleri hukuki yollardan bahsedilmiştir. Buna göre bir kamu kuruluşu tarafından, gerçek ya da tüzel kişilerin, kişisel verilerinin korunması hakkının ihlal edilmesi halinde, bu kişiler idari mahkemeye başvurabilecektir.

Kanunun ikinci bölümüne geldiğimizde bu bölümde Avrupa Birliği Genel Veri Koruma Tüzüğü'nün ikinci maddesine referansla, özel nitelikli hassas verilerin işlenmesi, kamu kuruluşlarının ve özel kurumların başka amaçlar için veri işlemesi, kişisel verilerin kamu kuruluşları tarafından transferi, işçi işveren ilişkisine ilişkin amaçlarla kişisel verilerin işlenmesi, bilimsel, tarihsel ve istatiksel amaçlarla kişisel verilerin işlenmesi, kamu yararı için arşiv amacıyla kişisel verilerin işlenmesi, kişisel veri sahiplerinin hakları ve denetim otoritelerinin gizlilik yükümlülükleri, tüketici kredileri ve sair ticari sebepler için kişisel verilerin işlenmesi, kişisel veri sahibinden doğrudan temin edilen kişisel veriler açısından bilgilendirme ve kişisel veri sahibinden doğrudan temin edilemeyen kişisel veriler açısından bilgilendirme, kişisel veri sahibinin erişim, silme talep etme, itiraz etme hakları, profil yaratma dahil otomatik veri işleme, veri sorumlularının ve işleyicilerin yükümlülükleri, hukuki ve idari cezalar, hukuki yollar gibi kişisel verilerin korunması hukuku kapsamında pek çok konu düzenlemiştir. Görüldüğü üzere Alman Veri Koruma Kanunun da diğer ulusal kanunlara göre daha ayrıntılı düzenlemelere yer verilmiş ve kanun neredeyse her detay düşünülerek kaleme alınmıştır.

Bu başlıklar arasında ilk olarak hassas nitelikli kişisel verilerin korunmasına ilişkin 22. maddeye baktığımızda bu maddede Avrupa Birliği Genel Veri Koruma Tüzüğü'nün özel nitelikli kişisel verilerin işlenmesi hususunu düzenleyen 9. maddesinin tadil edildiği belirtilerek, özel nitelikli verilerin işlenmesi bakımından kamu kuruluşları ve özel kurumlar bu verileri veri işlemenin sosyal güvenlik ve sosyal koruma ve sair yükümlülüklerin yerine getirilmesi amacıyla; önleyici tıp, işçinin çalışma kapasitesinin değerlendirilmesi, tıbbi tanı, sağlık ve sosyal bakım yönetimi ve hizmetleri veya veri sahibinin bir sağlık profesyoneli ile sözleşmesinin bulunması ve bu verilerin sağlık profesyonelleri ya da veri gizliliği yükümlülüğüne konu kişi ya da bunların denetiminde kişiler tarafından işlenmiş olması halinde; kamu sağlığı ile

medikal ürün ve araçların güvenliği gibi sebeplerle gerekli güvenlik önlemleri alınmak şartıyla işlenebileceği düzenlenmiştir.

Kanunun 23. ve 24. maddelerinde ise farklı olarak nitelendirilebilecek iki düzenlemeye yer verilmiş ve kamu kuruluşlarına ve özel kurumlara verilerin topladıkları amaçlar dışında işleyebilmeleri için bazı istisnai haller düzenlenmiştir. Genel olarak sair ulusal ve uluslararası düzenlemelere baktığımızda veri koruma hukukunda kişisel verilerin toplandığı amaç dışında kullanılmasının veri güvenliğinin ihlali olarak düzenlendiğini görmemize rağmen, Alman Kanunu'ndaki bu düzenleme ilginç ve farklı bir düzenleme olmuştur.

Kanunu'nun 27. maddesinde ise yine farklı bir düzenleme ile Avrupa Birliği Genel Veri Koruma Tüzüğü'nün 9. maddesine atıfla, hasas nitelikli kişisel verilerin bilimsel, tarihsel ve istatiksel amaçlı olarak rıza aranmaksızın işlenebileceği düzenlenmiştir. Elbette aynı maddede veri sorumlusuna her türlü önlemi alma yükümlülüğü getirilmiştir. Yine kanunun 28. maddesinde ise, kamu yararı bulunan hallerde arşivlemek amacıyla verilerin işlenebileceği ifade edilmiştir.

Kanun kapsamında bir diğer dikkat çeken madde ise, kişisel verilerin veri sahibinden elde edilemeyecek durumda olması halinde veri sahibinin bilgilendirilmesi konusunda getirilen düzenlemedir. İşbu konuyu düzenleyen 33. maddeye göre örneğin kamu güvenliğini tehlikeye atmamak için veri sahibine kişisel verisinin işlendiği bilgisinin verilmeyebileceği ifade edilmiştir.

Kanun kapsamında dikkat çeken bir diğer madde ise kişisel verilerin silinmesine ilişkin 35. maddedir. Bu maddede, yine Avrupa Birliği Genel Veri Koruma Tüzüğü'nden farklı bir düzenleme yapılmış ve Tüzük'ün ilgili 17. maddesindeki istisnalara ek bir istisna getirilerek, otomatik olmayan kişisel verilerin silinmesinin imkânsız olması veya verinin saklanma şeklinden ötürü verinin silinmesinin orantısız bir çaba gerektirmesi ve veri sahibinin verinin silinmesine ilişkin yararı minimum ise veri sorumlusu veri sahibinin kişisel verilerinin silinmesi yönündeki talebini reddedilebilecektir.

Kanunun 3. bölümünde ise 2016/680 sayılı Avrupa Birliği Direktifi'nin 1. maddesine uygun olarak veri işlemeye ilişkin hükümlerin uygulanması hususu düzenlenmiştir. Bu bölümdeki hükümler, bir suçun önlenmesine, araştırılmasına, tespitine veya soruşturulmasına yetkili ya da bir cezai ya da idari yaptırımı uygulayan kamu kuruluşları tarafından işlenen kişisel verilere ilişkin olarak uygulanmaktadır. 3. bölümde genel olarak kişisel verilerin işlenmesine ilişkin temel prensiplere, özel nitelikli hassas verilerin işlenmesine ilişkin hükümlere, arşiv, bilimsel ve istatiksel amaçlarla verilerin işlenmesi, rıza, veri sorumlusunun talimatları, gizlilik, otomatik birey kararları, veri sorumlusunun hakları, Federal Komisere şikâyette bulunma hakkı, veri sorumlusunun yükümlülükleri, veri işleme güvenliği için gereklilikler, veri güvenliğinin ihlali halinde Federal Komisere bildirim ve veri sahibine bildirim, işleme faaliyetlerinin kaydedilmesi, verilerin kendiliğinden ya da veri sorumlusu tarafından alınacak önlemler aracılığı ile korunması, verilerin düzeltilmesi, silinmesi ve veri işlemenin sınırlandırılması, veri güvenliği ihlallerinin bildirilmesi, verilerin üçüncü ülkelere ve uluslararası organizasyonlara aktarılması, sorumluluklar ve cezalar yer verilmiştir. Bu bölümdeki tüm düzenlemeler genel olarak 2016/680 sayılı Avrupa Birliği Direktifi ile uyumludur.

Almanya, Veri Koruma Kanunu'nda düzenlemeler yaparken, 2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü'ne ilişkin hususlarda pek çok istisna ve değişiklik düzenlemeleri yapmışken, 2016/680 sayılı Direktif 'e ise genel olarak uyumlu düzenlemeler getirmiştir.

Veri Koruma Hukukuna ilişkin olarak Alman Ceza Kanunu'nda[150] da ilgili maddeler bulunmaktadır. Esasen Alman Ceza Kanunu'nun da ülkemiz ceza kanununda olduğu gibi ya da Fransız Ceza Kanunu'nda olduğu gibi doğrudan kişisel verilerin korunması yönelik suçlardan oluşan bir bölüm bulunmamaktadır. Alman Ceza Kanunu'nun ilgili bölümlerine baktığımızda, verilerin ilk olarak özel hayatın gizliliğinin korunmasına ilişkin 201 ve 202. maddeleri altında, 'Veri Casusluğu', 'Elektronik Dolandırıcılık', 'Veri Casusluğu ve Kimlik Hırsızlığı için Yapılan Hazırlıklar', suçları ile korunduğunu görüyoruz. Kanunun 'Veri Casusluğu' başlıklı

[150] Kanunun İngilizce metnine ulaşmak için bakınız. (Çevrimiçi) https://www.gesetze-im-internet.de/englisch_stgb/index.html (Erişim Tarihi:01.03.2019)

202a maddesinde "…yetkisiz erişimlere karşı korunan verileri kendi ya da başkası için ele geçiren kimse 3 yıla kadar hapis cezası ile cezalandırılacaktır" şeklinde düzenlenmiştir. Kanunun 'Elektronik Dolandırıcılık' başlıklı 202b başlıklı maddesinde ise "kamuya açık olmayan veri işleme tesislerinden teknik yöntemler aracılığıyla veya kamuya açık olmayan veri işleme tesisinin elektromanyetik yayınlarından kendisine ait olmayan verileri kendisi ya da başkası için ele geçiren kimse 3 yıla kadar hapis cezası ile cezalandırılacaktır." şeklinde düzenlenmiştir. Aynı şekilde kanunun 202c maddesinde de yukarıda yer verdiğimiz suçların işlenebilmesi için şifrelerin ya da diğer güvenlik kodlarının ele geçirilmesi de suç olarak düzenlenmiştir. Görüldüğü üzere kanunun bu maddeleri her kadar özel hayatın gizliliğinin ihlali bölümünde düzenlenmiş olsa da doğrudan kişisel verilerin korunmasından ziyade bilişim suçlarına ilişkindir. Bu halde bu suçlar kapsamında ele geçirilen verilerin kişisel veriler olması halinde, bu suçların kişisel verilere karşı işlenmesi söz konusu olabilecektir.

Kanunun 203-2a numaralı maddesinde ise, bir veri koruma yetkilisinin, sahip olduğu yetkilerden ötürü vakıf olduğu sırları açıklaması halinde de bu madde kapsamında cezalandırılacağı düzenlenmiştir. Nitekim Alman Veri Koruma Kanunu'nun ikinci bölümünün 29. maddesinde de Alman Ceza Kanunu'nun bu maddesine atıf yapılmış ve denetleyici yetkilinin dahi, veri koruma yetkilisinin gizlilik yükümlülüğünü ihlal etme ihtimalinin olması durumunda, bu kişiler hakkında soruşturma yetkisinin olmayacağı ifade edilmiştir.

Diğer yandan Kanun'un 'Kişinin Özgürlüğüne Karşı İşlenen Suçlar' başlıklı 18. maddesi kapsamında düzenlenen ve stalking olarak da bilinen 'Takipçi Tacizi' başlıklı 238. maddesinin 3. fıkrası kapsamında, "kendisine ürün ve hizmet siparişi vermek veya 3. kişilerin bu kişi ile iletişim kurmasını sağlamak amacıyla bir kişinin kişisel verilerini kötüye kullanan kimsenin 3 yıla kadar hapis cezası ile cezalandırılacaktır" şeklinde düzenleme öngörülmüştür. Bu düzenleme Alman Ceza Kanunu'nda 'kişisel veri' kavramına doğrudan yer verilen tek düzenleme olma niteliğini de taşımaktadır. Zira bu madde dışında Alman Ceza Kanunu'nda kişisel veri kavramının doğrudan kullandığı başka bir madde bulunmamaktadır.

c. İtalya

İtalya'da kişisel verilerin korunmasına ilişkin olarak ilk adım 31 Aralık 1996 tarihinde yürürlüğe giren, Bireylerin ve Diğer Veri Öznelerinin Kişisel Verilerinin İşlenmesine İlişkin Olarak Korunması Kanunu' ile atılmıştır. Söz konusu kanunun önsözünde de belirtildiği üzere bu kanun ile birlikte 1995 tarihli Avrupa Veri Koruma Direktifi'nin hükümlerine geçerlilik tanınmak istenmiştir. [151] Ayrıca bu kanun ile beraber kişisel verilerin işlenmesine ilişkin bir denetleyici otorite oluşturulmuştur. Buna göre İtalya'da denetleyici kurum İtalyan Veri Koruma Kurumu'dur.[152] 1996 tarihli ve on bölümden oluşan Kanun kapsamında genel olarak, genel prensiplere, veri sorumlusunun yükümlülüklerine, verilerin ve özel nitelikli verilerin işlenmesi hususlarına, adli ve idari yollara, denetleyici otoriteye, cezalara yer verilmiştir. Görüldüğü üzere konu hakkında çıkarılan ilk kanun son derece basit düzeyde ve temel konulara yer veren bir kanundur.

Bu kanunun yürürlüğe girmesinden sonra, Avrupa Birliği nezdinde yaşanan gelişmeler veri koruma konusundaki ihtiyaçları artırmış ve 2002 tarihli Avrupa Konseyi Kişisel Verilerin ve Özel Hayatın ve Elektronik İletişim Sektörünün Korunmasına İlişkin Direktif 'in yürürlüğe girmesi akabinde ise on bölümden oluşan 1996 tarihli veri koruma kanunu, 30 Haziran 2003 tarihinde 'Kişisel Verilerin Korunmasına İlişkin Kanun' ile değiştirilmiştir. [153] 30 Haziran 2003 tarihli kanun ile çok daha kapsamlı ve ihtiyaçlara cevap veren bir kanun hazırlanmıştır. Bu kanun kapsamında 1996 tarihli kanundan farklı olarak, kamu ve özel sektöre ilişkin ayrı düzenlemeler yapılmış[154], veri güvenliği konusuna değinilmiş[155], yargı alanındaki kişisel verilerin işlenmesi, kolluk kuvvetleri tarafından işlenen verilere, devlet güvenliği kapsamında işlenen verilere, kamu sektörü alanında işlenen verilere, sağlık sektöründe işlenen verilere, eğitim alanında işlenen verilere, tarihi, istatiksel ve

---

[151] 1996 tarihli İtalyan veri koruma kanunun İngilizce metni için bakınız. (Çevrimiçi) http://www.privacy.it/archivio/legge675encoord.html (Erişim Tarihi:02.03.2019)

[152] 1996 tarihli kanunun 30. Maddesine bakıldığında, bu madde ile birlikte bağımsız bir otoritenin kurulmasına karar verilmiştir. Buna göre altı kişiden oluşan Kurum'da hukuk ve bilgisayar bilimleri konusunda uzman kişilerin tam bağımsızlık ile görev yapacağı ifade edilmiştir.

[153] 2003 tarihli İtalyan veri koruma kanunun İngilizce metni için bakınız. (Çevrimiçi) http://www.privacy.it/archivio/privacycode-en.html (Erişim Tarihi:02.03.2019)

[154] 2003 tarihli İtalyan veri koruma kanunun genel veri koruma kuralları başlığını taşıyan 3. Başlığının altında yer alan ikinci ve üçüncü bölümlerde özel sektörde ve kamu sektöründe kişisel verilerin işlenmesine ilişkin hususlara yer verilmiştir. Bu yönüyle yasa yapma tekniği açısından bu yapı Alman Veri Koruma Kanunu ile benzerlik göstermektedir.

[155] 2003 tarihli İtalyan veri koruma kanunun veri ve sistem güvenliği başlıklı 5. Başlığının altında konu düzenlenmiş ve veri koruma için veri güvenliğine ilişkin alınacak asgari önlemler ile verilerin elektronik yöntemlerle ve otomatik yollarla işlenmesi durumunda alınacak tüm önlemlere yer verilmiştir.

bilimsel amaçlı işlenen verilere, sosyal güvenlik, bankacılık ve finans, elektronik iletişim kapsamında işlenen verilere, gazetecilik kapsamında işlenen verilere[156] yönelik olarak ayrı başlıklar açılmış ve aynı kanunda yine denetleme prosedürlerine ve yaptırımlara da yer verilmiştir. Bu bakımından kanunun oldukça kapsamlı olduğu açıkça görülmektedir.

Söz konusu kanunda özel nitelikli sektörlere baktığımızda burada dikkat çekici alanlardan biri de Avrupa İnsan Hakları Mahkemesi kararlarında da sıklıkla karşımıza çıkan gazetecilik sektörüne ilişkin olarak yapılan düzenleme olduğunu düşünmekteyiz. Zira ifade özgürlüğü kapsamında korunan gazetecilik faaliyetleri ile kişisel verilerin korunması arasındaki hassas denge düşünüldüğünde, söz konusu kanunda bu alanda düzenleme yapılmış olmasının dikkat çekici olduğunu düşünmekteyiz. [157]

Avrupa Birliği Genel Veri Koruma Tüzüğü'nün de yürürlüğe girmesi ile birlikte tıpkı Almanya ve Fransa'da olduğu üzere mevcut kanun bir kez daha revize edilmiş ve Tüzük, İtalyan veri korumu hukuku bakımından pek çok değişikliği beraberinde getirmiştir. İtalya Veri Koruma Kanunu'nun son haline baktığımızda, özellikle belirlenen alanlarda bazı değişikliklere gidildiğini görmekteyiz. Buna göre öncelikle çocukların kişisel verilerinin işlenmesine yönelik olarak yaş sınırı 14 olarak değiştirilmiş, biyometrik, genetik ve sağlık verilerinin işlenebilmesi için alınacak güvenlik önlemlerinin ölçüsüne ilişkin Avrupa Birliği Genel Veri Koruma Tüzüğü ile uyumluluk sağlanmış, yargı sektöründe işlenecek kişisel verilerin yalnızca kanunlarda ya da sair hukuki düzenlemelerde yer alan hükümlere dayalı olarak işlenebileceği belirtilmiş, veri sorumluları ve veri işleyen kavramları mevcut organizasyonel yapıyı değiştirecek şekilde ulusal hukuktaki düzenlemeye dahil olmuş, Avrupa Birliği Genel Veri Koruma Tüzüğü'nün 88. Maddesine uygun olarak, özel ve kamu sektörü tarafından yürütülecek işe alım süreçlerinde işlenecek kişisel veriler konusunda etik kurallara uyulacağı belirtilmiş ve elbette yaptırımlar konusunda büyük ölçüde değişikliklere gidilmiştir. [158] Zira daha evvel de belirttiğimiz üzere Avrupa Birliği Genel Veri Koruma Tüzüğü veri ihlallerine ilişkin olarak çok yüksek miktarda idari

---

[156] 2003 tarihli İtalyan veri koruma kanunun özel nitelikli sektörlerin veri işlemesi başlıklı 2. Bölümünde pek çok sektöre ilişkin olarak düzenleme ve açıklama yapılmıştır.

[157] Kanun kapsamında sıklıkla AİHM kapsamında karşımıza çıkan bir hususta düzenleme yapılmış ve bireylerin haber alma hakkının ağır bastığı durumlara ilişkin olarak basın özgürlüğünün kişilerin verilerinin korunması konusundaki bireysel hakkına karşı korunacağı ifade edilmiştir.

[158] Konuya ilişkin açıklama için bakınız. (Çevrimiçi) http://www.mondaq.com/italy/x/740422/data+protection/Italian+Data+Protection+Code+Reformed+To+Enact+GDPR+What+Is+New (Erişim Tarihi:22.03.2019)

cezalar öngörmüştür. Buna göre Avrupa Birliği Genel Veri Koruma Tüzüğü'nün 83.maddesinin 4. fıkrasına göre idari ceza 10 milyon Euro'dan başlayarak yıllık gelirin yüzde 2'sine varan bir ceza öngörürken, aynı maddenin 5. fıkrasına göre ise 20 milyon Euro'dan başlayarak yıllık gelirin yüzde 4'üne varan bir ceza öngörülmüştür.

Diğer yandan mevcut kanunu suç tipleri bakımından incelediğimizde, 167 ve 172. [159]maddeleri arasında konuya ilişkin suçların düzenlendiğini görmekteyiz. Bu kapsamda suç olarak, hukuka aykırı veri işleme, denetim organına doğru olmayan beyanda bulunma, denetim organı tarafından getirilen hükümlere aykırı hareket etme gibi suçlara yer verilmiş ve Avrupa Birliği Genel Veri Koruma Tüzüğü ile de bu suçlara ek olarak verilerin hukuka aykırı olarak yayılması ve verilerin dolandırıcılık yolu ile elde edilmesi suçları da kanun kapsamına eklenmiştir. [160] Diğer yandan kanun kapsamındaki cezalara baktığımızda ise genel olarak taban cezanın altı ay ile 1 yıl, ceza üst sınırının ise 3 yıl olduğunu görmekteyiz. Bu bakımdan ceza oranlarının Türk Ceza Hukukundaki oranlar ile benzer olduğu görmekteyiz.

d. Amerika Birleşik Devletleri

Çalışmamızın kişisel veriye mülkiyet hakkı yönünden yaklaşım bölümünde bahsetmiş olduğumuz üzere, Amerika Birleşik Devletleri'nde, kişisel verilerin korunması hakkına yaklaşım insan hakları değil, mülkiyet hakkı üzerinden şekillenmektedir. Amerika'da kişisel verilerin korunmasına yönelik bu ekonomik yaklaşım esasen ülkede kişisel verilerin korunmasına yönelik olarak düzenlemelerin az miktarda ve yetersiz oluşunun da temellerini oluşturmaktadır. Zira Amerika'da genel nitelikli tüm Amerika düzeyinde bir veri koruma kanunu bulunmamakta olup, kişisel verilerin korunması sektörel bazlı olarak, özellikle sağlık, finans, telekomünikasyon ve sigorta sektörü başta olmak üzere[161] yalnızca bazı eyaletlerde düzenlenen hukuki metinler aracılığı ile korunmaktadır. Örneğin Amerika'da özellikle finans ve sağlık sektöründe çok fazla kişisel veri işlendiğinden bu sektörler için

---

[159] Korkmaz, **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, s. 237

[160]Konuya ilişkin açıklama için bakınız. (Çevrimiçi) https://www.dentons.com/en/insights/articles/2018/september/25/italian-data-protection-code-reformed-to-enact-gdpr-what-is new?utm_source=Mondaq&utm_medium=syndication&utm_campaign=inter-article-link (Erişim Tarihi:22.03.2019)

[161]İlgili içerik için bakınız. (Çevrimiçi) https://www.dlapiperdataprotection.com/index.html?t=authority&c=US Erişim Tarihi: 20.03.2019

düzenlenen kanunlarda veri güvenliğine ilişkin bazı hükümler yer almaktadır.[162] Nitekim kişisel verilerin korunması hakkı Amerika'da anayasal bir hak olmayıp[163], bu hak bir temel hak ve hürriyet olarak korunmamakta ve bu konuda sektörel yaklaşımlar[164] aracılığı ile veri güvenliği sağlanmaya çalışılmaktadır. Bu durumun Amerika vatandaşlarının kişisel verilerinin korunduğuna ilişkin inancını oldukça azalttığını ve yapılan son araştırmaların da bu yönde olduğunu söylemek yanlış olmayacaktır. [165]

Kişisel verilerin korunması konusunun, özel hayatın gizliliği ile bağlantısı göz önünde bulundurulduğunda, Amerika'da bu konuda atılmış en önemli adımlardan biri Amerika'da özel hayatın korunmasına ilişkin en önemli kararlardan biri olan, 1965 yılında verilen Griswold v. Connecticut[166] kararıdır. Karara göre, Connecticut eyaletinde, bireylerin hamileliği önlemek amacıyla her türlü ilaç, medikal cihaz ya da aracın yasaklanması söz konusu olmuş ve mahkeme düzenlemeyi içeren kanunu anayasaya aykırı bulmuştur. Yüksek mahkeme bahsi geçen yasanın evliliğin gizliliğini ve bireylerin özel hayatını ihlal ettiği gerekçesiyle iptal etmiştir. Bu noktada önemli olan husus, bu kararın verildiği tarihte Amerikan Anayasası'nda özel hayatın gizliliğine ilişkin bir madde bulunmazken, hâkim Byron White ve John Marshall Harlan tarafından bu kararda özel hayatın gizliliği hakkının korunmasından bahsetmiş olmalarıdır.

Amerika'da özel hayatın korunmasına ilişkin olarak yapılan ilk hukuki düzenleme ise 1974 tarihli Özel Hayatın Gizliliği Kanunu'dur.[167] Bu kanunun özelliği

---

[162] Atul Singh, **Protecting Personal Data as a Property Right**, s. 126

[163] Murat Volkan Dülger, "İnsan Hakları ve Temel Hak ve Özgürlükler Bağlamında Kişisel Verilerin Korunması", **İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi**, C. 5 (1), Bahar 2018, s. 76. Ayrıca bakınız. Viktor Mayer-Schonberger, "Beyond Privacy, Beyond Rights- Toward a Systems Theory of Information Governance", **California Law Review,** Vol. 98, 2010, s. 1857

[164] Atul Singh, "Protecting Personal Data as a Property Right ", **ILI Law Review**, Winter Issue 2016, S.123-139, s. 126. Ayrıca bakınız. Pamela Samuelson, Privacy as Intellectual Property, **Stanford Law Review**, Vol. 52, 1999, s. 2.

[165] 2016 yılında 1040 yetişkine sorularak yapılan ulusal bir anket onucuna göre Amerikalıların %64'ü bireysel olarak kişisel verilerinin korunmasına yönelik bir ihlale maruz kaldığını ve özellikle federal hükümetler ve sosyal medya siteleri olmak üzere pek çok kuruluşa güvenini kaybettiği ortaya konmuştur.
İlgili araştırma için bakınız. (Çevrimiçi) https://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/ Erişim Tarihi: 22.03.2019

[166] 381 U.S. 479 (1965) sayılı ve tarihli kararının tam metni için bakınız. Çevrimiçi https://supreme.justia.com/cases/federal/us/381/479/ (Erişim Tarihi:22.03.2019)

[167] 1974 tarihli kanunun tam metni için bakınız. (Çevrimiçi) https://www.govinfo.gov/content/pkg/USCODE-2012-title5/pdf/USCODE-2012-title5-partI-chap5-subchapII-sec552a.pdf (Erişim Tarihi:22.03.2019)

kişisel verilerin Federal Devlet tarafından işlenmesi halinde uygulanacak olmasıdır.[168] Bu kanuna göre genel olarak bireylerin rızaları dışında veri işlenmeyecek olsa da bazı durumlarda bireylerin izni olmaksızın veriler işlenebilecektir. Bu istisnalara örnek olarak Nüfus Müdürlüğü'nün ve Çalışma İstatistik Ofisi'nin istatiksel amaçları, devlet kurumlarının rutin kullanımları, arşiv amaçlı olarak verilerin tutulması, hukukun uygulanması için gerekli olması, kongre soruşturmaları ve diğer idari amaçlar sayılabilecektir. [169] Bu noktada bahsi geçen istisnai hallerin son derece ucu açık ve bireylerin kişisel verilerinin korunması bakımından sakıncalı yönleri olduğu aşikardır. Özellikle devletin rutin uygulamaları ifadesi dikkate alındığında bu ifadenin kanunilik ilkesi bakımından sorunlu olduğunu söyleyebilir. Bu kanun dışında Amerika'da Sağlık Sigortası Taşınabilirliği ve Sorumluluğu Kanunu, Adil Kredi Raporlama Kanunu, Elektronik İletişim Gizliliği Kanunu gibi kanunlar özel hayatın gizliliği ve yer yer kişisel verilerin korunmasına ilişkin bazı maddeler taşıyan kanunlara örnek olarak verilebilecektir.

Ayrıca Amerika'da *U.S. Federal Trade Commission* (FTC) olarak da bilinen kurum resmi olarak böyle bir görevi olmamasına rağmen, bir nevi veri koruma otoritesi olarak faaliyet göstermektedir. Komisyon bu noktada FTC Kanunu'nun 5. bölümünde yer 'Haksız ve Yanıltıcı Ticaret' uygulamalarının yasaklanmasına ilişkin maddelere dayanarak uzun yıllardır veri koruma faaliyetini sürdürmektedir. Bahsi geçen bölümde haksız ve yanıltıcı ticaret aracılığı ile veri koruma ihlaline maruz kalan şirketleri, veri güvenliği konusunda yeterince önlem almadıkları ve güvenlik açıkları sebebi ile veri ihlalini yaşadıkları gerekçesiyle sorumlu tutmaktadır. [170]

Bunun dışında Amerika'da kişisel verileri ilgilendiren en önemli hukuki düzenlemelerden biri ise 2001 yılında yürürlüğe giren Patriot Act'tir. Bu kanun Amerika'da 11 Eylül tarihinde yaşanan terör olayları üzerine yürürlüğe sokulmuş olup, yasayla terör şüphesi ile bireylerin kişisel verilerine aşırı müdahale edilmesi söz konusu olabilecektir. Bu yasa ile birlikte az da olsa bireylerin kişisel verilerini koruyan

---

[168] Korkmaz, **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, s.241
[169] İlgili açıklama için bakınız. (Çevrimiçi) https://en.wikipedia.org/wiki/Privacy_Act_of_1974#Provisions_of_the_Privacy_Act Erişim (Tarihi:22.03.2019)
[170] İlgili FCA metni için bakınız. (Çevrimiçi) https://www.federalreserve.gov/boarddocs/supmanual/cch/ftca.pdf Erişim Tarihi: 20.03.2019

pek çok kanun değiştirilmiş ve bireylerin konuya ilişkin hakları cılız hale getirilmiştir.[171]

Elbette kişisel verilerin korunması konusuna ilişkin olarak Amerika ile Avrupa Birliği ülkeleri arasında derin bir farklılık olduğu aşikardır.[172] Amerika'da kişisel verilerin yeteri kadar korunmadığı, veri güvenliğinin sıklıkla ihlal edildiği, Avrupa Birliği Adalet Divanı tarafından da kabul edilmektedir.[173] Ancak Amerika'nın veri koruma hukukuna yaklaşımının da Avrupa Birliği Genel Veri Koruma Tüzüğü ile farklı bir yola girdiğini söylemek mümkün olacaktır. Dolayısıyla çalışmamızın bu bölümünde genel bir kanun incelemesinden ziyade, parçalı[174] bir nitelik taşıyan koruma sistemi kapsamında genel bir inceleme yapılmış ve Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Amerikan yaklaşımına etkisinden bahsedilmiştir. Avrupa Birliği Genel Veri Koruma Tüzüğü'nün yürürlüğe girmesi ile birlikte Amerika'nın pek çok eyaletinde veri ihlalinin bildirilmesine ilişkin kanunlar yürürlüğe girmiştir. Amerika'nın yaklaşık 50 eyaletinde bu kanunlar yürürlüğe girmiş, var olanlar güncellenmiş olup, kanunlar bireylerin kişisel verilerinin korunması hakkının ihlal edilmesi durumunda, bireylere bildirimde bulunma yükümlülüğünü içermektedir. [175]

2. Türk Hukukunda Kişisel Verilerin Korunması

a. 1982 Anayasası

Türkiye Cumhuriyeti, Avrupa Konseyi tarafından düzenlenen Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması başlıklı 108 sayılı sözleşmeyi 28 Ocak 1981 tarihinde imzalanmış fakat bu sözleşme uzun yıllar boyunca onaylamamıştır. Bu sözleşmenin onaylanmamasının Türkiye'nin Avrupa Birliği ile

---

[171] Korkmaz, **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, s. 255
[172] Kuşkonmaz, **Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması**, s. 19
[173] Çalışmamızın ikinci bölümünde açıklandığı üzere Avrupa Birliği tarafından kişisel verilerin korunmasına ilişkin olarak yapılan düzenlemelerin pek çoğunda, veri güvenliğinin yeteri kadar sağlanmadığı ülkelere Avrupa birliği ülkelerinden veri transferi yasaklanmaktadır ve Amerika da bu ülkelerden biridir. Nitekim Amerika ile ticaretin tüm dünya için önemli olması ve dünyanın ileri gelen elektronik ticaret şirketlerinin Amerika menşeli olması noktasında, Amerika ile veri transferine ilişkin özel olarak imzalanan Safe Harbour sözleşmesi de Avrupa Birliği Adalet Divanı tarafından verilen karar ile geçersiz kılınmıştır. Bu kararın ayrıntılı incelemesine ikinci bölümde yer verildiğinden tekrar olmaması açısından burada yalnızca atıf yapmakla yetinilmiştir.
[174] Korkmaz, **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, s.238
[175] İlgili yazı için bakınız, (Çevrimiçi) https://www.dataprotectionreport.com/2018/07/u-s-states-pass-data-protection-laws-on-the-heels-of-the-gdpr/ (Erişim Tarihi: 22.03.2019)

olan ilişkilerinde hep bir engel olarak yer alması ve bireylerin de kişisel verilerin korunmasına yönelik artan ihtiyaçları karşısında 5982 sayılı Türkiye Cumhuriyeti Anayasasının Bazı Maddelerinde Değişiklik Yapılması Hakkında Kanun kapsamında, 1982 tarihli Anayasası'nın 'Kişinin Hakları ve Ödevleri' başlıklı İkinci Bölümünün 20. maddesine ek bir düzenleme aracılığı ile kişisel verilerin korunmasına ilişkin anayasal bir düzenleme yapılmak istenmiştir. Söz konusu kanuna ilişkin gerekçede işbu ek düzenleme değerlendirilmiş ve mevcut anayasamızda kişisel verilerin korunması hakkını korumaya dayanak olabilecek bazı maddeler bulunmasına rağmen bunların zamanın ihtiyaçlarını karşılamadığı ifade edilmiştir. Yine aynı gerekçede, bahsi geçen ek düzenleme ile kişisel verilerin korunması hakkının artık doğrudan anayasal bir zemini olduğu vurgulanmış ve konu hakkındaki gerekli diğer usul ve esasların ise bir kanun ile düzenleneceği ifade edilmiştir. Görüldüğü üzere yasa koyucu bu ek düzenleme ile birlikte Türkiye'nin tarafı olduğu uluslararası sözleşmelere uygun bir düzenleme yapmak istemiştir.

Buna göre 2010 yılında 1982 Anayasasında yapılan değişiklik kapsamında, anayasanın "Özel hayatın gizliliği" başlıklı 20. maddesine "*Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.*" şeklindeki ifade eklenmiştir.[176] Böylelikle anayasada yapılan işbu değişiklik ile kişisel verilerin korunması hakkı bir temel hak ve özgürlük olarak anayasamızda doğrudan korunmuştur.[177] Anayasa Mahkemesi de bu tarihten sonra vermiş olduğu kararlarında, 20. madde kapsamında yer verilen kişisel verilerin korunması hakkına temel hak ve özgürlükler düzeyinde atıf yapmıştır.

[176]Anayasanın 20. Maddesinin tam metni için Bkz. Türkiye Cumhuriyeti Anayasası, (Çevrimiçi) https://www.tbmm.gov.tr/anayasa/anayasa_2018.pdf (Erişim Tarihi: 24.10.2018)

[177] Murat Volkan Dülger, "Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması", **İstanbul Medipol Üniversitesi Hukuk Dergisi,** S.3/2, 2016, s.120-121

b. 6698 sayılı Kişisel Verilerin Korunması Kanunu

Hukukumuzda kişisel verilerin korunması konusunda bir yasa yapılmasına yönelik ihtiyaç uzun yıllar dile getirilmiş ve fakat konuyla ilgili adımların atılması uzun zaman almıştır. Nitekim Türkiye Avrupa Konseyi tarafından hazırlanan Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması başlıklı 108 sayılı Sözleşmeyi 28 Ocak 1981 tarihinde imzalanmış fakat bahsi geçen sözleşmeyi uzun yıllar boyunca onaylamamıştır. [178] Bu sözleşmenin uzun yıllar onaylanmamasının sebeplerinden biri bu sözleşmenin, sözleşmeyi onaylayan ülkelere kişisel verilerin korunması konusunda bir kanun oluşturma yükümlülüğü getiriyor olmasıdır.[179] Zira Türkiye 1981 yılında imzalamış olduğu sözleşmeye uygun olarak bu konudaki ilk kanun tasarısını ilk kez 1 Haziran 2004 tarihinde Başbakanlığa sevk edebilmiştir. Açıkçası Türkiye'nin ancak 2004 yılında atabildiği bu adımın da Avrupa Birliği süreci gerekliliklerinden ötürü olduğunu söylemek yanlış olmayacaktır. Bu dönemde bahsi geçen bu tasarı kanunlaşmadan TCK'da düzenlenen suç tiplerinin bir anlam ifade etmeyeceği görüşleri dile getirilmiştir.[180] Ancak ne yazık ki Türkiye'de uzun yıllar ne 108 sayılı sözleşme onaylanmış ne de bahsi geçen tasarı bir sonuca varmıştır. Türkiye uzun yıllar kişisel verilerin korunması kapsamında aksiyon almayan tek Avrupa Konseyi üyesi devlet olarak kalmıştır.[181] Bu noktada kanunun içeriğinin ne denli önemli olduğunu dikkate alındığında, söz konusu tasarı üzerine yapılan tartışmaların bitmek bilmemesinin bu gecikmelere sebep olduğunu söylemek yanlış olmayacaktır.[182]

Nihayet 108 sayılı sözleşme, 6669 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesinin Onaylanmasının Uygun

---

[178] Songül Atak, "Avrupa Konseyinin Kişisel Veriler Açısından Sağladığı Temel Güvenceler", **Türkiye Barolar Birliği Dergisi**, Sayı 87, 2010. s.93 Atak bahsi geçen çalışmasında Türkiye'nin 108 sayılı sözleşmeyi imzalamış olmasına rağmen onaylamamasının sebebini sözleşmenin 4. Maddesine bağlayarak, söz konusu maddede yer alan ve sözleşmenin onaylanması ile birlikte taraf devletlere iç hukuklarında bazı önlemler alma yükümlülüğü düzenleyen maddenin Türkiye'yi bu sözleşmeyi onaylamaktan alıkoyduğunu ifade etmiştir.

[179] Ali Karagülmez, **Bilişim Suçları ve Soruşturma – Kovuşturma Evreleri**, Seçkin Yayınları, Mayıs 2005, Ankara, s.228

[180] Olgun Değirmenci, "Türk Ceza Kanunu'nun Bilişim Suçları Bakımından Değerlendirilmesi", **Türkiye Barolar Birliği Dergisi**, S.58, 2005, s.202. Değirmenci Kişisel Verilerin Korunması Konusunda bir kanun çıkarılmadığı müddetçe, Türk Ceza Kanunu'nda yer alan kişisel verilerin korunmasına yönelik suç tiplerinin konu bakımından bir anlam ifade etmeyeceği şeklinde görüş bildirmiştir.

[181] Küzeci, **Kişisel Verilerin Korunması**, 2018, s. 285

[182] Özel, **6698 Sayılı Kişisel Verilerin Korunması Kanunu Üzerine Genel Bir Değerlendirme**, s.1

Bulunduğuna Dair Kanun ile onaylanmış ve sözleşme 18 Şubat 2016 Tarihli Resmî Gazetede yayımlanarak yürürlüğe girmiştir. 108 sayılı Sözleşmenin onaylanması ve yürürlüğe girmesi ile birlikte, aynı sözleşmenin yukarı bahsedilen 4. maddesi kapsamında, Türkiye'nin ulusal mevzuatında kişisel verilerin korunmasına hakkında bir düzenleme yapması kaçınılmaz hale gelmiştir.[183] Bunun üzerine ise 24 Mart 2016 tarihinde TBMM Genel Kurulu tarafından kabul edilmiş ve aynı tasarı 7 Nisan 2016 tarih ve 29677 sayılı Resmî Gazetede yayımlanarak yürürlüğe girmiştir.

6698 sayılı Kişisel Verilerin Korunması Kanunu, yasa yapma tekniği açısından değerlendirildiğinde, kanunun yedi bölümden oluşan ve temel olarak kişisel verilerin korunmasına ilişkin temel ilkeleri, verilerin işlenmesine ilişkin esasları, kişilerin hak ve yükümlülüklerini, denetim sistemini ve bu sisteme başvuru ve şikâyet süreçlerini, teşkilat yapısını ve kanuna aykırılık halinde yaptırımlarını düzenleyen ve geçici maddeleri barındıran kısa bir kanun olduğu görülecektir.

Kanunun akabinde ise, yasa koyucu tarafından, kanunun uygulaması bakımından yol gösterici olması için bazı yönetmelikler ve tebliğler de yürürlüğe girmiştir. Buna göre 5 Mayıs 2018 tarihli Kişisel Verileri Koruma Kurumu Personeli Görevde Yükselme ve Unvan Değişikliği Yönetmeliği, 26 Nisan 2018 Kişisel Verileri Koruma Kurumu Teşkilat Yönetmeliği, 9 Şubat 2018 Kişisel Verileri Koruma Uzmanlığı Yönetmeliği, 30 Aralık 2017 Veri Sorumluları Sicili Hakkında Yönetmelik, 16 Kasım 2017, Kişisel Verileri Koruma Kurulu Çalışma Usul ve Esaslarına Dair Yönetmelik 28 Ekim 2017 Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik, bugüne dek çıkarılan yönetmelikler kapsamında sayılabilecektir. Diğer yandan 10 Mart 2018 tarihinde ise Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ ve Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ yürürlüğe girmiştir. Kanundaki maddelerin uygulanması için düzenleyici nitelikte olan bu hukuki metinler ikinci bölümde ayrıntılı olarak incelendiğinden burada tekrar olmaması açısında bir kere daha tekrar edilmemiştir.

[183] 100 soruda kişisel verilerin korunması. https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/7d5b0a2f-e0ea-41e0-bf0b-bc9e43dfb57a.pdf 25.10.2018

c. Türk Ceza Kanunu

Türk Ceza Hukuku bakımından kişisel verilerin korunmasına ilişkin ilk düzenlemeler 5237 sayılı Türk Ceza Kanunu kapsamında düzenlenmiştir. 765 sayılı Türk Ceza Kanunu'na baktığımızda kişisel verilerin korunmasına ilişkin bir düzenleme bulunmamaktaydı. Uygulamada ise yasa uygulayıcı makamlar kişisel verilerin korunması hakkını 765 sayılı kanunun 'Sırrın Masuniyeti Aleyhinde Cürümler' başlıklı beşinci faslının 195. ve 200. Maddeleri arasında özel yaşam ve haberleşme dokunulmazlığı kapsamında değerlendirmeye çalışmışlardır.

765 sayılı Türk Ceza Kanunu'nun 'Sırrın Masuniyeti Aleyhinde Cürümler faslında özel yaşam ve haberleşme dokunulmazlığına ilişkin anayasal güvenceye aykırılık yaptırımı öngörülmüş bulunmaktaydı.[184] Söz konusu fasıl incelendiğinde bu faslın mektup, telgraf gibi haberleşme araçlarının ifşası etrafında toplandığı ve bununla sınırlı olarak ele alındığı görülecektir. Genel olarak söz konusu fasıl altındaki suçları inceleyecek olursak, kanunun 195. maddesi (haberleşmenin ihlali), 196. maddesi (haberleşme kağıtlarını ortadan kaldırma) ve 197. maddesinde (hususi mektupların veya telgrafların neşir ve ifşası) özel sıfatı olmayan kimselerin işleyebilecekleri haberleşme hürriyetini ihlal suçlarının, 198. Maddesinde resmi mevkii veya sıfatı veya meslek sanatı dolayısıyla öğrendikleri sırrı ifşa edenlerin suçlarının ve son olarak 200. Maddesinde ise posta, telgraf ve telefon idaresi memurları ile müstahdemlerinin sırrın ifşasına ilişkin olarak işleyebilecekleri suçların düzenlendiği görülmektedir.

Elbette bu düzenlemelerin kişisel verilerin korunması bakımından son derece yetersiz olduğu aşikardı. Nitekim kanunun işbu beşinci faslı kanunun yürürlükte olduğu dönemde de hem uygulama bakımından yetersiz kalması hem de ilgili faslın düzenleme tekniğine ilişkin olarak eleştirilere maruz kalmıştır. Doktrindeki bazı yazarlara göre haberleşme özgürlüğüne ilişkin suçların hem bu faslın altında olması hatalıdır hem de kapsamı bakımından uygulama ile bağdaşmamaktadır.[185]

---

[184] Durmuş Tezcan, Mustafa Ruhan Erdem, R. Murat Önok, **Teorik Ve Pratik Ceza Özel Hukuku**, 9.Baskı, Ankara, Seçkin Yayınevi, Şubat 2013, s. 498

[185] Mehmet Emin Artuk**,** Ahmet Gökçen**,** Caner Yenidünya, **Ceza Hukuku Özel Hükümler**, 4.Baskı, Turhan Kitapevi, Ekim 2003, s.227. Artuk, Gökçen ve Yenidünya Türk Ceza Kanunu'nda Sırrın Masuniyeti Aleyhinde Cürümler başlığı altında haberleşme hürriyeti aleyhinde işlenen suçlarında düzenlenmiş olmasını hatalı bulmuş ve kanundaki amacın esasen haberleşme araçlarını haksız müdahalelerden korumak olduğunu ve dolayısıyla başlıktan bağımsız olarak bu bölümdeki suçların oluşması için haberleşme aracındaki bilginin sır teşkil edip etmediğinin önemsiz olduğunu

Gerçekten de 765 sayılı kanunda kişisel verilerin korunmasına ilişkin bağımsız suç tiplerinin düzenlenmemiş olması uygulamada büyük ölçüde sorunlara sebebiyet vermiştir. Söz konusu kanunda yalnızca haberleşme dokunulmazlığının ihlaline ilişkin düzenlemeler yapıldığından, bunun dışında kalan kişisel verilerin korunması ve özel hayatın gizliliği kapsamında korunması gereken kişi haklarının ihlali halinde uygulanacak düzenleme bakımından kanun boşlukları ortaya çıkmıştır. Bu boşluklar ise dönem itibariyle Yüksek Mahkeme tarafından oluşturulan içtihatlar aracılığı ile doldurulmaya çalışılmıştır.

Nihayet ilk kez 2004 tarihli 5237 sayılı Türk Ceza Kanunda kişisel verilerin korunmasına ilişkin bağımsız suç tipleri düzenlenmiş ve 765 sayılı kanundaki bu eksiklikler, 5237 sayılı kanununda kişisel verilerin korunmasına ilişkin suç tiplerinin, haberleşme hakkının ve özel hayatın gizliliği hakkının ihlali suçlarından ayrı olarak düzenlenmesi ile giderilmeye çalışılmıştır.

5237 sayılı Türk Ceza Kanunu'nun 'Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar' başlıklı dokuzuncu bölümünün 134. Maddesi ve bunu izleyen maddelerinde kişisel verilerin korunmasına ilişkin özel suç tipleri düzenlenmiştir. Söz konusu kanunda yer verilen ve kişisel verilerin korunmasına ilişkin bağımsız suç tipleri şu şekilde sıralanmıştır; 'Kişisel Verilerin Hukuka Aykırı Olarak Kaydedilmesi' (m.135), 'Verileri Hukuka Aykırı Olarak Verme Veya Ele Geçirme' (m.136), 'Verileri Yok Etmeme' (m.137).

5237 sayılı Türk Ceza Kanunu'nda kişisel verilerin korunması ile ilintili olabilecek, kişisel verilerin dolaylı olarak korunduğu başka suç tipleri de bulunmaktadır. Bu suç tipleri 132. Maddede düzenlenen haberleşmenin gizliliğinin ihlali, 133. Maddede düzenlenen bireyler arasındaki konuşmaların dinlenmesi ve kayda alınması, 134. Maddede düzenlenen özel hayatın gizliliğini ihlal, 239. Maddede düzenlenen ticari sır, bankacılık sırrı veya müşteri sırrı niteliğindeki bilgi veya belgelerin açıklanması ve 243 ve 244. Maddelerde düzenlenen bilişim sistemine girme, sistemi engelleme, bozma verileri yok etme veya değiştirme suçları olarak

---

vurgulamıştır. Yazarlara göre önemli olan haberleşme aracına haksız müdahalenin varlığıdır; örneğin bu bir mektup ise bu mektup içinde yer alanların sır olması suçun oluşması için şart değildir.

sayılabilecektir. Çalışmamızın konusunu bu suç tipleri oluşturmadığından söz konusu suç tipleri ayrı başlıklar altında incelenmeyecek ancak suçların içtimaına ilişkin bölümlerde kişisel verilerin korunmasına ilişkin suç tipleri ile bağlantılarına yer verilecektir.

Yukarıda da ifade ettiğimiz üzere zaman içerisinde yaşanan teknolojik gelişmeler ve uluslararası zeminde kişisel verilerin korunması konusunda daha somut adımlar atılması yönündeki taleplerin artması ile 5237 sayılı TCK kapsamında yapılan düzenlemeler de yetersiz kalmaya başlamıştır. Kişisel verilerin korunması temel hak ve özgürlüklerin ayrılmaz bir parçası olduğundan, ülkemizde kişisel verilerin korunması konusunda yeterli ve detaylı bir yasanın olmayışı, özellikle siyasi olarak yoğun gündemlerin yaşandığı yıllarda kişilerin başta siyasi görüş ve etnik kimlik gibi hassas verileri olmak üzere "*fişlenmelerine, güvenlik soruşturmaları geçirmelerine*" sebebiyet vermiştir.[186] Hal böyleyken kişisel verilerin korunması hususuna özellikle bu yönü ile yaklaşıldığında, Türkiye'de uzun yıllardır konuya ilişkin kapsamlı bir kanunun olmayışının ne denli büyük bir eksiklik olduğu kolaylıkla anlaşılabilir. 5237 sayılı Türk Ceza Kanunu kapsamında yapılan düzenlemeler, yetersiz olmaları ve birtakım ihtiyaçları karşılamaktan uzak kalmaları sebebiyle eleştirilmişlerdir.[187]

Bu noktada belirtmek isteriz ki, 5237 sayılı Türk Ceza Kanunu kapsamında yer verilen kişisel verilerin korunmasına konusundaki suç tipleri incelenecek ise bu suç tipleri 6698 sayılı Kişisel Verileri Koruma Kanunu dikkate alınarak incelenmesi gerekmektedir. Çünkü gerek söz konusu kanunda Türk Ceza Kanunu'na yapılan atıflar bulunması gerek ise Türk Ceza Kanunu'nun da konuya ilişkin suç tiplerinin kişisel verilerin tanımı başta olmak üzere pek çok eksikliği işbu kanun ile tamamlıyor olması, bu bölüme konu suç tiplerinin söz konusu kanun ile birlikte değerlendirilmesini zorunlu kılmıştır. Nitekim çalışmamızın ilgili üçüncü bölümünde de inceleme bu şekilde yapılmıştır.

---

[186] İbrahim Korkmaz, "Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme", **Türkiye Barolar Birliği Dergisi,** Ankara, S.124, Mayıs-Haziran 2016, s.85

[187] Hakan Karakehya, "Türk Ceza Kanununda Bilişim Sistemine Girme Suçu", **Türkiye Barolar Birliği Dergisi,** Ankara, S.81, 2009, s.4

İKİNCİ BÖLÜM

KİŞİSEL VERILERIN KORUNMASI KANUNU KAPSAMINDA KİŞİSEL VERİLERİN KORUNMASI

I. KİŞİSEL VERİLERİN KORUNMASI KANUNU İLE GETİRİLEN DÜZENLEMELER

A. KİŞİSEL VERİLERİN KORUNMASI KANUNU'NUN KAPSAMI

1. Amaç ve Kapsam

Kişisel Verilerin Korunması Kanunu'nun amacı, kanunun amaç başlıklı birinci maddesinde düzenlenmiştir. Buna göre bu kanunun amacı en başta özel hayatın gizliliğinin korunması olmak üzere kişisel verilerin işlenmesinde bireylerin temel hak ve özgürlüklerini korumak ve bireylerin kişisel verilerini işleyen gerçek veya tüzel kişilerin tüm yükümlülükleri ile bu kişilerin uyacakları tüm usul ve esasları düzenlemektir. Görüldüğü üzere çalışmamızın birinci bölümünde de belirtildiği gibi ülkemizde de kişisel verilerin korunması konusunda, insan hakları yaklaşımı benimsenmiş ve yasayla başta özel hayatın gizliliğinin korunması olmak üzere bireylerin temel hak ve özgürlüklerinin[188] kişisel verileri işleyen tüm gerçek ya da tüzel kişilere karşı korunması amaçlanmıştır. Doktrinde bazı yazarlar bu yasa kapsamında özel hayatın gizliliği ile yakından ilişkili bilgi alma hakkının da bu yasa kapsamında korunduğunu ifade etmiştir.[189] Dikkat edileceği üzere, yasa kapsamında lafzi olarak kişisel verilerin korunması hakkına yer verilmemiştir.[190] Doktrinde bu husus da eleştirilere neden olmuş ve söz konusu hakka mevzuatta yer verilmesinin son derece önemli olduğu vurgulanmıştır. [191]

---

[188] Küzeci, **Kişisel Verilerin Korunması**, 2018, s.319
[189] Dülger, **Kişisel Verilerin Korunması Hukuku**, s.197
[190] Küzeci, **Kişisel Verilerin Korunması**, 2018, s.320
[191] Dülger, **Kişisel Verilerin Korunması Hukuku**, s.197

Kişisel Verilerin Korunması Kanunu'nun kapsamı ise, yine kanunun ikinci maddesinde düzenlenmiştir. Buna göre kanun, kişisel veri sahibi ve verileri işlenen gerçek kişiler başta olmak üzere, bu kişilerin kişisel verilerini tamamen otomatik veya kısmen otomatik yollarla işleyen gerçek ve tüzel kişiler hakkında veya kişisel verileri hiçbir otomatik yol ile işlemediği halde işlenen verilerin herhangi bir veri kayıt sistemine dahil olması durumunda bu verileri işleyen gerçek ve tüzel kişiler hakkında uygulanacaktır. Görüldüğü üzere, Kişisel Verilerin Korunması Kanunu kapsamına kişisel verileri işlenen gerçek kişiler girmektedir. Bunun yanında veri işleyen olarak ise bu verileri otomatik ya da kısmen otomatik yollarla işleyen ya da otomatik yöntemler kullanmaksızın bir veri kayıt sisteminin parçası olan verileri işleyen gerçek ya da tüzel kişiler girmektedir.

Bu madde ile hukukumuzda kişisel verileri korunacak olan kişilere tüzel kişilerin de dahil olup olmadığına ilişkin tartışma son bulmuştur. Zira madde ile net bir şekilde kişisel verileri korunacak olan kişilerin gerçek kişiler olduğu ifade edilmiştir. Her ne kadar üçüncü bölümde ayrıntılı olarak açıklandığı üzere Türk Ceza Kanunu'ndaki düzenlemeler bakımından da doktrindeki ağırlıklı görüş kişisel verilerin korunması hukuku bakımından gerçek kişilere ait kişisel verilerin koruma kapsamında olduğu yönünde olsa da bu kanun ile bu hususun netleştirilmesi yerinde olmuştur.

2. Kanun Kapsamı Dışında Kalan Haller

Kişisel Verilerin Koruma Kanunu kapsamında verileri korunacak olan kişilerin gerçek kişiler olduğunu daha önce de belirtmiştik. Bu durumda yasa koyucunun tüzel kişilere ait verileri bu kanunun kapsamı dışında tuttuğunu söyleyebiliriz. Yasa koyucu bu kanun kapsamında yalnızca gerçek kişilere ait kişisel verilerin korunduğunu düzenledikten sonra, kişisel verilerin kayıt edilme sistemi bakımından da bir ayrım yaparak, tamamen veya kısmen otomatik olan yöntemlerle işlenen verileri ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen verileri bu kanun kapsamında koruma altına alarak bunun dışındaki yöntemlerle işlenen kişisel verilerin bu kanun kapsamı dışında bırakmıştır. Bu durumda, otomatik olmayan yöntemlerle işlenen ve bir veri kayıt sisteminin parçası olmayan tüm kişisel veriler bu kanun kapsamı dışında bırakılmıştır.

Diğer yandan kanunun 28. Maddesinde kanun kapsamı dışında tutulan haller düzenlenmiştir. Buna göre ilgili maddenin ilk fıkrasında tamamen kanun kapsamı dışında tutulan haller düzenlenmiştir. Buna göre; kanun maddesinde öngörülen sınırlara uyulmak şartıyla gerçek kişilerin bizzat şahsı ile ilgili ya da bu kişilerin aileleri ile ilgili hususlar kapsamında verilerinin işlenmesi, kişisel verilerin anonim hale getirilmeleri şartıyla çeşitli araştırma, istatistik gibi faaliyetlerde işlenmesi, kişisel verilerin yine kanunda öngörülen sınırları dikkate alınmak şartıyla bilimsel gerekçelerle işlenmesi, kişisel verilerin ulusal güvenlik ya da ulusal savunma gibi milli sebeplere dayanmak suretiyle devletin kurum ve kuruluşları tarafından istihbarat kapsamında işlenmesi ya da yargı mercileri tarafından yargı ya da infaz sürecindeki gerekliliklerin yerine getirilebilmesi amacıyla işlenmesi halleri tamamen kapsam dışında bırakılmıştır.

Aynı maddenin ikinci fıkrasında ise kısmen kanun kapsamı dışında tutulan haller sayılmıştır. Buna göre kişisel veri işlemenin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması, suçun önlenmesi amacıyla kişisel veri işlemenin gerekli olması, kişisel verilerin bizzat veri sahibi tarafından aleni hale getirilmesi, kamu kurum ve kuruluşları ile bu nitelikteki meslek örgütlerinin kendi içlerindeki denetim faaliyetleri kapsamında disiplin süreçleri için gerekli olması, devletin finansal ve mali menfaatlerinin korunması için gerekli olması, hallerinin söz konusu olması durumunda bu hallere ilişkin olarak Kanun'un veri sahiplerinin haklarına ilişkin 11. Maddesi ve veri sorumlularının sicile kayıt yükümlülüğüne ilişkin 16. maddesi uygulanmayacaktır. Ancak bu hallerde dahi kanunun amacı ve ilkeleri ile uyumlu ilkesi baki tutulmuş ve veri sorumlularının aydınlatma yükümlülüklerine ilişkin 10. Madde ve veri sahibinin zararın giderilmesini talep hakkının da bu hallerde dahi uygulanmaya devam edeceği belirtilmiştir. Bu bakımından söz konusu haller kanunun kısmi[192] istisnaları olarak tanımlanmıştır.

3. Tanımlar

Kişisel Verilerin Korunması Kanunu kapsamında yer verilen kavramlar kanunun tanımlar başlıklı 3. maddesinde ayrıntılı olarak düzenlenmiştir. Buna göre söz konusu madde çerçevesinde açık rıza, anonim hale getirme, veri sahibi, kişisel veri, kişisel verilerin işlenmesi, verileri işleyen kişi, veri sorumluları, veri kayıt sistemi gibi önemli

[192] Dülger, **Kişisel Verilerin Korunması Hukuku**, s. 201

kavramlar açıklanmıştır. Biz bu başlık altında saydığımız bu kavramları inceleyip, geri kalan kavramlardan ise bu bölüm kapsamında sırası geldikçe ayrıntılı olarak bahsedeceğiz.

a. Kişisel Veri

6698 sayılı Kişisel Verilerin Korunmasına İlişkin Kanunu yürürlüğe girmeden önce kişisel verinin tanımı için öncelikle uluslararası düzenlemelere atıf yapılmıştır. 108 sayılı sözleşmenin ikinci maddesinin a bendinde kişisel veri bir kişinin kimliğini belirli ya da belirlenebilir kılan her türlü bilgi şeklinde açıklanmıştır. Sözleşme'nin özel nitelikli hassas verileri düzenleyen 6. maddesinde ise ulusal hukuklarda gereken önlemler alınmadıkça bireylerin din, etnik köken, cinsel yaşam, ceza mahkumiyetleri gibi hassas verilerinin otomatik yöntemlerle işlenemeyeceği ifade edilmiştir.

Ekonomik Kalkınma ve İşbirliği Örgütü yani kısaca OECD tarafından yayınlanan ve kişisel verilerin korunmasına ilişkin rehber niteliğindeki ilkelerde de kişisel veri kimliği belirli ya da belirlenebilir olan gerçek bir kişiye ait bilgilerin tamamı olarak açıklanmıştır. 95/46/EC sayılı Veri Koruma Direktifi'nin 2. maddesinde ise kişisel veri tanımı biraz daha genişletilerek yukarıdaki açıklamaya ek olarak ayrıca yine gerçek kişinin doğrudan ya da dolaylı şekilde tanınmasına olanak veren veriler olarak açıklanmış ve buna örnek olarak da kişinin vatandaşlık numarası ya da psikolojik kimliği gibi bu kişiyi tanınabilir hale getirebilecek her türlü bilginin bu kapsamda değerlendirileceği ifade edilmiştir.

Diğer yandan bu direktifi mülga eden Avrupa Birliği Genel Veri Koruma Tüzüğü'nün 4. Maddesinde ise kişisel veri yine yukarıdaki açıklamalarımıza uygun şekilde tanımlandıktan sonra kişinin lokasyon bilgi ya da çevrimiçi kimlik belirleyici verileri ya da genetik, mental, psikolojik verileri gibi verilerinin de kişisel veri olduğu ve bireyin birden fazla kişisel verisine atıfta bulunarak bireyin tanımlanabilmesine olanak veren tüm veriler şeklinde ifade edilmiştir. Görüldüğü üzere burada öncekinden farklı olarak, kişisel veri kapsamında değerlendirilecek veri kategorileri artırılmıştır.

