



AKDENİZ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ



Melike KÖSE AYSUN

KİŞİSEL VERİLERİN KAYDEDİLMESİ SUÇU
(TCK m. 135)

Kamu Hukuku Ana Bilim Dalı
Yüksek Lisans Tezi

Antalya, 2018



AKDENİZ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ



Melike KÖSE AYSUN

KİŞİSEL VERİLERİN KAYDEDİLMESİ SUÇU
(TCK m. 135)

Danışman

Dr. Öğr. Üyesi Mahmut KAPLAN

Kamu Hukuku Ana Bilim Dalı

Yüksek Lisans Tezi

Antalya, 2018

T.C.
Akdeniz Üniversitesi
Sosyal Bilimler Enstitüsü Müdürlüğüne,

Melike KÖSE AYSUN'un bu çalışması, jürimiz tarafından Kamu Hukuku Ana Bilim Dalı Yüksek Lisans Programı tezi olarak kabul edilmiştir.

Başkan : Dr. Öğr. Üyesi Yılmaz YURTSEVEN (İmza)

Üye (Danışmanı) : Dr. Öğr. Üyesi Mahmut KAPLAN (İmza)

Üye : Dr. Öğr. Üyesi R. Barış ATLADI (İmza)

Tez Başlığı: Kişisel Verilerin Kaydedilmesi Suçu (TCK m. 135)

Onay: Yukarıdaki imzaların, adı geçen öğretim üyelerine ait olduğunu onaylarım.

Tez Savunma Tarihi : 29/05/2018

Mezuniyet Tarihi : 09/07/2018

(İmza)
Prof. Dr. İhsan BULUT
Müdür

AKADEMİK BEYAN

Yüksek Lisans Tezi olarak sunduğum “Kişisel Verilerin Kaydedilmesi Suçu (TCK m. 135)” adlı bu çalışmanın, akademik kural ve etik değerlere uygun bir biçimde tarafımda yazıldığını, yararlandığım bütün eserlerin kaynakçada gösterildiğini ve çalışma içerisinde bu eserlere atıf yapıldığını belirtir; bunu şerefimle doğrularım.

İmza

Melike KÖSE AYSUN





T.C.
AKDENİZ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
TEZ ÇALIŞMASI ORJİNALLİK RAPORU



SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜ'NE

ÖĞRENCİ BİLGİLERİ	
Adı-Soyadı	Melike Köse AYSUN
Öğrenci Numarası	20135228002
Enstitü Ana Bilim Dalı	Kamu Hukuku
Programı	Tezli Yüksek Lisans
Programın Türü	(x) Tezli Yüksek Lisans () Doktora () Tezsiz Yüksek Lisans
Danışmanın Unvanı, Adı-Soyadı	Dr. Öğr. Üyesi Mahmut KAPLAN
Tez Başlığı	Kişisel Verilerin Kaydedilmesi Suçu (TCK m. 135)
TurnItIn Ödev Numarası	973724288

Yukarıda başlığı belirtilen tez çalışmasının a) Kapak sayfası, b) Giriş, c) Ana Bölümler ve d) Sonuç kısımlarından oluşan toplam 170 sayfalık kısmına ilişkin olarak, 08/06/2018 tarihinde tarafımdan TurnItIn adlı intihal tespit programından Sosyal Bilimler Enstitüsü Tez Çalışması Orijinallik Raporu Alınması ve Kullanılması Uygulama Esasları'nda belirlenen filtrelemeler uygulanarak alınmış olan ve ekte sunulan rapora göre, tezin/dönem projesinin benzerlik oranı;

alıntılar hariç % 13

alıntılar dahil % 17 'dir.

Danışman tarafından uygun olan seçenek işaretlenmelidir:

(x) Benzerlik oranları belirlenen limitleri aşmıyor ise;

Yukarıda yer alan beyanın ve ekte sunulan Tez Çalışması Orijinallik Raporu'nun doğruluğunu onaylarım.

() Benzerlik oranları belirlenen limitleri aşıyor, ancak tez/dönem projesi danışmanı intihal yapılmadığı kanısında ise;

Yukarıda yer alan beyanın ve ekte sunulan Tez Çalışması Orijinallik Raporu'nun doğruluğunu onaylar ve Uygulama Esasları'nda öngörülen yüzdelik sınırlarının aşılmasına karşın, aşağıda belirtilen gerekçe ile intihal yapılmadığı kanısında olduğumu beyan ederim.

Gerekçe:

Benzerlik taraması yukarıda verilen ölçütlerin ışığı altında tarafımca yapılmıştır. İlgili tezin orijinallik raporunun uygun olduğunu beyan ederim.

08/06/2018

(imza)

Danışmanın Unvanı-Adı-Soyadı
Dr. Öğr. Üyesi Mahmut KAPLAN

İÇİNDEKİLER

TABLO LİSTESİ	v
KISALTMALAR LİSTESİ.....	vi
ÖZET.....	viii
SUMMARY	ix
TEŞEKKÜR	x
ÖNSÖZ.....	xi
GİRİŞ	1

BİRİNCİ BÖLÜM

KİŞİSEL VERİ KAVRAMI VE KİŞİSEL VERİLERİN KORUNMASI HUKUKU’NUN TARİHSEL GELİŞİMİ

1.1. Kişisel Veri Kavramı.....	3
1.1.1. Her Türlü Bilgi.....	4
1.1.1.1. Genel Olarak.....	4
1.1.1.2. Özel Veri Kategorileri (Hassas Veri).....	7
1.1.2. Bilginin Gerçek Kişiye İlişkin Olması.....	10
1.1.3. Bilginin Kişi ile İlgili Olması.....	11
1.1.4. Kişinin Belirli ya da Belirlenebilir Olması.....	11
1.2. Kişisel Verinin Hukuki Niteliği.....	13
1.2.1. Kişilik Hakkı Görüşü	13
1.2.2. Mülkiyet Hakkı Görüşü	15
1.2.3. Fikri Mülkiyet Hakkı Görüşü.....	16
1.3. Kişisel Verilerin Korunmasına Yönelik Düzenlemelerin Tarihsel Gelişimi	17
1.3.1. Genel Olarak	17
1.3.2. Uluslararası Düzenlemelerde Kişisel Verilerin Korunması.....	18
1.3.2.1. Ekonomik İşbirliği ve Kalkınma Örgütü (OECD)	18
1.3.2.2. Birleşmiş Milletler	19
1.3.2.3. Avrupa Konseyi	20
1.3.2.3.1. Genel Olarak	20
1.3.2.3.2. Avrupa İnsan Hakları Sözleşmesi	22
1.3.2.3.3. 108 Sayılı Avrupa Konseyi Sözleşmesi	25
1.3.2.4. Avrupa Birliği	29

1.3.2.4.1. Genel Olarak	29
1.3.2.4.2. 95/46/AT Sayılı Kişisel Verilerin Korunması Yönergesi (Direktifi).....	31
1.3.2.4.3. 2016/679 Sayılı Genel Veri Koruma Tüzüğü (General Data Protection Regulation-GDPR).....	34
1.3.2.5. Asya – Pasifik Ekonomik İşbirliği (APEC)	41
1.3.2.6. Çeşitli Ülke Düzenlemelerinde Kişisel Verilerin Korunması.....	42
1.3.2.6.1. Amerika Birleşik Devletleri (ABD)	42
1.3.2.6.2. Almanya	44
1.3.2.6.3. İngiltere	46
1.3.2.6.4. Türkiye	47
1.3.2.6.4.1. 12 Eylül 2010 Tarihli Anayasa Değişikliği	47
1.3.2.6.4.2. 10 Haziran 2003 Tarihli İş Kanunu	48
1.3.2.6.4.3. 12 Ekim 2004 Tarihli Türk Ceza Kanunu	49
1.3.2.6.4.4. 11 Ocak 2011 Tarihli Türk Borçlar Kanunu.....	50
1.3.2.6.4.5. 18 Şubat 2016 Tarihli Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun.....	50
1.3.2.6.4.6. 7 Nisan 2016 Tarihli Kişisel Verilerin Korunması Kanunu	51
1.3.2.6.4.6.1. Genel Olarak.....	51
1.3.2.6.4.6.2. Kanunun Amacı.....	52
1.3.2.6.4.6.3. KVKK'nın Kapsamı.....	52
1.3.2.6.4.6.4. Kişisel Verilerin İşlenmesi Kavramı	53
1.3.2.6.4.6.5. Veri Sorumlusu ve Veri İşleyen Kavramları	54
1.3.2.6.4.6.6. Kişisel Verilerin İşlenmesi Sırasında Uyulması Gereken Esaslar (Genel İlkeler).....	55
1.3.2.6.4.6.7. Kişisel Verilerin İşlenmesinin Şartı: Açık Rıza	59
1.3.2.6.4.6.8. Kişisel Verilerin İşlenmesinde İlgilisinin Açık Rızası Bulunması Kuralının İstisnaları	61
1.3.2.6.4.6.9. Veri Sorumlusunun Yükümlülükleri ile İlgili Kişinin Hakları ...	63

1.4. Kişisel Verilerin Korunması Sorunu	64
1.4.1. Medeni Hukuk.....	67
1.4.2. İdare Hukuku.....	68
1.4.3. Ceza Hukuku	73
1.4.3.1. 5237 sayılı TCK'da Yer Alan Düzenlemeler	74
1.4.3.1.1. Kaydetme	74
1.4.3.1.2. Verme, Yayma veya Ele Geçirme	74
1.4.3.1.3. Yok Etmeme	79

İKİNCİ BÖLÜM

KİŞİSEL VERİLERİ KAYDETME SUÇUNUN UNSURLARI VE ÖZEL GÖRÜNÜŞ BİÇİMLERİ

2.1. Korunan Hukuki Değer	84
2.2. Tipiklik (Tipe Uygunluk).....	85
2.2.1. Suçun Maddi Unsurları	86
2.2.1.1. Fiil – Hareket	86
2.2.1.2. Konu	88
2.2.1.3. Fail.....	94
2.2.1.4. Mağdur.....	95
2.2.1.5. Nitelikli Unsurlar.....	95
2.2.1.5.1. Özel Nitelikli (Hassas) Kişisel Verilerin Kaydedilmesi	95
2.2.1.5.1.1. Genel Olarak	95
2.2.1.5.1.2. Siyasi Görüş	96
2.2.1.5.1.3. Felsefî ve Dini Görüş	97
2.2.1.5.1.4. Irki Köken	98
2.2.1.5.1.5. Ahlaki Eğilim	100
2.2.1.5.1.6. Cinsel Yaşam	102
2.2.1.5.1.7. Sağlık Durumu	103
2.2.1.5.1.8. Sendikal Bağlantı	104
2.2.1.5.2. Suçun Kamu Görevlisi Tarafından ve Görevinin Verdiği Yetkinin Kötüye Kullanılması Suretiyle İşlenmesi	107

2.2.1.5.3. Suçun Belli Bir Meslek ve Sanatın Sağladığı Kolaylıktan Yararlanmak Suretiyle İşlenmesi.....	109
2.2.2. Manevi Unsur	110
2.3. Hukuka Aykırılık	111
2.4. Suçun Özel Görünüş Biçimleri	128
2.4.1. Teşebbüs	128
2.4.2. İştirak.....	129
2.4.3. İçtima.....	130
2.5. Yaptırım ve Muhakeme.....	133
2.5.1. Yaptırım	133
2.5.2. Muhakeme	133
SONUÇ.....	135
KAYNAKÇA.....	139
ÖZGEÇMİŞ.....	154

TABLO LİSTESİ

Tablo 1.1 Uluslararası Düzenlemeler ile Birtakım Ülkelerin Ulusal Mevzuatında Özel Veri Kategorilerinin Kapsamı.....	8
--	---



KISALTMALAR LİSTESİ

AB	Avrupa Birliği
ABAD	Avrupa Birliği Adalet Divanı
ABD	Amerika Birleşik Devletleri
AIDS	Acquired Immune Deficiency Syndrome
AİHM	Avrupa İnsan Hakları Mahkemesi
AİHS	Avrupa İnsan Hakları Sözleşmesi
APEC	Asia-Pacific Economic Cooperation
AÜHFD	Ankara Üniversitesi Hukuk Fakültesi Dergisi
AÜSBF	Ankara Üniversitesi Siyasal Bilgiler Fakültesi
B. No	Başvuru numarası
bk.	Bakınız
BverfGE	Bundesverfassungsgericht Entscheidung (Federal Anayasa Mahkemesi Kararı – Almanya)
CCTV	Closed Circuit Television
CD	Ceza Dairesi
CGK	Ceza Genel Kurulu
CMK	Ceza Muhakemesi Kanunu
Çev.	Çeviren
DNA	Deoksiribo Nükleik Asit
E.	Esas numarası
GBT	Genel Bilgi Toplama
GDPR	General Data Protection Regulation
HTS	Historical Traffic Search
IP	Internet Protocol
İİBF	İktisadi ve İdari Bilimler Fakültesi
K. T.	Karar tarihi
K.	Karar numarası
KVKK	Kişisel Verilerin Korunması Kanunu
m.	Madde
MERNİS	Merkezi Nüfus İdaresi Sistemi
OECD	Organisation for Economic Co-operation and Development

Parg.	Paragraf
TCK	Türk Ceza Kanunu
TDK	Türk Dil Kurumu
TMK	Türk Medeni Kanunu
USB	Universal Serial Bus
vb.	ve benzeri
vd.	ve devamı
vs.	ve saire



ÖZET

Kişisel verilerin korunması, dünyada 1970’lerden bu yana tartışılmakta olan ve hukuki metinlerde yer verilen bir hak alanıdır. Özellikle teknolojik gelişmelerin etkisi ile bilginin kaydedilmesi, depolanması ve sınıflandırılmasının kolaylaşması sonucunda kişisel verilerin korunmasının önemi her geçen gün artmaktadır. Bireylerin davranışlarını devamlı bir gözetime konu olmaksızın şekillendirebilmeleri, insan onuru ve kişiliğin serbestçe geliştirilmesi hakkı ile yakından ilişkilidir. Bu nedenle, kişisel verilerin korunması hakkı temel hak ve özgürlükler kapsamında değerlendirilmektedir. Hatta öyle ki, hukukumuzda kişisel verilerin korunması hakkı toplumsal yaşamın temel bir değeri olarak kabul edilerek buna yönelik birtakım ihlallere karşı cezai yaptırım öngörülmüştür.

Hukuki metinlerin pek çoğunda kişisel veri, “kimliği belirli ve belirlenebilir gerçek kişiye ilişkin her türlü bilgi” olarak tanımlanmıştır. Kişisel verilerin işlenmesi ise birtakım şartlar altında kişisel veriler üzerinde gerçekleştirilen her türlü işlem olarak açıklanmaktadır. Bu açıklamaların genel ve soyut yapısı, gerek kavramların içeriğinin ve gerekse hakkın kapsamı ile onu koruma mekanizmalarının öğreti ve uygulama aracılığı ile somutlaştırılmasını gerektirmektedir.

Bu çalışmada öncelikle kişisel veri kavramı uluslararası düzenlemeler ve çeşitli ülkelerin ulusal mevzuatları ile yargı kararları ışığında irdelenmiştir. Ardından kişisel verilerin korunmasına yönelik düzenlemelerin tarihsel gelişimi ve 7 Nisan 2016 tarihinde yürürlüğe giren Kişisel Verilerin Korunması Kanunu başta olmak üzere Türk Hukuku açısından mevcut durum değerlendirilmiştir. Son olarak 5237 sayılı Türk Ceza Kanunu’nda kişisel verilerin korunmasına yönelik olarak yer verilen suç tiplerine değinilerek kanunun 135. maddesinde düzenlenen kişisel verilerin kaydedilmesi suçu ayrıntılı olarak incelenmiştir.

Anahtar Kelimeler: Kişisel Veri, Kişisel Verilerin İşlenmesi, Hukuka Aykırı Olarak Kaydetme, Ceza Hukuku, Türk Ceza Kanunu m. 135.

SUMMARY

THE OFFENCE OF RECORDING PERSONAL DATA (TCC article 135)

Personal data protection is a contentious field worldwide and it has been subjected to legislations since 1970s. As a result of facilitation of recording, storage and classification of information with the effect of technological developments, the importance of personal data protection is increasing day by day. The capability of individuals to shape their behavior without constant monitoring is closely linked to human dignity and the right of free development of his/her personality. Therefore, the right of personal data protection has been considered in the concept of fundamental rights and freedoms. Even so, the right of personal data protection has been accepted as a merit of communal life as such criminal sanctions have been implemented in our laws to address certain violations.

In most legal texts, the concept of personal data has been defined as “any information relating to identified or identifiable individual”. Processing of personal data has been stipulated as any operation which is performed on personal data in certain conditions. The general and abstract nature of these explanations require both the context of concepts and the scope of right as well as the protection mechanisms to be embodied by doctrine and enforcement.

In this study, the concept of personal data has been firstly studied in the light of international regulations, national legislations of various countries and precedent. Secondly, the historical development of the regulations for personal data protection and the current position, mainly Personal Data Protection Act which came into force on 7 April 2016, have been evaluated under Turkish law. Finally, the criminal offences that are intended to protect personal data in the Turkish Criminal Code no. 5237 have been considered and offence of recording personal data that is under article 135 has been examined in detail.

Keywords: Personal Data, Processing Of Personal Data, To Record Illegally, Criminal Law, Article 135 Of Turkish Criminal Code.

TEŞEKKÜR

Bu çalışmanın hazırlanması sürecinde, değerli zamanını ve enerjisini benimle paylaşmaktan çekinmeyen; fikir, eleştiri ve tavsiyeleri ile ufkumu açan, sonuca ulaşma konusunda ümitsizliğe kapıldığım bir anda beni motive ederek çalışmamı nihayete erdirmemdeki katkılarını asla unutmayacağım kıymetli danışman hocam Dr. Öğr. Üyesi Mahmut Kaplan'a;

Yüksek lisans eğitimine başlamam konusundaki teşviki ve eğitim sürecindeki desteği nedeni ile Prof. Dr. Muharrem Kılıç'a;

Tecrübeleri ile yolumu aydınlatan ve ihtiyaç duyduğum her an yanımda olacağından emin olduğum babam Mustafa Köse'ye;

Bütün eğitim hayatım boyunca karşılaştığım zorlukları benimle birlikte göğüsleyen, heyecanımı ve sevincimi paylaşan sevgili annem Asuman Köse ve ablam Neslihan Dağlı'ya;

Lise ve lisans üzerine bir mezuniyeti daha omuz omuza yaşayacak olmaktan gurur duyduğum dostum E. Esra Uysal İbat'a;

Son olarak, çalışmamın başlangıcından bitişine kadar oldukça zorlu geçen yaklaşık bir buçuk senelik zaman zarfında bana duyduğu inanç, gösterdiği manevi destek, sabır ve fedakarlığı ile çalışmamın sonuçlanmasındaki büyük katkısından dolayı değerli eşim Cahit Aysun'a teşekkürü bir borç bilirim.

ÖNSÖZ

1960'lı yıllardan itibaren yaşanan toplumsal olaylar, bilimsel gelişmelerin rotasını sanayiden bilgiye çevirmesinin etkisi ile ortaya çıkan gözetim toplumu düşüncesi, özel yaşamın gizliliği hakkını gündeme getirmiştir. Bilgi ve iletişim teknolojilerindeki bu ilerlemenin sonucunda, kişilere ait bilgilerin kaydedilmesi, toplanması, sınıflandırılması, muhafaza edilmesi, aktarılması kolaylaşmış ve dolayısı ile bireylerin özel hayatının korunmasına dair ihtiyacı her zamankinden daha büyük önem kazanmıştır.

Kişisel verilerin elde edilmesi ve depolanmasındaki kolaylık, farklı yöntemlerle ve farklı amaçlarla toplanıp depolanan verilerin bir araya getirilerek veri eşleştirme ve veri madenciliği gibi tekniklerle analiz edilmesi suretiyle veriden yeni veriler üretme imkanı elde edilmesi, verilere erişim, paylaşım ve transferin kolaylaşması ve bu işlemlerin maliyetinin düşmesi, kişisel verilerin ticari açıdan kıymetli hale gelmesi sonucunda özel sektör tarafından kişisel verilerin hukuka aykırı işlenmesi riski yaratılması gibi nedenler dünyada ve özellikle Avrupa Birliği nezdinde 1970'li yıllardan itibaren ulusal ve uluslararası boyutta veri korumasına yönelik düzenlemeler ihdas edilmesine sebep olmuş ve olmaktadır.

Bununla birlikte, kişisel verilerin korunması hususunda ulusal düzenlemelerin birbiri ardına yürürlüğe konması ve ülkelerin veri koruma hukukuna ilişkin sergilediği farklı yaklaşımlar, kişisel verilerin korunması alanında yeterli veri koruması sağlamayan ülkelerle veri paylaşımında sorunlar yaşanmasına sebep olmuştur. Ülkeler arası veri transferinde yaşanan sorunlar ve getirilen sınırlamalar, kolluk güçleri ve adli anlamda işbirliği başta olmak üzere, uluslararası ticaret ve vergilendirmeye kadar pek çok işbirliği potansiyelini olumsuz etkilemektedir.

Çalışmamızda, öncelikle kişisel veri kavramının tanımı ile hukuki niteliğine ilişkin görüşlere, ardından kişisel verilerin korunmasına yönelik olarak yürürlüğe konulan uluslararası ve bir kısım ulusal düzenlemeye yer verilmiştir. Akabinde, yukarıda bahsi geçen olumsuzlukların önüne geçilmesi amacı ile ülkemizde 2016 yılında yürürlüğe konulan 6698 sayılı Kişisel Verilerin Korunması Kanunu incelenmiş ve 5237 sayılı Türk Ceza Kanunu'nun 135. maddesinde düzenlenen “kişisel verilerin kaydedilmesi suçu”nun unsurları mevzuat, öğreti ve içtihatlar temelinde irdelenmiştir.

Melike KÖSE AYSUN

Antalya, 2018

GİRİŞ

Modern hukuk devletlerinde birey her yönüyle bir bütün olarak kabul edilmektedir ve bireyin özel hayatı da bu bütünün bir parçasıdır. Zira bireyin özel hayatının korunması, insan kişiliğinin serbestçe gelişmesi, kişiye kendisi ve yakınları ile baş başa kalabileceği, devlet veya bir başkası tarafından rahatsız edilmeyeceği özerk bir alana sahip olma imkanı tanımaktadır¹.

İlmin güç ile eşdeğer olduğu yönündeki geleneksel düşünce; günümüzde yerini bilgi ile güç arasındaki sıkı ilişkiye bırakmış durumdadır². Yakın bir geçmişe kadar, bütün dünyada gerçekleşen her bir telefon görüşmesi, e-posta ve fax trafiğinin gizlice izlendiği bir global casusluk ağının varlığı bilim kurgu ile ilişkilendirilirken 2013 yılında Edward Snowden isimli bir Ulusal Güvenlik Ajansı çalışanının bu faaliyetin Amerika Birleşik Devletleri tarafından gerçekleştirildiğini açıklaması ile birlikte bilgi ile güç arasındaki ilişki hiç olmadığı kadar net bir görünüme kavuşmuştur³. 2017 yılı itibarı ile Çin Halk Cumhuriyeti'nde 170 milyon güvenlik (CCTV⁴) kamerasının bulunduğu ve gelecek üç yıl içerisinde yaklaşık 400 milyon kameranın daha faaliyete geçeceği bilinmektedir⁵. Gözetim toplumu düşüncesi yalnızca kamusal alanların izlenmesi ile değil; DNA örneklerinin, parmak izlerinin, retina tarama görüntülerinin ve kan gruplarının kaydedilmesi, muhafaza edilmesi ve kullanılması sonucunda yaygınlaşmakta ve insan hakları bakımından ciddi ihlal endişelerini gündeme getirmektedir⁶. Üstelik bu endişe başlangıçta devletin bireyin özel yaşamına müdahalesi ekseninde yoğunlaşmakta ise de bu verilerin özel kişilerce de suiistimal edilmesi tehlikesini beraberinde taşıdığı tartışmasızdır⁷.

Bu bağlamda kişilerin kimlik ve nüfus bilgileri, vergi kayıtları, hastaneler tarafından hastaların sağlık durumları ve geçirdiği rahatsızlıklara ilişkin tutulan kayıtlar; banka ve sigorta şirketleri ile benzeri finans kuruluşları tarafından müşterilerinin mali durumları, kredi notları ve harcamalarına ilişkin tutulan kayıtların yetkisiz üçüncü kişiler tarafından ele geçirilerek

¹ Kılınç, 2012: 1099.

² Lloyd, 2014: 4.

³ <https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded> (erişim tarihi:16.01.2018)

⁴ *Closed-Circuit Television* teriminin kısaltılmışıdır.

⁵ <http://www.bbc.com/news/av/world-asia-china-42248056/in-your-face-china-s-all-seeing-state> (erişim tarihi:16.01.2018)

⁶ <https://www.hrw.org/news/2017/12/13/china-minority-region-collects-dna-millions> (erişim tarihi:16.01.2018)

⁷ Stute, 2015: 652.

veri sahiplerini zarara uğratacak amaçlarla kullanılmaları oldukça sık karşılaşılan bir sorun haline gelmiştir⁸. Kişilerin, kişisel verilerinin çalınması ve bu verilerin suç işlemede araç olarak kullanılması esasen internetin varlığından çok öncesine dayanıyor olsa da; bilgi çağının değiştirdiği nokta, kimlik hırsızlığının kişisel verilere erişme ve bunları suiistimal yöntemidir; zira günümüzde tek bir kimlik hırsızlığı girişi yüzbinlerce ve hatta milyonlarca bireyi risk altına alabilmektedir⁹. Veri güvenliğini sağlamaya yönelik önlemler verilerin yalnızca üçüncü kişilerce kötüniyetli kullanımına değil, bunların kaza sonucu kaybı veya tahribata uğramasına yönelik olarak da önem arz etmektedir¹⁰.