Esasen uluslararası düzenlemelere baktığımızda tüzel kişilerin kişisel veri tanımı kapsamına alınmasında bir engel bulunmadığı görülmektedir. 1995/46/EC Veri Koruma Direktifinde ve onu mülga eden Avrupa Birliği Genel Veri Koruma

Tüzüğünde yer alan kişisel veri tanımında yalnızca gerçek kişilerin sahibi olduğu kişisel veriler ifade edilmiş olmasına rağmen ulusal hukuklarda yapılan düzenlemelerde kişisel veri sahibinin gerçek kişiler yanında tüzel kişiler olarak da tanımlanması mümkün gözükmektedir. Ancak ülkemizde kişisel verilerin korunması hukuku kapsamına yalnızca gerçek kişiler dikkate alınmıştır. Ancak örneğin Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Hakkında Yönetmelik kapsamında kişisel veri tanımına tüzel kişiler dahil edilmiştir.[193]

AİHM kararlarında da kişilere ait *"görüntü", "fotoğraf", "parmak izi", "DNA*[194] *profili", "hücre örnekleri", "ev adresi" ve "yaş, doğum tarihi ve fiziksel özellikler"* kişisel veri kapsamında değerlendirilmektedir.[195] AİHM vermiş olduğu bir kararında; hakkında gözaltı kararı verilen kişilerin hücre örneklerinin, kanının ve bunun yanı sıra parmak izinin alınmasına rağmen bu kişilerin kendilerine isnat edilen suçla bağlantıları kesildikten sonra bu hassas kişisel verilerinin tutulmaya devam edilmesini Avrupa İnsan Hakları Sözleşmesinin özel hayata ve aile hayatına saygı başlıklı 8. maddesinin ihlâl edildiği yönünde değerlendirmiştir.[196]

Anayasa Mahkemesi de çeşitli kararlarında da kişisel verinin tanımına ilişkin bazı ifadelere yer vermiştir. Buna göre Anayasa Mahkemesi kararlarında kişisel veri, bireyi ortaya koyan ya da onu belirlenebilir kılan bütün bilgileri ifade etmekle birlikte yalnızca bireyin kimliğini ortaya koyan bilgiler değil; araç plakası, pasaport numarası, cv, bireye ait görüntü, bireyin sesi ve hatta hobileri, iletişim içinde olduğu kişiler, dahil olduğu toplulukları gibi bireyi bir şekilde tanınabilir hale getiren bütün veriler kişisel veri kapsamında değerlendirilmiştir.

---

[193] Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Hakkında Yönetmeliği'nin 3.maddesinde görüleceği üzere kişisel veri tanımına tüzel kişiler de dahil edilmiştir.

[194] Gülsün Ayhan Aygörmez Uğurlubay, Almanya, İsviçre ve Avusturya Hukuku Bağlamında Türk Ceza Muhakemesi Hukukunda Adlî DNA Analizleri, **İstanbul Üniversitesi Ceza Hukuku ve Kriminoloji Dergisi,** 2017, S.5(2), s..58**.** Uğurlubay konuyu şöyle değerlendirmiştir. "*DNA profilleri, 'kişinin DNA'sına birebir karşılık gelen şifrelenmiş numara dizileridir'. Bu numara dizileri her kişide farklı farklı olduklarından 'kişinin kimlik belirteci' niteliğindedirler. Şu hâlde genetik parmak izi mahiyetinde olan DNA profillerinin (kimlik şablonları) kişiyi belirli veya belirlenebilir kılan biyometrik bir veri olarak, kişisel veri mahiyetinde olduklarından şüphe yoktur."*

[195] Alkaya v Türkiye, B. No:42811/06, 09.10.2012. Başvurucu ev adresinin gazetede yayınlanması üzerine mahkemeye başvurmuş ve kamuya mal olmuş kişi olması gerekçesi ile reddedilen davasını önce Anayasa Mahkemesi'ne daha sonra da AİHM' e taşımıştır. AİHM başvurucuyu haklı bulmuş ve Türkiye'yi tazminat ödemeye mahkûm etmiştir.

[196] S. Marper v. UK, B. No: 30562/04 ve 30566/04, 04.12.2008.

Anayasa Mahkemesi söz konusu kişisel veri tanımı ışığında pek çok yasal düzenlemeyi de kişisel verilerin korunmasına ilişkin Anayasa'nın 20. Maddesine aykırı bularak iptaline karar vermiştir. Anayasa Mahkemesi bir kararında kişisel verilerin korunmasına ilişkin tüm düzenlemelerin Anayasa'nın 20. Maddesi gereğince yalnızca kanunlarla düzenlenebileceği gerekçesiyle elektronik haberleşme sektöründe kişisel verilerin işlenmesi ve gizliliğinin korunmasına ilişkin düzenlemeyi yapma yetkisini Bilgi Teknolojileri ve İletişim Kurumuna tanıyan ve söz konusu itiraza konu edilen kuralın iptaline karar vermiştir.[197]

Yine Anayasa Mahkemesi, hiçbir bir hukuki inceleme kapsamında yer almaksızın TİB tarafından internet trafik bilgisinin işletmecilerden alınmasını ve hâkim kararına bağlı olarak bu bilginin birtakım kuruluşlara iletilmesini düzenleyen kuralı trafik bilgisinin de kişiyi kimliği belirlenebilir kılmasından ötürü kişisel veri olduğu ve TİB tarafından istenen bu bilginin işlenmesi bakımından bahsi geçen kuralda hiçbir sınırlama olmadığı gerekçeleriyle Anayasanın ilgili maddelerine aykırılıktan iptaline karar vermiştir.[198]

Yargıtay kararlarında da kişisel verinin tanımına ilişkin açıklama yapılmış olup buna göre Yargıtay kararlarında kişisel veri bireyin, bu verilere erişim konusunda yetkisi bulunmayan 3. kişilere açıklamadığı, aleni olmayan ve genel olarak herkes tarafından bilinmesi mümkün olmayan, bireyin kimliğini ortaya koyan ya da bireyin kimliğini tespit edilebilir kılan ve gerçek kişilere ait tüm bilgiler olarak tanımlanmıştır.[199]

Bu noktada belirtmek gerekir ki, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun yürürlüğe girmeden önce kişisel verinin tanımına yönelik tartışmalar kapsamında herkes tarafından bilinen veya ulaşılması kolay kişisel verilerin yasal anlamda kişisel veri kapsamında değerlendirilemeyeceği belirtilmiştir.[200] Yargıtay'ın yukarı da yer verildiği üzere eski tarihli bazı kararları da bu yöndeydi. Ancak Yargıtay

---

[197] Anayasa Mahkemesi Kararı için bkz. Mahkemenin 2013/122E., 2014/74K., 09.04.2014T. sayılı kararı.
[198] Anayasa Mahkemesi kararı için bkz. Mahkemenin 2014/149E., 2014/151K., 02.10.2014T. sayılı kararı
[199] Yargıtay 12. Ceza Dairesi 2012/16872 Esas, 2012/18221.
[200] Korkmaz, **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, s. 343

teknolojik gelişmeler karşısında son yıllarda görüş değiştirmiş olup vermiş olduğu güncel kararlarda açıkça, mevcut olayın koşulları göz önünde bulundurulmak ve detaylı şekilde incelenmek koşuluyla herkes tarafından bilinen ya da kolaylıkla bilinmesi mümkün olan verilerin de kişisel veri olarak değerlendirilmesi gerektiğini ifade etmiştir. Yargıtay mevcut olay değerlendirilmeksizin her türlü verinin kişisel veri kabul edilmesi halinde bunun pratikte her türlü fiilin suç teşkil etmesi gibi problemlere sebebiyet vereceğini belirtmiştir. [201]

Nitekim gelişen teknoloji ve sosyal medya kullanımı dikkate alındığında kanaatimizce de aksi yöndeki görüşün uygulama bakımından problemlere yol açacağı açıktır. Örneğin günümüzde sosyal medyanın hızla gelişmesi sonucunda kişisel veri olduğu şüphesiz olan fotoğraflara sosyal medya hesapları aracılığı ile kolaylıkla ve çaba sarf etmeksizin ulaşılabilmektedir. Bu durumda bir kişinin fotoğrafına ulaşan ve bu fotoğrafı başka amaçlar için yetkisiz olarak kullanan 3.kişilerin, fotoğraf sahibinin kişisel verilerinin korunmasına yönelik hakkını ihlal ettikleri aşikardır. Yargıtay tarafından verilen yakın tarihli emsal kararlar da bu yöndedir. [202]

Nihayet 6698 sayılı Kişisel Verilerin Korunmasına İlişkin Kanunun 3.maddesinde kişisel verinin tanımı yapılmış ve uzun yıllardır süregelen kişisel verinin tanımına ilişkin tartışmalara bir son verilmiştir. 6698 sayılı kanunun 3. maddesine göre "*kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilg*i" olarak tanımlanmıştır. İlgili kanunun gerekçesinde ise kişisel veri "mevcut verilerin herhangi bir şekilde bir gerçek kişiyle ilişkilendirilmesi suretiyle, o kişinin tanımlanabilir hale getirilmesi" olarak tanımlanmıştır.[203] Keza yine kanunun

---

[201] Yargıtay ilgili kararında kolaylıkla ulaşılması mümkün olan ve herkes tarafından bilinebilecek durumda olan verilerin kişisel veri kabul edilip edilmemesi konusunda, pratikte her türlü veriye ilişkin her eylemin suç teşkil etmesini engellemek için, her olayın kendi içerisinde değerlendirilmesi gerektiğini, söz konusu olayda bir hukuka uygunluk sebebi uygulanabilecek ise bunun göz önünde bulundurulması gerektiğini ve sanığın gerçekleştirdiği eylemle ilgili olarak hukuka aykırılık bilincini taşıması gerektiğini ifade etmiştir. Yargıtay Ceza Genel Kurulu 17.06.2014 T., 2012/12-1510E., 2014/331K.

[202] Yargıtay ilgili kararında bir kişinin suç tarihinden önce kendi rızası ile çektirdiği ve kendi sosyal medya hesabında yayınladığı fotoğraflarının, şüpheli tarafından fotoğrafların sahibinin rızası ve bilgisi haricinde diğer şüpheliye iletilip bu fotoğraflarında şüphelilerden birinin firmasının reklamlarında kullanmasının, dosyada bu iddiayı ispata yarar delillerinde varlığı dikkate alındığında, Türk Ceza Kanunu'nun 136. maddesinde düzenlenen kişisel verilerin hukuka aykırı şekilde verilmesi ya da ele geçirilmesi suçunu teşkil ettiğinden şüpheliler hakkında dava açılması gerektiğini ifade etmiştir. Yargıtay 12. Ceza Dairesi'nin 2016/12683 E., 2017/3796 K. ve 07/10/2015 T. Kararı.

[203] 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 3. maddesi'nin gerekçesine göre Yargıtay bu kararında kişisel veri tanımındaki 'belirlenebilirlik' ifadesi değerlendirilirken orantılılık ilkesinin dikkat alınması gerektiğini ifade etmiştir. Bu ilkeyi ise eldeki veriler ile bir bireyin tespiti için normalden fazla

gerekçesinde isim, telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler gibi verilerin kişileri belirli veya belirlenebilir kılma özelliklerinin bulunması nedeniyle kişisel veri olduğu ifade edilmiştir.

Bir diğer dikkat çeken husus ise, 6698 sayılı kanunun gerekçesinde kişiye ait görüntü ve ses kayıtları da kişisel veriler kapsamında sayılmıştır. Kişiye ait ses ve görüntü kayıtlarının kişisel veri olarak nitelendirilmesi, 6698 sayılı kanunun gerekçesinde yer verilen eldeki kayıtların ve verilerin değerlendirilmesi neticesinde bir kişinin tespit edilebilir hale gelmesi şeklindeki tanımıyla da paralellik göstermektedir.

Konuyla ilgili dikkat çeken diğer bir husus ise, ilgili kanunun tasarı aşamasındaki metninde kişisel veri belirli ya da eldeki verilerin bir araya getirilmesi suretiyle belirlenebilir hale gelebilen ve gerçek kişiler ile tüzel kişilere ait olan her türlü veri olarak tanımlanırken, daha sonra yürürlüğe giren 6698 sayılı kanun metninde kişisel veri tanımı yalnızca gerçek kişilere ait verileri kapsayacak şekilde değiştirilmiştir. Madde metninde yapılan bu yerinde değişiklik ile söz konusu kanun ile Türk Ceza Kanunu arasında doğabilecek çelişki ortadan kaldırılmıştır. Nitekim Türk Ceza Kanunu'nda yer alan 135. madde ve bu maddenin devamında yer alan maddelerde düzenlenen kişisel verilerin korunmasına ilişkin suç tiplerinin konusunu yalnızca gerçek kişilere ilişkin veriler oluşturmaktadır.

b. Açık Rıza

Açık rıza Kişisel Verilerin Korunması Kanunu'nun tanımlar başlıklı 3.maddesinde tanımlanmıştır. Buna göre açık rıza bir kişinin belirli bir konuda bilgilendirilmesi üzerine kendi özgür iradesiyle verdiği rıza şeklinde açıklanmıştır. Kanun'un kişisel verilerin işlenmesi başlıklı 5. maddesinde ise bireyin açık rızası

---

bir çalışma ve emek gerekiyorsa, bu durumda orantılılık ilkesi gereği bu bireyin belirlenebilir olduğunu söylenemeyeceğini ifade etmiştir. Yargıtay bir bireyin eldeki veriler ile tespitinde ortalama bir kişisinin ortalama yöntemler kullanarak sonuca ulaşması gerektiğini aksi takdirde bu yöntemlerin aşırı çaba içerisinde değerlendirileceğini ifade etmiştir. Ayrıca Yargıtay aynı kararında kişisel verilerin kişileri belirli ya da belirlenebilir kılmasında önemli olanın kişinin mevcut veriler değerlendirilerek tespit edilebilmesi olduğunu ifade etmiştir.
(Çevrimiçi) https://www.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf (Erişim Tarihi: 11.10.2018)

bulunmaksızın kişisel verilerinin işlenemeyeceği ifade edilmiştir. Yine Kanunu'nun 5.maddesinin ikinci fıkrada ise açık rızanın aranmayacağı haller sayılmıştır.

Nitekim Avrupa Birliği Veri Koruma Direktifine ve onu mülga hale getiren Tüzük'e bakıldığında da benzer bir düzenlemenin olduğu görülecektir. Buna göre söz konusu uluslararası düzenlemelerde de kişinin ırki kökeni, siyasi düşüncesi, dini ve felsefi görüşü, sendikal üyelikleri, genetik datası veya biyometrik datası, sağlık, cinsel yaşam ve cinsel yönelimine ilişkin verileri hassas veri kategorisinde toplanmış ve bu verilerin kaydedilmesi hukuka aykırı kabul edilmiş ve ancak aynı madde metninin ikinci paragrafında kişinin açık rızasının bulunması halinde söz konusu yasağın uygulanmayabileceği ifade edilmiştir. [204]

Doktrinde bazı yazarlar tarafından kanunda açık rızanın sınırlarının çizilmesi gerektiği belirtilmiş ve kanun yapış tekniği açısından bu madde eleştirilmiştir.[205] Kanımızca açık rızanın her olay için ayrı ayrı değerlendirilmesi gerektiği düşünüldüğünde, açık rıza kavramının sınırlarının olabilecek en iyi şekilde çizildiğini düşünmekteyiz. Zira açık rıza en temel haliyle veri işleyene, verisi işleneni bilgilendirme yükümlülüğü ve verisi işlenene ise rızasını özgür iradeyle verebilme hakkı olarak tanımlanmış ve genel olarak açık rızanın sınırları çizilmiştir.

Açık rıza kavramı, Kişisel Verilerin Korunması Kanunu ile mevzuatımıza giren yeni bir kavram olması açısından son derece önemlidir. Nitekim çalışmamızın üçüncü bölümünde ayrıntılı olarak yer verildiği üzere, Türk Ceza Kanunu kapsamında kişisel verilere ilişkin suç tipleri bakımından rıza kavramı hukuka uygunluk sebebi olsa da Kişisel Verilerin Korunması Kanunu kapsamında rıza kavramından farklı olarak açık rıza kavramından bahsedilmiştir. Bu anlamda açık rıza kavramının anlaşılması, ayrıntılı olarak ortaya konulması, kanunun uygulaması açısından oldukça önemlidir. Zira kanunda sınırlı olarak sayılan, açık rıza aranmaksızın kişisel verilerin işlenebileceği hallerden birinin uygulanması söz konusu değilse, bireylerin kişisel verileri yalnızca açık rızaları alınmak suretiyle işlenebilecek ya da aktarılabilecektir.[206] Bu durumda bireyin açık rızası yasaya uygun şekilde alınmaksızın kişisel verilerin işlenmesi halinde hukuka aykırılık söz konusu olacağından açık rıza kavramı kanunun

---

[204] Avrupa Birliği Genel Veri Koruma Tüzüğü'nün tam metni, (Çevrimiçi) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL (Erişim tarihi: 14.08.18)
[205] Özel, **6698 Sayılı Kişisel Verilerin Korunması Kanunu Üzerine Genel Bir Değerlendirme**, s.3
[206] Dülger, **Kişisel Verilerin Korunması Hukuku**, s. 23

en önemli kavramlarından biridir. Buna göre açık rızanın tanımına baktığımızda, açık rızanın söz konusu olabilmesi için, bu rızanın öncelikle spesifik bir konuya ilişkin olması, bireyin bilgilendirilmesi ve bireyin özgür iradesi ile verilmiş olması gerekmektedir.

Açık rızanın belirli bir konuya ilişkin olması, kişiden verilerinin işlenmesine ilişkin onayı alınırken, ilgili kişiye verilerinin hangi konu kapsamında işleneceğini açıkça ve ayrıntılı olarak ifade etmek olarak açıklanabilecektir. Yani kişiye hangi kişisel verilerinin, hangi konuyla sınırlı olmak üzere işlendiği bildirilmelidir. Bu durumda kişi, yalnızca kendisine bildirilen kişisel verilerinin, yine yalnızca kendisine bildirilen konu kapsamında işlenmesine açık rıza göstermiş olacaktır. Bu sebeple doktrinde veri işleyenin, kişisel verilerin işlenmesi için gösterdiği amacın değişmesi halinde otomatik olarak konu da değişmiş olacağından, kişiden yeni bir açık rıza alınması gerektiği ifade edilmiştir. Yani kişiden belli bir konu için açık rıza alınması, bundan sonrasında farklı konular için de bu açık rızanın geçerli olduğu anlamına gelmeyecektir.[207]

Açık rızanın bilgilendirilmeye dayanması, yine açık rıza bakımından oldukça önemli kriterlerden biridir. Uluslararası düzenlemelere de uygun olan bu kriter kapsamında, kişisel verileri işlenecek olan kişinin, hangi verilerinin, hangi konuda, hangi süreyle işleneceği, bu konudaki hakları, işlenen verilerinin nasıl korunduğu şeklindeki tüm bilgilerin kişiye bildirilmesi gerekmektedir. Aksi takdirde kişinin verilerinin işlenmesine onay vermiş olsa bile bu rızanın kanuna uygun bir açık rıza olduğu söylenemeyecektir.

Burada açık rızanın tanımına bakıldığında dikkat çeken bir diğer kriter ise, açık rızanın kişinin özgür iradesine bağlı kılınmasıdır. Doktrinde özgür iradeden ne anlaşılması gerektiği ve uygulamada ne gibi durumlarla karşılaşılabileceği tartışılmıştır. Dülger özgür iradeyi "*kişinin kendi kararını kendisinin verebilme ve bunu dışarıya açıklama özgürlüğüne sahip olması ve yaptığı davranışın bilincinde*

---

[207] Dülger "*Açık rıza beyanının taşıması gereken özellikler göz önüne alındığında veri ilgilisinin veri sorumlusuna yönelteceği „'Kişisel verilerimin işlenmesini onaylıyorum' veya 'Bütün kişisel verilerin her türlü konuya ilişkin olarak işlenmesine rıza gösteriyorum' gibi genel ifadelerin Kanun'un aradığı nitelikte bir beyan olmadığına dikkat edilmelidir.*" şeklinde ifade ettiği görüşünde genel nitelikli ifadelerin açık rıza kavramı ile bağdaşmayacağını açıkça dile getirmiştir. Dülger, **Kişisel Verilerin Korunması Hukuku**, s.24

olması anlamına gelir" şeklinde tanımlamıştır.[208] Örneğin doktrinde kişinin verilerinin işlenmesine rıza göstermemesi halinde de istediği ürün veya hizmeti alabilmesinin açık rızanın özgür iradeye dayalı olup olmadığının tespitinde önemli bir unsur olduğu ifade edilmiştir.[209] Bizim de katıldığımız bir görüşe göre "*zorlamaya varmayacak derecede*" etkilemeye çalışmasının özgür iradenin sakatlanması anlamına gelmeyeceği, aksi yöndeki yorumun ticaret hayatına ket vuracağı ifade edilmiştir. [210] Buna göre örneğin bir ticari kuruluşun üyelik kartını alarak, ek indirimlerden ve fırsatlardan faydalanacak kişi bakımından artık bu kişinin özgür iradesinin sakatlandığı söylenemeyecektir. Nitekim bu halde kişi söz konusu hizmete bahsi geçen üyelik kartını almadan da ulaşabilecekken, bu üyelik kartını alarak yani kişisel verilerinin işlenmesine rıza göstererek, ek imkanlardan faydalanmaktadır. Diğer yandan Kişisel Verileri Koruma Kurulu tarafından özellikle taraflar arasında bir hiyerarşinin söz konusu olduğu ilişkilerde, örneği işçi ve işveren ilişkisinde, işçinin özgür iradesinin olup olmadığı hususunun dikkatli şekilde incelenmesi gerektiği ifade edilmiştir. [211] Yani Kurul bu kararı ile taraflar arasındaki ilişkinin türü dikkate alınarak, her olay bazında, özgür irade bakımından yeni bir değerlendirme yapılması gerektiğini ifade etmiştir.

Kişisel Verileri Koruma Kurulu da ilgili kişilerin açık rızaları olmaksızın, e-posta adreslerine, SMS veya çağrı ile cep telefonlarına reklam bildirimleri gönderilmesi konusunda vermiş olduğu ilke kararında, ilgili kişilerin açık rızaları bulunmaksızın kişisel verileri kullanan ya da bu verileri işleyenlerin söz konusu veri işleme faaliyetlerini 6698 sayılı Kişisel Verilerin Korunması Kanunu'nda yer alan 15.madde gereğince derhal durdurmaları gerektiğini belirtmiş aksi takdirde veri sorumluları hakkında Cumhuriyet Başsavcılığına bildirimde bulunulacağını ifade etmiştir. [212] Görüldüğü üzere açık rıza, kişisel verilerin hukuka uygun şekilde işlenmesi bakımından vazgeçilmez bir unsur olup, kişinin açık rızası olmadan

---

[208] Dülger, **Kişisel Verilerin Korunması Hukuku**, s. 25

[209] Murat Volkan Dülger, **KVKK Uygulamasında ve Uyum Sürecinde Ortaya Çıkan Soru ve Sorunlar**,s.2 (Çevrimiçi)https://www.academia.edu/37979285/KVKK_Uygulamas%C4%B1nda_ve_Uyum_S%C3%BCrecinde_Ortaya_%C3%87%C4%B1kan_Soru_ve_Sorunlar (Erişim Tarihi: 30.11.2018).
Dülger, kişisel veri sahibi kişisel verilerinin işlenmesine açık rıza vermesi koşuluyla ekstra imkanlardan yararlandırılıyorsa bu durumun açık rızayı etkilemeyeceğini, zira burada kişinin istediği temel hizmeti alabildiğini yalnızca ek imkanlardan ve fırsatlardan yararlandırılmadığını belirtmiştir.

[210]Dülger, **Kişisel Verilerin Korunması Hukuku**, s. 25

[211] Kişisel Verileri Koruma Kurulu, **Açık Rıza**, s.6

[212] Kişisel Verileri Koruma Kurulu tarafından verilen 16/10/2018 Tarih ve 2018/119 Sayılı İlke Kararı için bkz. (Çevrimiçi) https://kvkk.gov.tr/Icerik/5299/2018-119 (Erişim Tarihi: 24.10.218)

verilerinin işlenmesi halinde veri sorumluları hem hukuki hem de cezai anlamda sorumlu olacaklardır.

Diğer yandan maddenin ikinci fıkrasında kişinin açık rızası olmaksızın kişisel verilerin işlenebileceği hallerden bahsedilmiştir. Bu haller şu şekilde sıralanabilecektir: Kişisel verilerin işlenmesinin kanunlardan doğan yükümlülüklerden kaynaklanması, somut olayın koşulları neticesinde kişinin açık rızasını açıklayamaması ya da bir kişinin açık rızasının hukuki bir geçerlilik taşımadığı durumlarda bu kişilerin ya da bir başka bir kişinin hayatını korumak amacıyla kişisel veri işlemenin zorunlu olması, bir sözleşmenin vuku bulması neticesinde tarafların verilerinin işlenmesinin gerekmesi, veri sorumlusunun yükümlülükleri gereği verileri işlemesinin gerekmesi, bir kişinin bizzat kendi rızası ile aleni hale getirdiği verilerinin işlenmesi, bir hakkın kullanılması veya korunması ya da kurulması için veri işlemenin gerekli olması, bireyin temel hak ve özgürlükleri sınır olmak üzere veri sorumlusunun çıkarları için verileri işlemenin kaçınılmaz olması durumlarında bireylerin açık rızası aranmaksızın kişisel veriler işlenebilecektir.

Doktrinde bu hallerin bulunması halinde yine de kişinin açık rızasının alınmasının hukuka uygun olup olmadığına ilişkin olarak, Kişisel Verilerin Korunması Kurulu'nun bu halde kişinin aynı zamanda açık rızasının alınmasının hukuka aykırı olduğuna işaret ettiği belirtilmiştir. [213] Bu halde açık rızanın olduğu hallerde açık rıza bir hukuka uygunluk nedeni olacak ve ancak istisnai hallerin varlığında ayrıca açık rıza alınmayacak aksi halde bu durum hukuka aykırı olaraktır.

---

[213] Murat Volkan Dülger, **Kişisel Verileri Koruma Kurulu'nun 20.4.2018 Tarihinde Yayınlamış Olduğu Karar Özetlerine İlişkin Değerlendirme**, (Çevrimiçi) https://www.hukukihaber.net/kisisel-verileri-koruma-kurulunun-2042018-tarihinde-yayinlamis-oldugu-karar-ozetlerine-iliskin-degerlendirme-makale,5857.html (Erişim Tarihi:10.01.2019)
Dülger bu yazısında "*Ancak bu durumun hukuka aykırılık oluşturup oluşturmadığı belirsizdi. Yine Kurulun bu sorularımıza karşı yaptığı açıklamaya göre; istisna hallerinin varlığı halinde açık rızanın alınması ilgili kişiyi yanıltacak ve yanlış yönlendirecek nitelikte olduğundan; veri sorumlusu açısından Kanun ile belirtilen veri işlemeye yönelik istisna hallerinden herhangi birinin var olması halinde açık rıza alınması yalnızca gereksiz değil; yasak ve hukuka aykırıdır. Zira böyle bir durumda ilgili kişi nezdinde, açık rızasını geri aldığı takdirde veri sorumlusunun veri işleme faaliyetine son vermesi gerektiği algısı oluşmaktadır. Oysa veri sorumlusu Kanun ile kendisine getirilen yükümlülükleri yerine getirebilmek için söz konusu veri işleme faaliyetine devam etmelidir. Bu nedenle de istisna halinin varlığı halinde; veri işleme faaliyeti veri sorumlusu tarafından bu istisnaya dayandırılacak ve ilgili kişiden açık rıza alınamayacaktır "* şeklinde görüş bildirmiştir.

Konuyla ilgili olarak Kişisel Verileri Koruma Kurulu tarafından bir karar verilmiş ve kararda ilgili duruma atıf yapılmıştır. Buna göre: *"Veri sorumlusu tarafından Kanunun 5 inci maddesinin (2) numaralı fıkrasının (c) bendi kapsamında sözleşmenin taraflarına ait kişisel veri işlenmesi durumunda ayrıca açık rıza alması ve de açık rızayı üyeliğin ve hizmetin dolayısıyla sözleşmenin bir koşulu olarak dayatmasının; diğer kişisel veri işleme şartlarının varlığı durumunda açık rıza alınmasının ilgili kişinin yanıltılması ve yanlış yönlendirilmesi dolayısıyla veri sorumlusunca hakkın kötüye kullanılması anlamına geleceği, ayrıca hizmetin açık rıza şartına bağlanmış olmasının açık rızayı sakatlayacağı dikkate alındığında, bu durumun Kanunun 4 üncü maddesinde yer alan hukuka ve dürüstlük kurallarına uygun olma ve işlenme amacı ile bağlı, sınırlı ve ölçülü olma ilkelerine aykırılık teşkil etmesi nedeniyle, Kurul tarafından Kanunun 12 nci maddenin (1) numaralı fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri alma yükümlülüğünü yerine getirmeyen veri sorumlusu hakkında Kanunun 18 inci maddesi uyarınca idari yaptırım uygulanmasına karar verilmiştir."* şeklinde görüş beyan edilmiştir. Görüldüğü üzere kurul açıkça kanundan doğan diğer kişisel veri işleme şartları varken, kişiden açık rıza alınmasını kişinin yanlış yönlendirilmesi olarak yorumlamış ve bu durumun hukuka aykırılık teşkil edeceğini ifade etmiştir. [214] Zira bu halde kişide kişisel verilerinin kendi onayı ve rızası dahilinde işlendiğini, gerekirse rızasını geri alma hakkını kullanabileceğini düşünecek[215] ve fakat bu durum gerçeklik teşkil etmeyeceğinden kişi yanlış bilgilendirilmiş olacaktır.

Ayrıca son olarak açık rızanın geri alınıp alınamayacağı hususunda Kişisel Verilerin Koruma Kurulu tarafından "*kişiye sıkı sıkıya bağlı bir hak"*[216] olarak tanımlanan açık rızanın da bu sebeple geri de alınabileceği ifade edilmiştir. Elbette geri alma talebinin iletildiği andan önceki tüm işlemler, açık rıza karşılığında gerçekleştirildiğinden geri alma talebi, kendinden önceki kişisel işlemleri hukuka aykırı hale getirmeyecektir ve ileriye dönük olarak etkili olacaktır.

---

[214] Açık rızanın hizmet şartına bağlanması başlıklı karar özeti için bakınız. (Çevrimiçi) https://www.kvkk.gov.tr/Icerik/4214/Kurul-Kararlari (Erişim Tarihi:21.03.2019)

[215] Dülger, **Kişisel Verilerin Korunması Hukuku**, s.28

[216] İlgili açıklama için bkz. Açık Rıza Alırken Dikkat Edilecek Hususlar (Çevrimiçi) https://www.kvkk.gov.tr/Icerik/2037/Acik-Riza-Alirken-Dikkat-Edilecek-Hususlar (Erişim Tarihi:24.03.2019)

Görüldüğü üzere açık rıza, belirlenmiş bir konuyla ilgili, kişinin bilgilendirilmesi üzerine verilmiş ve yine kişinin özgürce vermesi gereken bir rıza olup, bir somut olayda açık rızanın bulunup bulunmadığının dikkatle incelenmesi son derece önemlidir. Uygulamada verilen kurul kararları arttıkça konunun daha da netleşeceği kanaatindeyiz.

c. Kişisel Verilerin İşlenmesi

Kişisel verilerin işlenmesi, Kişisel Verilerin Korunması Kanunu kapsamında otomatik veya kısmen otomatik yollarla işlenen kişisel verilerin ya da otomatik yöntemlerle olmasa bile bir veri kayıt sistemine dahil şekilde bulunan kişisel verilerin kaydı, depo edilmesi, muhafazası, değişiklik yapılması, revize edilmesi, aktarılması, açıklanması, devir alınması, elde edilebilecek duruma getirilmesi, kullanılmasının, sınıflandırılması ya da kullanımın engellenmesi gibi her çeşit işlem olarak ifade edilmiştir.

Görüldüğü üzere kanun kapsamında kişisel verilerin işlenmesi kapsamında kişisel verilerin kaydı, depo edilmesi, muhafazası, değişiklik yapılması, revize edilmesi, aktarılması, açıklanması, devir alınması, elde edilebilecek duruma getirilmesi, kullanılması, sınıflandırılması ya da kullanımın engellenmesi gibi işlemler sayılmıştır. Bu noktada belirtmek gerekir ki kanunun gerekçesine baktığımızda, gerekçenin lafzından sayılan bu işlemlerin sınırlı olarak sayılmadığını anlamaktayız. Kanun gerekçesinde bir kişisel verinin işlenmesinin sadece bu verinin işlenmesini değil, kişisel veri elde edildikten sonra bu veri üzerinde yapılan her türlü işlemi ifade etmektedir.[217] Bu ifadeden anlaşılabileceği üzere başkasının kişisel verisi üzerinde yapılacak her türlü işlem[218], kişisel verilerin işlenmesi kapsamında sayılabilecektir.

Diğer yandan ilgili tanıma baktığımızda kişisel verilerin işlenmesi işleminin bu kanun kapsamında sayılabilmesi için ayrıca söz konusu kişisel verilerin kısmen veya tamamen otomatik sistemler ile ya da bir otomatik sistem ile işlenmemesine rağmen herhangi bir veri kayıt sistemine dahil olan kişisel verilerin işlenmesi gerekmektedir. Dolayısıyla bunun dışında kalan, örneğin veri kayıt sistemine dahil olmayan kişisel

---

[217] İlgili gerekçe metni için bakınız. (Çevrimiçi) https://www.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf (Erişim Tarihi:22.03.2019)

[218] Küzeci, **Kişisel Verilerin Korunması**, yeni, s. 327

verilerin otomatik olmayan yöntemlerle[219] işlenmesi gibi, her türlü işlem bu kanun kapsamı dışında kalacaktır.

d. İlgili kişi

Kişisel Verilerin Korunması Kanunu'nun 3. Maddesinde ilgili kişi kişisel verileri işlem gören gerçek kişi olarak tanımlanmıştır. Görüldüğü üzere bu kanun kapsamında kişisel verileri korunan gerçek kişiler, bu kanun kapsamındaki ilgili kişi ifadesini tanımlamaktadır. Kanunun söz konusu düzenlemesinin uluslararası düzenlemeler ile uyumlu olduğunu, Avrupa Birliği Genel Veri Koruma Tüzüğü de dahil olmak üzere uluslararası düzenlemelerin hemen hepsinde yalnızca gerçek kişilere ait verilerin koruma kapsamına alındığını ifade etmek isteriz. Bu noktada Kişisel Verilerin Korunması Kanunu'nun taslak metninde her ne kadar tüzel kişiler de bu kanun kapsamına dahil edilmişlerde de daha sonra uluslararası düzenlemelere uyumlu olması açısından tüzel kişiler kanun kapsamından çıkarılarak yalnızca gerçek kişiler kanunun koruma kapsamında bırakılmıştır.[220] Yukarıda kişisel veri başlığının altında hem gerçek kişi kavramından hem de kişisel veri kavramından ayrıntılı olarak bahsedildiğinden burada tekrar olmaması açısından ilgili açıklamalarımıza atıf yapmakla yetiniyoruz.

e. Veri Sorumlusu ve Veri İşleyen

Veri sorumlusu kanunun 3. maddesinde bir kişisel veririnin neden işlendiğini, hangi araçlar ile işleneceğini belirleyen ve veri kayıt sistemi dediğimiz sistemin oluşturulmasından ve idaresinden sorumlu olan gerçek veya tüzel kişi olarak tanımlanmıştır. Veri sorumlusu kavramı, hukukumuza Kişisel Verilerin Korunması Kanunu ile giren kavramlardan biridir. Esasen uluslararası düzenlemelerde, örneğin Avrupa Birliği Genel Veri Koruma Tüzüğü kapsamında da veri sorumlusu ve veri işleyen kavramlarına yer verilmiştir.[221] Burada dikkat çekici hususlardan biri veri sorumlusu olarak yalnızca gerçek kişilerin değil tüzel kişilerin de belirtilmiş olmasıdır. Buna göre gerçek kişilerin kişisel verilerini işleyen bir başka gerçek kişi veri sorumlusu olabileceği gibi, bu verileri işleyen tüzel kişiler de yani bir kurum ya da

---

[219] Dülger, **Kişisel Verilerin Korunması Hukuku**, s.16
[220] Küzeci, **Kişisel Verilerin Korunması**, s.324
[221] Bu konuda ayrıntılı bilgi için çalışmamızın Avrupa Birliği Veri Koruma Tüzüğü'nü işlediğimiz bölümüne bakınız.

kuruluş da veri sorumlusu sıfatına sahip olabilecektir. Veri sorumlusu, kişisel verileri işleme tabi tutulan gerçek kişilerin bilgi sahibi olabilmeleri, haklarını arayabilmeleri ve karşılarında sorumlu birini bulabilmeleri açısından oldukça önemlidir.

Doktrinde veri sorumlusunun kim olduğunun tespit edilebilmesi için bazı kriterler sayılmıştır. Buna göre "Kişisel verilerin işlenip işlenmeyeceği ile işleme amacının ne olduğu, hangi kişisel veri türlerinin işleneceği, kimlerin kişisel verilerinin işlenmesinin gerekli olduğu, kişisel verilerin üçüncü kişilere ne amaçla aktarılacağı, kişisel verilere kimlerin erişim yetkisinin olduğu, kişisel verilerin saklanması için gerekli/yasal sürenin ne olduğu, saklama süresi sona erdikten sonra erdikten sonra izlenecek yöntemin ne olması gerektiği (silme-yok etme-anonimleştirme)"[222] konuları konusunda karar verme yetkisine sahip kişilerin veri sorumlusu olacağı ifade edilmiştir. Yukarıda da belirttiğimiz üzere veri sorumlusu hem gerçek bir kişi hem de tüzel kişi olabilecektir.

Kanunu'nun 10. maddesinde ise veri sorumlusunun aydınlatma yükümlülüğüne ilişkin hususlar düzenlemiştir. Buna göre veri sorumlusu kişisel verilerin elde edildiği ilk andan itibaren veri sahibi gerçek kişilere kendisinin ve mümkünse temsilcisinin kimliğini, bu verileri hangi amaçlarla işleyeceğini, bu verileri 3. Kişilere aktarıp aktarmayacağı bilgisini ve aktaracak ise hangi amaçlarla sınırlı olarak aktaracağını, kişisel verileri hangi araçlarla ve sebeplerle toplayacağını ve kanununda yer verilen diğer haklarını bildirmekle yükümlüdür.

Veri sorumlularının aydınlatma yükümlülüğünün yerine getirilmesi konusunda 10 Mart 2018 Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ yayınlanmıştır.[223] Bu tebliğe göre, Tebliğ'in 4. maddesi aydınlatma yükümlülüğü yerine getirilirken, veri sahibine veri sorumlusunun ve varsa temsilcisinin kimliği, kişisel verilerin hangi amaçla işleneceği, kişisel verilerin aktarılabileceği kişiler ve amaçlar, kişisel veri toplamanın yöntemi ve hukuki sebebi ile ilgili kişinin kanun kapsamında sayılan tüm hakları bildirilecektir.

Tebliğ kapsamında yer verilen hususlardan biri de veri sorumlusunun aydınlatma yükümlülüğünü yerine getirirken, aydınlatma yükümlülüğünün her durumda yerine getirilmesi, veri işleme amacının değişmesi halinde aydınlatma

[222] Dülger, **Kişisel Verilerin Korunması Hukuku**, s.18

yükümlülüğünün de yenilenmesi, sicile sunulan bilgiler ile bireye sunan bilgilerin aynı olması, aydınlatma yükümlülüğünün yapıldığının ispatının veri sorumlusuna ait olması, veriler açık rızaya dayalı olarak işleniyorsa aydınlatma ve açık rıza işlemlerinin ayrı ayrı yapılması, aydınlatma beyanının açık ve net olması, açık, anlaşılır ve sade olması, kanun hangi maddesine dayanılarak verilerin işlendiğinin belirtilmesi, kişisel verilerin kimlere ve hangi amaçla aktarıldığının belirtilmesi, verilerin elde edilme yöntemlerinin bildirilmesi, veri sorumlusunun yükümlülükleri arasındadır. Burada kanımızca dikkat edilecek hususlardan biri de Tebliğ'in 5.maddesinin 'g' fıkrasında ifade edildiği üzere olası durumlar ya da ortaya çıkabilecek sair sebepler ile kişisel verilerin işlenebileceğine ilişkin herhangi bir ifade de bulunulmamalıdır. Nitekim kişisel verilerin hangi amaçlar ile işleneceği aydınlatma metninde açık ve net bir şekilde belirtilmeli, buna yeni amaçlar eklenmesi ya da bu amaçların değişmesi halinde aydınlatma yükümlülüğünün yenilenmesi gerekmektedir.

Kişisel verilerin veri sahibinin kendisinden elde edilmediği durumlarda ise kişilerin nasıl aktarılacağı sorusu akıllara gelmektedir. Tebliğ'de bu konuya da açıklık getirilmiş ve kişisel verilerin 3. kişiden elde edilmesi halinde makul sürede kişisel verilerinin işlendiğine ilişkin veri sahibine aydınlatma yükümlülüğünün gerçekleştirilmesi gerektiği ifade edilmiştir.

Veri sorumlusunun kişisel verilerin güvenliği konusunda alması gereken önlemler ve bu konudaki yükümlülüklerine ilişkin düzenleme ise kanunun 12. maddesinde yapılmıştır. Buna göre bir veri sorumlusu kişisel verilerin her daim hukuk kurallarına uygun şekilde işlenmesini sağlamak, bu verilere ancak erişim yetkisi bulunan kişilerin erişimine açmak ve yetkisiz kişileri bu erişimden men etmek[224],

[224] Bir hazır giyim firmasının internet sitesi üzerinden üyelik bilgileri ile alışveriş yapan kişinin kişisel bilgilerinin şirkete ait bu internet sitesinden alışveriş yapan diğer kişilere erişilebilir hale gelmesi sebebiyle yapılan Kurul şikayetinde, Kişisel Verileri Koruma Kurulu tarafından 2018/91 sayılı karar verilmiştir. Bu kararda şikâyette bulunan kişiye ait kişisel verilerin kişinin alışverişinin gerçekleştirilmesi için girildiği ve fakat bu bilgilerin bir şekilde diğer müşterilerin görebileceği bir hale gelmesi neticesinde yapılan şikâyette, şirket yetkilileri bu sonucun sistemden kaynaklı bir hatadan ötürü oluştuğunu ve bu hatadan olayın vuku bulması ile birlikte haberdar olduklarını ve akabinde gerekli önlemleri aldıklarını ifade etmişlerdir. Ancak olayın Kurul'a intikali ile kurul tarafından yapılan inceleme neticesinde şirket yetkililerinin işlenen kişisel verilerin korunması için gerekli güvenlik önlemlerini almadığı sonucuna varılmış ve şirket hakkında Kurul tarafından idari para cezasına hükmedilmiştir. Ayrıca yine Kurul tarafından şikayetçiye ait kişisel verilerin tüm şirket sistemlerinden silinmesi ya da erişilemez hale getirilmesi ya da bu veriler aktarıldı ise aktarılan verilerin de silinmesi ve bu işlemlerin uygulandığına dair şikayetçinin belgelerle bilgilendirilmesi yönünde karar verilmiştir. Kişisel Verileri Koruma Kurulu tarafından verilen 26/07/2018 Tarih ve 2018/91 Sayılı Karar

kişisel verilerin korunmasını sağlayabilmek için gerekli güvenliği oluşturmak ve bunun için tüm tedbirleri almak zorundadır. Veri sorumlusunun alacağı bu tedbirler idari tedbirler olabileceği gibi teknik tedbirler de olabilir. Yine kanunda veri sorumlusunun yukarıda belirtmiş olduğumuz güvenlik tedbirlerinin alınması konusunda veri işleyen ile birlikte sorumlu olacağı, veri sorumlusunun bağlı bulunduğu tüzel kişilik içerisinde kanunun gerekliliklerinin yerine getirilmesini sağlamak için tüm denetimleri gerçekleştirmek zorunda olduğu, kişisel verileri yalnızca işledikleri amaç için kullanacağı ve başkalarına açıklayamayacağı, kişisel verilerin yetkisiz 3. kişiler tarafından ele geçirilmesi halinde verileri ele geçirilen kişiyi bilgilendireceği de düzenlenmiştir.

Kanunun 13. Maddesinde ise veri sorumlusuna başvuru hususu düzenlenmiştir. Bu maddeye göre kişisel verileri işlenen kişisel veri sahipleri, konuya ilişkin taleplerini veri sorumlularına yazılı olarak iletebilirler. Veri sorumluları ise kendilerine iletilen talepleri değerlendirerek azami 30 gün içerisinde talepleri neticelendirirler. Veri sorumlusu bu talebi kabul veya gerekçeli olarak reddedilir. Ayrıca talebin yerine getirilmesi için bir maliyet söz konusu olacak ise, ücret talep sahibinden istenebilecektir. Diğer yandan 14. maddede ise bu talebin reddi halinde talep sahiplerinin kurula şikâyette bulunma hakları olduğu düzenlenmiştir.

Veri sorumlusuna başvuru usul ve esaslarına ilişkin hususlar 10 Mart 2018 tarihinde yürürlüğe giren tebliğde düzenlenmiştir. Tebliğ'e göre kişisel verileri işlenen gerçek kişiler veri sorumlusuna başvurma hakkına sahiptirler. Tebliğ'e göre veri sahipleri bu başvuruları Türkçe dilinde yapmakla yükümlüdürler. Başvuru sahibi, kanundan kaynaklı isteklerini, yazılı şekilde veya KEP yani kayıtlı elektronik posta adresi, mobil imza, güvenli elektronik imza ya da başvuru sahibinin kayıtlı elektronik posta adresini kullanmak suretiyle veri sorumlusuna iletebilecektir.

Veri sorumlusuna yapılan başvuru neticesinde, veri sorumlusu ya gerekçesini açıklamak suretiyle reddeder ya da kabul eder. Veri sorumlusu talebe ilişkin olarak kararını asgari sürede ve azami otuz gün içinde hiçbir ücret talep etmeden sonuçlandırmakla yükümlüdür. Ancak talebin karşılanması için ücret gerekmesi durumunda bu ücret başvuru sahibinden talep edilebilecektir.

Konuya ilişkin olarak Kişisel Verileri Koruma Kurulu tarafından bir karar verilmiştir. Karar veri sorumlusuna başvuru yolunu tüketen veri sahiplerinin Kurula

şikâyette bulunmaları sürecinde kanunda yer alan sürelerin farklı yorumlanmasına ilişkindir. Kurul söz konusu kararda:

"Kanunun 14. maddesinin (1) numaralı fıkrası uyarınca, ilgili kişi tarafından yapılan başvuruya veri sorumlusunca 30 gün içinde bir cevap verilmesi halinde ilgili kişinin veri sorumlusunun cevabını müteakip 30 gün içerisinde şikâyette bulunabileceği, bu itibarla söz konusu hallerde ilgili kişinin veri sorumlusuna başvurduğu tarihten itibaren 60 günlük süresinin bulunmadığı,

İlgili kişi tarafından yapılan başvuruya veri sorumlusunca bir cevap verilmediği durumda ise ilgili kişinin veri sorumlusuna başvurduğu tarihten itibaren 60 gün içinde Kurula şikâyette bulunabileceği,

İlgili kişi tarafından yapılan başvuruya veri sorumlusunca Kanunda tanınan 30 günlük süre sonrasında bir cevap verilmesi halinde ilgili kişinin, Kanunda veri sorumlusuna tanınan 30 günlük süre sonrasında verilecek cevabı beklemekle yükümlü olmadığı ve veri sorumlusuna tanınan sürenin dolması ile birlikte Kurula şikâyette bulunabileceği göz önüne alınarak, ilgili kişinin veri sorumlusunun kendisine cevap verdiği tarihten itibaren 30 gün değil, veri sorumlusuna başvurduğu tarihten itibaren 60 gün içinde Kurula şikâyette bulunabileceği" şeklinde görüşünü ifade etmiştir. [225]

Veri sorumlularının tüzel kişi olması halinde, örneğin bir şirketin veri sorumlusu olduğu durumlarda, veri sorumlusu şirket kişisel verileri bizzat işleyebileceği gibi[226], bu verileri işleyecek bazı gerçek ya da tüzel kişiler istihdam edilebilecektir. İşte bahsi geçen bu gerçek ya da tüzel kişiler ise bu kanun kapsamında veri işleyen olarak tanımlanmıştır. Veri işleyen kavramını incelemeden evvel, veri sorumlusunun kendisine bir veri işleyen ataması halinde dahi kişisel verilerin korunması hukuku kapsamındaki yükümlülüklerini taşımaya devam ettiğini ve ilgili yükümlülüklerin veri işleyen tarafından yerine getirilmemesi halinde de sorumluluğun veri sorumlusunda olacağını ifade etmek isteriz.

Kanunun tanımlar başlıklı 3. Maddesinin 'ğ' fıkrasında veri işleyen kavramına yer verilmiş ve veri işleyenin veri sorumlusundan aldığı yetki ile veri sorumlusu adına veri işleyen gerçek kişi ya da tüzel kişi olabileceğini ifade etmiştir.

---

[225] Kişisel Verileri Koruma Kurulunun 24.01.2019 tarih ve 2019/9 sayılı Kararı
[226] Kişisel Verileri Koruma Kurulu, **Veri Sorumlusu ve Veri İşleyen Rehberi**, s. 2

Bu noktada veri işleyen ve veri sorumlusu arasındaki farka bakacak olursak veri işleyen kişinin daha ziyade kişisel veri işlemenin teknik gereklilikleri ile ilgilenmekte olduğunu, veri sorumlusunun ise karar veren konumda olduğunu ifade edebiliriz.[227] Bu durumda veri sorumlusu kişisel verilerin toplanmasına ilişkin olarak hangi araçların, sistemlerin ya da yöntemlerin kullanılacağı, bu verilerin muhafazası için hangi metotların kullanılacağı, kişisel verilerin güvenli şekilde muhafaza edilebilmesi için alınabilecek önlemlerin ayrıntılarını, eğer veriler aktarıma konu edilecekse hangi yöntemler ile aktarılacağını, kişisel verilerin yok edilmesi ya da silinmesi ya da anonim getirilmesi için hangi yöntemlerin uygulanacağı gibi konuları *veri* işleyene bırakılabilecektir. Görüldüğü üzere, yukarıda da belirttiğimiz üzere veri sorumlusu tarafından veri işleyene bırakılacak hususlar teknik hususlardır. Bu noktada veri sorumlusunun bazı hususları veri yetkilisine devri halinde, veri sorumlusunun sorumluluğu devretmediğini, aksine hala tüm sorumluluğun veri sorumlusunda olduğunu bir kere daha vurgulamak isteriz. [228]

Kanunun 16. Maddesinde ise veri sorumluları sicili düzenlenmiştir. Bu maddede kişisel verileri işleyen veri sorumlularının, herhangi bir veri işleme sürecine başlamadan evvel kendilerini veri sorumluları siciline kaydetmekle yükümlüdürler. Elbette Kurul'un bazı veri sorumlularını bu sicile kayıt yükümlülüğünden muaf tutma hakkı bakidir. Buna göre Kurul kişisel verilerin niteliğini ya da sayısını ya da benzeri bazı kriterleri dikkate alarak bu sicile kayıt zorunluluğuna bazı istisnalar düzenleyebilir. Görüldüğü üzere kanun koyucu veri sorumlularının veri sorumluları siciline kaydını zorunlu tutmuş ve ancak belirli durumlarda ise bu zorunluluğun uygulanmayabileceği ifade edilmiştir. Akabinde ise aynı maddenin 5. fıkrasında Veri Sorumluları Siciline ilişkin usul ve esasların yönetmelikle düzenleneceği belirtilmiştir. Bunun üzerine 30 Aralık 2017 tarihinde Veri Sorumluları Sicili Hakkında Yönetmelik yürürlüğe girmiş ve bu yönetmelik[229] kapsamında veri sorumluları siciline ilişkin esaslar düzenlenmiştir. Aşağıda bu sicile ilişkin esaslara da kısaca yer verilmiştir.

---

[227] Kişisel Verileri Koruma Kurulu, **Veri Sorumlusu ve Veri İşleyen Rehberi**, s. 3

[228] Dülger, **Kişisel Verilerin Korunması Hukuku**, s. 21

[229] Kişisel Verilerin Korunması Kanunu çerçevesinde bazı hususların yönetmelik ile yapılacak düzenlenmelere bırakıldığı görülmektedir. Bunlardan bazıları yukarıda konusu kapsamında işlemiş olduğumuz Kişisel Verileri Koruma Kurumuna ilişkin 5 Mayıs 2016 tarihinde yürürlüğe giren Kişisel Verileri Koruma Kurumu Personeli Görevde Yükselme ve Unvan Değişikliği Yönetmeliği ile 26 Nisan 2018 tarihinde yürürlüğe giren Kişisel Verileri Koruma Kurumu Teşkilat Yönetmeliği, Kişisel Verileri Koruma Kurulu ile hizmet birimlerine ilişkin 16 Kasım 2017 tarihinde yürürlüğe giren Kişisel Verileri Koruma Kurulu Çalışma Usul ve Esaslarına Dair Yönetmelik ve Kişisel Verileri Koruma Uzmanlığına ilişkin 9 Şubat 2018 tarihinde yürürlüğe giren Kişisel Verileri Koruma Uzmanlığı Yönetmeliğiydi. Kanun tarafından detayları yönetmelik ile düzenlenmesi öngörülen diğer iki konu ise veri sorumlularına

aa. Veri Sorumluları Sicili

Kişisel Verilerin Korunması Kanunu'nun veri sorumluları sicilini düzenleyen 16. maddesinde veri sorumluları sicili özetle Kişisel Verileri Koruma Kurulu'nun denetiminde aleni olarak tutulan ve sicile kayıt yükümlülüğü olan veri sorumlularının veri işlemeye başlamadan önce kendilerini kayıt ettirecekleri bir sicil olarak ifade edilmiştir. Ayrıca yine kanunun aynı maddesinde veri sorumluları siciline kayıt yükümlülüğünden istisna tutulacak veri sorumlularının kimler olduğuna ise Kişisel Verileri Koruma Kurulu'nun ayrıca karar vereceği belirtilmiştir. Veri sorumluları siciline ilişkin idare, denetim, erişim, başvuru, kayıt yenileme ve silme gibi ayrıntılı esaslar ise Veri Sorumluları Sicili Hakkında Yönetmelikte düzenlenmiştir.

30 Aralık 2017 tarihinde Veri Sorumluları Sicili Hakkında Yönetmelik'in ikinci bölümünde veri sorumluları sicilinin oluşturulması, idaresi, gözetimi ve sicile erişim esasları düzenlenmiştir. Buna göre, genel ilke veri sorumlularının veri işlemeye başlamadan evvel sicile kaydolmak zorunda olmalarıdır. Eğer bir veri sorumlusu Türkiye'de ikamet etmiyor ise bu durumda temsilcisi aracılığı ile sicile kaydolacaktır. Yukarıda da belirttiğimiz üzere sicil kamuya açık bir şekilde tutulmaktadır. Yani herkes bir gerçek ya da tüzel kişinin, eğer sicile kayıt yükümlülüğünden istisna tutulan sorumlular arasında değil ise, sicile kayıtlı olup olmadığını görebilecektir.

bb. Sicilin Oluşturulması, İdaresi, Gözetimi ve Sicile Erişim

İlgili yönetmeliğin 'Sicilin oluşturulması, idaresi ve gözetimi' başlıklı 6. maddesinde veri sorumluları sicilinin yukarıda teşkilat kapsamında bahsetmiş olduğumuz Başkanlık tarafından oluşturulacağı ifade edilmiş ve Başkanlığın sicilin oluşturulması, muhafazası ve idaresi için gerekli olan VERBİS (Veri Sorumluları Sicili Bilgi Sistemi) için tüm idari ve teknik gereklilikleri yerine getireceği ifade edilmiştir. Yine yukarıda bahsettiğimiz üzere Kişisel Verileri Koruma Kurumu çatısı altında hizmet birimleri bulunmakta olup bunlardan birisi de Veri Yönetimi Dairesi Başkanlığı'dır. Bu başkanlık sicilin oluşturulmasından ve idaresi konusunda

---

siciline ilişkin esaslar ile kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesidir. Bu noktada 28 Ekim 2017 tarihinde "Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmelik" ile 30 Aralık 2017 tarihinde yayınlanan "Veri Sorumluları Sicili Hakkında Yönetmelik" yürürlüğe girmiştir.

görevlidir. Diğer yandan sicilin denetimi ise Kişisel Verileri Koruma Kurulu tarafından yapılmaktadır. Kurul bu denetimi, bahsi geçen hizmet birimi tarafından kendisine sunulacak olan faaliyet raporları üzerinden gerçekleştirmektedir.

cc. Kayıt Yükümlülüğünün Başlangıcı, VERBİS'e Girilecek Bilgiler, Kayıt Başvurusu, Kaydın Yenilenmesi ve Silinmesi

Kayıt yükümlülüğünün başlangıcı, VERBİS'e girilecek bilgiler, kayıt başvurusu, kaydın yenilenmesi ve silinmesi konuları, Yönetmelik'in üçüncü bölümünde düzenlenmiştir. Veri sorumlularının kayıt yükümlülüğü kişisel verilerin işlenmesinden evvel başlayacaktır. Yani sicile kayıt yükümlüğü olan tüm veri sorumluları veri işlemeye başlamadan önce veri sorumluları siciline kayıtlarını yapmakla yükümlüdürler. Yukarıda Kurul kararı ile bazı veri sorumlularının veri kayıt siciline kayıt yükümlülüğünden istisna tutulacağını ifade etmiştik. Bu durumda veri siciline kayıt yükümlülüğü olmamasına rağmen daha sonra sicile kayıt yükümlülüğü doğarsa en geç 30 gün içerisinde bu veri sorumluları siciline kaydolacaklardır. Veri sorumlularının teknik, hukuki fiili aksaklıklar neticesinde sicile kayıt yükümlülüklerini yerine getirememeleri durumunda Kurul'da ek süre talep etme hakları bulunmaktadır. Veri sorumlularının, sicile kayıt için ilgili bazı bilgileri VERBİS üzerinden girişini yapacaklarını belirtmiştik. Veri sorumlularının sicile kayıt başvurularında vermeleri gereken bilgiler şu şekilde sayılabilecektir: Kurul tarafından belirlenecek başvuru formunda veri sorumlusunun varsa temsilcisi ve iletişim kişisine ait kimlik ve adres bilgilerine, kişisel verilerin işleme amaçlarına, işlenecek verilerin kategorileri hakkındaki açıklamalara, kişisel verilerin aktarılması ihtimali varsa kimlere ya da kime aktarılabileceği konusundaki bilgilere, kişisel verilerin yurtdışına aktarımı söz konusu olabilecekse bu konu hakkındaki bilgiye, veri güvenliği için alınan tedbirlere ve kişisel verilerin en fazla ne kadar muhafaza edileceğine ilişkin süreye yer verilir. [230]

Yönetmelik çerçevesinde azami sürelerin belirlenmesi de bu konuda önemli hususlardan biridir. Kişisel verilerin muhafaza süresine ilişkin olarak kanunlarda bir süre olması durumunda zaten uygulanacak olan süre kesindir. Ancak kanunlarda belirlenen bir süre olmaması durumunda, kişisel verilerin muhafaza edileceği azami

[230] Veri Sorumluları Sicili Hakkında Yönetmelik'in 9.maddesi

sürenin olacağı konusunda yönetmelikte dikkat edilecek kriterlere yer verilmiştir. Buna göre ilgili süre belirlenirken, faaliyet gösterilen alana ilişkin genel olarak kabul gören süre, ilgili kişiyle kurulan hukuki ilişki sebebiyle kişisel verinin işlenmesini gerektiren süre, hukuka ve dürüstlük kuralları sınırı çerçevesinde veri sorumlusunun meşru menfaati için gerekli süre, verilerin muhafazasının ortaya çıkaracağı tehlike, maddi külfet ve sorumlulukların hukuken devam edeceği süre, veri kategorisinin doğru ve güncel tutulmaya elverişli olup olmadığı, hukuki yükümlülüğü gereği veri sorumlusunun kişisel verileri muhafaza etmekle yükümlü olduğu süre, bir hakkın ileri sürülmesi için belirlenen zamanaşımı süresi dikkate alınacaktır.

Veri Sorumlularının VERBİS'e kayıt başvuruları ise yine yönetmeliğe göre yukarıda yer vermiş olduğumuz bilgilerin VERBİS'e yüklenmesi ile gerçekleştirilmiş olacaktır. Veri sorumlularının, veri sorumluları sicilindeki bilgileri üzerinde değişiklik yapmak istemesi durumunda ise veri sorumluları bu değişiklikleri VERBİS aracılığı ile yedi gün süresince bildirebileceklerdir. Sicil kaydının silinmesi ise yine VERBİS üzerinden yapılacak taleple sağlanacaktır. Veri sorumlusunun sicil kaydının silinmesi talebinin gerçekleştirilmesi için veri sorumlusunun kayıt yükümlülüğünün ortadan kalkmış olması halinde kabul edilecektir. Ancak yönetmelik kapsamında bu noktada önemli bir düzenlemeye yer verilmiştir. Buna göre yönetmeliğin 14. Maddesinin 3. fıkrasına göre, veri sorumlusu kaydını sicilden sildirmiş olsa bile, görev yaptığı süreye ilişkin sorumlulukları ve yükümlülükleri devam edecektir.

dd. Kayıt Yükümlülüğünün İstisnaları

Veri Sorumluları Sicili Yönetmeliği'nin dördüncü bölümünde 'Kayıt Yükümlülüğünün İstisnaları' konusu düzenlenmiştir. Bu düzenlemeye göre, yönetmeliğin 15. Maddesinde kişisel verilerin suç işlenmenin engellenmesi veya soruşturma için gerekli olması halinde, veri sahibi tarafından bizzat kamuya açılmış, aleni hale getirilmiş kişisel verilerin işlenmesi halinde, görevli kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları tarafından kanunun verdiği yetkiye dayanılarak kişisel verilerin işlenmesi halinde, disiplin, soruşturma veya kovuşturması, denetleme için gerekli olması halinde, devletin mali menfaatleri için finansal konulara ilişkin olarak kişisel verilerin işlenmesi halinde veri sorumlularının bu faaliyetlerini sicile kayıt ettirmesi ya da bildirmesi gerekmemektedir.