Bu nedenle kişisel verilerin korunması, pek çok ulusal ve uluslar arası düzenlemede temel bir hak olarak kabul edilmektedir. Dünya çapında devletlerin %58'inde kişisel verilerin korunmasına ilişkin yasal düzenleme bulunmakta, %9'unda ise tasarı çalışmaları yürütülmekte, %21'inde ise herhangi bir yasal düzenleme bulunmamaktadır¹¹.

Türkiye'de ise 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 07.04.2016 tarihli Resmi Gazete' de yayımlanarak yürürlüğe girmesi ile birlikte Anayasa'nın 20. maddesinde tanımlanan kişisel verilerin korunması hakkı kanuni bir düzenlemeye kavuşmuştur. Böylece TCK'da kişisel verileri korumaya yönelik olan suçlar bakımından uygulamada karşılaşılan problemlerin çözüme kavuşturulması amaçlanmıştır¹².

⁸ Ergün, 2008: 113.

⁹ Peretti, 2008: 375.

¹⁰ United Nations, 2016: 3.

¹¹ http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx (erişim tarihi:16.01.2018). Devletlerin %12'sinde ise kişisel verilerin korunmasına ilişkin herhangi bir mevzuatın bulunup bulunmadığı bilinmemektedir.

¹² "Ülkemizde kişisel verilerin korunmasını sağlayacak bir kanunun yürürlüğe girmesini gerektiren değişik sebepler bulunmaktadır. Öncelikle, 5237 sayılı Türk Ceza Kanununun 135 ve devamı maddelerinde, kişisel verilerin hukuka aykırı olarak elde edilmesi, kaydedilmesi veya ifşa edilmesi fiilleri suç olarak düzenlenmiş ve yaptırımı bağlanmıştır. Bununla birlikte, kişisel verilerin işlenmesine yönelik özel bir kanunun bulunmaması sebebiyle, bu fiillerin ne zaman hukuka aykırı, ne zaman hukuka uygun olduğunun belirlenmesinde tereddütlerin yaşandığı görülmektedir." (KVKK'nın genel gerekçesinden).

BİRİNCİ BÖLÜM

KİŞİSEL VERİ KAVRAMI VE KİŞİSEL VERİLERİN KORUNMASI HUKUKU'NUN TARİHSEL GELİŞİMİ

1.1. Kişisel Veri Kavramı

07.04.2016 tarihli Resmi Gazete' de yayımlanarak yürürlüğe giren 6698 sayılı KVKK'nın 3. maddesine göre kişisel veri kavramı, *"kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi"* yi ifade etmektedir. Dolayısıyla, öncelikle bilginin bir kişiye ilişkin olması ve ardından bu kişinin belirli veya belirlenebilir nitelikte olması kişisel verinin unsurlarını oluşturur¹³.

Kişisel veri kavramının yukarıda işaret edilen tanımı, geniş ve müphem olması nedeni ile yalnızca bir çerçeve niteliği taşımaktadır. Bu sebeple, gerek ulusal ve gerekse uluslararası düzenlemelerde bu tanım yeknesak şekilde benimsenmiş ise de, hangi tür bilginin kişisel veri sayılıp hangilerinin sayılmayacağı hususu her ülke mevzuatında farklı şekilde değerlendirilmiştir¹⁴.

KVKK'nın yukarıda değinilen kişisel veri tanımının; Türkiye'nin de taraf olduğu ve 02.05.2016 tarihinde onaylayarak 01.09.2016 tarihinde yürürlüğe koyduğu *"108 Sayılı Avrupa Konseyi Sözleşmesi"* ile Avrupa Birliği veri koruma hukukunun temelini oluşturan *"Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Hakkındaki 95/46/EC sayılı Avrupa Birliği ve Avrupa Konseyi Yönergesi"*¹⁵ ve son olarak 27 Nisan 2016 tarihinde yayınlanan ve 25 Mayıs 2018 tarihinde yürürlüğe girecek olan *"2016/679 sayılı Genel Veri Koruma Tüzüğü"*¹⁶ nde düzenlenen veri tanımı ile uyduğu görülmektedir. Bu nedenle, kişisel veri kavramının çerçeve niteliği taşıyan tanımının yorumlanmasında ve içinin doldurulmasında bu metinlerden faydalanılmalıdır.

95/46/AT sayılı Yönerge'nin 29. maddesi ile veri koruma ilkelerinin uygulanmasında birlikteliği sağlamak amacı ile uygulamada ortaya çıkan sorunları incelemek, üye ülkeler ile üçüncü ülkelerin koruma düzeyleri hakkında Avrupa Birliği Komisyonu'na görüş bildirmek ve yapılabilecek yeni düzenlemelere ilişkin tavsiyede bulunmak üzere bir "Çalışma Grubu" kurulmuştur^{17, 18}.

¹³ Küzeci, 2010: 9.

¹⁴ Aksoy, 2010: 12.

¹⁵ Bundan böyle "95/46/AT sayılı Yönerge" olarak anılacaktır.

¹⁶ Bundan böyle "2016/679 sayılı Tüzük" olarak anılacaktır.

¹⁷ Uygun, 2010: 76.

Madde 29 Çalışma Grubu, 4/2007 sayılı görüşü¹⁹ ile kişisel veri tanımını ayrıntılı şekilde analiz etmiştir. Buna göre; 95/46/AT sayılı Yönerge’de yer alan kişisel veri tanımı dört temel yapıtaşından oluşmaktadır: "kimliği belirli veya belirlenebilir olan", "gerçek bir kişi", "ile ilgili", "her türlü bilgi".

1.1.1. Her Türlü Bilgi

1.1.1.1. Genel Olarak

Kişisel verinin unsurları bakımından açıklanmaya ve yorumlanmaya en çok ihtiyaç duyulan kavramın "her türlü bilgi" kavramı olduğu aşîkârdır. Burada belirtmek gerekir ki, esasen birbirlerinden farklı kavramlar olan veri (data); enformasyon (information) ve bilgi (knowledge) kavramları, veri koruması hukuku bağlamında birbirlerinin yerine geçer şekilde kullanılmaktadır²⁰. Zira her ne kadar farklı anlamlar taşıyalar da, yararlandıkları hukuki koruma bakımından bir ayrım gözetilmemiştir²¹. Kişiyeye ait olan ad, soyadı, doğum tarihi ve doğum yeri gibi kişinin kesin olarak teşhis edilmesi olanağını sunan bilgilerin yanında onun fiziki, ailevi, ekonomik ve sosyal hayatına ilişkin verilerin de kişisel veri olduğu ifade edilmektedir²². Bilginin mahiyeti açısından incelendiğinde; bir kişiye ait olmak kaydı ile gerek objektif, yani bir durumu herhangi bir değer yargısından bağımsız olarak tespit eden bilgiler²³, örneğin bir kimsenin kanında belli bir maddenin bulunup bulunmadığı gibi; gerekse

¹⁸ Avrupa Birliği tarafından hazırlanan ve 25.05.2018 tarihinde yürürlüğe girecek olan 2016/679 sayılı Genel Veri Koruma Tüzüğü (GDPR)’nın 94. maddesi ile, Madde 29 Çalışma Grubu’nun yetki ve görevleri Avrupa Veri Koruma Kurulu (European Data Protection Board) ’na devredilmiştir. Bk. http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf (erişim tarihi:09.11.2017).

¹⁹ Madde 29 Çalışma Grubu’nun 4/2007 sayılı görüşünün orijinal metni için bk. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf (erişim tarihi:09.11.2017).

²⁰ Aksoy, 2010: 11.

²¹ Küzeci, 2010: 12.

²² Bk. KVKK’ nın 3. madde gerekçesi. Ayrıca bk. Avrupa Birliği’nin 2016/679 sayılı Genel Veri Koruma Tüzüğü’nün 4. maddesi, http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf (erişim tarihi:06.11.2017); Aynı yönde bk. Dölger, 2016: 108.

²³ AİHM ve Anayasa Mahkemesi’nin pek çok kararında, kişiye ilişkin objektif bilgilerin kişisel veri niteliğinde olduğu sonucuna varılmıştır:

“9. Anayasa Mahkemesinin kararlarında da belirtildiği üzere, "kişisel veri", "belirli veya kimliği belirlenebilir olmak şartıyla, bir kişiye ilişkin bütün bilgileri ifade etmektedir. Bu bağlamda adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil; telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, IP adresi, e-posta adresi, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri, sağlık

bireysel görüş ve değer yargısı içeren subjektif bilgiler, örneğin bir kişinin güvenilir, adil ya da çalışkan olduğu gibi, kişisel veri kabul edilir²⁴. Kişisel verinin gerçek ya da kanıtlanmış bir bilgi olması gerekmez²⁵. Esasen kişisel verinin korunmasına ilişkin düzenlemeler de bilginin yanlış olma ihtimalini gözeterek veri öznesine bu bilgiye erişme, düzeltme veya itiraz etme mekanizmaları öngörmüşlerdir.

bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler" kişisel veri olarak kabul edilmektedir (E.2013/122, K.2014/74, 9.4.2014; E.2014/149, K.2014/151, 2.10.2014; E.2013/84, K.2014/183, 4.12.2014; E.2014/74, K.2014/201, 25.12.2014; E.2014/180, K.2015/30, 19.3.2015).

10. Türkiye'nin imzaladığı ancak uygulama kanununun yürürlüğe konmaması nedeniyle henüz taraf olmadığı 1981 tarihli ve 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Kişilerin Korunmasına Dair Avrupa Konseyi Sözleşmesi'nin 2. maddesinde "kişisel veri", "kimliği belirli veya belirlenebilecek verinin öznesi olan gerçek kişiyle ilgili tüm bilgiler" şeklinde tanımlanmaktadır. Sözleşme'nin "özellikli veri kategorileri" başlıklı 6. maddesinde ise "iç hukukta uygun güvenceler sağlanmadıkça, ırk menşesini, politik düşünceleri, dinî veya diğer inançları ortaya koyan kişisel nitelikteki verilerle sağlık veya cinsel yaşamla ilgili kişisel nitelikteki veriler ve ceza mahkûmiyetleri, otomatik bilgi işlemine tâbi tutulamazlar" demek suretiyle söz konusu verilerin kişisel veri kapsamında olduğunu belirlemektedir. Ekonomik Kalkınma ve İşbirliği Örgütü'nün (OECD) yayınladığı Kişisel Verilerin Korunması Rehber İlkeleri'nde "kişisel veri", "belirli veya belirlenebilir bir gerçek kişiye ilişkin tüm bilgiler" şeklinde tanımlanmaktadır. Avrupa Birliği'nin 95/46/EC sayılı Veri Koruma Direktifi'nin 2. maddesinde de "kişisel veri", "belirli ya da kimliği belirlenebilir gerçek kişi ile ilişkilendirilebilen her türlü bilgi" şeklinde tanımlandıktan sonra "bir kişinin doğrudan veya dolaylı olarak tanımlanabilmesine imkân sağlayan kişinin kimlik numarası, fiziksel, psikolojik, duygusal, ekonomik ve kültürel kimliği veya sosyal kimliğin"nin bu kapsamda değerlendirildiği ifade edilmektedir.

11. "Kişisel veri" kavramı tarafı olduğumuz Avrupa İnsan Hakları Sözleşmesi'nde (AİHS) açık bir şekilde düzenlenmemekle birlikte, Sözleşme'nin uygulanmasına ilişkin Avrupa İnsan Hakları Mahkemesi (AİHM) kararlarında Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına Dair Sözleşme'ye atıfta bulunulmakta ve bu verilerin özel yaşamın gizliliğinin bir parçası olduğu kabul edilmektedir. AİHM kararlarında kişilere ait "görüntü", "fotoğraf", "parmak izi", "DNA profili", "hücre örnekleri", "ev adresi" ve "yaş, doğum tarihi ve fiziksel özellikler" "kişisel veri" kapsamında değerlendirilmektedir (Peck/Birleşik Krallık, B.No: 44647/98, 28.01.2003; Sciacca/İtalya, B.No:50774/99, 11.01.2005; S. ve Marper/Birleşik Krallık, (Büyük Daire), B.No: 30562/04, 30566/04, 04.12.2008; Alkaya/Türkiye, B.No:42811/06, 09.10.2012; K.U./Finlandiya, B.No:2872/02, 02.12.2008)." bk.; Anayasa Mahkemesi'nin 12.11.2015 tarihli ve 29550 sayılı Resmi Gazete'de yayımlanan 2015/32 Esas, 2015/102 Sayılı kararı.

²⁴ Madde 29 Veri Koruma Çalışma Grubu, 2007: 6, bk. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf (erişim tarihi:09.11.2017).

²⁵ Madde 29 Veri Koruma Çalışma Grubu, 2007: 6, bk. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf (erişim tarihi:09.11.2017).

Bilginin içeriği açısından incelendiğinde, bireyin özel ve aile yaşamının yanında, onun tarafından gerçekleştirilen iş ilişkileri, ekonomik ya da sosyal yaklaşımlarına ait bilgiler kişisel veridir²⁶. Kişisel verinin yalnızca bireyin özel ve aile yaşamı ile ilişkili bilgiler olmadığı, 95/46/AT sayılı Yönerge'nin lafzından anlaşılmaktadır. Her ne kadar özel yaşamın gizliliği hakkı Avrupa İnsan Hakları Mahkemesi içtihatlarında da vurgulandığı üzere oldukça geniş yorumlansa da kişisel verinin korunmasına ilişkin düzenlemeler, özel yaşamın gizliliği hakkının ötesine geçmiştir²⁷. Birçok ulusal düzenlemede olduğu gibi, 2000 tarihli Avrupa Birliği Temel Haklar Şartı'nda da kişisel verilerin korunması hakkına, özel yaşamın gizliliği hakkından bağımsız bir hak olarak ayrıca yer verilmiştir. Bunun yanında, 95/46/AT sayılı Yönerge'nin 1. maddesi ile *"kişisel verilerin işlenmesine dair 'başta' kişisel mahremiyet hakkı olmak üzere gerçek kişilerin temel hak ve özgürlüklerini koruyacaktır"* ifadesi kullanılarak 95/46/AT sayılı Yönerge'nin koruma alanının kişilerin özel hayatlarının gizliliği hakkına işaret eden mahremiyet hakkı ile sınırlı olmadığı teyit edilmiştir. Ayrıca, 95/46/AT sayılı Yönerge'nin 8. maddesi ile iş hukuku, suçlar, adli hükümler ve güvenlik tedbirleri, hukuk davaları ve idari müeyyidelere ilişkin verilerin yanında 14. maddesi ile doğrudan pazarlamaya ilişkin verilere özel olarak atıfta bulunduğu, bununla kişisel veri koruma mekanizmasının aile ve özel hayatın gizliliği hakkının dışına çıkacak şekilde temellendirildiği görülmektedir.

Bilginin biçimi açısından incelendiğinde ise, hangi formatta olursa olsun; alfabetik, sayısal, grafiksel, fotoğrafik ya da akustik, bilgi ihtiva eden herhangi bir form kişisel veri olarak kabul edilmiştir²⁸. Hal böyle iken, bilginin kağıda dökülmüş olması, bilgisayar hafızasında ikili kod ile muhafaza edilmesi ya da video kaydında bulunması fark yaratmamaktadır. Bu bakımdan bireye ait bir bilgi içerdiği müddetçe ses ve görüntü verilerinin de kişisel veri kapsamında olduğu kabul edilmelidir ki, 95/46/AT sayılı Yönerge'nin 33. maddesi ile bu hususa ayrıca yer verilmiştir. Buna göre, telefon bankacılığı

²⁶ Madde 29 Veri Koruma Çalışma Grubu, 2007: 6, bk. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf (erişim tarihi:09.11.2017).

²⁷ Kişisel verilerin korunması hakkının, özel yaşamın gizliliği hakkına ilişkin yaklaşımlarla korunmasının yaşanan teknolojik gelişmeler neticesinde mümkün olmadığı ve bu hakkın temeli özel yaşamın gizliliği hakkına dayanan ancak ondan bağımsız bir alan haline geldiği konusundaki tartışmalar için bk. Dülger, 2016: 103-104.

²⁸ Madde 29 Veri Koruma Çalışma Grubu, 2007: 7, bk. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf (erişim tarihi:09.11.2017).

kapsamında kaydedilen, müşterinin direktiflerine ilişkin ses kayıtları veya bireyin videolu gözetli sistemi ile kaydedilen görüntüleri kişisel veridir²⁹.

1.1.1.2. Özel Veri Kategorileri (Hassas Veri)

Kişiye ait birtakım veriler, işlenmeleri halinde bireylerin hak ve özgürlüklerinin önemli ölçüde ihlal edilmesi tehlikesi bulunması ve bu bağlamda hassasiyet arz etmeleri nedeni ile birçok ülke ve kurum tarafından “özel veri kategorileri” olarak kabul edilmişlerdir. Bu “hassas veriler” veya “özel veri kategorileri” yönünden nitelikli ve kapsamlı şekilde koruma usulleri öngörülmüş olup hangi tür verilerin hassas veri olarak kabul edileceği ve hangi hallerde işlenebileceği uluslararası düzenlemelerde ve devletlerin ulusal mevzuatlarında belirtilmektedir³⁰.

Özel veri kategorileri; her ülke mevzuatında farklılık arz etmekle birlikte³¹, genel olarak kişilerin ırksal veya etnik kökenine, siyasi görüşüne, dini ve felsefi inancına, sendika üyeliğine, sağlığına, cinsel yaşamına ilişkin verileri ile genetik ve biyometrik verileri olarak sayılabilir³².

Özel veri kategorileri içerisinde yer alan, dini ve felsefi inanç, siyasi görüş ve sendika üyeliği gibi kişiye ilişkin verilerin korunması yalnızca Avrupa İnsan Hakları Sözleşmesi’nin 8. maddesi ile güvence altına alınan özel yaşamın gizliliği hakkı kapsamında değil; Sözleşmenin 9. maddesinde yer alan düşünce, din ve vicdan özgürlüğü, 10. maddesinde yer alan ifade özgürlüğü, 11. maddede yer alan toplantı ve dernek kurma özgürlüğü ile 14. maddede düzenlenen ayrımcılık yasağının da konusunu oluştururlar³³.

Bu veri kategorilerinin içerisinde; kişinin davranışsal ve fizyolojik karakteri ile ilişkili olması ve kişinin kimliğini doğrudan belirleme imkanı sağlayan kendine özgü niteliği sebebi ile biyometrik verilerin geniş ve kontrolsüz olarak işlenmesi, bu kategoriye dahil verilerin kişisel verilerin korunmasına ilişkin düzenlemelerde hassas veri olarak kabul edilmesi

²⁹ Madde 29 Veri Koruma Çalışma Grubu, 2007: 7, bk. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf (erişim tarihi:09.11.2017).

³⁰ Korff, 2002: 81; Kaya, 2011: 317.

³¹ Özel veri kategorilerinin ülkeler bazında arz ettiği farklılıklar hakkında ayrıntılı bilgi için bk. Kaya, 2011: 319.

³² 2016/679 sayılı GDPR madde 9, http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf (erişim tarihi:09.11.2017).

³³ Korff, 1998: 15.

sonucunu doğurmaktadır³⁴. Bir kişinin belirlenmesi ihtiyacına doğal ve güvenilir bir çözüm sunan biyometrik veriler; kişinin parmak izi, avuç içi izi, yüz, iris, retina, kulak, ses, imza, yürüyüş biçimi, el damarı, vücut kokusu gibi bilgilerden oluşmaktadır³⁵.

Uluslararası düzenlemeler ile birtakım ülkelerin ulusal mevzuatında özel veri kategorilerinin kapsamı aşağıdaki tabloda gösterilmiştir.

Tablo 1.1 Uluslararası Düzenlemeler ile Birtakım Ülkelerin Ulusal Mevzuatında Özel Veri Kategorilerinin Kapsamı

108 Sayılı Sözleşme (m. 6)	95/46/AT Sayılı Yönerge (m. 8)	2016/679 Sayılı Tüzük	İngiltere Veri Koruma Kanunu (m. 2)³⁶	Fransız Ceza Kanunu (m. 226- 19)³⁷	Türk Ceza Kanunu (m. 135/2)	6698 Sayılı Kanun (m. 6)
Irki köken	Irki veya etnik köken	Irki veya etnik köken	Irki veya etnik köken	Irki veya etnik köken	Irki köken	İrk veya etnik köken
Siyasi görüş	Siyasi görüş	Siyasi görüş	Siyasi görüş	Siyasi görüş	Siyasi görüş	Siyasi düşünce
Dini ve diğer inanç	Dini veya felsefi inanç	Dini veya felsefi inanç	Dini veya benzer mahiyetteki diğer inanç	Dini veya felsefi görüş	Felsefi veya dini görüş	Din, mezhep ile felsefi ve diğer inanç

³⁴ Madde 29 Çalışma Grubu'nun 3/2005 sayılı, biyometrik verilerin Birlik üyesi devletler tarafından düzenlenen pasaport ve vizelerde kullanılmasına ilişkin görüşü için bk. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp112_en.pdf (erişim tarihi: 15.11.2017)

³⁵ Akgül, 2015: 202-203.

³⁶ https://www.legislation.gov.uk/ukpga/1998/29/pdfs/ukpga_19980029_en.pdf (erişim tarihi: 02.01.2018)

³⁷ https://www.legifrance.gouv.fr/affichCode.do;jsessionid=41ED3CB20161448EBD6835FDAE939576.tplgfr25s_1?idSectionTA=LEGISCTA000006165313&cidTexte=LEGITEXT000006070719&dateTexte=20180102 (erişim tarihi: 02.01.2018)

Sağlık	Sağlık	Sağlık	Fiziksel ya da ruhsal sağlığı veya durumu	Sağlık	Sağlık durumu	
Cinsel yaşam	Cinsel yaşam	Cinsel yaşam veya cinsel yönelim	Cinsel yaşam	Cinsel yönelim veya cinsel kimlik	Cinsel yaşam	
Ceza mahkumiyeti	Ceza mahkumiyeti	Ceza mahkumiyeti	İşlediği veya işlediği iddia edilen herhangi bir suç veya buna ilişkin yargılama ya da mahkumiyet			
	Sendika üyeliği	Sendika üyeliği	Sendika üyeliği	Sendika üyeliği	Sendikal bağlantı	Dernek, vakıf veya sendika üyeliği
					Ahlaki eğilim	
						Kılık ve kıyafet
		Genetik ve biyometrik veri				Biyometrik ve genetik veri

1.1.2. Bilginin Gerçek Kişiyne İlişkin Olması

Kişisel verilerin korunmasına ilişkin düzenlemeler bakımından “kişi” kavramının kapsamı, bu düzenlemelerin vaat ettiği hukuki korumadan kimlerin yararlanacağına belirlenmesi açısından önem taşımaktadır. 108 Sayılı Avrupa Sözleşmesi ve 95/46/AT sayılı Yönerge’ de yapılan kişisel veri tanımında “gerçek kişi (natural person)” ifadesinin kullanılmış olması karşısında, tüzel kişilere ait verilerin bu düzenlemelerin sağladığı hukuki korumadan faydalanması mümkün görünmemektedir.

Bunun yanında, üye devletlerin iç hukuklarında yürürlüğe koydukları veri koruma yasaları ile 95/46/AT sayılı Yönerge’nin uygulama alanını genişletmelerinin ve tüzel kişilere ait verileri de kişisel veri olarak kabul etmelerinin önünde herhangi bir engel bulunmamaktadır³⁸. Nitekim; Fransa, İsveç, Hollanda, Polonya ve Estonya ilgili kanunlarında kişiyi tanımlarken “natural person (gerçek kişi)”; Almanya “individual (birey, gerçek şahıs)”; Finlandiya “private individual (özel birey, gerçek kişi)”; İngiltere “living individual (yaşayan birey, gerçek kişi) terimlerini kullanmakta iseler de; İtalya ve Avusturya’ nın “natural or legal person (gerçek veya tüzel kişi)” terimlerini kullandıkları görülmektedir³⁹. Benzer şekilde Danimarka ve Lüksemburg ile Avrupa Birliği üyesi olmayan İzlanda, Norveç ve İsviçre de sözleşmenin kapsamını genişleterek veri koruma yasaları ile tüzel kişilere ait verileri koruyan ülkelerdendir⁴⁰.

Türk hukukunda ise, 5237 sayılı Türk Ceza Kanunu’nun kişisel verilere yönelik suçları düzenleyen 135. ve devamı maddelerinde, suçun konusu olan kişisel verinin tanımı yapılmamış ve kapsamı belirlenmemiş olup bunun sonucu olarak suçun mağdurunun hem gerçek kişi hem de kendi yapılarına has kişisel verileri bulunan tüzel kişi olabileceği savunulmuştur^{41, 42}. Buna karşılık, esasen özel hayat kavramının gerçek kişilerle alakalı olduğu ve tüzel kişiler yönünden “ticari gizlilik” kavramının söz konusu olabileceği⁴³ bu nedenle tüzel kişilere ait bilgilerin kişisel veri olarak değil ticari sır olarak kabul edilmesi

³⁸ Aksoy, 2010: 19.

³⁹ Akgül, 2014: 14.

⁴⁰ Korff, 1998: 23-38.

⁴¹ Şen, 2011: 202; Akgül, 2014: 15.

⁴² 24.07.2012 tarihli ve 28363 sayılı Resmi Gazete’de yayımlanarak yürürlüğe giren "Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik"te kişisel veri kavramı, yönetmeliğin 3. maddesinin 1. fıkrasının (h) bendinde, belirli veya kimliği belirlenebilir gerçek ve tüzel kişilere ilişkin bütün bilgiler olarak tanımlanmıştır.

⁴³ Tezcan, 1991: 389.

gerektiği ileri sürülmektedir⁴⁴. Tüzel kişilere ait ticari sır, bankacılık sırrı veya müşteri sırrı niteliğindeki bilgiler de TCK'nın 239. maddesi ile korunmakta, bu tür bilgi ve belgelerin açıklanması halinde sorumluların hürriyeti bağlayıcı ceza ve adli para cezası ile cezalandırılması öngörülmektedir.

KVKK'nın kişisel veri kavramını, “kimliği belirli ya da belirlenebilir gerçek kişiye dair her türlü bilgi” olarak tanımlaması karşısında kanunkoyucunun tüzel kişilere ait verilerin kişisel veri olarak kabul edilmemesinden yana tercih gösterdiği anlaşılmaktadır. Bu sebeple TCK'nın 135. ve devamı maddelerinde düzenlenen suçların konusunu gerçek kişiye ilişkin bilgiler oluşturmaktadır.

1.1.3. Bilginin Kişi ile İlgili Olması

Kural olarak, bir bilgi kişi “hakkında” olduğunda, o bilginin kişi ile ilgili olduğu kabul edilmekte olup bu durumun istisnası, verinin ilettiği bilginin bireyden önce objelere ilişkin olmasıdır; örneğin bir evin değeri o ev hakkında bir bilgidir ve veri koruma kurallarının bu veri bakımından uygulanmayacağı aşikârdır⁴⁵. Fakat bu evin belirli bir kişiye ait olması durumunda, evin değeri o kişi ile ilgili bir kişisel veri haline gelecektir; zira bu veri kişinin malvarlığı ve vergisel yükümlülüğü hakkında bir bilgi ihtiva edecektir.

Madde 29 Çalışma Grubu, verinin kişinin kimliği, karakteri, davranış biçimine işaret ettiğinde veya o kişiye ne şekilde davranılıp kişinin nasıl değerlendirileceğini belirlemek için kullanıldığında kişi ile ilgili olduğu sonucuna varmıştır⁴⁶.

1.1.4. Kişinin Belirli ya da Belirlenebilir Olması

Gerçek bir kişinin belirli olması, o kişinin bulunduğu grubun diğer üyelerinden ayırt edilebilmesi anlamına gelir⁴⁷. Belirlenebilir olması ise, kişinin henüz belirlenmemiş olmakla birlikte verilerin doğrudan veya dolaylı olarak bir kişi ile ilişkilendirilmesi sonucunda kişinin tanımlanabilmesi, belirlenmesinin mümkün olmasıdır⁴⁸.

95/46/AT sayılı Yönerge'nin 2. maddesinde, kişinin fiziksel, fizyolojik, zihinsel, ekonomik, kültürel ve sosyal özelliklerine ilişkin bir veya birkaç faktörün değerlendirilmesi

⁴⁴ Tezcan, 1991: 389.

⁴⁵ Madde 29 Veri Koruma Çalışma Grubu, 2007: 9, bk. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf (erişim tarihi:09.11.2017).

⁴⁶ Madde 29 Veri Koruma Çalışma Grubu, 2007: 10, bk. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf (erişim tarihi:09.11.2017).

⁴⁷ İtişgen, 2015:183.

⁴⁸ Ergün, 2008:114.

sureti ile kişinin doğrudan ya da dolaylı olarak tespit edilmesi veya edilebilecek durumda olması durumunda bu kişiye ait her türlü bilginin kişisel veri olduğu kabul edilmiştir.

95/46/AT sayılı Yönerge’de, belirli veya belirlenebilir kişisel veriler arasında herhangi bir ayırım yapılmayarak, her ikisi de kişisel veri kavramı içerisinde ele alınmıştır⁴⁹. Dolayısıyla kişinin kimliğinin belirli ya da belirlenebilir olması, bilginin kişisel veri olarak değerlendirilmesi ve hukuki korumadan yararlanması açısından önem arz etmektedir. Bir kişinin kimliğinin belirlenebilirliği doğrudan olabilir; örneğin kişinin ismi bilindiği takdirde, kimliği doğrudan belirlenebilecektir. Ancak kişinin kullandığı telefon numarası, sosyal güvenlik numarası, pasaport numarası ya da ait olduğu grubun içerisinde yaşı, mesleği, oturduğu yer gibi önemli kriterlerin birleşimi ile tespit edilebildiği durumda kimliği dolaylı olarak belirlenmesi mümkün kılınabilir.⁵⁰ Yine, kişiler ses ve görüntüleri aracılığı ile de dolaylı olarak belirlenebilir; örneğin güvenlik maksadı ile alınan parmak izi veya kamera görüntülerinden alınan resim ve ses bilgileri gibi⁵¹. Bir kişiye ilişkin bir bilginin hangi durumlarda onu diğerlerinden ayırt ederek onun kimliğini belirlenebilir kıldığını her somut olay açısından ayrıca değerlendirmek gerekecektir. Örneğin, yaygın bir soyisim, o kişinin yaşadığı ülkede onu belirlenebilir kılmazken, bir öğrenciyi sınıfındaki diğer öğrencilerden ayırt etmeye elverişlidir.

Burada belirtmek gerekir ki, kişinin ismi, onu belirlenebilir kılan en önemli faktör olsa da, her koşulda yalnız başına yeterli olmayabilir. Bu durum, bir kişinin diğerlerinden ayırt edilebilmesinde diğer belirleyici faktörler kullanıldığında karşımıza çıkar. Örneğin internet üzerinde, internet trafiğini izleme araçları bir cihazın ve dolayısıyla onun kullanıcısının davranışlarını belirleme imkânı sağlamaktadır. Bu durumda, kullanıcının ismi veyahut adresi dahi araştırılmaksızın, o kişiyi sosyo-ekonomik, psikolojik, felsefi açıdan kategorize etme ve onun hakkında belirli bir kanıya varma mümkün olacaktır. Bir başka deyişle, bir kişinin belirlenebilir olması o kişinin isminin tespit edilmesini gerektirmemektedir.

Kişiye ilişkin olan bir verinin; araştırma, istatistik vb. amaçlar kapsamında kullanılmak saiki ile ilgili olduğu kişi ile ilişkilendirilemeyecek ve kaynağına ulaşamayacak hale getirilmesi durumunda, artık o veri "anonim veri" olarak adlandırılır ve kişisel verinin

⁴⁹ Damman/Simitis, 109, PN. 1-3’ten aktaran: Özdemir, 2009: 124.

⁵⁰ Madde 29 Veri Koruma Çalışma Grubu, 2007: 13, bk. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf (erişim tarihi:09.11.2017).

⁵¹ Özdemir, 2009: 124.

kimliği belirli veya belirlenebilir olma unsurunu taşımadığından meydana gelen bu tür veriler kişisel veri olarak kabul edilmez⁵².

1.2. Kişisel Verinin Hukuki Niteliği

Kıta Avrupası hukuk sisteminde kişisel veri kişilik hakkının; Amerikan hukukunda ise mülkiyet hakkının bir parçası olarak kabul edilirken kişisel verinin hukuki niteliğine dair diğer bir görüşe göre hakkın özü fikri mülkiyet hakkına dayanmaktadır. Bireyin kişisel verilerinin korunmasını isteme hakkının bulunduğu tartışmasız olmakla birlikte bu hakkın korunması ile amaçlanan menfaatin ne olduğu, başka bir deyişle kişisel verinin hukuki niteliği konusunda henüz bir görüş birliğine varılabilmiş değildir⁵³.

1.2.1. Kişilik Hakkı Görüşü

Kişilik hakkı; kişiye, onun manevi ve bedeni bütünlüğü ile kişisel menfaat ve ilişkilerine haksız tecavüzlerden kaçınılmasını diğer kişilerden isteme yetkisi verir⁵⁴. Bu anlamda kişilik hakkı, niteliği itibari ile mutlak bir hak olup herkese karşı ileri sürülebilir⁵⁵. Bunun yanında, şahsa sıkı sıkıya bağlı bir hak olduğundan mirasçılara geçmez, zamanaşımına uğramaz ve kişi tarafından üzerinde tasarrufta bulunulamayacağından devredilemez, feragat edilemez ve vazgeçilemez⁵⁶.

Kişilik hakkının sınırına ilişkin olarak ortaya atılan ilk görüşe göre kişilik hakkı adı altında bağımsız bir kavramın kabulüne gerek bulunmayıp bu görüşü benimseyen Alman Medeni Kanunu'nda kişilik hakkına ilişkin genel nitelikte bir hükme yer verilmemekte; sadece belirli kişisel varlıkların ihlaline ilişkin olarak koruma öngörülmekte idi⁵⁷. Kişilik hakkının sınırına dair savunulan ikinci görüşe göre ise kişilik hakkı adı altında bağımsız bir hak vardır ve bu hak her kişiye kendi kişilik alanını oluşturan varlıkları üzerinde egemenlik sağlar⁵⁸. Bu görüşü temel alan ilk Medeni Kanun İsviçre Medeni Kanunu'dur ve bu kanunun iktibas edilmesi sonucunda Türk hukukunda da kişilik hakkı genel bir çerçeve hak olarak kabul edilmiştir⁵⁹. Buna göre TMK'nun 24. maddesi uyarınca, *“hukuka aykırı olarak kişilik hakkına saldırılan kimse, hâkimden, saldırıda bulunanlara karşı korunmasını isteyebilir”*.

⁵² Dülger, 2016:110.

⁵³ Küzeci, 2010: 60.

⁵⁴ Simonius, 1955: 188.

⁵⁵ Simonius, 1955:188; Akipek ve Akıntürk, 2007: 347; Kaya: 2010: 280.

⁵⁶ Akipek ve Akıntürk, 2007: 347; Aksoy, 2010: 43; Özdemir, 2009: 111.

⁵⁷ Aksoy, 2010: 39-40.

⁵⁸ Aksoy, 2010: 40.

⁵⁹ Aksoy, 2010: 40-42.

Kişilik hakkının, kanunda genel ve kapsayıcı bir biçimde düzenlenmesi, kişilik hakkı türlerini somut olaya ve günün şartlarına uygun olarak belirlenmesi imkanı yaratmaktadır⁶⁰. “Genel kişilik hakkı, bireye içerisinde gözetlenmeksizin yalnız kalabileceği, kendisini geliştirebileceği ve kendisinin özel güvenini taşıyan kişilerle iletişimde bulunabileceği özel bir alanın korunmasını garanti etmektedir”⁶¹.

Kıta Avrupası Hukuku’nda baskın görüş, kişisel verilerin hukuki mahiyetini kişilik hakkı bağlamında değerlendirmektedir; zira gerek 108 sayılı Avrupa Konseyi Sözleşmesi ve gerekse 95/46/AT sayılı Yönerge’nin amacının kişilerin özel yaşamın gizliliği hakkı⁶² temelinde temel hak ve özgürlüklerinin korunması olduğu belirtilmiştir⁶³.

Özel yaşamın gizliliği hakkı, ilk kez Warren ve Brandeis tarafından “yalnız bırakılma hakkı (right to be let alone)” olarak tanımlanmıştır⁶⁴. Ancak bu tanım özel yaşamın gizliliği kavramını tam olarak açıklayamamakla birlikte bugüne dek de özel yaşamın gizliliğinin genel geçer bir tanımı da yapılmamıştır. Bununla birlikte özel yaşamın gizliliği; kişinin üstünün, eşyasının ve konutunun dokunulmazlığı; kişinin telefon görüşmeleri, mesajları ve e-postaları gibi iletişim kaynaklarını ilgilendiren haberleşmenin gizliliği; kişinin vücut tamlığına ilişkin uyuşturucu, DNA testine olanak sağlayan müdahaleleri kapsayan vücut bütünlüğü ve son olarak kişisel verilerinin işlenmesi sürecine ilişkin olarak kişisel verilerinin korunması olmak üzere dört ana başlık halinde ifade edilebilir⁶⁵.

Kişisel verilerin korunması hakkı, kişiye kendisine ait verilerin kim tarafından, nerede ve ne zaman, hangi koşullar altında veya hangi amaçlarla kullanıldığı konularında bilgi sahibi olma ve karar verme yetkisi bahşeder⁶⁶. Kişisel verilerin veri öznesine bu yetkiyi vermeksizin işlenmesi ve kötüye kullanılmasının Nazi Almanyası’nda yarattığı sonuçlar, kişisel verilerin

⁶⁰ Aksoy, 2010: 45.

⁶¹ Şimşek, 2008:133.

⁶² Metnin orijinalinde yer alan “privacy” kavramı, pek çok çalışmada “mahremiyet” olarak kullanılmış olup mahremiyet kavramının kişinin herkesle paylaşmadığı ve paylaşmama hakkının bulunduğu düşünce, kanaat, hissiyat ve yaşamına dair olayları ifade etmesi, buna karşın özel hayatın gizliliği hakkının kişinin yalnızca mahrem alanını değil kısmen kamuya açık alanını da kapsaması nedeni ile çalışmada özel yaşamın gizliliği kavramı tercih edilmiştir (Aynı yönde bk. Küzeci, 2010: 14).

⁶³ Aksoy, 2010: 47.

⁶⁴ Warren ve Brandeis, 2007: 1.

⁶⁵ Ketizmen, 2008: 192-193.

⁶⁶ Aydın, 2015: 21.

korunması hakkının kişilik hakkının bir parçası olarak kabul edilmesi ve kapsamlı hukuki düzenlemelere konu edilmesine yol açmıştır⁶⁷.

1.2.2. Mülkiyet Hakkı Görüşü

Kişisel verilerin hukuki niteliğine dair öne sürülen diğer bir görüş, kişisel bilgilerin bir mülkiyet türü olduğu görüşüdür⁶⁸. Mülkiyet hakkı görüşü, özellikle Amerikan Hukuku'nda kabul edilmekte ve herkesin kendisine ait kişisel verilerin sahibi olduğu kabul edilirse; veri öznesinin kendisine ilişkin bilgiler üzerinde denetim hakkını elinde bulunduracağı, böylece mülkiyetindeki verilerin hangi koşullarda kullanılabileceğini kendisinin belirleyebileceğini savunmaktadır⁶⁹.

Mülkiyet hakkı görüşüne göre, veri öznelere yaptıkları anlaşmalarla verilerinin kullanımını uygun bir karşılığa bağlayabileceklerdir⁷⁰. Böylelikle kişisel verilerini çeşitli kurum ve kuruluşlara satmak ya da açıklamak konusunda istekli olan bireyler nazara alındığında kişisel veri pazarının daha adil işlemesi sağlanabilecektir⁷¹. Diğer yandan, kişisel verilerin kullanılmasının doğuracağı maliyet, şirketleri hangi verilerin toplanıp işleneceği konusunda daha dikkatli karar almaya yönlendirecektir⁷².

Mülkiyet hakkı yaklaşımı savunucularına göre bu görüşün sağladığı bir diğer fayda, özel yaşamın gizliliğini önemli bulan ve verilerini paylaşmak istemeyen bireylerin de bu verilerin kötüye kullanılması durumunda ilgili kişiden zararının giderilmesini isteme hakkına sahip olacağıdır⁷³.

Mülkiyet hakkı görüşü, çeşitli açılardan eleştirilmektedir. Örneğin mülkiyet hakkının malike sağladığı tasarruf yetkisi kapsamı itibariyle malı devretme, değişiklik yapma ve yok etme imkanı sağlamakta iken bu seçeneklerin kişisel veriler bakımından kabulü mümkün değildir; zira bir kişinin kişisel verilerini satın alan kişinin veri öznesinin rızası aranmaksızın

⁶⁷ Aksoy, 2010: 55-57. 1930'lu yıllarda Hollanda'nın kamu hizmetlerinin geliştirilmesi amacı ile nüfus bilgi sistemini yeniden düzenleme faaliyeti çerçevesinde oldukça masumane saikle toplanan ve vatandaşların dini inançlarını içeren bilgilerin yer aldığı veri sisteminin II. Dünya Savaşı sırasında Naziler tarafından ele geçirilmesinin sonucunda Batı Avrupa'daki diğer ülkelerde bulunan Yahudilere oranla çok fazla sayıda Hollandalı Yahudi vatandaşların öldürüldüğü bilinmektedir (Stute, 2015: 652).

⁶⁸ Küzeci, 2010: 62, Aksoy, 2010: 57.

⁶⁹ Küzeci, 2010: 62, Aksoy, 2010: 57.

⁷⁰ Samuelson, 2000: 1128-1129.

⁷¹ Küzeci, 2010: 62.

⁷² Samuelson, 2000: 1129.

⁷³ Küzeci, 2010: 62.

bu verileri üçüncü kişilere devretme hakkına sahip olması gerekir ki bu durum kişisel verilerin korunmasına ilişkin düzenlemeler ile bağdaşmamaktadır⁷⁴.

1.2.3. Fikri Mülkiyet Hakkı Görüşü

Kişisel verilerin hukuki niteliğinin fikri mülkiyet hakkı kapsamında değerlendirilmesi gerektiğine dair görüş, temelini fikri mülkiyetin bilginin korunarak dağılımının kontrol edilmesi amacı ile kişisel verilerin korunması amacının benzerlik taşımasından almaktadır⁷⁵.

Amerikan hukuk sistemi içerisinde ortaya atılan bu görüşe göre telif benzeri bir yaklaşım ile kişisel verilerin korunabileceği savunulsa da; telifin ekonomik temeli ve fikri mülkiyet ürünlerinin oluşumu aşamasındaki gösterilen emek, zeka ve fikri çaba nazara alındığında kişisel verilerin bir fikri mülkiyet ürünü olarak kabul edilmesi mümkün değildir⁷⁶.

Kişisel verilerin korunmasına ilişkin uluslararası düzenlemeler ile KVKK incelendiğinde, bu metinlerin kişisel verilerin hukuki niteliği bakımından yukarıda anılan görüşlerden hiçbirini tam anlamıyla karşılamadığı, bu metinlerin veri işleyenler ve veri öznesi arasındaki menfaat dengesini kurmayı amaçladığı görülmektedir. Mülkiyet hakkı ve fikri mülkiyet hakkı görüşlerinin kişisel verilerin metalaştırılması sonucunu doğurması; temelini özel yaşamın gizliliği hakkına dayandıran kişilik hakkı görüşü bakımından ise kişinin özel yaşamına dair olmayan kamusal alanına ilişkin verilerin özel yaşamın gizliliğinin korunması hakkı kapsamında değerlendirilemeyeceği; ancak bu tür verilerin kimliği belirli veya belirlenebilir kişiye ilişkin olması halinde korunması gerekliliğinin bulunması nedenleri ile kişisel verilerin hukuki niteliğinin esasen kişilik hakkının bir görünümü olan enformasyonel self-determinasyon hakkı olduğu da savunulmaktadır⁷⁷. Nitekim 2016/679 sayılı Tüzük'te düzenlemenin amacının 95/46/AT sayılı Yönerge'den farklı olarak, kişisel verilerin korunması hakkı temelinde kişilerin temel hak ve özgürlüklerinin korunması olduğu belirtilmiştir. Bu durum, kişisel verilerin korunması hakkının, özel yaşamın gizliliği hakkından bağımsız bir kişilik hakkı alanı olarak kabul edilme yaklaşımının benimsenmeye başlandığının bir göstergesi olarak değerlendirilebilir.

⁷⁴ Aksoy, 2010: 65.

⁷⁵ Samuelson, 2000: 1134.

⁷⁶ Küzeci, 2010: 64; Aydın, 2015: 17; Uncular, 2014: 24.

⁷⁷ Aksoy, 2010: 68-72.

1.3. Kişisel Verilerin Korunmasına Yönelik Düzenlemelerin Tarihsel Gelişimi

1.3.1. Genel Olarak

Kişisel veriler hakkında bilgi sahibi olma, farklı gerekçelerle ve farklı bilgilere yönelik olarak eşler, akrabalar, arkadaşlar, komşular, hasımlar gibi diğer kişiler veya işverenler, cemaatler ya da dernekler gibi topluluklar için önemli olmuştur⁷⁸. Bu bilme isteğinin temelinde yatan neden insani bir duygu olan merak olabileceği gibi; işverenler açısından verimliliği arttırmak, ticari açıdan karlılığı yükseltmek, idari açıdan akılcı yönetimi ve güvenliği sağlamak gibi girişimler de olabilir⁷⁹. Fakat hangi nedene dayanırsa dayansın, insanın birey olarak kendine özgü kişiliğinin kabul edilmesiyle birlikte ona ait verilerin korunması düşüncesi de bazı alanlarda kendini göstermeye başlamıştır; örneğin günümüzden 2500 yıl öncesine uzanan sır saklama yükümlülüğü belirli bir meslek grubuna güven ilişkisine dayalı olarak özel yaşamını açan bireylerin bu alanlarının korunmasının bir gereği olarak ortaya çıkmıştır⁸⁰.

Dünyada özellikle, İkinci Dünya Savaşı sonrası oluşan atmosferde, kişiliğin devlet karşısında yüceltilmesi gereken bir değer olduğu bilincine varılmış ve bu bilinç, ulusal ve uluslararası alanda hukuksal düzenin inşasında önemli rol oynamıştır⁸¹. Yeni gelişen teknolojilerin, kişilik hakkının gerek devlet ve gerekse diğer kişiler tarafından ihlal edilmesini kolaylaştırması karşısında bireylerin bu ihlallerden korunması ihtiyacı da artmıştır. Böylece, kişilik hakkının bir parçası olan kişisel verilerin korunması hakkı da 1960'larda tartışılmaya ve 1970'lerde hukuksal metinlere konu olmaya başlar. Neticede, bir yanda devletin vatandaşlar; bireylerin ise birbirine karşı gözetim isteği, diğer yanda teknolojik ilerlemeler ile bu isteğin eski dönemlerde görülmeyen ölçüde kapsayıcı bir şekilde gerçekleşme olasılığı, bireysel özerkliğe ilişkin kaygıların gelişmesine neden olmuştur⁸². Fakat teknoloji ile kişilik hakkı karşı karşıya geldiğinde, hukuk kişiliği mutlak anlamda korunması gereken bir değer olarak öngörmeli ve kanunkoyucular kişisel alanın korunmasını sağlayacak önlemler almalıdır⁸³.

⁷⁸ Küzeci, 2010: 17.

⁷⁹ Küzeci, 2010: 17.

⁸⁰ Akgül, 2014: 165; Yılmaz, 2014: 24.

⁸¹ Başalp, 2004: 21.

⁸² Küzeci, 2010: 17.

⁸³ Başalp, 2004: 23.

1.3.2. Uluslararası Düzenlemelerde Kişisel Verilerin Korunması

1.3.2.1. Ekonomik İşbirliği ve Kalkınma Örgütü (OECD)

Kişisel verilerin korunmasına dair girişimde bulunan ilk organizasyon, Ekonomik İşbirliği ve Kalkınma Örgütü' dür⁸⁴. 1980 yılında "*Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Yönlendirici İlkeler*"⁸⁵ başlığı ile yayınlanan metnin, OECD'ye üye ülkeler bakımından herhangi bir bağlayıcılığı bulunmamakta olup ulusal düzeydeki veri koruma yasalarının birbiri ile uyumlulaştırılması amacını taşımaktadır⁸⁶. OECD'nin serbest piyasa ekonomilerinin gelişimine yönelik politika izleyen bir ticaret örgütü olması nedeni ile OECD İlkeleri, çatışan menfaatler olan veri koruması ile bilginin serbest dolaşımı arasında bir denge kurulmasını hedeflemektedir⁸⁷. Söz konusu ilkeler, yalnızca OECD'ye üye ülkeler tarafından değil, bütün ülkeler tarafından takip edilebilir niteliktedir⁸⁸.

Sekiz maddeden oluşan Rehber İlkeler⁸⁹, üye devletlerle kişisel verilerin korunması ve bireysel özgürlüklerle ilgili bu ilkeleri, iç hukuklarında yapacakları yasal düzenlemelerde dikkate almalarını, sınır aşan veri trafiğinin haksız yere engellenmemesini, mevcut engellerin kaldırılmasını, bu ilkelerin yaşama geçirilmesinde işbirliği yapılmasını tavsiye etmektedir⁹⁰. OECD'nin bu kılavuz ilkeleri esasen, getirdiği düzenlemelerin hayata geçirilmesi yolu ile üye devletlerde çoğulcu demokrasinin, insan haklarına riayet ve serbest piyasa ekonomisinin gerçekleşmesini amaçlamaktadır⁹¹. OECD'nin kişisel verilerin korunmasına ilişkin kılavuz

⁸⁴ Room, 2007: 10.

⁸⁵ Metnin orijinal hali için bk.

<http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprivacyandtransborderflowsofpersonaldata.htm> (erişim tarihi: 09.04.2017)

⁸⁶ Aksoy, 2010: 4.

⁸⁷ Aksoy, 2010: 5. OECD tarafından kişisel veri korumasına ilişkin olarak rehber ilkelerin kabul edilmesi, kişisel verilerin korunmasının ekonomik boyutunun öneminin bir göstergesidir. (Küzeci, 2010:119.)

⁸⁸ United Nations, 2016: 26.

⁸⁹ Bu sekiz ilke şu şekildedir:

1. Veri toplamanın sınırlı olması,
2. Veri kalitesi,
3. Amacın belirli olması,
4. Kullanımın sınırı olması,
5. Veri güvenliği,
6. Açıklık,
7. Bireyin katılımı,
8. Hesap verilebilirlik.

⁹⁰ Küzeci, 2010: 119.

⁹¹ Şimşek, 2008: 13.

ilklerinde öngörülen kuralların iç hukukta hayata geçirilmesi bakımından üye devletlerin uygun iç hukuk düzenlemelerini yapmak, bireyin haklarını kullanabileceği uygun araçları sağlamak, ilkelere uyulmadığı zaman başvurulabilecek etkili hukuki yolları ve yaptırımları öngörmek ve ilgililerin haksız suretle ayrımcılığa tabi tutulmasını önlemek konularında yükümlülükleri bulunmaktadır. OECD Rehber İlkeleri 2013 yılında revize edilerek yeniden yayınlanmıştır⁹².