Veri sorumlularının sicile kayıt istisnasına ilişkin olarak Kurul'un karar verme yetkisi olduğunu daha önce de belirtmiştik. Yasa koyucu, Kurul'un bu kararı verirken tamamen takdir ile hareket etmesini engellemek amacıyla, yönetmeliğin 16. Maddesinde Kurul'un bu kararı verirken dikkate alacağı kriterlere yer vermiştir. Buna göre bu kriterler kişisel verinin özelliği, kişisel verinin miktarı, kişisel verinin işleme amacı, kişisel verinin işlendiği sektör ya da faaliyet alanı, kişisel verinin aktarılma ihtimali, kişisel verinin kanunlardan kaynaklı olarak işleniyor olması, kişisel verilerin saklama süresi, veri kategorileri ya da veri sahipleri şeklinde ifade edilmiştir.[231] Nitekim Kişisel Verileri Koruma Kurulu da konuya ilişkin olarak bu kriterleri dikkate alarak bazı kararlar almıştır.

Kişisel Verileri Koruma Kurulu tarafından verilen konuya ilişkin 02.04.2018 tarih ve 2018/32 sayılı kararda hangi veri sorumlusunun veri sorumluları siciline kayıt yükümlülüğünden istisna tutulduğunu belirtmiş ve hemen akabinde vermiş olduğu 28/06/2018 Tarihli ve 2018/68 sayılı kararı ve 18.08.2018 tarih ve 2018/87 sayılı karar ile de sicilden istisna tutulacak veri sorumlularına ek yapılmıştır.

Kişisel Verileri Koruma Kurulu tarafından verilen 02.04.2018 tarih ve 2018/32 sayılı ilk kararda bir veri kayıt sisteminin parçası olmak şartıyla sadece otomatik olmayan yöntemlere kişisel veri işleyenler, noterlik kanununa göre faaliyet gösteren noterler, dernekler, vakıflar, sendikalar kapsamında faaliyet gösterdikleri alanla sınırlı olarak ve yalnızca kendi çalışanlarına, üyelerine ya da bağışçılarına yönelik kişisel veri işleyenler, siyasi partiler, avukatlar, serbest muhasebeci ve yeminli mali müşavirlerin veri sorumluları siciline kayıt yükümlülüğüne istisna olarak sayılmışlardır.[232]

Kişisel Verileri Koruma Kurulu'nun 28/06/2018 Tarihli ve 2018/68 sayılı kararında 4458 sayılı Gümrük Kanunu gereğince görev yapan gümrük müşavirleri ile yetkilendirilmiş gümrük müşavirleri için veri sorumluları siciline kayıt yükümlülüğüne istisna getirilmesine karar verilmiştir.

[231] Veri Sorumluları Sicili Hakkında Yönetmelik'in 16. maddesi.
[232] Kişisel Verilerin Koruma Kurumu'nun sayılı 02.04.2018 tarih ve 2018/32 sayılı kararı

Kişisel Verilerin Koruma Kurumu'nun 19.07.2018 tarih ve 2018/87 sayılı kararında ise çalışan sayısı yıllık olarak elliden az ve yıllık mali bilanço toplamı 25 milyon TL'den az olan, veri sorumlularından esas faaliyet konusu özel nitelikli kişisel veri işleme olmayanların da bu kayıt sistemine kayıt yükümlülüğünün olmadığı yönünde karar verilmiştir.

f. Veri Kayıt Sistemi

Veri kayıt sistemi kanunun tanımlar başlıklı 3. Maddesinin 'h' fıkrasında bazı kriterler göz önünde bulundurulmak suretiyle kişisel verilerin işlendiği sistem olarak tanımlanmıştır. Kişisel verilerin işlenmesi başlığında ifade ettiğimiz üzere kişisel verilerin otomatik olmayan yöntemler ile işlenmesi durumunda ancak veri kayıt sisteminin parçası olması halinde Kişisel Verilerin Korunması Kanunu kapsamında sayılacaktır. Kişisel Verileri Korumu Kurulu veri kayıt sisteminin elektronik ya da fiziki ortamda oluşturulabileceğini ifade etmiştir. Burada önemli olan kaydedilen verilerin belirli kriterlere uygun şekilde ve sistemli biçimde kaydedilmesidir. Aksi halde hiçbir kriter olmaksızın bir araya gelmiş verilerin bir veri kayıt sisteminin parçası olduğu söylenemeyecektir.[233]

B. KVKK'DA DÜZENLENEN KİŞİSEL VERİLERİN İŞLENMESİNE İLİŞKİN TEMEL İLKELER

1. Kişisel Verilerin Hukuka ve Dürüstlük Kurallarına Uygun Olarak İşlenmesi

Kişisel Verilerin Korunması Kanunu'nda yer alan 4. Madde kapsamında kişisel veriler işlenirken dikkate alınması zorunlu ilkeler düzenlenmiştir. Bu ilkelerin ilki, kişisel veriler işlenirken bu verilerin hukuka ve dürüstlük kurallarına uygun şekilde işlenmesidir. Bu ilke diğer ilkelerin de temeli niteliğinde ve en önemlisidir. Buna göre söz konusu ilkeyi hukuka uygunluk ve dürüstlük kuralına uygunluk olarak iki bölümde inceleyebiliriz. Hukuka uygun olmak yalnızca kişisel verilerin korunması hukuku

[233] Kişisel Verileri Koruma Kurumu, **100 soruda Kişisel Verilerin Korunması Kanunu**, s. 25

kapsamındaki mevzuata değil, genel olarak tüm hukuk kurallarına ve evrensel hukuk normlarına uygunluk olarak yorumlanmalıdır.[234]

Dürüstlük kurallarına uygunluk denildiğinde ise Medeni Kanunu'nun 2. maddesindeki dürüstlük kuralarına bakmamız gerekecektir. Buna göre dürüstlük kuralı ile ilgili olarak madde metninde tüm bireylerin hukuk düzeninden doğan haklarını kullanırken ya da bu hukuk düzenin kendilerine yükledikleri yükümlülükleri yerine getirirken bu eylem ya da işlemleri dürüstlük kuralı doğrultusunda yapacakları ve aksi yönde bir biçimde bir hakkın kötüye kullanılmasının hukuk tarafından korunmayacağı ifade edilmiştir.

Bu halde kişisel veriler işlenirken, veri sorumluları ve veri işleyenler dürüstlük kuralına uyarak bu verileri işlemekle yükümlü olacaklardır. Ayrıca yine bu alanda dürüstlük kuralına uygunluk veri sorumlularının ya da veri işleyenlerin, bu verilerin işlenmesi konusunda kendilerine hukuka uygun şekilde rıza gösteren kişilerin öngörebilecekleri şekilde hareket etmeleri ya da bu verileri amacına uygun olarak ve yalnızca amacı gerçekleştirecek miktarda işlemeleri[235] olarak da yorumlanabileceklerdir. Dürüstlük kuralına uygunluk aynı zamanda veri işlemenin ilgili kişi için *şeffaf* olması durumunu da kapsamaktadır.[236] Bu durumda kişisel veriler her ne kadar kanun normlarına uygun şekilde işlense bile dürüstlük kuralına aykırılık bulunması halinde, veri işlemenin hukuka uygun olduğu söylenemeyecektir.[237]

2. Kişisel Verilerin Gerektiğinde Güncellenmesi ve Doğru Olması

Kişisel verilerin işlenmesine ilişkin olarak uyulması gereken ikinci ilke ise, doğru ve gerektiğinde güncel olma ilkesidir. Bu ilke işlenen kişisel verilerin doğru işlenmesi ve gerektiğinde ya da talep edilmesi halinde güncellenmesine ilişkindir. Bu ilke kişisel verilerin işlenmesine ilişkin uluslararası düzenlemelerde veri sahiplerine tanınan verilerine erişme ve düzeltme hakları ile uyumlu olduğu kadar işbu kanunun

---

[234] Dülger, **Kişisel Verilerin Korunması Hukuku**, s. 109
[235] Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler**, s.3
[236] Küzeci, **Kişisel Verilerin Korunması**,2018, s.207
[237] Konuyla ilgili verilen bir örnekte kişisel verilerin kanuna uygun şekilde işlenmesi durumunda, bu verilere erişim konusunda belli kişilere yetki verilmesi gerekirken, kişi sayısının amacını aşan şekilde fazla olması durumunda burada veri işlemenin dürüstlük kuralına uygun olmadığı belirtilmiştir. Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler**, s.4

11. maddesinde düzenlenen kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme hakkı ile de paraleldir.

Nitekim Kişisel Verilerin Korunması Kanunun 11. maddesinin 'd' fıkrasında veri sahiplerine kişisel verilerinin yanlış ya da eksik şekilde işlendiğini düşünmeleri ya da tespit etmeleri halinde bu verilerin düzeltilmesini talep edebilme hakkı verilmiştir. Avrupa Birliği Veri Koruma Tüzüğü'nün 13. maddesinde de veri sahiplerine gerektiğinde verilerinin güncellenmesi ya da düzeltilmesi konusunda hak sahibi olduklarının bilgilendirilmesi yükümlülüğünün veri sorumlularında olduğu düzenlenmiştir. Görüldüğü üzere Tüzük kapsamında da veri sahiplerine gerektiğinde verilerini düzeltmesini talep etme hakkı düzenlenmiştir.

Kişisel verileri işlenen bireylerin bu verilerin doğru şekilde işlenmesi, güncelliğini kaybetmesi halinde ise güncellenmesini talep etme hakkı bireyler için hem de veri sorumlusu için oldukça önemlidir. Özelikle kişisel verilerin bireylerin sağlık verisi gibi hassas verilerine ilişkin olması halinde, bu verilerin doğru ve güncel olması bireyler açısından son derece önemlidir. Zira aksi halde veri sahibinin bu durumdan maddi veya manevi zarar görme ihtimali bulunmakta olup, özellikle veri sorumlusunun *aktif özen yükümlülüğünün*[238] bulunduğu veri sahibinin sonuçtan etkilendiği durumlarda veri sorumlusunun verileri güncel ve doğru tutması oldukça önemlidir.

3. Belirli, Açık ve Meşru Amaçlara Yönelik İşlenme

Bu ilke kapsamında kişisel verilerin işlenmesi verilerin işlenme amacının belirli olmasını ve kişisel verilerin meşru amaçlarla işlenmesini gerektirmektedir. Kişisel veriler işlenirken, bu veriler ya bireylerin açık rızası dahilinde işlenebilecek ya da kanunda belirtilen istisna hallerde açık rıza aranmaksızın işlenebilecektir.

Bu bakımdan 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. İşte bu noktada bireylere açıklanan kişisel verilerin işleme amaçları belirli ve açık olmalıdır. Kişisel verilerin hangi amaçlarla, hangi kapsamda, hangi sınırlarla ve hangi süreyle işleneceği

---

[238] Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler**, s.6

bireylere açık bir şekilde iletilmelidir. Kişisel Verileri Koruma Kurumu tarafından konuyla ilgili olarak, kişisel verilerin işlenmesi için veri sahibi bilgilendirilirken kullanılan açık rıza, aydınlatma metni gibi metinlerde bireylerin anlayabileceği ve terminolojik bir dil kullanılmasının dürüstlük ilkesine uygunluk açısından son derece önemli olduğunu ifade etmiştir. [239] Nitekim amaçların belirsiz ya da yeterince açık olmaması bireylerin kişisel verileri üzerindeki denetimini azaltacağından ve veri sorumlularının bu kişisel verileri işleme konusundaki sınırlarını belirsiz hale getireceğinden, kişisel verilerin işlenmesi konusunda uyulması gereken en önemli ilkelerden biridir.

Ayrıca veri sorumlusu kişisel verileri işlenen kişi ya da kişilere bildirdikleri amaçlarla sınırlı olup, bu amaçların dışındaki hiçbir sebeple kişisel verileri işleyemezler. Yani veri sahibinden hangi amaç ya da amaçlar dahilinde açık rıza alındı ise, veriler bu amaçlar dahilinde işlenecek ve bireyin açık rıza vermiş olduğu bu amaçların genişletilmesi halinde bu durum hukuka aykırılık teşkil edecektir.

Diğer yandan bireylerin açık rızası olmaksızın kişisel verilerin işlenebilmesi için ise, bu işlemenin mutlaka meşru bir dayanağının ve amacının olması gerekmektedir. Örneğin Kişisel Verilerin Korunması Kanunu kapsamında açık rıza aranmaksızın kişisel verilerin işlenebileceği haller sınırlı olarak sayılmıştır. Bu hallerin dayanak olması halinde, kişisel veriler açık rıza olmaksızın işlenebilecektir.

4. Kişisel Verilerin İşlendikleri Amaçla Sınırlı, İlişkili ve Ölçülü Olması

Kişisel verilerin işlenmesi bakımından yukarıda yer verilen ilke ile bağlantılı bir diğer ilke de kişisel verilerin işlendikleri amaçla sınırlı, ilişkili ve ölçülü olma ilkesidir.

Buna göre ilk olarak kişisel verilerinin niteliği ile bu verilerin işlenme amacı birbirleriyle uyumlu olmalıdır. İlgili amaç için gerekli olmayan hiçbir kişisel veri için işlenmemeli ve kişisel veri işlemenin amacı hangi kişisel verilerin işlenmesini gerektiriyorsa yalnızca o kişisel veriler işlenmelidir. Kişisel Verileri Koruma Kurumu

[239] Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler**, s.8

konu hakkında sonradan ortaya çıkabilecek muhtemel ihtiyaçlara dayanarak kişisel verilerin işlenemeyeceğini belirtmiştir.[240]

İkinci olarak ise kişisel verilerin toplanma amaçlarının sınırlandırılması da bu ilke kapsamındaki önemli hususlardan biridir. Bu ilke kapsamında veri sorumlusunun kişisel verileri toplama amaçlarını sınırlandırması gereği düzenlenmiştir. Avrupa Birliği Genel Veri Koruma Tüzüğü kapsamında da bu husus amacın sınırlandırılması, *purpose limitation* olarak düzenlenmiştir. Bu husus Tüzük'ün 5. maddesinde kişisel verilerin belirtilen açık ve meşru amaçlara yönelik olarak toplanacağı ve bu amaçlara uygun olmayan şekilde işlenemeyeceği düzenlenmiştir. Doktrinde yeni ihtiyaçların ortaya çıkmasının yeni amaçlar oluşturduğu, bu bakımdan bunun yeni bir veri işleme faaliyeti olduğu ve gerekirse kişinin yeniden açık rızasının alınması gerektiği ifade edilmiştir.[241] Bu durumu bireylerin kişisel verilerinin kaderini tayin hakları ile yakından ilgilidir. [242]

Konu hakkındaki üçüncü ilke ise kişisel verilerin ölçülü olarak işlenmesidir. Bu husus da Avrupa Birliği Veri Koruma Tüzüğü'nün 5. maddesinde yer verilmiş ve kişisel verilerin işlendikleri amaçlarla ilgili olarak yeterli ve gerekli olanla sınırlı olarak işlenmesi gerektiği düzenlenmiştir. Kişisel Verileri Koruma Kurumu tarafından bu ilke kapsamında kişisel verilerin işlenmesi ile amaç arasında makul bir denge kurulması gerektiği ifade edilmiştir. Örneğin pazarlama amacıyla kişisel veri işleyen bir giyim mağazasının, kişinin özel nitelikli kişisel verilerine ilişkin kişisel veri işlemesi ölçülülük ilkesinden uzaktır.

5. Kişisel Verilerin İşlendikleri Amacın Gerektirdiği Süre Boyunca ya da Mevzuatın Öngördüğü Süre Kadar Muhafaza Edilmesi

Veri sahiplerinin kişisel verileri üzerindeki hak sahipliğinin en önemli uzantılarından biri de işlenen verilerin yalnızca ilgili mevzuatta belirlenen süre ya da veri işleme amacının gerektirdiği süre kadar muhafaza edilmeleridir. Zira kişisel verilerin işlendikten sonra sonsuz ve sınırsız bir süre ile muhafaza edilmeye devam edilmesi bireylerin verileri üzerindeki haklarını zayıflatacak ve bireylerin sınırsız bir

---

[240] Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler**, s.9. Küzeci, **Kişisel Verilerin Koruması** (2010), s.198
[241] Ayözger, **Kişisel Verilerin Korunması**, s. 128
[242] Ayözger, **Kişisel Verilerin Korunması**, s. 128

süre ile kayıt altına alınmasına sebebiyet verecektir. Buna göre ilk olarak veri sorumluları eğer bir kanundan kaynaklanan bir sebeple kişisel verileri işliyorsa ve bu düzenleme kapsamında verilerin işlenmesi için bir süre öngörülmüşse bu süre çerçevesinde veri depolayacak ve sürenin bitmesi ile birlikte kişisel verileri yok edecek, silecek ya da anonim hale getirecektir. Veri sorumlusunun bu süre bittikten sonra veriyi muhafaza etmeye devam etme gibi bir takdir yetkisi bulunmamaktadır. Kaldı ki bu husus aynı zamanda çalışmamızın üçüncü bölümünde işlemiş olduğumuz Türk Ceza Kanunu'nda yer alan 138. Maddesinde düzenlenen verileri yok etmeme suçunu oluşturacaktır.

Diğer yandan kişisel verilerin muhafazası için belli bir süre öngörülmemiş ise bu durumda, kişisel verilerin işlenmesi için belirtilen amaç her ne ise o amacın gerçekleşmesi ile birlikte kişisel verilerin yok edilmesi, silinmesi ya da anonim hale getirilmesi söz konusu olacaktır. Aksi takdirde bu durum hukuka aykırılık doğacaktır. Tıpkı yukarıda belirttiğimiz üzere bu halde de veri sorumlusunun ne olur ne olmaz diyerek kişisel verileri depolamaya devam etmesi gibi bir takdir yetkisi bulunmamaktadır.

Kaldı ki, kişisel verilerin muhafazası ile birlikte imhasına ilişkin hususları düzenlemek ve gerekli teknik ve idari tedbirleri almak da veri sorumlularının görevlerinden birini teşkil etmektedir. Nitekim kanunun 12. Maddesinde kişisel verilerin hukuka uygun şekilde sağlanmasını sağlamak, kişisel verilere yalnızca yetkili kişilerin erişimini sağlamak ve yetkisiz kişilerin erişimini engellemek, kişisel verilerin sağlıklı şekilde saklanmasını sağlamak amacıyla gerekli güvenlik önlemlerini almak ve bunun için tüm idari ve teknik tedbirleri almak zorunda olduğu açıkça düzenlenmiştir. Yine kanunun 16. Maddesinde veri sorumlularının veri sorumluları siciline yapacakları kayıtlarda kişisel verileri işleme amaçları ile birlikte verileri işleyecekleri azami süreleri de bildirme yükümlülükleri düzenlenmiştir.

Burada doktrinde önemli bir hususa yer verilmiş ve kişisel verilerin muhafazasına ilişkin süre veri sorumlusu tarafından veri sorumluları siciline bildirilmiş olsa dahi artık ihtiyaç duyulmayan ve amacını gerçekleştiren kişisel verilerin silinmesine yönelik temel ilke, bu bildirilen sürelerin tamamını geçersiz kılacak ve veri sorumlusu artık ihtiyacı bulunmayan kişisel verileri silmek

mecburiyetinde kalacaktır.[243] Bu hususun uygulama bakımından son derece önemli olduğunu düşünmekteyiz.

C. KVKK'DA DÜZENLENEN KİŞİSEL VERİLERİN İŞLENMESİNE İLİŞKİN VERİ İŞLEME KOŞULLARI

Kişisel Verilerin Korunması Kanunu'nda yer alan 5. ve 6. maddelerde kişisel verilerin işlenmesine ilişkin düzenlemelere yer verilmiştir. Buna göre kanunun kişisel verilerin işlenme şartlarını düzenleyen 5. maddesinde ve özel nitelikli kişisel verilerin işlenmesi başlıklı 6. maddesinde kişisel verilerin hangi şartlarda işlenebileceği konusu düzenlenmiştir. Veri sorumlusu kişisel verileri işlerken bu koşullardan bir ya da birkaçına dayanabilecek ve yalnızca bu koşullara dayanabilecektir. Yani madde metinlerinde belirtilen koşullar sınırlı olup bu koşullar dışında bir koşulla kişisel verilerin işlenmesi söz konusu olamaz. [244]

1. Özel Nitelikli Olmayan Kişisel Verilerin İşlenme Şartları

Kişisel Verilerin Korunması Kanunu'nun 5. maddesinde kişisel verilerin işlenmesine ilişkin şartlar düzenlenmiştir. Maddenin bu fıkrasında yer verilen kişisel verilerin özel nitelikli veriler olmadığını belirtmek isteriz. Buna göre maddenin ilk fıkrasında kişisel verilerin bireylerin açık rızaları olmaksızın işlenmelerinin mümkün olmadığı ifade edilmiştir. Açık rızaya ilişkin açıklamalar yukarıda ayrıntılı olarak yapıldığından burada tekrar edilmeyecektir ancak özetle kişinin açık rızasının belirli bir konuya ilişkin, bilgilendirmeye dayalı ve özgür irade ile verilmiş olması gerektiğini bir kere daha vurgulamak isteriz.

Diğer yandan maddenin ikinci fıkrasında ise açık rıza aranmaksızın kişisel verilerin işlenebileceği durumlara yer verilmiştir. Buna göre kişisel veri işlemenin kanunlardan kaynaklı olması, fiili olanaksızlık sebebiyle rızasını açıklayamayan veya rızası hukuki geçerlilik taşımayan kişinin ya da bir başka kişinin hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin oluşturulması veya sözleşmeden doğan yükümlülüklerin yerine getirilmesi ile ilgili olması şartıyla,

[243] Dülger, **Kişisel Verilerin Korunması Hukuku**, s. 137
[244] Dülger, **Kişisel Verilerin Korunması Hukuku**, s.214

sözleşme taraflarının kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüklerini yerine getirebilmesi için mecburi olması, kişinin bizzat kendisi tarafından verilerinin kullanılması veya hakkın korunması için veri işlemenin mecburi olması, bir kişinin temel haklarına ve özgürlüklerine zarar vermemek şartıyla, veri sorumlusunun meşru çıkarları için veri işlenmesinin mecburi olması şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenebileceği düzenlenmiştir.

Buna göre kişisel verilerin işlenmesi için ya ilk fıkrada düzenlendiği üzere kişinin açık rızası alınacak ya da ikinci fıkradaki hallerden birinin varlığı halinde kişinin açık rızasının alınmasına gerek kalmaksızın kişisel veriler işlenebilecektir. Bu noktada doktrinde açık rıza ile diğer veri işleme koşulları arasında bir hiyerarşi olmadığı ve hepsinin eş değer durumda olduğu ifade edilmiştir. [245] Bunun önemi ise, kişisel verilerin işlenmesi konusunda öncelikli olarak kişilerin açık rızasının alınması gerektiği şeklindeki algının yanlış olduğunu ortaya koymasıdır. Zira yine yukarıda açık rıza başlığında incelediğimiz üzere eğer maddenin ikinci fıkrasında yer alan hallerden birinin varlığı söz konusu ise bu durumda veri sorumlusunun kişinin açık rızasını alması söz konusu olmayacaktır. Bu halde kişinin açık rızasının da alınması söz konusu olursa bu durum kişinin yanlış bir izlenime kapılması yolu ile dürüstlük ilkesine aykırı ve dolayısıyla hukuka aykırı bir işlem tesis edilmiş olacaktır.

a. Kanunlarda Öngörülen Yükümlülüklerin Varlığı

Kanunlarda kişisel verilerin işlenmesi konusunda ilişkin açıkça öngörülen yükümlülükler mevcut ise, kişisel veriler bu yükümlülüklere dayanılarak işlenecektir. Bu hallerin bulunması halinde artık veri sorumlusunun kişisel veri sahibinden rızası almak gibi bir yükümlülüğü bulunmayıp doğrudan kanundan doğan yükümlülüğüne dayanarak kişisel verileri işleyebilecektir. Doktrinde maddenin lafzından yola çıkarak ‘açıkça’ ifadesine dikkat edilmesi gerektiği ve gerçekten de kişisel verilerin işlenmesine ilişkin açık bir ifade bulunmadığı durumlarda başka bir kişisel veri işleme koşulu araştırılması gerektiği ifade edilmiştir. [246]

[245] Dülger, **Kişisel Verilerin Korunması Hukuku**, s.215
[246] Dülger, **Kişisel Verilerin Korunması Hukuku**, s.216

b. Fiili Olanaksızlık Nedeniyle Rızasını Açıklayamayacak Kişinin veya Rızası Hukuki Geçerlilik Taşımayan Kişinin veya Bir Başka Kişinin Hayatı veya Beden Bütünlüğünün Korunması için Mecburi Olması Durumunda

Madde lafzından da anlaşılabileceği üzere eğer fiili bir olanaksızlık sebebiyle veri sahibi rızasını açıklayabilecek bir durumda değil ise ya da veri sahibinin rızası hukuki geçerlilik taşımıyorsa, bu kişinin ya da başkalarının hayat ve beden bütünlüğünün korunması için veri sahibinin rızası aranmaksızın kişinin verileri işlenebilecektir. Bu düzenleme kanaatimizce son derece yerinde bir düzenleme olmuştur. Gerçekten de bazı durumlarda bireyden açık rızası alınmak her zaman mümkün olmayabilir. Bu gibi yaşamsal durumlarda, kişisel verilerin işlenmesine yönelik prosedürlerine takılı kalmak bireylerin hayatını ya da beden bütünlüğünü geri dönülmez şekilde tehlikeye atabilecektir.

c. Taraflar Arası Bir Sözleşmenin Varlığı Sebebiyle Sözleşmenin Taraflarının Kişisel Verilerinin İşlenmesi Gerekliliği Durumunda

Taraflar arasında bir sözleşmenin imzalanması halinde, doğal olarak sözleşmenin taraflarının bazı kişisel bilgilerinin işlenmesi söz konusu olabilecektir. Bu durumda sözleşmenin tarafının açık rızasına tabi olmak, taraflar arasında kurulan sözleşmenin doğası ile bağdaşmayacaksa kişisel veriler açık rıza olmaksızın işlenebilecektir. Örneğin taraflar arasında kurulmuş bir ticari sözleşme kapsamında tarafların birbirlerinin adlarını, adreslerine ilişkin kişisel verileri işlemeleri sözleşmenin ifası bakımından zorunlu olduğundan bu halde artık verilerin işlenmesi için bireyin açık rızasına ihtiyaç bulunmamaktadır.

d. Veri Sorumlusunun Hukuki Yükümlülüklerini Yerine Getirebilmesi Amacıyla Zorunlu Olması Durumunda

Veri sorumlusu hukuki bir yükümlülük olarak kişisel veri işlemek mecburiyetinde ise artık bireyin açık rızası aranmayacak ve veri sorumlusu bu istisnaya dayanarak kişisel verileri işleyebilecektir. Örneğin işçi ve işveren arasında

kurulan bir iş sözleşmesinde işverenin yükümlülüklerini yerine getirebilmesi amacıyla işçinin adının, soyadının, SGK numarasının kaydedilmesi bu sözleşmenin kurulması ile doğrudan ilgilidir. Bu durumda işçiden bu bilgilerinin işlenmesi için ayrıca açık rıza alınmasına gerek yoktur.

e. Kişisel Verinin Bizzat Sahibi Tarafından Aleni Hale Getirilmesi

Kanunda ilgili kişinin kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi halinde işbu kanunun uygulanmayacağı belirtilmiştir. Bu noktada yasa koyucu kişisel verilerini kendi rızası ile alenileştiren kişilerin verilerini, bu kanun kapsamı dışında tutarak esasen hayatın olağan akışına uygun bir düzenlemeye yapmaya çalışmıştır."[247]

Bu noktada yasanın söz konusu maddesinin doğrudan uygulanmasının kişisel verilerin korunması hukukunun amacını aşacağı düşüncesindeyiz. Nitekim herhangi bir alenileştirilmiş verinin amacına aykırı şekilde başka bir deyişle kişinin verisini alenileştirirken göstermiş olabileceği rızanın dışında işlenmesi halinde artık bu orantısız kullanımın kişinin verilerinin kendi rızası ile alenileştirilmiş olduğu gerekçesi ile korunamayacağı aşikardır.[248] Doktrinde de kişi tarafından bizzat sosyal medyada paylaşılmış olsa dahi, bunun kişiye ait kişisel verilerin 3.kişiler tarafından kullanılmasına rıza gösterdiği anlamına gelmeyeceği ifade edilmiştir.[249] Nitekim yukarıda daha evvel de işlediğimiz üzere Yargıtay'da bu konudaki görüşlerini değiştirmiş ve her somut olayda aleniyete konu olan verinin özel olarak değerlendirilmesi gerektiğini ifade eden kararlar vermiştir.

---

[247] Yargıtay ilgili kararında, sanığın katılanın sosyal medya hesabındaki fotoğrafını alarak kendi sosyal medya hesabına koyduğunu, bahsi geçen fotoğrafın katılanın özel hayatına ilişkin kimsenin görmesini istemediği ya da istemeyeceği bir fotoğraf niteliğinde olmadığını, sanığın da katılanı özel olarak takibi ve katılanın özel hayatına müdahale niteliğindeki eylemlerle katılanın özel hayatını ihlal etmediği, bu eylemin 136. maddede belirtilen verileri hukuka aykırı olarak yayma ve ele geçirme suçu kapsamında değerlendirilmesi gerektiğini belirttikten sonra; bahsi geçen fotoğrafın katılan tarafından sosyal medya hesabında aleni hale getirilen bir fotoğraf olması sebebiyle bu suçun da oluşmayacağını ifade etmiştir. Yargıtay 12. CD. 13.10.2014, E. 2014/4081, K. 2014/19490.

[248] Dülger, **Kişisel Verilerin Korunması Hukuku**, s. 325

[249] Dülger, **Bilişim Suçları**, *s.684. Dülger konuyu şöyle değerlendirmiştir. "Rızanın geçerli olabilmesi için hangi eyleme ilişkin olduğunun belirlenebilir ve açık olması gerekir. Kişinin önceden verdiği belirli olmayan var olup olmadığı açıkça bilinmeyen genel geçer bir rızanın var olduğunun kabul edilmesi mümkün değildir*."

f. Kişisel Verinin İşlenmesinin Bir Hakkın Mevcudiyeti, Korunması Veya Bu Hakkın Kullanılması İçin Mecburi Olması

Veri işlemenin bir hakkın mevcudiyeti, yerine getirilmesi veya korunması için zorunlu olması durumunda bireyin açık rızası aranmayacaktır. Bu hususta personelinin dava açma zamanaşımı boyunca verilerini saklayan işveren örnek olarak gösterilebilecektir. Bu örnekte artık işverenin işçiden açık rıza almasına gerek bulunmamaktadır. [250]

g. Veri Sorumlusunun Meşru Menfaatleri Sebebiyle Kişisel Verilerin İşlemenin Mecburi Olması

Veri sorumlusunun meşru menfaatleri için veri işlemek zorunlu ise, ilgili kişinin temel hak ve özgürlüklerine zarar vermemek koşulu ile kişisel verilerin işlenmesi mümkün olacaktır. Bu koşul kanunun tartışmalı noktalarından biridir. Kanunun bazı maddelerine ilişkin Anayasa Mahkemesinde açılan iptal davasında, 5. maddenin 2. fıkrasının işbu bendine de yer verilmiştir.

Anayasa Mahkemesi nezdinde görülen davada, iptal talebine gerekçe olarak meşru menfaat ifadesinin kapsamı dikkate alındığında belirsiz olduğu, temel hak ve özgürlüklere getirilen sınırlamaların Anayasal olarak uygun olabilmesi için bu hak ve özgürlüklerin sınırlandırılması ile ilgili ilkelere aykırılık teşkil etmemesi ve bu noktada özel hayatın korunması ve kamu yararı arasında bir adil denge oluşturulması gerektiği, davaya konu edilen kuralın ise özel hayata bir müdahale niteliğinde olduğu, bireylerin kişisel verilerinin korunması hakkını orantısız şekilde sınırlandırdığı ve bu hakkın esasına zarar verdiği, davaya konu kuralın kamu yararının temin edilmesi gibi bir amaç taşımadığı ifade edilerek Anayasa'nın ilgili 2,13,20 ve 90. Maddelerine aykırılık iddia edilmiştir.

Görüldüğü üzere söz konusu g bendine ilişkin olarak en çok eleştirilen husus meşru menfaat kavramının belirsizliğidir. Ancak Anayasa Mahkemesi konuya ilişkin vermiş olduğu kararında[251] meşru menfaat kavramının belirsiz olduğunun

---

[250] Dülger, **Kişisel Verilerin Korunması Hukuku**, s. 218

[251] Anayasa Mahkemesi Kararı, E. 2016/125, K. 2017/143, K.T. 28.09.2017, R.G. Tarih – Sayı 23.01.2018- 30310

söylenemeyeceğini, zira bu noktada çalışanların temel haklarına ve özgürlüklerine zarar getirmemek şartıyla ve bu kavramın bu kişiler ile veri sorumluları arasında bir menfaat dengesi gözetilerek değerlendirilmesi gereken bir ifade olduğunu belirtmiş ve konuyu örneklemek açısından da bir şirketin çalışanlarının maaşları, zamların, sosyal hakları gibi sair idari düzenlemelerini yapılandırmak amacıyla kişisel verilerinin işleyebileceği, bu yapılandırmaya dayanarak da şirketin terfi gibi yönetimsel kararlarına imza atabilecekleri bunun da şirket sahibinin menfaatini ifade ettiğini ve elbette şirketin bunu yaparken çalışanların hak ve özgürlüklerini gözetmekle yükümlü olduğunu ortaya koymuştur.

Bu durumda mahkemenin kararından anlaşıldığı üzere bahsi geçen g bendinin uygulanması söz konusu olduğu durumlarda iki kritere dikkate edilecek ve somut olayda önce veri sorumlusunun meşru menfaatinin bulunup bulunmadığı konusunda bir karar verilecek eğer meşru menfaat tespiti yapıldıysa kişilerin temel hak ve özgürlüklerinin etkilenip etkilenmediği incelenecektir.

2. Özel Nitelikli Verilerin İşlenme Şartları

Özel nitelikli verilerin işlenmesi hakkındaki düzenlemelere kanunun 6. maddesinde yer verilmiştir. Bu maddenin ilk fıkrasında ırk, etnik köken, siyasi görüş, felsefi düşünce, dini inanç, mezhep veya sair inançlar, sendikalara, derneklere ya da vakıflara üyeliği, kılık ve kıyafet, kişinin sağlığına ilişkin bilgileri, bireyin cinsel hayatı, varsa hakkında verilmiş ceza mahkûmiyetleri ve/veya güvenlik tedbirleriyle ilgili bilgileri ve genetik ya da biyometrik bilgileri kişinin özel nitelikli verileri olarak sayılmıştır. Bu maddenin ikinci fıkrasında ise özel nitelikli verilerin ilgilinin açık rızası olmaksızın işlenmesi kesin olarak yasaklanmıştır. Görüldüğü üzere kanun koyucu kişilerin özel nitelikli kişisel verilerinin açık rıza olmaksızın işlenmesini yasaklamıştır.

Maddenin 3. fıkrasında ise özel nitelikli verilerin açık rıza olmaksızın işlenebileceği haller ayrıntılı biçimde düzenlenmiştir. Buna göre bireylerin özel alanında bulunan bireyin sağlığına ilişkin verileri ile yine bireylerin özel alanına giren cinsel hayatına ilişkin veriler dışındaki özel nitelik taşıyan kişisel veriler, işleme

yükümlülüğünün kanundan doğması halinde bireyin açık rızası alınmaksızın işlenebilir. Diğer yandan bireyin sağlığına ya da bieyin cinsel yaşamına ilişkin özel nitelikli verileri ise ancak ve ancak sır saklama yükümlülüğü bulunan bireyler veya bu konuda yetkili kılınmış kurumlar ve kuruluşlar tarafından, halk sağlığının korunması, sağlık sektöründeki hizmetlerin ve mali, finansal konuların düzenlenebilmesi ve bunları yönetilebilmesi, koruyucu hekimlik, bireylerin tedavilerinin ve bakım hizmetlerinin yürütülebilmesi, tıbben teşhis konulabilmesi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilecektir.

Bu noktada işbu üçüncü fıkra düzenlemesi, bireyin sağlığına ve cinsel hayatlarıyla ilgili verilerin işlenmesi durumunda madde metninde gösterilen ve yukarıda sayılan amaçların kanuni dayanağının aranmamış olması bakımından doktrinde eleştirilmiştir.[252] Tarafımızca da benimsenen bu eleştirilere göre fıkrada oldukça geniş tutulan bir amaçlar silsilesi bulunmakta olup, bu amaçların meşruluğunu oluşturması açısından kanunlarda açıkça öngörülme şartı aranmamıştır. Nitekim Kişisel Verilerin Korunması Kanunu'nun 6.maddesinin işbu 3. Fıkrasının iptali (ve sair pek çok madde) için Anayasa Mahkemesine iptal başvurusunda bulunulmuştur. Söz konusu başvuruda katıldığımız üzere kanun maddesinde yer alan bireylerin sağlığına ve cinsel yaşamına ilişkin verilerin işlenebilmesi için sağlık hizmetlerinin yönetimi ve bu hizmetlerinin mali ve finansal olarak analizi şeklindeki amacın bir gerekçe olarak sayılmasının, bireylerin sağlık sistemine başvurularında endişeler yaşayarak bu hakkı kullanmamalarına, bireylerin son derece mahrem olan bu gibi verilerinin hiçbir ayırt edici kriter olmaksızın sadece bu amaçla toplanabilecek olmasının bireylerin yaşam hakkına dahi müdahale niteliğinde olduğu, madde metninde yeterli korumanın ve tedbirin özelliğine ve içeriğine yer verilmeyerek belirsizlik oluşturuldu, bu düzenlenenin uluslararası mevzuata aykırı olduğu ve verileri işleyecek kurum ve kuruluşlar bakımından da bir sınırlama getirilmediğinden bu

[252] Küzeci, **Kişisel Verilerin Korunması**, 2018, s. 353. Aksi yönde görüş bkz. Dülger "*İptali talep edilen fıkra, Anayasaya aykırılık taşımasa da; bu hükmün belirttiğim şekilde yorumlanması ve amacını aşmaması gerekliliği Kurul tarafından veya diğer mahkemeler tarafından verilecek kararlarla net bir şekilde ortaya konulmalıdır"* şeklinde ifade etmiştir. Murat Volkan Dülger, "Anayasa Mahkemesi'nin Kişisel Verilerin Korunması Kanunu'nun Konu Edildiği İptal Davası Kararına İlişkin Bir Değerlendirme", s.6. www.academia.edu

kuralın Anayasa'nın 2, 10, 17, 20, 24, 25, 56. ve 90. Maddelerine aykırılık teşkil ettiği şeklinde gerekçeler ileri sürülmüştür. [253]

Anayasa Mahkemesi işbu maddeye ilişkin iptal başvurusunu iptal davasına konu edilen kural ile yasa koyucunun kamu sağlığının korunmasına ilişkin olarak yönetimsel ve idari olarak tedbirler almak istediğini, bu amaçla sağlık ve cinsel hayata ilişkin verilerin toplanmasının kamunun sağlığının korunması, sağlık servislerinin yürütülebilmesi, konu hakkında eğitim, araştırma faaliyetlerinin gerçekleştirilebilmesi, verimin yükseltilmesi için gerekli olduğunu ve diğer yandan ilgili kanunda amaç, kapsam ve sınırlandırmaların yer aldığını, kanun kapsamında Kurul'a gerekli önlemlerin alınması için yetki verildiği ve dolayısıyla gerekli tedbirlere ilişkin kararın Kurul tarafından verileceğini ve ayrıca yetkili kişi ve kuruluşların belirsizliği iddiasının da yerinde olmadığını zira sır saklama yükümlülüğü altındaki kişilerin kanunen belirli olduğunu, bu kişilerin de avukat, mali müşavir ya da doktor gibi hiçbir zaman ve hiçbir şekilde öğrendiklerini açığa vurmaları yasak edilmiş kişiler olduğunu belirterek reddetmiştir. [254]

Görüldüğü üzere özel nitelik taşıyan verilerin bireylerin açık rızası bulunmaksızın işlenmesi mümkün olmayıp, sağlık ve cinsel hayata ilişkin veriler dışında kalan özel nitelik taşıyan kişisel verilerin yalnızca kanunlar yer verilen hâllerde; sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak yukarıda belirtildiği üzere kanunda sınırlı olarak sayılan amaçlarla ve yalnızca sır saklama yükümlülüğü bulunan bireyler veya yetkilendirilmiş kurum veya kuruluşlar tarafından bireylerin açık rızaları bulunmasa dahi işlenebileceklerdir.

---

[253] Anayasa Mahkemesi Kararı, E. 2016/125, K. 2017/143, K.T. 28.09.2017, R.G. Tarih – Sayı 23.01.2018- 30310

[254] Bu konuyla ilgili olarak belirtmek isteriz ki, 20 Ekim 2016 tarihli Resmi Gazetede yayınlanarak yürürlüğe giren Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik, Danıştay 15. Dairesi tarafından verilen 2016/10500 ve 06.07.2017 T.'li karar ile durdurulmuştur. Danıştay bahsi geçen kararında Kişisel Verileri Koruma Kurulu'nun kontrol ve denetim yetkisine atıfta bulunarak Kurul'un, bu alanda hazırlanan her türlü mevzuat taslağı bakımından görüşünün alınması gerektiği ifade etmiş ve buna dayanarak Kurul'un denetiminde geçmeyen, görüşüne başvurulmayan düzenlemenin yürürlüğe girmesinin mevzuata ve hukuka uygun olmadığını belirtmiştir. Akabinde söz konusu yönetmelik iddia edilen hukuka aykırılıklar giderilmeksizin 24.11.2017'de bir kez daha yürürlüğe konulmuş ve bu yönetmelik hakkında yine Danıştay tarafından 25.06.2018 tarihinde yürütmeyi durdurma kararı verilmiştir. Danıştay 15. Dairesi 26.06.2018 T. ve 2018/844 E. sayılı kararı için bakınız. http://www.tdb.org.tr/tdb/ek/Danistay_15.Daire_2018-844_Karari.pdf

Diğer yandan maddenin 4. fıkrasında yine yukarda yer verdiğimiz üzere özel nitelikli hassas verilerin işlenmesine ilişkin olarak alınması gereken önlemler hakkında Kurul görevli kılınmış ve Kurul tarafından bu önlemlerin tespit edileceği ifade edilmiştir. Kişisel Verileri Koruma Kurulu, söz konusu yükümlülüğü doğrultusunda 31.01.2018 tarihinde vermiş olduğu 2018/10 sayılı kararında veri sorumluları tarafından alınacak işbu yeterli önlemlerin neler olduğunu ifade etmiştir. Buna göre Kurul altı maddeden oluşan önlemler kapsamında ilk madde olarak özel nitelikli kişisel verilerin işlenmesi durumunda, bu verilerin güvenli şekilde korunabilmesi için kuralları belirli, sistemli ve kapsamlı bir prosedür ya da politika düzenlenmesi[255] gerektiğini belirtmiştir. Görülüğü üzere veri sorumlusu özel nitelikli kişisel verilerin güvenliğine ilişkin ayrı bir politika oluşturmakla yükümlüdür.

İkinci madde ise özel nitelikli kişisel verilerin işlenme sürecinde çalışan kişiler içindir. Buna göre özel nitelikli hassas verilerin işlenmesinde faaliyet gösteren çalışanlar özel nitelikli kişisel verilerin işlenmesi durumunda bu verilerin güvenliği için düzenli şekilde eğitimler vermeli, gerekirse gizlilik sözleşmeleri imzalamalı, bu verilere erişim konusunda yetki sahibi kişilerin verilere hangi süre ve hangi yetkiler ile erişebilir olacağına ilişkin yetki ve süre tanımlarını yapmalı, eğer yetki sahibi bir kişi görevinden ayrılırsa verilere erişim yetkisini derhal kaldırmalı ve eğer bu kişiye verilmiş bir envanter var ise bu envanteri kendisinden almalıdır.

Üçüncü madde özel nitelikli hassas verilerin muhafaza edildiği ortamın elektronik ortamlar olması durumuna ilişkindir. Buna göre özel nitelikli hassas veriler özel kriptografik yöntemler kullanılmak suretiyle korunmalı, kriptografik anahtar birbirinden farklı ve güvenli alanlarda tutulmalı, özel nitelikli kişiler veriler üzerinde gerçekleştirilen tüm işlemlere ilişkin kayıtların güvenli şekilde loglanması, özel nitelikli verilerin bulunduğu ortamlarda gerektiğinde güvenlik güncellemelerinin gerçekleştirilmesi, bu ortamların düzenli olarak takip edilmesi, güvenlik testlerinin gerektiğinde yinelenmesi ve sonuçların kaydı, verilere erişim sağlayan bir yazılım varsa bu yazılama erişimin spesifik hale getirilmesi, verilere uzaktan erişim söz konusu olacaksa bir kimlik doğrulama sisteminin olması ve bunun en az iki kademeli olması şeklindeki önlemlerin alınması gerekmektedir. [256]

[255] Kişisel Verileri Koruma Kurulu'nun 31.01.2018 tarih ve 2018/10 sayılı kararı
[256] Kişisel Verileri Koruma Kurulu'nun 31.01.2018 tarih ve 2018/10 sayılı kararı

Dördüncü maddede ise özel nitelikli kişisel verilerin işlendiği ortamların fiziksel ortam olması durumunda bu kişisel verilerin muhafaza edildiği yerlerin her türlü hırsızlık, yangın, sel gibi ani olaylara karşı önleminin alınması gerekmektedir.[257]

Beşinci maddede ise özel nitelikli kişisel veriler aktarılması durumunda alınacak önlemlere ilişkin özel nitelik taşıyan veriler aktarılacak ise verilerin e-mail yoluyla aktarılacak olması halinde şifreli kurumsal hesaptan ya da KEP hesabı üzerinden aktarılması, taşınabilir harici yöntemlerle aktarılması söz konusu ise bunların şifrelenmesi yoluyla, farklı sunucular arasında bir aktarım söz konusu olacaksa bu sunucular arasındaki veri güvenliğini sağlayacak VPN, sFTP gibi yazılımların kullanılması ile veriler fiziki ortamda ise bu fiziki evrakların yetkisiz kişilerin eline geçmesine önleyecek güvenlik tedbirlerinin alınması ile aktarılması gerekmektedir.[258]

Altıncı madde olarak ise Kurul, kişisel veri güvenliğine ilişkin yayınladığı rehbere atıf yapmış ve bu rehberde yayınlanan güvenlik önlemlerinin de dikkate alınması gerektiğini ifade etmiştir. Görüldüğü üzere Kurul, kanunda belirtilen yükümlülükleri yerine getirmiş ve özel nitelikli hassas verilerin işlenmesine ilişkin olarak alınacak önlemleri belirleyerek ilgili kurul kararı ile yayınlamıştır.

D. KİŞİSEL VERİLERİN AKTARILMASI

Kişisel Verilerin Korunması Kanunu'nun 8. maddesinde[259] kişisel verilerin yurtiçinde[260] aktarılmasına ilişkin husus düzenlenmiştir. Buna göre ilk olarak maddenin birinci fıkrasında kişisel verilerin kişinin açık rızası olmadan işlenemeyeceği belirtilmiştir. Maddenin ikinci fıkrasında ise kişisel verilerin açık rıza aranmaksızın aktarılabileceği haller düzenlenmiştir. Tasarı halindeki kanunda madde metninde verilerin 'üçüncü kişilere" aktarımı şeklinde düzenlenmiş ancak daha sonra karışıklıklara mahal verilmemesi için bu ifade maddeden çıkarılmıştır. [261] Adalet komisyonu raporunda uluslararası ticaretin gelişmesi için kişisel veri paylaşımının son

[257] Kişisel Verileri Koruma Kurulu'nun 31.01.2018 tarih ve 2018/10 sayılı kararı
[258] Kişisel Verileri Koruma Kurulu'nun 31.01.2018 tarih ve 2018/10 sayılı kararı
[259] Kişisel Verilerin Korunması Kanunu, m.8
[260] Küzeci, **Kişisel Verilerin Korunması**, (2018), s. 355
[261] TBMM kişisel verilerin korunması kanununa ilişkin adalet raporunda kişisel verilerin aktarılması konusunda iç hukuklarda düzenlememe yapılmamasının uluslararası zeminde kişisel verilerin paylaşımını ve hem yargı alanında hem de ekonomik alanda uluslararası iş birliklerini olumsuz etkileyeceği, dolayısıyla bu alandaki eksikliklerin giderilmesinin hem uluslararası alanda iş birliklerini güçlendireceği hem de bireylerin temel hak ve özgürlüklerini temin edeceği tartışmasızdır. https://www.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf (Erişim Tarihi: 27.03.2019)

derece önemli olduğu ve bu yüzden konuya ilişkin mevzuat düzenlemelerinin yapılması gerektiği ifade edilmiştir.[262]

Buna göre kişisel veri işlemenin kanunlardan kaynaklı olması, fiili olanaksızlık sebebiyle rızasını açıklayamayan veya rızası hukuki geçerlilik taşımayan kişinin ya da bir başka kişinin hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin oluşturulması veya sözleşmeden doğan yükümlülüklerin yerine getirilmesi ile ilgili olması şartıyla, sözleşme taraflarının kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüklerini yerine getirebilmesi için mecburi olması, kişinin bizzat kendisi tarafından verilerin alenileştirilmiş olması, bir hakkın kurulması, bu hakkın kullanılması veya hakkın korunması için veri işlemenin mecburi olması, bir kişinin temel haklarına ve özgürlüklerine zarar vermemek şartıyla, veri sorumlusunun meşru çıkarları için veri işlenmesinin mecburi olması şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası olmadan da kişisel verilerinin aktarılabileceği ifade edilmiştir.

İkinci olarak ise özel nitelikli kişisel verilerin işlenme şartları başlıklı 6. maddenin 3. fıkrasında sayılan ve yine yukarıda değinmiş olduğumuz üzere, kişinin sağlığına ve cinsel yaşamıyla ilgili kişisel veriler dışında kanunlarda yer verilen hallerde, sağlığa ve cinsel yaşama ilişkin verilerde ise halk sağlığının korunması, tıbbî hastalıkların teşhisi, tedavisi ve bakım hizmetlerinin idaresi ile koruyucu hekimlik ve sağlık servislerinin idaresi ve finansmanının planlanması amacıyla kişinin açık rızası olmasa dahi kişisel veriler aktarılabilecektir. Kişisel Verileri Koruma Kurulu tarafından verilen bir kararda da bu konuya değinmiş ve doktor kontrolünde ilaç kullanan bireyin ilacını temin ettiği eczane tarafından özel nitelikle hassas verilerinin bireyin hiçbir meşru dayanak olmaksızın üçüncü kişilere aktarılması hususunda vermiş olduğu kararında şikâyete konu eczane hakkında idari tedbir kararı vermiştir. [263]

---

[262] ibid.

[263] Kişisel Verileri Koruma Kurulu konu hakkında vermiş olduğu kararında, ilgili maddenin 4. Fıkrasında veri sorumluları ve veri işleyenlerin muhafaza ettikleri kişisel verileri yetkisiz kişilere açıklayamayacaklarının ve işledikleri amaç haricinde kullanamayacaklarının hükme bağlandığını, bu noktada doktor tarafından kendisine reçete edilen ilaçları kullanan bir hastaya ilişkin özel nitelikli sağlık verilerinin bu ilaçları aldığı eczane tarafından kanunda kişisel verilerin aktarılmasına ilişkin şartlar sağlanmadan 3. Kişiler ile paylaşılmasını kanunun ilgili maddelerine aykırılık teşkil ettiğini ve bu sebeple eczane hakkında idari para cezasına hükmedilmesi gerektiğini ifade ederek, eczaneyi idari para cezasına çarptırmıştır. Kişisel Verileri Koruma Kurulunun 05/12/2018 Tarihli ve 2018/143 Sayılı Kararı

Kanunun 9. maddesinde[264] ise kişisel verilerin yurtdışına[265] aktarılması düzenlenmiştir. Buna göre ilk olarak yine kişisel verilerin ilgili kişinin açık rızası bulunmaksızın yurtdışına aktarılamayacağı ifade edilmiş olup, ikinci fıkrada ise yine kanunun 5. ve 6. maddelerinde belirtilen şartlardan birinin olması durumunda yeterli korumanın kişisel verilerin aktarılacağı ülkede var olması, bu korumanın mevcut olmaması durumunda ise Türkiye'de ve aktarımın yapılacağı ülkedeki veri sorumlularının gereken korumayı yazılı şekilde taahhüt etmeleri ve Kurul'un izninin mevcudiyeti şartıyla ilgili bireyin açık rızası bulunmaksızın yurt dışına aktarılabileceği ifade edilmiştir.

Bu konuyla ilgili ilk olarak yeterli korumanın bulunduğu ülkelere ilişkin olarak Kurul tarafından bir liste yayınlanacağı ifade edilmiş ancak söz konusu liste henüz yayınlanmamıştır. Kanunun 9. maddesinin 2. fıkrasının b bendinde kişisel verilerin aktarılacağı ülkede kişisel verilerin güvenliğine ilişkin gerekli korumanın bulunmaması halinde Türkiye'de ve söz konusu yabancı ülkede yer alan veri sorumlularının gereken korumayı yazılı şekilde taahhüt etmeleri yükümlülüğü düzenlenmiş olup, Kişisel Verileri Koruma Kurumu tarafından da yurtdışına veri aktarımında veri sorumluları ya da veri işleyen tarafından verilecek olan taahhütnamedeki asgari unsurlara ilişkin bir emsal taahhütname de yayınlanmıştır.

Kanunun ilgili maddesinin 4.fıkrasında da Kurul'un kişisel verilerin aktarıma konu edileceği yabancı ülkede gerekli ve yeterli koruma bulunup bulunmadığı hususunda karar verirken Kurul'un ülkemizin taraf olduğu uluslararası sözleşmeleri, kişisel verinin aktarılacağı ülke ile ülkemiz arasında kişisel verilerin aktarımıyla ilgili karşılıklılık halini, aktarıma konu olacak kişisel verilerin niteliği ile bu verilerin işlenme amaç ve süresini, ilgili yabancı ülkede yer alan mevzuatı, kişisel verinin aktarılacağı ülkede bulunan veri sorumlusu tarafından alınacağı ifade edilen önlemleri, değerlendireceği ve ihtiyaç olması durumunda gerekli kurum ve kuruluşlardan da görüşlerinin istenebileceği düzenlenmiştir.

Burada önemli bir diğer düzenleme de kişisel verilerin aktarımında kişisel verileri aktarılacak kişinin menfaatinin ya da ülkemizin ciddi bir şekilde zarar göreceği hallerin ortaya çıkma ihtimalinde ancak konuyla ilişkili kamu kurum veya

[264] Kişisel Verilerin Korunması Kanunu, m.9
[265] Küzeci, **Kişisel Verilerin Korunması**, (2018), s. 355

kuruluşunun görüşleri alınmak suretiyle ve Kurul'un izniyle yurt dışına aktarılabileceği düzenlemesidir. Bu düzenleme doktrinde belirsizliği ve hangi durumlarda zararın oluşacağına ilişkin bir açıklamanın olmaması bakımından eleştirilmiştir.[266] Burada yasa koyucu ilgili ülkeler arasında imzalanan uluslararası sözleşmeleri saklı tutmuştur.

E. KVKK'DA DÜZENLENEN KİŞİSEL VERİLERİN İŞLENMESİNE İLİŞKİN VERİ SAHİBİNİN HAKLARI

Kişisel Verilerin Korunması Kanunu'nda yer alan 11. madde kapsamında veri sahibinin hakları düzenlenmiş olup buna göre veri sahibinin kişisel verilerinin işlenip işlenmediğini öğrenme; eğer kişisel verileri işlenmiş ise işlenen kişisel verileri hakkında bilgi alma; kişisel verilerin hangi amaçla işlendiğini ve bu verilerin işlendikleri amaçlara uygun kullanılıp kullanılmadıklarını öğrenme; eğer bu kişisel veriler aktarılmış ise bu verilerin aktarıldığı üçüncü kişiler hakkında bilgi alma; kişisel verilerin gerekli hallerde düzeltilmesini talep etme, kanunda öngörülen haller mevcutsa kişisel verilerin silinmesini veya yok edilmesini talep etme; maddenin (d) ve (e) bentleri gereğince işlem yapılmışsa kişisel verilerin aktarıldığı üçüncü kişilere de bu işlemlerin bildirilmesini talep etme; işlenen kişisel verilerin sadece otomatik sistemler aracılığı ile analizi halinde, kişinin kendisi aleyhinde bir sonuç ortaya çıkmasına itiraz etme, kişisel verilerin hukuka aykırı şekilde işlenmesi neticesinde kişinin zarara uğraması söz konusu olursa bu zararın giderilmesini talep etme, haklarına sahiptir. Aşağıdaki bu haklar ayrıntılı olarak incelenmiştir. Bu düzenleme uluslararası mevzuatla da uyumludur.

Nitekim Avrupa Birliği Genel Veri Koruma Tüzüğü bağlamında baktığımızda da Tüzük'ün kişisel verileri işlenen kişilerin haklarına ilişkin 3. bölüm kapsamında düzenlemelere yer verilmiş ve veri sahibinin hakları ayrıntılı olarak düzenlenmiştir. Veri sahibinin haklarının kullanımına ilişkin şeffaf bilgilendirme, bildirim ve yöntemler, veri sahibinden kişisel verilerin toplandığı hallerde sağlanacak bilgiler, kişisel verilerin veri sahibinden alınmadığı hallerde sağlanacak bilgiler, veri sahibinin erişim hakkı, düzeltme hakkı, silme hakkı, işleme faaliyetini kısıtlama hakkı, Kişisel verilerin düzeltilmesine ya da silinmesine veya işleme faaliyetinin kısıtlanmasına

[266] Küzeci, **Kişisel Verilerin Korunması**, (2018), s. 357

ilişkin bildirim yükümlülüğü, veri taşınabilirliği, itiraz hakkı ve otomatik münferit karar verme hakkı, profil çıkarma da dahil olmak üzere otomatik münferit karar verme hakkı gibi haklar Tüzük kapsamında tanınan haklardır.

1. Kişinin Kişisel Verilerin İşlenip İşlenmediğini Öğrenme Hakkı

Kişisel veri sahibi, kişisel verilerinin işlenip işlenmediğini öğrenmek hakkına sahiptir. Bu hakkın önemi doktrinde iki yönden ele alınmıştır. Buna göre kişilerin verilerinin işlenip işlenmediğini bilmesi ilk olarak kişilerin sair tüm haklarını kullanabilmesi açısından önemli, çatı niteliğinde bir haktır. Diğer yandan ise kişilerin verilerinin işlenip işlenmediğini bilmeleri veri işleyenlerin şeffaf[267] hareket etmesi için de son derece önemlidir. Doktrinde veri sahiplerinin söz konusu bu hakkı ile yine kanunun 10. maddesinde düzenlenen veri sorumlusunun aydınlatma yükümlülüğünün birbirini tamamlayan haklar olduğu ifade edilmiştir.[268]

Nitekim kanunun veri sorumlusunun aydınlatma yükümlülüğü başlıklı 10. maddesinde de veri sorumlusunun kişisel veri sahiplerine, kendisinin ve varsa temsilcisinin kimliği, bireyin kişisel verilerinin hangi amaçla işleneceği, kişisel verilerin hangi amaçlarla ve kimlere aktarılabileceği, kişisel verilerin nasıl toplanacağı ve toplamanın hukuki sebepleri ile yukarıda ayrıntılı olarak saymış olduğumuz kanunun 11.maddede yer verilen sair hakları hususunda bilgilendirmekle yükümlüdür.

Veri sorumlusu tarafından, veri sahibinin yukarıdaki hususlara göre bilgilendirilmesi için bu bilgilendirmenin açık ve anlaşılır bir dilde olması gerektiği vurgulanmıştır. [269] Zira yukarıda da belirttiğimiz üzere kişinin haklarının bilmesi ve doğru şekilde kullanabilmesi için yapılacak bilgilendirmenin anlaşılabilir nitelikte ve zamanında yapılması son derece önemlidir. Aydınlatma yükümlülüğüne ilişkin olarak hususlar ayrıntılı olarak çalışmamızın ilgili bölümünde işleneceğinden burada tekrar olmaması için daha fazla yer verilmemiştir.