OECD'ye üye olan 34 ülkeden 32'sinin ulusal veri koruma yasaları mevcut iken Türkiye'nin de 2016 yılında KVKK'nın yürürlüğe koyması ile birlikte mevcut durumda ulusal bir veri koruma mevzuatı bulunmayan tek üye ülke Amerika Birleşik Devletleri'dir⁹³.

1.3.2.2. Birleşmiş Milletler

Bilgisayar teknolojilerinin insan hakları boyutu üzerinde yoğunlaşan Birleşmiş Milletler Genel Kurulu, 14 Aralık 1990 tarihinde "Bilgisayarla İşlenen Kişisel Veri Dosyalarına İlişkin Yönlendirici İlkeler"^{94, 95} i kabul ederek üye devletlerin bu konuda asgari bir standartta buluşmasını hedeflemiştir⁹⁶. Gerek kamusal ve gerekse özel sektöre yönelik düzenlemeler içermekte olan bu metnin, tıpkı OECD Rehber İlkeleri gibi sadece tavsiye niteliğinde olması nedeni ile üye devletler açısından uluslararası hukuk bağlamında herhangi bir bağlayıcılığı yoktur. Bunun yanında, kişisel verilerin korunması için yetkili ve bağımsız

⁹² 11 Temmuz 2013 tarihli güncellenmiş metin için bk.

http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (erişim tarihi:16.01.2018).

⁹³ United Nations, 2016: 26.

⁹⁴ United Nations, *Guidelines Concerning Computerized Personal Data Files*, orijinal metin için bk.: <http://hrlibrary.umn.edu/instrree/q2grcpd.htm> (erişim tarihi:23.04.2017)

⁹⁵ "Birleşmiş Milletler Bilgisayarlarla İşlenen Kişisel Veri Dosyalarına İlişkin Yönlendirici İlkeler uyarınca ulusal hukuk sistemlerinde tanınması gereken güvenceler şu konulara ilişkindir;

-Yasal ve dürüst yollarla toplama ve işleme,

-Verilerin doğruluğu,

-Amacın belirliliği,

-İlgili kişinin erişimi,

-Ayrımcılık yapmama,

-Veri güvenliği,

-Denetim ve yaptırım,

-Verilerin sınır ötesi akışı" (Küzeci, 2010: 124).

⁹⁶ Başalp, 2004: 24-25; Aksoy, 2010: 6

verilerin korunması organlarının kurulmasını öngören ilk uluslararası hukuk belgesi olması nedeni ile önem taşımaktadır⁹⁷.

1.3.2.3. Avrupa Konseyi

1.3.2.3.1. Genel Olarak

Avrupa Konseyi, II. Dünya Savaşı'ndan hemen sonra Avrupa'nın demokratik temeller üzerinde yeniden inşası için harcanan yoğun çabanın sonucunda kalıcı barışın sağlanması, insan hakları ve hukuk devleti ilkelerini Avrupa'da sürekli olarak güvence altına almak için 1949 yılında kurulmuş uluslararası bir örgüttür⁹⁸. Avrupa Konseyi, insan hakları alanında en çok katkıda bulunmuş uluslararası kuruluşların başında gelmekte olup temel faaliyet alanları olan insan hakları ve temel özgürlüklerinin korunması bağlamında 4 Kasım 1950 tarihinde Avrupa İnsan Hakları Sözleşmesi'ni kabul etmiştir⁹⁹.

Kişisel verilerin korunmasının önemi ve gerekliliği de Avrupa Konseyi tarafından kısa sürede kavranarak bu bağlamda bulunulan ilk girişimler 1973¹⁰⁰ ve 1974¹⁰¹ yıllarında otomatik veri bankalarındaki kişisel verileri korumaya yönelik özel ve kamu sektörünü kapsayan iki kararın açıklanması ile meyvelerini vermiştir¹⁰². Her ne kadar bu tavsiye kararları ile ulusal hukuk sistemlerinde kişisel verilerin korunmasına yönelik düzenlemeler yapılması amaçlanmış olsa da, ülkelerin ulusal mevzuatında etkin bir koruma sağlanmasının ancak bağlayıcı uluslararası normlar ile mümkün olabileceği anlaşılmıştır¹⁰³. Bunun üzerine, uzun süren görüşme ve çalışmaların ardından 1981 yılında 108 sayılı "*Kişisel Verilerin Otomatik Olarak İşlenmesi Sırasında Bireylerin Korunmasına İlişkin Sözleşme*"¹⁰⁴ kabul edilmiştir.

⁹⁷ Şimşek, 2008: 16.

⁹⁸ Akgül, 2014:177.

⁹⁹ Şimşek, 2008: 19.

¹⁰⁰ *Özel Sektörde Elektronik Veri Bankaları Karşısında Bireylerin Özel Yaşamlarının Korunmasına İlişkin Karar*.

¹⁰¹ *Kamu Sektöründe Elektronik Veri Bankaları Karşısında Bireylerin Özel Yaşamlarının Korunmasına İlişkin Karar*.

¹⁰² Küzeci, 2010:126; Akgül, 2014:186.

¹⁰³ Küzeci, 2010:126.

¹⁰⁴ Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data; orijinal metin için bk. <http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37>, (erişim tarihi:23.04.2017). Türkçe metin için bk.

http://www.uhdigm.adalet.gov.tr/sozlesmeler/coktarafilsoz/ak/turkce/108_tur.pdf. (erişim tarihi:23.04.2017)

Bunun yanında, Avrupa Konseyi tarafından 4 Nisan 1997 tarihinde kabul edilen Biyotıp ve İnsan Hakları (Biyoetik) Sözleşmesi'nde¹⁰⁵ gen teknolojisi, embriyo üzerine araştırmalar, organ nakli gibi konularda genel kuralları düzenlenmekte olup sözleşmenin başlangıç bölümünde Evrensel İnsan Hakları Beyannamesi ile AİHS yanında Avrupa Konseyi Verilerin Korunması Sözleşmesi'ne de atıfta bulunulmuştur. Ancak bu sözleşmede kişisel verilerin korunmasına ilişkin hükümlerin yetersiz olduğu görülmektedir¹⁰⁶.

Avrupa Konseyi tarafından kabul edilen ve Verilerin Korunması Sözleşmesine atıfta bulunulan bir diğer metin de 23 Kasım 2001 tarihli ve 185 sayılı Avrupa Konseyi Siber Suç Sözleşmesi'dir¹⁰⁷. Bu sözleşmenin temel amacı, bilgisayar vasıtası ile işlenen suçlar karşısında toplumun korunması için ortak bir ceza hukuku politikasının izlenmesi, buna uygun yasal düzenlemelerin yapılması ve işbirliğinin gerçekleştirilmesi olup internet veya diğer bilgisayar ağlarıyla işlenen suçlarla mücadele için yapılan ilk sözleşme olma niteliğini taşımaktadır¹⁰⁸. Her ne kadar Siber Suç Sözleşmesi'nde siber suçlulukla mücadelede izlenecek yol olarak kişisel verilerin toplanması, işlenmesi ve uluslararası işbirliği içerisinde başka devletlerle paylaşılması öngörülmüş ise de bu metinde yer verilen, kişisel verilerin korunmasına yönelik önlemlerin oldukça zayıf olduğu görülmektedir¹⁰⁹.

Tüm bu düzenlemelerin yanında, Avrupa kamu düzeninin temeli olan AİHS de veri koruması hukuku bakımından oldukça önemli bir belge niteliği taşımaktadır. Her ne kadar kişisel verilerin korunması hususu sözleşme metninde ayrıca ve açıkça düzenlenmemiş olsa da, Avrupa Konseyi'nin kişisel verilerin korunması yaklaşımının değerlendirilmesinde sözleşmenin "özel ve aile yaşamına saygı hakkı" başlıklı 8. maddesini irdilemekte fayda bulunmaktadır.

¹⁰⁵ *Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine* (Sözleşmenin tam adı , Biyoloji ve Tıbbın Uygulanması Bakımından İnsan Haklarının ve Haysiyetinin Korunması Sözleşmesi: İnsan Hakları ve Biyotıp Sözleşmesi'dir.) Orijinal metin için bk.: <http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168007cf98> (erişim tarihi:23.04.2017)

¹⁰⁶ Tinnefeld ve diğerleri, 2005:104'ten aktaran: Şimşek, 2008: 19-20.

¹⁰⁷ *Convention on Cybercrime*, orijinal metin için bk. <http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561> (erişim tarihi:23.04.2017)

¹⁰⁸ Şimşek, 2008: 20.

¹⁰⁹ Tinnefeld ve diğerleri, 2005:105'ten aktaran: Küzeci, 2010: 128.

1.3.2.3.2. Avrupa İnsan Hakları Sözleşmesi

Avrupa Konseyi tarafından 4 Kasım 1950 tarihinde kabul edilen Avrupa İnsan Hakları Sözleşmesi, insan haklarının ve özgürlüklerinin korunması bakımından en temel uluslararası hukuk düzenlemelerinden biridir¹¹⁰. Bu sözleşmenin garanti ettiği hak ve özgürlüklerin korunması da yine sözleşme ile kurulan Avrupa İnsan Hakları Mahkemesi' ne yapılan bireysel başvuru ve devlet başvurusu yolları ile sağlanmaktadır¹¹¹.

Her ne kadar, kişisel verilerin korunması hakkı AİHS'de ayrıca ve açıkça düzenlenmemiş olsa da, AİHM' nin içtihatları ile 1980li yıllardan itibaren AİHS' nin koruma alanı içerisinde bulunduğunu kabul ettiği gözlenmektedir.¹¹² Nitekim sözleşmenin 8. maddesinde yer alan;

"1. Herkes özel ve aile yaşamına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahiptir.

2. Bu hakkın kullanılmasına bir kamu otoritesinin müdahalesi, ancak ulusal güvenlik, kamu emniyeti, ülkenin refahı, dirlik ve düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için demokratik bir toplumda gerekli olan ölçüde ve yasayla öngörülmüş olmak koşuluyla söz konusu olabilir."

düzenlemesi ile kişinin özel yaşamı, aile yaşamı, evi ve haberleşmesinin temel bir insan hakkı olduğu yönünde mutabakata varıldığı; AİHM' nin de bireysel özerkliği ve bilgilerin geleceğini belirleme hakkını 8. madde kapsamında değerlendirdiği görülmektedir^{113, 114}. Bunun yanında, kişisel verilerin hukuka aykırı olarak toplanması, kaydedilmesi, tekrar kullanılması ve devredilmesine karşı bireyin korunması hakkının *"özel yaşama saygı gösterilmesi hakkı"*nın özel olarak şekillendirilmiş kısmi bir alanını oluşturduğu savunulmaktadır¹¹⁵. Burada belirtmek gerekir ki, 8. madde kapsamındaki haklar bakımından taraf devletlere yalnızca keyfi müdahalede bulunmayı yasaklayan negatif bir yükümlüğe değil, bununla birlikte bu hakların kullanılmasına olanak verecek önlemlerin alınması konusunda pozitif bir yükümlülüğe de yer verilmektedir^{116, 117}.

¹¹⁰ Şimşek, 2008: 30; Küzeci, 2010: 135.

¹¹¹ Şimşek, 2008: 30.

¹¹² Küzeci, 2010: 136.

¹¹³ Küzeci, 2010: 136.

¹¹⁴ *Leander/İsveç*, Başvuru no:9248/81, 26.03.1987, parag. 48;

[https://hudoc.echr.coe.int/tur#{"fulltext":\["leander"\],"documentcollectionid2":\["GRANDCHAMBER","CHAMBER"\],"itemid":\["001-57519"\]}](https://hudoc.echr.coe.int/tur#{). (erişim tarihi:15.01.2018).

¹¹⁵ Şimşek, 2008: 31.

¹¹⁶ Atak, 2010: 102.

AİHM' nin kişisel verilerin korunmasına ilişkin verdiği ilk ve önemli kararlardan biri *Klass ve diğerlerinin* Almanya aleyhine yaptıkları başvuruya ilişkin 6 Eylül 1978 tarihli karardır¹¹⁸. Bu kararla AİHM, demokratik bir toplumda gizli gözetleme tedbirlerinin ancak olağanüstü bir durumda uygulanabileceğine, müdahalenin sınırlarının yasal bir düzenleme ile çizilmesinin gerekliliğine, elde edilen verilerin hukuki sınırlar içerisinde değerlendirilebileceğine ve bu verilerin suistimaline karşı etkili denetim mekanizmalarına ihtiyaç bulunduğuna vurgu yapmıştır¹¹⁹.

Leander'in İsveç aleyhine yaptığı başvuru sonucunda verilen 26 Mart 1987 tarihli kararda ise, devletin bireyin özel yaşamına ilişkin bilgileri yalnızca toplama amacı çerçevesinde değerlendirmesi zorunluluğu, bu durumun istinasının sözleşme'nin 8. maddesinin 2. fıkrası uyarınca "ulusal güvenlik" gibi yasal bir temele dayanması gerektiği tartışılmıştır¹²⁰.

Amann'ın İsviçre aleyhine yaptığı başvuru sonucunda verilen 16 Şubat 2000 tarihli kararda¹²¹, resmi makamlar tarafından kişisel verilerin kaydedilmesi ve muhafaza edilmesi tartışılmıştır¹²². Sovyetler Birliği elçiliğinde çalışan birinin ticaretle uğraşan başvurusu arayarak siparişte bulunması üzerine görüşmeyi dinleyen Federal Savcılık başvuru hakkında Sovyetler Birliği'nin 'bağlantı elemanı' olduğuna ilişkin bir fiş oluşturmuştur. Bu durumu öğrenen başvurunun tazminat talebinin yerel makamlarca reddedilmesi üzerine AİHM' nin önüne gelen uyuşmazlıkta kişisel verilerin saklanması kişinin özel yaşamını ilgilendirdiğine hükmeden Mahkeme, başvuru hakkında toplanan bilginin yasal bir temele

¹¹⁷ AİHM'e yapılan başvuruların sözleşme hükümlerini ihlal ettiği iddiası ile taraf devlete karşı yapılması ve bu anlamda devlet tarafından gerçekleştirilen eylem ve işlemlerin Sözleşme'nin 8. maddesi ile getirilen güvence kapsamında olduğu tartışmasız olsa da, Mahkemenin " (*Devletin*) buradaki yükümlülükleri, bireylerin arasındaki ilişki alanında da özel yaşama saygıyı koruyacak önlemlerin kabulünü de içermektedir. (X ve Y, Hollanda'ya karşı, b.n. 8978/80, k.t. 26.03.1985, parag.23)" hükmü karşısında özel kişi ve kurumlarca yapılan gizli dinlemeler gibi eylemleri önleyecek mekanizmalar tesis etmeyerek pozitif yükümlülüğünü ihmal etmiş devletin de doğrudan sorumlu tutulabileceği savunulmaktadır. (Küzeci, 2010:137-138)

¹¹⁸ *Klass ve diğerleri/Almanya*, başvuru no: 5029/71, 6.9.1978 -

[https://hudoc.echr.coe.int/tur#{"fulltext":\["klass"\],"documentcollectionid2":\["GRANDCHAMBER","CHAMBER"\],"itemid":\["001-57510"\]}](https://hudoc.echr.coe.int/tur#{) (erişim tarihi:15.01.2018)

¹¹⁹ Şimşek, 2008: 33.

¹²⁰ *Leander/ İsveç*, 9248/81, 26.3.1987.

¹²¹ *Amann/İsviçre*, Başvuru no: 27798/95, 16.2.2000 -

[http://hudoc.echr.coe.int/tur#{"fulltext":\["amann"\],"documentcollectionid2":\["GRANDCHAMBER","CHAMBER"\],"itemid":\["001-58497"\]}](http://hudoc.echr.coe.int/tur#{), (erişim tarihi: 07.05.2017)

¹²² Küzeci, 2010: 141.

dayanmasına karşın mevcut düzenlemenin savcılık makamının veri toplama, kaydetme ve muhafaza etme koşullarını belirlemediği ve hangi verilerin hangi usulle saklanacağı açısından açık olmadığı gerekçesi ile AİHS'nin 8. maddesinin ihlal edildiği kanaatine ulaşmıştır¹²³.

Bir ceza soruşturması kapsamında parmak izleri ve DNA örnekleri alınan *S. ve Marper*'in bu soruşturmalarda kovuşturmaya yer olmadığına karar verilmesi üzerine parmak izleri ve DNA örneklerinin imha edilmesi taleplerinin ulusal makamlarca reddedilmesi üzerine AİHM'ye yaptıkları başvuru sonucu verilen 4 Aralık 2008 tarihli kararda ise, DNA profillerinin, bireyler arasındaki genetik ilişkilerin tespit edilmesini sağlayacak bir araç olmaları, bunların muhafaza edilmesinin, bu bireylerin özel hayatına saldırı oluşturduğu sonucuna ulaşmak için yeterli olması; DNA profillerinin, etnik kökene ilişkin çıkarsamalar yapılmasına imkân vermeleri, bu durumun bunların muhafazasının hassasiyetle yapılmamasını özel hayata saldırı oluşturabilecek hale getirmesi; parmak izlerinin ise, objektif şekilde, ilgili bireye ilişkin bilgiler taşıdıkları ve birçok durumda, kesin olarak kimlik belirlemeye izin vermeleri nedeni ile haklı gerekçe olmaksızın muhafaza edilmelerinin özel yaşama saygı gösterilmesi hakkının ihlali olduğu sonucuna varılmıştır¹²⁴.

AİHM'nin kişisel verilere erişim hakkını tartıştığı karar ise 7 Temmuz 1989 tarihli *Gaskin/Birleşik Krallık* kararıdır¹²⁵. Bu kararda, kişinin kimliği, ailesi ve doğumu konusunda bilgi edinme hakkının onun kişiliğini serbestçe geliştirme hakkının kapsamında olduğu ve bu bilgilerin onun özel yaşamının bir parçası olduğu, bu nedenle devletlerin arşivlediği kişisel verilere ilgililerinin erişebilmesini sağlayacak usuller öngörmesi gerektiğinden bahisle başvurusunun resmi makamların elinde bulunan ailevi ilişkilerine ulaşmasının engellenmesinin sözleşmeye aykırı olduğuna hükmetmiştir¹²⁶.

Bayan Z.'nin Finlandiya aleyhine yaptığı başvuruyu inceleyen AİHM'ye göre, sosyal ve tıbbi verilerin korunması resmi makamlara ve sağlık hizmeti sunanlara güvenin korunması açısından oldukça önemlidir ve bu nedenle taraf devletler iç hukuklarında bu hassas verilerin

¹²³ Atak, 2010:108.

¹²⁴ *S. Ve Marper/Birleşik Krallık*, başvuru no:30562/04, 4.12.2008 -

[https://hudoc.echr.coe.int/tur#{"fulltext":\["marper"\],"documentcollectionid2":\["GRANDCHAMBER","CHAMBER"\],"itemid":\["001-90051"\]}](https://hudoc.echr.coe.int/tur#{) (erişim tarihi: 15.01.2018)

¹²⁵ *Gaskin/ Birleşik Krallık*, başvuru no: 10454/83, 7.7.1989 -

[http://hudoc.echr.coe.int/tur#{"fulltext":\["gaskin"\],"documentcollectionid2":\["GRANDCHAMBER","CHAMBER"\],"itemid":\["001-57491"\]}](http://hudoc.echr.coe.int/tur#{) (erişim tarihi: 07.05.2017)

¹²⁶ Akgül, 2014:181-182.

kötüye kullanımının önlenmesi için gerekli ve etkin düzenlemeler geliştirmeli, sosyal ve tıbbi verilerin ilgisinin rızası olmadan açıklanmasını sıkı koşullara bağlamalıdır¹²⁷.

Sonuç olarak, AİHS'nin kabul edildiği tarih itibariyle henüz tartışılmaya başlanmamış olan kişisel verilerin korunması hakkına sözleşmede açıkça yer verilmemiş olmasına rağmen AİHM somut olaylar bağlamında bu hakkın içeriğini geliştirdiği içtihatlar ile bireyin özel yaşamına saygı gösterilmesi hakkı çerçevesinde yorumlamakta ve taraf devletlere yol gösterici olmaktadır.

1.3.2.3.3. 108 Sayılı Avrupa Konseyi Sözleşmesi

Avrupa Konseyi, hızla gelişen teknolojinin bireyin kişisel verilerinin korunmasına dair duyulan ihtiyacı arttırması ve bu ihtiyacın AİHS'nin özel yaşamın gizliliği hakkının korunmasına yönelik geleneksel kuralları ile giderilmesinin zorlaşması üzerine Avrupa Konseyi nezdinde, sınır aşan veri trafiğini de kapsar biçimde kişisel verilerin korunmasına yönelik bir sözleşme hazırlanması amacı ile 1976 yılında bir Uzmanlar Komitesi görevlendirilmiştir¹²⁸. Bu çalışmanın temelinde, veri koruması hukukunun iki temel amacı olan özel hayatın gizliliğinin korunması ve sınır aşan veri trafiğinin sürdürülebilirliği için yeknesak ve bağlayıcı bir düzenlemenin gerekli olduğu konusunda Avrupa Devletleri'nin görüş birliğine varmış olması yatmaktadır. Zira özel hayatın gizliliğine ilişkin yüksek seviyede tedbirler alan bir ülkeden bu konuda koruma düzeyini daha düşük öngören bir ülkeye veri akışı engellenmekte, başka bir deyişle ülkelerin kişisel verilerin korunmasına ilişkin ulusal hukuk mevzuatlarındaki farklılık, verilerin serbest dolaşımını sekteye uğratmaktadır¹²⁹.

Uzmanlar Komitesi tarafından üç yıllık bir çalışmanın ardından hazırlanan tasarı metni, Bakanlar Komitesi tarafından kabul edilmiş ve kişisel verilerin korunması hukukunda uluslararası bağlayıcı ilk hukuk belgesi özelliğini taşıyan *"Kişisel Verilerin Otomatik İşleme Tabi Tutulması Sırasında İnsanın Korunmasına İlişkin Sözleşme"*¹³⁰ 28 Ocak 1981 tarihinde kabul edilerek imzaya açılmıştır. Sözleşme, 5 Konsey üyesi İsveç, Norveç, Fransa, Almanya ve İspanya'nın onaylaması sonucunda 1 Ekim 1985 tarihinde yürürlüğe girmiştir¹³¹. 108 Sayılı Avrupa Konseyi Sözleşmesi, Türkiye tarafından da aynı tarihte imzalanmış; fakat onaylanması 2 Mayıs 2016 tarihinde, yürürlüğe konulması ise 1 Eylül 2016 tarihinde mümkün

¹²⁷ Şimşek, 2008: 37.

¹²⁸ Akgül, 2014: 187.

¹²⁹ Room, 2007: 4.

¹³⁰ Bundan böyle 108 Sayılı Sözleşme olarak anılacaktır.

¹³¹ Akgül, 2014: 187.

olabilmiştir¹³². Avrupa Konseyi tarafından sözleşmenin geniş bir etki alanına sahip olması amaçlandığından, sözleşmenin 23. maddesi ile Avrupa Konseyi üyesi olmayan ülkelerin de katılımı mümkün kılınmıştır¹³³.

108 sayılı Sözleşme'nin 4. maddesi uyarınca, taraf devletlerin sözleşme metninde yer alan, verilerin korunmasına ilişkin ilkelere işlerlik kazandıracak önlemleri alma, başka bir deyişle bu ilkeleri sözleşmeyi onaylamadan önce yapacakları yasal düzenlemeler ile iç hukuk düzenlerinin bir parçası haline getirme zorunluluğu bulunmaktadır¹³⁴. Bunun yanında sözleşme, veri korumasına ilişkin asgari zorunlulukları vurgulamakta, Sözleşmenin 11. Maddesi ile âkit devletlere sözleşmenin öngördüğü korumadan daha geniş koruma sağlamalarına cevaz vermektedir.

108 Sayılı Sözleşme'nin kabulü aşamasında, özellikle özel sektörde kişisel verilerin bilgisayar ortamında işlenmesi durumunda Avrupa İnsan Hakları Sözleşmesi'nin yeterli güvence sağlayıp sağlamayacağı hususu tartışılmış, 108 sayılı Sözleşme ile bu boşluğun doldurulması hedeflenmiştir¹³⁵. Bunun yanında, kamu sektöründe işlenen kişisel veriler de sözleşme kapsamına dahil edilmiştir¹³⁶. Yine, sözleşmenin koruma alanı yalnızca otomatik işlenen verilerle sınırlandırılmış; ancak işleme sürecinin tamamının otomatik olması aranmamış, kısmen otomatik işlenen veriler de güvencenin kapsamına dahil edilmiştir¹³⁷.

108 sayılı Sözleşme'nin 5. maddesi ile *otomatik işleme tabi tutulabilecek verilerin niteliği* düzenlenmiştir. Buna göre veriler; meşru ve yasal yollardan elde edilmeli ve işlenmeli, belirli ve meşru amaçlar için kaydedilmeli ve bu amaca aykırı şekilde kullanılmamalı, uğruna kaydedildikleri amacı gerçekleştirmeye elverişli olmalı ve yalnızca gerektiği kadar kaydedilmeli, doğru ve gerektiğinde güncel olmalı, ilgili kişinin kimliğine ulaşılacak biçimde ve kaydedilme amacı yönünden gerekli süreden fazla saklanmamalıdır.

108 sayılı Sözleşme'nin 6. maddesi ile kişilerin etnik kökenleri, politik düşünceleri, dini ve diğer inançları, sağlık ve cinsel yaşamla ilgili kişisel nitelikteki veriler ile ceza mahkumiyetleri *özellikli veri kategorileri; başka bir deyişle hassas veriler* olarak

¹³² Sözleşmenin 15.01.2018 tarihi itibarıyla güncel imza ve onay durumu için bk.

https://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/treaty/108/signatures?p_auth=cOAvxJNk (erişim tarihi:15.01.2018)

¹³³ United Nations, 2016: 25; Şimşek, 2008: 22.

¹³⁴ Küzeci, 2010: 132.

¹³⁵ Küzeci, 2010: 131.

¹³⁶ bk. 108 sayılı Verilen Korunması Sözleşmesi, madde 3.

¹³⁷ Küzeci, 2010: 131.

düzenlenmiştir ve bu veriler iç hukukta uygun güvence sağlanmadıkça otomatik işleme tabi tutulamazlar¹³⁸.

108 sayılı Sözleşme'nin 7. maddesi ile taraf devletlere otomatik olarak işlenen verilerin kazaen veya izinsiz olarak yok edilmesi, elde edilmesi, değiştirilmesi, izinsiz olarak dağıtılmasına karşı uygun güvenlik önlemleri alınması zorunluluğu yüklenmiştir.

108 sayılı Sözleşmenin 8. maddesinde ise ilgili kişi hakkındaki ek güvenceler belirlenmiş olup bu güvenceler; ilgili kişinin kendisine ilişkin otomatik olarak işlenen veri bulunup bulunmadığını, işleme amaçlarını, veri yöneticisinin bilgilerini öğrenme, işlenen verilerin kendisine bildirilmesini sağlama, gerektiği takdirde işleme tabi tutulan verileri düzelttirme ve hukuka aykırı olarak işlenmesi halinde bu verileri sildirme, bu talepleri yerine getirilmediği takdirde yasal yollara başvurma biçiminde açıklanmıştır.

108 sayılı Sözleşme'nin verilerin niteliğine ilişkin 5. maddesi, özel veri kategorilerini ve bunların işlenme koşullarını düzenleyen 6. maddesi ile verinin ilgisine tanınan ek güvence ve hakları düzenleyen 8. maddesine ancak devlet güvenliğinin korunması, kamu güvenliği, devletin mali menfaatleri ve suçların önlenmesi ile ilgili kişinin korunması ve başkasının hak ve özgürlüklerinin korunması için zorunluluk bulunması durumunda ve ancak demokratik bir toplum açısından buna zorunluluk duyuluyor ise istisna getirilebilir¹³⁹.

Taraf devletler özel yaşamın korunması gerekçesi ile birbirleri arasındaki kişisel nitelikteki verilerin sınır ötesi akışını yasaklayamazlar veya veri aktarımını özel bir izne tabi tutamazlar. Bu durumun istinası, 6. maddede düzenlenen veri kategorileri açısından aktarımın yapılacağı taraf devlette eşdeğer korumanın bulunmaması durumu ile aktarımın sözleşmeye taraf olmayan bir devlet aracılığıyla yapılacak olması durumudur¹⁴⁰.

108 sayılı Avrupa Konseyi Veri Koruma Sözleşmesi ile,

*Sözleşmenin uygulanmasını kolaylaştırmak, geliştirmek ve bu amaçla önerilerde bulunmak,

*Sözleşmede değişiklik önerisinde bulunmak,

*Değişiklik önerileri hakkında görüş bildirmek,

*Sözleşmenin uygulanması ile ilgili sorular hakkında görüş bildirmek,

¹³⁸ Küzeci, 2010: 132.

¹³⁹ 108 sayılı Sözleşme, madde 9.

¹⁴⁰ Küzeci, 2010: 133.

konularında yetkili bir Danışma Komitesi kurulmuştur¹⁴¹. Bunun yanında, sözleşmenin asıl metninde veri işleme faaliyetlerini kontrol edilecek bağımsız bir organ öngörülmemiş olup sözleşmeye yapılan ek protokol ile bağımsız kontrol organları oluşturulmuştur¹⁴².

Sözleşmede, kişisel verilerin korunmasına ilişkin çerçeve niteliğinde olan asgari standartlar belirtilmiş, Avrupa Konseyi bu standartları geliştirmek amacı ile çeşitli alanlara yönelik olarak tavsiye kararları almıştır¹⁴³.

Sonuç olarak; 108 sayılı Sözleşme, gerek konsey üyesi devletlere ve gerekse konsey üyesi olmayı sözleşmenin tarafı olan ülkelere kişisel verilerin korunması konusunda temel ilkeleri belirlemiş olup 18 Şubat 2016 tarihli Resmi Gazete’de Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun’un yayımlanması sonucunda son olarak Türkiye'nin de sözleşmeyi yürürlüğe koyması ile birlikte Avrupa Konseyi'ne üye devletlerin tamamı tarafından sözleşme imzalanmış, onaylanmış ve yürürlüğe konulmuş bulunmaktadır¹⁴⁴.

¹⁴¹ 108 Sayılı Sözleşme, madde 18-19.

¹⁴² Şimşek, 2008: 27.

¹⁴³ Tavsiye kararlarından örnekler:

- Bilimsel Araştırma ve İstatistiki Amaçlar İçin Kişisel Verilerin Korunmasına İlişkin Tavsiye <https://rm.coe.int/16804bc647>, (erişim tarihi: 28.05.2017)
- Doğrudan Reklam Amacıyla Kullanım Sırasında Kişisel Verilerin Korunması Hakkında Tavsiye <https://rm.coe.int/16804bd336>, (erişim tarihi:28.05.2017)
- Sosyal Güvenlik Amacıyla Kullanım Sırasında Kişisel Verilerin Korunması Hakkında Tavsiye <https://rm.coe.int/16804dd352>, (erişim tarihi:28.05.2017)
- Polisiye Faaliyetler Alanında Kişisel Verilerin Korunması Hakkında Tavsiye <https://rm.coe.int/16804e7a3c>, (erişim tarihi:28.05.2017)
- İş İlişkisi Amacıyla Kullanılan Kişisel Verilerin Korunması Hakkında Tavsiye <https://rm.coe.int/1680500b15>, (erişim tarihi: 28.05.2017)
- Ödeme İlişkisi ve Bununla Bağlantılı İşlemler İçin Kullanılan Kişisel Verilerin Korunmasına İlişkin Tavsiye <https://rm.coe.int/16804e15cd>, (erişim tarihi:28.05.2017)
- Tıbbi Verilerin Korunması Hakkında Tavsiye <https://rm.coe.int/16804f0ed0>, (erişim tarihi: 28.05.2017),
- İstatistiki Amaçlar İçin Toplanan Kişisel Verilerin Korunması Hakkında Tavsiye <https://rm.coe.int/1680508d7e>, (erişim tarihi: 28.05.2017)
- Sigorta Amacıyla Toplanan ve İşlenen Kişisel Verilerin İşlenmesi Hakkında Tavsiye <https://rm.coe.int/16804d9ddd>, (erişim tarihi: 28.05.2017).

¹⁴⁴ Şimşek, 2008: 28; Konsey üyesi ülkelerin sözleşmeyi imzaladıkları ve yürürlüğe koydukları tarihler için bk. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=MIAxQjzm (erişim tarihi:30.11.2017)

1.3.2.4. Avrupa Birliği

1.3.2.4.1. Genel Olarak

II. Dünya Savaşı'nın en önemli sonuçlarından biri, Avrupa'nın bütünleşme sürecini hızlandırmış olmasıdır. Tarihin en büyük ve kanlı savaşlarından biri olan bu savaşın yıkıntılarını gidermek ve öteden beri birbirleri ile mücadele halinde olan Avrupa devletlerinin kalıcı bir barış içerisinde yaşama arzusunun sonucu olarak 1951 yılında Avrupa Kömür ve Çelik Topluluğu, 1957 yılında da Avrupa Ekonomik Topluluğu ile Avrupa Atom Enerjisi Topluluğu kurulmuştur¹⁴⁵.

1965 yılında imzalanan Füzyon Anlaşması ile bu üç topluluk tek bir komisyon ve konsey kurulması sonucunda Avrupa Toplulukları olarak anılmaya başlamış; Avrupa Birliği Antlaşması olarak da bilinen 1992 tarihli Maastricht Antlaşması ile öngörülen üç sütunlu yapının da ilk sütununu oluşturmuştur¹⁴⁶. Maastricht Antlaşması ile kararlaştırılan Avrupa Birliği yapısının diğer iki sütunu ise ortak dışışleri güvenlik politikası ile adalet ve içişleri konularında üye devletler arasında işbirliğinin sağlanmasından ibarettir¹⁴⁷.

Avrupa Birliği'nin temel amaçlarını gerçekleştirebilmesi için kişilerin, hizmetlerin, malların ve sermayenin serbest dolaşımının sağlanması gerekmekte olup kişisel verilerin işlenmesi de bu noktada bir zorunluluk olarak ortaya çıkmaktadır¹⁴⁸. Bu nedenle, birliğe üye devletlerin kişisel verileri koruma düzeylerinin uyumlulaştırılması ile sorunsuz bir şekilde işlev görmesi istenmiştir¹⁴⁹. Her ne kadar Avrupa Birliği'ne üye olan bütün devletler Avrupa Konseyi'nin bir üyesi olarak 108 Sayılı Avrupa Konseyi Sözleşmesi'ni onaylamış olsalar da, sözleşmeye rağmen ülkelerin iç hukuklarındaki veri korumasına ilişkin farklılıklar devam etmiş ve verilerin korunmasına ilişkin etkili bir koruma sağlanamamıştır¹⁵⁰.

Avrupa'nın kişisel verilerin korunmasına verdiği önemin temelinde Almanya'da kişisel verilerin kötüye kullanılması sonucunda milyonlarca Yahudi'nin toplama kamplarına gönderilmesinin yattığı öne sürülse de, esasen bu koruma Avrupa'daki özel hayatın gizliliği konusundaki geçmişe dayanan bir gelenekten kaynaklanmaktadır. Zira birlik üyesi devletlerin çoğunun anayasasında özel hayatın gizliliğinin korunması hakkına yer verildiği görülmektedir¹⁵¹. Bunun yanında, kişisel verilerin korunması ülküsünün anavatanı olarak

¹⁴⁵ Akgül, 2014: 195-196.

¹⁴⁶ <http://www.ab.gov.tr/105.html> , (erişim tarihi:04.06.2017).

¹⁴⁷ Akgül, 2014: 196.

¹⁴⁸ Akgül, 2014: 197.

¹⁴⁹ Şimşek, 2008: 39.

¹⁵⁰ Akgül, 2014: 211.

¹⁵¹ Akgül, 2014: 199.

nitelendirilebilecek Avrupa'da, gerek Avrupa Birliği, gerekse ülkelerin ulusal hukuk sistemlerinde buna ilişkin oldukça açık ve gelişmiş bir mevzuat bulunmaktadır¹⁵².

Avrupa Birliği'nde kişisel verilerin korunmasına ilişkin düzenlemeler, birlik içerisinde ortak pazarın gereklerini dikkate almak ve serbest veri trafiğini temel haklara zarar vermeden genişletmek amacı ile yürürlüğe konmuştur¹⁵³. Bunun yanında, üye ülkelerin bu konudaki uygulamalarının yeknesak hale getirilmesi amaçlanmıştır. Bu amaç doğrultusunda, Avrupa Birliği Komisyonu tarafından 1990 yılında verilerin korunmasına ilişkin ilk taslak hazırlanmış, bu taslak 24 Ekim 1995 tarihinde kabul edilerek "*Kişisel Verilerin İşlenmesinde Gerçek Kişilerin Korunması Yönergesi (95/46/AT Sayılı Yönerge)*" yürürlüğe konmuştur¹⁵⁴.

İlerleyen yıllarda, özellikle telekomünikasyon sektörünün kendine özgü yapısı nedeni ile tamamlayıcı bir düzenleme olarak 1997 yılında 97/66/AT sayılı "Telekomünikasyon Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Yönergesi"¹⁵⁵ kabul edilmiştir; ancak bu yönerge 2002 yılında 2002/58/AT sayılı "Elektronik İletişim Alanında Özel Yaşamın Gizliliğinin Korunması ve Kişisel Verilerin İşlenmesine İlişkin Yönerge"¹⁵⁶ nin kabul edilmesi ile yürürlükten kalkmıştır¹⁵⁷.

Tüm bu düzenlemelere ilaveten 2000 yılında, kişisel verilerin korunması hakkına, bireyin özel hayatı yanında ilk kez temel ve ayrı bir hak alanı olarak Avrupa Birliği Temel Haklar Şartı'nın 8. maddesinde¹⁵⁸ yer verilmiştir¹⁵⁹.

¹⁵² Küzeci, 2010: 154.

¹⁵³ Başalp, 2004: 25.

¹⁵⁴ Başalp, 2004: 26.

¹⁵⁵ *Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector* , <http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1496587871952&uri=CELEX:31997L0066> , (erişim tarihi:04.06.2017)

¹⁵⁶ *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector* , <http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1496588313140&uri=CELEX:32002L0058> , (erişim tarihi: 04.06.2017)

¹⁵⁷ Küzeci, 2010: 187-188.

¹⁵⁸ *Madde 8*

Kişisel verilerin korunması

1. Herkes, kendisini ilgilendiren kişisel verilerin korunması hakkına sahiptir.

2. Bu veriler, adil bir şekilde, belirli amaçlar için ve ilgili kişinin rızasına veya yasa ile öngörülmüş diğer meşru bir temele dayanarak tutulur. Herkes, kendisi hakkında toplanmış verilere erişme ve bunları düzelttirme hakkına sahiptir.

1.3.2.4.2. 95/46/AT Sayılı Kişisel Verilerin Korunması Yönergesi (Direktifi)

24 Ekim 1995 tarihinde kabul edilen "*Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımında Bireylerin Korunmasına İlişkin 95/46/AT sayılı Avrupa Parlamentosu ve Konseyi Yönergesi*"¹⁶⁰, Avrupa Birliği'nin kişisel verilerin korunmasına ilişkin en önemli hukuksal metinlerinden biri olup bütün üye devletlerde geçerli olacak asgari veri koruma ölçütlerini belirlemiştir¹⁶¹.

95/46/AT sayılı Yönerge'nin yürürlüğe konduğu tarihte Avrupa Birliği üyesi devletlerin pek çoğunda kişisel verilerin korunması hususu ulusal yasalar ile düzenlemiş bulunmaktadır; ancak bu düzenlemeler arasında ciddi farklılıkların bulunduğu göze çarpmaktadır. Örneğin, Almanya, Fransa ve İskandinav ülkelerinin yasalarında kişisel verilerin korunması hakkı bir insan hakkı olarak kabul edilirken, Birleşik Krallık'ta buna ilişkin düzenlemenin uluslararası ticareti korumayı hedeflediği görülmektedir¹⁶². Farklı devletlerin kişisel verilerin ve buna bağlı olarak bireylerin temel hak ve özgürlüklerinin korunmasına ilişkin benimsedikleri düzenlemelerin farklılığı ülkeler arasındaki veri akışını sekteye uğrattığından, rekabetin sağlıklı yürümesine engel olmakta, bireylerin kişisel verilerine ilişkin hakları ile bunların aktarıldıkları ülkedeki akıbetini takip edememeleri ve hak ihlali meydana gelmesi durumunda bunlara ilişkin etkili bir başvuru yolu kullanamadıklarından hak kayıplarına yol açmakta idi¹⁶³.

İşte bu olumsuzlukların önüne geçilebilmesi adına Avrupa Birliği üyesi ülkeler tarafından açık ve kalıcı bir düzenleme ortaya konmuş ve 95/46/AT sayılı Yönerge kabul edilmiştir¹⁶⁴. 95/46/AT Sayılı Yönerge ile hem "ortak pazar" politikasının hayata geçirilmesi için gerekli olan verilerin serbest dolaşımının sağlanması hem de bu sırada kişilerin temel hak ve özgürlüklerinin korunması amaçlanmıştır¹⁶⁵. Metnin çerçeve bir belge niteliğinde hazırlanmış olması karşısında, üye ülkeler tarafından iç hukuklarında yapılacak

3. Bu kurallara uyulması, bağımsız bir makam tarafından denetlenir.

¹⁵⁹ Başalp, 2004: 27.

¹⁶⁰ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, <http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1496574544000&uri=CELEX:31995L0046> (erişim tarihi: 04.06.2017).

¹⁶¹ Küzeci, 2010: 165; Wong, 2013: 3.

¹⁶² Küzeci, 2010: 164; Uncular, 2014: 39.

¹⁶³ Mendos Kuşkonmaz, 2013: 71.

¹⁶⁴ Yüksel Civelek, 2011: 72; Aydın, 2015: 44.

¹⁶⁵ Bk. 95/46/AT Sayılı Yönerge madde 1 ve 2. Ayrıca bk. Uncular, 2014: 39; Akgül, 2014: 212; Özdemir, 2009: 29.

düzenlemelerde uyulması gereken asgari standartlar belirlenmiş olup ülkelerin bunların üzerinde bir koruma düzeyi öngörmeleri mümkündür¹⁶⁶.

95/46/AT Sayılı Yönerge'ye göre;

-*Kişisel veri*; başta bir kimlik numarası ile ilişkilendirilmek veya fiziksel, psikolojik, ekonomik, kültürel kimliği yansıtan bir içerik taşımak sureti ile bir kişiyi belirli ya da belirlenebilir kılan gerçek kişiye ilişkin herhangi bir bilgiyi; örneğin isim, pasaport numarası, sosyal güvenlik numarası, telefon numarası, motorlu taşıt plakası, fotoğraf, ses, özgeçmiş, parmak izi, genetik bilgileri¹⁶⁷,

-*İşleme*; kişisel verilerin toplanması, elde edilmesi, kaydedilmesi, saklanması, organize edilmesi, değiştirilmesi, kullanılması, başkalarına transfer edilmesi, yayılması, kombinasyonu veya ilişkilendirilmesi, bloke edilmesi, silinmesi, yok edilmesi gibi kişisel verilerle bağlantılı her türlü süreci¹⁶⁸,

-*Verilerin otomatik olarak işlenmesi*; otomasyon sistemlerinin (bilgisayar, vs.) kullanıldığı yöntemler ile işlenmesini,

-*Verilerin otomatik olmayan araçlarla işlenmesi*, otomasyon sistemleri kullanılmadan fakat örneğin alfabetik ya da kronolojik olarak erişimin organize edilmesi sureti ile işlenmesini¹⁶⁹ ifade eder.

95/46/AT sayılı Yönerge, bir dosyalama sisteminin parçası olmak kaydı ile kişisel verilerin otomatik araçlar dışında işlenmesi ile kısmen ya da tamamen otomatik araçlarla işlenmesi halinde uygulama alanı bulmaktadır. Bununla beraber, ceza hukuku alanındaki devlet faaliyetleri, kamu güvenliği, ülke savunması, devlet güvenliği ve AB Antlaşması'nın V. ve VI. başlıklarıyla belirtilenler gibi Topluluk hukukunun uygulama alanı haricindeki faaliyetler ile gerçek kişiler tarafından tamamen kişisel veya ev içi faaliyetler esnasında işlenen kişisel veriler; 95/46/AT Sayılı Yönerge 'nin kapsamı dışında bırakılmıştır¹⁷⁰.

Avrupa Birliği Adalet Divanı, 6 Kasım 2003 tarihinde verdiği *Bodil Lindqvist* kararında, 95/46/AT sayılı Yönerge'nin kapsamını tartışmıştır¹⁷¹. Karara konu olan olay, İsveç'te kilise öğretmeni ve temizlik görevlisi olan Lindqvist'in şahsi bilgisayarında oluşturduğu internet sayfalarında kiliseye kabul töreni hazırlığı yapmakta olan cemiyet

¹⁶⁶ Mendos Kuşkonmaz, 2013: 72; Uncular, 2012: 39.

¹⁶⁷ Başalp, 2004: 33-34.

¹⁶⁸ Başalp, 2004: 33; Akdağ, 2013: 71.

¹⁶⁹ Başalp, 2004: 33.

¹⁷⁰ Bk. 95/46/AT Sayılı Yönerge madde 3/2.

¹⁷¹ Kararın orijinal metni için bk. <http://curia.europa.eu/juris/document/document.jsf?docid=48382&doclang=en> (erişim tarihi:21.01.2018).

üyelerine yönelik olarak kilisedeki 18 meslektaşı ile ilgili onların rızalarını almaksızın onların işlerini, hobilerini, ailevi durumlarını ve telefon numaralarını içerir bilgilerin yanında bir meslektaşının ayağını incittiğini ve bu nedenle yarı zamanlı olarak çalıştığı bilgisine de yer vermesi üzerine Lindqvist hakkında açılan davada mahkemenin 95/46/AT sayılı Yönerge'nin yorumu ile ilgili bilgi almak üzere ABAD'ın birtakım konularda ön karar vermesini istemesi biçiminde gerçekleşmiştir¹⁷². Bunun üzerine ABAD, kişilerin mesleklerini, hobilerini, ailevi durumlarını ve telefon numaralarını içerir bilgilerin kişisel veri olduğuna, bu verilerin internet sayfasına yüklenmesinin veri işleme faaliyeti olarak kabul edilebileceğine ve faaliyetin otomatik yollarla gerçekleştirilmiş olduğuna, 95/46/AT sayılı Yönerge'nin kapsam bakımından istisnasını oluşturan 2. maddesinde yer verilen, kişisel verinin tamamen kişisel veya ev içi faaliyeti esnasında işlenmesi durumunun özel ve aile hayatı sırasında yürütülen faaliyetlerde uygulanabileceği, bu nedenle belirsiz sayıda kişi tarafından erişilebilme imkanı veren internette yayınlanma sureti ile gerçekleştirilen işlemenin bu istisna kapsamında değerlendirilemeyeceğine, bir kişinin ayağını inciterek tıbbi nedenlerle yarı zamanlı çalışmasına ilişkin bilginin kişinin sağlığına ilişkin hassas kişisel veri niteliğinde olduğuna, kişisel bilgilerin internet sayfasına yüklenmesi ile birlikte bu verilerin üçüncü bir ülkede yer alan kişiler tarafından da erişilebilir olması durumunun veri transferi olarak değerlendirilemeyeceğine karar vermiştir.

95/46/AT sayılı Yönerge, verileri işlenen kişilerin bilgi edinme hakkı olarak da adlandırılabilir erişim hakkı, verilerin düzeltilmesini, silinmesini ve bloke edilmesini isteme hakkı ile itiraz hakkı gibi birtakım haklar bahsetmektedir. Erişim hakkı, veri öznesinin kişisel verilerin serbestçe ulaşabilmesi anlamına gelmekte olup verilerin hangi amaçlar için işlendiği, bu amaca ulaşabilmek için ne gibi işlemlerin yapıldığını, kişinin verisi işlenmiyor olsa bile bu durumun bildirilmesini kapsamaktadır ve bu hakka dayanarak veri öznesinin bu bilgileri muhtelif aralıklarla tekraren öğrenebilme imkanı bulunmaktadır¹⁷³. Verilerin düzeltilmesi, silinmesi ve bloke edilmesini isteme hakkı, kişisel verilerin 95/46/AT sayılı Yönerge uyarınca veri işleme ilkelerine uygun işlenmemesi halinde söz konusu olacaktır. İtiraz hakkının ise üye devletlerce asgari düzeyde tanınması zorunlu olup kamusal görevlerin ifası veya haklı çıkarların korunması için veri öznesinin veri işleme faaliyetine itiraz etmesi mümkündür¹⁷⁴.

¹⁷² Bodil Lindqvist kararı, parg. 12-14.

¹⁷³ Başalp, 2004: 48-49.

¹⁷⁴ Başalp, 2004: 50.

95/46/AT sayılı Yönerge’de kişisel verilerin üçüncü ülkelere aktarımı hususu ayrıntılı olarak düzenlenmiştir. Gelişen teknolojinin veri transferini oldukça kolaylaştırmış olması nedeni ile verilerin bir kez transfer edildiğinde akıbetinin belirsizleşeceği yönünde endişelerin artması sonucunda kişisel verilerin uluslararası boyutlarda korunması önem kazanmış görünmektedir¹⁷⁵. Kişisel verilerin, Avrupa Birliği dışındaki ülkelere aktarılabilmesi, aktarım yapılacak ülkenin veri koruma mevzuatının 95/46/AT sayılı Yönerge’nin temel prensipleri ile uyumlu olması şartına bağlanmıştır¹⁷⁶. Mevzuatın uyumlu olması, kişisel verilerin işlenmesi nedeni ile kişilerin temel hak ve özgürlüklerinin korunması düzeyinin denkliğini ifade etmekte olup aktarılabilecek verinin niteliği, ilgililerin kimliğinin belirlenebilirliği, amaca bağlılık, ilgililerin erişim hakkının bulunup bulunmadığı, kişisel verilerin işlenmesi faaliyetinin hukuka uygunluğunu denetleyen makamların bulunup bulunmadığı ve bunların etkinliği, hukuka aykırı işleme faaliyetleri bakımından öngörülen yaptırımlar gibi kriterlerin değerlendirilmesi sonucunda belirlenmektedir¹⁷⁷.

1.3.2.4.3. 2016/679 Sayılı Genel Veri Koruma Tüzüğü (General Data Protection Regulation-GDPR)

95/46/AT sayılı Yönerge, kişisel verilerin korunmasına dair birçok ülke tarafından kabul edilen ve uygun görülen bir çerçeve niteliği taşımaktadır. Ancak bu Yönerge'nin yürürlüğe girdiği tarihten bu yana geçen sürede teknolojiye gelişmeler, bilhassa bulut bilişim, sosyal ağlar, konum bazlı hizmetler, elektronik ticaret ve globalleşme kişisel verilerin işlenmesi yöntemlerini oldukça değiştirmiş ve bu durumun yarattığı güvenlik açıkları ile bireysel mahremiyetin kolaylıkla ihlal edilebilirliğine ilişkin tehditler, kişisel verilerin korunmasına ilişkin ihtiyacın kapsamını genişletmiştir¹⁷⁸. Bu kapsam değişikliğinin, 95/46/AT sayılı Yönerge'yi kabul eden ülkeler arasında zaman içerisinde farklı ve birbiri ile uyumsuz pratikler ile bir araya gelmesi sonucunda, kişisel verilerin korunması alanında reforma ihtiyaç duyulmuştur¹⁷⁹. Zira tıpkı 108 sayılı Sözleşme gibi 95/46/AT sayılı Yönerge

¹⁷⁵ Mendos Kuşkonmaz, 2013: 78.