2. Kişisel Verilere İlişkin Bilgi Talep Etme Hakkı

Kişisel veri sahibinin kendisi hakkında işlenen verilere ilişkin olarak bilgi alma hakkı mevcuttur. Bu hak çalışmamızın birinci bölümünde bahsettiğimiz üzere Avrupa

---

[267] Korkmaz, **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, s. 123-124
[268] Dülger, **Kişisel Verilerin Korunması Hukuku**, s.153
[269] Dülger, **Kişisel Verilerin Korunması Hukuku**, s.153

ülkelerinde olduğu üzere Türkiye'de de kişisel verilerin korunması hukukuna yaklaşımın insan hakları bağlamından yapılmış olmasıdır. Nitekim insan hakları yaklaşımında kişisel verileri işlenen kişinin veri üzerindeki hakimiyeti bitmez. Aksi halde bu durum mülkiyet hakkı yaklaşımını ortaya koyacaktır. Bu halde de kişisel verileri 3. kişiler tarafından işlenen bireylerin verileri hakkında bilgi alma ve süreci takip etme hakkı bulunmaktadır. Doktrinde bu hak, verilerin geleceğini belirleme hakkı olarak ifade edilmiştir.[270]

Buna göre, Tüzük'ün 15. maddesinde[271] de veri sahibinin erişim hakkı adı altında bir düzenleme yapılmıştır. Bu düzenlemeye göre veri sahibi, verilerinin işlenip işlenmediğine ilişkin veri sorumlusundan bilgi almak ve işlenen verileri ile birlikte, veri işleme amacı, işlenen verinin kategorisi, özellikle üçüncü ülkelerde ya da uluslararası organizasyonlarda yer alan alıcılar başta olmak üzere, işlenen kişisel verinin paylaşılacağı ya da paylaşıldığı kimseler, kişisel verinin ne kadar süre ile tutulacağı ve eğer bu süre belli değilse belirlemek için hangi kriterlerin uygulanacağı, veri sahibinin verilerinin silinmesini, yok edilmesini talep hakları ve veri işlenmesine kısıtlama getirme haklarına ilişkin, denetim mekanizmasına şikayette bulunma, veri sahibinden elde edilmeyen ancak veri sahibine ilişkin olarak toplanan kişisel verilere ilişkin, profil çıkarma dahil olmak üzere otomatik karar alma kapsamında işlenen veriler ve bunların sonuçlarına ilişkin, konular hakkında bilgi sahibi olabileceği ifade edilmiştir.

Doktrinde bir bireyin kişisel verilerine erişimi halinde başka bir bireyin de verilerine erişiminin de söz konusu olacağı hallerde, veri sorumlusunun kanunun 13. maddesine göre gerekçesini açıklayarak bu talebi reddedebilecektir. Görüldüğü üzere bireylerin kişisel verilerin erişim hakkı hem ulusal mevzuatımızda hem de uluslararası mevzuat kapsamında bireylerin verilerinin yalnızca işlenirken değil işlendikten sonra da takip edebilmeleri ve gerekirse kanundan doğan sair haklarını kullanabilmeleri için oldukça önemli bir düzenlemedir.

---

[270] Dülger, **Kişisel Verilerin Korunması Hukuku,** s.156
[271] Avrupa Birliği Veri Koruma Tüzüğü, m.15

3. Kişisel Verilerin Hangi Amaçlarla İşlendiğini ve İşlenen Verilerin Amacına Uygun Olarak Kullanılıp Kullanılmadığını Öğrenme Hakkı

Kişisel veri sahiplerinin verileri işlenirken, bu verilerin hangi amaçla işlendiğini bilme hakları bulunmaktadır. Nitekim yukarıda da belirttiğimiz üzere kanunun 10. maddesi uyarınca veri sorumlularının da aydınlatma yükümlülüğü kapsamında bu bilgiyi kişisel verisi işlenen kişiye bildirme yükümlülüğü bulunmaktadır. Ayrıca bu veriler işlendikten sonra da işlenen verilerin amacına uygun kullanılıp kullanılmadığını öğrenme hakkı bulunmaktadır. Zira aksi halde veri sahibinin kişisel verilerin kendisine bildirildiği şekilde kullanılmadığını öğrenmesi durumundan açık rızasının geri alabileceği gibi, itiraz edebilecek ve gerekirse ilgili kurula başvuruda bulunabilecektir. Bu bakımından kişisel veriler işlendikten sonra da kişinin verilerinin akıbetini takip etmesi son derece önemlidir.

4. Kişisel Verilerin Aktarılmasına İlişkin Bilgi Talep Etme Hakkı

Kişisel Verilerin Korunması Kanunu'nun 8. maddesinde kişisel verilerin veri sorumluları tarafından yurtiçinde 3. kişi ya da kuruluşlara aktarımı düzenlenmiş olup, kanunun 9. maddesinde ise verilerin veri sorumluları tarafından yurtdışına aktarımı düzenlenmiştir. Bu konu yukarıda kişisel verilerin aktarılmasına ilişkin bölüm altında ayrıntılı olarak incelendiğinden burada tekrara düşmemek için yeniden yer verilmemiştir.

Diğer yandan Avrupa Birliği Veri Koruma Tüzüğü'nün 20. maddesinde de kişisel verilerin veri sahibi tarafından veri sorumlusundan başka bir veri sorumlusuna aktarılmasını talep hakkı düzenlenmiştir. Bu hak kapsamında veri sahibi özel olarak verileri alıp başka bir veri sorumlusuna vermeyecek ve bu talep hakkını kullanarak veri sorumluları arasında veri naklini talep edecektir. İlgili maddede bu işlemin talep edilebilmesi için veri transferinin makine tarafından okunabilir olma gibi kişisel verinin transferine uygun teknik altyapının mevcut olması gerekmektedir.

5. Kişisel Verilerin Düzeltilmesini İsteme Hakkı

Düzeltme hakkı hem mevcut kanunumuz kapsamında hem de Avrupa Birliği Veri Koruma Tüzüğü kapsamında yer verilen önemli haklardan biridir. Kanunun 11. maddesinin d bendine göre kişi, kendisine ait kişisel verilerin eksik veya yanlış şekilde

işlenmiş olması durumunda bu eksik ve yanlış kişisel verilerin düzeltilmesini talep etme hakkına sahiptir. Özellikle kişisel verilerin işlenmesinden kişisel verileri işlenen kişilerin doğrudan etkilendiği durumlarda oldukça önemlidir. Örneğin bir bankanın müşterisinin kişisel verisini yanlış veya eksik işlemiş olması halinde, veri sahibine ulaşamama ya da o kişiye ait özel bilgileri yanlış adreslere ulaştırma gibi bir duruma sebebiyet verebilecektir. İşte bu gibi durumların engellenmesi için kişisel veri sahiplerine böyle bir hak tanınmıştır.

Avrupa Birliği Veri Koruma Tüzüğü'nün 16. maddesinde de bireylerin düzeltme hakkı düzenlenmiştir. Buna göre, veri sahipleri veri sorumlularından eğer bir yanlışlık varsa verilerinin düzeltilmesini ve eksik ise tamamlanmasını isteme hakkına sahiptir.

6. Kişisel Verilerin Silinmesini veya Yok Edilmesini İsteme Hakkı

Kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesini talep etme hakkı veri sahibinin en önemli haklarından biridir. Kanunun 7. maddesinde hukuka uygun şekilde işlenen kişisel verilerin, işlenme amaçlarının gerçekleştirilmesi ve artık bu verilerin işlenmesine gerek kalmaması neticesinde kişisel verilerin bizzat veri sorumlusunun kendisi tarafından ya da veri sahibinin talebi üzerine silinmesi, yok edilmesi ya da anonim hale getirilmesi mümkündür.

Esasen kanunun lafzı dikkate alındığında, kişisel verilerin işlenmeye devam etmesini gerektiren bir sebep bulunmamakta ise kişisel verilerin silinmesi, yok edilmesi ya da anonim hale getirilmesi hem veri sorumlusu tarafından resen yerine getirilebileceği bir yükümlülük olarak düzenlenmiş hem de bu veri sahibi tarafından veri sorumlusunda talep edilebilecek bir hak olarak düzenlenmiştir. Nitekim veri sahibinin haklarının düzenlendiği 11. maddede, 7. maddeye atıfla kişisel verilerin silinmesini ve yok edilmesini talep etme hakkına yer verilmiştir.

Esasen 6698 sayılı KVKK'nın 7.maddesi değerlendirildiğinde, unutulma hakkına yönelik yerinde bir düzenleme yapıldığını da söyleyebiliriz. Zira Yargıtay Hukuk Genel Kurulu da yakın tarihte vermiş olduğu bir kararında unutulma hakkına atıf yapmış ve unutulma hakkını kişinin 3. Kişiler tarafından bilinmesini istemediği

kişisel verilerinin ortadan kaldırılmasını talep etme hakkı olarak ifade etmiştir.[272] Unutulma hakkına ilişkin detaylı açıklama birinci bölümünde yapıldığından burada tekrar edilmeyecektir.

Avrupa Birliği Veri Koruma Tüzüğü'nün 17. maddesinde kişisel verilerin silinmesi hakkı düzenlenmiştir. Madde kapsamında dikkat edilecek nokta ise madde başlığından parantez içinde bu hak unutulma hakkı olarak da tanımlanmıştır. Doktrinde mevcut kanunumuzda konuya ilişkin ayrıntılı hususlara yer verilmediği için Avrupa Birliği Genel Veri Koruma Tüzüğü'nde şartlar dikkate alınarak konu açıklanmaya çalışılmıştır.[273]

Bu maddeye göre madde metninde ayrıntılı olarak ifade edilen şartların bulunması halinde veri sahibi veri sorumlusundan kişisel verilerinin silinmesini talep edebilecektir. Bu şartlar, kişisel verilerin işlenmesi için sunulan sebeplerin ortadan kalkmış olması, veri işleme için başka bir hukuki gerekçenin olmadığı durumlarda veri sahibinin açık rızasının geri alması, veri sahibinin veri işlemesine itiraz etmesi, kişisel verinin hukuka aykırı olarak işlenmesi, veri sorumlusunun tabi olduğu Avrupa Birliği hukukunda kaynaklı bir yükümlülüğün yerine getirilmesi için kişisel verinin silinmesi, kişisel verilerin Tüzük'ün 8.maddesinde düzenlenen bilgi toplumu hizmetlerinin sağlanması ile ilgili toplanmış olması, şeklinde sayılabilecektir.

Yukarıdaki açıklamalarımız çalışmamız kapsamında ayrıca yer verilen unutulma hakkı ve konuya emsal Avrupa Adalet Divanı'nın Google Spain vs Mario Costeja Gonzalez kararı ile birlikte değerlendirildiğinde, kişisel verilerin silinmesini talep etme hakkının ne denli önemli olduğu görülecektir.

---

[272] Yargıtay unutulma hakkıyla ilgili olarak kişisel verilerin depolanmasının kişisel verilerinin korunması hakkının çatısını oluşturduğunu, unutulma hakkının bireyin kişisel verileri üzerinde tasarrufta bulunabilme hakkına dayandığını ve bu hakkın geçmişte her ne olduysa bu olanları bir kenara bırakarak kişinin hayatına devam edebilmesini sağlamak ve bu bilgilerin ileride bireyin aleyhinde kullanılmasını önlemek adına oldukça önemli olduğunu, bir kamu yararının söz konusu olacağı durumlar haricinde, bireyin bu haktan yararlanarak geleceğini şekillendirmek konusunda hakka sahip olduğunu ve bireyin bu hakla beraber geçmişte yaşamış olduğu olaylara dair kişisel verilerinin yok edilmesini talep edebileceğini ve dolayısıyla bireylere geçmişleri üzerinde kontrol sahibi olabilme hakkı tanındığını, bu hakkı kullanan bir kişinin 3. kişilerden bu verileri kullanmamalarını veya 3. kişilerin kullanmasını ve hatırlamasını engelleyecek şekilde önlemlerin alınmasını isteyebileceğini belirttikten sonra, örnek olarak bireyin geçmişteki olumsuz fotoğraflarının ya da kendileri hakkındaki içeriklerin kaldırılmasını talep edebileceğini ifade etmiştir. Yargıtay Hukuk Genel Kurulu E. 2014/4-56 K. 2015/1679 T. 17.6.2015

[273] Dülger, **Kişisel Verilerin Korunması Hukuku**, s. 172

Söz konusu 7. maddenin devamında ise kişisel verilerin hangi yöntemlerle, hangi usul ve esaslara uyarak silineceği, yok edileceği veya anonim hale getirileceğinin yönetmelik vasıtası ile düzenleneceği belirtilmiş ve bunun üzerine 28 Ekim 2017 tarihinde Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik yayınlanarak yürürlüğe girmiş ve konuya ilişkin detaylar bu yönetmelik kapsamında düzenlenmiştir. Nitekim bu durum yönetmeliğin 'dayanak' başlıklı 3. maddesinde de belirtilmiş ve bu yönetmeliğin Kişisel Verilerin Korunması Kanunu'nun ilgili 7. Maddesi ile ilgili 22. Maddesine dayanarak hazırlandığı ifade edilmiştir. Bu yönetmelik kapsamında kişisel verilerin saklanması ve imha politikası, veri imha politikası yöntemleri kapsamında kişisel verilerin yok edilmesi, silinmesi veya anonim hale getirilmesi esasları düzenlenmiştir.

a. Kişisel Veri Saklama ve İmha Politikası

Yönetmeliğin tanımlar başlıklı 4. maddesinde kişisel veri saklama ve imha politikası veri sorumluları tarafından hazırlanan, veri sorumlularının kişisel verileri hangi süre ile işleyeceklerini belirlemek ve silme, yok etme ya da anonim hale getirme gibi işlemleri gerçekleştirmek için uyulması gereken esasları belirledikleri politika olarak tanımlanmıştır. Yönetmeliğin "Kişisel Veri Saklama ve İmha Politikası" başlıklı ikinci bölümünde ise kişisel veri saklama ve imha politikasına ilişkin esaslar ile kişisel veri saklama ve imha politikasının kapsamına ilişkin düzenlemelere yer verilmiştir.

Öncelikle Yönetmelik'in 5. maddesinde Kişisel Veri Saklama ve İmha Politikasına ilişkin esaslara yer verilmiştir. Bu maddeye göre kişisel veri saklama ve imha politikasını hazırlamak ile görevli kişilerin veri sorumluları olduğu ifade edilmiştir. Veri sorumluları bu politikayı veri işleme envanterine uygun olarak hazırlamakla yükümlüdürler.

Bu madde kapsamında dikkat çeken bir düzenleme de maddenin 3. fıkrasıdır. Bu fıkraya göre yasa koyucu kişisel veri saklama ve imha politikası hazırlamakla yükümlü olmayan veri sorumlularının da bu yönetmelik çerçevesinde kişisel verileri saklama, silme, yok etme ve anonim hale getirme yükümlülüklerinin bulunduğunu ifade etmiştir. Burada yasa koyucunun anlatmak istediği husus, Kanun'un 'veri sorumluları sicili' başlıklı 16. maddesinde belirtilen ve Kurul tarafından işlenen kişisel

verinin özellikleri, bu verilerin miktarı, veri işlemenin kanundan kaynaklanması veya üçüncü kişilere aktarılma durumu gibi durumlara dayanarak veri sorumluları siciline kaydolma zorunluluğuna istisna getirilebilecek olan veri sorumlularıdır.

Nitekim Yönetmelik'in yukarıda yer vermiş olduğumuz 'kapsam' başlıklı 5. maddesinde bu Yönetmelik'e göre kişisel veri ve imha politikası hazırlayacak olan veri sorumlularının, veri sorumluları siciline kaydolmakla yükümlü veri sorumluları olduğu ifade edilmiştir. Bu durumda Kurul'un sicile kayıttan istisna tuttuğu veri sorumluları bu veri saklama ve imha politikasını hazırlamıyor olsalar dahi bu Yönetmelik' göre kişisel verileri saklama, silme, yok etme veya anonim hale getirme yükümlülükleri devam edecektir.

Aynı bölümün 6. maddesinde ise kişisel veri saklama ve imha politikasının kapsamına ilişkin asgari esaslar düzenlenmiştir. Buna göre kişisel veri saklama ve imha politikası, hazırlanma amacına, bu politikada ifade edilen tüm terimlerin tanımlarına kişisel verilerin kayıt edildiği ortamlara, teknik ya da hukuki konuya dair tüm açıklamalara, kişisel verilerin güvenli şekilde saklanması ve yetkisiz erişimlerin engellenmesi için alınmış teknik ve idari tedbirlere, kişisel verilerin imhası için alınmış hukuka uygun teknik ve idari tedbirlere, veri politikalarında görev alanlar hakkındaki bilgilere, kişisel verilerin muhafaza ve imha sürelerini işaret eden tabloya, periyodik imha zamanlarına, politika hakkında güncelleme yapılmış ise işbu değişikliğe ilişkin esaslara yer verilir.

b. Veri İmhaya İlişkin Yöntemler

Yönetmeliğin üçüncü bölümünde ise pratikte veri sorumluları için en önemli bölümlerden birine, Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi esaslarına yer verilmiştir. Buna göre Kişisel Verilerin Korunması Kanunu'nun kişisel verilerin işlenmesi ve özel nitelikli kişisel verilerin işlenmesi başlıklı 5. ve 6. maddelerine göre işlenen verilerin işlenmesi için gerekli sebepler ortadan kalktığında söz konusu kişisel verilerin yok edilmesi, silinmesi ya da anonim

hale getirilmesi gerekmektedir.[274] İşte bu noktada uygulanacak yöntemlerle ilgili işbu yönetmeliğe bakılacaktır.

Yasa koyucu kişisel verilerin yok edilmesi, imha edilmesi veya anonim hale getirilmesine ilişkin işlemler yapılırken 6698 sayılı kanunun ilgili maddelerine[275], varsa sair mevzuat hükümlerine, kurul kararlarına ve imha politikalarına uyumlu olarak bu işlemlerin gerçekleştirilmesi gerektiğini ifade etmiştir. Bir diğer önemli husus ise kişisel verilerin silinmesi, yok edilmesi ya da anonim hale getirilmesine ilişkin tüm kayıtların 3. yıl süre ile saklanma yükümlülüğüdür.[276] Veri sorumlusu bu süreçte hangi yöntemi seçeceğine karar verirken talep edilmesi halinde seçtiği yöntemi neden seçtiğini açıklamakla yükümlüdür. Aşağıda bahsi geçen yöntemler açıklanmıştır.

Bu noktada kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin olarak dikkat edilecek sürelere de ilgili yönetmelikte yer verilmiştir. [277] Buna göre, yukarıda yer vermiş olduğumuz üzere imha politikasını hazırlamakla yükümlü olan veri sorumlusu, kişisel verilerin yok etmekle, silmekle ya da anonim hale getirme işlemlerinin yerine getirilmesinin gerekli olduğu tarihten sonra gelen imha politikasında önceden belirlemiş olduğu ilk periyodik imha işlemi tarihinde, kişisel verileri silecek, yok edecek veya anonim hale getirecektir. Ancak eğer veri sorumlusu imha politikası hazırlamak mecburiyetinde değilse bu durumda kişisel verilerin, silinmesi yok edilmesi ya da anonim hale getirilmesi ihtiyacının ortaya çıktığı tarihten itibaren üç ay içerisinde söz konusu verileri silecek, yok edecek veya anonim hale getirecektir.

Yönetmelik kapsamında bireylerin bizzat talep etmesi halinde, kişisel verilerin silinmesi durumuna da yer verilmiştir. Buna göre kişisel veriler bireylerin talebi üzerinde, veri sorumlusu tarafından incelenecektir. Veri sorumlusu eğer kişisel verilerin işlenmesi için gerekli şartlar ortadan kalmadı ise, bireyin talebini gerekçesini

---

[274] Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in 7. maddesinin 1. Fıkrasında Kanun'da yer alan 5. ve 6. Maddelerdeki veri işleme şartlarının artık mevcut olmaması halinde ya veri sahibinin talebi üzerine ya da veri sorumlusunun bizzat kendisi tarafından veriler yok edilecek, anonim hale getirilecek veya silinecektir.

[275] 6698 sayılı kanunun ilgili hükümleri kanunun 'Genel İlkeler' başlıklı 4. maddesi ile 'Veri Güvenliğine İlişkin Yükümlülükler' başlıklı 12. maddesidir.

[276] Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in 7. maddesinin 3. fıkrası

[277] Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in 11. maddesi

de açıklayarak 30 gün içerisinde reddetmek suretiyle bireye bildirimde bulunacaktır. Diğer yandan eğer gerçekten de verilerin işlenmesi için gerekli şartlar artık ortadan kalktı ise veri sorumlusu talepten itibaren en geç 30 gün içerisinde bireyin talebini sonuçlandıracaktır. [278]

Elbette bu noktada Yönetmeliğin iş bu maddelerinin yanı sıra genel olarak diğer mevzuat hükümleri de dikkate alınacaktır. Örneğin Kişisel Verileri Koruma Kurulu tarafından verilmiş olan bir kararda, Kurul, devlet memurlarının haklarında açılmış olan inceleme ve soruşturma kapsamındaki evrakların imhasına yönelik talebin veri sorumlusu kamu kurumu tarafından reddedilmesine ilişkin olarak vermiş olduğu kararda, 657 sayılı Devlet Memurları Kanunu ve Kamu Personeli Genel Tebliğine göre devlet memurlarının görev yaptıkları döneme dair özlük dosyalarının saklanacağına ilişkin hüküm karşısında veri sorumlusu tarafından verilmiş olan kararı uygun bulmuştur.[279]

aa. Kişisel Verilerin Silinmesi

Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemeyecek ya da tekrar kullanılamayacak hale getirilmesi anlamını taşımaktadır.[280]

Kişisel verilerin silinmesi ile ilgili olarak gerçekleştirilecek süreç öncelikle silinecek kişisel verilerin tespiti, kişisel verilere erişim imkânı olan kullanıcıların tespiti, kullanıcıların hangi yöntemler aracılığı ile bu verilere ulaştıklarının tespiti ve son olarak ise verilerin silinmesi yani kişisel verilere erişim imkânı olan kullanıcıların

---

[278] Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in 11. maddesi

[279] İlgili karara göre Kurul durumu şu şekilde ifade etmiştir. "*Devlet memurlarının, memuriyet döneminde haklarında açılmış inceleme-soruşturma dosyalarına ilişkin evrakların imha edilme talebinin veri sorumlusu kamu kurumunca yerine getirilmemesi üzerine Kuruma yapılan başvuru kapsamında, imha edilmesi talep edilen kişisel bilgilerin, ilgili kişinin devlet memuru olduğu dönemde hakkında açılmış inceleme-soruşturma dosyalarına ilişkin evraklar olması ve bu itibarla söz konusu evrakların, 657 sayılı Kanun gereğince özlük dosyalarında saklanması gerektiği, Kamu Personeli Genel Tebliğine (Seri No: 2) göre özlük dosyalarının dördüncü bölümünde yer alacağı ile görevi herhangi bir şekilde sona eren memurların özlük dosyalarının kurumlarınca saklanacağı ve Devlet Arşiv Hizmetleri Hakkında Yönetmeliğe göre son işlem tarihi üzerinden yüz bir yıl geçmemiş memuriyet sicil dosyaları içerisinde yer aldığı hususlarından hareketle, 6698 sayılı Kanunun 7 inci maddesinde belirtildiği üzere kişisel verilerin işlenmesini gerektiren sebeplerin de henüz ortadan kalkmaması dolayısıyla şikayetçinin talebinin veri sorumlusu tarafından karşılanmamasının uygun olduğuna karar verilmiştir."* Kişisel Verileri Koruma Kurulunun 28/06/2018 Tarihli ve 2018/69 Sayılı Kararı

[280] Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in 8. maddesi

söz konusu kişisel verilere erişim imkanlarının ortadan kaldırılması olarak özetlenebilecektir.[281] Kişisel Verileri Koruma Kurumu tarafından kişisel verilerin silinmesine ilişkin hizmet türü olarak bulut çözümlerin kullanıldığı durumlarda kişisel verilerin silinmesine ilişkin silme komutu verilmesi gerektiği, kağıt ortamda bulunan kişisel veriler için karartma yönteminin kullanılması gerektiği, işletim sisteminde kayıtlı kişisel veriler için ise yine verilerin silinmesi ve erişim yetkilerinin kaldırılması gerektiği, taşınabilir ortamlarda yani USB bellek gibi medyalarda bulunan kişisel veriler içinse bu verilerin taşınabilir medyalara uygun yazılımlar vasıtasıyla silinmesi gerektiği, veri tabanlarında bulunan kişisel verilerin ise veri tabanı silme komutları ile silinmesi gerektiği ifade edilmiştir.[282]

bb. Kişisel Verilerin Yok Edilmesi

Kişisel verilerin yok edilebilmesi için, kişisel verilerin muhafaza edildiği tüm kopyaların ortaya konulması ve kişisel veriler hangi tür bir sistemde bulunuyorsa o sisteme özgü teknik bir yöntemle yok edilmesi gerekir. Kişisel verilerin yok edilmesi ise kişisel verilere bir daha hiç kimse tarafından erişilememesi, bu verilerin geri getirilemeyecek ya da tekrar kullanılamayacak biçime getirilmesi anlamına gelmektedir.[283] Kişisel verilerin silinmesi ve yok edilmesi arasındaki fark ise, kişisel verilerin silinmesi bu verilere ilgili kullanıcılar tarafından bir daha erişilememesini ifade ederken, kişisel verilerin yok edilmesi ise hiç kimse tarafından bir daha bu verilere erişilememesi anlamına gelmektedir.

Kişisel Verileri Koruma Kurumu tarafından kişisel verilerin yok edilmesine ilişkin olarak yerel sistemlerde olan kişisel verilerin yok edilmesine ilişkin bazı teknik tavsiyelerde bulunulmuştur. Bu teknikler yerel sistemlerde bulunan kişisel veriler için manyetize etme, fiziksel yok etme, üzerine yazma, kâğıt ve mikrofiş ortamlarında bulunan veriler için ana ortamın yok edilmesi gerekli olduğundan geri birleştirilmesi mümkün olamayacak biçimde parçalamak, bulut ortamında olan kişisel veriler içinse erişimi sağlayan tüm şifrelerin yok edilmesi gibi yöntemlerdir.

---

[281] Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi**, s.6

[282] Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi**, s.9

[283] Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in 9. maddesi

cc. Kişisel Verilerin Anonim Hale Getirilmesi

Kişisel verilerin anonim hale getirilmesi, 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 dahil olmak üzere, başka verilerle eşleştirilme gibi uygun tekniklerin kullanılması yoluyla dahi bir gerçek kişiyle ilişkilendirilemez hale getirilmesi gerekmektedir.

Konuya ilişkin olarak daha evvel de Netflix örneğini vermiş ve Netflix'in başarısız anonim hale getirme işleminden bahsetmiştik. Bahsi geçen olayda Netflix tarafından kullanıcı verileri anonim hale getirilmek suretiyle yayınlanmış ancak bahsi geçen kişisel veriler bazı araştırmacılar tarafından tersine işlem yöntemi ile açığa çıkarılarak kişisel verilerin ait olduğu bireyler tespit edilmişti.[284]

7. Kişisel Verilerin Üçüncü Kişilere Aktarılmış Olması Durumunda Bu Kişilere Bildirimde Bulunulmasını İsteme Hakkı

Yukarıda yer vermiş olduğumuz 11. maddenin (d) fıkrasında düzenlenen veri sahibinin kişisel verilerinin eksik ya da hatalı olması durumunda bu kayıtların düzeltilmesini talep etme hakkı ile ve aynı maddenin (e) fıkrasında düzenlenen veri sahibinin kişisel verilerinin yok edilmesini talep etme hakkı veri sahibi tarafından kullanılır ve sorumlusu tarafından da bu talepler yerine getirilir ise, veri sahibi veri sorumlusundan bu taleplerini verilerin aktarıldığı 3. kişilere de bildirmesini isteyebilir. Avrupa Birliği Veri Koruma Yönetmeliği'nin 19. maddesinde de yerine getirilen düzeltme talebinin, kişisel verilerin hatalı ya da eksik olarak açıklandığı diğer alıcılara da bildirilmesi durumu düzenlenmiş ve fakat bu bildirimin aşırı bir efor gerektirmesi ya da imkânsız olması durumunda bu bildirimin yapılmayabileceği düzenlenmiştir.

[284] İlgili haber için bakınız.https://www.computerworld.com/article/2987050/data-privacy/are-datasets-truly-anonymized-two-well-suited-researchers-are-going-to-find-out.html. (Erişim Tarihi: 10.02.2019)

8. İşlenen Verilerin Otomatik Sistemler Aracılığı ile Analiz Edilmesi Durumunda Kişinin Şahsı Aleyhine Bir Sonucun Ortaya Çıkmasına İtiraz Etme Hakkı

Kişisel veri sahibinin bu hakkıyla ilgili olarak Adalet Komisyonu Raporunda bireylerin rızaları olmaksızın, kişinin zarar görmesine neden olabilecek nitelikte sonuçlar doğmasına sebep olacak her türlü işleme itiraz etme hakkı getirildiği ve bu hakkın bireyin kendisi dışında işlenen verileri üzerinde de denetim sahibi olması bakımında oldukça önemli olduğu ifade edilmiştir. Aynı raporda buna örnek olarak bir çalışanın performansının ve işlerinin, otomatik bir sisteme işlenip analiz edilmesi ve buna göre değerlendirilmesine çalışanın itiraz edebilmesi örnek olarak gösterilmiştir.[285] Avrupa Birliği Genel Veri Koruma Tüzüğü'nün 21. maddesinde bu hak itiraz etme hakkı başlığı altında düzenlenmiştir. Bu hakka göre kişisel veri sahibi kendi özel durumuna dayanarak veri sahibinin, kendi özel durumu ile ilgili gerekçelere dayalı olarak, (6)1 maddesinin (e)[286] veya (f)[287] bentlerindeki dayalı olarak kendisiyle ilgili kişisel verilerin işlenmesine herhangi bir zamanda itiraz etme hakkı bulunduğu ve veri sorumlusunun bu noktada veri sahibinin yararından, temel hak ve özgürlüklerinden daha ağırlıklı bir meşru sebebinin olduğunu ortaya koymadıkça artık veri işleyemeyeceği ifade edilmiştir.

9. Zararın Giderilmesini Talep Etme

Kişisel Verilerin Korunması Kanunu kapsamında veri sahiplerinin bir diğer hakkı da zararın giderilmesini talep etme hakkıdır. Kişisel veri sahipleri kişisel verilerinin ihlal edilmesi sebebiyle eğer bir zarara uğrarlarsa, bu zararın giderilmesini talep etme hakkına sahip olacaklardır. Bu hak aynı zamanda kanunun istisnalarının düzenlendiği 28.maddesinin 2. fıkrasının kanun kapsamı dışında tutulacak hallerinde dahi, veri sahiplerinin zararın giderilmesini talep hakkı uygulanmaya devam edecektir. Bu hak uluslararası düzenlemeler ile de uyumlu olmuştur. Buna göre Avrupa Birliği

---

[285] TBBM, Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu, s. 12 https://www.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf (Erişim Tarihi:27.03.2019)

[286] Avrupa Birliği Genel Veri Koruma Tüzüğü 6.maddenin e. bendi *"Kamu yararına gerçekleştirilen bir görevin yerine getirilmesi veya kontrolöre verilen resmi bir yetkinin uygulanması hususunda işleme faaliyetinin gerekli olması."*

[287] Avrupa Birliği Genel Veri Koruma Tüzüğü 6.maddenin e. bendi "*özellikle veri sahibinin çocuk olması halinde veri sahibinin kişisel verilerin korunmasını gerektiren menfaatleri veya temel hakları ve özgürlüklerinin bir kontrolör veya üçüncü bir kişi tarafından gözetilen meşru menfaatlere ağır basması haricinde, söz konusu menfaatler doğrultusunda işleme faaliyetinin gerekli olması.*"

Genel Veri Koruma Tüzüğü kapsamında da 82. maddede veri sahiplerinin kişisel veri haklarının ihlal edilmesi halinde, bu ihlalden doğan zararın tazmin edilmesini talep etme hakkına sahiptirler.

F. KVKK'DA KİŞİSEL VERİLERİN İŞLENMESİNE İLİŞKİN DENETİM MEKANİZMASI

Kişisel verilerin işlenmesine ilişkin denetim mekanizması ülkemizde Kişisel Verileri Koruma Kurumu olarak düzenlenmiştir. Kişisel Verileri Koruma Kurumu ve teşkilatın yapısı, Kişisel Verileri Koruma Kanunu'nun 6. bölümünde düzenlenmiştir. Buna göre kişisel verilerin korunmasına ilişkin denetim mekanizması Kişisel Verilerin Korunması Kurumu ve Kişisel Verilerin Korunması Kurulu olarak iki ayrı yapıdan oluşmaktadır.

Kişisel Verileri Koruma Kurumu kanunun 19. maddesinde düzenlenmiştir. Kanunun 19. maddesine göre Kişisel Verileri Koruma Kurumu, Kişisel Verileri Koruma Kanunu'nda yer verilen görevleri yerine getirmek amacıyla, hem idari hem de mali bağımsızlığa haiz bir kamu tüzel kişiliği olarak kurulmuştur. Kanımızca burada en önemli unsur, Kurum'un idari ve mali olarak özerk bir yapı olarak kurulmuş olmasıdır. Nitekim bireylerin kişisel verileri yalnızca özel kurumlara karşı değil devlete yani kamu kurumlarına karşı da koruma altında olmalıdır. Dolayısıyla kurumun özerk bir yapı olarak inşa edilmesi son derece önemlidir. Maddenin hemen devamında ise Kurum'u Cumhurbaşkanının görevlendireceği bakan ile ilişkili olacağı, merkezinin Ankara olduğu ifade edilmiştir. Kişisel Verileri Koruma Kurumu, Kişisel Verileri Koruma Kurulu ve başkanlıktan oluşmakta olup, Kurum'un karar mekanizması Kişisel Verileri Koruma Kurulu'dur.

Kişisel Verileri Koruma Kurumu'nun görevleri ise kanunun 20. maddesinde sayılmıştır. Buna göre Kurum'un görevleri kişisel verilerin korunması alanındaki tüm yenilikleri izlemek, gelişmeleri değerlendirmek ve gerekirse bu konular hakkında görüş bildirmek ya ad önerilerde bulunmak, görev alanında bulunması ve durumun da gerektirmesi halinde çeşitli meslek örgütlerinden sivil toplum kuruluşlarına kadar çeşitli kurum ve kuruluşlarla işbirliği içerisinde olmak, kişisel verilere ilişkin tüm uluslararası gelişmeleri izlemek ve gerekirse uluslararası kurum ya da kuruluşlarla ortak çalışmalarda bulunmak, varsa toplantılara katılım sağlamak, yıllık faaliyet

raporunu sunmak ve varsa kanunlarda Kurum'a verilmiş diğer görevleri yerine getirmek olarak sayılabilecektir.

Kişisel Verileri Koruma Kurumu personeline ilişkin olarak 05 Mayıs 2016 tarihinde Kişisel Verileri Koruma Kurumu Personeli Görevde Yükselme ve Unvan Değişikliği Yönetmeliği yürürlüğe girmiş olup, Kurum personelinin görevde yükselme ve unvan değişikliği ilişkin olarak esaslar bu yönetmelik kapsamında düzenlenmiştir. Bu yönetmelik kapsamında, yükselmeye tabi kadrolar, görevde yükselme veya unvan değişikliği suretiyle yapılacak atamalarda aranacak genel şartlar, bu kişilerde aranacak özel şartlar ile görevde yükselme ve unvan değişikliği için yapılacak sınavın esasları düzenlenmiştir.

Diğer yandan yine Kişisel Veri Koruma Kurumuna ilişkin olarak 26 Nisan 2018 tarihinde Kişisel Verileri Koruma Kurumu Teşkilat Yönetmeliği yürürlüğe girmiştir. Bu yönetmelikte öncelikle kanun kapsamında yer verilen Kurum ve Başkanlık tanım ve görevleri benzer şekilde tekrar edildikten sonra, kanundan farklı olarak Kurum'un hizmet birimleri ve görevlerine ilişkin düzenlemelere yer verilmiştir. Bu düzenlemelere göre Kurum'un hizmet birimleri Veri Yönetimi Dairesi Başkanlığı, İnceleme Dairesi Başkanlığı, Hukuk İşleri Dairesi Başkanlığı, Veri Güvenliği ve Bilgi Sistemleri Dairesi Başkanlığı, Rehberlik, Araştırma ve Kurumsal İletişim Dairesi Başkanlığı, İnsan Kaynakları ve Destek Hizmetleri Dairesi Başkanlığı, Strateji Geliştirme Dairesi Başkanlığı olarak sayılmıştır. Görüldüğü üzere Kurum'un hizmet birimler işbu 7 teşkilattan oluşmaktadır.

Kurum'un karar mekanizması olan Kişisel Verileri Koruma Kurulu ise kanunun 21. maddesinde düzenlenmiştir. Buna göre kanunda Kurul'a ilişkin olarak başta Kurul'un görevlerini yerine getirirken tam bağımsız olmasına atıf yapılmış ve hiçbir kurum, kuruluş, makam ya da merci ya da kişi tarafından Kurul'un kendi görev alanındaki konular hakkında Kurul'a tavsiye, öneri, telkin, talimat, ya da emir veremeyeceği ifade edilmiştir. Görüldüğü üzere tıpkı Kurum bakımından olduğu üzere Kurul bakımından da ısrarla bağımsızlık vurgusu yapılmış ve Kurul'a hiçbir şekilde başka bir merciden ya da kişiden emir ve talimat verilemeyeceği gibi, Kurul'a tavsiye de dahi bulunulamayacağı ifade edilmiştir. Kanuna göre Kurul toplamda dokuz üyeden

oluşacak ve bu dokuz kişinin beş üyesi meclis tarafından geri kalan dört üyesi ise Cumhurbaşkanı tarafından seçilecektir. [288]

Kurul'un görev ve yetkilerine ilişkin ise kanunun 22. maddesinde düzenleme yapılmış olup, Kişisel Verileri Koruma Kurulu'nun görevleri kişisel verilerin temel hak ve özgürlüklere halel getirmeyecek şekilde işlenmesini sağlamak, kişisel verilere ilişkin olarak hak sahipleri tarafından kendilerine yapılacak başvuru ve şikayetleri değerlendirerek bu konuda bir karar vermek, resen görev alanına giren konularda, ilgili iddia veya şikayeti haber alması ile birlikte kişisel verilere ilişkin işlemlerin Kanun'a uygun yapılıp yapılmadığını incelemek ve gerekirse önlemler almak, özel nitelikli hassas verilerin işlenmesi konusunda gerekli önlemlerin neler olduğunu tespit etmek iade etmek, daha evvel de bahsetmiş olduğumuz veri sorumluları sicilinin tutulmasını sağlamak, teşkilatın işleyişine ilişkin konularda eğer görev alanına giriyorsa ilgili düzenlemeleri yapmak, veri güvenliğine ilişkin düzenleyici işlemleri gerçekleştirmek, veri sorumluları ile bunların temsilcilerine ilişkin görev ve yetkiler konusunda ilgili işlemleri yapmak, kanun çevresinde yer verilen idari yaptırımlara karar vermek, eğer kişisel verilerin korunmasına ilişkin bir mevzuat taslağı hazırlanmış ise bu hangi kurum ve kuruluştan gelirse gelsin bu konuda görüşünü ifade etmek, kurumun amaçlarını, standartlarını, performans kriterlerini ve stratejik planlarını belirleyerek bunları gerekirse karara bağlamak, kurumun bütçe teklifini görüşmek ve karara bağlamak, kuruma dair ihtiyaç duyulan konularda hazırlanan rapor taslaklarını onaylamak ve yayımlamak, taşınmaz işlemleri konularındaki önerilere dair karar vermek ve kanunlarda öngörülen sair görevleri yerine getirmek olarak sayılmıştır.

Teşkilatın bir diğer önemli ayağı ise Başkanlık'tır. Başkan ve Başkanlık kanunun 24 ve 25. maddelerinde düzenlenmiştir. Bu maddelere göre başkan Kurum'un temsilinden ve yönetiminde sorumlu kişidir. Başkanlık ise kanunun 25. maddesinde düzenlenmiş olup, buna göre başkanlık, başkan yardımcı ve sair hizmet birimlerinden oluşan bir birimdir. Hizmet birimleri, başkanlığa kanun tarafından verilen görevlerin yerine getirilmesi hususunda aracılık ederler. Başkanlığın görevleri veri sorumluları hakkındaki sicili tutmak, Kurum'un ve Kurul'un sekretaryasını ifa etme, kurumun

[288] Kanunun 21. maddesinin 3. fıkrasında Kurul'a üye olabilmek için sahip olunması gereken hususlara yer verilmiştir. Buna göre kurula üye olabilmek için Kurum'un görev alanına giren hususlarda deneyim sahibi olmak, Devlet Memurları Kanunu'nun 48. Maddesinde 1/A/1-4-5-6-7 alt bentlerinde yer alan özellikleri bulundurmak, siyasi partiye üye bulunmamak, 4 yıllık bir fakülteden lisans sahibi olmak.

hukuk işlerini idare etmek, kurumdaki görevlilerin ve kurul üyelerinin özlük işlemlerini idare etmek, kanunlar tarafından mali hizmet ve strateji geliştirme birimlerine verilen görevleri yerine getirmek, kurumda bilişim sistemlerinin kurmak, Kurul'un rapor taslaklarını hazırlamak ve bu taslakları Kurul'a sunmak, stratejik plan taslaklarını hazırlamak, personel politikaları üzerine çalışmak, personelin kariyeri ve alması gereken eğitimler üzerine çalışmak, özlük işlemlerini idame ettirmek, kurum içinde uyulacak kuralları belirlemek, kurumun ihtiyacı olan satın alma, kiralama gibi her türlü işlemi ilgili mevzuata uygun şekilde yürütmek, kurumun mülkiyetinde bulunan taşınır ve taşınmazların kayıtlarını sağlamak, ve varsa sair görevleri yapmak olarak ifade edilebilecektir.

Kişisel Verileri Koruma Kurulu'na ilişkin olarak 16 Kasım 2017 tarihinde Kişisel Verileri Koruma Kurulu Çalışma Usul ve Esaslarına Dair Yönetmelik yayınlanarak yürürlüğe girmiştir. Bu yönetmelik kapsamında Kişisel Verileri Koruma Kurulu'na, görev ve yetkilerine ilişkin, Kanun'da sayılan ve yukarıda da yer vermiş olduğumuz düzenlemeler tekrar edildikten sonra Kurul'un çalışma usul ve esaslarına yer vermiştir. Yönetmeliğin üçüncü bölümünde yer alan Kurul'un çalışma usul ve esaslarına göre, Kurul'un, başkan da dahil olmak üzere en az altı üyenin katılımı ile toplanacağı ve üye tam sayısının salt çoğunluğu ile de karar vereceği ifade edilmiştir. Ayrıca Kurul üyelerinin çekimser oy kullanma hakları bulunmamaktadır. Ayrıca yönetmelikte Kurul'un gerekli gördüğü hallerde bu kararları kamuoyu ile paylaşacağı da düzenlenmiştir. Nitekim kamuoyuna açıklanan Kurul kararlarını çalışmamız kapsamında ayrıca inceleyeceğiz.

Kanunun devam eden 26. maddesinde ise teşkilat yapısına Kişisel Verileri Koruma Uzmanı ve Kişisel Verileri Koruma Uzman Yardımcısı dahil edilebileceği de düzenlenmiştir. Konuya ilişkin olarak 09 Şubat 2018 tarihinde de Kişisel Verileri Koruma Uzmanlığı Yönetmeliği yürürlüğe girmiştir. Buna göre eğer teşkilat yapısına Kişisel Verileri Koruma Uzmanı ve Kişisel Verileri Koruma Uzman Yardımcısı dahil edilmesine karar verilmiş ise söz konusu yönetmeliğin esasları uygulanacaktır. Nitekim bu yönetmelik kapsamında Kişisel Verileri Koruma Uzman Yardımcılarının mesleğe alınmalarına, yetiştirilmelerine, Kişisel Verileri Koruma Uzmanlığına atanmalarına ilişkin usul ve esaslar ile Kişisel Verileri Koruma Uzman ve Uzman Yardımcılarının görev, yetki ve sorumlulukları düzenlenmiştir.

ÜÇÜNCÜ BÖLÜM

KİŞİSEL VERİLERİN 5237 SAYILI TÜRK CEZA KANUNU VE 6698 SAYILI KİŞİSEL VERİLERİN KORUNMASI KANUNU KAPSAMINDA KORUNMASI

I. KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN TÜRK CEZA KANUNUNDA DÜZENLENEN SUÇ TİPLERİ

Genel olarak kişisel verilerin korunması konusuna mevzuatları kapsamında yer vermiş ülkelerin düzenlemeleri incelendiğinde, hukuki açıdan iki yaklaşım olduğu ve bu iki yaklaşımdan birinin tercih edildiği görülmektedir. Bunlardan birincisi kişisel verilerin korunmasına karşı işlenen suçların genel kanunlar kapsamında korunması, ikincisi ise kişisel verilerin korunmasına ilişkin ve tamamen bu konuya özgü bir kanunun çıkarılmasıdır.[289] Ancak zaman içerisinde bu yaklaşımlardan ikincisi, kişisel verilerin korunmasını konu alan özel bir kanun düzenlemesi yaklaşımı, daha fazla benimsenmeye başlanmıştır.

Elektronik ticaretin artışı, sosyal medya gibi bireylerin kişisel verilerinin artık sıradan ve günlük bir rutin olarak paylaşılmasına aracılık eden araçların çoğalması ve bunlar aracılığı ile dünya üzerinde pek çok kurum ve kuruluşta büyük dataların var olması, bu dataların ise siyasetten ticarete kadar çok çeşitli alanlarda çıkar sağlamak, toplumu ve tercihlerini etkilemek adına kullanılması gibi sosyolojik ve siyasi vakaların yaşanması[290] ve bir yandan da gerek toplumun artan veri güvenliği baskısı gerek ise başta Avrupa Birliği'nin üye veya üyelik sürecinde olan ülkelere yönelik hukuki

---

[289] Küzeci, **Kişisel Verilerin Korunması**, 2010, s. 286

[290] 2018 yılı Nisan ayında Cambridge Analytica isimli politik danışmanlık ve strateji firması tarafından, Facebook kullanıcılarının yüklediği bir uygulama aracılığı ile profil bilgilerine, kullanıcı geçmişine ve bu kişilerin arkadaş listesinde olan diğer kişilerin de aynı bilgilerine ulaşıldığı, bu şekilde toplamda Facebook'un seksen yedi milyon kullanıcısının kişisel verisine sahip olunduğu ve firmanın bu verileri 2016 tarihli Amerikan Başkanlık seçiminde Donald Trump lehine kullandığı iddiaları hem Facebook hem de bahsi geçen firma adına soruşturma açılmasına sebebiyet vermiştir. Daha ayrıntılı bilgi için bakınız.https://www.techrepublic.com/article/facebook-data-privacy-scandal-a-cheat-sheet/. 15.12.2018.

düzenleme talebi ikinci yaklaşımın daha çok benimsenmeye başlamasına sebebiyet vermiştir. [291]

Yukarıda da belirttiğimiz gibi yaklaşık on yıl öncesine kadar kişisel verilerin korunması konusu bazı ülkelerde özel düzenlemeler kapsamında korunurken, bazı ülkelerde ise Türkiye'de olduğu gibi genel düzenlemeler ile korunduğu, bununla yetinildiği görülmekteydi ancak yaşanan bu gelişmeler karşısında bu ülkeler de mevzuatlarında değişikliğe gitmiş ve kişisel verilerin korunması hususunu özel kanunlar kapsamına almaya başlamışlardır. Avrupa ülkelerinin çok büyük bir kısmında ise günümüzde büyük ölçüde ikinci yaklaşımın benimsendiğini söyleyebiliriz.[292] Elbette özellikle Avrupa Birliği ülkeleri için düşünüldüğünde, GDPR'ın yürürlüğe girişinin başta Avrupa Birliği ülkeleri olmak üzere pek çok ülkeyi böyle bir değişime ittiğini söylemek yanlış olmayacaktır.

Ülkemize baktığımızda ise uzun yıllar sadece birinci yaklaşım yani kişisel verilerin korunmasına yönelik düzenlemelerin genel kanunlar kapsamında doğrudan ya da dolaylı olarak[293] korunması yaklaşımı benimsenmiştir. Bu kapsamda 5237 sayılı Türk Ceza Kanunu çerçevesinde, kişisel verilerin kaydedilmesi suçu, verileri hukuka aykırı olarak verme veya ele geçirme suçu ve verileri yok etmeme suçu düzenlenmiştir.

---

[291] Avrupa Birliği, 27 Nisan 2016 tarih ve 2016/679 sayılı direktifin 45. Maddesine dayanarak Avrupa Birliği üyesi olmayan ülkelerin gerek iç hukuk sistemlerinde gerekse uluslararası zeminde taraf olduğu anlaşmalar bakımından Avrupa Birliği veri güvenliği standartlarını sağlayıp sağlamadığı konusunda karar verme yetkisine sahiptir. Avrupa Birliği Parlamentosu ve Avrupa Birliği Konseyi Kişisel Verilerinin İşlenmesi ve Kişisel Verilerin Serbest Dolaşımına İlişkin Bireylerin Korunması Hakkındaki Direktif. https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN. 05.12.2018. Bundan sonra "**Avrupa Birliği Genel Veri Koruma Tüzüğü"** olarak anılacaktır.

[292] Küzeci, **Kişisel Verilerin Korunması**, 2010, s. 286

[293]Kadir Can Özel, "6698 Sayılı Kişisel Verilerin Korunması Kanunu Üzerine Genel Bir Değerlendirme", s.1 (Çevrimiçi) Özel konu hakkında başta Anayasa, Ceza Kanunumuz, Ceza Muhakemeleri Kanunu olmak üzere mevzuatımızda yer alan pek çok kanunda ya da sair düzenlemede kişisel verilerin korunmasıyla ilgili hükümler mevcuttur şeklinde görüş bildirmiştir. https://www.academia.edu/35234866/6698_SAYILI_K%C4%B0%C5%9E%C4%B0SEL_VER%C4%B0LER%C4%B0N_KORUNMASI_KANUNU_%C3%9CZER%C4%B0NE_KISA_B%C4%B0R_DE%C4%9EERLEND%C4%B0RME . (Erişim Tarihi: 05.12.2018)

A. KİŞİSEL VERİLERİN KAYDEDİLMESİ SUÇU

1. Genel Olarak

5237 sayılı Türk Ceza Kanunu'nun "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" başlıklı dokuzuncu bölümünün 135. Maddesinde kişisel verilerin hukuka aykırı olarak kaydedilmesi suçuna yer verilmiştir. Yukarıda 765 sayılı Türk Ceza Kanundan bahsederken de belirttiğimiz üzere, ilgili kanunda kişisel verilerin korunmasıyla doğrudan ilişkili bir madde bulunmadığı için işbu 135. Madde 5237 sayılı Türk Ceza Kanunu'nda ilk defa yer verilen bir düzenleme niteliğindedir.[294]

Türk Ceza Kanunu'nun 135. Maddesinin 1. fıkrasında kişisel verilerin hukuka aykırı şekilde kaydedilmesi halinde bu eylemi gerçekleştiren kişinin bir yıldan üç yıla kadar hapis cezası ile cezalandırılacağı ifade edilmiştir. Maddenin ikinci fıkrasında ise bireylerin felsefi görüş, siyasi düşünce, dini inanç gibi kişisel verilerinin ya da ırk, ahlaki eğilim, sağlık bilgisi ya da sendikal bilgisi gibi kişisel verilerinin hukuka aykırı şekilde kaydedilmesi halinde verilecek cezanın yarı oranında artırılacağı ifade edilmiştir. Bu düzenleme kişilik haklarına saldırı niteliği taşıyan[295] bu eylem tipleri önlenmek amacındadır.

Esasen 135.maddenin yukarıda yer verilen metni ile ilk kez 5237 sayılı Türk Ceza Kanunu'nda yer verilen metni arasında pek çok farklılık vardır. Nitekim süreç içerisinde hem madde metninin ilk halinin doktrinde eleştirilmesi hem de 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun yürürlüğe girmesi üzerine, madde metni üzerinde değişikliklere gidilmiştir. Kanımızca bu değişikliklerin tamamı yerinde ve gerekli değişikliklerdir. Dolayısıyla çalışmamızın bu bölümünde ilk olarak bu değişikliklerden bahsedilecektir.

---

[294] Karagülmez, **Bilişim Suçları**, s.227: Ayrıca bkz. Şaban Cankat Taşkın, **Bilişim Suçları**, Beta Basım, Kasım 2008, İstanbul, s. 97

[295] Murat Volkan Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku**, 6. Baskı, Ankara, Seçkin Yayınevi, Eylül 2015, s. 674. Murat Volkan Dülger, **Kişisel Verilerin Korunması Hukuku**, Hukuk Akademisi, Ocak 2019, İstanbul, s. 309

Öncelikle maddenin birinci fıkrasını ele alacak olursak, işbu maddenin birinci fıkrasında hukuka aykırı olarak kişisel verileri kaydeden[296] kişinin eylemi için öngörülen hapis cezasının miktarı 06 Mart 2014 tarihinde yürürlüğe giren 21 Şubat 2014 tarihli ve 6526 sayılı Terörle Mücadele Kanunu ve Ceza Muhakemesi Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun ile artırılarak, daha önce altı ay olan cezanın alt sınırı bir yıla çıkarılmıştır. Değişikliğe gerekçe olarak ise anayasanın 20. Maddesinde yer verilen herkesin kişisel verilerinin korunmasını talep etme hakkına sahip olduğuna ilişkin düzenleme gösterilmiştir. Kişisel verilerin ve özel hayatın daha etkin korunması amacıyla, kişisel verileri hukuka aykırı olarak kaydedenlere verilecek ceza artırılmaktadır." hususları belirtilmiştir.[297] Madde gerekçesinden de anlaşılacağı üzere Anayasamızın 20. Maddesine ek üçüncü fıkrayla, özel hayatın gizliliğinin korunması hakkı kapsamında kişisel verilerin korunması hakkı ceza kanunumuzda da temel bir hak olarak düzenlenmiş ve bu hakkın da daha etkin bir şekilde korunabilmesi ve caydırıcılığın artırılması amacıyla suç nedeniyle verilecek ceza artırılmıştır.[298]

Söz konusu Türk Ceza Kanunu'nun 135. Maddesinin ikinci fıkrası ise, 6698 sayılı Kişisel Verilerin Korunması Kanunun 30. Maddesiyle değiştirilmiştir.[299] Buna göre söz konusu değişiklikten önce maddenin ikinci fıkrasında "…*kişilerin siyasi,*

---

[296] Yargıtay da vermiş olduğu bir kararında, görülmekte olan bir ceza davasında sanığın üzerine atılı suçu işlediğinin ispatı için mahkemeye sunulan konuşma kayıtlarının, her ne kadar bu kayıtlar sanığın tehdit suçunu işlediğini ortaya koyar nitelikte olsa dahi, hukuka aykırı olarak elde edildiğini belirterek davaya katılanlar hakkında Türk Ceza Kanunu'nun 135. Maddesi uyarınca suç duyurunda bulunulmasının yerinde olduğunu ve davanın sonucu için bu suç duyurusu neticesinin beklenmesi gerektiğini ifade etmiştir. "*Mahkeme tarafından CD'nin çözümü yaptırılmış, görüşme detaylarında sair tehdit niteliğinde sözlerin sarf edildiği kabul edilmiş ve hükme esas alınmış ayrıca hukuka aykırı olarak kişisel verileri kaydeden katılan ve eşi hakkında TCK'nın 135/1 maddesi uyarınca suç duyurusunda bulunulmasına karar verilmiştir. Her ne kadar yerel mahkemece hüküm kurulmuş ise de, söz konusu CD'nin hukuka aykırı olarak elde edilmiş olması halinde hükme esas alınamayacağı ve dosyadaki mevcut diğer yasal delillere göre bir karar verilmesinin gerektiği gözetilerek, Cumhuriyet Başsavcılığı'na katılan ve eşi hakkında yapılan suç duyurusunun sonucu beklenip neticesine göre karar verilmesi gerektiği …*" Yargıtay 4. Ceza Dairesi'nin 2018/7276 E., 2018/21206 K. Ve 06.12.2018 T. Sayılı kararı.

[297] 6526 sayılı Terörle Mücadele Kanunu ve Ceza Muhakemesi Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun için bkz. (Çevrimiçi) https://www.tbmm.gov.tr/kanunlar/k6526.html (Erişim Tarihi: 01.10.2018)

[298] Metin Çokmutlu, **Türk Ceza Hukukunda Kişisel Verilerin Korunması,** Doktora Tezi, Kocaeli Üniversitesi Sosyal Bilimler Enstitüsü, 2014, s.173. Korkmaz, **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, s. 324.

[299] 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 30.Maddesi ile Türk Ceza Kanunu'nun 135.maddesinin 2.fıkrasında yer verilen "*Kişilerin*" ifadesi "*Kişisel verinin, kişilerin*" olarak; "*bilgileri kişisel veri olarak kaydeden kimse, yukarıdaki fıkra hükmüne göre cezalandırılır*" ifadesi ise "*olması durumunda birinci fıkra uyarınca verilecek ceza yarı oranında artırılır*" olarak değiştirilmiştir. Bkz,Kişisel Verilerin Korunması Kanunu (Çevrimiçi) https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf (Erişim Tarihi: 13.10.2018)

felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına ilişkin bilgileri kişisel veri olarak kaydeden…" ifadesi yer almaktaydı. 135. maddenin ikinci fıkrası yürürlükte olduğu süreçte eleştirilere konu olmuştur.[300] Doktrinde, hem 108 sayılı sözleşme hem de Kişisel Verilerin Korunmasına İlişkin Kanun Tasarısında bu veriler özel nitelikli veri olarak belirtilmelerine rağmen, 135.maddenin ikinci fıkrasının bu halinden, sanki bu fıkrada sayılan kişinin ahlâkî eğilimleri, siyasi, felsefi, dini, ırki verileri ile kişinin cinsel yaşamına, sağlık durumuna, sendikal bilgilerine ilişkin verilerinin aslen kişisel veri olmadığı yönünde bir anlam çıktığı, aksine bu verilerin kişisel veri olmaktan da öte özel nitelikli kişisel veri olduğu ve maddenin ilk fıkrasına kıyasla çok daha ağır cezayı gerektirdiği ve hata suçun nitelikli halleri arasında sayılması gerektiği belirtilmiştir. [301]

Yine maddenin ilk halinde ikinci fıkrada sayılan özel nitelikteki verilerin kaydedilmesi durumunda öngörülen ceza "*bilgileri kişisel veri olarak kaydeden kimse, yukarıdaki fıkra hükmüne göre cezalandırılır*" şeklinde düzenlenmişti. Özel nitelikli veriler için cezanın daha fazla olması gereği düşünüldüğünde, bu cezanın özel nitelikli olmayan verilerin kaydedilmesi halinde öngörülen ceza ile aynı olması da doktrinde eleştirilere konu olmuştur.[302]

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 30.maddesiyle yapılan değişiklik ile 135.maddenin eski ikinci fıkrasına getirilen iki eleştiri de ortadan kaldırılarak, madde metninin eski halinde yer alan "*kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına ilişkin bilgileri kişisel veri olarak kaydeden kimse*" ibaresi "*Kişisel verinin, kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması durumunda"* şeklinde değiştirilmiş; "*bilgileri kişisel veri olarak kaydeden kimse, yukarıdaki fıkra hükmüne göre cezalandırılır*" ibaresi ise "*olması durumunda birinci fıkra uyarınca verilecek ceza yarı oranında artırılır*"

---

[300] Çokmutlu bu konudaki görüşlerini, kişilerin siyasi ve dini verilerinin de kişisel veri olduğunu ve nedenle bu madde fıkrasının daha iyi kaleme alınması gerektiğini ifade ederek dile getirmiştir. Bkz. Çokmutlu, **Türk Ceza Hukukunda Kişisel Verilerin Korunması**, s.186.

[301] Veli Özer Özbek, **Yeni Türk Ceza Kanunu'nun Anlamı (TCK İzmir Şerhi),** Madde 76-169, C. II, Ankara, 2008, s.949 (Bundan sonra TCK İzmir Şerhi olarak anılacaktır)

[302] Korkmaz, **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, s. 325. Özbek, **Yeni Türk Ceza Kanunu'nun Anlamı (TCK İzmir Şerhi)**, s. 949

şeklinde değiştirilmiştir.[303] Söz konusu verilerin Kişisel Verilerin Korunması Kanunu ve pek çok uluslararası düzenlemede özel nitelikli veri olarak düzenlenmiş olduğu düşünüldüğünde, bu değişiklikler yerinde olmuştur. [304]

Değişiklik Yapan Kanun	**Değişen Metin- Eski TCK m.135/1**	**Değişen Metin-Yeni TCK m.135/1**
6526 sayılı Terörle Mücadele Kanunu ve Ceza Muhakemesi Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun	"*Hukuka aykırı olarak kişisel verileri kaydeden kimseye altı aydan üç yıla kadar hapis cezası verilir. "*	"*Hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir. "*
Değişiklik Yapan Kanun	**Değişen Metin- Eski TCK m.135/2**	**Değişen Metin-Yeni TCK m.135/2**
6698 sayılı Kişisel Verilerin Korunması Kanunu	"*Kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına ilişkin bilgileri kişisel veri olarak kaydeden kimse…"*	*"Kişisel verinin, kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması durumunda…"*
6698 sayılı Kişisel Verilerin Korunması Kanunu	*"…bilgileri kişisel veri olarak kaydeden kimse, yukarıdaki fıkra hükmüne göre cezalandırılır*"	"*…olması durumunda birinci fıkra uyarınca verilecek ceza yarı oranında artırılır*"

Tablo-1

Ancak bu noktada Türk Ceza Kanunu ile Kişisel Verilerin Korunması Kanunu birbirileriyle çelişmektedir. Kişisel Verilerin Korunması Kanunu'nda özel nitelikli verilere ilişkin yapılan düzenlemeye bakıldığında kanunun özel nitelikli kişisel verilerin işlenmesine ilişkin 6.maddesinde, Türk Ceza Kanunu'nun 135.maddesi kapsamında sayılan özel nitelikli verilerin genişletildiği görülecektir.

---

[303] Türk Ceza Kanunu'nun tam metni için bakınız. (Çevrimiçi) http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf (Erişim Tarihi: 13.10.2018)

[304] Özbek, **TCK İzmir Şerhi**, s.949

Buna göre Kişisel Verilerin Korunması 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 tedbirleriyle ilgili verileri ile biyometrik[305] ve genetik verileri' özel nitelikli veri olarak düzenlenmiştir. Oysa TCK'nın 135. Maddesinde özel nitelikli veri olarak yalnızca kişilerin 'siyasi, felsefi, dini, ırki köken, cinsel yaşam, sağlık, sendikal bilgilerine ve ahlaki eğilimlerine' ilişkin veriler sayılmıştır. Yine TCK'nın 135.maddesi kapsamında kişinin ahlaki eğilimleri özel nitelikli veri olarak sayılmışken, Kişisel Verilerin Korunması Kanunu'nun 6. maddesinde ise kişinin ahlaki değerleri özel nitelikli veri olarak sayılmamıştır.

Kişisel Verilerin Korunması Kanunu'nun ilgili 6. Maddesi Avrupa Birliği Genel Veri Koruma Tüzüğü'nün özel nitelikli verileri düzenleyen 9. Maddesi ve sair uluslararası düzenlemeler tam olarak uyumlu olduğu söylenemeyecektir. Zira Avrupa Birliği Genel Veri Koruma Tüzüğü'nün özel nitelikli verileri düzenleyen 9. Maddesinde kişinin ırki kökeni, siyasi düşüncesi, dini ve felsefi görüşü, sendikal üyelikleri, genetik datası veya biyometrik datası, sağlık, cinsel yaşam ve cinsel yönelimine ilişkin verileri özel nitelikli veri olarak tanımlanırken, kişinin ahlaki eğilimleri ve cinsel yönelime ilişkin verileri ise özel nitelikli veri olarak belirtilmemiştir.[306]

Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu arasındaki bu farklılığın giderilmesi gerektiği aşikardır. Nitekim Kişisel Verilerin Korunması Kanunu yürürlüğe girmeden önce verilmiş olan bir Anayasa Mahkemesi kararında

---

[305] Danıştay vermiş olduğu bir kararında yüz tarama ile mesai takip sisteminin özel hayatın gizliliği kapsamında olduğunu ve yasal dayanak olmadan bu sistemin uygulanmasını hukuka aykırı bulmuştur. Danıştay vermiş olduğu kararında yüz tanıma sisteminin bireyin özel hayatına ilişkin olduğunu, dava konusu işleme esaslarını gösteren hiçbir hukuki dayanak olmadığını, sistem ile elde edilen kişisel verilerin ileride ne şekilde kullanılacağına ilişkin alınmış bir önlemin ya da güvencenin olmadığını ve bu hali ile uygulamanın temel hak ve özgürlüklerle ve anayasa ile bağdaşmadığını ifade ederek, davayı reddeden mahkemenin kararını hukuka uygun bulmamıştır. Danıştay 11. Dairesi E. 2017/816, K. 2017/4906, T. 13.06.2017. Benzer yönde bir görüş için bkz. Aydın Akgül, "Kişisel Verilerin Korunması Bağlamında Biyometrik Yöntemlerin Kullanımı ve Danıştay Yaklaşımı", **Türkiye Barolar Birliği Dergisi**, Ankara, S.118, 2015, s. 211 Danıştay ilgili kararında personellerin mesai takibinde parmak izinin alınması, göz retinasının taranması gibi biyometrik yöntemlerin kullanımının, mesai sisteminin niteliği de dikkate alınarak amaçlanan kamu yararının elde edilemeyeceğini, bu iki değişken arasında bir orantılılık olmadığını ifade etmiştir. Danıştay bu noktada ölçülülük ilkesine uyulmadığını belirtmiştir.

[306] Avrupa Birliği Genel Veri Koruma Tüzüğü'nün tam metni, (Çevrimiçi) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL (Erişim tarihi: 13.08.2018)

biyometrik verinin muhakkak kişisel veri olduğu ancak özel nitelikli kişisel veri kapsamında sayılamayacağı belirtilmiştir.[307] Görüldüğü üzere gerek Türk Ceza Kanunu'nda özel nitelikli veri kategorileri bakımından mevcut eksiklikler, gerek ise kanunlar arasındaki lafzi farklılıklar uygulamada bu gibi kanaatimizce yanlış olan yorumlamalara sebebiyet vermekte olup, Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu arasındaki bu farklılığın giderilmesi uygulamada sorunlara sebebiyet vermemesi adına önemlidir. [308] Nitekim doktrinde bazı yazarlar, Türk Ceza Kanunu ve Kişisel Verilerin Korunması Kanunu arasındaki bu farktan ötürü, Türk Ceza Kanunu kapsamında yer verilmeyen özel nitelik hassas verilerin hukuka aykırı olarak kaydedilmeleri halinde 135. Maddenin özel nitelikli hassas verilere ilişkin fıkrasının değil genel nitelikli kişisel verilerin işlenmesine ilişkin birinci fıkranın uygulanmasının kanunilik ilkesinin bir gereği olduğunu ifade etmişlerdir. [309]

Burada bir diğer önemli nokta ise yasa koyucunun kişisel verinin kişinin ahlaki eğilimlerine, cinsel yaşamına, sağlık durumuna veya sendikal bağlantılarına ilişkin olması halinde bu verilerin kaydı ve işlenmesi için hukuka aykırılık unsurunu şart olarak aramasıdır.

Madde metni dikkate alındığında yasa koyucunun kişilerin siyasi, felsefi, dini görüşü ve ırki kökeni gibi mutlak korunması gereken verilerinin kaydı ya da işlenmesi için hukuka aykırılık unsuru aramamış olmasındaki amacın, mutlak korunması gereken verilerin kaydı ya da işlenmesine ilişkin bir hukuk kuralı yaratılmasının da önüne geçmek olduğunu söyleyebiliriz. Bu demektir ki, söz konusu verilerin kaydedilmesine yönelik herhangi bir işlem her ne şart altında olursa olsun hukuka aykırı olarak ifade edilmiştir.

---

[307] Dülger, "**Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması**", s. 109-110. Dülger konuya ilişkin makalesinde Anayasa Mahkemesi'nin biyometrik yöntemlerle kimlik doğrulamasının kişisel veri olmadığını ifade ettiğini belirtse de esasen Mahkeme bu kararında biyometrik verilerin de özel nitelikli hassas verilerden olduğunu ancak 108 sayılı sözleşmenin özel nitelikli hassas verileri düzenleyen 6. maddesinde yer verilen politik düşünce, siyasi görüş ya da din, ırk gibi çok hassas verilerden olmadığını ifade etmiştir. AYM kararı için bkz. AYM, 19.03.2015, E.2014/180, K.2015/30, R.G.03.04.2015-29315. (Çevrimiçi) http://www.resmigazete.gov.tr/eskiler/2015/04/20150403-8.pdf (Erişim Tarihi 10.10.2018)

[308] Küzeci konuyu şöyle değerlendirmiştir: "TCK'nın *madde gerekçesinde bazı veri kategorilerinin ikinci fıkrada ayrıca düzenlenmesinin nedeni açıklanmamıştır. Ancak bu kategorilerin gerekçede de atıf yapılan AK Sözleşmesinde de düzenlendiği dikkate alındığında, bu tercihin nedeninin özel nitelikli kişisel verileri TCK açısından da ayrı bir düzenlemeye tabi tutmak olduğu düşünülebilir."* Küzeci, **Kişisel Verilerin Korunması**, 2010, s. 405

[309] Korkmaz, **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, s.336

Ancak yukarıda da belirttiğimiz üzere aynı maddenin devamında kişilerin ahlaki yönelimlerine, cinsel hayatlarına, sağlıklarına veya sendikal bilgilerine ilişkin verilerin ise hukuka aykırı olarak kaydedilmesi halinde söz konusu eylemin suç teşkil edeceğine ilişkin düzenleme getirilmiştir. Bu haliyle yasa koyucu bahsi geçen verilerin kaydedilebilmesi için açıkça hukuki bir yol açmıştır. Bu durumda söz konusu verilerin kaydı veya işlenmesi kanunlarda öngörülen bir düzenlemeden kaynaklanıyorsa bu verilerin kaydı ya da işlenmesi hukuka uygunluk kazanacaktır. Kanunun gerekçesinde de bu durum, söz konusu verilerin kaydedilmesine suçla mücadele kapsamında belirli ölçüde olmak üzere kanunlarda izin verilebileceği şeklinde belirtilmiştir. Kanımızca bu düzenleme, kişinin ahlaki eğilimleri, cinsel yaşamı, sağlık durumu veya sendikal bağlantıları gibi verilerin niteliği düşünüldüğünde yerinde olmamıştır. Zira kanun gerekçesinde belirtilen suçlulukla mücadele zemininde ahlaki eğilime, cinsel yönelime, sendikal bağlantıya ilişkin verilerin nasıl bir suça konu olacağı tarafımızca anlaşılamamıştır. Kanımızca kişilerin özel hayatının merkezinde olan cinsel yaşam, ahlaki eğilimler ve sendikal verileri gibi verilerin, sağlık verilerinin kamu sağlığı gereğince kayda alınması gereğini bir kenarda tutarak, tıpkı maddenin ilk kısmında belirtilen siyasi, felsefi, dini görüş ve ırkı köken verisi gibi mutlak şekilde korunması gerekirdi. Bu husus doktrinde de eleştirilere neden olmuştur. [310]

Nitekim hem 95/46/EC sayılı Veri Koruma Direktifi hem de onu mülga hale getiren Avrupa Birliği Genel Veri Koruma Tüzüğü'nde de benzer bir düzenlemenin olduğu görülecektir. Buna göre söz konusu uluslararası düzenlemelerde de kişinin ırki kökeni, siyasi düşüncesi, dini ve felsefi görüşü, sendikal üyelikleri, genetik datası veya biyometrik datası, sağlık, cinsel yaşam ve cinsel yönelimine ilişkin verileri özel nitelikli veri kategorisinde toplanmış ve bu verilerin kaydedilmesi hukuka aykırı kabul edilmiş ve aynı maddenin ikinci fıkrasında kişinin açık rızasının bulunması halinde söz konusu yasağın uygulanmayabileceği ifade edilmiştir. [311]

---

[310] Küzeci, **Kişisel Verilerin Korunması**, 2010, s. 288. Küzeci konuyu değerlendirirken madde metninde yer verilen hukuka aykırılık ayrımını vurgulamış ve bu ayrım ile yasa koyucunun bazı türden bilgiler için hukuka aykırılık ararken bazı türden bilgiler için ise her şartta suçun oluşacağına ilişkin düzenleme ile bazı türden bilgileri özel nitelikte gördüğünü ve dolayısıyla farklı bir düzenlemeye tabi tuttuğunu ifade etmiştir. Küzeci yasa koyucunun bu ayrımı eleştiren yazarlardan biri olarak özellikle kamu kuruşlarının bu tipteki bilgiler kişisel verilerin kaydından nasıl bir kamu yararı sağlayacaklarına anlam veremediğini ve bu gibi bilgilere karşı esasen devletin ve yönetimin kayıtsız ve adeta gözleri kapalı şekilde hareket etmesi gerektiğini ifade etmiştir.

[311] Bkz., Avrupa Birliği Genel Veri Koruma Tüzüğü'nün tam metni, (Çevrimiçi) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL (Erişim tarihi: 14.08.18)

Diğer yandan Kişisel Verilerin Korunması Kanunu'nun 6. Maddesi ile uluslararası mevzuata görece uygun bir düzenleme yapılmış ve ancak bir kez daha Türk Ceza Kanunu ve Kişisel Verilerin Korunması Kanunu arasında farklılık ortaya çıkmıştır. İlgili 6.maddeye göre bu madde kapsamında sayılan tüm özel nitelikli veriler mutlak olarak korunmak durumunda olup, Türk Ceza Kanunu'nda olduğu üzere bir 'hukuka aykırılık' ayrımına gidilmemiştir. Ancak hemen akabinde madde metninin 2. ve 3. fıkralarında özel nitelikli kişisel verilerin işlenebileceği haller düzenlenmiştir.

Buna göre maddenin ikinci fıkrası kapsamında kişilerin rızası olması halinde bahsi geçen veriler işlenebilecektir. Bu düzenleme bu yönüyle yine uluslararası mevzuata uygun olmuştur. Zira kişinin kendi rızası ile siyasi düşüncesini, dini inançlarını ya da cinsel kimliğini ve benzeri verilerini ortaya koymasının kişinin ifade özgürlüğü kapsamında olduğu da tartışmasızdır. Kaldı ki, kişinin rızası ilgili başlık altında da ayrıntılı olarak inceleneceği üzere, Türk Ceza Kanunu'nda yer alan ilgili suç tipleri bakımından da bir hukuka uygunluk sebebidir.

Diğer yandan maddenin üçüncü fıkrası kapsamında ise bu madde kapsamında sayılan özel nitelikli verilerden sağlık ve cinsel hayat dışındaki tüm verilerin kanunlar da öngörülmesi halinde kişinin rızasına ihtiyaç olmaksızın işlenebileceği; diğer yandan sağlık ve cinsel hayata ilişkin verilerin ise yalnızca halk sağlığı, koruyucu hekimlik, teşhis, tedavi ve bakım servislerinin idaresi, sağlık hizmetleri ile bu hizmetlerin mali koşullarının planlanması ve idaresi amacıyla işlenebileceği düzenlenmiştir. Ayrıca bu veriler ancak sır saklama konusunda yükümlülüğü bulunan kişiler tarafından ya da yetkili kurum ve kuruluşlar tarafından işlenebilecektir.

Aşağıda yer vermiş olduğumuz tablo yukarıda özetlediğimiz maddelerin özetlenmesi bakımından sunulmuştur.

	Özel Nitelikli Veriler	**Açıklama**
5237 sayılı Türk Ceza Kanunu	Siyasi, Felsefi veya Dini Görüşlere, Irki Kökenlere ilişkin kişisel veriler	Kişinin rızasının olması hukuka uygunluk sebebidir.

5237 sayılı Türk Ceza Kanunu	Ahlaki eğilimlere, cinsel yaşama, sağlık durumuna veya sendikal bağlantılara ilişkin kişisel veriler	İşlenmeleri halinde suç oluşması için özel olarak hukuka aykırılık aranan kişisel verilerdir. Kişinin rızasının olması hukuka uygunluk sebebidir.
6698 sayılı Kişisel Verilerin Korunması Kanunu	Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri	Kanunlarda öngörülmesi halinde bu verilerin işlenmesi mümkündür. Kişinin rızasının olması halinde bu verilerin işlenmesi mümkündür.
6698 sayılı Kişisel Verilerin Korunması Kanunu	Sağlık ve cinsel hayata ilişkin veriler,	Kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla kişinin rızası olmadan işlenebileceklerdir. Kişinin rızasının olması halinde bu verilerin işlenmesi mümkündür.

Tablo 2

Sonuç olarak tüm eksikliklere, eleştirilere ve giderilmesi gereken karışıklıklara rağmen bu suç tipi ile anayasanın yirminci ve devamı maddeleri ile Avrupa İnsan Hakları Sözleşmesi'nin sekizinci maddesinde tanınan özel hayat ve aile hayatı hakkının tecavüzlere karşı güvencesi sağlanmaya çalışılmış ve ayrıca Avrupa Konseyi bünyesinde hazırlanan Türkiye'nin de taraf olduğu 108 sayılı sözleşmenin ilgili hükümleri de bir anlamda uygulamaya konulmuştur.[312]

[312] Ali Parlar, Muzaffer Hatipoğlu, **Türk Ceza Kanunu Yorumu**, Seçkin Yayıncılık, 2.Bası, 2008, s. 2043

2. Suçla Korunan Hukuksal Değer

Kişisel verilerin kaydedilmesi suç tipi Türk Ceza Kanunu'nun 'Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar' başlıklı dokuzuncu bölümünde ve 135. Madde kapsamında düzenlenmiştir.

Doktrinde bazı yazarlar bu suç ile korunan hukuksal değerin doğrudan 'özel hayat' olduğunu ifade etmektedir.[313] Diğer yandan bazı görüşler ise bu suç ile korunan hukuksak değerin başta özel hayatın gizliliği olmak üzere aynı zamanda özel olarak ise kişisel verilerin gizliliği ya da kişisel verilerin korunması hakkı olduğunu ifade etmektedirler.[314] Bu yazarların bazılarına göre ayrıca bu suç kapsamında kişisel verinin niteliğine göre korunan hukuksal değer de değişecektir.[315] Yukarıdaki açıklamalarımızdan da anlaşılabileceği üzere kanaatimizce bu suç tipi ile korunmak istenen hukuki yarar temel hak ve özgürlükler kapsamında genel olarak özel hayata saygı ve özel olarak ise kişisel verilerin korunması hakkıdır. Nitekim Yargıtay Ceza Genel Kurulu da konu hakkında vermiş olduğu bir kararında, bu suç tipleri ile korunan hukuki değer konusunda benzer yönde bir görüş bildirmiştir. [316]

Doktrinde bu suç kapsamında korunan hukuki değer konusunda, 765 sayılı kanuna atıfla sırrın dokunulmazlığı olup olmadığı sorusu sorulsa da bir kişisel verinin kişinin sırrına ilişkin olması söz konusu olabilecekse de her kişisel verinin bir sır kapsamında olduğunu söylemek doğru olmayacaktır. Örneğin bir kişinin vatandaşlık numarası, o kişinin kişisel verisi olmasına rağmen, bir sır niteliğinde değildir. Bu durumda suç kapsamında korunan değerin sırrın dokunulmazlığı olduğunu söyleyemeyiz. [317]

---

[313] Veli Özer Özbek, Koray Doğan, Pınar Bacaksız, İlker Tepe, **Türk Ceza Hukuku Özel Hükümler**, Seçkin Yayınevi, 12. Bası, Ankara, Eylül 2017, s.569. Özbek, **TCK İzmir Şerhi**, s. 948. Ayrıca bkz. Karagülmez, **Bilişim Suçları**, s.230

[314] Taşkın, **Bilişim Suçları**, s. 98. Ayrıca bkz. Kuşkonmaz, **Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması**, s. 675. Dülger, **Kişisel Verilerin Korunması Hukuku**, s. 313

[315] Dülger, **Bilişim Suçları**, s. 676 Dülger konuyla ilgili olarak "*Örneğin bireyin sağlık durumuna ilişkin bir verinin bu suçların konusunu oluşturması halinde korunan hukuksal değeri kişinin sağlık hakkı oluşturacaktır*" şeklinde ifade etmiştir. Dülger, **Kişisel Verilerin Korunması Hukuku**, s. 313

[316] Yargıtay bu kararında hem 135. madde hem de 136. madde bakımından korunan hukuki yararın genel olarak özel hayatın korunması ve genel olarak ise kişisel verilerin korunması olduğunu belirtmiştir. Yargıtay Ceza Genel Kurulu, Esas No: 2012/12-1510 Karar No: 2014/331 Karar Tarihi.17.06.2014

[317] Dülger, **Kişisel Verilerin Korunması Hukuku**, s. 311

3. Suçun Unsurları

a. Maddi Unsurlar

aa. Fail

Türk Ceza Kanunu'nun kişisel verilerin kaydedilmesi başlıklı 135. maddesinde kişisel verileri hukuka aykırı şekilde kaydeden kimsenin maddede öngörülen ceza miktarı uyarınca cezalandırılacağı ifade edilmiştir. Buna göre madde metninden de anlaşılabileceği üzere herkes söz konusu suçun faili olabilecektir.[318]

Diğer yandan ise kanunun 137. maddesinde suçun nitelikli halleri düzenlenmiş ve bu suçun kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanarak ya da belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenmesi halinde, verilecek cezanın yarı oranında artırılacağı ifade edilmiştir. Bu anlamda suçun nitelikli halleri dikkate alındığında, kişisel verileri kaydetme suçunun yalnızca bu haller çerçevesinde görünüşte özgü suç[319] olduğunu söylemek yanlış olmayacaktır.[320]

bb. Mağdur

Türk Ceza Kanunu'nun 135.maddesinde düzenlenen kişisel verilerin kaydedilmesi suçu bakımından suçun mağduru herkes olabilir.[321] Suçun mağduru olmakla ilgili özel bir düzenleme yer almamaktadır.[322] Buradan anlaşılmaktadır ki, söz konusu suçun mağduru tüm gerçek kişiler olabilecektir. Doktrinde bazı görüşler bu suçun mağdurunun tüzel kişiler de olabileceğini belirtmekte ise de, bu görüşe katılmak mümkün değildir. Nitekim kişisel verinin gerçek kişilere ait veriler olduğunu daha

---

[318] Köksal Bayraktar v. dğr., **Özel Ceza Hukuku**, Cilt:3, 1.Baskı, İstanbul, On İki Levha Yayıncılık, Mart 2018, s.635. Çokmutlu**, Türk Ceza Hukukunda Kişisel Verilerin Korunması,** s.183. Korkmaz, **Türk Ceza Hukukunda Kişisel Verilerin Korunması**, s.337. Karagülmez, **Bilişim Suçları**, s.236. Yaşar, Gökcan, Artuç, **Yorumlu Uygulamalı Türk Ceza Kanunu**, s.4433. Dülger, **Bilişim Suçları**, s.677. Dülger, **Kişisel Verilerin Korunması Hukuku**, s. 314. Doğan, Bacaksız, Tepe, Özbek, **Türk Ceza Hukuku Özel Hükümler**, s. 574

[319] Türk Ceza Kanunu'nun '40.maddesinin 2.fıkrasına göre ancak özel fail niteliklerini barındıran kişi tarafından işlenebilecek suçlara özgü suç denilmektedir.

[320] Korkmaz, **Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması**, s.337. Ayrıca bkz. Melike Köse Aysun, **Kişisel Verilerin Kaydedilmesi Suçu,** Akdeniz Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, s.95

[321] Dülger, **Kişisel Verilerin Korunması Hukuku**, s. 314

[322] Özbek, TCK İzmir Şerhi, s. 950. Ayrıca bkz. Yaşar, Gökcan, Artuç, **Yorumlu Uygulamalı Türk Ceza Kanunu**, s 4433. Ayrıca bkz. Parlar, Hatipoğlu, **Türk Ceza Kanunu Yorumu,** s.2043. Karagülmez, **Bilişim Suçları**, s.236.

evvel ayrıntılı olarak incelemiştik. Bu durumda tüzel kişiler ancak suçtan zarar gören statüsünde yer alabileceklerdir.[323]

Nitekim yukarıda ayrıntılı olarak açıkladığımız üzere 6698 sayılı Kişisel Verilerin Korunması Kanunu'na göre, kişisel verileri işleme tabi tutulan tüm gerçek kişiler ilgili kişi olarak ve gerçek kişilere ait olan ve bu kişilerin kimliğini belirli ya da belirlenebilir hale getiren her türlü bilgi de kişisel veridir. Burada önemli bir nokta, bu suçun mağduru olmak için bahsi geçen verilerin *zilyedi ya da maliki* olunmasının şart olup olmadığıdır. Doktrinde bu konuda farklı görüşler bulunmaktadır. Bu görüşlerden birine göre kişiye ait verilerin bir şekilde hukuka aykırı olarak işlenmesi halinde bu suç işlenmiş sayılacak ve verileri işlenen gerçek kişi bu suçun mağduru sıfatını alacaktır, kişinin bu verilerin zilyedi ya da maliki olup olmadığı önemli değildir.[324] Aksi yöndeki görüşe göre ise bu suçun mağduru ancak kişisel verilerin zilyedi ya da maliki olacaktır.[325] Bizim görüşümüz de bu suçun mağdurunun kişisel verilerin zilyedi ya da maliki olmak zorunda olmadığı yönündedir. Zira çalışmamızın birinci bölümünde de kişisel verilerin korunması hakkına yaklaşımlar çerçevesinde, mülkiyet hakkı yaklaşımını kabul etmediğimizi ifade etmiştik.

Örneğin bir kişinin kişisel verileri, gerçek ya da tüzel kişi veri sorumlusu tarafından hukuka uygun şekilde işlendikten sonra, 3. kişiler tarafından hukuka aykırı olarak elde edilir, verilir ya da yayılırsa bu durumda elbette bundan esas zarar görecek olan kişisel verileri işleyen veri sorumlusu değil kişisel verileri hukuka aykırı olarak verilen, yayılan ya da ele geçirilen kişi olacaktır. Bu durumda kişisel verilerin zilyedi ya da maliki olmamakla beraber suçun mağduru olacaktır.

Bu haliyle mevcut madde uluslararası düzenlemelere de uygun olmuştur. Nitekim çalışmamızın daha önceki bölümlerinde ayrıntılı olarak ifade ettiğimiz üzere uluslararası düzenlemeler kapsamında da kişisel verilerin korunması hususunda

---

[323] Dülger, **Kişisel Verilerin Korunması Hukuku**, s. 314

[324] Dülger, **Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması**, s. 123. "*Esasen verilerin maliki her zaman ilgili olduğu bireylerdir. BU noktada belirtilmek istenen verilerin tutulduğu, saklandığı veya kaydedildiği fiziksel veya otomatik alanın mutlaka veri ilgilisine ait olmaması gerektiğidir...Kişisel veri her nerde ve ne şekilde olursa olsun ilgili olduğu kişiye aittir ve yasal korumalardan faydalanabilmektedir. Dolayısıyla suçun mağduru olmak kişisel verilerin kaydedildiği alanın maliki olunmasını gerektirmez bizatihi kişisel verinin ilgili olmak mağdur sıfatını haiz olmak için yeterlidir.*" Dülger, **Kişisel Verilerin Korunması Hukuku**, s. 314

[325] Taşkın, **Bilişim Suçları**, s.106.

yalnızca kişisel verilerin kimliği belirli ya da belirlenebilir gerçek kişiye ait veriler olarak ifade edilmiştir. Bu anlamda tüzel kişiler bu suçun mağduru sıfatını alamayacaklardır. [326] Diğer yandan, Türk Medeni Kanunu'nun 28. maddesine göre kişiliğin sona ermesi ölüme bağlı olduğundan, kişinin ölmesi halinde bu suçun artık bu kişiye karşı kişilik hakları zedelenmek suretiyle işlenmesi mümkün olmayacaktır. [327]

cc. Suçun Konusu

Türk Ceza Kanunu'nun 135.maddesinde düzenlenen suç tipinin konusu kişisel verilerdir.[328] İlgili maddenin gerekçesinde kişisel verinin tanımına ilişkin olarak, *gerçek kişi ile ilgili her türlü bilgi kişisel veri olarak kabul edilecektir* şeklinde açıklamada bulunulmuştur.[329] Öğretide de çoğunluk görüş kişisel verilerin korunmasına ilişkin suç tiplerinin konusunu yalnızca gerçek kişilerin verilerinin oluşturduğu ve kişisel verinin de gerçek kişiye ait olan ve bu gerçek kişinin geleceğini belirleme hakkının bulunduğu veriler olduğu yönündedir. [330] Buna rağmen kanun metninde kişisel verinin ne olduğuna ilişkin bir tanım bulunmamaktadır.

Ulusal mevzuat bakımından, kişisel verinin ne olduğu konusunda Ceza Muhakemesi Kanununun ilgili hükümleri de dikkate alınmıştır. Kanunun 81.maddesinin birinci fıkrasında sayılan "*kişinin fotoğrafı, beden ölçüleri, parmak ve avuç içi izi, bedeninde yer almış olup teşhisini kolaylaştıracak diğer özellikleri ile sesi ve görüntüleri*" ile 78 – 80. Maddelere göre "*moleküler genetik inceleme sonucu"*, 75-76.maddelere göre "*beden muayenesi ve/veya vücuttan örnek alınması suretiyle elde edilen*" veriler ve 135.maddeye göre "*kayda alınan telekomünikasyon yoluyla iletişim*" gibi.[331] Türk Ceza Kanunu'nda kişisel verinin tanımı ya da en azından bu kavramdan

---

[326] Aysun, **Kişisel Verilerin Kaydedilmesi Suçu**, s.95. Aksi yönde görüş için bkz. Taşkın, **Bilişim Suçları**, s.106

[327] Korkmaz, **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, s.337

[328] Dülger, **Bilişim Suçları**, s.678. Dülger, **Kişisel Verilerin Korunması Hukuku**, s. 314. Özbek, **TCK İzmir Şerhi**, s. 948. Osman Yaşar, Hasan Tahsin Gökcan, Mustafa Artuç, **Yorumlu İçtihatlı Türk Ceza Kanunu**, Cilt Sayı 6, Baskı Sayı 2, Ankara, Adalet Yayınevi, Ocak 2014, Cilt No. 3, s. 4433, Parlar - Hatipoğlu, **Türk Ceza Kanunu Yorumu,** s. 2043

[329] Ali Nevzat Açıkgöz, Gerekçeli – Karşılaştırmalı ve Açıklamalı Yeni Türk Ceza Kanunu**,** s.304 (Çevrimiçi) www.ceza-bb.adalet.gov.tr/makale/187.doc. (Erişim Tarihi: 10.09.2018). Ayrıca Türk Ceza Kanunu Madde Gerekçeleri Tam Metni için bkz. (Çevrimiçi) www.ceza-bb.adalet.gov.tr/mevzuat/maddegerekce.doc (Erişim Tarihi: 10.09.2018).

[330] Özbek, **TCK İzmir Şerhi**, s.950. Özbek, Doğan, Bacaksız, Tepe, **Türk Ceza Hukuku Özel Hükümler**, s. 570

[331] Özbek, **TCK İzmir Şerhi**, s. 948.

ne anlaşılması gerektiği konusunda bir netlik bulunmayışı doktrinde görüş ayrılıklarına sebebiyet vermiştir. Buna göre, kanunda kişisel verinin tanımının yapılmamış olması, bazı yazarlar tarafından kanunilik ilkesine aykırı bulunurken,[332] bazı yazarlar tarafından ise bu tanımın yapılmasının öğretiye bırakılması doğal karşılanmıştır.[333]

Bu noktada Yargıtay ve Anayasa Mahkemesi de konu bakımından farklı görüşler ifade etmişlerdir. Anayasa Mahkemesi konu ile ilgili olarak vermiş olduğu bir kararında kişisel verinin tanımının öğreti ve uygulamaya bırakılmasını yerinde bulmuştur.[334]

Anayasa Mahkemesi söz konusu kararında Batman 2.Asliye Ceza Mahkemesi tarafından 26.9.2004 tarihli ve 5237 sayılı Türk Ceza Kanunu'nun, 21.2.2014 tarihli ve 6526 sayılı Kanun'un 4. maddesiyle değişik 136. maddesinin (1) numaralı fıkrasının, Anayasa'nın 38. maddesine aykırılığı ileri sürülerek iptaline karar verilmesi talebini, zaman geçtikçe ve teknoloji ilerledikçe kişisel veri kavramının da değiştiği, Yasakoyucunun bunu önceden sürekli olarak öngöremeyeceği, bu kavramın açıklanmasına ilişkin olarak bazı yargı kararlarında ve içtihatlarda tanıma yer verildiği ve genel anlamda ortak bir ifadenin kabul edildiği ve zamanla bu kabulün de değişeceği, bu nedenle itiraza konu kuralın belirsiz olmadığı gerekçeleriyle, bu belirsizliğin suçta ve cezada kanunilik ilkesine aykırılık teşkil etmediğini ifade etmiştir. Görüldüğü üzere Anayasa Mahkemesi de Ceza Kanununda kişisel verinin tanımının yapılmamış olmasını kanunilik ilkesine aykırı görmemiştir.

---

[332] Ersan Şen konuyu şöyle değerlendirmiştir. **"***Kanunda kişisel verinin tanımının yapılmamış olması kanunilik ilkesine aykırıdır.*" Ersan Şen, **Yeni Türk Ceza Kanunu'nun Yorumu**, Vedat Yayıncılık, İstanbul, 2006, s.601.Taşkın'a göre ise TCK'da kişisel verinin tanımının yapılmamış olması, uygulamada kişisel verinin ne olduğu konusunda uygulamada sıkıntılara ve adaletsizliklere yol açacaktır. Taşkın, **Bilişim Suçları**, s. 101.
Yaşar – Gökcan - Artuç ise konu hakkında "*…ceza hukukunda bir suçun tanımının bu kadar geniş olması da önceden öngörülemeyen olumsuz sonuçlar doğuracağı pek tabidir.*" şeklinde ifade etmişlerdir. Yaşar – Gökcan – Artuç, **Yorumlu İçtihatlı Türk Ceza Kanunu**, s.4433

[333] Özbek konuyu şöyle değerlendirmiştir. "*...yasa koyucunun bazı kavramları tanımlamayıp içeriğinden ne anlaşılması gerektiğini öğreti ve uygulamaya bırakması doğal karşılanmalıdır...*" Özbek, **TCK İzmir Şerhi**, s. 948. Özbek, Doğan, Bacaksız, Tepe, **Türk Ceza Hukuku Özel Hükümler**, s.569. Doğan, Bacaksız, Tepe, Özbek' de ceza hukukunda yorumun serbest kıyasın yasak olduğunu, bu bakımından kişisel veri tanımının yapılmamış olmasının olağan olduğunu ifade etmişlerdir.

[334] Anayasa Mahkemesinin ilgili kararı için bkz. 2015/32 E. ve 2015/102 K. Sayılı 12.11.2015 T. Kararı Resmî Gazete Tarihi:02.12.2015 (Çevrimiçi)http://www.resmigazete.gov.tr/eskiler/2015/12/20151202-16.pdf (Erişim Tarihi:10.09.2018)

Diğer yandan Yargıtay ise, Türk Ceza Kanunu'nda kişisel verinin tanımının da içinde bulunduğu kişisel verilerin korunmasına ilişkin çerçeve niteliğinde bir kanun olmayışını kararlarında eleştiriye tabi tutmuştur.[335] Esasen uygulamada karar merci olarak görev yapan Yargıtay'ın kişisel verilerin korunmasına ilişkin çerçeve niteliğinde bir yasanın olmaması sebebiyle her somut olayda uygulama bakımından sorun ile karşılaştığı göz önünde bulundurulduğunda, Yargıtay'ın tutumu anlaşılabilecektir. Nitekim bu durum Yargıtay için son derece problemli bir alan olduğundan, Yargıtay Ceza Genel Kurulu bir kararında öğreti görüşleri doğrultusunda somut olaylar üzerinde uygulayabileceği bir kişisel veriler tasnifi ve tanımı dahi yapmaya çalışmıştır.[336]

6698 sayılı Kişisel Verilerin Korunmasına İlişkin Kanun yürürlüğe girene kadar, kanundaki kişisel verinin tanımına ilişkin bu boşluk kişisel verilerin korunmasına ilişkin uluslararası düzenlemelerde yer alan tanım vasıtasıyla giderilmeye çalışılmıştır. Bunlarda biri de 108 sayılı "Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme olup, madde gerekçesinde söz konusu suç tanımı ile işbu sözleşmeye geçerlilik kazandırıldığı ifade edilmiştir. Aynı doğrultuda her ne kadar bu ifade yalnızca 135. Maddenin gerekçesinde belirtilmiş olsa da konuya ilişkin diğer suç tipleri için de 108 sayılı sözleşmenin dikkate alındığı kabul edilmelidir[337].

---

[335] Yargıtay'ın ilgili kararında bugüne değin kişisel verinin tanımını ya da nelerin kişisel veri olduğunu gösteren bir kanun çıkarılmadığından, 135 ve 136. Maddede düzenlenen suçları eksik norm olarak nitelendirmiştir. Yargıtay bu kararında Kişisel Verilerin Korunma Kanunu Tasarısına atıf yapmış ve belki bu kanun ile çerçeve bir düzenleme yapılabileceğini ifade ettikten sonra doktrinde kişisel verinin tanımına ilişkin bazı belirlemeler olduğunu ancak her türlü kişisel verinin ceza normlarıyla korunamayacağını bir de hayatın özel alanına giren kişisel verilerin de ayrıca korunması gerektiğini belirterek yine o dönem yürürlükte olmayan tasarı halindeki KVKK'ya atıf yapmıştır. YCGK 2012/1510E, 2014/331K, 17.06.2014T

[336] Yargıtay ilgili kararında kişisel verilerin tanıma ilişkin bir değerlendirme yapmaya çalışmış ve noktada kişisel verileri bazı başlıklar altında sınıflandırmıştır. Yargıtay kişisel verileri hayat şekline göre veriler, kişinin mali durumuna ilişkin veriler, bilişim alanındaki veriler, sağlık verileri, politik veriler şeklinde sınıflandırmıştır. Yargıtay hayat şekli kapsamındaki kişisel verilere örnek olarak bireylerin cinsel yönelimlerini, etnik kökenlerini, varsa ceza mahkumiyetleri geçmişini göstermiştir. Mali duruma ilişkin veriler için ise kişinin yaptığı alışverişler, kredi kartı bilgileri, hisseleri gibi hisselerinden bahsetmiştir. Bilişim alanındaki veriler için ise e-postalar, kişinin internet alanındaki izleri, internet ortamında kişinin paylaştığı verileri örnek olarak işaret etmiştir. Yargıtay'a göre sağlık verileri için ise kişinin biyometrik verileri, toplum içindeki konumu etkileyen veriler, sigorta verileri gibi verileri ve politik veriler ise bilinmesi halinde topluma ayrımcılığa sebep olabilecek nitelikteki kişinin politik görüşüne, siyasi tutumuna ilişkin verileridir. Yargıtay Ceza Genel Kurulu 2012/1510E, 2014/331K, 17.06.2014T kararı

[337] Küzeci, **Kişisel Verilerin Korunması**, 2018, s. 287.

Bunun dışında kalan yani kişisel veri olma özelliğini taşımayan veriler ise Türk Ceza Kanunu'nun ilgili başka hükümlerinde koruma altına alınmışlardır. Buna örnek olarak Türk Ceza Kanunu'nun bankacılık sırları, ticari sırları, müşteri sırları niteliğindeki dokümanların açıklanması başlıklı 239. Maddesini örnek olarak verilebilir. Nitekim bu maddede kişisel veriler değil ticari sır niteliğindeki verilerin korunması düzenlenmiştir.[338] Nitekim uluslararası düzenlemelere de baktığımızda hem 95/46/EC Veri Koruma Direktifi'nde hem de bunu yürürlükten kaldıran Avrupa Genel Veri Koruma Tüzüğü'nde de kişisel verilerin yalnızca gerçek kişilere ait veriler olduğu belirtilmiştir. [339] Öğretide de azınlık olan bazı yazarlar, gerçek kişilerin yanında tüzel kişilere ait verilerin de kişisel veri olduğunu ve dolayısıyla kişisel verilerin kaydedilmesi suçunun konusunu teşkil ettiğini savunmaktadırlar.[340] Elbette doktrindeki bu tartışmalar 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun yürürlüğe girmesiyle son bulmuştur nitekim bu kanunda uluslararası pek çok düzenleme ile uyumlu olarak kişisel verilerin yalnızca gerçek kişilere ait veriler olduğu açıkça belirtilmiştir.

dd. Hareket ve Netice

Türk Ceza Kanunu'nun 135. maddesiyle düzenlenen suçun hareket unsuru kişisel verilerin hukuka aykırı olarak kaydedilmesidir.[341] Buna göre suçun oluşması için kişisel verilerin hukuka aykırı olarak kaydedilmesi yeterlidir. Bu noktada hukuka

---

[338] **İbid.**

[339] 95/46/EC Veri Koruma Direktifinde kişisel veri doğrudan ya da dolaylı olarak kimliği belirli veya belirlenebilir gerçek kişiyle ilgili her türlü bilgi; kimlik numarası, kişinin fiziksel, psikolojik, metal, ekonomik, kültürel veya sosyal kimliği gibi kişinin doğrudan ya da dolaylı olarak kimliğinin belirlenmesini sağlayacak her türlü bilgi olarak tanımlanmıştır. Diğer yandan direktifi mülga eden 27 Nisan 2016 Avrupa Genel Veri Koruma Tüzüğü'nde ise kişisel veri kişisel veri yine belirli ya da kimliği belirlenebilir gerçek kişi ile ilişkilendirilebilen her türlü bilgi şeklinde tanımlandıktan sonra bir kişinin kimlik numarası, lokasyon verisi, çevrimiçi bir kimlik belirleyici gibi verileri ile, özellikle fiziksel, psikolojik, genetik, duygusal, mental, ekonomik, kültürel veya sosyal kimliği gibi bir veya birden fazla öğeye referansta bulunmak suretiyle doğrudan veya dolaylı olarak tanımlanabilmesine imkân sağlayan verilerdir olarak tanımlanmıştır.

[340] Şen, Türk Ceza Kanunu'nun 135. maddesinde kişisel verilere ilişkin bir tanımın yapılmadığını ancak ilgili maddenin gerekçesine bakıldığında, kişisel veriden anlaşılması gerekenin gerçek kişilere ait bilgiler olduğunun anlaşıldığı ve bu suçun mağdurunun yalnızca gerçek kişileri hukuka aykırı olarak kaydedilen kişiler olduğunu ortaya koyan ifadeler yer verildiğini ve nacak bu ifadelerin amacını aştığını zira kişisel verilerin sahibinin gerçek kişiler olabileceği gibi tüzel kişiler de olabileceğini savunmuştur. Ersan Şen, "**Kişisel Verilerin Korunması Kanunu Son Tasarısı**" (Çevrimiçi) http://www.hukukihaber.net/kisisel-verilerin-korunmasi-kanunu-son-tasarisi-makale,3742.html (Erişim Tarihi:10.10.2018)

[341] Yaşar, Gökcan, Artuç, **Yorumlu Uygulamalı Türk Ceza Kanunu,** s.4436

aykırılığa ilişkin ise hukuka aykırılıktan kastın "…*fiilin hukuk normu ile çelişmesi…"*[342] ve *"…hukuk düzeninin yasakladığı tüm alanları kapsadığını…"*[343] söyleyebiliriz.

Anlaşılabileceği üzere bu suç icrai hareketle işlenen bir suçtur.[344] Madde metnine bakıldığında, ilgili suçun kişisel verilerin kaydedilmesi ile oluşacağı ve suçun oluşması için bunun yeterli olduğu açıktır. Bu anlamda suç serbest hareketli bir suçtur.[345] Yani kişisel verilerin kaydedildiği an itibariyle Türk Ceza Kanunu'nun 135. Maddesinde düzenlenen işbu suç oluşmuş olacaktır.[346] Ayrıca madde metnine bakıldığında suçun oluşması için bir zarar doğmuş olması aranmadığından bu suç aynı zamanda bir tehlike suçu olarak da tanımlanabilecektir.[347] Bu noktada doktrinde bazı görüşler bu suçun bağlı hareketli bir suç olduğunu belirtse de,[348] bizim de katıldığımız bir görüşe göre bu suça konu kaydetmek fiili Kişisel Verilerin Korunması Kanunu'nun ilgili 3.maddesi dikkate alındığından birden fazla şekilde ortaya çıkabilecektir ve bu durumda bu suçun serbest hareketli bir suç olduğunu söylemek daha doğru olacaktır. [349] Diğer yandan suçun oluşması için, netice itibariyle bir zararın doğmuş olması aranmadığından bu suç aynı zamanda bir soyut tehlike suçudur.[350]

Kişisel verilerin kaydedilmesi suçu kapsamında kaydetmek fiili bazı yazarlar tarafından kişisel verilerin daha sonra kullanılabilecek şekilde hazır bulundurulma olarak anlaşılması gerektiğini ileri sürmüşlerdir.[351] Bazı yazarlar ise kişisel verilerinin kaydedilmesi suçundaki kaydetmek fiilini "…*kişisel verilerin düzenlenmesi, depolanması, değerlendirilmesi, kullanılması, açıklanması, aktarılması, elde edilebilir*

---

[342] Neslihan Göktürk, "Suçun Yasal Tanımında Yer Alan "Hukuka Aykırılık" İfadesinin İcra Ettiği Fonksiyon", **İnönü Üniversitesi Hukuk Fakültesi Dergisi**, Cilt.7, Sayı.1, 2016, s. 418
[343] Yaşar, Gökcan, Artuç, **Yorumlu Uygulamalı Türk Ceza Kanunu**, s.4436
[344] Korkmaz, **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, s. 330
[345] Dülger, **Bilişim Suçları**, s.680. Dülger, **Kişisel Verilerin Korunması Hukuku**, s. 317
[346] Taşkın, **Bilişim Suçları**, s. 102. Yaşar, Gökcan, Artuç, **Yorumlu Uygulamalı Türk Ceza Kanunu**, s. 4438. Korkmaz, **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, s.333.
[347] Özbek, **TCK İzmir Şerhi**, s.951. Taşkın, **Bilişim Suçları**, s. 102. Korkmaz, **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, s.333. Çokmutlu, **Türk Ceza Hukukunda Kişisel Verilerin Korunması**, s. 187. Doğan, Bacaksız, Tepe, Özbek, **Türk Ceza Hukuku Özel Hükümler**, s. 575
[348] Özbek, **TCK İzmir Şerhi**, s. 950.
[349] Korkmaz, **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, s. 334
[350] Dülger, **Kişisel Verilerin Korunması Hukuku**, s. 319
[351] Yaşar, Gökcan, Artuç, **Yorumlu Uygulamalı Türk Ceza Kanunu,** s. 4437, Çokmutlu, **Türk Ceza Hukukunda Kişisel Verilerin Korunması**, s. 186

hale getirilmesi..."[352] şeklinde ifade etmişlerdir. Ancak 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 3. Maddesinin (e) fıkrası ile bu konuya bir açıklık getirilmiş ve kişisel verilerin kaydedilmesinden ne anlaşılması gerektiği ifade edilmiştir. Bu maddeye göre kişisel verilerin işlenmesi ifadesi kişisel verilerin kaydedilmesi, muhafaza edilmesi, depolanması, değiştirilmesi, yeniden düzenlenmesi, aktarılması, açıklanması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi kişisel veriler üzerinde gerçekleştirilecek her türlü işlem olarak tanımlanmıştır.

Öğretide kişisel verinin tanımında olduğu üzere bu konuda da kanunilik ilkesi bağlamında farklı görüşler ortaya çıkmıştır. Bazı yazarlara göre Kişisel Verilerin Korunması Kanunu kapsamında düzenlenen ancak Türk Ceza Kanunu kapsamında sayılmayan verinin depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi şeklinde bir fiil söz konusu ise bu eylem ancak Türk Ceza Kanunu kapsamında sayılan fiillerle bağlantı kurulabilmesi halinde cezalandırılabilecektir.[353] Kanunilik anlamında bizim de katıldığımız bu görüş doğrultusunda Türk Ceza Kanunu ve Kişisel Verilerin Korunması Kanunu arasındaki bu farkın bir an evvel düzeltilmesi gerekmektedir.

İlgili maddede suçun oluşması için kişisel verilerin elektronik ortamda mı yoksa fiziksel olarak mı kayıt edilmesi gerektiğine ilişkin bir bilgi verilmemiş olup, maddenin gerekçesinde kişisel verilerin bilgisayar ortamında veya kâğıt üzerinde kayda alınması arasında bir ayırım gözetilmediği ifade edilmiştir.[354] Görüldüğü üzere kişisel verilerin otomatik yöntemlerle işlenmesi gibi otomatik sistemler kullanılmadan işlenmesi halleri de kişisel verilerin işlenmesi kavramı kapsamı içerisindedir. Nitekim doktrindeki çoğunluk görüş de bu yöndedir. [355] Diğer yandan kanun gerekçesinin aksine görüş bildiren yazarlar da bulunmaktadır. Bu görüşler kişisel verilerin

---

[352]Yaşar, Gökcan, Artuç, **Yorumlu Uygulamalı Türk Ceza Kanunu**, s. 4437; Ayrıca bkz. Ayözger, **Kişisel Verilerin Korunması Hukuku**, s.121 Ayözger'e göre kişisel verilerin işlenmesi kişisel verilerin depo edilmesi, değiştirilmesi, silinmesi gibi pek çok işlemi kapsayıcı niteliktedir.

[353] Korkmaz, **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, s.335; Ayrıca bkz. Özbek, **TCK İzmir Şerhi**, s. 951 "*…kanımızca kanunilik ilkesinin bir sonucu olarak kaydetmekten ne anlaşılacağına ilişkin olarak suç tipinde ayrı bir düzenlemeye yer verilmelidir."*

[354] Dülger, **Bilişim Suçları**, s. 679

[355] Ayözger, **Kişisel Verilerin Korunması Hukuku**, s.122. Karagülmez, **Bilişim Suçları**, s.231, **Taşkın**, **Bilişim Suçları,** s.102.

kaydedilmesi kavramından kâğıt kalem ile kaydetmenin anlaşılmaması gerektiğini kalem kağıtla kaydetmenin amacını olan yeniden kullanılabilirliği ve saklanabilirliği sağlamayacağını ifade etmişlerdir. [356] Ayrıca yine doktrinde akılda tutma, ezberleme şeklindeki eylemlerin de kaydetmek anlamına gelmeyeceği ifade edilmiştir. [357]

Kişisel Verilerin Korunması Kanunu'nun 3. Maddesinde yer alan kişisel verilerin işlenmesine yönelik tanım gözetildiğinde, kişisel verilerin işlenmesinden kişisel verilerin tümden veya kısmi olarak otomatik olan ya da otomatik yöntemlerle işlenmediği halde bir veri kayıt sisteminin parçası olmak şartıyla kaydedilmesinin anlaşılması gerekmektedir.[358] Dolayısıyla burada kişisel verilerin kaydedilmesi suçunun otomatik olmayan yollarla da yani örneğin kâğıda yazmak suretiyle de işlenebileceği belirtilmiştir. Burada önemli olan suçun oluşabilmesi için kâğıt ve kalem ile kaydedilen kişisel verilerin mutlaka bir veri kayıt sisteminin parçası olması gerektiğidir.[359] Aksi takdirde veri kayıt sisteminin bir parçası olmayan veriler kişisel verilerin korunması kapsamına dahil edilemeyeceklerdir. Veri kayıt sistemi, Kişisel Verilerin Korunması Kanunu'nda kişisel verilerin belirli kriterler kullanılmak suretiyle tasnif edilerek kaydedildiği bir sistem olarak tanımlanmıştır.

Yine Kişisel Verilerin Korunması Kanunu'nun 4.maddesinde kişisel verilerin işlenme sürecinde temel alınması gereken ilkelerden bahsedilmiştir. Bu maddeye göre kişisel veriler işlenirken, bu işlemlerin hukuka ve dürüstlük kurallarına uygun olarak yapılması, işlem gören kişisel verilerin tam ve doğru şekilde tutulması ve gerektiğinde güncellenmesi, kişisel verilerin net ve hukuka uygun amaçlar için işlenmesi, işlendikleri amaçla ilişkili olarak depo edilmeleri, varsa mevzuatta yer verilen süre kadar yoksa işlendikleri amacın gerektirdiği süre kadar muhafaza edilme şeklinde beş adet temel ilkeden bahsedilmiştir. Görüldüğü üzere bu ilkeler kişisel verilerin işlenmesi sürecinin hukuka uygun olması bakımından son derece önemli olup bu

---

[356] Özbek, **TCK İzmir Şerhi**, s. 951. Doğan, Bacaksız, Tepe, Özbek, **Türk Ceza Hukuku Özel Hükümler**, s. 574

[357] Doğan, Bacaksız, Tepe, Özbek, **Türk Ceza Hukuku Özel Hükümler**, s. 574

[358] Kişisel Verileri Korumu Kurumu tarafından da veri kayıt sistemi belirli kriterlere göre sınıflandırılan elektronik ya da fiziki ortamda tutulabilecek bir sistem olarak tanımlanmıştır. Bu sistem kişilerin adı soyadına göre sınıflandırılabileceği gibi, örneğin kredi kartı borcu olan kişilerin bilgilerine göre de sınıflandırılması mümkündür (çevrimiçi) https://www.kisiselverikanunu.com/veri-kayit-sistemi-nedir/

[359] Korkmaz, **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, s.332

ilkeler gözetilmeksizin kişisel verilerin işlenmesi halinde kişisel veriler hukuka uygun şekilde işlenmiş sayılamayacaklardır.

b. Manevi Unsur

Türk Ceza Kanunu'nun 135.maddesinde düzenlenen kişisel verilerin kaydedilmesi suçunun manevi unsuru kasttır. Nitekim kanun maddesi de dikkate alındığında söz konusu suçun işlenmesi için herhangi bir saik belirtilmediğinden bu suçun kast ile işlenebilen suçlardan olduğunu söyleyebiliriz. Dolayısıyla suçun oluşması için failin bilerek ve isteyerek kişinin rızası olmaksızın kişisel verileri kaydetmesi yeterli olacaktır. Bu suçun taksirle işlenmesi ise mümkün değildir. [360]

Yargıtay da vermiş olduğu bir kararında, sanığın hakaret davasında delil olarak kullanılmak üzere, bir devlet hastanesinde bulunan ve katılana ait kimlik verileri, sağlık verileri gibi kişisel verileri içeren birtakım kayıtlara ulaşarak, bazı verileri kaydettiği ve birden fazla sayıda hastane belgesini kopyalayarak, söz konusu hakaret davasında ispat olarak sunduğu olayda, sanığın ilintili suçu işlemek için kastının bulunmadığı, sanığın başka bir davaya ispat araçları sunmaya çalıştığı gerekçesiyle sanığın atılı suçu işlemediğine kanaat getirmiştir. [361] Esasen Yargıtay bu kararda sanığın hukuka aykırılık bilinci bulunup bulunmadığını araştırmış ve sanığın hukuka aykırılık bilinci bulunmadığına kanaat getirerek sanığın atılı suçu işlemediğine kanaat getirmiştir. Oysa bu olayda sanık, devlet hastanesinde bulunan ilgili kayıtlara ve dolayısıyla mağdurun verilerine ulaşırken açıkça hukuka aykırı olduğunu bildiği bir eylemi gerçekleştirmektedir. Bu noktada sanığın amacının, verileri mahkeme nezdinde delil olarak kullanmak olmasının sanığın hukuka aykırılık bilinci ile hareket ettiği gerçeğini değiştirmeyeceği kanaatindeyiz. Bu bakımından Yargıtay'ın vermiş olduğu bu karara katılmadığımızı belirtmek isteriz. Nitekim doktrinde bazı yazarlar da, bu suçun olası kast ile işlenebileceğini savunmuşlardır.[362] Bu durumda, sanığın kastının

---

[360] Parlar, Hatipoğlu, **Türk Ceza Kanunu Yorumu**, s. 2045. Yaşar, Gökcan, Artuç, **Yorumlu ve Uygulamalı Türk Ceza Kanunu**, s.4121. Dülger, **Bilişim Suçları**, s.681. Dülger, **Kişisel Verilerin Korunması Hukuku**, s. 321

[361] Yaşar, Gökcan, Artuç, **Yorumlu ve Uygulamalı Türk Ceza Kanunu,** s. 4442. Korkmaz, **Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması**, s. 345, İlgili Yargıtay kararı için bkz. Yargıtay 12. CD 12.06.2012, 2012/23504 E. 2012/ 14795K.

[362] Özbek, **TCK İzmir Şerhi**, s.958. Özbek'e göre bir suç genel kast ile işlenebiliyorsa olası kast ile de işlenebilecektir. Özbek, Doğan, Bacaksız, Tepe, **Türk Ceza Hukuku Özel Hükümler**, s. 582.

olmaması, hukuka aykırılık bilincinin olmadığını ya da bu suçun olası kast ile işlenmiş olabileceği ihtimalini ortadan kaldırmayacaktır.

c. Hukuka Aykırılık

Türk Ceza Kanunun 135. Maddesi incelendiğinde görüleceği üzere hukuka aykırılık unsuruna madde metninin her iki fıkrasında da yer verilmiş olup, buna göre maddenin birinci fıkrasında genel olarak kişisel verileri hukuka aykırı olarak kaydeden kimsenin cezalandırılacağı belirtilmiş; ikinci fıkrasında ise kişinin ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin kişisel verileri hukuka aykırı olarak kaydeden kimsenin cezalandırılacağı düzenlenmiştir.

Görüldüğü üzere yasa koyucu maddenin ikinci fıkrasında bilinçli bir ayrıma gitmiş ve bu fıkrada sayılan kişilerin siyasi, felsefi, dini görüşleri ile ırki kökenlerine ilişkin özel nitelikli kişisel verilerinin kaydının mutlak suretle yasaklamak istemiş[363] ve özel bir hukuka aykırılık bilinci aramamıştır.[364] Doktrinde, yasa koyucunun kişilerin siyasi, felsefi, dini ve ırki kökenlerine ilişkin verilerinin özel bir hukuka aykırılık şartı aramaksızın kaydını kişisel verilerin kaydedilmesi suçu kapsamında değerlendirmedeki gerekçesinin, bu verilerin kaydının kişiler arasında ayrımcılığa neden olabilecek olması ve toplumda bölücülük yapılmasının engellenmesi olduğu şeklinde görüşler mevcuttur.[365] Bazı yazarlar maddenin ikinci fıkrasında yer verilen ve kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine ilişkin verilerinin

---

[363] Özbek, **TCK İzmir Şerhi**, s.949; Özbek'e göre söz konusu veriler mutlak dokunulmaz veriler olup, maddenin devamında yer alan kişinin ahlâkî eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin verileri ise nisbi dokunulmaz verilerdir. Özbek konuyu ifade ederken, Türk Ceza Kanunu'nun 135. maddesinin ikinci fıkrasında sayılan özel nitelikli veriler arasında bir ayrım yapılmış ve kişilerin siyasi görüşü, felsefi düşüncesi, dini inancı ve ırki bilgisine ilişkin kişisel verilerinin kaydı her şekilde suç teşkil ederken; kişilerin ahlak eğilimleri, cinsel hayatları, sağlık verileri veya sendikal bilgilerine ilişkin verileri ile hukuka aykırı şekilde kaydedilmesi halinde suç teşkil edecektir. Bu bakımdan ilk cümlede sayılan veriler mutlak dokunulmaz veriler olarak değerlendirilirken ikinci cümlede yer alan veriler nispi dokunulmaz veriler olarak ifade edilebilecektir, şeklinde görüşünü bildirmiştir.

[364] Karagülmez, **Bilişim Suçları**, s.232. Dülger, **Bilişim Suçları**, s.272

[365] Parlar, Hatipoğlu, **Türk Ceza Kanunu Yorumu**., s. 2044 "*Kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine ilişkin bilgilerin kişisel veri olarak kaydedilmesi, vatandaşlar arasında bu sayılan etmenlere dayanan grup mensubiyeti nedeniyle ayrımlar yapılması, yürürlükteki kanun ve nizamların, uluslararası düzenlemelerin izin vermediği bir durum olduğundan, bu tür bilgilerin kişisel veri olarak kaydedilmesi başlı başına hukuka aykırılık içeriği taşımaktadır. Yasa koyucu bu düzenleme ile aslında millet bireyleri arasında bölücülük yapılmasını önlemek ve özel hayatın gizliliği ve korunması hakkında müdahale içeriği taşıyan bu fiilleri yaptırım altına almak suretiyle bu hakka güvence sağlamak amacını gütmektedir*."

kaydedilmesi hususunda hukuka aykırılık unsuru aramayan düzenlemeyi hatalı bularak eleştirmişler. Düzenlemeye yönelik eleştiriler kapsamında Türk Ceza Kanunu ile kişisel verilerin hukuka aykırı olarak kaydedilmesi halinin cezalandırılmak istendiğini, kamu düzeni ve kamu güvenliği gereğince bu verilerin kaydedilmesinin gerektiği durumlarda bu suçun oluşmaması için gereken düzenlemenin yapılmış olması gerektiği ifade edilmiştir.[366] Bu görüşte olan yazarlar dayanak olarak Türk Ceza Kanunu'nun gerekçesinde de yer alan 108 sayılı Avrupa Konseyi Sözleşmesine atıf yapmaktadırlar.[367] Elbette ki bu eleştirilere katılmak mümkün değildir. Nitekim kamu düzeni ve kamu güvenliği gibi soyut gerekçeler ile kişinin bu denli özel ve hassas verilerinin kaydedilmesi dahi düşünülmemelidir. Kaldı ki bir kişinin siyasi, felsefi, dini veya ırki kökenine ilişkin verilerinin kaydedilmesinin herhangi bir şekilde kamu düzenine ya da kamu güvenliğine hizmet edebileceği beklenmemelidir.[368]

Diğer yandan kişilerin ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin kişisel verilerin ise yalnızca hukuka aykırı olarak kaydedilmeleri halinde faillerin cezalandırılacağına ilişkin bir düzenleme getirilmiştir. Yani yasa koyucu 135. Maddenin ikinci fıkrasında yer alan ve özel nitelikli kişisel verilerin kaydedilmesine ilişkin suç tipinde, bazı özel veriler ile sınırlı olmak kaydıyla, suç bakımından tipe uygunluk ile birlikte özel bir hukuka aykırılık aramıştır.[369] Yasakoyucunun amacı bu fiilin bazı durumlarda hukuka uygunluk sebepleri ile birlikte hukuka uygun olabileceğini göstermek istemesidir.[370] Burada esasen ilgili hukuka uygunluk sebebi, kişinin menfaatinin zedelendiği gerçeğini

---

[366] **Yaşar, Gökcan, Artuç**, op.cit., s.4120: Bahsi geçen eleştiriler kapsamında kanun koyucunun milli güvenlik, milli savunma, kamu düzeni ve kamu güvenliğinin korunması amacıyla istihbarat birimine kişilerin siyasi, felsefi, dini ve ırki kökenlerine ilişkin veri toplama görevi verildiğinde bu suçun oluşmaması gerektiğine ilişkin görüş ifade edilmiştir. Parlar, Hatipoğlu, op.cit., s.2044

[367] 108 sayılı sözleşmenin Özel Veri Kategorileri başlıklı 6. maddesinde iç hukukta uygun güvenceler sağlanmadıkça, ırksal kökeni, siyasi düşünceleri, dini veya diğer inançları ortaya koyan kişisel veriler ile sağlık veya cinsel hayatla ilgili kişisel veriler, otomatik işleme tabi tutulamayacağı yönünde düzenleme yapılmıştır. Bu düzenlemeden anlaşılan iç hukukta uygun güvencelerin sağlanması halinde bu hassas verilerin kaydedilebileceği yönündedir.