¹⁷⁶ Başalp, 2004: 68.

¹⁷⁷ Başalp, 2004: 68-69.

¹⁷⁸ Akıncı, 2017: 4.

¹⁷⁹ Diaz, 2016: 208. 95/46/AT sayılı Yönerge'nin başlıca amacının, AB üyesi devletler arasında veri koruma hukukunun yeknesak bir bünyeye kavuşması olsa da zaman içerisinde üye devletlerinin iç hukuklarındaki veri koruma uygulamalarında ortaya çıkan farklılığa; üye ülkelerde birden fazla soruşturmaya tabi tutulan Google firmasının Street View uygulaması ile ilgili olarak bu soruşturmalarda ülkelerin birbirinden farklı kararlara imza atmış olması örnek gösterilmektedir (Başalp, 2015: 82).

de veri koruma hukukunun yeknesaklığı ihtiyacına çare olamamış; birlik üyesi ülkeler arasında veri koruma düzeyleri ve kapsamaları arasındaki farklılık, veri transferinin koruma düzeyi düşük üye devlet üzerinden gerçekleştirilmeye çalışılması sonucunu doğurduğundan birliğin ortak pazar stratejisine gölge düşürmüştür¹⁸⁰.

Avrupa Birliği'nde veri koruma hukukunda reform düşüncesi 2010 yılında kendini göstermeye başlamış, 2012 yılında Avrupa Birliği Komisyonu tarafından kabul edilen Genel Veri Koruması Tüzüğü taslağı ile ilk meyvesini vermiştir¹⁸¹. 27 Nisan 2016 tarihinde, 95/46/AT sayılı Yönerge ile belirlenen ilkelerin geliştirilmesi ve gelişen teknoloji karşısında bireylerin temel haklarının daha kapsamlı bir şekilde korunması amacı ile ortaya konan 2016/679 sayılı Tüzük 25 Mayıs 2018 tarihinde yürürlüğe girmek üzere kabul edilmiştir¹⁸². Bu yeni düzenleme, 95/46/AT sayılı Yönergeyi ilga edecektir¹⁸³. Avrupa Birliği'nin yeni veri koruma düzenlemesi için tercihini, yeni bir yönerge yerine genellikle sektörel konularda kullandığı regülasyondan (tüzükten) yana kullanması, kişisel verilerin korunması hakkının üye ülkelere layığı ile benimsenmesi yönündeki kararlı tutumunun önemli bir yansımasıdır.

Avrupa Birliği'nin İşleyişi Hakkındaki Antlaşma'nın 288. maddesi uyarınca, tüzük (regülasyon), genel uygulama alanına sahip olup bütünüyle bağlayıcıdır ve yürürlük tarihinden itibaren tüm üye devletlerde doğrudan uygulanır¹⁸⁴. Başka bir anlatımla, tüzüklerin uygulanabilmesi için ülkelerin bir düzenleme ile tüzük hükümlerini iç hukuklarına aktarmalarına gerek bulunmamaktadır. Dahası, birliğin etkinliğinin zedelenmemesi ve uluslar üstü yapısına gölge düşürmemesi bakımından üye ülkelerin tüzük hükümlerini iç hukuklarına aktarmaları engellenmiştir¹⁸⁵. Birlik üyesi devletlerde halihazırda bulunan veri koruma yasalarının hükümleri ile tüzük hükümleri arasında farklılık bulunması halinde ise tüzük

¹⁸⁰ Dix, 2013: 268; Başalp, 2015: 83.

¹⁸¹ Diaz, 2016: 209; Başalp, 2015: 79; http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (erişim tarihi:23.11.2017).

¹⁸² http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf (erişim tarihi: 25.11.2017)

¹⁸³ Bk. GDPR madde 94.

¹⁸⁴ "BİRLİĞİN HUKUKİ TASARRUFLARI

Madde 288

Kurumlar, Birliğin yetkilerinin kullanılması için tüzük, direktif, karar, tavsiye ve görüşler kabul eder. Tüzükler genel uygulama alanına sahiptir. Bütünüyle bağlayıcıdır ve tüm üye devletlerde doğrudan uygulanır. yönergeler, muhatap alınan her üye devleti, ulaştırılması gerekli sonuçları itibarıyla bağlar, şekil ve yöntem seçimini ise ulusal otoritelere bırakır. Kararlar bütünüyle bağlayıcıdır. Muhatabı belirtilen bir karar, yalnızca muhatabı için bağlayıcıdır. Tavsiye ve görüşler bağlayıcı değildir. " (Avrupa Birliği'nin İşleyişi Hakkında Antlaşma, <https://www.ab.gov.tr/files/pub/antlasmalar.pdf> (erişim tarihi:25.11.2017))

¹⁸⁵ Waele, 2014: 76.

hükümlerine üstünlük tanınır. Bunun istisnası, devletin iç hukukundaki veri koruma kuralının çelişki yaratmadığı müddetçe, tüzükteline nazaran daha kapsamlı olmasıdır¹⁸⁶. Gerek gerçek veya özel hukuk tüzel kişilerinin idareye açacakları davalar (dikey olarak) ve gerekse bireylerin ve özel hukuk tüzel kişilerinin birbirlerine karşı açacakları davalar (yatay olarak) tüzük hükümlerine doğrudan dayandırılabilir ve bu hükümler mahkemenin kararına da esas alınabilir¹⁸⁷.

2016/679 sayılı Tüzük, temelde veri sahibinin daha etkin korunması amacı ile veri işleyenlere ve veri kontrolörlerinin sorumluluklarının artırılmasını öngören hükümler ile donatılmıştır.

Buna göre mülki açıdan;

-İşlemenin Birlik içerisinde gerçekleşip gerçekleşmediğine bakılmaksızın, Birlik içerisinde yer alan bir kontrolör veya bir işleyici kuruluşunun veri işleme faaliyetleri bağlamında yapılması,

-Birlik içerisinde yer almayan bir kontrolör veya işleyici kuruluş tarafından Birlik içerisinde yer alan veri öznelerinin verilerinin işlenmesi durumunda işleme faaliyetinin:

- a. Birlik içerisindeki veri öznesinin bir ödeme yapma gerekliliği bulunmaksızın ürün veya hizmet sunmasına veya
- b. Davranışın birlik içerisinde gerçekleşmesi şartıyla veri öznelerinin davranışlarının izlenmesine ilişkin olması durumunda,

-Veri işlemenin bir kontrolör tarafından Birlik içerisinde yer almayan fakat uluslararası kamu hukukuna göre Birlik üyesi devletin hukukunun geçerli olduğu bir yerde gerçekleşmesi durumunda uygulanır¹⁸⁸.

2016/679 sayılı Genel Veri Koruma Tüzüğü; veri kontrolörlerine veri sahibine sahip oldukları haklara ilişkin olarak bilgilendirme ve bunu belgelendirme yükümlülüğü getirmesi ve ayrıca veri sahibinin verilerinin işlenmesi için mutlak suretle izninin alınması ve ücretsiz, kolay ve hızlı bir biçimde sistemden çıkma hakkı (opt-in¹⁸⁹) verilmesi, verilerin işlenmesi için veri sahibinin rızasının özgürce, aydınlatılmış, belirli bir amaca matuf ve açık olarak verilmiş olmasının gerekmesi, bu kapsamda rıza koşulunun güçlendirilmiş olması¹⁹⁰, veri işleyenlerin tamamının veri işlemeden sorumlu tutulması¹⁹¹, veri sahibine verilerini taşıma hakkı

¹⁸⁶ Waele, 2014: 78-79.

¹⁸⁷ Waele, 2014: 76.

¹⁸⁸ Bk. GDPR madde 3.

¹⁸⁹ İngilizce, 'optional in' teriminin kısaltılmışıdır.

¹⁹⁰ Bk. GDPR madde 4/11, 7, 8.

¹⁹¹ Bk. GDPR, madde 6/f.

verilmesi¹⁹², veri kontrolörüne veri ihlalinin kişilerin temel hak ve özgürlüklerini ihlal etme riski taşıması durumunda veri koruma otoritesinin 72 saatten geç olmamak şartı ile mümkün olan en kısa sürede ve veri sahibinin de gecikmeksizin bilgilendirilmesi sorumluluğu yüklenmesi¹⁹³, veri kontrolörüne riskli veri işleme faaliyetleri bakımından (örneğin, hassas verilerin, ceza mahkûmiyetlerine ilişkin verilerin; teknolojik gelişmelere bağlı olarak ortaya çıkan yeni otomatik veri işleme metotları kullanılarak işlenmesi gibi) bu faaliyetlerden önce veri koruma etki değerlendirmesi yapılması sorumluluğu getirilmesi¹⁹⁴, Avrupa Birliği vatandaşlarına ait verilerin sınır ötesi aktarımının daha sıkı koşullara bağlanması, kişisel verilerin hukuka aykırı olarak işlenmesi durumunda, veri sahibine sağlanan tazminat hakkı düzenlemesinin geliştirilmesi ve rücu imkanı tanınması¹⁹⁵, ilaveten daha ağır yaptırım¹⁹⁶ ve kişisel verilerin korunmasına ilişkin daha elverişli mekanizmaların öngörülmesi gibi yenilikler barındırmaktadır¹⁹⁷.

Bu yeniliklerin içerisinde kuşkusuz ki kamuoyunda en çok ses getiren ve tartışılan, "*unutulma hakkı*" olarak da bilinen ve 2016/679 sayılı Tüzüğün 17. maddesinde yer alan "*silinme (right to be forgotten)*" hakkıdır. Esasen bu hak, 95/46/AT sayılı Yönerge'nin 12. maddesinde düzenlen "*erişim hakkı (right of access)*" kapsamında veri öznesine yönerge hükümlerine aykırı olarak verilerinin işlenmesi durumunda düzeltme, silinme veya bloke konulmasını temin etme hakkının daha geniş bir biçimde ve yeni bir isimle öngörülmüş biçimidir¹⁹⁸. Kural olarak, toplama ve işleme amaçlarının sağlanması için artık gerekli olmaması, veri sahibinin vermiş olduğu rızayı geri çekmesi, veri sahibinin verilerinin işlenmesine itiraz etmesi ve bu işleme faaliyeti için gerekli hukuka uygunluk şartlarının ortadan kalkması, verilerin başlangıçtan itibaren hukuka aykırı olarak işlenmesi gibi sebeplere dayalı olarak veri sahibinin verilerinin silinmesini istemesi halinde veri kontrolörüne bu verileri gecikmeksizin silme yükümlülüğü yüklenmiştir¹⁹⁹. Bu yükümlülük, verinin kamuya açık hale getirilmiş olması halinde buna ilişkin bütün bağlantıların, kopyaların ortadan

¹⁹² Bk. GDPR madde 20.

¹⁹³ Bk. GDPR madde 33-34.

¹⁹⁴ Bk. GDPR, madde 35.

¹⁹⁵ Bk. GDPR madde 82.

¹⁹⁶ Bk. GDPR madde 83; bu yaptırımlar tüzük hükümlerinin ihlali durumunda ihlalin niteliğine göre 20 milyon Avro veya daha yüksek olması durumunda ihlal edenin bir mali yıla ilişkin toplam küresel cirosunun %4'üne kadar ulaşabilmektedir.

¹⁹⁷ Diaz, 2016: 233; Ayrıntılı bilgi için bk.; Akıncı, 2017.

¹⁹⁸ Başalp, 2015: 93.

¹⁹⁹ Bk. GDPR madde 17/1; Başalp, 2015: 93.

kaldırılması için gerekli teknik tedbirler dahil, bütün tedbirleri almayı da kapsamaktadır²⁰⁰. Özetlemek gerekirse; unutulma hakkı, toplanma amacı bakımından artık ihtiyaç bulunmayan verilerin tamamen silinmesini isteme hakkıdır²⁰¹.

Esasen 2016/679 sayılı Tüzük'te yer alan düzenlemeden önce de mahkeme kararlarında unutulma hakkına atıf yapılmakta idi. Örneğin, 1939 yılında İsviçre'de idam edilmiş bir mahkumun hayatını konu alan bir radyo piyesinin yayınlanmasından önce söz konusu mahkumun oğlu tarafından mahkemeye yapılan başvuru sonucunda mahkeme, kişinin bir ceza mahkumiyetinin ardından tam olarak topluma kazandırılmasının ancak bu durumun toplumda unutulması sonucunda sağlanabileceğine, hafızalardan tam olarak silinmemiş bir geçmişin bu piyes ile tekrar canlandırılarak kişinin adının tekrar toplumun farkındalığına açılacağına ve bu durumun ölen mahkumun oğlunun itibarını ve baba ile içsel ilişkisini de zedeleyeceğine işaret ederek yayının önlenmesi sonucu doğuracak bir karara imza atmıştır²⁰².

Unutulma hakkına atıf yapılan diğer bir karar ise, Avrupa Birliği açısından bu hakkın mihenk taşı olarak kabul edilebilecek, Birlik kurumlarının karar ve tasarruflarının Birlik hukukuna uygun olup olmadığını denetleyen ABAD'ın 13 Mayıs 2014 tarihli "*Google Kararı*"dır²⁰³. Karar, İspanya vatandaşı olan Costeja González tarafından İspanyol Veri Koruma Ajansına, bir İspanyol Gazetesi ('La Vanguardia') ile Google İspanya ve Google Inc. şirketleri aleyhine yapılan; González'in isminin Google grubuna ait arama motorlarında aratıldığında anılan gazetenin 19 Ocak ve 9 Mart 1998 tarihlerindeki yayınlarının González'in sosyal güvenlik borçlarının tahsili için gerçekleştirilecek bir açık artırmanın ilanının yer aldığı sayfaların bağlantılarının verilmesine dair şikayete dayanmaktadır²⁰⁴.

İspanyol Veri Koruma Ajansı, kendisine yapılan bu şikayetin La Vanguardia yönünden, haberin açık artırmanın mümkün olduğunca çok yayılması ve alıcı bulunması amacına dayalı olarak yapıldığından hukuka uygun olduğundan bahisle reddine; fakat Google İspanya ve Google Inc. yönünden ise bu şirketlerin gerçekleştirdikleri veri işleme faaliyetlerinden sorumlu olduklarına, bireylerin kişisel verilerinin korunmasına dair temel

²⁰⁰ Bk. GDPR madde 17/2.

²⁰¹ EU Press Release: Data Protection Reform – Frequently Asked Questions, 4.11.2010 - http://europa.eu/rapid/press-release_MEMO-10-542_en.htm?locale=EN (erişim tarihi:26.11.2017)

²⁰² BGE 109 II 353; aktaran: Başalp, 2015: 94-95.

²⁰³ Ayrıntılı bilgi için bk. Akgül, 2016.

²⁰⁴ ECLI:EU:C:2014:317,

<http://curia.europa.eu/juris/document/document.jsf?jsessionid=9ea7d0f130d5a87cc50a1c8b478399a7d411c2280f12.e34KaxiLc3eQc40LaxqMbN4PaNiPe0?text=&docid=152065&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=99126> (erişim tarihi: 27.11.2017)

haklarının ve geniş anlamda insan onurunun korunmasına yönelik olarak bu verilerin silinmesinin talep edilebileceğinden kabulüne karar vermiştir.

Google İspanya ve Google Inc. şirketlerinin bu karara karşı Ulusal Yüksek Mahkemeye başvurması üzerine Yüksek Mahkeme, Avrupa Birliği'nin İşleyişi Hakkında Antlaşma'nın 267. maddesine dayalı olarak Avrupa Birliği Adalet Divanı'ndan vaki uyuşmazlık nedeni ile ön karar vermesi talebinde bulunmuştur²⁰⁵.

Bunun üzerine ABAD,

- Arama motorlarının üçüncü kişiler tarafından internette yayınlanan bilgilerin bulunması, bu bilgilerin otomatik olarak kataloglandırılması, geçici olarak depolanması ve son olarak internet kullanıcılarının tercihi göre sıralı olarak sunmasından ibaret eylemlerinin, kişisel verilerin işlenmesi faaliyeti olduğu ve bu nedenle arama motorlarının 95/46/AT sayılı Yönerge'nin 2. maddesi kapsamında veri kontrolörü olarak kabul edilmesi gerektiği,
- Arama motorlarının bireylere 95/46/AT sayılı Yönerge'nin 12. maddesi ile tanınan 'erişim hakkı' kapsamında Yönerge hükümlerine aykırı olarak işlenen yetersiz, ilgisiz, geçersiz verilerinin silinmesi veya düzeltilmesinden sorumlu oldukları,
- Arama motorlarının kişinin adının aranması sonucunda, başından çok uzun süre önce geçmiş bir olay ile ilgili bilgilerin bulunduğu bağlantıları vermesinin ilgili verinin kamu yaşamında önemli rol oynaması ve kamunun bu veriye yönelik baskın bir ilgisinin bulunması şeklinde söz konusu olan "üstün kamu yararı"nın ortaya konması hali kapsamında kabul edilemeyeceği ve bu nedenle bu verilerin arama sonuçlarına ilişkin dökümden çıkarılması gerektiği²⁰⁶

yönünde birtakım sonuçlara vararak ön kararını açıklamıştır. Bu karar, Mahkemenin Amerikan menşeli teknoloji sektörü üzerinde Avrupa mevzuatını uygulamaya koymak sureti

²⁰⁵ Madde 267

Avrupa Birliği Adalet Divanı, aşağıdakiler hakkında ön karar verme yetkisine sahiptir:

a) Antlaşmalar'ın yorumu,

b) Birlik kurum, organ, ofis veya ajanslarının tasarruflarının geçerliliği ve yorumu.

Bu tür bir sorunun bir üye devlet mahkemesinde ortaya konması halinde, bu mahkeme kendi kararını vermek için konuya ilişkin bir karara gerek duyarsa, Adalet Divanı'ndan bu sorun hakkında karar vermesini talep edebilir. Bu tür bir sorunun, iç hukuka göre kararlarına karşı kanun yolunun kapalı olduğu bir ulusal mahkemede görülmekte olan bir davada ortaya konması halinde, bu mahkeme Divan'a başvurmakla yükümlüdür. Bu tür bir sorunun bir üye devlet mahkemesinde görülmekte olan tutuklu bir kişiyle ilgili bir davada ortaya konması halinde, Avrupa Birliği Adalet Divanı mümkün olan en kısa sürede harekete geçer.

²⁰⁶ Akgül, 2016: 32.

ile düzenleyici bir görev üstlenme arzusunda olduğunun bir göstergesidir. Devamla Mahkeme, kamuoyunda yer alan, internet çağında özel yaşamın gizliliği konusundaki tartışmalar bakımından tutumunu bu karar ile ortaya koymuş bulunmaktadır²⁰⁷.

Türk hukukunda ise Anayasa Mahkemesi, 2013/5653 sayılı ve 3.3.2016 tarihli kararında unutulma hakkını ayrıntılı olarak tartışmıştır²⁰⁸. Mahkemeye yapılan başvuru, ulusal ölçekte yayımlanan bir gazetenin internet arşivi sayfalarında, başvuru hakkında uyuşturucu kullandığı iddiası ile yürütülen ve başvuru aleyhine adli para cezasına hükmedilmesi ile sonuçlanan bir kamu davasına ilişkin olarak 1998 ve 1999 yıllarında yapılan haberlerin başvuru kişinin şeref ve haysiyetini zedelediği, özel hayatına ilişkin mahremiyeti ortadan kaldırdığı, topluma mal olmuş ünlü bir kişi olmamasına rağmen aile, iş ve sosyal hayatını olumsuz etkilediği gerekçesi ile Anayasa'nın temel hak ve özgürlüklere ilişkin hükümlerinin ihlal edilmesine ilişkindir.

Anayasa Mahkemesi unutulma hakkını Anayasa'nın 5. maddesi, 17. maddesi ile 20. maddesi bağlamında değerlendirecek;

"...Basının interneti etkin kullanmasıyla beraber ifade ve basın özgürlükleri ile şeref ve itibarın korunması arasındaki dengeyi ilkinin lehine bozmuştur. İfade ve basın özgürlüğü ile şeref ve itibarın korunması hakkı, eşit düzeyde koruma gerektiren temel hak ve özgürlüklerdir. Bu nedenle bozulan dengenin her iki temel hak arasında tekrar kurulması zorunluluk olmuştur. İnternet haberciliği ile birlikte unutulmanın zor olduğu günümüzde anılan dengenin tekrar kurulabilmesi şeref ve itibar yönünden bireylerin unutulma hakkının kabul edilmesi ile mümkün olabilir..."

...Anayasa'nın "devletin temel amaç ve ödevleri" başlığı altında düzenlenen 5. maddesinde "insanın maddi ve manevi varlığının gelişmesi için gerekli şartları hazırlamaya çalışmak" ifadesi ile devlete pozitif bir yükümlülük yüklenmiştir. Bu yükümlülük bağlamında Anayasa'nın 17. maddesinde düzenlenen kişinin manevi bütünlüğü bağlamında şeref ve itibarının korunması hakkı ve Anayasa'nın 20. maddesinin 3. fıkrasında güvence altına alınan kişisel verilerin korunmasını isteme hakkı ile birlikte düşünüldüğünde, devletin bireye geçmişte yaşadıklarının başkaları tarafından öğrenilmesi engellenerek "yeni bir sayfa açma" olanağı verme hususunda bir sorumluluğu olduğu açıktır. Özellikle kişisel verilerin korunması hakkı kapsamında kişisel verilerin silinmesini talep edebilme hakkı, kişilerin geçmişlerinde yaşadıkları olumsuzlukların unutulmasına imkan tanımayı kapsamaktadır. Dolayısıyla Anayasa'da açıkça düzenlenmeyen unutulma hakkı, internet vasıtasıyla ulaşılması kolay olan ve dijital hafızada bulunan haberlere erişiminin engellenmesi için Anayasa'nın 5., 17. ve 20. maddelerin doğal bir sonucu olarak karşımıza çıkmaktadır. Diğer taraftan, unutulma hakkının kabul edilmemesi, internet vasıtasıyla kolayca ulaşılabilir ve uzun süre muhafaza edilebilir kişisel veriler nedeni ile başkaları

²⁰⁷ Stute, 2015: 679.

²⁰⁸ <http://www.anayasa.gov.tr/icsayfalar/basin/kararlarailiskinbasinduyurulari/bireyselbasvuru/detay/pdf/2013-5653.pdf> (erişim tarihi:27.11.2017). Ayrıca bk. YGHK 2014-4/56 E., 2015/1679 K., 17.06.2015T.

tarafından kişiler hakkında ön yargı oluşturabilmesi nedeni ile manevi varlığının geliştirilmesi için gerekli onurlu bir yaşam sürdürmesine ve manevi bağımsızlığına müdahaleyi sürekli kılmaktadır."

tespitlerinde bulunarak ülkemizde henüz kişisel verilerin korunmasına ilişkin özel bir yasanın dahi bulunmadığı bir tarihte unutulma hakkını kabul etme hususunda yenilikçi ve çağdaş bir yaklaşım göstermiş, başvuruyu kabul ederek Anayasa'nın ihlal edildiğine hükmetmiştir.

1.3.2.5. Asya – Pasifik Ekonomik İşbirliği (APEC)

Asya-Pasifik bölgesinde sürdürülebilir ekonomik gelişim ve refahı desteklemek amacı ile 1989 yılında Avusturalya, Brunei Darussalam, Kanada, Endonezya, Japonya, Kore, Malezya, Yeni Zellanda, Filipinler, Singapur, Tayland ve Amerika Birleşik Devletler'in öncülüğünde kurulan Asya- Pasifik Ekonomik İşbirliği'nin (Asia-Pacific Economic Cooperation), halihazırda 21 üyesi bulunmaktadır²⁰⁹.

APEC üyesi devletler, düşük maliyetli, etkili ve küçük ekonomilerin dahi dünyaya açılması imkanı sağlayan elektronik ticaretin, ülkelerinde geliştirilmesi ve yaygınlaştırılması adına özellikle 95/46 sayılı AB Yönergesi'ne uygun olarak veri akışının sağlanması ve özel hayatın gizliliğinin korunması amacı ile 2005 yılında Özel Yaşamın Gizliliği Çerçeve Belgesi'ni (APEC Privacy Framework) kabul etmiştir²¹⁰. OECD Rehber İlkeleri'nin etkisinde tanzim edilen bu belgede Asya-Pasifik ülkelerinin, AB veri koruma mevzuatından farklı olarak kendine özgü bir veri koruma hukuku yaklaşımı geliştirmeyi hedefledikleri görülür²¹¹.

2004 tarihli Özel Yaşamın Gizliliği Çerçeve Belgesi, kişisel verilerin korunmasında hakim olacak genel ilkeler²¹² ve sınır ötesi veri akışının kurallarına ilişkin olmak üzere iki

²⁰⁹ <https://www.apec.org/About-Us/About-APEC/History> (erişim tarihi: 19.03.2018)

²¹⁰ <https://www.apec.org/Publications/2005/12/APEC-Privacy-Framework> (erişim tarihi: 19.03.2018)

²¹¹ Küzeci, 2010: 147.

²¹² Bu dokuz ilke şu şekildedir:

1. Kötüye kullanımın önlenmesi,
2. Bildirimde bulunma,
3. Veri toplamanın sınırlı olması,
4. Kişisel verilerin hukuka uygun kullanılması,
5. Veri öznesine seçme hakkı verilmesi,
6. Veri kalitesi,
7. Veri güvenliği,
8. Erişim ve düzeltme hakkı,
9. Hesap verilebilirlik. (Ayrıntılı bilgi için bk. <https://www.apec.org/Publications/2005/12/APEC-Privacy-Framework> , (erişim tarihi:19.03.2018))

bölümden oluşur²¹³. Üye devletler bakımından bağlayıcı olmamakla birlikte, özel yaşamın gizliliği konusunda yeknesak ve AB ülkelerine kıyasla etkili bir koruma öngörmeyen Asya-Pasifik ülkelerinde daha güçlü yasal düzenlemeleri desteklemesi ve ticaretin ekonomik getirileri ile temel hak ve özgürlükler bağlamında kişisel verilerin korunması arasında denge kurulmasını sağlaması yönünden olumlu karşılanmıştır²¹⁴.