[368] Küzeci, **Kişisel Verilerin Korunması**, s.288: Küzeci'ye göre "… *Belirtilen türdeki bilgilerin kaydının her durumda hukuka aykırı olacağı söylenebilir. Burada bazı veri türleri özel nitelikte görülmüş ve farklı bir düzenlemeye tabi tutulmuştur. Çalışmamız kapsamında daha önce de belirttiğimiz üzere özellikle devlet kurum ve kuruluşlarının kamu hizmeti yerine getirirken bu türdeki bilgileri kişisel veri olarak tutmalarından herhangi bir yarar beklemek güçtür. Nitekim bir hukuk devletinde yönetimin bu bilgiler karşısında gözlerinin bağlı olması gerekir.* "

[369] Korkmaz, **Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması**, s. 398

[370] Özbek'e göre yasa koyucu hukuka aykırılığı özel olarak düzenlediği bazı durumlarda fiil tipe uygun olsa bile hukuka aykırılık olmayabilir. Özbek, **TCK İzmir Şerhi**, s. 955

ortadan kaldırmasa da bu zedelenmeye izin verme niteliğindedir.[371] Hukuka uygunluk sebepleri bir sonraki konunun başlığı olduğundan burada ayrıntılı olarak incelenmeyecektir.

Doktrinde 135. Maddenin her iki fıkrası kapsamında özel olarak belirtilen hukuka aykırılık kavramı bakımından farklı görüşler bulunmaktadır. Yazarların bir bölümü bahsi geçen hukuka aykırılık kavramının hukuka özel aykırılık olarak yorumlanması gerektiğini ve yargılama esnasında failin suça ilişkin özel hukuka aykırılık eğiliminin ispatlanması gerektiği aksi takdirde bu suçun işlenmiş sayılamayacağını ifade etmişlerdir.[372] Yine bu yazarlara göre, suçun işlenmesi halinde kişinin fiili bilerek ve isteyerek gerçekleştirmesine rağmen fiilin hukuka aykırılığını bilmemesi yani kişinin fiilinin Türk Ceza Kanunu'nun 30.maddesinde[373] düzenlenen 'hata' kapsamında değerlendirilebilecek durumda olması ile hukuka özel aykırılık bilinci karıştırılmamalıdır.[374]

Bu görüşü eleştiren yazarlar ise genel olarak 135. Madde kapsamında öngörülen hukuka aykırılık kavramı bakımından esasen özel bir hukuka aykırılık aranmadığı, bu ifadenin özel bir hukuka aykırılık bilinci olarak yorumlanması halinde bu durumun yargılama safhasında ispatlama yükümlülüğü getireceği ve bu hali yargılamaları kitleyeceğini ifade edilmiştir. [375] Bu görüşte olan yazarlar suçun işlenmesine ilişkin olarak hukuka aykırılığın karine olarak var olduğunu, hukuka uygunluk sebebi varsa da bunun ayrıca iddia üzerine araştırılması gerektiği ifade edilmiştir. [376]

Yargıtay vermiş olduğu bir kararında sanığın, davaya konuyu kişinin resmi belgede sahtecilik suçunu işlediğini ispatlamak amacıyla, bu kişi ile arasında geçen

---

[371] Göktürk, **Suçun Yasal Tanımında Yer Alan "Hukuka Aykırılık" İfadesinin İcra Ettiği Fonksiyon**, s.418

[372] Özbek, Doğan, Bacaksız, Tepe, **Türk Ceza Hukuku Genel Hükümler**, s.26. Dülger, **Kişisel Verilerin Korunması Hukuku,** s. 321. Özbek, Doğan, Bacaksız, Tepe, **Türk Ceza Hukuku Özel Hükümler**, s. 579. Konuyla ilgili olarak Özbek, Doğan, Bacaksız, Tepe konuyla ilgili olarak işlenen eylemin ceza kanundaki suç tipine uygunluğu söz konusu olsa bile, suçun oluşması için hakimin özel olarak hukuka aykırılık araması gerektiğini ifade etmişlerdir.

[373] Türk Ceza Kanunu'nun 30. Maddesinde hata kavramı düzenlenmiş ve eylemi gerçekleştirirken suçun maddi unsurları konusunda bilgi sahibi olmayan kişinin kasten hareket etmiş olmayacağını bunun hukuken hata kavramı içerisinde değerlendirileceği ifade edilmiştir.

[374] Özbek, **TCK İzmir Şerhi**, s.956. Özbek, Doğan, Bacaksız, Tepe, **Türk Ceza Hukuku Özel Hükümler**, s. 579..

[375] Dülger, **Bilişim Suçları**, s.683

[376] Dülger, **Kişisel Verilerin Korunması Hukuku**, s.323

konuşmaları kaydederek bu konuşmaları CD olarak mahkemeye sunduğu olayda sanığın herhangi bir hukuka aykırılık kastının olmadığını, hukuka aykırılık bilinci olmadığını, kişisel verilerin kaydedilmesi suçunun unsurlarının oluşmadığını ifade etmiştir. Görüldüğü üzere Yargıtay başka bir suçu kanıtlamak için söz konusu konuşmaları kaydeden kişiyi 135. Madde kapsamında cezalandırmamış ve sanığın hukuka aykırılık bilinci olmadığını ifade etmiştir.[377] Yargıtay'ın bu görüşüne katılmadığımızı yukarıda da belirtmiştik. Nitekim Yargıtay bu kararında her ne kadar sanığın hukuka aykırılık bilinci olmadığı ifade etmiş olsa bile, esasen incelemesini yaparken sanığın suç işleme kastını ya da hukuka aykırı hareket etme bilincini değil, hatalı şekilde sanığın amacını incelemeye esas almaktadır. Bu bakış açısının meşru bir amaç için işlenecek her türlü suça ya da hukuka aykırı harekete kapı açacağı görüşündeyiz.

aa. İlgili Kişinin Rızası

Türk Ceza Kanunu'nun hakkın kullanılması ve ilgilinin rızası başlıklı 26.maddesinin ikinci fıkrasında bir kimsenin mutlak kendisine ait ve üzerinde tasarrufta bulunabileceği haklarla ilgili olarak göstermiş olduğu bir rıza söz konusu ise, bu rıza üzerine işlenen fiilden ötürü kimse cezalandırılamayacaktır.

135. Maddenin gerekçesinde de kişinin rızası ile kendisiyle ilgili kişisel verilerin kayda alınmasının suç oluşturmayacağı ifade edilmiştir.[378] Dolayısıyla kişinin söz konusu hassas verileri kendi rızası ile açıklaması ve bunun kayıt altına alınması halinde bu durumun 135. Maddede düzenlenen suçu oluşturmayacak ve aksine böyle bir açıklama ifade özgürlüğü kapsamında değerlendirilecektir.[379] Bu halde kanun maddesinde açıkça ifade edildiği üzere bir kişinin rızası dahilinde kişisel verilerinin kaydedilmesi halinde kişisel verileri kaydeden kişi ya da kişiler bu fiillerinden ötürü kanunun 135. Maddede düzenlenen 'kişisel verilerin kaydedilmesi' suçunu işlemiş sayılmayacaklardır. [380]

---

[377] Yargıtay 12. Ceza Dairesi, 2014/17630 E., 2015/1672 K., 02.02.2015 T. sayılı kararı

[378] Kanun gerekçesinde açıkça kişinin rızası ile kendisiyle ilgili bilgilerin kayda alınmasının suç oluşturmayacağı muhakkak denilerek ilgilinin rızasını bir hukuka uygunluk sebebi olduğu ifade edilmiştir.

[379] Küzeci, **Kişisel Verilerin Korunması**, 2010, s.289

[380] Dülger, **Bilişim suçları**, s. 684

Diğer yandan bu madde bakımından ilgilinin rızasının bir hukuka uygunluk sebebi olup olmadığı hususunda doktrinde bazı yazarlar bu suçun şikâyete bağlı bir suç olmamasından yola çıkarak, burada kamu yararının ağır bastığını ve dolayısıyla kişinin rızasının bir hukuka uygunluk sebebi olamayacağını belirtmişlerdir. [381] Bizim de katıldığımız doktrindeki ağırlık görüşe göre ise bu suç bakımından ilgili kişinin rızasının bir hukuka uygunluk sebebi olduğunu ifade etmişlerdir. [382] Yargıtay'ın görüşü de ilgili kişinin rızasının bir hukuka uygunluk sebebi olduğu yönündedir. Nitekim Yargıtay vermiş olduğu bir kararında, sanıklara ait ortak işyerinde birtakım vatandaşlara ilişkin nüfus cüzdan fotokopilerinin bulunduğu ve bu fotokopilerin ise sahiplerinin rızası dışında ele geçirilerek muhafaza edildiği iddia edilmiş olmasına rağmen, vatandaşların bir takım hukuki işlemlerin gerçekleştirilmesi amacıyla bu fotokopileri kendi rızaları ile teslim ettiklerini beyan etmeleri ve sanıkların da vatandaşların kişisel verilerini bulunduran nüfus cüzdan fotokopilerini herhangi bir şekilde 3. kişilere yaydıklarına ilişkin bir delil olmadığının gözetilmesine üzerine, sanıklar hakkında verilen mahkumiyet kararı yerine beraat kararı verilmesi gerektiğini ifade ederek mağdurların kendi rızaları ile vermiş olduğu nüfus cüzdanları sebebiyle sanık hakkında 135. maddeye dayanarak mahkumiyetine karar verilemeyeceği ifade edilmiştir. [383]

Bu noktada Türk Ceza Kanunu ve Kişisel Verilerin Korunması Kanunu yasa yapma tekniği olarak karşılaştırıldığında, Türk Ceza Kanunu'nun 26.maddesinde rıza kavramı düzenlenirken yalnızca "*ilgilinin rızası"* şeklinde ifade edilmiş olduğundan, Türk Ceza Kanunu kapsamında kişisel verilerin kaydedilmesine ilişkin suç tipi için ilk anda açık rızanın aranmasına gerek olmadığı ve zımni rızanın bu suç bakımından bir hukuka uygunluk sebebi olarak yeterli olacağı söylenebilecektir. Ancak 6698 sayılı KVKK'nın tanımlar başlıklı 3.maddesinde de açık rıza 'spesifik bir konuya ilişkin olarak verilen ve veri sahibinin bilgilendirilmesi üzerine kendi özgür iradesi ile vermiş olduğu bir rıza olarak tanımlanmış ve 5.maddesinde ise bir kişinin kişisel verilerinin ilgili kişinin açık rızası olmadan işlenemeyeceği ifade edilmiştir. Aynı kanunun

[381] Özbek ise konuyu değerlendirirken, madde 135 kapsamında düzenlenen suç tipinin şikâyete bağlı olmadığını ve dolayısıyla bu suç tipinin işlenebilmesi bakımından ilgilinin rızasının bulunmasının kamu menfaati karşısında bir hukuka uygunluk sebebi olarak değerlendirilemeyeceğini ifade etmiştir. Özbek, **TCK İzmir Şerhi**, s.962. Özbek, Doğan, Bacaksız, Tepe, **Türk Ceza Hukuku Özel Hükümler**, s. 582.
[382] Taşkın, **Bilişim Suçları**, s.108. Parlar, Hatipoğlu, **Türk Ceza Kanunu Yorumu**, s.2049. Korkmaz, **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, s.401
[383] Yargıtay 5. Ceza Dairesi, 2014/10479 E., 2018/4622 K. ve 21.06.2018 T. sayılı kararı

17.maddesinde kişisel verilere ilişkin suçlar bakımından 5237 sayılı Türk Ceza Kanunu'nun 135 ila 140 ıncı madde hükümleri uygulanacağı ifade edilmiştir.

Doktrinde bazı yazarlara göre, 6698 sayılı KVKK kapsamına giren kişisel verilere ilişkin olarak işlenen suçlar bakımından, aynı kanunun 17. Maddesi gereğince Türk Ceza Kanunu'nun 135. ve 140. Maddelerinin uygulanacağı belirtildiğinden, 6698 sayılı KVKK kapsamına giren kişisel verilere karşı işlenen ve Türk Ceza Kanunu'nun ilgili suç tanımlarına giren durumlarda kişilerin açık rızasının olup olmadığı hukuka uygunluk sebebinin varlığını tespit etme hususunda kriter olacak; bunun dışında kalan yani 6698 sayılı KVKK kapsamına girmeyen kişisel veriler için ise bu verilere karşı işlenen suçların yine Türk Ceza Kanunu'nun ilgili maddelerince suç teşkil etmesi halinde zımni rızanın hukuka uygunluk sebebi olarak yeterli olacağı belirtilmiştir. [384] Bizim kanunilik ilkesi gereğince bu görüşe katılmaktayız. Ancak bu durumdan kaynaklanabilecek olası mağduriyetlere mahal verilmemesi için biran evvel her iki kanun arasındaki lafzı farklılıkların giderilmesi gerektiğini düşünüyoruz. Bu noktada son olarak belirtmek isteriz ki elbette her iki durumda da açık rızanın da zımni rızanın da suça konu fiilin işlendiği anda mevcut olması gerekmektedir.[385]

Bu noktada bir diğer önemli husus da kişisel verilerin kişilerin rızaları hangi konuya ilişkin verilmiş ise o konunun sınırlarına riayet edilmesidir.[386] Kişisel veri sahibi, verilerinin işlenmesi bakımından hangi konuda ve hangi işlemlerle bilgilendirilmiş ise o konu ve işlemler çerçevesinde verileri işlem görmek zorundadır. Aksi takdirde, kişinin rıza vermiş olduğu konu ve işlemler dışında kişinin rızasının var olduğu söylenemeyecektir. Örneğin kişisel verilerinin yalnızca kaydedileceği hususunda bilgilendirilen ve buna yönelik rızasını göstermiş olan kişinin verileri

---

[384] Dülger, **Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması**, s.141. Dülger, **Kişisel Verilerin Korunması Hukuku**, s. 323

[385] Dülger, **Bilişim Suçları**, s. 684. Benzer görüşteki bir Yargıtay kararı için bkz. Türk Ceza Kanunu'nun 26. Maddesinin 2. fıkrasında kişinin mutlak şekilde kendine ait olduğu haklara ilişkin olarak göstermiş olduğu rızadan ötürü kimseye ceza verilmeyeceği ifade edilmiştir. Bu hukuka uygunluk sebebine dayanılabilmesi için kişinin üzerinde mutlak tasarrufta bulunabileceği bir hak ve kişinin rızası gereklidir. Aynı zamanda bu hukuka uygunluk nedenine dayanılabilmesi için rızanın en geç eylemin gerçekleştiği noktada var olması gerekmektedir. Fiilin işlendiği sırada rıza gösterilmemişse, sonradan gösterilen rıza fiili hukuka uygunluk nedeni olamaz. Yargıtay Ceza Genel Kurulu, E: 2012/12-1510 K: 2014/331 K:17.06.2014

[386] Korkmaz, **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, s. 351

ayrıca 3. Kişiler ya da kurumlar ile paylaşılırsa artık bu noktada kişinin rızasının olduğundan bahsedilemeyecektir. [387]

bb. Kişisel verinin ilgilisi tarafından alenileştirilme halinde

Kişisel verilerin veri sahibi tarafından aleni hale getirilmesi durumunda, örneğin bir sosyal medya hesabında paylaşması durumunda, bu verilerin başkaları tarafından kaydedilmesi halinde 135. Madde kapsamındaki suçun oluşup oluşmayacağı konusunda doktrinde farklı görüşler bulunmaktadır. Bu noktada doktrinde 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[388] ve bu verilerin artık kişinin özel yaşam alanından çıkarak koruma kapsamı dışında kaldığını[389] ifade etmektedirler. Biz bu görüşe katılmamaktayız.[390] Zira bu 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.

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 Türk Ceza Kanunu çerçevesinde

---

[387] Çokmutlu, **Türk Ceza Hukukunda Kişisel Verilerin Korunması**, s.208
[388] Karagülmez, **Bilişim Suçları**, s.352.
[389] Doğan, Bacaksız, Tepe, Özbek, **Türk Ceza Hukuku Özel Hükümler,** s. 573
[390] Yargıtay Ceza Genel Kurulu ilgili kararında, Türk Ceza Kanunu kapsamında düzenlenen 135. ve 136. Maddelerindeki 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. Ceza Dairesi E. 2017/2960 K. 2018/1541 T. 14.2.2018

kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçunun oluştuğunu gözetmiş ve ilgili yerel mahkeme kararını bozmuştur. [391]

Yargıtay Ceza Genel Kurulu tarafından verilen bir kararda da bu yönde görüş bildirilmiş ve bir kişisel verinin aleni hale gelmesinin bu verinin artık 3. Kişiler tarafından kullanılabilmesi sonucunu doğurmayacağı ifade edilmiştir. Kurul kararında 5237 sayılı Türk Ceza Kanunu'nun hazırlanması aşamasında fiil sayısı kadar suç, suç sayısı kadar da ceza olduğunu, bu kuralın istisnaları için ise birleşik suç, zincirleme suç ve fikri içtima kavramlarının bulunduğunu, sanığın genel yayın yönetmenliği yaptığı gazetede yer alan fotoğrafının sanığa bilgisi olmaksızın bir arkadaşlık sitesinde sair diğer bilgileri verilmeksizin kullanıldığını ve erkek arkadaş aradığına dair ibareler kullandığını Türk Ceza Kanunu'nun 136. Maddesinde yer alan suçun bu hali ile oluştuğunu, aynı zamanda sanığın mağduru bu şekilde rencide ettiğini ve haysiyet ve şerefi ile oynadığını ve bu durumunda Türk Ceza Kanunu'nun 125. maddesinde düzenlenen hakaret suçunun da işlenmiş olduğunu, bu durumda farklı neviden suçların birlikte işlenmiş olduğu yani fikri içtima ile sanığın en ağır cezayı gerektiren suçtan cezalandırılması gerektiğini ve bu nedenle sanığın eyleminin 136. Maddede düzenlenen kişisel verileri yayma ve ele geçirme suçunu oluşturduğu gerekçesi ile verilen cezanın yerinde olduğunu ve bu bakımdan verilen cezanın uygun olduğu şeklinde görüş ifade etmiştir. [392]

Görüldüğü üzere her ne kadar kişinin verilerini kendi rızası ile aleni hale getirmesi bir hukuka uygunluk sebebi olarak değerlendirilebilecekse de bu konu değerlendirilirken her somut olay bakımından ayrı bir değerlendirilmeye gidilmesi ve maliki tarafından aleni hale getirilen her türlü kişisel verinin 3. Kişiler tarafından kullanılabileceği yönünde bir yorum getirilmemelidir.

---

[391] Yargıtay ilgili kararında 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. Ceza Dairesi 12. C.D. 2017/150 E. 2017/6231 K.

[392] Yargıtay Ceza Genel Kurulu, 2012/12-1510 E. 2014/331 K. Ve 17.06.2014 T. sayılı kararı

cc. Kanun hükmü veya amirin emrinin yerine getirilmesi

Türk Ceza Kanunu'nun 24.maddesinde kanun hükmü veya amir emrinin yerine getirilmesi halinde kişinin cezalandırılmayacağı düzenlenmiştir. Buna göre suçun hukuka uygunluk sebepleri bakımından kanun hükmünün yerine getirilmesinin bir hukuka uygunluk sebebi olduğu söylenebilecektir. [393] Kanunun gerekçesine göre de kanundan doğan bir yükümlülük olduğu hallerde[394] kişisel veriler kişilerin rızası olmaksızın dahi işlenebilecektir. Bu anlamda yapılan hareketin sebebi kanundan kaynaklanıyor ise bu durumda kanun hükmünü yerine getirmekte olan kimse bu süreçte görevini yerine getiriyor demektir.[395] Burada kanundan anlaşılması gerekenin genel olarak mevzuat olduğunu söyleyebiliriz.[396] Yani tüzük, yönetmelik, KHK gibi mevzuat kapsamındaki tüm hukuki düzenlemeler de kanun emrinin yerine getirilmesi kapsamında yorumlanabilecektir. Kolluk kuvvetlerinin bir suç soruşturması kapsamında, Polis Vazife ve Salahiyet Kanunu'nun beşinci maddesi gereğince şüphelilerden parmak izi alması ya da Adli Sicil Kanunu gereğince Adalet Bakanlığı tarafından kişilerin önceden aldıkları cezalara ilişki kayıtları işlemesi, Ceza Muhakemesi Kanunu gereğince suçla mücadele edebilmek için kişisel verilerin kaydedilmesi gibi düzenlemeler örnek olarak sayılabilir.

Nitekim kanunlardan doğan yükümlülük kavramı, ceza kanunun gerekçesi ile uyumlu olarak Kişisel Verilerin Korunması Kanunu'nun 5. Maddesinin ikinci fıkrasında da sayılmıştır.[397] Yine aynı kanunun 6. Maddesinde özel nitelikli kişisel verilere ilişkin olarak sağlık ve cinsel hayata ilişkin veriler hariç olmak üzere kanun hükmünün yerine getirilmesi amacıyla özel nitelikli verilerin dahi işlenebileceği belirtilmiştir. Ayrıca sağlık ve cinsel hayata ilişkin veriler için ise kanunun 6. maddesinin 3. fıkrasında ayrıntılı olarak belirtildiği üzere ancak bu maddede sayılan sağlık hizmetleri ve bu hizmetlerin finansmanı ve yönetime ilişkin amaçlar, teşhis ve

---

[393] Özbek, **TCK İzmir Şerhi**, s.962. Taşkın, **Bilişim Suçları**, s.108. Dülger, **Bilişim Suçları**, s.695

[394] Türk Ceza Kanunu'nun gerekçesinde bazı kişisel verilerin kanun gereğince kayda alındığı ve dolayısıyla bazı kamu kurumlarından hizmetin gereği olarak kişisel verilerin işlenmesi ve bu verilerin kaydedilmesinin suç teşkil etmeyeceği ifade edilmiştir. Özbek, Doğan, Bacaksız, Tepe, **Türk Ceza Hukuku Özel Hükümler**, s. 580.

[395] Özbek, **TCK İzmir Şerhi**, s. 956

[396] Korkmaz, **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, s. 352. Özbek, **TCK İzmir Şerhi**, s. 957. Özbek, Doğan, Bacaksız, Tepe, **Türk Ceza Hukuku Özel Hükümler**, s. 581.

[397] **TBMM Kişisel Verilerin Korunması Kanunu Komisyon Raporuna** göre bu hususla ilgili kişinin açık rızası olmasa dahi eğer kanunlarda açıkça kişisel verilerin işlenmesine ilişkin bir düzenleme varsa kişisel veri işlenebilecektir.

tedavi gibi sağlık hizmetleri, koruyucu hekimlik hizmetlerinin verilmesi sebepleri ile yalnızca kanunda sır saklama yükümlülüğü getirilen kişiler tarafından veya yetkilendirilmiş kurumlar ya da kuruluşlar tarafından işlenebilecektir.[398]

dd. Zorunluluk Hali

Türk Ceza Kanunu'nun 25.maddesinde meşru savunma ve zorunluluk hali başlıklı maddede hukuka uygunluk sebebi olarak zorunluluk hali düzenlenmiştir.[399] Ayrıca yine Ceza Muhakemesi Kanunu'nun 223. maddesinde, yüklenen suçun zorunluluk hali içinde işlenmesi halinde sanık hakkında kusurunun bulunmaması nedeniyle ceza verilmesine yer olmadığına dair karar verilmesi gerektiği ifade edilmiştir. Diğer yandan 6098 sayılı Kişisel Verilerin Korunması Kanunu'nun 6. Maddesinde de eğer fiili olarak bir kişinin rızasını açıklaması olanaklı değilse ya da bu kişinin rızası hukuken geçerli değilse bu kişinin bizzat kendisinin ya da başkasının hayatını korumak amacıyla kişisel verilerin işlenebileceği düzenlenmiştir.[400] Görüldüğü üzere Kişisel Verilerin Korunması Kanunu'nda da Türk Ceza Kanunu'na uyumlu bir düzenleme yapılmıştır. Ancak bu noktada aynı kanunun özel nitelikli kişisel verilerin düzenlendiği 6. Maddesinde zorunluluk halinin bir istisna olarak sayılmadığını ve zorunluluk halinin özel nitelikli kişisel veriler bakımından bir hukuka uygunluk sebebi olmadığını belirtmek isteriz. [401]

ee. Sözleşmenin ifası için gerekli olması

Kişisel Verilerin Korunması Kanunu'nun 5. Maddesinin 2-c Fıkrasında sözleşmenin ifası için gerekli olması halinde kişinin açık rızası bulunmasa dahi kişisel

---

[398] Dülger, **Kişisel Verilerin Korunması Kanunu**, s.335

[399] Türk Ceza Kanunu'nun 25. Maddesinde bireyin kendisine ya da bir başkasına yönelmiş ya da yönelmesi muhtemel bir haksız saldırıyı engellemek amacıyla o andaki hal ve koşullara göre orantılı biçimde engelleme çabası içerisinde işlediği fiillerden ötürü cezalandırılmayacağı ve yine kendisine ya da başkasına ait bir hakka ilişkin olarak, kişinin kasten neden olmadığı ve o kişiyi ya da kendini ağır bit tehlikeden kurtarmak amacı ile kişinin gerçekleştirdiği eylemlerden cezalandırılmayacağı düzenlenmiştir.

[400] **TBMM Kişisel Verilerin Korunması Kanunu Komisyon Raporuna** göre bu husus şöyle ifade edilmiştir. Kişinin rızasını açıklayamayacak ya da açıklanan rızanın geçerli olamayacağı hallerde, bireylerin hayat ve beden bütünlüğünü korumak için kişisel verilerinin işlenebileceği, örnek olarak, kişinin bilincinin yerinde olmadığı ya da akli dengesinin bulunmadığı ya da tıbbi müdahale altında olduğu durumlarda kişinin verilerinin işlenmesi için rızasının alınmasının mümkün olmadığı, alınsa da geçerli olamayacağı, bu noktada kişinin kan grubu ya da ilaç bilgileri gibi tüm sağlık verilerine ilişkin bilgilerin işlenebileceği ifade edilmiştir.

[401] Korkmaz, **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, s. 357.

verilerin işlenebileceği düzenlenmiştir. [402] Esasen bu düzenleme Türk Ceza Kanunu kapsamında düzenlenmemiştir.[403] Bu düzenleme doğrudan uluslararası düzenlemelere paralel olarak mevzuatımıza eklenmiştir. Örneğin, yapılan bir sözleşme gereği, o kişiye ait adı, soyadı ya da hesap numarası gibi verilerin işlenmesi örnek olarak verilebilecektir. [404]

ff. Bir hakkın tesisi için gerekli olması

Türk Ceza Kanunu'nun 26. maddesi kapsamında hakkını kullanan kimseye ceza verilmeyeceği düzenlenmiştir. Kişisel Verilerin Korunması Kanunu'nun 5. Maddesinin 2-e fıkrasında bir hakkın tesisi için gerekli olması halinde, kişinin açık rızası aranmaksızın kişisel verilerin işlenebileceği düzenlenmiştir[405]. Yani 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.

gg. Veri sorumlusunun hukuki yükümlülüğün yerine getirilmesi için zorunlu olması

Kişisel Verilerin Korunması Kanununun 5. Maddesinin 2-ç fıkrasında veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması halinde kişinin açık rızası olmaksızın kişisel verilerinin işlenebileceği ifade edilmiştir. Zira daha evvel de yer verdiğimiz üzere veri sorumlusu kavramı mevzuatımıza Kişisel Verilerin Korunması Kanunu ile girmiştir. Bu anlamda Türk Ceza Kanunu'nda yer almayan ancak uluslararası düzenlemelere uygun şekilde mevzuatımıza giren bir hukuka uygunluk sebebidir. Örneğin bir şirket tarafından veri sorumlusunun kişinin, kişisel veri sahibine ilişkin sosyal sigorta yükümlülüklerini yerine getirebilmek bu

---

[402] **TBMM Kişisel Verilerin Korunması Kanunu Komisyon Raporuna** göre bu husus şöyle ifade edilmiştir." *Fıkranın (c) bendine göre, bir sözleşmenin kurulması veya ifasıyla ilgili olarak kişisel veri işlenebilecektir."*

[403] Çokmutlu, **Türk Ceza Hukukunda Kişisel Verilerin Korunması**, s.208

[404] Korkmaz, **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, s.358

[405] **TBMM Kişisel Verilerin Korunması Kanunu Komisyon Raporuna** göre bu husus şöyle ifade edilmiştir. Bir hakkın kullanılabilmesi ya da bu hakkın korunabilmesi için kişisel verilerin işlenmesinin zorunlu olduğu durumlarda kişisel verilerin işlenebileceği belirtilmiş ve bu duruma örnek olarak bir çalışan işten ayrıldıktan sonra işverene karşı açmış olduğu davada şirketin bu çalışana ait bazı verileri davaya sunmasının ya da hakkında kısıtlılık kararı verilmiş vasisi ya da kayyımı tarafından finansal bilgilerinin kaydedilmesinin hukuka uygun olacağı ifade edilmiştir.

kişinin kişisel verilerini kaydetmesi halinde işbu hukuka uygunluk sebebi söz konusu olacaktır. [406]

hh. Veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması

Kişisel Verilerin Korunması Kanununun 5. Maddesinin 2-f fıkrasında bu hukuka uygunluk sebebi düzenlenmiş olup, burada da veri sorumlusunun açık rıza aramaksızın kişisel veri işleyebileceği bir durum ifade edilmiştir. Ancak görüldüğü üzere yasa koyucu veri sorumlusunun meşru menfaatleri dahilinde kişisel veri işleyebilmesine izin verirken, bir yandan da veri sorumlusuna bu meşru menfaatleri kişinin temel hak ve özgürlükleri ile dengeleme yükümlülüğü getirmiştir. Bu bakımından yerinde bir düzenleme olduğu kanaatindeyiz. Kanun metninde meşru menfaatin tanımı yapılmamış ancak komisyon raporunda meşru menfaatten ne anlaşılması gerektiğine ilişkin bazı örnekler verilmiştir. Bu rapora göre örneğin bir şirketteki terfi sürecini planlayabilmek ve kimlerin terfi edileceğine liyakatli şekilde karar verebilmek çalışanların kişisel verilerinin işlenmesi meşru menfaate örnek gösterilmiştir.

ii. Sağlık ve cinsel hayata ilişkin kişisel verilerin işlenmesi ile ilgili hukuka uygunluk sebebi

Kişisel Verilerin Korunması Kanununun 6. Maddesinde özel nitelikli veriler düzenlenmiş olup, aynı maddenin ikinci fıkrasında sağlık ve cinsel hayata ilişkin kişisel verilerin işlenmesine ilişkin hukuka uygunluk sebebinden bahsedilmiştir. Buna göre kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından açık rıza olmaksızın işlenebileceği ifade edilmiştir. [407] Görüldüğü üzere kanun koyucu sağlık ve cinsel hayata ilişkin verilerin açık rıza

---

[406] **TBMM Kişisel Verilerin Korunması Kanunu Komisyon Raporuna** göre bu husus şöyle ifade edilmiştir. Veri sorumlularının hukuki yükümlülüklerini yerine getirilebilmek amacıyla, kişisel verileri işleyebileceği, örneğin bir şirketin çalışanın maaşlarını ödeyebilmek için hesap numaralarını, açil durumlarda haber verebilmek için yakınlarından birinin ismi ve telefon numarasını ya da sosyal sigorta kayıtları için sair bilgilerini işleyebileceğini ifade etmiştir.

[407] Bu konuya ilişkin tartışmalar ve açıklamalar için kişisel verilerin kaydedilmesi suçu başlıklı bölümü inceleyeniz.

olmaksızın kaydedilmesi için özel bazı hukuka uygunluk sebepleri düzenlemiştir. Komisyon raporunda sağlık bakanlığı, sağlık kuruluşları ve sosyal güvenlik kurumunun yukarıda sayılan amaçlarla tuttukları veriler ve kayıtlar örnek olarak gösterilmiştir.

jj. Kişisel Verileri Korunma Kanunu Kapsamı Dışında Tutulan Haller

Kişisel Verileri Korunma Kanunu'nun 28. maddesinde bu kanunun kapsamı dışında kalan istisnai haller düzenlenmiştir. Buna göre madde kapsamında, kişisel verilerin bu verilerin yetkisiz kişilere verilmemesi ve veri güvenliğine ilişkin tedbirlerin alınması şartıyla bireylerin kendilerine ya da yalnızca onunla birlikte yaşayan aile mensuplarına ilişkin faaliyetleri kapsamında işlenmesi, kişisel verilerin anonim hale getirilerek bir istatistiğe dönüştürülmeleri kaydıyla, araştırma ya da istatistik çalışmaları kapsamında kullanılmaları, kişisel verilerin ulusal güvenliği ve halk güvenliğini gibi kamusal menfaatler başta olmak üzere bireylerin özel hayatını veya kişilik haklarını ihlal etmemek ya da suç oluşturmamak şartıyla, edebi ya da bilimsel amaçlarla ya da tamamen ifade özgürlüğü kapsamında işlenmesi, kişisel verilerin ulusal savunma ve ulusal güvenlik gibi kamu menfaatlerini sağlamaya yönelik amaçlarla kanunla görevlendirilmiş kamu kurum ve kuruluşları tarafından yönetilen bir takım faaliyetler kapsamında işlenmesi, kişisel verilerin yargı mercileri veya infaz yetkilileri tarafından işlenmesi, halinde bu kanun hükümlerinin uygulama alanı bulmayacağı ifade edilmiştir. Elbette yukarıda sayılan hallerin Kişisel Verileri Korunma Kanunu'nun kapsamı dışında bırakılması, bu hallerin somut olay bakımından Türk Ceza Kanunu'nda yer alan suç tiplerinden birini oluşturması halinde, Türk Ceza Kanunu'nun uygulanmayacağı anlamına gelmemektedir. Bu haller Türk Ceza Kanunu kapsamında da bir suç teşkil etmiyorsa, Kişisel Verileri Korunma Kanunu'nun kapsamı dışında kalan haller somut olay bakımından hukuka uygunluk sebebi sayılacaklardır.

4. Suçun Nitelikli Halleri

a. Özel Nitelikli Kişisel Verilerin Kaydedilmesi

Türk Ceza Kanunu 135. maddesinin 2. fıkrasında kişisel verinin, kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması durumunda birinci fıkra uyarınca verilecek ceza yarı oranında

artırılacağı düzenlenmiş olduğundan, bu maddenin suçun nitelikli hallerinden birini oluşturduğunu söyleyebiliriz.

6698 sayılı Kişisel Verilerin Korunması Kanunun 30. Maddesiyle Türk Ceza Kanunu'nun işbu 135. Maddesi üzerinde değişiklik yapılmış ve söz konusu değişiklikten önce "*bilgileri kişisel veri olarak kaydeden kimse, yukarıdaki fıkra hükmüne göre cezalandırılır*" şeklinde olan madde metni "*olması durumunda birinci fıkra uyarınca verilecek ceza yarı oranında artırılır*" şeklinde değiştirilmiştir. [408] Buradan da anlaşılacağı üzere suçun nitelikli halinin cezalandırılması konusunda yerinde bir ayrıma gidilmiş[409] ve kişinin özel nitelikli verilerinin hukuka aykırı şekilde kaydedilmesi halinde ilk fıkraya göre verilen ceza oranı yarı oranında artırılmıştır. Bu konu yukarıda ayrıntılı şekilde anlatıldığından burada tekrara düşmemek açısından yinelenmemiştir.

b. Kamu Görevlisi Tarafından ve Görevinin Verdiği Yetki Kötüye Kullanmak Suretiyle Kaydedilmesi

Türk Ceza Kanunu'nun Nitelikli Haller başlıklı 137.maddesinde, kişisel verilerin kaydedilmesi suçunun kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle işlenmesi halinde öngörülen cezanın yarı oranında artırılacağı belirtilmiştir. [410] Yani kişisel verilerin kaydedilmesi ve kişisel verilerin hukuka aykırı olarak ele geçirilmesi suçlarının kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle işlenmesi halinde yarı oranında artırılacağı belirtilmiştir.[411]

Yargıtay vermiş olduğu bir kararda bu hususa değinerek kendilerine kötü muamelede bulunduğunu iddia ettikleri bir Cumhuriyet Savcısı ile ilgili olarak delil toplamaya çalışan ve bunun için de savcının odasında odaya çağrıldıkları esnalarda cep telefonlarının ses kayıt özelliğini açık bırakarak savcının konuşmalarını kayıt altına alan ve adliyede zabıt katibi olarak görev yapan evli karı koca sanıklar hakkında 134. madde kapsamındaki suçun işlenip işlenmediğinin tartışıldığı davada, 137. maddede düzenlenen kamu görevlisinin görevini kötüye kullanmak suretiyle suçu

---

[408] Dülger, **Kişisel Verilerin Korunması Hukuku**, s.319
[409] Doğan, Bacaksız, Tepe, Özbek, **Türk Ceza Hukuku Özel Hükümler**, s.578
[410] Dülger, **Bilişim Suçları**, s.681
[411] Dülger, **Bilişim suçları**, s.677. Dülger, **Kişisel Verilerin Korunması Hukuku**, s. 314

işlemesi halinde bu durumun suçun nitelikli halini teşkil ettiği gözetilmeksizin verilen kararı bu gerekçe ile bozmuş ve kamu görevlisi sıfatını haiz sanıkların 137. madde kapsamında düzenlenen suçun nitelikli haline göre cezalandırılması gerektiğini ifade etmiştir.[412]

Kamu görevlisi ile ilgili olarak doktrinde failin yalnızca kamu görevlisi olmasının bu suçun işlenmesi için yetmeyeceği, bu suçun aynı zamanda kamu görevlisinin görevini kötüye kullanmak suretiyle işlenmesi gerektiği açıkça belirtilmiştir.[413] Yargıtay vermiş olduğu bir kararında biri Danıştay tetkik hakimi sanık diğeri ise Danıştay üyesi katılan olan olayda, sanığın katılana karşı işlediği kesin olarak konut dokunulmazlığını ihlal suçu bakımından sanık hakkında verilecek cezanın tespitinde 137. Maddede yer alan nitelikli halin, yani suçun sanığın kamu görevi sıfatını kötüye kullanmak suretiyle işlediği gerekçesi ile verilen cezanın ağırlaştırılması yönündeki kararının, sanığın katılanın evinde özel hayatını ihlal edecek şekilde ses ve görüntü kaydı yaptığı sabit olsa da, sanığın gerçekleştirdiği eylemlerin görevi ile bir ilgisi bulunmadığı gerekçesi ile yerinde olmadığı ve 137. Maddenin olayda uygulanmasını yanlış bulduğu yönünde görüş bildirerek sanık her ne kadar kamu görevlisi olsa da atılı suçu kamu görevini kötüye kullanmak suretiyle işlemediğinden sanık hakkında 137. maddenin uygulanmasını kanuna aykırı olarak değerlendirmiştir.[414]

Bu konu bağlamında kamu görevlisi kavramının tanımı da önem kazanmaktadır zira bilindiği üzere hukukumuz uzun yıllar önce memur kavramı terk edilerek, bundan çok daha geniş ve kapsamlı bir kavram olan "kamu görevlisi "kavramı kabul edilmiştir. [415] Türk Ceza Kanunu'nun "Tanımlar" başlıklı 6.maddesinde "kamu görevlisi" kavramı kamusal faaliyetin yürütülmesine atama veya seçilme yoluyla ya da herhangi bir surette sürekli, süreli veya geçici olarak katılan kişi olarak tanımlanmıştır. Ayrıca madde metnini bakıldığında kamu görevlisi bakımından özel ya da kamuda çalışıyor olmasına ilişkin bir ayrım yapılmamıştır. Bu halde kamu

[412] Yargıtay 12. Ceza Dairesi E. 2018/3553 K. 2018/12027 T. 12.12.2018
[413] Karagülmez, **Bilişim Suçları**, s. 234
[414] Yargıtay 12. Ceza Dairesi E. 2018/2226 K. 2018/8746 T. 26.9.2018
[415] Hüseyin Aydın, Ceza Hukukunda Kamu Görevlisi Kavramı, **Ankara Barosu Dergisi,** 2010, S. 2010/1, s. 111

görevlisi kamusal faaliyete katılan herkes olabileceğinden, bu kişiler de aynı zamanda bu suçun faili de olabilecektir.

Yargıtay da vermiş olduğu bir kararında bu konuya değinmiş ve Sanığın, mağdurun özel alanına girdiği tartışmasız olan evi içerisinde özel yaşantısına müdahale etmek suretiyle Türk Ceza Kanunu'nun 134. Maddesinde yer verilen özel hayatın gizliliğini ihlal suçunu işlediği sabit olup, sanığın bu suçu işlediği esnada askerlik vazifesini yerine getirdiği ve dolayısıyla ilgili suçu işlerken askerliğin kendisine vermiş olduğu yetkiyi kötüye kullanarak bu suçu işlediği, kamu görevlisi kavramından anlaşılması gerekenin kamusal faaliyetin idaresine katılmak olarak anlaşılması gerektiği, bu faaliyete katılmanın atama ya da seçme yoluyla olabileceğini ve bu bakımından asker sıfatını haiz sanığın bu noktada kamu görevlisi olarak değerlendirilerek 137. Maddenin bu olay kapsamına da uygulanması gerektiği [416] şeklinde görüş bildirerek askerlik görevini yapmakta olan sanığın kamusal faaliyetin yürütülmesine geçici olarak katılan kişi olarak kamu görevlisi sıfatına haiz olacağı ve bu bakımından hakkında 137. maddenin uygulanabileceğini ifade etmiştir.

c. Belli Bir Meslek Ve Sanatın Sağladığı Kolaylıktan Yararlanmak Suretiyle Kaydedilmesi

Türk Ceza Kanunu'nun Nitelikli Haller başlıklı 137.maddesinde, kişisel verilerin kaydedilmesi suçunun belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle kaydedilmesi halinde öngörülen cezanın yarı oranında artırılacağı belirtilmiştir. [417]

Yargıtay konuya ilişkin olarak vermiş olduğu bir kararında bir hastanede görev yapan doktorun, çalıştığı hastanede farklı kadınlarla ilişkiye girdiği ve bu ilişkilerin görüntülerini de bilgisayarına kaydettiği, doktorun bilgisayarını tamir için gelen şahsın ise bu görüntüleri fark etmesi üzerine görüntüleri hard diskine kopyalaması ve diğer sanıklarla beraber bu görüntüleri CD'ler ile çoğalttıkları olayda, sanığın doktor katılanın özel hayatını ihlal etiği ve bu sebeple 134. Maddede yer alan suçu işlediği

---

[416] Yargıtay 12. Ceza Dairesi E. 2016/1129 K. 2017/6742 T. 27.9.2017

[417] Dülger, **Kişisel Verilerin Korunması Hukuku**, s.320. Özbek, Doğan, Bacaksız, Tepe, **Türk Ceza Hukuku Özel Hükümler,** s.578. Yazarlar bu konuyla ilgili olarak eğer bir suçun failinin, sahip olduğu mesleğin ya da sanatın kendisine sağlamış olduğu bir kolaylığı kullanmak suretiyle bir kişinin kişisel verilerine erişmesi durumunda ancak ceza kanununun 137. maddesi uygulanabilecektir. Bu konuya örnek olarak hastanelerde çalışan doktor ya da sair sağlık görevlilerinin hastane bilgisayarlara erişimi göstermişlerdir.

sabit olduğunu, bu noktada sanığın mesleğinin sağladığı bir kolaylıktan ötürü bu bilgisayara ve içindeki verilere ulaştığını, aksi takdirde bu görüntülere erişme imkanın olmayacağını ve bu sebeple sanık hakkında 134. Maddede düzenlenen ceza uygulanırken, 137. maddenin de dikkate alınması gerekeceği şeklinde görüş bildirerek, yaptığı mesleğin sağladığı kolaylıktan faydalanarak mağdurun bilgisayarında bulunan ve özel hayatına ilişkin görüntüleri ele geçiren sanıklar hakkında atılı suçlar değerlendirilirken 137. maddenin de dikkate alınması gerektiğini ifade etmiştir. [418] Bu noktada verinin anonim olarak yayınlanması halinde örneğin bir sağlık verisinin genel bir istatistik belirtmek amacıyla ve herhangi bir kişisel veriye yer vermeksizin yayınlanması halinde bu durum suç teşkil etmeyecektir.[419]

5. Suçun Özel Görünüş Biçimleri

a. Teşebbüs

Kişisel verilerin hukuka aykırı olarak kaydedilmesi suçuyla ilgili bu suçun teşebbüs ile de işlenip işlenemeyeceği konusunda bir görüş birliği bulunmamaktadır. Bazı yazarlar bu suçun teşebbüs ile de işlenebileceği savunurken[420] bazı yazarlar ise suç kişisel verilerinin hukuka aykırı olarak kaydedilmesi ile oluştuğundan, yani hareket ile suçun sonucu birbirine bağlı olduğundan, bu yönüyle teşebbüs ile işlenmeye elverişli bir suç olmadığı gibi aynı zamanda ani bir suç niteliği taşıdığını ifade etmişlerdir.[421]

Bu suçun teşebbüsle işlenebileceğini ifade eden yazarlar, icra hareketlerinin bölünmesi halinde bu suçun teşebbüs ile işlenebileceğini, yani icra hareketlerinin bölünebilir olduğu ölçüde bu suçun teşebbüse konu olabileceğini belirtmişlerdir.[422] Bazı yazarlar ise bu suçun teşebbüse elverişli olmadığını zira bu suçun hareket suçu olması sebebiyle, söz konusu icrai hareketin gerçekleşmesi ile suçun işlenmiş

---

[418] Yargıtay 12. Ceza Dairesi E. 2015/5128 K. 2016/10207 T. 15.6.2016

[419] Karagülmez konuyla ilgili olarak "*x bölgesinde y hastalığı yaygındır*" şeklinde bir örnek vermiş ve bu durumda söz konusu açıklamanın suç teşkil etmeyeceği ifade edilmiştir. Karagülmez, **Bilişim Suçları**, s. 352

[420] Dülger, **Bilişim Suçları**, s.680 Dülger bu suçun teşebbüs ile işlenemeye elverişli olduğunu belirtmiştir. Dülger, **Kişisel Verilerin Korunması Hukuku**, s. 344

[421] Doğan, Bacaksız, Tepe, Özbek, **Türk Ceza Hukuku Özel Hükümler**, s. 575-582. Özbek, **TCK İzmir Şerhi**, s.951.

[422] Parlar, Hatipoğlu, **Türk Ceza Kanunu Yorumu**, s. 2045; Yaşar, Gökcan, Artuç, **Yorumlu Uygulamalı Türk Ceza Kanunu**, s.4122. Dülger, **Kişisel Verilerin Korunması Hukuku**, s. 318

sayılacağını, çünkü suçun hareketi ile neticesinin birleşik olduğunu ve bu sebepten ötürü Türk Ceza Kanunu'nun 136. Maddesinde kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçunun ayrıca düzenlendiğini ifade etmişlerdir. [423]

Bu durumda söz konusu suçun teşebbüs aşamasında kalıp kalmadığının her somut olayın özelliğine ve icra hareketlerinin bölünebilir olup olmamasına göre değerlendirilmesi gerekecektir. Eğer işbu suçun işlenmesi saiki ile hareket ederken birtakım icra hareketlerine başlanmış ancak söz konusu suçun icra hareketlerinin tamamlanması için gereken '*kaydedilme*' işlemi gerçekleşmemiş ise bu suçun teşebbüs aşamasında kaldığı ifade edilebilecektir.[424]

b. İştirak

Türk Ceza Kanunu'nun 37. maddesinde suçun kanunî tanımında yer alan fiili birlikte gerçekleştiren kişilerden her birinin fail olarak sorumlu olacağı ve suçun işlenmesinde bir başkasını araç olarak kullanan kişinin de fail olarak sorumlu tutulacağı düzenlenmiştir. Dolayısıyla bu suç tipi Türk Ceza Kanunu genel hükümleri çerçevesinde iştirak ile işlenebilecektir. [425]

c. İçtima

Bu suçun işlenmesi için kanunda özel bir içtima kuralı düzenlenmediğinden Türk Ceza Kanunu genel hükümleri çerçevesinde içtima kuralları uygulanacaktır. Türk Ceza Kanunu'nun Suçların İçtimaı başlıklı bölümünde bir suç işleme kararının icrası kapsamında, değişik zamanlarda bir kişiye karşı aynı suçun birden fazla işlenmesi durumunda zincirleme suç oluşacağı ve bir cezaya hükmedileceği; işlediği bir fiil ile birden fazla farklı suçun oluşmasına sebebiyet veren kişinin bunlardan en ağır cezayı gerektiren suçtan dolayı cezalandırılacağı (fikri içtima) düzenlenmiştir.[426] Diğer yandan gerçek içtima ise failin işlediği her bir suçtan ayrı ayrı olacak şekilde

---

[423] Özbek, **TCK İzmir Şerhi**, s.958

[424] Dülger, **Kişisel Verilerin Korunması Hukuku**, s.344

[425] Dülger, **Bilişim Suçları**, s.702. Dülger, **Kişisel Verilerin Korunması Hukuku**, s. 344. Özbek, Doğan, Bacaksız, Tepe, **Türk Ceza Hukuku Özel Hükümler**, s. 582.

[426] Özen fikri içtima kavramının ortaya çıkabilmesi için, öncelikle ortada bir fiil olması ve bu fiil ile ceza kanununda yer alan birden fazla maddenin ihlal edilmesi gerektiği ifade etmiş ve bu durumda kişinin en ağır suçtan cezalandırılacağı belirtmiştir. Mustafa Özen, "Ceza Hukukunda Fikri İçtima", **Türkiye Barolar birliği Dergisi**, Ankara, S.73, *2003*, s. 137

cezalandırılması halidir ve ceza hukukunun genel prensibinin gerçek içtima olduğu[427] ve her bir suçun ve cezanın bağımsızlığını koruduğunu söylemek yanlış olmayacaktır.[428] Diğer yandan ise kişiye ait ses ve görüntülerin kişinin özel hayatına ait olmaları halinde ceza hukuku bakımından hangi suç kapsamında değerlendirileceği hususunda da tartışma bulunmaktadır. Nitekim 5237 sayılı Türk Ceza Kanunu'nun 'Özel Hayatın Gizliliğini İhlal' başlıklı 134. Maddesinde kişilerin özel hayatına ilişkin ses ve görüntülerin kayıt altına alınması ve bunların ifşasına ilişkin fiiller suç olarak düzenlenmiştir.[429] Öğretide konuyla ilgili olarak kişisel verilerin özel hayatın gizliliğini ihlal suretiyle ele geçirilmesi halinde, söz konusu fiillerin Türk Ceza Kanunu'nun 134. Maddesinde tanımlanan suçu oluşturacağı belirtilmektedir.[430] Yargıtay da vermiş olduğu kararlarında ses ve görüntünün kişinin özel hayatına ilişkin olması halinde bu verilerin kayda alınması ve/veya ifşası fiillerini özel hayatın gizliliğini ihlal başlıklı 134. Maddesi kapsamında değerlendirmiştir. Yargıtay bir kararında boşanma davasında delil olarak kaydetmek üzere resmi nikahlı eşine ait bir takım ses ve görüntüleri kaydeden kişinin gerçekleştirmiş olduğu eylemi 134. Madde kapsamında incelemeye tabi tutmuş ve fakat kişinin hukuka aykırılık bilinci olmadığından beraatine karar vermiştir. [431]

---

[427] Neslihan Göktürk, "Türk Hukuku'nda Suçların İçtiması", s.1, (Çevrimiçi) http://dergipark.gov.tr/download/article-file/14656 (Erişim Tarihi: 24.11.2018)

[428] Yargıtay Ceza Genel Kurulu da ilgili kararında Türk Ceza Kanunu'nun esasında her bir cezanın birbirinden ayrık olduğu, hangi sayıda suç işlendiyse o sayıda suç oluştuğu, hangi sayıda suç var ise o sayıda ceza olacağı özetler gerçek içtimanın esas olduğu ancak gerçek içtimanın da istisnaları olduğu bu istisnaların da birleşik suç, fikri içtima ve zincirleme suç olarak sayılabileceğini ifade etmiştir. Yargıtay Ceza Genel Kurulu 2012/1510E., 2014/331K. 17.06.2014T.

[429] Türk Ceza Kanunun 134. Maddesine göre kişilerin özel hayatının gizliliğini ihlal eden kişilerin cezalandırılacağı, özel hayatın ses ve görüntü kaydı ile ihlali halinde ezanın artırılacağı, maddenin ikinci fıkrasında ise bireylerin özel hayatına ilişkin görüntüleri ve sesleri ortaya çıkaran kimselerin bu madde kapsamında cezalandırılacağı ve bu görüntülerin ve seslerin basın yayın aracılığı ile yayılması halinde de cezalanın artırılacağı düzenlenmiştir.

Yaşar, Gökcan, Artuç, **Yorumlu-Uygulamalı Türk Ceza Kanunu**, s.4375 "…*Özel hayat kavramından, kişinin kimse ile paylaşmak istemediği, sadece kendisi ve eşi ve/veya çocukları, anne babası gibi maksimum güven duyduğu kimselere açtığı ve bunun dışında kimsenin bilmesini istemediği başta cinsel yaşamı olmak üzere, çıplaklığı, tuvalet ihtiyacı, banyo yapması, bedeni, düşünceleri, inançları, ümitleri, korkuları, aile ilişkileri, özel mektup, telgraf, günlük, hatıra defteri gibi olay, hal ve ilişkiler anlamına gelen gizli hata alanı ile kişinin özel yaşamına dahil olmayan dostları, arkadaşları, ailesi ya da yakın ilişkili olduğu kimselerin dahil olduğu az miktarda insanla paylaşmak isteyebileceği özel alan bu suçun konusunu oluşturmaktadır…"*

[430] Korkmaz, **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, s.367. Dülger, **Bilişim Suçları**, s. 702

[431] Yargıtay vermiş olduğu bir kararında, bir boşanma davasıyla ilgili olarak, bu davada delil olarak kullanmak ve aile içi geçimsizliğin sebebinin diğer eş yani katılan olduğunu kanıtlamak için katılana ait bazı birtakım ses ve görüntüleri kaydetmiş olması konusunda, sanığın herhangi bir hukuka aykırılık bilincinin olmadığını, sanığın bu ses ve görüntüleri çoğaltarak yaydığına ilişkin bir iddia da bulunmadığı dikkate alınarak, sanığın beraatine karar verilmesi gerektiği yönünde görüş bildirmiştir. Yargıtay 4. CD 2017/12189 E., 2018/9465 K. 10.10.2018 T. sayılı kararı

Bu konuda doktrinde farklı değerlendirmeler yapılmaktadır. Örneğin doktrindeki bir görüşe göre fail hem kişisel verilerin hukuka aykırı şekilde kaydetmiş hem de bu kişisel verileri başkalarına yaymış ise bu durumda hem Türk Ceza Kanunu'nun 135. Maddesi çerçevesinde hem de 136. Maddesince ayrı ayrı cezalandırılacaktır.[432] Başka bir görüşe göre ise 136. Maddedeki suçun işlenmesi halinde 135.maddedeki suç geçit suç niteliğinde olacağından bu durumda fail yalnızca 136. Madde kapsamında cezalandırılacaktır.[433] Doktrinde bazı diğer görüşler ise bu iki suç tipinden birinin işlenmesi için diğerinin zorunlu olmadığı gerekçesi ile bu suçlar arasında geçit ilişkisinin oluşmayacağını bu bakımından failin her iki suçtan ayrı ayrı gerçek içtima kuralları uygulanmak suretiyle cezalandırılması gerektiğini ifade etmektedirler. [434] Yargıtay ise konuya ilişkin olarak ikinci görüşe uygun olarak karar vermektedir. Buna göre Yargıtay bir kararında eşinin eski eşi ile olan konuşmalarına ait ve içerisinde bu kişilere arayan kişilerin telefon numaraları, arama tarihi ve süresini içeren arama dökümlerini eşinin akrabalarına gönderen sanığın eyleminin 136. maddede düzenlenen verileri hukuka aykırı olarak verme ve ele geçirme suçunu oluşturduğunu ifade etmiştir.[435].

---

[432] Parlar, Hatipoğlu, **Türk Ceza Kanunu Yorumu,** s.2046, Yaşar, Gökcan, Artuç, **Yorumlu-Uygulamalı Türk Ceza Kanunu**, s. 4440. Değirmenci, **Türk Ceza Kanunu'nun Bilişim Suçları Bakımından Değerlendirilmesi**, s. 203

[433] Özbek, Doğan, Bacaksız, Tepe, **Türk Ceza Hukuku Özel Hükümler**, s. 582. Özbek, **TCK İzmir Şerhi**, s.962-963. Taşkın, **Bilişim Suçları**, s. 109. Ayrıca benzer yönde bir kararda Yargıtay kişisel verilere karşı işlene suçlara ilişkin olarak içtima kavramını değerlendirdiği ilgili kararında, suçun failinin kişisel verilerin verilmesi ve yayılması ile kaydetmek fiillerini aynı anda gerçekleştirebileceğini ifade etmiştir. Yargıtay bu kararında, kişisel verilerin herkes tarafından ulaşılabilecek bir internet sitesine kaydedilmesi halinde aynı anda hem kaydetmek hem de yaymak fiillerinin ortaya çıkacağını belirterek, bu gibi durumlarda fikri içtima konusunun ele alınması gerektiğini belirtmiştir. Yargıtay bu noktada sanığın en ağır cezayı öngören suçtan cezalandırılması gerektiğini ifade etmiştir. Benzer bir değerlendirmede Yargıtay olayın oluş şekli göz önünde bulundurulduğunda hem 136. maddedeki kişisel verileri verme ve ele geçirme eylemlerinin hem de 125.maddede yer alan hakaret eyleminin birlikte ortaya çıktığını, bu halde ise sanık hakkında Türk Ceza Kanunu'ndaki 44. Maddesindeki farklı neviden fikri içtima kurallarının uygulanması gerektiğini ifade etmiş ve sanığın en ağır cezayı gerektiren suçtan cezalandırılması gerektiğini, bu halde de sanığın 136. Maddede yer alan suçtan cezalandırılması gerektiği yönünde karar vermiştir. Yargıtay Ceza Genel Kurulu'nun ilgili kararı için bakınız 2012/1510E. 2014/331K., 17.06.2014T. sayılı karar

[434] Dülger, **Bilişim Suçları**, s.715

[435] Yargıtay 12. Ceza Dairesi 2014/22994 E, 2015/2630 K., 16.02.2015 T. Sayılı kararı. Ayrıca belirmek isteriz ki Yargıtay aynı kararında bahsi geçen arama dökümlerinin kişilerin mesaj içeriklerini ya da konuşma içeriklerini içermemesi sebebiyle haberleşmenin gizliliğini ihlal suçunu oluşturmayacağını ifade etmiştir.

6. Yaptırım ve Yargılama Usulü

Türk Ceza Kanunu'nun 135. Maddesinin 1.fıkrasına göre hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir. Daha evvel de bahsettiğimiz üzere bu fıkrada tanımlanan suça konu yaptırımın alt sınırı 21/2/2014 tarihli ve 6526 sayılı kanunun 3. maddesiyle değiştirilmiş ve daha önce altı ay olan alt sınır bir yıl olarak değiştirilmiştir.

Türk Ceza Kanunu'nun 135. Maddesinin 2. fıkrasına göre ise kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin hassas verilerinin kaydedilmesi halinde ise aynı maddenin birinci fıkrasında öngörülen ceza yarı oranında artırılarak uygulanacaktır. Yine daha evvel bahsettiğimiz üzere bu fıkrada tanımlanan suçun yaptırımı daha önce aynı maddenin 1.fıkrasında yer alan ceza yaptırımına tabi tutulmuşken, fıkranın eski halinde yer alan "*yukarıdaki fıkra hükmüne göre cezalandırılır*" ibaresi 24/3/2016 tarihli ve 6698 sayılı Kanunun 30. maddesiyle, "*olması durumunda birinci fıkra uyarınca verilecek ceza yarı oranında artırılır*" şeklinde değiştirilmiştir.

Türk Ceza Kanunu'nun 139. Maddesine göre ise kişisel verilerin kaydedilmesi, suçunun soruşturulması ve kovuşturulması şikâyete bağlı değildir. Türk Ceza Kanunu'nun 140. Maddesine göre ise bu suçun işlenmesi dolayısıyla tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur.

B. VERİLERİ HUKUKA AYKIRI OLARAK VERME VEYA ELE GEÇİRME

1. Genel Olarak

Türk Ceza Kanunu'nun 136.maddesine göre verileri, hukuka aykırı olarak başkasına veren veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılacaktır.[436] Görüldüğü üzere bu maddede kişisel verilerin hukuka uygun

[436] Hüseyin Akarslan, **Bilişim Suçları**, Güncellenmişi 2. Baskı, Seçkin, Mayıs 2015, Ankara, s. 70. Akarslan uygulamada en çok karşılaşılan suç tipinin bu suç tipi olduğunu ve kişisel verilerin çoğu zaman reklam şirketlerinden istihbarat birimlerine kadar pek çok kurum ve kuruluşla paylaşıldığını belirtmiştir.

olarak toplanıp toplanmadığına, kaydedilip kaydedilmediğine bakılmaksızın söz konusu verilerin hukuka aykırı olarak verilmesi veya ele geçirilmesinin engellenmesi amaçlanmıştır.[437]

Doktrinde de bu maddenin amacının kişisel verilerin yetkisiz kişilere aktarılmasının[438] ve 3.kişiler tarafından ele geçirilmesinin[439] engellenmesi olduğu ve bu maddenin 765 sayılı Türk Ceza Kanunu'nda karşılığı bulunmadığı belirtilmiştir. Ancak bu maddenin 765 sayılı Türk Ceza Kanunu'ndaki karşılığının 525/a1 maddesi olduğunu ifade eden yazarlar da bulunmaktadır.[440] Kanımızca her iki maddenin kapsamı aynı olmadığından ve 136. Maddenin konusunu yalnızca gerçek kişilere ait veriler oluşturduğundan bu maddenin karşılığının 525/a.1[441] maddesi olmadığı görüşündeyiz.[442]

Burada kanun yapış tekniği açısından bazı hatalar olduğu aşikardır. Zira kanun koyucu madde metninin kendisinde suçu oluşturan fiiller içerisinde yayma filini de saymış olmasına rağmen madde başlığında verileri hukuka aykırı olarak verme ve ele geçirme şeklinde suçu ifade ederek yayma fiilini saymamıştır. Oysa madde kapsamı madde başlığı ile birlikte değerlendirildiğinde, kanun koyucunun burada kişisel verilerin hukuka aykırı olarak yayılması, verilmesi ve ele geçirilmesini cezalandırmak istediği açıktır. Aynı şekilde madde metninin başlığında 'verileri' hukuka aykırı olarak kaydetmek olarak belirttiği suç başlığı esasen "kişisel verileri" olarak yazılmalıydı.[443]

---

[437] Taşkın, **Bilişim Suçları**, s.105. Küzeci, **Kişisel Verilerin Korunması**, 2018, s. 407. Korkmaz, **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, s. 392. Özbek, **TCK İzmir Şerhi**, s.469

[438] Yaşar, Gökcan, Artuç, **Yorumlu Uygulamaları Türk Ceza Kanunu**, s.4444. Parlar, Hatipoğlu, **Türk Ceza Kanunu Yorumu**, s. 2047.

[439] Küzeci, **Kişisel Verilerin Korunması**, 2018, s. 407

[440] Taşkın, **Bilişim Suçları**, 105. Taşkın konuyu şu şekilde ifade etmiştir. "*765 sayılı TCK 525/a1 maddesi eski yasa bu suçun karşılığını oluşturan suçtur. 525a.1'deki düzenleme TCK'daki düzenlemeye göre 'program veya diğer herhangi bir unsur' iadesi nedeniyle daha geniştir; bu nedenle tüzel kişilere ait veriler hakkında da uygulanabilecektir."*

[441] Madde 525/a.1 maddesine göre bilgilerin otomatik bir sistemde işlendiği durumlarda, bu sistemden verileri hukuka aykırı şekilde ele geçiren kimse hakkında 1 yıldan 3 yıla kadar hapis ve para cezası uygulanacağı düzenlenmiştir.

[442] Değirmenci bazı yazarların 765 sayılı Türk Ceza Kanunu'nda yer alan 525a maddesi ile 5237 sayılı Türk Ceza Kanunu'nun 136. Maddesinin birbirlerine karşılılık teşkil ettiğini ancak 136. Madde kapsamında konunun kişisel veri olduğunu ancak 525a maddesindeki verinin ise bilişim sistemlerinde yer alan tüm verileri ifade ettiğini ve bu verilerin kişisel veri olmayabileceğini, bu hali ile iki maddenin birbirileri ile teğet geçtikleri bir gerçek ise de 136. Maddenin özel olarak kişisel verilere ilişkin olduğunu oysa 525a maddesinin daha geniş bir alanı kapsayarak 136. Maddeden ayrıldığını ifade etmiştir. Değirmenci, **Türk Ceza Kanunu'nun Bilişim Suçları Bakımından Değerlendirilmesi**, s. 203.

[443] Karagülmez konuyla ilgili olarak, madde başlığında kişisel veriler yerine verileri ibaresinin kullanılmış olmasının yerinde olmadığını, veri ile kişisel veri arasında kavramsal olarak farklılık bulunduğunu, kişisel veri kavramının gerçek kişilere ait verileri, veri kavramının ise genel olarak her

Zira bu haliyle suça konu verilerin kişisel veri mi yoksa genel olarak veri mi olduğu anlaşılamadığından teorik olarak çelişkilere sebebiyet vermiştir.[444] Ancak kanaatimizce kanunun ilgili maddeleri bir bütün halinde düşünüldüğünde kanun koyucu burada kişisel verileri kastetmektedir. Doktrinde bu suçun en yaygın halinin internette yani bilişim alanında özellikle kimlik hırsızlığı şeklinde işlendiğine dair görüş mevcuttur. [445] Ayrıca Kişisel Verilerin Korunması Kanunu'nda da bu maddeye uygun bir düzenleme yapılmıştır. Nitekim bahsi geçen kanunun 8.maddesinde kişilerin açık rızası olmadan bu verilerin aktarılamayacağı düzenlenmiştir. Yine bahsi geçen kanunun 9.maddesinde ise kişisel verilerin yurtdışına aktarılması hususu düzenlenmiştir. Bu maddelere göre kişisel veriler açık rıza olmaksızın ne yurt içinde ne de yurtdışında yetkisiz üçüncü kişilere aktarılamayacaktır. Ancak aynı maddeler kapsamında bu hususun istisnaları düzenlenmiştir. Bu halde söz konusu istisnai durumlar çerçevesinde kişinin açık rızası aranmaksızın kişisel verilerin aktarılması mümkün olacak ve bu durumda kişisel veriler hukuka uygun şekilde aktarılmış olacaktır.

2. Suçla Korunan Hukuksal Değer

Türk Ceza Kanunu'nun 136. Maddesinde düzenlenen verileri hukuka aykırı olarak verme ve ele geçirme suç tipi, 135. Maddede düzenlenen kişisel verilerin hukuka aykırı olarak kaydedilmesi suç tipi gibi 'Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar' başlıklı dokuzuncu bölümünde düzenlenmiştir. Buna göre ilgili suç tipi ile korunmak istenen hukuki yararın uluslararası düzenlemelere paralel şekilde genel olarak kişilerin özel hayatının gizliliği[446] ve özel olarak da kişisel verilerinin

---

türlüyü veriyi ifade ettiğini ancak maddenin kanunda düzenlendiği yer dikkate alındığında madde metninin lafzı ne olursa olsun, maddede düzenlenen suçun konusunu da kişisel verilerin oluşturduğunu söylemenin mümkün olduğunu ifade etmiştir. Karagülmez, **Bilişim Suçları**, s. 233.

[444] Korkmaz, **Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması**, s. 380. Korkmaz, suçun düzenleniş tekniği ile madde başlığının kanun yapma tekniği açısından birbirlerine uyumlu olmadığını belirtmiştir.

[445] Karagülmez konuyu şöyle değerlendirmiştir. Karagülmez konuyla ilgili olarak bu suçun aynı zaman kimlik hırsızlığı olarak da bilindiğini, bu suçun genel olarak internet üzerinden bireylerin isimleri, doğum tarihleri, kredi kartı numaraları gibi bilgilerinin bireylerden habersiz ele geçirilmesi olarak işlendiğini, daha sonra bu veriler ile de dolandırıcılık suçlarının da işlendiğini ifade etmiştir. Karagülmez, **Bilişim Suçları**, s. 233. Ayrıca bakınız Korkmaz, **Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması**, s. 381. Dülger, **Bilişim Suçları**, s. 704. Dülger, **Kişisel Verilerin Korunması Hukuku**, s. 346

[446] Yaşar, Gökcan, Artuç, **Yorumlu Uygulamaları Türk Ceza Kanunu**, s.4444. Yaşar, Gökcan, Artuç konuyla ilgili olarak bu suç kapsamında korunmak istenen hukuki yararın özel hayatın gizliliğinin korunması olduğunu nitekim İnsan Hakları Sözleşmesi'nde ve anayasamızda da bu hakkın koruma altında olduğunu ifade etmiştir. Taşkın, **Bilişim Suçları**, s.106. Özbek, **TCK İzmir Şerhi**, s.969. Parlar,

korunması olduğunu[447] ve bu anlamda 135.madde kapsamında korunan hukuki değer ile aynı olduğunu söyleyebiliriz.[448] Doktrinde bu suçun, 135. Maddede düzenlenen verilerin hukuka aykırı olarak kaydedilmesi suçu ile karşılaştırılınca daha kapsamlı bir suç olduğu ifade edilmektedir. [449]

3. Suçun Unsurları

a. Maddi Unsurlar

aa. Fail

Türk Ceza Kanunu'nun 136.maddesinde düzenlenen 'Verileri hukuka aykırı olarak verme ve ele geçirme' suçunun faili, kanunun metninden de anlaşılabileceği üzere herkes olabilecektir. [450] Nitekim bu madde kapsamında özel olarak bir fail tanımı yapılmamıştır. Doktrindeki, bu suçun verme ve yayma fiili ile işlenmesi halinde, suçun failinin kişisel verilerin zilyedi ya da maliki olan kişi olacağı belirtilmiştir. [451]

Diğer yandan bu suçun failine ilişkin olarak Türk Ceza Kanunu'nun 137. Maddesi de dikkate alınmalıdır. Buna göre kişisel verileri hukuka aykırı olarak veren, yayan ya da ele geçiren kişinin görevini kötüye kullanan bir kamu görevlisi olması ya da belirli bir sanatın veya mesleği sağladığı kolaylıktan yararlanması ile bu suçu işlemesi halinde faile uygulanacak yaptırım artırılacaktır.[452] 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 doktrinde failin yalnızca kamu

---

Hatipoğlu, **Türk Ceza Kanunu Yorumu**, s.2047. Parlar, Hatipoğlu konuyu şöyle ifade etmektedir. "*Yasa koyucu 136.madde hükmüyle özel hayata hukuka aykırı bir şekilde saldırı oluşturan bu fiillerin suç olarak tanımlamak suretiyle özel hayatın gizliliği ve korunması hakkına yardımcı olmakta onu tanımakta, güvenceler sağlamakta ve ihlalini yaptırım altına almaktadır.* " Özbek, Doğan, Bacaksız, Tepe, **Türk Ceza Hukuku Özel Hükümler**, s. 583.

[447] Korkmaz, **Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması**, s. 384. Dülger, **Bilişim Suçları**, s.704

[448] Kuşkonmaz, **Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması**. s.129; Ayrıca bkz. Dülger, **Bilişim Suçları**, s. 675, 704. Dülger, **Kişisel Verilerin Korunması Hukuku**, s. 346

[449] Karagülmez, **Bilişim Suçları**, s. 233

[450] Yaşar, Gökcan, Artuç, **Yorumlu Uygulamalı Türk Ceza Kanunu**, s.4444. Karagülmez, **Bilişim Suçları,** s. 236. Taşkın, **Bilişim Suçları,** s.106. Özbek, **TCK İzmir Şerhi**, s.960. Parlar, Hatipoğlu, **Türk Ceza Kanunu Yorumu**, s.2048. Korkmaz, **Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması**, s. 394. Dülger, **Bilişim Suçları**, s. 704. Dülger, **Kişisel Verilerin Korunması Hukuku**, s. 347. Özbek, Doğan, Bacaksız, Tepe, **Türk Ceza Hukuku Özel Hükümler**, s. 583.

[451] Korkmaz, **Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması**, s. 394.

[452] Yaşar, Gökcan, Artuç, **Türk Ceza Kanunu Yorumu**, s. 4445. Korkmaz, **Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması**, s. 394.

görevlisi olmasının bu suçun işlenmesi için yetmeyeceği, bu suçun aynı zamanda kamu görevlisinin görevini kötüye kullanmak suretiyle işlenmesi gerektiği özellikle belirtilmiştir.[453] Kamu görevlisinin tanımı konusunda daha önceki bölümümüzde açıklama yapıldığından burada tekrar olmaması açısından bahsedilmeyecektir.

bb. Mağdur

Türk Ceza Kanunu'nun 136.maddesinde düzenlenen 'Verileri hukuka aykırı olarak verme ve ele geçirme' suçunun mağduru tıpkı 135. Maddede olduğu üzere herkes olabilecektir.[454] Zira kanunun ilgili maddesinde özel bir düzenleme bulunmamaktadır. [455] Ancak burada herkesten anlaşılması gerekenin, gerçek kişiler olduğunu da belirtmek isteriz.[456] Zira bu suçun konusu, yukarıda ayrıntılı olarak açıkladığımız üzere kişisel veriler olup, kişisel veriler de yalnızca gerçek kişilere ait olabilecektir. [457] Suçun mağdurunun verilerin zilyedi ya da maliki olup olmaması hususundaki tartışmaya daha önce ayrıntılı olarak yer vermiş olduğumuzdan bu konu burada tekrar tartışılmayacaktır.[458]

cc. Suçun Konusu

Türk Ceza Kanunu'nun 136.maddesinde düzenlenen 'Verileri hukuka aykırı olarak verme ve ele geçirme' suç tipinin konusu 135. Maddedeki suç tipi ile aynıdır. Bu suç tipinin de konusu 135. Maddede olduğu gibi kişisel veriler[459] ve bu verilerin hukuka aykırı olarak verilmesi, yayılması ve ele geçirilmesidir. Kanun metninde kişisel verilere ilişkin herhangi bir özellikten bahsedilmediği için her türlü kişisel

---

[453] Karagülmez, **Bilişim Suçları**., s.234, Yaşar, Gökcan, Artuç, **Yorumlu Uygulamalı Türk Ceza Kanunu**., s.4445. Dülger, **Kişisel Verilerin Korunması Hukuku**, s. 347

[454] Taşkın, **Bilişim Suçları**, s.106. Parlar, Hatipoğlu, **Türk Ceza Kanunu Yorumu**, s.2048. Korkmaz, **Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması**, s. 395. Dülger, **Bilişim Suçları**, s.704. Dülger, **Kişisel Verilerin Korunması Hukuku**, s. 347. Özbek, Doğan, Bacaksız, Tepe, **Türk Ceza Hukuku Özel Hükümler**, s. 583.

[455] Özbek, **TCK İzmir Şerhi**, s. 950. Ayrıca bkz. Yaşar, Gökcan, Artuç, **Yorumlu Uygulamalı Türk Ceza Kanunu**, s 4433. Ayrıca bkz. **Parlar, Hatipoğlu**, **Türk Ceza Kanunu Yorumu,** s.2043. Karagülmez, **Bilişim Suçları**, s.236.

[456] Taşkın aksi yöndeki görüşünde bu suçun mağdurunun tüzel kişiler de olabileceğini belirtmiştir. Bkz. Taşkın, **Bilişim Suçları**, s.106

[457] Ayrıntılı bilgi için çalışmamızın "Kişisel Verilerin Kaydedilmesi Suçu" başlığı altındaki "Suçun Konusu" başlığı incelenebilir.

[458] Ayrıntılı bilgi için çalışmamızın "Kişisel Verilerin Kaydedilmesi Suçu" başlığı altındaki "Mağdur" başlığı incelenebilir.

[459] Parlar, Hatipoğlu, **Türk Ceza Kanunu Yorumu**, s.2047; Korkmaz, **Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması**, s. 395. Dülger, **Bilişim Suçları**, s.704. Özbek, Doğan, Bacaksız, Tepe, **Türk Ceza Hukuku Özel Hükümler**, s. 583.

verinin hukuka aykırı olarak, verilmesi, yayılması ve ele geçirilmesi halinde bu suç işlenmiş olacaktır. [460]

Bu noktada önemle belirtmek gerekir ki, yasa koyucunun kanun yapış tekniğindeki hatasından ötürü kişisel verileri hukuka aykırı olarak verme ve ele geçirme olarak düzenlenmesi gereken suç tipi verileri hukuka aykırı olarak verme ve ele geçirme suçu olarak ifade edilmiştir. Türk Ceza Kanunu'nda kişisel verilerin korunmasına yönelik suç tipleri düzenlenirken henüz Kişisel Verilerin Korunmasına yönelik bir kanun olmaması, Yargıtay içtihatları ve Anayasa Mahkemesi kararları dışında genel olarak mevzuatımızda kişisel verinin ne olduğuna yönelik bir tanımın olmamasının bu karışıklığa sebebiyet verdiği kanaatindeyiz. Buradaki problem veri kavramının oldukça geniş bir kavram olması ve bu suç tipinin olduğu gibi yorumlanması halinde kişisel veriler ile birlikte her türlü verinin bu suçun kapsamına girebilecek olmasıdır. Ancak Türk Ceza Kanunu'nda kişisel verilerin korunmasına yönelik suç tipleri birlikte gözetildiğinde burada bahsi geçen veri kavramının 'kişisel veri' olarak değerlendirilmesi gerektiği açıktır. Nitekim kişisel veri kavramından gerçek kişilere ait kişisel veriler ifadesinin anlaşılması gerektiğine ilişkin tartışmalardan kişisel verinin tanımını tartıştığımız 135.madde kapsamında ayrıntılı olarak bahsetmiştik. Nitekim doktrinde de bu suçun konusunun kişisel veriler olduğu açıkça belirtilmiştir.[461] Kaldı ki 6698 sayılı Kişisel Verilerin Korunması Kanunu da dikkate alındığında bu maddenin konusunun kişisel veriler olduğu tartışmasız şekilde ortadadır.

dd. Hareket

Türk Ceza Kanunu'nun 136.maddesinde düzenlenen 'Verileri hukuka aykırı olarak verme ve ele geçirme' suçunda suç başlığından da anlaşılabileceği üzere verilerin hukuka aykırı şekilde 'verilmesi' ve 'ele geçirilmesi' bu suç tipinin 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

---

[460] Korkmaz, **Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması**, s. 385.

[461] Yaşar, Gökcan, Artuç, **Yorumlu Uygulamalı Türk Ceza Kanunu** s.4445. Yaşar, Gökcan, Artuç konuyu şu şekilde değerlendirmiştir. "… *Yeni Türk Ceza Kanunu'nun 136. Maddesiyle düzenlenen kişisel verileri hukuka aykırı olarak başkalarına vermek, yaymak ve ele geçirmek suçunun konusu kapsamına gerçek kişinin tanımlanması için kullanılabilecek her türlü bilgi dahil edilmiştir*."

olarak verilmesi, yayılması ve ele geçirilmesinden[462] 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.[463] Bu suçun ortaya çıkması için bir zararın doğması da şart olmadığından, bu suç seçimlik hareketli bir soyut tehlike suçu[464] olup, verme, yayma ve ele geçirme hareketlerinden birinin gerçekleştirilmesi halinde bu suç tipi işlenmiş sayılacaktır. [465] Burada verme ve yayma kavramlarından ne anlaşılması gerektiği konusunda doktrinde 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[466], yayma fiili için ise verilerin birden fazla kişiye ulaşması aranmalıdır.[467] Yani diğer bir deyişle yayma, verme fiilinin daha geniş daha ileri seviyede bir halini ifade etmektedir.[468] Doktrinde yayma seçimlik hareketinden sadece kişisel verilerin doğrudan iletilmesinin anlaşılmaması gerektiği, kişisel verilerin çevrimiçi ortamda[469] ifşanın da bir çeşit yayma olduğu ifade edilmiştir. [470] Diğer yandan bu fiiller konusunda kanunda özel bir yöntem belirtilmediğinden, kişisel verilerin her şekilde yetkisiz bir 3. Kişiye verilmesi

---

[462] Dülger, **Bilişim Suçları**, 705

[463] Özbek konuyu şu şekilde ifade etmiştir. "*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

[464] Taşkın, **Bilişim Suçları**, s. 107. Özbek, Doğan, Bacaksız, Tepe, **Türk Ceza Hukuku Özel Hükümler**, s. 585. Özbek, **TCK İzmir Şerhi**, s.961. Dülger, **Bilişim Suçları**, s.714

[465] Yaşar, Gökcan, Artuç, **Yorumlu Uygulamalı Türk Ceza Kanunu**, s.4446. Özbek, **TCK İzmir Şerhi**, s.960. Parlar, Hatipoğlu, **Türk Ceza Kanunu Yorumu**, s.2049. Özbek, Doğan, Bacaksız, Tepe, **Türk Ceza Hukuku Özel Hükümler**, s. 584.

[466] Yargıtay vermişi olduğu bir kararında "*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 nedenidi*r" şeklinde görüş bildirerek, mağdurun kişisel verisinin kimliği belirsiz bir kişiye verilmesini verileri hukuka aykırı olarak verme olarak değerlendirmiştir. Yargıtay 12. Ceza Dairesi E. 2015/12823 K. 2017/873 T. 8.2.2017

[467] Yaşar, Gökcan, Artuç, **Yorumlu Uygulamalı Türk Ceza Kanunu**, s.4446. Özbek, **TCK İzmir Şerhi**, s.960. Dülger yayma fiiliyle ilgili olarak, bu fiilin kişisel verilerin örneğin sosyal medya hesapları üzerinden ya da e-mail ya da mesaj göndermek suretiyle dahi gerçekleştirilebileceğini ifade etmiştir. Dülger, **Bilişim Suçları**, s.713

[468] Karagülmez, **Bilişim Suçları**, s.234. Taşkın, **Bilişim Suçları**, s.107

[469] 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 ceza verilmesine ilişkin kararın yerinde olduğunu ifade etmiştir. Yargıtay 12. Ceza Dairesi E. 2015/13248 K. 2017/3108 T. 12.4.2017

[470] Karagülmez, **Bilişim Suçları**, s.234

mümkündür. Nitekim doktrine göre kişisel veriler fiziksel ya da çevrimiçi fark etmeksizin pek çok biçimde verilebilecektir. [471]

Doktrinde 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.[472] 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. [473] Ayrıca doktrinde bilgilerin kulaktan kulağa şekilde aktarılması da bu suçun oluşması için yeterli olmadığı ve mutlaka bir araç kullanılması gerektiği ifade edilmiştir. [474] Nitekim Yargıtay kararı da bu yönde olup, 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.[475] Diğer yandan bu fiillerin ortak noktası ise ikisinin de verilerin aktarılması kavramını ifade etmesidir.[476] Doktrinde bu fiillerden ne anlaşılması gerektiğinin kanun maddesinde belirtilmemesinin, suçların ve

---

[471] Karagülmez, **Bilişim Suçları**, s.234, **Taşkın** konuyu şu şekilde değerlendirmiştir. "*Verme, Yayma veya Ele geçirme fiilleri verilerin elden yazılı olarak bir CD'ye, diskete ya da taşınabilir belleğe aktarılarak veya internet üzerinden elektronik ileti ya da web sitesinden verilerin ilanı gibi yollarla gerçekleştirilebilecektir. Hatta kişisel verilerin yayılması fiili yazılı veya sanal basın aracılığıyla da işlenebilecektir. Kişisel verilerin ele geçirilmesi de verilerin üzerinde yazılı olduğu belgelerin bulunduğu yerden alınması veya verilerin bulunduğu bilişim sistemine girilerek bu verilerin veri taşımaya yarayan bir araca kaydederek (CD, disket, taşınabilir bellek gibi) bu aracın alınması yoluyla da işlenebilecektir"* Taşkın, **Bilişim Suçları**, s.107

[472] Korkmaz, **Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması**, s. 393

[473] Dülger, **Kişisel Verilerin Korunması Hukuku**, s.349. Dülger konuyla ilgili olarak bu durumun kabul edilmesi halinde suç tipinin oldukça genişletilmiş sayılacağını ifade etmiştir.

[474] Özbek, Doğan, Bacaksız, Tepe, **Türk Ceza Hukuku Özel Hükümler**, s. 584.

[475] Yargıtay 12. Ceza Dairesi E. 2017/12083, K. 2018/2539, T. 7.3.2018

[476] Özbek, **TCK İzmir Şerhi**, s.960

cezaların belirliliği ilkesi kapsamında uygulamada şüpheye düşülmesine neden olacağı ifade edilmiştir.[477]

Ele geçirme kavramı ise açıkça hukuka aykırı şekilde kişisel verilerin tüm yöntemler ile[478] ele geçilmesini ifade etmekte olup sıklıkla bilişim ortamında işlenen suçların arasında yer almaktadır. Burada ele geçirme kavramı ile kaydetme kavramı arasındaki farka doktrinde dikkat çekilmiştir. Zira hukuka aykırı olarak kişisel verilerin kaydedilmesi Türk Ceza Kanunu'nun 135. Maddesinde düzenlendiğinden, burada ele geçirmenin 135. madde kapsamı dışında kalan fiillerden oluşması gerekmektedir. [479] 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. [480] Burada bir diğer önemli husus ise kişisel verilerin verildiği ya da yayıldığı yetkisiz kişi ya da kişilerin kim olacağı sorusudur. Bu sorunun cevabı için kanun maddesine baktığımızda, kişisel verilerin hukuka aykırı şekilde verilmesi ya da yayılması halinde 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. [481]

b. Manevi Unsur

Türk Ceza Kanunu'nun 136.maddesinde düzenlenen 'Verileri hukuka aykırı olarak verme ve ele geçirme' suçunun tanımında bu suçun işlenebilmesi bakımından

---

[477] Küzeci, **Kişisel Verilerin Korunması**, 2018, 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 mahkumiyet kararı verilirken beraat kararı verilmesini uygun bulmadığını açıklamıştır. Yargıtay 12. Ceza Dairesi 2015/4006 E. , 2015/18748 K. 02.12.2015T sayılı karar

[478] Dülger, **Bilişim Suçları**, s.713

[479] Özbek, **TCK İzmir Şerhi**, s. 961

[480] Yargıtay 12. Ceza Dairesi E. 2015/11703 K. 2017/870 T. 8.2.2017

[481] Karagülmez, **Bilişim Suçları**. s.234

verilerin, hukuka aykırı şekilde verilmesi, yayılması ve ele geçirilmesi halinde bu suçun oluşacağı belirtilmiştir.

Bu halde söz konusu suçun işlenmiş sayılabilmesi için bu suçun kast ile işlenmesinin yeterli olduğunu söyleyebiliriz[482] zira bahsi geçen suç tanımından suçun oluşması için gerekli özel bir saikten bahsedilmemiştir. Bu halde kast kavramının genel tanımında da yer aldığı üzere söz konusu fiillerin 'bilerek' ve 'isteyerek' işlenmesi halinde bu suçun manevi unsuru tamamlanmış olacaktır. Türk Ceza Hukukunda 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. [483]

c. Hukuka Aykırılık

Türk Ceza Kanunu'nun 136.maddesinde düzenlenen 'Verileri hukuka aykırı olarak verme ve ele geçirme' suçunun tanımında bu suçun işlenebilmesi için suça konu fiillerin hukuka aykırılık bilinci içerisinde işlenmesi gerektiği özel olarak belirtilmiştir.[484] Bu durumda kişisel veriler hukuka uygun şekilde verildiğinde, yayıldığında ya da ele geçirildiğinde bu suç oluşmayacaktır. Bu suçun oluşması için suça konu fiillerin hukuka aykırı şekilde gerçekleştirilmiş olması gerekmektedir. Doktrindeki bir görüşe göre bu madde metninde hukuku aykırılık özel olarak arandığından, hukuka uygunluk burada bir hukuka uygunluk sebebi değil, suçun unsurudur.[485]. Hukuka aykırılığın özel olarak arandığı hallere ilişkin konu 135. Maddeyi işlediğimiz bölümde ayrıntılı olarak incelendiğinden tekrar olmaması açısından yinelenmeyecektir.

Bu suç tipinde de tıpkı 135. Maddede olduğu üzere mağdurun rızası bir hukuka uygunluk sebebi olarak karşımıza çıkmaktadır.[486] Türk Ceza Kanunu'nun hakkın kullanılması ve ilgilinin rızası başlıklı 26. Maddesinde ilgilinin rızasının bulunması halinde kimsenin cezalandırılamayacağı düzenlenmiş olup bu madde bu suç tipi

---

482 Taşkın**, Bilişim Suçları,** s. 108. Karagülmez, **Bilişim Suçları**, s.236, Parlar, Hatipoğlu, **Türk Ceza Kanunu Yorumu**, s.2049. **Dülger**, Bilişim Suçları, s.714

483 Yaşar, Gökcan, Artuç, **Yorumlu Uygulamalı Türk Ceza Kanunu Yorumu** s. 4448. Taşkın**, Bilişim Suçları**, s. 108.

484 Taşkın, **Bilişim Suçları**, s.108

485 Yaşar, Gökcan, Artuç, **Yorumlu Uygulamalı Türk Ceza Kanunu Yorumu**., s. 4447. Korkmaz, **Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması**, s. 398

486 Dülger, **Bilişim Suçları**, s.714

bakımından da uygulama alanı bulacaktır. Buna göre kişinin kendi rızası dahilinde kişisel verisini veren ya da bu verilerin yayılmasına ve ele geçirilmesi halinde bu suç tipinin oluşmayacağını söyleyebiliriz.[487] Ayrıca Kişisel Verilerin Korunması Kanunu'nun kişisel verilerin aktarılması başlıklı 8. Maddesinde kişisel verilerin ilgili kişinin açık rızası olmaksızın aktarılamayacağı düzenlenmiş ve akabinde ise aynı maddenin ikinci fıkrasında bu kanun kuralının istisnaları düzenlenmiştir. Buna göre kişisel veriler aynı kanunun beşinci maddesinin ikinci fıkrasında ve gerekli önlemlerin alınmış olması şartıyla altıncı maddenin üçüncü fıkrasında yer alan koşullardan birinin olması hâlinde, veri sahibinin açık rızası olmaksızın aktarılabilecektir. Daha evvel işlediğimiz üzere 5. maddesinin ikinci fıkrasında kişisel verilerin kişinin açık rıza aranmaksızın işlenebileceği haller ve aynı şekilde 6. maddenin üçüncü fıkrasında da özel nitelikli verilerden olan sağlık ve cinsel hayata ilişkin verilerin açık rıza olmaksızın işlenebileceği haller düzenlenmiştir. Bu demektir ki, bu hallerin bulunması halinde veriler açık rıza olmaksızın işlenebileceği gibi aynı zamanda da aktarılabilecektir.

Kişisel Verilerin Korunması Kanunu'nun kişisel verilerin yurtdışına aktarılması başlıklı 9. Maddesinde kişisel verilerin veri sahiplerinin açık rızaları bulunmadan aktarılamayacağı düzenlenmiş ve akabinde ise aynı maddenin ikinci fıkrasında bu kuralın istisnaları düzenlenmiştir. Kişisel veriler, aynı kanunun 5. maddesinin 2. fıkrasında yer alan şartlardan biri veya 6. maddenin 3. fıkrasında belirtilen şartlardan birinin bulunması hâlinde ve makul güvenlik düzeyi sağlanmış ise yurt dışına aktarılabilicektir. Elbette bu noktada makul koruma düzeyinin bulunmaması halinde aktarımın yapılacağı ülkedeki veri sorumlularından taahhüt ve aynı zamanda Kurul'dan da izin alınacaktır.

Hukuka uygunluk sebepleri bakımından daha evvel yapmış olduğumuz tüm açıklamalar bu bölüm için de geçerli olduğundan tekrara düşmemek adına aynı konu bir kez daha işlenmemiştir.[488]

4. Suçun Nitelikli Halleri

[487] Dülger, **Bilişim Suçları**, s.714

[488] Hukuka uygunluk sebepleri 135. Madde kapsamında işlendiğinden ayrıntılı açıklama için lütfen ilgili bölümü inceleyiniz.

Öncelikle Türk Ceza Kanunu'nun Nitelikli Haller başlıklı 137.maddesi çerçevesinde 'Verileri hukuka aykırı olarak verme ve ele geçirme' suçunun kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanmak suretiyle işlenmesi halinde bu suç için öngörülen ceza yarı oranında artırılacaktır.[489] Diğer yandan yine aynı maddede 'Verileri hukuka aykırı olarak verme ve ele geçirme' suçunun belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle kaydedilmesi halinde öngörülen cezanın yarı oranında artırılacağı belirtilmiştir. Görüldüğü üzere söz konusu suç tipi bakımından nitelikli haller 137. Maddede sayılan suçun kamu görevlisi [490]tarafından ve görevinin verdiği yetki kötüye kullanmak suretiyle ya da belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle[491] işlenmesi halleri ile sınırlandırılmıştır. Bu noktada 135. Maddede olduğu üzere hassas kişisel veriler bakımından yasa koyucu tarafından bir ayrıma gidilmemiş ve kişisel veririnin hassas veri olup olmadığına bakılmaksızın her türlü kişisel verinin hukuka aykırı olarak verilmesi ve ele geçirilmesi suçu için aynı ceza oranı öngörülmüştür.

5. Suçun Özel Görünüş Biçimleri

a. Teşebbüs

Bu suçun teşebbüs ile işlenmesinin mümkün olup olmadığı konusunda doktrinde farklı görüşler bulunmaktır. Nitekim suç tanımında yer alan hareketlerin teşebbüse elverişli olup olmadığı pek çok yönden tartışılmıştır. Doktrindeki bazı görüşler[492] bu hareketlerin suçun neticesi ile bitişik olduğunu ve bu sebepten teşebbüs

---

[489] Taşkın, **Bilişim Suçları**, s.109. Parlar, Hatipoğlu, **Türk Ceza Kanunu Yorumu**., s.2050. **Korkmaz**, Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması, s. 419.

[490] Parlar, Hatipoğlu konuyla ilgili olarak bireylere ait adli sicil kayıtlarının ya da ceza geçmişlerini gösteren arşiv kayıtlarının yetkisiz herhangi bir kuruma, kuruluşa ya da veri sahibini resmi bir vekaletle temsil etmeyen yetkisiz bir kişiye veren görevlinin fiili ya da bu belgeleri kendisine verilen amaç dışında kullanan görevlinin eylemi ya da bu verileri yetkisiz bir erişim ile ele geçiren kişinin eylemi kişisel verileri hukuka aykırı olarak verme ve ele geçirme suçunu oluşturacaktır. Parlar, Hatipoğlu, **Türk Ceza Kanunu Yorumu,** s. 2049

[491] Parlar, Hatipoğlu konuyla ilgili olarak hukuka uygun şekilde verileri işlediği halde, daha sonra bu verileri hukuka aykırı biçimde bir başkasına veren ya da yayan kişilerin ya da kurumların, örneğin müşterilerinin bilgilerini pazarlama amacıyla kaydeden bir mağazanın daha sonra bu verileri erişim yetkisi olmayan kişilere iletmesi gibi, gerçekleştirdiği eylem kişisel verileri hukuka aykırı olarak verme ve ele geçirme suçunu oluşturacaktır. Parlar, Hatipoğlu, **Türk Ceza Kanunu Yorumu,** s. 2049

[492] Özbek, Doğan, Bacaksız, Tepe, **Türk Ceza Hukuku Özel Hükümler**, s. 586. Özbek, **TCK İzmir Şerhi**, s. 962

ile işlenemeyeceğini belirtirken, bazı diğer görüşlerde[493] ise bu suçun hareketlerinin bölünebilir olduğu durumlarda suçun teşebbüs ile işlenebileceğini belirtmektedirler.[494] Kanaatimizce işbu suçun teşebbüs aşamasında kalması mümkündür. Yargıtay kararları da bu yöndedir. Yargıtay, sanıkların mağdurların kartlarının manyetik şerit bilgilerini kopyaladığı bir somut olayda Yargıtay eğer sanıklar suç işlemek amacıyla ATM'ye koydukları hafıza kartında ilgili kişisel veriler varsa, bu durumda kişisel verilerin hukuka aykırı verilmesi ve ele geçirilmesi suçunun oluşacağını; diğer yandan bu kayıtlar yoksa bu suça teşebbüsün söz konusu olacağını ifade etmiştir.[495]

b. İştirak

Türk Ceza Kanunu'nun 136. maddesinde düzenlenen verileri hukuka aykırı olarak verme ve ele geçirme suçu iştirak halinde işlenmesi işlenebileceği görüşündeyiz. [496] Bu suç iştirak bakımından bir özellik arz etmemektedir.[497] Bu suçun iştirak halinde işlenebilmesi için faillerin her birinin seçimlik hareketleri birbirleri ile anlaşmalı şekilde gerçekleştirmeleri gerekmektedir. [498]Zira eğer birden fazla fail birbirlerinden habersiz şekilde ve ortada birlikte suç işleme kastı bulunmaksızın seçimlik hareketleri gerçekleştirmişler ise bu durumda her bir fail ayrı ayrı olarak bu suçu işlemiş sayılarak ayrı ayrı cezalandırılacaklardır. Yani örneğin faillerden biri kişisel verileri ele geçirmiş ve daha önce bu suçu işlemek için anlaşmış olduğu diğer fail de bu verilerin yayılmasına sebebiyet vermiş ise bu durumda söz konusu failler bu suçu iştirak halinde işlemiş sayılacaklardır. Diğer yandan ise bu failler birbirlerinden

---

[493] Yaşar, Gökcan, Artuç konuyla ilgili olarak olayda suçu oluşturan hareketlerin bölünebiliyor olması durumunda kişisel verileri hukuka aykırı olarak verme ve ele geçirme suçunun teşebbüse elverişli olduğunu ifade etmiş ve bir doktorun hastasına ait bir sağlık verisini hastasının bilgisi haricinde yetkisiz kişilerle paylaşma konusunda anlaştıktan sonra verileri paylaşacağı anda eylemin yarım kalması durumunda suçun teşebbüs aşamasında kalacağını ifade etmiştir. Yaşar, Gökcan, Artuç, **Yorumlu Uygulamalı Türk Ceza Kanunu Yorumu**, s. 4448. Taşkın ise konuyu *"Suça teşebbüs mümkündür. Eylemler tamamlanamazsa suç teşebbüs aşamasında kalacaktır."* şeklinde değerlendirmiştir. Taşkın, **Bilişim Suçları,** s.108. Parlar, Hatipoğlu, **Türk Ceza Kanunu Yorumu**, s.2050.

[494] Korkmaz, **Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması**, s. 408. Korkmaz konuyu şu şekilde örneklendirmiştir. "*Fail birinin kişisel verilerini başkasına vermek için harekete geçtikten sonra elinde olmayan sebeplerle veri vermeye çalıştığı kişiye ulaşamaz ise kişisel vermek suçuna teşebbüs söz konusu olacaktır.*" Dülger, **Bilişim Suçları**, s.714. Dülger, **Kişisel Verilerin Korunması Hukuku**, s.356

[495] Yargıtay 8. Ceza Dairesi, E. 2016/12565, K. 2017/12892 T. 20.11.2017

[496] Yaşar, Gökcan, Artuç, **Yorumlu Uygulamalı Türk Ceza Kanunu Yorumu**, s. 4448. **Parlar, Hatipoğlu**, Türk Ceza Kanunu Yorumu, s.2050.

[497] Özbek, Doğan, Bacaksız, Tepe, **Türk Ceza Hukuku Özel Hükümler**, s. 585. Özbek, **TCK İzmir Şerhi**, s. 962. Taşkın, **Bilişim Suçları**., s.108. Dülger, **Bilişim Suçları**, s.715

[498] **Korkmaz**, Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması, s. 410.

bağımsız olarak bu suçları işlemişlerse her bir fail hareketi tamamladığı noktada söz konusu suçu ayrı ayrı işlemiş sayılacaklardır.

c. İçtima

Türk Ceza Kanunu'nda düzenlenen içtima hükümleri burada da uygulama alanı bulacaktır.[499] Buna göre kanunun 43. Maddesi çerçevesinde söz konusu suçun değişik zamanlarda bir kişiye karşı birden fazla kez işlenmesi durumunda ya da aynı suçun birden fazla kişiye tek bir hareket ile işlenmesi halinde bir cezaya hükmedileceği ve bu suçun zincirleme suçu oluşturacağını söyleyebiliriz. [500] Bu durumda verilecek ceza, dörtte birinden dörtte üçüne kadar artırılacaktır. Bu kapsamda 136. Maddenin Türk Ceza Kanunu'nda düzenlenen ilgili diğer suçlar ile ilişkisini incelemek yerinde olacaktır. [501]

136. Madde ile Türk Ceza Kanunu'nda düzenlenen 134. Maddesindeki "Özel Hayatın Gizliliğini İhlal Suçu"nun birlikte değerlendirildiği Yargıtay kararında, "*Sanığın, mağdurun fotoğrafını mağdur adına açtığı sahte facebook hesabında yayınlaması şeklinde sübutu kabul edilen eyleminin, mağdurun gündelik elbiseler ile poz vermiş ve baş bölgesi ile vücudunun bir kısmını gösteren fotoğrafı ile ad ve soyadının kişisel veri niteliğinde olması karşısında sanık hakkında 136. Madde kapsamında hüküm kurulması gerekirken, "özel hayatın gizliliğini ihlal" suçundan mahkumiyete karar verilmesi…isabetsizdir"* şeklinde görüş bildirilmiştir. Görüldüğü üzere Yargıtay somut olayda hangi suçun söz konusu olduğunu incelerken, çekilen fotoğrafın durumunu dikkate alarak olayı 136. madde kapsamında değerlendirmiştir.

136. Madde ile Türk Ceza Kanunu'nda düzenlenen 135. Maddesindeki "Kişisel Verilerin Hukuka Aykırı Kaydedilmesi Suçu"nun birlikte değerlendirildiği Yargıtay kararında, "*…sanığın katılanın ad ve soyadıyla birlikte katılanın göz bölgesinin resmini kendi facebook adresinde yayınlayan sanığın verileri hukuka aykırı olarak*

---

[499] Prof. Dr. Fatih Selami Mahmutoğlu, **Türk Ceza Kanunu'nda Yer Alan Bilişim Alanındaki Suçlar Ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi,** Çevrimiçi http://fsmahmutoglu.av.tr/pdf/aec4ba0684aa8f46aec75249e66d910173a2f8f47818077253.pdf (Erişim Tarihi:13.01.2019). Taşkın, **Bilişim Suçları,** s. 108. **Parlar, Hatipoğlu**, **Türk Ceza Kanunu Yorumu**, s.2050.

[500] Özbek, **TCK İzmir Şerhi**, s. 962

[501] Türk Ceza Kanunu'nun 135. ve 136. Maddesi arasındaki içtima açıklamaları için kişisel verilerin kaydedilmesi suçu başlıklı bölümün içtima başlıklı bölümünü inceleyiniz.

verme veya ele geçirme ve kişisel verilerin kaydedilmesi suçlarını işlediğinin iddia edildiği olayda; sanığın katılanın ad ve soyadı ile göz bölgesine ait resmi yayımlaması eyleminin bir bütün halinde verileri hukuka aykırı olarak verme veya ele geçirme suçunu oluşturduğu gözetilmeden yasal, yeterli ve geçerli bir gerekçeye dayanılmaksınız eylemin iki ayrı suç oluşturduğundan bahisle verileri hukuka aykırı olarak verme veya ele geçirme ve kişisel verilerin kaydedilmesi suçlarından ayrı ayrı mahkumiyet hükmü kurulması, isabetsizdir…" şeklinde görüş bildirerek, somut olayda 136. madde kapsamındaki suçun oluşabilmesi için geçit niteliğinde olan 135. maddeden de ceza verilmesini hatalı bulmuş ve sanığın yalnızca 136. maddedeki verileri yayma ve ele geçirme suçundan cezalandırılması gerektiğini ifade etmiştir.[502]

136. Madde ile Türk Ceza Kanunu'nda düzenlenen 243. Maddesindeki "Hukuka Aykırı Olarak Bilişim Sistemine Girme ve Sistemde Kalma" suçu birlikte değerlendirildiğinde, yani fail hem mağdurun bilişim sistemine girmiş, orada kalmış ve akabinde verileri ele geçirmiş ise bu durumda bazı yazarlar iki suç arasında "*geçit ilişkisi* [503] oluştuğunu ve failin bu durumda 136. Madde kapsamında cezalandırılması gerektiğini ifade etmişlerdir. [504] Doktrinde bazı diğer görüşler ise bu iki suç tipinin aynı hukuki değerleri korumadığı ve birinin işlenmesi için diğerinin zorunlu olmadığı gerekçesi ile bu suçlar arasında geçit ilişkisinin oluşmayacağını bu bakımından failin her iki suçtan ayrı ayrı gerçek içtima kuralları uygulanmak suretiyle cezalandırılması gerektiğini ifade etmektedirler. [505]

136. Madde ile Türk Ceza Kanunu'nda düzenlenen 245. Maddesindeki "Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu'nun birlikte değerlendirildiği bir Yargıtay kararında mağdurların kişisel bilgileri ele geçirildikten sonra bu bilgiler ile kart bastırılmamış ve ancak kopyalama yapılan cihazda veriler bulunuyorsa 136. maddenin uygulanması gerektiğini, cihazda veri yok ise teşebbüs hükümlerinin uygulanması gerektiğini bildirmiştir. Görüldüğü üzere Yargıtay her iki suçu içtima ve teşebbüs bakımından değerlendirmiş ve bireylere ait kişisel verilerin kopyalanması durumunda 136. maddede düzenlenen suçun oluşacağını, bu bilgilerin kullanılarak kart oluşturulması ve harcama yapılması halinde ise 245. maddenin uygulanacağını

[502] Yargıtay 12. Ceza Dairesi E. 2017/5654, K. 2018/2911 T. 14.3.2018
[503] Taşkın, **Bilişim Suçları**, s.109
[504] Korkmaz, **Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması**, s. 416.
[505] Dülger, **Bilişim Suçları**, s.715

ifade etmiştir. Dolayısıyla Yargıtay 136. Madde ile Türk Ceza Kanunu'nda düzenlenen 245. Maddesindeki "Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu" arasında, verilerin hukuka aykırı olarak verme ve ele geçirme suçunun geçit niteliğini vurgulamış ve bu halde sanığın 245. madde kapsamında cezalandırılacağını ifade etmiştir.[506]

6. Yaptırım ve Yargılama Usulü

Türk Ceza Kanunu'nun 137. Maddesine göre verileri hukuka aykırı olarak verme veya ele geçirme suçunu işleyen kişi iki yıldan dört yıla kadar hapis cezası ile cezalandırılabilecektir. Yukarıda da belirttiğimiz üzere bu suçun kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanmak suretiyle ya da belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenmesi hallerinde verilecek ceza yarı oranında artırılabilecektir.[507] Elbette bu suçun failinin kamu görevlisi olması halinde kamu görevlisi hakkında soruşturma başlatılabilmesi için gerekli soruşturma izninin alınması gerekecektir.[508]

Yine Türk Ceza Kanunu'nun 139. Maddesinde Verileri hukuka aykırı olarak verme veya ele geçirme suçunun şikâyet bağlı olmadığı düzenlenmiştir. Yargıtay'da vermiş olduğu bir kararında bu konuya değinerek, mağdur sanıkların birbirlerine karşı sunmuş oldukları şikayetleri geri almalarının, bu suçun kovuşturulması ve soruşturulması şikâyete tabi olmadığından, düşme kararı verilmesinin kanuna aykırı olduğu belirtmiştir. [509] Ayrıca Türk Ceza Kanunu'nun 140. maddesi uyarınca tüzel

---

[506] Yargıtay 8. Ceza Dairesi, 08.10.2018T, 2018/10436 K., 2018/6171E sayılı karar

[507] Dülger, **Bilişim Suçları**, s.716

[508] Yaşar, Gökcan, Artuç**, Yorumlu Uygulamalı Türk Ceza Kanunu Yorumu,** s.4450. Parlar, Hatipoğlu, **Türk Ceza Kanunu Yorumu**, s.2050.

[509] „*Dosya kapsamına göre; erkek arkadaşının sanık D.ile kendisini aldattığını düşünen sanık A.'nın, bir sosyal paylaşım sitesine "O. E." adıyla üyelik işlemleri yaparak, elektronik posta adresi oluşturduğu sitede, bir başka bayana ait göğüs dekolteli bir resim koyup, sanık D.'e ait cep telefonu numarasına da yer vermesi sonucu, tanımadığı kişiler tarafından telefonundan aranarak cinsel içerikli arkadaşlık teklifleri alan sanık D.'in, cep telefonu numarasını yayan kişinin sanık A. olduğunu öğrenmesi üzerine, kendisini telefonundan arayan tanımadığı kişilere, telefon numarasını değiştirdiğini belirterek, sanık A.'nın kullanımındaki cep telefonu numarasını verdiği ve sanık A.'nın da tanımadığı kişiler tarafından telefonundan aranarak rahatsız edilmesi üzerine her iki sanığın birbirlerinden şikayetçi olup, bilahare şikayetlerinden vazgeçtikleri olayda, TCK'nın 139/1. maddesi gereğince, sanıkların üzerlerine atılı verileri hukuka aykırı olarak verme veya ele geçirme suçunun, soruşturulması ve kovuşturulmasının şikayete bağlı olmadığı gözetilmeden, kovuşturma aşamasında her iki mağdur sanığın şikayetlerinden vazgeçtiklerinden bahisle, yazılı şekilde düşme kararı verilmesi…kanuna aykırı olup…"* Yargıtay 12. Ceza Dairesi E. 2012/22005 K. 2013/24489 T. 4.11.2013

kişilerin bu suça konu verilerden yararlanması halinde de tüzel kişilere özgü güvenlik tedbirleri uygulanacaktır. [510]

C. VERİLERİ YOK ETMEME SUÇU

1. Genel Olarak

Türk Ceza Kanunu'nun 138. Maddesine göre kanunların belirlediği sürelerin geçmiş olmasına rağmen verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde bir yıldan iki yıla kadar hapis cezası verileceği düzenlenmektedir. Bu maddenin de 765 sayılı Türk Ceza Kanunu'nda karşılığının bulunmadığını[511] ve bu suçun bağımsız bir suç olarak düzenlendiğini belirtmek isteriz.[512] Esasen yasa koyucu bu madde ile amacı söz konusu verilerin saklanması için gerekli sebepler ortadan kalktıktan sonra yok edilerek sürekli bu verilere erişimi engellemek, insanların kendilerini güvende hissederek siyasal sisteme karşı güvenlerini kaybetmemelerini istemiştir.[513] Bu anlamda yerinde bir düzenleme olmuştur. Öncelikle tıpkı 'Verileri hukuka aykırı şekilde verme veya ele geçirme' suçunda olduğu üzere yasa koyucu burada da yine *kişisel veri* yerine *veri* olarak ifade ederek söz konusu suç tanımını yaparken bir kez daha yasa yapma tekniği açısından hataya düşmüştür. Bu hususstaki tartışmaya daha evvel yer verildiğinden tekrar olmaması açısından burada bir kez daha yer verilmeyecektir.

Türk Ceza Kanunu'nun 138. Maddesi değerlendirildiğinde, kişisel verilerin yok edilmesini gerektiren haller kapsamında, "*kişisel verilerin işlenmesini gerektiren sebeplerin ortadan kalkması"* ve "*kanunlarda yer alan sürelerin sona ermesi sebepleri"* karşımıza çıkmaktadır. Yasa koyucu bu suçun oluşabilmesi bakımından, kişisel verilerin saklanması için kanunlarda öngörülmüş bir süre ve bu sürelerin geçmiş olmasına rağmen kayıtlı kişisel verilerin ilgili sistemden yok etmekle görevli kişilerin bu kişisel verileri yok etmemesi şartlarını aramıştır. Doktrinde kanunda on beş gün, otuz gün gibi özel olarak bir süre belirtilmemesine rağmen, örneğin kişisel verilerin

---

[510] Taşkın, **Bilişim Suçları**, s.109
[511] Parlar, Hatipoğlu, **Türk Ceza Kanunu Yorumu,** s.2053. Yaşar, Gökcan, Artuç, **Yorumlu Uygulamalı Türk Ceza Kanunu Yorumu**, s.4460
[512] Karagülmez, **Bilişim Suçları**, s.237. Taşkın, **Bilişim Suçları**, s.110. **Özbek**, op.cit., s. 964
[513] Dülger**, Bilişim Suçları**, 7719

"*derhal"* [514] silinmesi hususuna atıf yapan bir kanun maddesine aykırı olarak kişisel verilerin yok edilmemesi halinde ne olacağı tartışılmış ve bizim de katıldığımız bir görüşe göre 138. Madde kapsamındaki bu suç bu halde de oluşacaktır.

Doktrinde bu suçun Türk Ceza Kanunu'nun 257. Maddesinde düzenlenen görevi kötüye kullanma suçunun özel bir şekli olduğu ifade edilmiştir.[515] Bu yazarlara göre bu suç kapsamında kanunda belirtilen sürelere uygun olarak kişisel verilerin yok edilmesi gerektiği için ve bu durumda bu suçun işlenmesi halinde, suçtan zarar görenin aynı zamanda kamu olduğu göz önünde bulundurulduğunda, suçu işleyen failin de kamu görevlisi sıfatı ile bu suçu işlemiş olacağı ve ancak burada 138. Madde daha özel bir düzenleme olduğundan, öncelikli olarak uygulama alanı bulacağı ifade edilmiştir[516] Ancak biz bu görüşe katılmamaktayız, zira söz konusu verileri yok etmekle görevli kişinin mutlaka kamu görevlisi olması gerekmemektedir.[517] Kaldı ki Kişisel Verilerin Korunması Kanunu da dikkate alındığında görülecektir ki bu kanun mevzuatımıza veri sorumlusu kavramını eklemiştir.

6698 sayılı KVKK kapsamında veri sorumlusu "Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi" ifade etmektedir. Görüleceği üzere ilgili kanuna göre kişisel verileri hukuka uygun şekilde işlemek ve zamanı geldiğinde usulüne uygun şekilde silip, yok etmekle yahut anonim hale getirmekle yükümlü olan veri sorumlusudur. Bu durum da Türk Ceza Kanunu'nun 138.maddesinde düzenlenen 'Verileri yok etmeme' suçunun failinin artık KVKK'da

---

[514] Yaşar, Gökcan, Artuç bu konuyla ilgili olarak süre bakımından kanunlarda belirli bir süre öngörülmüş olması ile verilerin hemen ya da derhal yok edilmesi gibi ifadelerin sonuç bakımında fark etmemekte olduğunu, her iki ifadenin de kişisel verilerin silinmesi bakımından belirli bir süre niteliğini taşıdığını ve bu sürelerin sonunda verilerin yok edilmesi gerektiğini ifade etmiştir. Yaşar, Gökcan, Artuç, **Yorumlu Uygulamalı Türk Ceza Kanunu Yorumu**, s.4460

[515] Yaşar, Gökcan, Artuç, **Yorumlu Uygulamalı Türk Ceza Kanunu Yorumu**, s. 4460. Taşkın, op.cit., 110. Taşkın konuyla ilgili olarak bahsi geçen suç ile korunmak istenilen hukuki menfaatin kamu görevlilerinin disiplinli şekilde idaresi ve kamu görevinin yerine getirilmesi ile kamu menfaatinin elde edilmesi olduğunu ifade etmektedir. Dülger, **Bilişim Suçları**, s.720

[516] Taşkın, **Bilişim Suçları**, 110

[517] Aynı yönde görüş için bkz. Korkmaz, **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, s.426. Nil Melek Gültekin, "**Kişisel Verilerin Ceza Hukuku Yönünden Korunması**", Yüksek Lisans Tezi, Galatasaray Üniversitesi, 2012, s.182. Gültekin konuyu şöyle değerlendirmiştir. " *Dolayısıyla bu tür verilerin yok edilmesi gerektiğinde bunu yapmakla yükümlü olan ancak kamu görevlisi olmayan pek çok kişi vardır. Bu itibarla verileri yok etmeme suçu açısından, madde metninde değinilen "görev" kavramını kamu görevi ile sınırlamak maddenin düzenleniş amacına da aykırı olacak, kamu görevlisi olmayıp kişisel verileri yok etme görevini yerine getirmeyen kişilere karşı bu yaptırımın uygulanamamasına sebep olacaktır.".* Ayrıca bakınız Dülger, **Bilişim Suçları**, s.720

düzenlenen veri sorumlusu kavramının da dikkate alınarak değerlendirilmesi gereğidir. Bu halde bu kişi Türk Ceza Kanunu kapsamındaki verileri yok etmeme suçunun faili kamu görevlisi olabileceği gibi, kamu görevlisi olmayan ancak örneğin çalıştığı şirket tarafından veri sorumlusu atanmış herhangi bir gerçek kişi de olabilecektir. Bu durumda Türk Ceza Kanunu'nun 138. Maddesinde yer alan suçun oluşması halinde, veri sorumlusu söz konusu suçun faili olacaktır. Bu noktada veri sorumlusunun tüzel kişi olması halinde özel hukuk bakımından sorumlu tutulabilecekse de ceza hukuku bakımından tüzel kişiler bu suçun faili olamayacaklarından gerçek kişi fail ya da faillere ulaşılması gerekecektir. [518]

Doktrinde bu düzenlemenin kişisel verilerin korunması bakımından temel ilkelerden biri olan süre sınırı ile uyumlu olduğu belirtilmiştir.[519] Ancak burada bahsedilen süre sınırı esasen kişisel verinin işlenmesi için mevcut amacın ortadan kalkmasını ifade etmektedir. Zira temel olan budur. Kişisel verilerin işlenmesi için belirtilen amacın ortadan kalkmış olması halinde, Türk Ceza Kanunu'nun 138. Maddesi kapsamında kişisel verilerin yok edilmesi gerekecektir. Ancak madde metni incelendiğinde burada esas alınan sürenin, amacın ortadan kalkmasına bağlı değil kanunların belirlediği sürelere bağlı olduğu görülecektir.[520]

Diğer yandan doktrindeki bizim de katıldığımız bazı görüşler, '*kanun'* ibaresinden anlaşılması gerekenin geniş tutulması gerektiğini ve bu ifadeden genel olarak mevzuatımızın tamamının anlatılmak istendiği belirtilmiştir.[521] Ayrıca doktrinde süre kavramından anlaşılması gerekenin on gün ya da otuz gün gibi kesin sürelerden ayrı, daha geniş şekilde anlaşılması gerektiği belirtilmiştir. [522]

---

[518] Dülger, **Bilişim suçları**, s.675

[519] Küzeci, **Kişisel Verilerin Korunması**, 2018, s.408

[520] Küzeci bu konuyla ilgili olarak bu durumun amaca bağlılık ilkesi ile örtüşmediğini ifade ederek eleştirmiştir. Küzeci, **Kişisel Verilerin Korunması**, 2018, s.408. Korkmaz, **Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması**, s.423. Korkmaz kişisel verilere hukuka uygun şekilde işlense dahi bu işlemenin en nihayetinde bireylerin özel hayatına müdahale etmek olduğu anlamına geldiğini ve bu bakımdan kişisel verilerin işlenmesine ilişkin amaç ortadan kalktıktan sonra yok edilmeleri ya da anonim hale getirilmeleri gerektiğini ifade etmiştir. Kuşkonmaz, **Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması**, s.161

[521] Karagülmez, **Bilişim Suçları**, s. 238. Karagülmez diğer türlü okunması halinde, madde kapsamının oldukça dar yorumlanması gerekeceğini belirtmiştir. Dülger, **Bilişim Suçları**, s.722

[522] Özbek, Doğan, Bacaksız, Tepe, **Türk Ceza Hukuku Özel Hükümler**, s. 589. Özbek, TCK İzmir Şerhi, s.965. Dülger, **Bilişim Suçları**, s.722

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 'Kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesi' başlıklı 7.maddesi çerçevesinde ise "hukuka uygun şekilde işlenmiş olmasına rağmen kişisel verilerin işlenmesini gerektiren sebepler ortadan kalktıysa veri sahibinin talebi üzerine veya resen söz konusu verilerin veri sorumlusu tarafından silineceği, yok edileceği veya anonim hale getirileceği" ifade edilmiştir. Görüldüğü üzere Kişisel Verilerin Korunması Kanunu'nun ilgili maddesinde süre ile sınırlılık amaca bağlı olarak tanımlanmış ve bu haliyle kişisel verilerin korunması konusunun temel ilkeleri ile uyumlu bir düzenleme yapılmıştır.