1.3.2.6. Çeşitli Ülke Düzenlemelerinde Kişisel Verilerin Korunması

1.3.2.6.1. Amerika Birleşik Devletleri (ABD)

Avrupa'ya kıyasla daha esnek bir veri koruma anlayışına sahip olan Amerika Birleşik Devletleri'nde bu konuda istikrarlı ve kapsayıcı bir düzenleme bulunmamaktadır²¹⁵. Bunun yanında, kişisel verilerin talep halinde açıklanması yönünden zorlayıcı bir Bilgi Edinme Hakkı Kanunu'nun (The Freedom of Information Act) bulunmasının kişisel verilerin korunması hususunu olumsuz olarak etkilediği savunulur²¹⁶.

Amerikan hukukunda kişisel verilerin korunmasına ilişkin düzenlemelerin bir örneği, Anayasada bulunmakta olup (Fourth Amendment to the Constitution) buna göre kişilerin evleri ve belgeleri hukuka aykırı arama ve el koymalara karşı korunur ancak bireyin bu korumadan faydalanabilmesi için özel hayatının korunmasına ilişkin meşru bir beklentisinin bulunması aranır²¹⁷.

Kişisel verilerin korunmasına yönelik diğer bir düzenleme, 1974 tarihli Özel Yaşamın Gizliliği Kanunu (The Privacy Act)'dur. Bu kanun, kişilerin isimleri, kimlik numaraları, parmak izi, ses izi veya fotoğraf gibi kişiyi belirlenebilir kılan hususları içerecek eğitimi, finansal işlemleri, sağlığına, mahkumiyetlerine ya da iş hayatlarına dair bilgilerin toplanması, kullanımı ve ifşasına ilişkindir²¹⁸. Yine, Amerikan yasalarının tüketiciler yararına özel şirketler için öngördüğü ve birtakım bilgilerin bu şirketler tarafından açıklanması biçimindeki yükümlülük -örneğin hastanelerin birtakım tıbbi operasyonların performans sonuçlarını açıklaması zorunluluğu gibi- veri güvenliği alanını da kapsar hale getirilmeye başlanmıştır. Buna göre özel şirketlerin, kişisel veri güvenliğinin ihlali durumunda bu ihlalden kişisel

²¹³ Küzeci, 2010: 148.

²¹⁴ Akgül, 2014: 216.

²¹⁵ Börding, 2017: 38.

²¹⁶ Schwartz ve Reidenberg , 1996: 140'tan aktaran: Kaya, 2011: 321.

²¹⁷ Avrupa Parlamentosu, 2015: 51.

²¹⁸ Avrupa Parlamentosu, 2015: 52.

verileri etkilenen şahıslara e-posta veya benzeri bir yöntem vasıtası ile bildirim yükümlülüğü bulunmaktadır²¹⁹.

Kişisel verilerin korunmasının temel bir insan hakkı olarak kabul edildiği Avrupa Birliği yaklaşımının aksine, ABD'nin özellikle yukarıda anılan düzenlemelerin ABD vatandaşı olmayan bireyleri kapsam dışı bırakması, bağımsız bir denetleme mekanizması öngörmemesi, kişisel verilerin işlenmesine ilişkin amaçla bağlılık, amacın gerektirdiğinden daha uzun süre elde tutulmama gibi temel ilkelerin ya hiç bulunmaması ya da eksik düzenlenmiş olması nedenleri ile eleştirildiği görülmektedir²²⁰.

AB ile ABD arasındaki kişisel verilerin korunmasına ilişkin bu farklılığın AB'den ABD'ye yapılacak veri transferinin aksamasına sebep olmasının önüne geçilmesi amacı ile yürütülen müzakereler sonucunda yedi temel maddeden oluşan "*Safe Harbour*" ilkeleri kabul edilmiştir²²¹. Bu ilkeler, AB'den veri transfer etmek isteyen ABD kurumlarının toplama amacına ilişkin olarak veri öznelerini bilgilendirmek, veri öznelerinin izni bulunmadan toplanan verileri üçüncü kişilerle paylaşmamak, bu iki şart gerçekleştiği takdirde bile verileri aynı düzeyde koruma sağlamayan üçüncü kişilere vermemek, verilerin güvenliği ve bütünlüğü için gerekli önlemleri almak, veri öznelerine verilerine erişim hakkı sağlamak ile veri öznelerinin şikâyetlerini yöneltebilecekleri bağımsız denetim organları oluşturmaktan ibarettir²²². Kuşkusuz, bu ilkelerin Amerikan menşeli ve dünya üzerinde en çok kişisel veri işleyen Google, Facebook, Amazon gibi şirketler için de bağlayıcılığı bulunmakta idi.

Ancak 2013 yılında Amerikan Ulusal Güvenlik Ajansı (NSA)'nın eski çalışanı olan Edward Snowden'ın sızdırdığı bilgilerden, Facebook şirketinin Avrupa vatandaşlarının kişisel verilerini Safe Harbour ilkelerine aykırı olarak işlediğinin ortaya çıkması sonucunda Max Schrems isimli bir Avusturalya vatandaşının İrlanda Veri Koruma Otoritesi'ne yaptığı başvurunun ardından konu ABAD'a taşınmış ve bunun üzerine ABAD Safe Harbour ilkelerinin geçersizliğine hükmetmiştir²²³. Bu kararın ardından, Amerikan kurumlarının Avrupa Birliği ülkelerinden gerçekleştirdikleri veri transferlerinde Safe Harbour ilkelerine dayanma imkanı bulunmadığından Avrupa Komisyonu tarafından alınan 2016/1250 sayılı ve

²¹⁹ Schwartz ve Janger, 2007: 915.

²²⁰ Avrupa Parlamentosu, 2015: 67-68.

²²¹ Aksoy, 2010: 105; Özdemir, 2009: 31.

²²² Aksoy, 2010:106.

²²³ Avrupa Adalet Divanı, 6 Ekim 2015, C-362/14, MMR 2015,

<http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=2294770> (erişim tarihi:18.11.2017); Börding, 2017:39-40.

12 Temmuz 2016 tarihli karar uyarınca daha güçlü bir veri koruma sistemi öngören "Privacy Shield" isimli bir çerçeve düzenleme yayınlanmıştır²²⁴.

1.3.2.6.2. Almanya

Almanya Anayasası'nda kişisel verilerin korunması hakkına açıkça yer verilmemiş olmakla birlikte, kişisel verilerin korunması hakkı Anayasa'da yer alan "genel kişilik hakkı" kapsamında korunmaktadır²²⁵. Bunun yanında, Alman Anayasa Mahkemesi'nin 15.12.1983 tarihinde verdiği Nüfus Sayımı Kararı'nda genel kişilik hakkı çerçevesinde "*enformasyonel self-determinasyon*" prensibine dayalı yeni bir hak alanı tanımlamıştır²²⁶. Dünyada kişisel verilerin korunması yönündeki ilk yasal düzenlemenin 1970 yılında Almanya'nın Hessen eyaletinde yapılması da kişisel verilerin korunması hakkına verilen önemin bir başka göstergesidir²²⁷.

Almanya'da kişisel verilerin korunmasına ilişkin düzenlemelerin en önemlisi Federal (Alman) Veri Koruma Kanunu'dur. 20 Aralık 1990 tarihli olan bu Kanun, 14 Ocak 2003 tarihinde yeniden düzenlenmiş ve 5 Eylül 2005 ile 14 Ağustos 2009 tarihlerinde birtakım değişikliklere uğramıştır²²⁸. Anılan kanun, 2016/679 sayılı Tüzük hükümlerine uyum sağlanması amacı ile 30 Haziran 2017 tarihinde revize edilmiştir²²⁹. Kanun'un genel hükümleri ihtiva eden ilk bölümünde kişisel veri kavramının tanımı, kapsamı, kişisel verilerin kamu makamlarınca işlenmesi, kamuya açık alanlarda elektronik cihazlar ile yapılan gözetimde uyulması gereken ilkeler ve Federal Veri Koruma Komisyonu'nun kuruluşu ve işleyişine hakkındaki hükümler; ikinci bölümünde kişisel verilerin 2016/679 sayılı Tüzüğün 2. maddesi uyarınca ve birtakım özel amaçlar doğrultusunda işlenmesine, veri öznesinin hakları ile veri sorumluları ve veri işleyenlerin yükümlülüklerine ve cezalara ilişkin hükümler; üçüncü bölümünde kişisel verilerin AB'nin 2016/680 sayılı yönergesinin 1. hükmü uyarınca işlenmesine ilişkin hükümler; dördüncü bölümünde ise kişisel verilerin 2016/679 sayılı Tüzük ve 2016/680 sayılı Yönerge kapsamı dışında işlenmesine dair hüküm yer almaktadır²³⁰.

²²⁴ Ayrıntılı bilgi için bk. <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016D1250&from=EN> (erişim tarihi:11.01.2018); Börding, 2017: 40.

²²⁵ Korff, 2002: 8.

²²⁶ (BverfGE 65, 1)

²²⁷ Yüksel Civelek, 2011: 85.

²²⁸ Ünver, 2008: 180.

²²⁹ https://www.gesetze-im-internet.de/englisch_bdsge/englisch_bdsge.pdf (erişim tarihi:08.06.2018)

²³⁰ Federal (Alman) Veri Koruma Kanunu'nun İngilizce metni için bk.

<http://www.legislationline.org/topics/country/28/topic/3> (erişim tarihi: 24.01.2018)

Kanun'un 42. maddesi ile yetkisiz erişimin mümkün olmadığı ve aleni olmayan, çok sayıdaki kişiye ait kişisel verilerinin ticari amaçlarla üçüncü kişilere aktarılması veya erişilebilir kılınması; aleni olmayan kişisel verilerin yetkisiz olarak işlenmesi veya hileli olarak ele geçirilmesi ile kendisi veya başkasına bundan kazanç sağlanması ya da bir başkasının zarara uğratılması biçimindeki birtakım eylemler bakımından şikâyet üzerine hürriyeti bağlayıcı ceza veya adli para cezası öngörülmüştür. Kanun, Alman Federal Veri Koruma Komiseri tarafından uygulanmakta olup kamu kurumları ve özel kurumların veri işleme faaliyetlerini kapsamaktadır²³¹.

Almanya'nın Avrupa Birliği üyesi olması vesilesiyle 25 Mayıs 2018 tarihinde yürürlüğe girecek olan 2016/679 sayılı Tüzüğün kişisel verilerin korunması ile ilgili konularda doğrudan uygulama alanı bulacağı ve bu nedenle Federal Veri Koruma Kanunu hükümlerinin yalnızca Tüzük hükümleri ile çelişmediği ve Tüzükten daha kapsamlı olması durumunda uygulanacağı unutulmamalıdır.

Federal Veri Koruma Kanunu'nun yanında, Alman Ceza Kanunu'nun "Özel Hayat ve Özel Hayatın Gizli Alanının İhlali" başlıklı 15. bölümünde de kişisel verilerin korunmasına yönelik suç tiplerine yer verilmiştir²³². Buna göre, başkasının aleni olmayan konuşmalarını izinsiz biçimde kaydetmek, bunları kullanmak veya üçüncü kişilerin kullanımına sunmak, aleni olmadığını bildiği konuşmaları dinleme cihazı ile dinlemek veya bunları ifşa etmek²³³;

²³¹ Gültekin, 2012: 52.

²³² Ünver, 2008: 175.

²³³ "Madde 201 – Konuşmanın gizliliğinin ihlali

(1) Her kim yetkisi olmaksızın,

1. başka birisinin alenî olmayan konuşmasını, ses taşıyıcı bir aletle kaydeder veya,
2. böyle oluşturulan bir kaydı kullanır veya üçüncü bir şahsın ulaşabilmesini sağlarsa, üç yıla kadar hapis cezası ile veya adli para cezası ile cezalandırılır.

(2) Her kim yetkisi olmaksızın,

1. Başka birisinin aleni olmayan ve kendisinin bilgisine sunulmuş olmayan konuşmasını bir dinleme aletiyle dinlerse, veya
2. Birinci fıkranın 1 numaralı bendine göre kaydedilmiş veya ikinci fıkranın 1 numaralı bendine göre dinlenmiş olan, bir başkasının alenî olmayan konuşmasının içeriğini, harfiyen veya ana hatları itibarıyla alenen bildirirse,

Aynı ceza ile cezalandırılır.

Birinci fıkranın 2 numaralı bendinde belirtilen fiilin cezalandırılabilmesi için, alenî bildirimin başka bir kişinin haklı menfaatini ihlal etmeye [beeinträchtigen] elverişli olması gerekir. Alenî bildirim, çok önemli [überragend] bir kamusal menfaatin kullanılmasının sağlanması için yapılmışsa, fiil hukuka aykırı değildir.

aleni olmayan veya yetkisiz erişime karşı özel olarak korunan verileri ele geçirmek²³⁴ eylemleri bakımından hürriyeti bağlayıcı ceza veya adli para cezası öngörülmüştür²³⁵.

1.3.2.6.3. İngiltere

Yazılı bir Anayasa'nın bulunmadığı İngiltere'de, Avrupa İnsan Hakları Sözleşmesi'nin ülkenin iç hukukuna dahil edilmesi ile birlikte sözleşmenin 8. maddesinde düzenlenen "özel hayata ve aile hayatına saygı" hakkı kapsamında değerlendirilen kişisel verilerin korunması hakkı da geliştirilmiş bir statü kazanmış bulunmaktadır²³⁶.

İngiltere'de kişisel verilerin korunması hakkının düzenlendiği en kapsamlı hukuksal metin, 1 Mart 2000 tarihinde yürürlüğe giren 1998 tarihli Veri Koruma Kanunu'dur²³⁷. Bu

(3) Her kim, kamu görevlisi veya kamu hizmeti için özel olarak görevlendirilen biri olarak, konuşmanın gizliliğini ihlâl ederse (fıkra 1 ve 2), beş yıla kadar hapis cezası veya adli para cezası ile cezalandırılır." (Bk. Yenisey ve Plagemann, 2015: 306-307.)

²³⁴ "Madde 202a – Veri casusluğu

- (1) Her kim, yetkisi olmaksızın, kendisinin bilgisine sunulmuş olmayan ve hak sahibi olmayanların girişine karşı özel olarak korunmuş bulunan verileri bu korumayı aşarak kendisine veya bir başkasına giriş yapma olanağı sağlarsa, üç yıla kadar hapis cezası veya adli para cezası ile cezalandırılır.
- (2) Birinci fıkra da belirtilen veriden, sadece elektronik, manyetik veya sair doğrudan doğruya algılanamayacak bir şekilde kaydedilmiş veya aktarılmış olan veriler anlaşılır.

Madde 202b – Verilerin iletilirken ele geçirilmesi

Her kim, yetkisi olmaksızın, teknik araçlardan yararlanarak kendisi veya bir başkası için, aleni olmayan veri iletiminden alarak veya bilgi işlem tesisatından yayılmakta olan elektromanyetik dalgalara girerek kendisi için belirlenmiş olmayan verileri (202a maddenin ikinci fıkrası) sağlarsa, fiil diğer hükümler uyarınca daha ağır bir ceza ile cezalandırılmadığı takdirde, iki yıla kadar hapis cezası veya adli para cezası ile cezalandırılır.

Madde 202c – Veri casusluğunun ve verilerin iletilirken ele geçirilmesinin hazırlığı

- (1) Her kim 202a veya 202b maddelerde belirtilen suçların işlenmesini hazırlamak üzere,
1. verilere giriş yapmayı sağlayan (m. 202a fıkra 2) şifre veya sair güvenlik kodlarını veya,
 2. bu tür fiilleri işlemeyi amaçlayan bilgisayar programları
- (4) Üretir, kendisine veya bir başkasına sağlar, satar, bir başkasına verir, yayar veya sair bir şekilde ulaştırabilmesini sağlarsa, bir yıla kadar hapis cezası veya adli para cezası ile cezalandırılır. (Bk. Yenisey ve Plagemann, 2015: 311-312.)

²³⁵ Gültekin, 2012: 49-50.

²³⁶ Korff, 2002: 8-9.

²³⁷ Özdemir, 2009: 72; Gültekin, 2012: 59; orijinal metin için bk. https://www.legislation.gov.uk/ukpga/1998/29/pdfs/ukpga_19980029_en.pdf (erişim tarihi: 25.01.2018). İngiltere Veri Koruma Yasası ilk kez 1984 yılında yürürlüğe girmiş olup bu metnin yeterince kapsayıcı olmayışı ve müphem hükümlere yer vermesi nedeni ile kişisel verilerin korunması hakkının yeterli güvenceye sahip olmadığı ifade edilmektedir. (Yüksek Civelek, 2011: 87).

kanunda, kişisel verinin tanımı yapılarak veri koruma ilkeleri belirlenmiş, veri öznesinin hakları, veri sorumlularının bildirim yükümlülüğü, kanunun kapsamı bakımından istisnalar ve yaptırımlar düzenlenmiştir. Kanunun uygulanması Veri Koruma Komiseri tarafından sağlanmaktadır²³⁸. İngiltere Veri Koruma Kanunu'nda Federal Alman Veri Koruma Kanunu'nun aksine, kişisel verilerin hukuka aykırı olarak işlenmesi eylemleri bakımından hürriyeti bağlayıcı ceza öngörülmemiştir²³⁹.

İngiltere'nin 23 Haziran 2016 tarihinde gerçekleştirdiği referandum sonucunda Avrupa Birliği'nden ayrılma kararı alması (Brexit) ile birlikte 25 Mayıs 2018 tarihinde yürürlüğe girecek olan 2016/679 sayılı Genel Veri Koruma Tüzüğü'nün doğrudan uygulanması mümkün olmayacaktır. Bu nedenle, İngiltere'nin Avrupa Birliği ile süregelen ekonomik ilişkilerin 2016/679 sayılı Tüzüğün kişisel verilerin aktarımına ilişkin öngördüğü kurallar nedeni ile sekteye uğramaması bakımından Tüzük ile eşdeğer koruma düzeyi öngören yeni bir hukuki düzenleme yapma ihtiyacı doğmuş ve bu nedenle Kişisel Verilerin Korunması Taslağı (Data Protection Bill) hazırlanmıştır²⁴⁰. 2017-19 sayılı bu Taslağa ilişkin Lordlar Kamarası görüşmeleri 18 Ocak 2018 tarihinde tamamlanarak Avam Kamarası'na iletilmiş bulunmakla buradaki görüşmeler halihazırda devam etmektedir²⁴¹. Taslakta dikkat çeken husus; kasten ve taksirle kişisel verileri ele geçirme, ifşa etme, başkalarına verme ve veri öznesinin rızası olmaksızın muhafaza etme eylemlerinin yanında veri öznesinin kimliği ile bağlantısı koparılmış verilerin yeniden veri öznesi ile ilişkilendirilebilir hale getirilmesi durumlarının da cezai yaptırıma tabi tutulmuş olmasıdır²⁴².

1.3.2.6.4. Türkiye

1.3.2.6.4.1. 12 Eylül 2010 Tarihli Anayasa Değişikliği

5237 sayılı Türk Ceza Kanunu'ndaki düzenlemelerin ardından, Anayasa'nın "Özel Hayatın Gizliliği" başlıklı 20. maddesine 5982 sayılı Kanun ile eklenen

"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.

²³⁸ Gültekin, 2012: 60.

²³⁹ Gültekin, 2012: 61.

²⁴⁰ Taslağın güncel orijinal metni için bk. <https://publications.parliament.uk/pa/bills/cbill/2017-2019/0153/18153.pdf> (erişim tarihi: 27.01.2018)

²⁴¹ <https://services.parliament.uk/bills/2017-19/dataprotection.html> (erişim tarihi: 27.01.2018)

²⁴² 2017-19 sayılı Kişisel Verilerin Korunması Taslağı madde 170 ve devamı.

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

hükmü ile kişisel verilerin korunması hakkı konusunda Anayasal bir güvenceye kavuşmuştur. Bunun yanında, Anayasa ile bu hakkın kapsamında belirlenen kuralların uygulanması, kişisel verilerin işlenmesi hususunda bağımsız bir denetim makamı öngörülmemiş olması ile Anayasa'nın 13. maddesinde yer alan, temel hak ve özgürlüklerin yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak sınırlanabileceği hükmüne rağmen kişisel verilerin kanunda öngörülen hallerde veya kişinin açık rızası ile işlenebileceği ifadesi, düzenlemenin eleştirilen yönleri olmuştur²⁴³.

1.3.2.6.4.2. 10 Haziran 2003 Tarihli İş Kanunu

4857 sayılı İş Kanunu'nun 75. maddesinde yer alan

"İşveren çalıştırdığı her işçi için bir özlük dosyası düzenler. İşveren bu dosyada, işçinin kimlik bilgilerinin yanında, bu Kanun ve diğer kanunlar uyarınca düzenlemek zorunda olduğu her türlü belge ve kayıtları saklamak ve bunları istendiği zaman yetkili memur ve mercilere göstermek zorundadır. İşveren, işçi hakkında edindiği bilgileri dürüstlük kuralları ve hukuka uygun olarak kullanmak ve gizli kalmasında işçinin haklı çıkarı bulunan bilgileri açıklamamakla yükümlüdür."

düzenlemesi ile işverene çalıştırdığı işçilerin birer özlük dosyasını tutma yükümlülüğü yüklenmiştir. İşçinin özlük dosyasında arşivlenen kayıtlar, onun doğrudan kimliğine ilişkin veya kimliğini belirlenebilir kıldıkları ölçüde kişisel veri olarak kabul edilecektir. Bu durumda işveren, işçinin özlük dosyasında bulunan kişisel verilerin kaydedilmesi, saklanması, üçüncü kişilere aktarılması gibi eylemlerinde mevzuata uygun hareket etmek ve kişisel verilerin işlenmesine dair ilkelere riayet etmek zorunda olup bu husus anılan maddenin 2. cümlesinde 'bilgileri dürüstlük kuralları ve hukuka uygun olarak kullanma' ifadeleri ile somutlaştırılmıştır. Aynı zamanda, işverenin işçinin özlük dosyasında bulundurduğu ve gizli kalmasında işçinin haklı çıkarı bulunan bilgileri açıklamamakla yükümlü olması bir tür sır saklama yükümlülüğü olarak değerlendirilir²⁴⁴. Ancak burada dikkat çeken husus, işveren işçinin özlük dosyasında yalnızca İş Kanunu ve diğer kanunlar uyarınca düzenlemek zorunda olduğu kayıtları tutabilecektir²⁴⁵. Bu düzenlemenin mefhum-u muhalifinden, işveren

²⁴³ Küzeci, 2010: 266.

²⁴⁴ Manav, 2015: 106.

²⁴⁵ Özlük dosyasının zorunlu içeriğine; 4857 sayılı İş Kanunu'nun 8. maddesinin 3. fıkrası örnek gösterilebilir. Bu maddede yer alan "Yazılı sözleşme yapılmayan hallerde işveren işçiye en geç iki ay içinde genel ve özel

tarafından yasal bir zorunluluk bulunmaksızın özlük dosyasında tutulan; örneğin fiziksel, ruhsal, ekonomik, veya sosyal durumuna ilişkin kişisel verileri yönünden işçinin kişisel verilerinin korunması hakkının ihlali gündeme gelecektir²⁴⁶. Kişisel verileri hukuka aykırı olarak işlenen işçinin İş Kanunu madde 24/II çerçevesinde iş akdini haklı nedenle feshedebileceği ve genel hükümlere göre zararının tazmin edilmesini isteyebileceği savunulmaktadır²⁴⁷.

1.3.2.6.4.3. 5237 sayılı Türk Ceza Kanunu

765 sayılı TCK'da "Hürriyet Aleyhine İşlenen Cürümler" kapsamında, beşinci fasıl içerisinde "Sırrın Masuniyeti Aleyhine Cürümler" düzenlenmiş olup 195. madde ile kişinin kendisine gönderilmiş olmayan bir mektup veya telgrafi veya kapalı bir zarfı kasten açması veya başka bir şahsın, posta ve telgrafla vâkı açık muhabere evrakını anlamak için hukuka aykırı olarak ele geçirmesi; 196. madde ile kendisine gönderilmiş olmayan posta ve telgraf muhaberesini ortadan kaldırması, 197. madde ile bu evrakın ifşa edilmesi fiilleri cezalandırılmakta idi. Bu hükümler haricinde kişisel verilerin korunmasına yönelik olarak ayrı, açık ve kapsamlı başka bir hüküm bulunmamaktaydı.

1 Haziran 2005 tarihinde yürürlüğe giren Türk Ceza Kanunu'nun, 765 sayılı TCK'dan farklı olarak 135. maddesinde yer verdiği 'kişisel verilerin kaydedilmesi', 136. maddesinde yer verdiği 'verileri hukuka aykırı olarak verme veya ele geçirme' ve 138. maddesinde yer verdiği 'verileri yok etmeme' suçlarına ilişkin hükümler, Türk Hukukunda kişisel verilerin korunması hakkına dair gerçekleştirilen ilk somut kanuni düzenlemelerdir.

Kişisel verilerin kaydedilmesi suçu; kişisel verilerin herhangi bir vasıta ile herhangi bir formatta hukuka aykırı olarak kayıt altına alınmasını ifade etmektedir. Söz konusu verilerin kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması durumu cezayı ağırlaştırıcı neden olarak öngörülmüştür.

çalışma koşullarını, günlük ya da haftalık çalışma süresini, temel ücreti ve varsa ücret eklerini, ücret ödeme dönemini, süresi belirli ise sözleşmenin süresini, fesih halinde tarafların uymak zorunda oldukları hükümleri gösteren yazılı bir belge vermekle yükümlüdür." düzenlemesi uyarınca işverene verilen bu belgenin yazılı olarak düzenlenmesi görevi, onu özlük dosyasında muhafaza etme zorunluluğunu beraberinde getirir. (Şık, 2012: 51.)