Türk Ceza Kanunu'nun 138. Maddesinden farklı olarak Kişisel Verilerin Korunması Kanunu'nun 7.maddesi ile kişisel verilerin yok edilmesi bakımından yeni ve farklı yöntemlerden bahsedilmesidir. Kişisel Verilerin Korunması Kanunu'nun 7. maddesinde; "*kişisel verileri silmeyen veya anonim hâle getirmeyenler 5237 sayılı Kanunun 138 inci maddesine göre cezalandırılır"* şeklinde düzenleme yapılmıştır. Anonim hale getirme ve silme yöntemlerinin eklenmesi ile uluslararası mevzuata uygun bir düzenleme yapılmıştır. Nitekim Kişisel Verilerin Korunması Kanunu'nun yürürlüğe girmesinden sonra 28 Ekim 2017 tarihinde *Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmelik* yürürlüğe girmiştir.

Kişisel Verilerin Korunması Kanunu'nun 7.maddesinde ise kişisel verilerin 'anonim getirilmesi 'silinmesi' veya 'yok edilmesi' yoluyla ortadan kaldırılmasından bahsedilmektedir. 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun '*suçlar'* başlıklı 17.maddesinde ise "*bu kanunun 7.maddesi hükmüne aykırı olarak; kişisel verileri silmeyen veya anonim hâle getirmeyenler 5237 sayılı Kanunun 138 inci maddesine göre cezalandırılır."* şeklinde düzenleme yapılmıştır. Burada 7. Madde kapsamında kişisel verilerin 'yok edilmesi'nden de bahsetmekteyken, 17.madde kapsamında ise yalnızca 'silme' ve 'anonim hale getirme 'eylemlerinden bahsedilmiştir. Doktrinde bu çelişki karşısında, Kişisel Verilerin Korunması Kanunu'nun 7.maddesinde kişisel verileri yok etmeyen kişi hakkında 138. Maddenin uygulaması hususunda kanunilik ilkesi bakımından sorun doğabileceği belirtilmiştir.[523] Ayrıca bir diğer tartışılması gereken husus ise 138. Madde

[523] Küzeci, **Kişisel Verilerin Korunması**, 2018, s.409. Korkmaz, K**işisel Verilerin Türk Ceza Kanunu Kapsamında Korunması**, s.424.

kapsamındaki '*sistemden yok edilmesi*' ibaresidir. Zira kanun metnine göre bu suçun işlenmesi için kişisel verilerin mutlaka bir sistem üzerinde işlenmiş olması gerekmektedir. Ancak bu algı doğru değildir. Kanımızca bu da yasa koyucunun kanun yapış tekniğinden kaynaklı bir hatasından ileri gelmektedir. Doktrinde buradaki sistem ibaresinden yalnızca bilişim sistemlerinin değil, aynı zamanda bilişim sistemleri kapsamında olmamakla birlikte kişisel verilerin tutulduğu yerin de anlaşılması gerektiği belirtilmiştir.[524] Zira kanunda kişisel verilerin korunmasını düzenleyen diğer 135 ve 136. Maddeler kapsamında böyle bir düzenleme yer almamaktadır. Diğer yandan bizim de katıldığımız bir görüşe göre, kanunun ilgili maddesindeki bu ifade son derece açık olup direk olarak bilişim sistemlerine gönderme yapmaktadır. Bu anlamda kanunilik ilkesi açısından bu ifadenin değiştirilmesi ya da çıkarılması gerektiği düşüncesindeyiz.[525]

2. Suçla Korunan Hukuksal Değer

Türk Ceza Kanunu'nun 138. Maddesinde düzenlenen verileri yok etme suç tipi, konusu kişisel veriler olan diğer suç tipleri gibi 'Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar' başlıklı dokuzuncu bölümünde düzenlenmiştir. Buna göre ilgili suç tipi ile korunmak istenen hukuki yararın uluslararası düzenlemelere paralel şekilde genel olarak kişilerin özel hayatı ve hayatın gizli alanı[526], özel olarak ise kişisel verilerin korunması olduğunu söyleyebiliriz.[527]

Doktrinde bu suçun kamusal yönü dikkate alınarak bu suç ile korunan hukuki değerin kamu idaresinin güvenirliği ve işleyişi olduğu ifade edilmiştir.[528] 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

---

[524] Karagülmez, **Bilişim Suçları**, s.239
[525] Küzeci, **Kişisel Verilerin Korunması**, 2018, s.408
[526] Yaşar, Gökcan, Artuç, **Yorumlu Uygulamalı Türk Ceza Kanunu Yorumu**, s.4461. Özbek, **TCK İzmir Şerhi**, s. 964. Özbek, Doğan, Bacaksız, Tepe, **Türk Ceza Hukuku Özel Hükümler**, s. 588.
[527] Taşkın, **Bilişim Suçları**, s. 111. Kuşkonmaz, **Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması**, s. 129, Dülger, **Bilişim Suçları**, s. 675,704. Karagülmez, **Bilişim Suçları**, s.237. Korkmaz, **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, s.427
[528] Dülger, **Bilişim Suçları**, s. 718. Dülger, **Kişisel Verilerin Korunması Hukuku**, s.360

edilmesi hususu ile bireyin özel hayatına keyfi müdahalelerin önlenmesi amaçlanmıştır.[529]

3. Suçun Unsurları

a. Maddi Unsurlar

aa. Fail

Türk Ceza Kanunu'nun 138.maddesinde düzenlenen 'Verileri yok etmeme' suçunun failinin kişisel verileri yok etmekle yükümlü olduğu belirli süreler geçtikten sonra bu kişisel verileri yok etmeyen kişiler olduğunu[530] ve bu bakımdan bu suçun özgü suç niteliğinde olduğunu söyleyebiliriz.[531] Burada önemli olan kişisel verileri yok etmekle yükümlü olan kişinin kanuni bir yükümlülüğünün olmasıdır ve kişinin kamu görevlisi olup olmaması bu bakımından önemli değildir.[532] Ceza Muhakemesi Kanunu'nda kişisel verilerin işlenmesine ilişkin pek çok madde bulunmakta olup aynı maddelerde bu kişisel verilerin yok edilmesi için gereken düzenleme de yapılmıştır. Örneğin "*Kararların yerine getirilmesi, iletişim içeriklerinin yok edilmesi"* başlıklı 137. Maddesinin 3. Fıkrasında görevlilerin kişisel verilerin kaydı akabinde bu verileri hangi süreler içerisinde yok etmesi gerektiği de düzenlenmiştir. Keza aynı şekilde "*Genetik inceleme sonuçlarının gizliliği"* başlıklı 80. Madde kapsamında da yine görevlilerin kişisel verilerin kaydı akabinde bu verileri hangi süreler içerisinde yok etmesi gerektiği de düzenlenmiştir.[533] Keza yukarıda ayrıntılı olarak işlediğimiz üzere Kişisel Verilerin Korunması Kanunu da dikkate alındığında görülecektir ki bu kanun mevzuatımıza veri sorumlusu kavramını eklemiştir. Bu durumda fail kamu görevlisi olabileceği gibi veri sorumlusu olarak atanan başka herhangi bir gerçek kişi de olabilecektir.[534]

---

[529] Parlar, Hatipoğlu, **Türk Ceza Kanunu Yorumu**, s.2053
[530] Dülger, **Bilişim Suçları**, s.720
[531] Taşkın, **Bilişim Suçları**, s. 111. Yaşar, Gökcan, Artuç, **Yorumlu Uygulamalı Türk Ceza Kanunu Yorumu,** s.4461. Özbek, **TCK İzmir Şerhi**, s. 964. Özbek, Doğan, Bacaksız, Tepe, **Türk Ceza Hukuku Özel Hükümler**, s. 588.
[532] Karagülmez, **Bilişim Suçları**, s.239, Yaşar, Gökcan, Artuç, **Yorumlu Uygulamalı Türk Ceza Kanunu Yorumu**, s.4461. Taşkın, **Bilişim Suçları**, s. 111. Dülger, **Bilişim Suçları**, s.720.
[533] Parlar, Hatipoğlu, **Türk Ceza Kanunu Yorumu,** s.2054
[534] Özbek, **TCK İzmir Şerhi,** s.965

bb. Mağdur

Türk Ceza Kanunu'nun 138.maddesinde düzenlenen 'Verileri yok etmeme' suçunun mağduru tıpkı 135. Maddede olduğu üzere yalnızca gerçek kişiler olacaktır. Madde tanımı dikkate alındığında bu suçun mağdurunun kişisel verileri hukuka uygun olarak işlendiği halde, kanunda belirtilen süreler içinde bu verileri yok etmekle görevli olan kişiler tarafından kişisel verileri yok edilmeyen herkes olabilecektir.[535]

Diğer yandan doktrindeki bazı görüşlerde ise bu suçun esas mağdurunun kamu olduğu ve kişisel verisi maddeye uygun şekilde yok edilmeyen gerçek kişinin ise suçtan zarar gören sıfatını alabileceği ifade edilmiştir.[536] Esasen daha evvel de belirttiğimiz üzere, bizim konudaki görüşümüz bu suçun mağdurunun yalnızca kişisel verisi usulüne uygun şekilde yok edilmeyen kişi olabilecektir.[537] Kaldı ki Türk Ceza Kanunu'nda düzenlenmiş tüm suç tipleri bir ölçüde kamu düzenini korumak amaçlı olduğu düşünüldüğünde bu suç tipi kapsamında mağdurun kamu olduğunu söylemek doğru olmayacaktır.[538]Zira bu suç tipleri kapsamında korunmak istenen kişilerin özel hayatı ve kişisel verilerinin korunması hakkı olduğundan, suçun mağduru da yalnızca bu kişiler olabilecektir. Nitekim tüm uluslararası düzenlemeler de bu yönde olup, Avrupa Birliği Veri Koruma Tüzüğü yürürlüğe girdikten sonra verilmiş olan bir Alman Mahkemesi kararında yargıya başvuruda başvurucunun yalnızca kişisel verilerinin sahibi olabileceği yönünde görüş bildirilmiş ve yargı yolu başvurusunu reddetmiştir.[539]

cc. Suçun Konusu

Türk Ceza Kanunu'nun 138.maddesinde düzenlenen 'Verileri yok etmeme' suç tipinin konusu kişisel verilere ilişkin diğer suç tipleri ile aynıdır. Bu suç tipinin de

---

[535] Yaşar, Gökcan, Artuç, **Yorumlu Uygulamalı Türk Ceza Kanunu Yorumu**, s.4461
[536] Taşkın, **Bilişim Suçları**, 112. Dülger, **Bilişim Suçları**, s.720
[537] Özbek, **TCK İzmir Şerhi**, s.965
[538] Korkmaz, **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, s.427. Dülger, **Kişisel Verilerin Korunması Hukuku**, s.362
[539] Mahkeme bu kararında GDPR'a dayanarak yalnızca kişisel verilerin sahibi olan kişilerin ve çok istisnai durumlarda sivil toplum kuruluşlarının kişisel veri hakkı ihlali ile mahkemeye başvurabileceğini belirtmiştir. Regional Court Bochum, 12th Civil Chamber, I-12 O 85/18, 08/07/2018 http://www.justiz.nrw.de/nrwe/lgs/bochum/lg_bochum/j2018/I_12_O_85_18_Teil_Versaeumnis_und_Schlussurteil_20180807.html

konusu hukuka uygun olarak işlenmiş kişisel verilerdir.[540] Kanaatimizce de bu suçun konusu kişisel verilere karşı işlenen diğer suçlarda olduğu üzere kişisel verilerdir.

dd. Hareket ve Netice

Türk Ceza Kanunu'nun 138.maddesinde düzenlenen 'Verileri yok etmeme' suç tipinde kanunların belirlediği sürelerin geçmiş olmasına[541] karşın kişisel verilerin sistem içinde yok edilmemesi halinde söz konusu suç işlenmiş sayılacaktır.[542] Bu durumda kanunların belirlediği sürelerin geçmesi ve bu sürelerin geçmesine rağmen kişisel verilerin sistemden yok edilmemesi eylemlerinin tamamlanması bu suçun işlenmesi için yeterli olacaktır.

Burada suçun oluşması için herhangi bir şekilde kişinin zarar görmesi ya da herhangi bir netice oluşmasına gerek yoktur.[543] Bu anlamda bu suç aynı zamanda soyut bir tehlike suçu olarak değerlendirilebilir. [544]

Diğer tartışılması gereken konu ise 'verilerin yok edilmemesinden' ne anlaşılması gerektiğidir. Doktrinde "*yok etmek"* kavramından anlaşılması gerekenin kişisel verilerin ortadan kaldırılması ve/veya imha edilmesi olduğu ifade edilmiştir.[545] Bazı görüşler ise, "*yok etmek"* kavramından anlaşılması gerekenin kişisel verileri geri dönülmesi, geri getirilmesi imkansız bir şekilde ortadan kaldırmak olduğunu ifade etmektedirler.[546] Ancak daha evvel de bahsettiğimiz üzere işbu madde ile Kişisel Verilerin Korunması Kanunu'nun ilgili 7. ve 17. Maddeleri ile birlikte değerlendirildiğinde verilerin yok edilmesi, silinmesi veya anonim hale getirilmesinin

---

[540] Parlar, Hatipoğlu, **Türk Ceza Kanunu Yorumu**, s.2053. Yaşar, Gökcan, Artuç, **Yorumlu Uygulamalı Türk Ceza Kanunu Yorumu,** s.4461. Taşkın, **Bilişim Suçları,** s. 112. Özbek, **TCK İzmir Şerhi**, s.965. Daha ayrıntılı açıklama için Kişisel Verilerin Kaydedilmesi başlıklı 135. Maddeyi açıkladığımız bölüme bakınız.

[541] Değirmenci, **Türk Ceza Kanunu'nun Bilişim Suçları Bakımından Değerlendirilmesi**, s. 203. Değirmenci konuyu şu şekilde değerlendirmiştir. Değirmenci mevzuatta sürelerin belirlenmesine ilişkin olarak, hem bireylerin hem de veri işleyenlerin yararlarının karşılaştırılması gerektiğini, bir yandan veri sorumlusunun amacının bir yandan da veri sahibinin kişilik haklarının korunması gerektiğini ifade etmiştir.

[542] Yaşar, Gökcan, Artuç, **Yorumlu Uygulamalı Türk Ceza Kanunu Yorumu**, s.4463. Dülger, **Bilişim Suçları**, s.721

[543] Parlar, Hatipoğlu, **Türk Ceza Kanunu Yorumu**, s.2055

[544] Özbek, Doğan, Bacaksız, Tepe, **Türk Ceza Hukuku Özel Hükümler**, s. 589. Özbek, **TCK İzmir Şerhi**, s.966

[545] Parlar, Hatipoğlu, **Türk Ceza Kanunu Yorumu,** s.2054. Yaşar, Gökcan, Artuç, **Yorumlu Uygulamalı Türk Ceza Kanunu Yorumu,** s.4463

[546] Karagülmez, **Bilişim Suçları**, s.239.

de verilerin yok edilmesi kapsamında ve kişisel verilerin yok edilmesine yönelik yöntemler kapsamında değerlendirilebileceğini söyleyebilir. [547]

Kişisel Verilerin Korunması Kanunu'nun yürürlüğe girmesi akabinde 28 Ekim 2017 tarihinden yürürlüğe giren Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in 8.maddesine göre kişisel verilerin silinmesi kişisel verilerin hiçbir kullanıcı tarafından erişilemez ve bir daha kullanılamaz şekilde ortadan kaldırılması şeklinde ifade edilmiştir. Aynı yönetmeliğin 9.maddesinde ise kişisel verilerin yok edilmesi tanımlanmış ve buna göre kişisel verilerin yok edilmesi kişisel verilerin kimse tarafından bir daha erişilemez, geri döndürülemez ve bir daha kullanılamaz şekle getirilmesi şeklinde ifade edilmiştir. Yine aynı yönetmeliğin 10. Maddesinde kişisel verilerin anonim hale getirilmesi kişisel verilerin başka veriler ile bir araya getirilmesi halinde bile asla bir gerçek kişinin kimliğini ortaya çıkaramayacak hale getirilmesi tanımlanmıştır. Kişisel verilerin anonim hale getirilmesi konusunda önemli olan, anonim hale getirilmiş kişisel verilerin başka veriler ile eşleştirilmesi ya da geri döndürülmesi halinde hiçbir şekilde gerçek bir kişi le ilişkilendirilmemesi gerekmektedir. Kişisel verilerin anonim hale getirilmesi yöntemi ile yok edilmesi tekniği tamamen uluslararası pratikle ve GDPR ile uyumludur. [548]

Görüldüğü üzere kişisel verileri yok etmenin birden fazla yolu bulunmaktadır ve KVKK kapsamında atanmış veri sorumluları, veri sorumlusu atanmamış ise veri işleyenin bizzat kendisi bu suçun faili olabilecek sair kişiler, kanundaki sürelerin dolması halinde ya da kişisel verilerin işlenmesini gerektirecek sebeplerin ortadan kalkması halinde, verileri yok edecek, silecek ya da anonim hale getirecektir. Aksi takdirde TCK'nın 138.maddesinde düzenlenen verileri yok etmeme suçunu işlemiş sayılacaklardır.

---

[547] Dülger, **Bilişim Suçları**, s.720. Dülger bu yöntemlerin çok çeşitli olabileceğini basılı dökümanlar ise yakılabileceğini, bilişim sistemlerine ait araçlar ise silinmesi şeklinde yok etmenin mümkün olabileceğini ifade etmiştir.

[548] Bu noktada *Pseudonymization* ve *Anonymization* yani takma isim verme ve anonim hale getirme gibi veri koruma dünyası bakımından sıkça karıştırılan iki kavramın birbirinden farklı olduğunu ve farklı amaçlara hizmet ettiğini hatırlatmanın faydalı olacağı görüşündeyiz. *Pseudonymization* veri sahibinin kimliğinin yerine farklı/takma bir kimlik kullanılması ve gerçek kimliğin yeniden ortaya çıkması için ek bir bilgiye ihtiyaç duyulan bir veri depolama yöntemidir. *Anonymization* yani anonim hale getirme ise kişisel verinin silinmesi, yok edilmesi gündeme geldiğinde uygulanan ve söz konusu kişisel verinin, veri sahibi ile tamamen ve geri dönülemez şekilde ilişkilendirilmesini engelleyen bir kişisel veri yok etme yöntemidir

b. Manevi Unsur

Türk Ceza Kanunu'nun 138.maddesinde düzenlenen 'Verileri Yok Etmeme' suçunun işlenmesi için kanunlarda belirtilen süreler geçmesine rağmen, kişisel verileri yok etmekle yükümlü kişiler tarafından kişisel verilerin yok edilmemesi gerektiğinden bu suçun ihmal ile işlenebilen bir suç olduğunu söyleyebiliriz.[549] Yine doktrinde bu suçun gerçek ihmali suçlar kategorisinde bulunduğu ve failin kişisel verileri kasıtlı bir şekilde yok etmemesinin yeterli olduğu belirtilmiştir.[550] Ayrıca kanuni süreler aşıldıktan sonra verilerin yok edilmesi halinde dahi eylemin yine de suç teşkil edeceğini belirtilmiştir.[551] Türk Ceza Hukukunda 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.[552]

c. Hukuka Aykırılık

Kanunların belirlediği sürelerin geçmiş olmasına karşın kişisel verileri sistem içinde yok etmekle yükümlü olanların kişisel verileri yok etmemeleri halinde bu suç oluşacaktır.[553] Aynı şekilde KVKK'nın 7. Maddesinde düzenlenen kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesi maddesine aykırı hareket edilmesi halinde de aynı kanunun 17.maddesinin 2. Fıkrasına atıfla, TCK'nın 138. Maddesine konu verileri yok etmeme suçu işlenmiş sayılacak ve bu suça konu yaptırım uygulanacaktır.

Esasen doktrinde kişinin rızasının, bu madde kapsamındaki eylemleri hukuka uygun hale getireceğini ifade eden görüşler[554] olmakla beraber biz bu görüşe katılmamaktayız. Zira 138.maddede yasa koyucu hukuka aykırılıktan değil özel olarak

---

[549] Küzeci, **Kişisel Verilerin Korunması,** 2018, s.408. Karagülmez, **Bilişim Suçları**, s.239. Yaşar, Gökcan, Artuç, **Yorumlu Uygulamalı Türk Ceza Kanunu Yorumu,** s.4463. Özbek, **TCK İzmir Şerhi,** s.965. Özbek, Doğan, Bacaksız, Tepe, **Türk Ceza Hukuku Özel Hükümler**, s. 588.
[550] Parlar, Hatipoğlu, op.cit., s.2054. Karagülmez, **Bilişim Suçları**, s.239. Yaşar, Gökcan, Artuç, **Yorumlu Uygulamalı Türk Ceza Kanunu Yorumu**, s.4464
[551] Küzeci, **Kişisel Verilerin Korunması**, 2018, s.408
[552] Karagülmez, **Bilişim Suçları**, s.239
[553] Yaşar, Gökcan, Artuç, **Yorumlu Uygulamalı Türk Ceza Kanunu Yorumu**, s.4464
[554] Yaşar, Gökcan, Artuç, **Yorumlu Uygulamalı Türk Ceza Kanunu Yorumu,** s.4464.

kanuna aykırılıktan bahsetmiştir. Burada söz konusu olan kanuna aykırılık olduğundan, kişinin rızası da işlenen fiilleri kanuna hale getiremeyeceğinden kişinin rızasının bu madde özelinde bir hukuka uygunluk sebebi olmayacağını düşünmekteyiz.[555]

4. Suçun Nitelikli Halleri

Türk Ceza Kanunu'nun Nitelikli Haller başlıklı 137.maddesi, 136.maddede düzenlenen 'Verileri Hukuka Aykırı Olarak Verme Ve Ele Geçirme' suçu ve 135. Maddede düzenlenen "Kişisel Verilerin Hukuka Aykırı Olarak Kaydedilmesi" suçu bakımından uygulama alanı bulurken, 138. Maddede düzenlenen verileri yok etmeme suçu için uygulanmayacaktır. [556] Zira bu durumda fail kamu görevlisi ya da belli bir meslek ve sanat sahibi olabileceği gibi, verileri yok etmekle görevli herhangi bir kişi de olabilecektir. [557] 138.Maddede düzenlenen verileri yok etmeme suçu bakımından nitelikli hal olarak yalnızca aynı maddeye 21.02.2014 tarihinde eklenen ikinci fıkra uygulama alanı bulacaktır. Bu fıkraya göre suçun maddi konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması hâlinde verilecek ceza bir kat artırılır. [558]

5. Suçun Özel Görünüş Biçimleri

a. Teşebbüs

TCK 138.madde kapsamında kişisel verilerin kanuna aykırı olarak yok edilmemesi suç olarak düzenlendiğinden, yani ihmali hareket ile suçun neticesi bitişik olduğundan bu suçun teşebbüsle işlenmeye elverişli bir suç olduğunu

---

[555] Karagülmez, **Bilişim Suçları,** s.239. Karagülmez konuyla ilgili bu suçun kanunda belirtilen sürelerin uygulanmamasında doğacağı ve bu bakımından esasen kamuya ilişkin olduğunu belirterek suçun oluşması halinde kişinin rızasının bu suçu hukuka uygun hale getirmeyeceğini belirtmiştir.
[556] Yaşar, Gökcan, Artuç, **Yorumlu Uygulamalı Türk Ceza Kanunu Yorumu**, s.4465
[557] Özbek, Doğan, Bacaksız, Tepe, **Türk Ceza Hukuku Özel Hükümler**, s. 588.
[558] Korkmaz, **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, s.436. Özbek, Doğan, Bacaksız, Tepe, **Türk Ceza Hukuku Özel Hükümler**, s. 589.

düşünmemekteyiz.[559] Doktrinde de bu suçun sırf hareket suçu olmasından kaynaklı olarak teşebbüse elverişli olmadığı ifade edilmiştir. [560]

b. İştirak

Türk Ceza Kanunu'nun 138. maddesi kapsamında 'Verileri Yok Etmeme' suçunun iştirak halinde işlenmesi hususunda suçun özgü suç olma niteliği göz önünde bulundurulmalıdır.[561] Zira yukarıda da bahsettiğimiz üzere bu suçun faili ancak kişisel verilerin yok edilmesinden sorumlu kişiler yani veri sorumluları olacaktır. Bu durumda bu suça diğer kişiler ancak azmettirme ya da yardım etme şeklinde dahil olabileceklerdir. [562]

c. İçtima

Türk Ceza Kanunu'nun 138. maddesi kapsamında düzenlenen 'Verileri Yok etmeme' suçu, Türk Ceza Kanunu'nun 43. Maddesi çerçevesinde birden fazla kişiye tek bir hareket ile işlenmesi halinde yani failin birden fazla kişinin verilerine sahip olmasına rağmen bu kişilerin verilerini kanundaki süreler geçmesine rağmen yok etmemesi halinde bir cezaya hükmedilecek ancak bu durumda verilecek ceza, dörtte birinden dörtte üçüne kadar artırılacaktır. [563] Diğer yandan failin bu suçu aynı kişiye birden fazla kez işlemesi halinde de zincirleme suç hükümleri uygulanacak ve failin cezası artırılacaktır.[564] Burada doktrinde failin bu suçun birden fazla kişisel verinin bulunması ve bunların kanunda belirtilen sürelerinin aynı anda geçmesi halinde tek suç oluşacağı belirtilmiştir.[565] Eğer fail kişisel verileri yok etmediği gibi bu verileri bir başkasına verir veya yayarsa bu durumda TCK'nın 136. Maddesinde düzenlenen verileri hukuka aykırı olarak verme veya ele geçirme suçunu da işlemiş sayılacak ve

---

[559] Özbek, Doğan, Bacaksız, Tepe, **Türk Ceza Hukuku Özel Hükümler**, s. 589.
[560] Parlar, Hatipoğlu, **Türk Ceza Kanunu Yorumu**, s.2056. Yaşar, Gökcan, Artuç, **Yorumlu Uygulamalı Türk Ceza Kanunu Yorumu**, s.4465. Özbek, **TCK İzmir Şerhi**, s.965. Dülger, **Bilişim Suçları**, s.724
[561] Yaşar, Gökcan, Artuç, **Yorumlu Uygulamalı Türk Ceza Kanunu Yorumu,** s.4465. Özbek, Doğan, Bacaksız, Tepe, **Türk Ceza Hukuku Özel Hükümler**, s. 589.
[562] Parlar, Hatipoğlu, **Türk Ceza Kanunu Yorumu**, s.2056
[563] Parlar, Hatipoğlu**, Türk Ceza Kanunu Yorumu,** s.2056
[564] Yaşar, Gökcan, Artuç, **Yorumlu Uygulamalı Türk Ceza Kanunu Yorumu**, s.4465. Dülger, **Bilişim Suçları**, s.724
[565] Parlar, Hatipoğlu, **Türk Ceza Kanunu Yorumu**, s.2056. Yaşar, Gökcan, Artuç, **Yorumlu Uygulamalı Türk Ceza Kanunu Yorumu**, s.4465.

gerçek içtima kuralları uygulanacaktır. [566] Aynı şekilde failin verileri önce hukuka aykırı şekilde elde etmesi sonra da bu verileri kanunda belirtilen usulüne uygun şekilde yok etmez ise yine iki ayrı suç oluşmuş olacaktır.[567]

6. Yaptırım ve Yargılama Usulü

Türk Ceza Kanunu'nun 138. Maddesine göre verileri yok etmeme suçunu işleyen kişi bir yıldan iki yıla kadar hapis cezası ile cezalandırılabilecektir. Yukarıda da belirttiğimiz üzere bu suça konu kişisel verilerin Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması hâlinde verilecek ceza bir kat artırılır.

Yine Türk Ceza Kanunu'nun 139. Maddesinde Verileri Yok Etmeme suçunun şikâyet bağlı olmadığı düzenlenmiştir.[568] Bu halde bu suç resen soruşturulacak suçlar arasındadır Ayrıca Türk Ceza Kanunu'nun 140. maddesi uyarınca tüzel kişilerin bu suça konu verilerden yararlanması halinde de tüzel kişilere özgü güvenlik tedbirleri uygulanacaktır. [569]

---

[566] Yaşar, Gökcan, Artuç, **Yorumlu Uygulamalı Türk Ceza Kanunu Yorumu** s.4465. Parlar, Hatipoğlu, **Türk Ceza Kanunu Yorumu**, s.2057.
[567] Özbek, **TCK İzmir Şerhi**, s.966
[568] Özbek, Doğan, Bacaksız, Tepe, **Türk Ceza Hukuku Özel Hükümler**, s. 591. Parlar, Hatipoğlu, **Türk Ceza Kanunu Yorumu**, s.2057. Yaşar, Gökcan, Artuç, **Yorumlu Uygulamalı Türk Ceza Kanunu Yorumu**., s.4465. Özbek, **TCK İzmir Şerhi**, s.967
[569] Dülger, **Bilişim Suçları**, s.725

SONUÇ

Çalışmamızda kişisel verilerin korunması konusu, hem kişisel verilerin korunması hakkına yaklaşım açısından, hem bu konuda bugüne kadar yapılan uluslararası düzenlemeler açısından hem de 5237 sayılı Türk Ceza Kanunu ve yakın zamanda yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu Kapsamında değerlendirilmeye çalışılmıştır.

Birinci bölümde ele alındığı üzere, kişisel verilerin korunması hakkının hukuki temeli konusunda yapılan tartışmalar bugün hala yoğun şekilde ve artarak devam etmektedir. Çünkü kişisel veri artık yalnızca bireylere ait bilgilerin korunmasından öte bir anlam ifade etmekte ve adeta yeni bir para birimi, yeni maddi değer ifade etmektedir. Günümüzde kişisel verileri, büyük veri tabanlarını elinde bulunduran şirketlerin artık bu verilerden maddi çıkar elde etmesi ve hatta veri toplamanın başlı başına bir amaç haline gelmesi kişisel verinin ekonomik değerini günden güne artırmaktadır. Kişisel verilerin ekonomik değerinin artışı, doğal olarak bu verilere ulaşma talebini ve müdahaleyi de aynı oranda artırmaktadır. Bu sebeple özellikle Avrupa Birliği ülkelerinde ve kıta Avrupası hukukunun uygulandığı ülkelerde kişisel verilerin korunması yönündeki önlemler hukuki düzenlemeler aracılığı ile artırılmaktadır. Ancak diğer yandan sermayesi kişisel veri olan Amazon, eBay gibi pek çok elektronik ticaret sitesi, Google, Facebook, Instagram gibi şirketler ve bunların dışında da pek çok şirket artık bireylerin kullanıcı alışkanlıklarından, siyasi görüşlerine kadar pek çok kişisel veriyi elinde bulundurmaktadır. Bu şirketlerin pek çoğunun tüm dünyada faaliyet göstermesi, veri güvenliğinin yeterli şekilde sağlanmadığı Amerika menşeli olması ve Amerika'da bireylerin verilerinin şirketlerden toplanmasını öngören bazı siyasi düzenlemelerin olması ise bireylerin kişisel verilerine ilişkin pek çok ihlal vakasının yaşanmasına sebep olmaktadır. Nitekim çalışmamız kapsamında da bahsedildiği üzere bugün halihazırda bu şirketlere yönelik pek çok dava devam etmektedir. Bu sebeplerle kişisel verilerin korunması konusuna ekonomik yönden

yaklaşan görüşler kişisel verilerin mülkiyet hakkı ya da fikri mülkiyet hakkı kapsamında korunması gerektiğini ileri sürerken, bu hakka insan hakları yönünden yaklaşan, kişilerin ve verilerinin korunmasını baz alan görüşler ise bu hakkı insan hakkı olarak ve bu kapsamda korunması gerektiğini ileri sürmektedir.

Bu noktada ülkemizde kişisel verilerin korunması hakkına ilişkin hukuki düzenlemelere baktığımızda, çalışmamızın ikinci bölümünde ayrıntılı olarak açıklanan, OECD rehber ilkeleri, 108 sayılı sayılı Avrupa Konseyi Sözleşmesi, 95 tarihli Veri Koruma Direktifi gibi uluslararası hukuki metinlerin dikkate alındığını söyleyebiliriz. Konuya ilişkin ulusal hukuki düzenlemelerimizin gerekçelerine de baktığımızda bu sözleşmelere atıf yapıldığını görmek mümkündür. Dolayısıyla ülkemizde bu yaklaşımlardan ikincisinin kabul edildiği ve kişisel verilerin korunması konusuna insan hakları zemininde yaklaşıldığını söylemek mümkündür. Elbette ülkemizde kişisel verilerin korunması konusuna yeterli ilginin ve özenin gösterilmediği aşikardır. Zira çalışmamız kapsamında da bahsedildiği üzere Türkiye tarafından 1981 yılında imzalanan 108 sayılı sözleşmenin onaylanmasına ilişkin kanun 2016 yılında çıkarılmıştır. Bunun sebebi ise bu sözleşmenin taraf devletlere, konuya ilişkin özel bir kanun çıkarma yükümlülüğü veriyor olmasıdır. Zira bu süre içerisinde ülkemizde kişisel verilerin korunmasına ilişkin özel bir kanun çıkarılamamıştır. İşte bu noktada böyle bir kanunun olmayışı neticesinde, hem bu konuya ilişkin kavramların tanımı, veri sahiplerinin hakları, veri işleyenlerin sorumlulukları gibi çok önemli konular havada kalmış başta kişisel verinin tanımı olmak üzere pek çok husus Yargıtay Kararları aracılığı ile yorumlanmıştır. Nihayet 24 Mart 2016 tarihinde 6698 sayılı Kişisel Verilerin Korunması Kanunu yürürlüğe girmiştir.

Kişisel verilerin korunmasına karşı işlenen suçlar ise 5237 sayılı Türk Ceza Kanunu'nun 135 ve 138. maddeleri arasında üç suç tipi ile düzenlenmiştir. Bu 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.

Çalışmamız boyunca, TCK'da düzenlenen suç tipleri hem kanun yapma sistematiği bakımından hem de KVKK ile aralarındaki uyumsuzluklar bakımından eleştirilmiş ve doktrindeki eleştiriler de çalışmamıza yansıtılmıştır. Elbette TCK kapsamında düzenlenen suç tipleri hakkında yapılan eleştiriler dikkate alınarak zaman içerisinde bazı değişikliklere gidilmiştir. Örneğin 2014 yılında 135. Maddenin birinci fıkrasında öngörülen ceza alt sınırı artırılmış ve KVKK ile de aynı maddenin özel nitelikli veri kategorilerinin kaydına ilişkin ikinci fıkrasında da yerinde bazı değişiklikler yapılmıştır. Ancak bu değişiklikler iki kanun arasındaki farklılıkların tamamını ortadan kaldıracak nitelikte değildir. Zira kişisel verilerin korunmasına ilişkin bir kanun olmadığı 2004 yılında hazırlanan ve yürürlüğe giren TCK ile 2016 yılında yürürlüğe giren KVKK arasında, bazı farklılıklar da bulunması doğal olup bunların bir an evvel giderilmesi gerekmektedir. Çalışmamızda ayrıntılı olarak bahsedildiği üzere örneğin 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. Yine örneğin TCK'nın verilerin yok edilmemesi başlıklı 138. Maddesi ile KVKK arasında verilerin yok edilmesi yöntemleri konusunda farklılıklar mevcuttur.

Tüm bu eleştirilere ve düzeltilmesi gereken noktalara rağmen, ülkemizde 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun yürürlüğü girmesi büyük bir adım olmuştur. Ayrıca bu kanun akabinde yürürlüğe giren yönetmelikler de kişisel verilerin korunması konusunda yol göstermektedir. Nitekim çalışmamızda yer verdiğimiz üzere Veri Koruma Kurulu tarafından ilkesel nitelikteki kararlar verilmeye başlanmıştır. Zaman içerisinde kanun uygulandıkça, bu konuda verilen kurul kararları arttıkça ve toplumda kişisel verilerin korunması yönündeki bilinç yükseldikçe hem KVKK metninde hem de TCK'nın ilgili suç tiplerinde ihtiyaçlara cevap veren değişikliklere gidileceği kanaatindeyiz.

KAYNAKÇA

Akarslan, Hüseyin — Bilişim Suçları, Güncellenmiş 2. Baskı, Ankara, Seçkin Yayınevi, Mayıs 2015.

Akgül, Aydın — "Kişisel Verilerin Korunması Bağlamında Biyometrik Yöntemlerin Kullanımı ve Danıştay Yaklaşımı", Türkiye Barolar Birliği Dergisi, Ankara, 2015, s. 200-222.

Akgül, Aydın — "Kişisel Verilerin Korunmasında Yeni Bir Hak: "Unutulma Hakkı" ve Ab Adalet Divanı'nın "Google Kararı", Türkiye Barolar Birliği Dergisi, 2016, s. 12-38.

Aksoy, Hüseyin Can — Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması, 1. Baskı, Ankara, Çakmak Yayınevi, Mart 2010.

Albrecht, Jan Philipp — "How the GDPR Will Change the World" **European Data Protection Law Review**, Volume 2, Issue 3, 2016, S. 287 – 289.

Artuk, Mehmet Emin Gökcen, Ahmet Yenidünya, Ahmet Caner — 5237 Sayılı Yeni TCK'ya Göre Hazırlanmış Ceza Hukuku Genel Hükümler, Ankara, Turhan Kitabevi, 2007.

Artuk, Mehmet Emin Gökcen, Ahmet Yenidünya, Ahmet Caner — Ceza Hukuku Özel Hükümler, 4. Baskı, Turhan Kitapevi, Ekim 2003.

Atak, Songül — "Avrupa Konseyi'nin Kişisel Veriler Açısından Sağladığı Temel Güvenceler" Türkiye Barolar Birliği Dergisi, 2010, s. 90-120.

Aydın, Hüseyin	"Ceza Hukukunda Kamu Görevlisi Kavramı", Ankara Barosu Dergisi, 2010, S. 2010/1, s. 109 – 127
Aygörmez Uğurlubay, Gülsün Ayhan	"Almanya, İsviçre ve Avusturya Hukuku Bağlamında Türk Ceza Muhakemesi Hukukunda Adlî DNA Analizleri" İstanbul Üniversitesi Ceza Hukuku ve Kriminoloji Dergisi-Journal of Penal Law and Criminology, 2017, S.5(2).
Ayözger, Çiğdem	Kişisel Verilerin Korunması- Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil, 1. Baskı, İstanbul, Beta, 2016
Aysun, Melike Köse	Kişisel Verilerin Kaydedilmesi Suçu, Akdeniz Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi.
Başalp, Nilgün	Avrupa Birliği Veri Koruması Genel Regülasyonunun Temel Yenilikleri, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, C.21, S.1.
Bayraktar, Köksal **Keskin Kiziroğlu, Serap** **Yıldız, Ali Kemal,** **Zafer, Hamide** **Aksoy Retornaz, Eylem** **Akyürek, Güçlü** **Evik, Ali Hakan** **Sınar, Hasan** **Altunç, Sinan** **Erman, Barış** **Erman Eroğlu, Fulya** **Aytekin İnceoğlu, Asuman**	Özel Ceza Hukuku, Cilt:3, 1.Baskı, İstanbul, On İki Levha Yayıncılık, Mart 2018
Bennett, Steven C.	The "Right to Be Forgotten": Reconciling EU and US Perspectives, 30 Berkeley J. Int'l Law. 161 (2012).
Blanke, Hermann Josef	The Right of Access to Public Information – An International Comparative Legal Survey, Springer, 2018

Ricardo Perlingeiro (Editors),

Boehm, Franziska, Information Sharing and Data Protection in the Area of Freedom, Security and Justice, Springer-Verlag Berlin Heidelberg, 2012.

Casagran, Cristina Blasi, Global Data Protection in the Field of Law Enforcement- An EU Perspective, Routledge, 2017, New York.

Cate, Fred H.
Cullen, Peter,
Mayer-Schönberger, Viktor
Data Protection Principles for the 21st Century Revising the 1980 OECD Guidelines, Oxford Internet Institute, Mart 2014, s.2.

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

De Busser, **Els** Data Protection in EU and US Criminal Cooperation, Antwerpen – Apeldoorn- Portland, Maklu, 2009.

Dedeoğlu, Gözde Gözetleme, Mahremiyet ve İnsan Onuru, TBD Bilişim Dergisi, 19 Nisan 2004, S. 153

Değirmenci, **Olgun** "Türk Ceza Kanunu'nun Bilişim Suçları Bakımından Değerlendirilmesi", Türkiye Barolar Birliği Dergisi, 2005, s. 195-208

Dülger, Murat Volkan Kişisel Verilerin Korunması Hukuku, 1. Baskı, Hukuk Akademisi, 2018 Aralık

Dülger, Murat Volkan Bilişim Suçları ve İnternet İletişim Hukuku, 6. Baskı, Seçkin Yayıncılık, Eylül 2015

Dülger, Murat Volkan "İnsan Hakları ve Temel Hak ve Özgürlükler Bağlamında Kişisel Verilerin Korunması", İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi, 5 (1), Bahar 2018, s.72-143

Dülger, Murat Volkan "Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza

Normlarıyla Korunması", İstanbul Medipol Üniversitesi Hukuk Dergisi, S.3/2, 2016, s. 102-167

Dülger, Murat Volkan "Anayasa Mahkemesi'nin Kişisel Verilerin Korunması Kanunu'nun Konu Edildiği İptal Davası Kararına İlişkin Bir Değerlendirme" (Çevrimiçi) www.academia.edu (Erişim Tarihi: 24.10.2018).

Dülger, Murat Volkan "KVKK Uygulamasında ve Uyum Sürecinde Ortaya Çıkan Soru ve Sorunlar"(Çevrimiçi) https://www.hukukihaber.net/kvkk-uygulamasinda-ve-uyum-surecinde-ortaya-cikan-soru-ve-sorunlar-makale,6324.html (Erişim Tarihi: 24.12.2018).

Dülger, Murat Volkan "Kişisel Verileri Koruma Kurulu'nun 20.4.2018 Tarihinde Yayınlamış Olduğu Karar Özetlerine İlişkin Değerlendirme",https://www.hukukihaber.net/kisisel-verileri-koruma-kurulunun-2042018-tarihinde-yayinlamis-oldugu-karar-ozetlerine-iliskin-degerlendirme-makale,5857.html (Erişim Tarihi: 05.05.2018).

Dieter, Dörr, Russell L. Weaver Perspectives on Privacy. Increasing Regulation in the USA, Canada, Australia and European Countries. Berlin, Boston: De Gruyter, 2014. Web. Retrieved 1 Feb. 2019.

European Commission E-privacy Directive: Assessment of Transposition, Effectiveness and Compatibility with Proposed Data Protection Regulation, 2013. (Çevrimiçi) https://ec.europa.eu/digital-single-market/en/news/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data (Erişim Tarihi: 24.10.2018)

Ferretti, **Federico** EU Competition Law, the Consumer Interest and Data Protection – The Exchange of Consumer Information in the Retail Financial Sector, Springer International Publishing, 2014

Fuster, G. González The Emergence of Personal Data Protection as a Fundamental Right of the EU, Springer International Publishing, 2014, 274 pp.

Karagülmez, Ali Bilişim Suçları ve Soruşturma– Kovuşturma Evreleri, Seçkin Yayınları, Ankara, Mayıs 2005.

Karakehya, Hakan "Türk Ceza Kanununda Bilişim Sistemine Girme Suçu", Türkiye Barolar Birliği Dergisi, Ankara, S.81, 2009.

Kaya, Cemil "Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi". Journal of Istanbul University Law Faculty 69 / 1-2, Aralık 2011, s. 317-334.

Koenig, Christian Andreas Bartosch, Jens Daniel Braun, Marion Romes EC Competition and Telecommunications Law, Second Edition, UK, Kluwer Law International, 2009.

Korkmaz, İbrahim Kişisel Verilerin Ceza Hukuku Kapsamında Korunması, 1.Baskı, Ankara, Seçkin Yayıncılık, Nisan 2017.

Korkmaz, İbrahim "Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme", Türkiye Barolar Birliği Dergisi, Ankara, Mayıs-Haziran 2016, S.82 – 152

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

Küzeci, Elif Kişisel Verilerin Korunması, Birinci Baskı, Ankara, Turhan Kitapevi, 2010.

Küzeci, Elif Kişisel Verilerin Korunması, Yenilenmiş ve Gözden Geçirilmiş, Ankara, Turhan Kitapevi, 2018.

Gemalmaz, Semih Ulusalüstü İnsan Hakları Hukukuna Giriş, Baskı 1, Legal Yayıncılık, Ekim 2011

Gilliot, Make Vashek Matyas Sven Wohlgemuth, The Future of Identity in the Information Society-Challenges and Opportunities, Kai Rannenberg, Denis Royer, André Deuker (Editors), Springer-Verlag Berlin Heidelberg, 2009.

Göktürk, Neslihan "Suçun Yasal Tanımında Yer Alan "Hukuka Aykırılık" İfadesinin İcra Ettiği Fonksiyon" İnönü Üniversitesi Hukuk Fakültesi Dergisi, Cilt.7, Sayı.1, 2016.

Göktürk, Neslihan Türk Hukuku'nda Suçların İçtimaı. Ceza Hukuku v Kriminoloji Dergisi / Journal of Penal Law & Criminology, 2014, 2 (1-2), 31-59

Gözübüyük, Şeref
Gölcüklü, Feyyaz Avrupa İnsan Hakları Sözleşmesi ve Uygulaması, 8. Baskı, Ankara, Turhan Kitabevi, Eylül 2009

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

Gratton, **Eloise** Internet and Wireless Privacy- A Legal Guide to Global Business Practices, CCH Canadian Limited, Kanada, 2003.

Hafızoğulları, Zeki
Muharrem Özen "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar". Ankara Barosu Dergisi (2009): S.9-22.

Henkoğlu,Türkay
Bülent Yılmaz, "Avrupa Birliği (AB) Bilgi Güvenliği Politikaları", Türk Kütüphaneciliği 27, 3 (2013), s. 451-471.

Hornung, Gerrit
Christoph Schnabel, "Data protection in Germany I: The population census decision and the right to informational self-determination" , Computer Law & Security Report, Volume 25, Issue 1, 2009, S. 84-88.

Leach, Philipp Taking a Case to the European Court of Human Rights, United Kingdom, Oxford University Press, 2011.

Letsas, George "The ECHR as a living instrument: Its meaning and legitimacy." In A. Føllesdal, B. Peters, & G. Ulfstein (Eds.), *Constituting Europe: The European Court of Human Rights in a National, European and Global Context* (Studies on Human Rights Conventions, 2013, pp. 106-141). Cambridge: Cambridge University Press.

Mahmutoğlu,
Fatih Selami "Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar Ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi" İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, 71 (1), 2010, s. 855-889.

Organisation for Economic Co-operation and Development	"Privacy Online-OECD Guidance on Policy and Practice" OECD Publishing 2003.
Organisation for Economic Co-operation and Development	"Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines", OECD Digital Economy Papers, No. 229, OECD Publishing, Paris, 2013
Özbek, Veli Özer Doğan, Koray Bacaksız, Pınar İlker Tepe	Türk Ceza Hukuku Özel Hükümler, 13. Baskı, Seçkin Yayıncılık, Eylül 2018, Ankara
Özbek, Veli Özer	Yeni Türk Ceza Kanunu'nun Anlamı (TCK İzmir Şerhi), Madde 76-169, C. II, Ankara, 2008.
Özel, Kadir Can	6698 Sayılı Kişisel Verilerin Korunması Kanunu Üzerine Genel Bir Değerlendirme, (Çevrimiçi) https://www.hukukihaber.net/6698-sayili-kisisel-verilerin-korunmasi-kanunu-uzerine-genel-bir-degerlendirme-makale,4758.html (Erişim Tarihi: 05.05.2018)
Özen, Mustafa	"Ceza Hukukunda Fikri İçtima", **Türkiye Barolar birliği Dergisi**, Ankara, S.73, 2003.
Papademetriou, Theresa	ECJ Invalidates Data Retention Directive, The Law Library of Congress, Global Legal Research Center, June 2014
Parlar, Ali Muzaffer Hatipoğlu	Türk Ceza Kanunu Yorumu, Seçkin Yayıncılık, 2.Bası, 2008.
Parlar, Ali,	Bilişim Suçları, 3. Baskı, Ankara, Bilge Yayınevi, nisan 2015
Prins, Corien	Property and Privacy: European Perspectives and the Commodification of Our Identity. Information Law Series, Vol. 16, pp. 223-257,
Purtova, Nadezhda	Property Rights in Personal Data: Learning from the American Discourse (February 17, 2010). Computer Law & Security Review, Vol. 25, No. 6, pp. 507-521, 2009.
Samuelson, Pamela	Privacy as Intellectual Property, 52 Stanford Law Review 1125 (1999),

Sedgewick, Margaret Byrne	"Transborder Data Privacy as Trade" 105 California Law Review 1513 (2017).
Schwartz, **Paul M.**	**"**European Data Protection Law and Restrictions on International Data Flows, Berkeley Law Scholarship Repository, 80 Iowa L. Rev. 471 (1994)
Schwartz, **Paul M**	**"**Property, Privacy and Personal Data" 117 Harvard Law Review, 2004, s. 2056.
Schwartz, **Paul M**	Cyberspace and Privacy: A New Legal Paradigm? Stanford Law Review, Vol. 52, No. 5, Symposium: (May, 2000), pp. 1559-1572.
Schonberger, **Viktor Mayer**	Beyond Privacy, Beyond Rights- Toward a Systems Theory of Information Governance, 98 Calif. L. Rev. 1853 (2010).
Schönfeld, Max	Big Data and Automotive – A Legal Approach Hoeren, Thomas Barbara Kolany- Raiser (Edt.) Big Data in Context Legal, Social and Technological Insights, Almanya, Springer, 2015.
Skalak, Steven L. Thomas Golden Mona Clayton Jessica Pill	A Guide to Forensic Accounting Investigation, Second Edition, New Jersey, Wiley&Sons, Inc.
Singh, **Atul**	**"**Protecting Personal Data as A Property Right", ILI Law Review, Winter Issue 2016,S.123-139.
Şen, **Ersan**	Yeni Türk Ceza Kanunu'nun Yorumu, Vedat Yayıncılık, İstanbul, 2006.
Şen, **Ersan**	Ersan Şen, "Kişisel Verilerin Korunması Kanunu Son Tasarısı"(Çevrimiçi) https://www.hukukihaber.net/kisisel-verilerin-korunmasi-kanunu-son-tasarisi-makale,3742.html (Erişim Tarihi: 05.05.2018)
Taşkın, Şaban Cankat	Bilişim Suçları, Birinci Baskı, İstanbul, Beta Basım, Kasım 2008.

Tezcan, **Durmuş Mustafa Ruhan Erdem, R. Murat Önok,**	Teorik Ve Pratik Ceza Özel Hukuku, 9.Baskı, Ankara, Seçkin Yayınevi, Şubat 2013.
Tezcan, **Durmuş**	"Özel Hayatın Gizliliğini İhlal ve Kişisel Verilerin Kaydedilmesi Suçu ile İlgili Bazı Gözlemler" İstanbul Üniversitesi Hukuk Fakültesi Dergisi, C. LXXI, S. 1, s. 1159-1164, 2013
Volokh, Eugene	"Personalization and Privacy - Does personalization jeopardize our privacy? If so, what should the law do about it?" August 2000/Vol. 43, No. 8.
Wild, Charles Stuart Weinstein, Neil MacEwan Neal Geach	Electronic and Mobile Commerce Law – An analysis of trade, finance, media and cybercrime in the digital age, University of Hertfordshire Press, Great Britain, 2011.
Yaşar, Osman Hasan Tahsin Gökcan, Mustafa Artuç	Yorumlu-Uygulamalı Türk Ceza Kanunu, C.6, Baskı 2, Ankara, Adalet Yayınevi, Ocak 2014, c.3.
Yee, George O.M.	Privacy Protection Measures and Technologies in Business Organizations- Aspects and Standarts, IGI Global, USA, 2012.
Zwaak,**Leo Pieter van Dijk, Fried van Hoof, Arjen van Rijn,**	Theory and Practice of the European Convention on Human Rights, Intersentia, Fourth Edition, C.2, 2006, Antwerpen – Oxford.

YARARLANILAN YAYINLAR

1. Kişisel Verilerin Korunması Kurumu, Açık Rıza, https://kvkk.gov.tr/yayinlar/A%C3%87IK%20RIZA.pdf

2. Kişisel Verilerin Korunması Kurumu, Veri Sorumlusu ve Veri İşleyen, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/f63e88cd-e060-4424-b4b5-f6413c602060.pdf

3. Kişisel Verilerin Korunması Kurumu, Kişisel Verilerin İşlenmesine ilişkin Temel İlkeler

https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/d0fbca08-30af-41fe-a7c9-65663b9c5231.pdf

4. Kişisel Verilerin Korunması Kurumu, 100 soruda kişisel verilerin korunması kanunu
https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/7d5b0a2f-e0ea-41e0-bf0b-bc9e43dfb57a.pdf

5. Kişisel Verilerin Korunması Kurumu, Kişisel Verilerin Yurtdışına Aktarılması
https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/ca163cb6-39ad-4024-870a-8a9508c92387.pdf

6. Kişisel Verileri Koruma Kurumu, Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi,
https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/bc1cb353-ef85-4e58-bb99-3bba31258508.pdf

YARARLANILAN BAŞLICA İNTERNET SİTELERİ

1. Anayasa Mahkemesi Kararları için,
http://www.anayasa.gov.tr/icsayfalar/kararlar/kbb.html

2. Avrupa İnsan Hakları Mahkemesi Kararları için,
http://www.echr.coe.int/ECHR/Homepage_EN

3. Avrupa Birliği Genel Veri Koruma Tüzüğü, Veri Koruma Direktifleri gibi Avrupa Birliği tarafından yapılan düzenlemelere ilişkin olarak,
https://ec.europa.eu/info/index_en

4. Kişisel Verilerin Korunmasına İlişkin Kurul Kararları ve Mevzuat için,
https://www.kvkk.gov.tr/

5. Konuya ilişkin çeşitli yabancı makalelere ve kitaplara erişim için,
https://scholarship.law.berkeley.edu/facpubs/
https://harvardlawreview.org/
http://www.californialawreview.org/
https://www.stanfordlawreview.org/
https://www.springer.com/de

6. OECD kişisel verilerin korunmasına ilişkin ilkeler ve sair bilgiler için,
http://www.oecd.org/

7. Türkçe makalelere ulaşım için,
https://www.academia.edu/

8. Yargıtay Kararlarına erişim için,
http://www.kazanci.com/kho2/ibb/giris.html

KİŞİSEL VERİLERİ KORUMA KURULU KARARLARI

1. Kişisel Verileri Koruma Kurulu'nun 16/10/2018 Tarihli ve 2018/119 Sayılı İlke Kararı
2. Kişisel Verileri Koruma Kurulu'nun 31/01/2018 tarih ve 2018/10 sayılı kararı
3. Kişisel Verilerin Koruma Kurumu'nun sayılı 02/04/2018 tarih ve 2018/32 sayılı kararı
4. Kişisel Verileri Koruma Kurulunun 05/12/2018 Tarihli ve 2018/143 sayılı Kararı
5. Kişisel Verileri Koruma Kurulunun 28/06/2018 Tarihli ve 2018/69 Sayılı Kararı
6. Kişisel Verileri Koruma Kurulunun 24.01.2019 tarih ve 2019/9 sayılı Kararı

YARGITAY KARARLARI

1. Yargıtay Hukuk Genel Kurulu 2014/4-56 E. ile 2015/1679 K. 17.06.2015T.

2. Yargıtay 12. Ceza Dairesi 2012/16872 Esas, 2012/18221.

3. Yargıtay Ceza Genel Kurulu 17.06.2014 T., 2012/12-1510E., 2014/331K.

4. Yargıtay 12. Ceza Dairesi 2016/12683 E., 2017/3796 K. ve 07/10/2015 T. Kararı.

5. Yargıtay 12. Ceza Dairesi 13.10.2014, E. 2014/4081, K. 2014/19490.

6. Yargıtay Hukuk Genel Kurulu E. 2014/4-56 K. 2015/1679 T. 17.6.2015

7. Yargıtay 4. Ceza Dairesi 2018/7276 E., 2018/21206 K. Ve 06.12.2018 T.

8. Yargıtay Ceza Genel Kurulu Esas No: 2012/12-1510 Karar No: 2014/331 Karar Tarihi.17.06.2014

9. Yargıtay Ceza Genel Kurulu 2012/1510E, 2014/331K, 17.06.2014T

10. Yargıtay 12. Ceza Dairesi 12.06.2012, 2012/23504 E. 2012/ 14795K.

11. Yargıtay 12. Ceza Dairesi, 2014/17630 E., 2015/1672 K., 02.02.2015 T. sayılı kararı

12. Yargıtay 5. Ceza Dairesi, 2014/10479 E., 2018/4622 K. ve 21.06.2018 T. sayılı kararı

13. Yargıtay Ceza Genel Kurulu, E: 2012/12-1510 K: 2014/331 K:17.06.2014

14. Yargıtay 12. Ceza Dairesi E. 2017/2960 K. 2018/1541 T. 14.2.2018

15. Yargıtay 12. Ceza Dairesi 12. C.D. 2017/150 E. 2017/6231 K.

16. Yargıtay Ceza Genel Kurulu, 2012/12-1510 E. 2014/331 K. Ve 17.06.2014 T.

17. Yargıtay 12. Ceza Dairesi E. 2018/2226 K. 2018/8746 T. 26.9.2018

18. Yargıtay 12. Ceza Dairesi E. 2016/1129 K. 2017/6742 T. 27.9.2017

19. Yargıtay 12. Ceza Dairesi E. 2015/5128 K. 2016/10207 T. 15.6.2016

20. Yargıtay Ceza Genel Kurulu 2012/1510E., 2014/331K. 17.06.2014T.

21. Yargıtay 4. Ceza Dairesi 2011/10616 E., 2013/7641 K. 18.03.2013 T.

22. Yargıtay 12. Ceza Dairesi 2014/11530 E., 2015/584 K. 19.01.2015 T.

23. Yargıtay 4. Ceza Dairesi 2017/12189 E., 2018/9465 K. 10.10.2018 T.

24. Yargıtay Ceza Genel Kurulu 2012/1510E. 2014/331K., 17.06.2014T.

25. Yargıtay 12. Ceza Dairesi 2014/22994 E, 2015/2630 K., 16.02.2015 T.

26. Yargıtay 12. Ceza Dairesi E. 2015/12823 K. 2017/873 T. 8.2.2017

27. Yargıtay 12. Ceza Dairesi E. 2015/13248 K. 2017/3108 T. 12.4.2017

28. Yargıtay 12. Ceza Dairesi E. 2017/12083, K. 2018/2539, T. 7.3.2018

29. Yargıtay 12. Ceza Dairesi E. 2015/11703 K. 2017/870 T. 8.2.2017

30. Yargıtay 8. Ceza Dairesi, E. 2016/12565, K. 2017/12892 T. 20.11.2017

31. Yargıtay 12. Ceza Dairesi E. 2017/5654, K. 2018/2911 T. 14.3.2018

32. Yargıtay 8. Ceza Dairesi, 08.10.2018T, 2018/10436 K., 2018/6171E

33. Yargıtay 12. Ceza Dairesi E. 2012/22005 K. 2013/24489 T. 4.11.2013

ÖZGEÇMİŞ

Sinem Göçmen UYARER 1989 yılında Zonguldak- KDZ. Ereğli'de doğdu. Lise öğrenimini TED KDZ. Ereğli Koleji Vakfı Özel Okulları'nda tam burslu başarı bursu ile okuyan Uyarer 2007 yılında okuldan mezun olmuştur. Akabinde aynı yıl İstanbul Üniversitesi Hukuk Fakültesi'ne girmiş ve 2011 yılında bu fakülteden mezun olmuştur. 2012 yılında avukatlık stajını tamamlayarak ruhsatını almış ve Galatasaray Üniversitesi Kamu Hukuku Tezli Yüksek Lisans Programına kayıt hakkı kazanmıştır. Bu süreçte derslerini başarı ile tamamlayan UYARER, Prof. Dr. Feridun Yenisey liderliğinde gerçekleşen ve Harvard Law School ve Max Planck Institute tarafından fonlanan ceza araştırmaları projelerinde faaliyet göstermiştir. UYARER, Gün+Partners Avukatlık Bürosunda uzun yıllar faaliyet gösterdikten sonra, bir finansal teknoloji firmasının da hukuk müşavirliğini yapmıştır. Şu an Berlin'de avukatlık faaliyetini sürdüren UYARER, halihazırda bir finansal teknoloji bir firmasında hukuk danışmanı olarak faaliyet göstermeye devam etmektedir.

TEZ ONAY SAYFASI

Üniversite	: T.C. GALATASARAY ÜNİVERSİTESİ
Enstitü	: SOSYAL BİLİMLER ENSTİTÜSÜ
Hazırlayanın Adı Soyadı	: SİNEM GÖÇMEN UYARER
Tez Başlığı	:5237 SAYILI TÜRK CEZA KANUNU VE 6698 SAYILI :KİŞİSEL VERİLERİN KORUNMASI KANUNU :KAPSAMINDA KİŞİSEL VERİLERİN KORUNMASI
Savunma Tarihi	:13/06/2019
Danışmanı	: DOÇ. DR. VESİLE SONAY EVİK

JÜRİ ÜYELERİ

Unvanı, Adı Soyadı	İmza
DOÇ. DR. VESİLE SONAY EVİK	
DOÇ. DR. E. EYLEM AKSOY RETORNAZ	
DOÇ. DR. MURAT VOLKAN DÜLGER	

Enstitü Müdürü
Prof. Dr. M. Yaman ÖZTEK