²⁴⁶ Başalp, 2004: 105.

²⁴⁷ Manav, 2015: 106.

Verileri hukuka aykırı olarak verme veya ele geçirme suçu, hukuka uygun veya aykırı olarak kaydedilmiş olmasına bakılmaksızın kişisel verilerin verilmesi, ele geçirilmesi veya yayılması seçimlik hareketlerinden birinin gerçekleştirilmesi halinde meydana gelmektedir.

Verileri yok etmeme suçu ise, hukuka uygun olarak kaydedilen kişisel verilerin, kaydedilme veya elde edilme amacının gerçekleşmesi, amacın ortadan kalkması, o veriye ihtiyacın kalmaması veya kişisel verinin muhafazasına olanak sağlayan kanuni düzenleme ile öngörülen muhafaza süresinin dolması gibi hallerde kişisel verinin imha edilmemesi halinde ortaya çıkmaktadır.

1.3.2.6.4.4. 11 Ocak 2011 Tarihli Türk Borçlar Kanunu

1 Temmuz 2012 tarihinde yürürlüğe giren 6098 sayılı Türk Borçlar Kanunu'nda da 'İşverenin Borçları' kapsamında "İşçinin Kişiliğinin Korunması"na ilişkin bölümün 'Kişisel Verilerin Kullanılmasında' başlıklı 419. maddesinde *"İşveren, işçiye ait kişisel verileri, ancak işçinin işe yatkınlığıyla ilgili veya hizmet sözleşmesinin ifası için zorunlu olduğu ölçüde kullanabilir. Özel kanun hükümleri saklıdır."* hükmüne yer verilmiştir. Buna göre, işverenin işçiye ait kişisel verileri işçinin kişiliğinin korunması bağlamında koruma yükümlülüğü bulunmakta olup işverenin işçinin kişisel verilerini yalnızca işçinin işe yatkınlığıyla ilgili ve hizmet sözleşmesinin ifası için zorunlu olduğu ölçüde işleyebileceği öngörülmüştür. Ancak bu iki istisnai durumun kapsamının genişliği ve uluslararası düzenlemelere kıyasla belirsiz bir içeriğe sahip olmasının, işçinin kişisel verileri açısından etkin bir koruma oluşturmama riskini beraberinde getireceği düşünülmektedir²⁴⁸.

1.3.2.6.4.5. 18 Şubat 2016 Tarihli Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun

Avrupa Konseyi'nin 1981 tarihli, "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşmesi" ya da "108 Nolu Sözleşme", Türkiye tarafından, sözleşmenin imzaya açıldığı ilk gün olan 28 Ocak 1981 tarihinde imzalanmış; ancak sözleşmenin 4. maddesinde öngörülen âkit devletlerin sözleşmeyi onaylamadan önce iç hukuklarında yapacakları düzenlemeler ile sözleşmede yer alan ilkeleri benimsemeleri şartını gerçekleştirilmediğinden onaylanamamış idi. 6669 sayılı Kanunun 18 Şubat 2016 tarih ve 29628 sayılı Resmi Gazete 'de yayımlanarak yürürlüğe girmesi ile birlikte 108 sayılı Avrupa Konseyi Sözleşmesi Türkiye'de de onaylanmış ve Türk hukukunda kişisel

²⁴⁸ Uncular, 2014: 44.

verilerin korunmasına ilişkin bir önemli uluslararası düzenleme hayata geçirilmiş bulunmaktadır.

1.3.2.6.4.6. 7 Nisan 2016 Tarihli Kişisel Verilerin Korunması Kanunu

1.3.2.6.4.6.1. Genel Olarak

Avrupa’da 1970’li yıllardan itibaren tartışılmaya başlayan kişisel verilerin korunması hakkının ve bu hakkın korunması ihtiyacına yönelik ulusal bir düzenleme yapılmasının Türkiye’de gündeme gelmesi “Kişisel Verilerin Korunması Kanunu Tasarısı”nı hazırlamak üzere 13 Eylül 1995 tarihinde bir komisyon oluşturulması ile mümkün olmuştur. Bu komisyonun çalışmalarını tamamlayamadan dağılması ile birlikte 18 Eylül 2000 tarihinde yeniden kurulması üzerine üç yıllık bir çalışmanın ardından 2003 yılında bir tasarı hazırlanmış ve bu tasarının Türkiye Büyük Millet Meclisi Başkanlığı’na iletilmesi 2008 yılını bulmuştur. TBMM Başkanlığı söz konusu tasarımı 2 Mayıs 2008’de esas komisyon olarak Adalet Komisyonuna, tali komisyon olarak Avrupa Birliği Uyum Komisyonu’na göndermiş, Adalet Komisyonu’nun 7 Mayıs 2008’de alt komisyona havale etmesinin ardından gündemin yoğunluğu ve TBMM seçimlerinin araya girmesi nedeni ile hükümsüz kalmıştır.

Tasarı, Adalet Bakanlığı tarafından revize edilmesinin ardından Başbakanlık tarafından ikinci kez TBMM Başkanlığı’na gönderilmiş fakat bu metin de bir önceki ile benzer sebeplerle hükümsüz kalmıştır.

Tasarının son olarak 18 Ocak 2016 tarihinde TBMM Başkanlığı’na gönderilmesi üzerine 24 Mart 2016 tarihinde TBMM Genel Kurulu’nda kabul edilerek kanunlaşmıştır. Kanunun genel gerekçesinde, Avrupa Konseyi’nin 108 sayılı Sözleşmesi’ne ve 95/46/AT sayılı Yönerge’ye atıf yapıldığı görülmektedir. Gerçekten, Kanun metni incelendiğinde; 95/46/AT sayılı Yönerge’nin sistematığının yaklaşık olarak benimsendiği söylenebilir. Ülkemiz açısından, uzun yıllar süren bekleyişin ardından kişisel verilerin korunmasına ilişkin ulusal ve bütüncül bir düzenlemenin hayata geçirilmiş olması büyük bir adımdır; ancak Avrupa Birliği tarafından 2012 yılında teklifi yayınlanan ve Kişisel Verilerin Korunması Kanunu Tasarısının yasalaşmasından oldukça kısa bir süre sonra kabul edilen 2016/679 sayılı Tüzük yerine bu tüzüğün 25 Mayıs 2018 ayında ilga edeceği 95/46/AT sayılı Yönerge’nin benimsenmiş olması Kanun’un daha başından değişikliğe muhtaç bir metin olduğunu göstermektedir. Zira 2016/679 sayılı Tüzük, 95/46/AT sayılı Yönerge’ye kıyasla veri öznelere tanınan hakların kapsamını genişletmiş, veri sorumlularına yüklenen yükümlülükleri ise arttırmıştır. Bu nedenle 95/46/AT sayılı Yönerge esas alınarak hazırlanan Türk mevzuatının 2016/679 sayılı Tüzük ile uyumlu olmaması; AB üyesi ülkeler ile Türkiye

arasındaki veri aktarımına engel teşkil edecek ve 2016/679 sayılı Tüzük’ün 83. maddesi uyarınca tüzük hükümlerini ihlal eden veri sorumlularının 20 milyon Avro’ya ulaşabilen para cezaları ile karşı karşıya kalmaları sonucunu doğurabilecektir.

1.3.2.6.4.6.2. Kanunun Amacı

6698 sayılı KVKK’nın amacı 1. maddesinde şu şekilde belirtilmiştir: *“kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemek”*ten ibarettir. Bu belirleme, 95/46/AT sayılı Yönergenin amacını düzenleyen 1. maddesi ile örtüşmektedir²⁴⁹.

1.3.2.6.4.6.3. KVKK’nın Kapsamı

Kanun’un 2. maddesi ile kapsam bakımından kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında uygulanacağı düzenlenmiştir. O halde kişisel verileri işleme faaliyetinin kamu sektörü veya özel sektör tarafından gerçekleştirilmesi arasında kanunen bir fark bulunmamaktadır²⁵⁰. Burada kapsam açısından önemli olan husus kişisel verilerin bir veri kayıt sisteminin parçası olarak işlenmesidir. Veri kayıt sistemi; Kanun’un 3/h maddesinde, *“kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi”* olarak tanımlanmış, madde gerekçesinde ise kişisel verilere ulaşımı kolaylaştıracak şekilde oluşturulan bir dosyalama sistemi şeklinde ifade edilmiştir²⁵¹.

Kanun’un kapsamının belirlenmesinde, 95/46/AT sayılı Yönerge’nin örnek alındığı ifade edilse de²⁵², Kanun’un kapsamı bakımından öngörülen istisnalara ilişkin 28. maddesi incelendiğinde, 95/46/AT sayılı Yönerge’ye nazaran oldukça geniş bir istisnalar listesi düzenlendiği ve böylelikle Kanun’un uygulama alanının büyük oranda daraltıldığı görülmektedir²⁵³. Hatta bu durum, Avrupa Komisyonu tarafından aday ülkenin Avrupa Birliği

²⁴⁹ 2016/689 sayılı Tüzüğün, amacını düzenleyen 1. Maddesinde “özel hayatın gizliliğinin korunması hakkı” kavramı yerine “kişisel verilerin korunması hakkı” kavramının tercih edildiği dikkat çekmektedir.

²⁵⁰ Korkmaz, 2016: 88.

²⁵¹ Bk. madde gerekçesi.

²⁵² Korkmaz, 2016: 91.

²⁵³ İstisnalar

MADDE 28- (1) Bu Kanun hükümleri aşağıdaki hâllerde uygulanmaz:

müktesebatına uyumuna ilişkin olarak kaydettiği ilerlemeleri ve gözlemlenen eksiklikleri yıllık olarak değerlendirdiği ilerleme raporlarında ve özellikle KVKK'nın yürürlüğe girmesinin akabinde hazırlanan 2016 Türkiye Raporu'nda eleştirilmiş ve bu istisnalar listesi nedeni ile 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun AB müktesebatına uygun olmadığı vurgulanmıştır²⁵⁴.

1.3.2.6.4.6.4. Kişisel Verilerin İşlenmesi Kavramı

Kişisel verilerin işlenmesi, kişisel veriler üzerinde herhangi bir yolla gerçekleştirilen herhangi bir işlem den ibaret olup bu kavramdan ne anlaşılması gerektiği, KVKK'da, 95/46/AT sayılı Yönerge'de ve 2016/679 sayılı Tüzük'te örneklendirilmek sureti ile açıklanmıştır. Buna göre işleme faaliyeti; kişisel verilerin elde edilmesi, kaydedilmesi,

a) Kişisel verilerin, üçüncü kişilere verilmemek ve veri güvenliğine ilişkin yükümlülüklerle uyulmak kaydıyla gerçek kişiler tarafından tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında işlenmesi.

b) Kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi.

c) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi.

ç) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi.

d) Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi.

(2) Bu Kanunun amacına ve temel ilkelerine uygun ve orantılı olmak kaydıyla veri sorumlusunun aydınlatma yükümlülüğünü düzenleyen 10 uncu, zararın giderilmesini talep etme hakkı hariç, ilgili kişinin haklarını düzenleyen 11 inci ve Veri Sorumluları Siciline kayıt yükümlülüğünü düzenleyen 16 ncı maddeleri aşağıdaki hâllerde uygulanmaz:

a) Kişisel veri işleminin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması.

b) İlgili kişinin kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi.

c) Kişisel veri işleminin kanunun verdiği yetkiye dayanarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olması.

ç) Kişisel veri işleminin bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olması.

²⁵⁴ Avrupa Komisyonu'nun 09.11.2016 tarihli, SWD(2016) 366 nihai sayılı AB Genişleme Politikasına İlişkin 2016 Türkiye Raporu, s. 71. - https://www.ab.gov.tr/files/pub/2016_ilerleme_raporu_tr.pdf, (erişim tarihi:17.01.2018)

depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi eylemlerinden herhangi birinin gerçekleştirilmesi biçiminde söz konusu olur. Kişisel verilerin işlenmesini ifade eden eylemler kanunda sınırlı sayıda düzenlenmediğinden kişisel verilere ilişkin olarak kanunda sayılmamış bulunan bunların kombine edilmesi, ilişkilendirilmesi, bloke edilmesi, silinmesi, yok edilmesi gibi işlemler de işleme faaliyeti kapsamında değerlendirilir²⁵⁵.

1.3.2.6.4.6.5. Veri Sorumlusu ve Veri İşleyen Kavramları

Gerek 95/46/AT sayılı Yönerge’de ve gerekse 2016/679 sayılı Tüzük’te “*veri kontrolörü (data controller)*” terimi ile ifade edilmekte olan ve kişisel verilerin işleme araç ve amaçlarını tek başına ya da diğerleriyle ortaklaşa belirleyen gerçek veya tüzel kişi, kamu otoritesi, devlet dairesi veya başka bir kuruluş bakımından KVKK’da “*veri sorumlusu*” terimi kullanılmıştır. Terminolojideki farklılığın yanı sıra KVKK’da veri sorumlusu kanun metninde yalnızca “*kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi*” olarak sınırlandırılmıştır. Ancak madde gerekçesinde veri sorumlusunun kamu kurumları, şirketler, dernekler veya vakıflar olabileceğinin belirtildiği görülmektedir²⁵⁶.

Veri işleyen ise veri sorumlusundan farklı olarak, veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi ifade etmektedir. Veri sorumlusu, veri işleyenin faaliyetlerini kanuna uygun olarak yürütmesini sağlayacak önlemleri almak ve düzenlemeleri yerine getirmekle mükelleftir²⁵⁷.

KVKK’nın 16. maddesi uyarınca kişisel verileri işleyen gerçek ve tüzel kişilerin, veri işlemeye başlamadan önce Veri Sorumluları Sicili’ne kaydolma zorunluluğu bulunmaktadır. Bu kapsamda, sicile dair usul ve esaslar Kişisel Verileri Koruma Kurumu tarafından “Veri Sorumluları Sicili Hakkında Yönetmelik” hazırlanmıştır. Anılan yönetmelik, 30.12.2017 tarihinde 30286 sayılı Resmi Gazete’de yayınlanarak yürürlüğe girmiş bulunmaktadır²⁵⁸.

²⁵⁵ Başalp, 2004: 33.

²⁵⁶ Bk. KVKK madde 3 gerekçesi.

²⁵⁷ Bygrave, 2003: 428.

²⁵⁸ [http://www.resmigazete.gov.tr/main.aspx?home=http://www.resmigazete.gov.tr/eskiler/2017/12/20171230.htm](http://www.resmigazete.gov.tr/main.aspx?home=http://www.resmigazete.gov.tr/eskiler/2017/12/20171230.htm&main=http://www.resmigazete.gov.tr/eskiler/2017/12/20171230.htm) (erişim tarihi:17.01.2018)

1.3.2.6.4.6.6. Kişisel Verilerin İşlenmesi Sırasında Uyulması Gereken Esaslar (Genel İlkeler)

KVKK'da “kişisel verilerin işlenmesi” başlığı altında sayılan ve “genel ilkeler” olarak adlandırılan esaslar, işlenen verinin sahip olması gereken nitelikleri belirler. Kimi yazarlarca bu nitelikler, işlenen “verinin kaliteli olması (data quality)” durumuna işaret etmektedir²⁵⁹. Bu ilkelere KVKK'da 95/46/AT sayılı Yönerge'nin 6. maddesine uygun olarak yer verilmiştir.

-Hukuka ve dürüstlük kurallarına uygun olma (95/46/AT sayılı Yönerge madde 6/a -lawful and fair processing):

Kişisel verilerin hukuk ve dürüstlük kurallarına uygun olarak işlenmesi, kapsayıcı niteliği gereği diğer ilkelerin çekirdeğini oluşturur²⁶⁰. Hukuka uygun olma, veri işleme faaliyeti sırasında yasalar ve diğer düzenlemelerde öngörülen usul ve ilkelere riayet edilmesi anlamına gelir²⁶¹. Dürüstlük kuralına uygun olma ise veri işleme faaliyeti sırasında veri öznesinin menfaatleri ile makul beklentilerinin nazara alınmasını ifade eder²⁶². Bu gereklilik, veri işleme faaliyetinin başından sonuna kadar geçirdiği bütün aşamalarda devam eder²⁶³. Veri işleme faaliyetine ilişkin sürecin şeffaf yürütülmesi, veri sorumlularının veri işleme faaliyetinden önce veri öznesini asgari olarak veri işlemenin amacı, veri sorumlusunun kimliği ve adres bilgileri gibi hususlarda bilgilendirmesi, kanunda açıkça öngörülen haller dışında veri işlemede gizlilik ve üstü kapalılık gözetilmemesi ve veri öznesinin verilerine erişim hakkı sağlanması dürüstlük kuralına uygun olma prensibinin gerekleridir²⁶⁴.

-Doğru ve gerektiğinde güncel olma (95/46/AT sayılı Yönerge madde 6/d - accuracy of data):

Veri işleme faaliyetinin genellikle istatistiksel bilgi oluşturma, müşteri eğilimini tespit etme veya bir hizmet sağlanması gibi bir hedefe yönelik olarak gerçekleştirildiği; öte yandan kişisel verilerin yanlış şekilde işlenmesinin veri öznesinin temel hak ve özgürlüklerini, manevi ve ekonomik durumunu olumsuz yönde etkileyebileceği nazara alındığında kişisel verinin doğru biçimde işlenmesinin, hem veri öznesi hem de veriyi işleyen kişi veya kurumun menfaatlerini gözetken çift yönlü bir prensip olduğu sonucuna varılır²⁶⁵.

²⁵⁹ Mäkinen, 2015: 273; Şimşek, 2008: 83.

²⁶⁰ Bygrave, 2003: 428; Başalp, 2004: 37; Akdağ, 2013: 71.

²⁶¹ Küzeci, 2010: 196; Akgül, 2014: 126.

²⁶² Küzeci, 2010: 197; Bygrave, 2003: 429; Akdağ, 2013: 72.

²⁶³ Şimşek, 2008: 85.

²⁶⁴ Handbook on European Data Protection Law, 73

https://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf (erişim tarihi:24.01.2018)

²⁶⁵ Küzeci, 2010: 208; Akdağ, 2013: 79.

Bu ilke, KVKK'nın 11. maddesi ile yakından ilişkilidir; zira veri öznesinin veri sorumlusundan kişisel verilerine yönelik talep hakları, başka bir deyişle kişisel verilerine erişim hakkı bulunmadan kendisine ait ve veri sorumlusu tarafından işlenen verilerin doğru ve/veya güncel olup olmadığının belirlenme imkanı neredeyse bulunmamaktadır²⁶⁶.

Her ne kadar verilerin doğru ve güncel tutulması yükümlülüğü veri sorumlusuna ait olsa da, bu yükümlülüğü yerine getirmek adına veri sorumlusunun veri öznesinin temel hak ve özgürlüklerini zedeleyebilecek devamlı bir takip tutumu yürütmesinin makul bir beklenti olmayacağı açıktır²⁶⁷. Bunun yanında, “gerektiğinde güncel olma” ilkesinin gerçekleştirilmesi bağlamında güncelleme işleminin ne zaman gerekli olacağına dair bir düzenleme öngörülmesi yerinde olacaktır.

-Belirli, açık ve meşru amaçlar için işlenme (95/46/AT sayılı Yönerge madde 6/b -purpose specification and limitation):

Verilerin işleme amacının belirli ve açık olması, veri işleme faaliyetinin hangi hedefe yönelik olduğunun başlangıçtan itibaren ortaya konabilir olmasıdır²⁶⁸. Bu ilke, veri sorumlularına verileri işlerken dayandıkları gerekçelerde belirsiz ifadelerden kaçınma yükümlülüğü yüklemektedir²⁶⁹. İlâveten, kişisel verinin gelecekte ortaya çıkabilecek ve halihazırda belirsiz amaçlar için depolanmasını da yasaklamaktadır²⁷⁰.

Kişisel verilerin işlenmesi bakımından ortaya çıkan her yeni amaç yönünden belirlilik, açıklık ve meşruluk kriterlerine uygunluk söz konusu olmalıdır. Bir örnekle açıklamak gerekirse; bir havayolu şirketi gerçekleştireceği uçuşun gerektiği gibi yürütülmesi için bilet satın alan yolcuların birtakım kişisel verilerine ihtiyaç duyar. Bu kişisel veriler; yolcuların koltuk numaraları, yolcuların tekerlekli sandalye vb. ihtiyaç duyabileceği engel halinin bulunup bulunmadığı, Yahudi veya Müslüman kültürüne özgü özel yiyecek tercihleri gibi bilgilerdir. Bu bilgilerin varılacak ülkenin göçmenlik bürosu tarafından talep edilmesi halinde ise ilk işleme amacından farklı olarak göçmenliğin kontrolü amacı ile işlenmeye başlayacağından bu transferin yeni ve ayrı bir hukuki temele dayandırılması gerekecektir²⁷¹.

²⁶⁶ Küzeci:2010: 209.

²⁶⁷ Küzeci, 2010: 209.

²⁶⁸ Akdağ, 2013: 74; Aydın, 2015: 113.

²⁶⁹ Küzeci, 2010: 198; Akgül, 2014: 127.

²⁷⁰ Başalp, 2004: 38; Akdağ'a göre, kişisel verinin toplanma anından sonra ortaya çıkabilecek, başlangıçta belirsiz bir amaca yönelik olarak toplanması yasağı “ölçülülük ilkesi”nin kapsamında değerlendirilmelidir; bk. Akdağ, 2013: 78.

²⁷¹ Handbook on European Data Protection Law, 2014: 69

https://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf (erişim tarihi:24.01.2018)

Veri işlemede meşru amaç, bir kamu menfaatinin bulunması veya işlemenin kişilerin hak ve özgürlüklerini ilgilendirmesi biçiminde söz konusu olacaktır²⁷². Örneğin; AIHM'in *Peck/Birleşik Krallık* kararında, başvurucunun sokakta güvenlik kamerası tarafından görüntülediğini bilmeden bileklerini keserek intihar girişiminde bulunması ve o anda güvenlik kameralarından bu durumu fark eden polisler tarafından kurtarılmasının ardından görüntülerinin yüzünün sansürlenmeden medya ile paylaşılması üzerine yaptığı başvuru sonucunda Mahkeme, başvurucunun bu görüntülerinin doğrudan ifşa edilmesinin meşru bir amaca dayanmadığı gerekçesi ile Sözleşmenin ihlal edildiğine kanaat getirmiştir²⁷³.

- *İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma* (95/46/AT sayılı Yönerge madde 6/c - *relevancy of data*):

Kişisel verinin işlendiği amaçla bağlantılı olması; işlenen kişisel veri ile verinin işlenmesi sonucunda ulaşılmak istenen hedef arasında illiyet bağı bulunması, başka bir anlatımla söz konusu hedefe ulaşabilme bakımından kişisel veriyi işlemenin gerekli olmasıdır²⁷⁴. Bu kapsamda kişisel verinin hangi amacın gerçekleştirilmesine yönelik olduğu açıklanmış ise, veri sorumlusu tarafından o amacın gerçekleştirilmesi için yeterli olduğu noktada veri işleme faaliyeti sınırlandırılmalıdır²⁷⁵.

-*İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme* (95/46/AT sayılı Yönerge madde 6/e – *limited retention of data*):

Kişisel verilerin gerektiğinden daha uzun süre kayıtlı bulundurulmaması, muhafaza edilmemesi gerekmektedir. Bu prensip kişilerin “unutulma hakkı” ile de yakından ilgilidir²⁷⁶. Veri işleme ile hedeflenen amaca ulaşılması, amaca ulaşmak için kişisel verinin ilgisiz veya gereksiz olduğunun anlaşılması veya verinin işlenmesi ile ulaşılması hedeflenen amacın ortadan kalkmasına rağmen kişisel verilerin muhafaza edilmeye devam edilmesi hukuka aykırı olacaktır²⁷⁷. Bu noktadan sonra yapılması gereken, kişisel verinin imha edilmesi veya imha edilmese bile veri ile kişinin kimliği arasındaki bağın koparılması, başka bir deyişle

²⁷²Handbook on European Data Protection Law, 2014: 64,

https://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf (erişim tarihi:24.01.2018)

²⁷³ Peck/Birleşik Krallık, B.No: 44647/98, 28.01.2003, [https://hudoc.echr.coe.int/tur#{"fulltext":\["CASE OF PECKv.THEUNITEDKINGDOM"\],"documentcollectionid2":\["GRANDCHAMBER","CHAMBER"\],"itemid":\["001-60898"\]}](https://hudoc.echr.coe.int/tur#{) (erişim tarihi:24.01.2018)

²⁷⁴ Bk. KVKK madde 4 gerekçesi. Aynı yönde bk. Başalp, 2004: 38; Akdağ, 2013: 77.

²⁷⁵ Handbook on European Data Protection Law, 2014: 70,

https://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf (erişim tarihi:24.01.2018); Akdağ, 2013: 78.

²⁷⁶ Küzeci, 2010: 209.

²⁷⁷ Başalp, 2004: 39; Küzeci, 2010: 210.

verinin ‘anonimleştirilmesi’²⁷⁸ veya ‘takma adlar altında toplanması’²⁷⁹dır²⁸⁰. Kişisel verilerin gelecekte yararlanma ihtimaline binaen muhafaza edilmesi hukuka aykırı olacaktır²⁸¹.

Kişilere ait verilerin değerinin artmasıyla birlikte bu verileri belirli bir amaç doğrultusunda ve hukuka uygun olarak toplayan ve muhafaza eden veri sorumluları bakımından verilerin güvenliğini sağlamak ve kötü niyetli üçüncü kişiler tarafından suiistimal edilmesini önlemek her geçen gün zorlaşmaktadır. Özellikle dijital ortamda depolanan ve muhafaza edilen bu verilerin güvenliği için gerekli tedbirlerin alınmaması halinde ortaya çıkan güvenlik açıklarından faydalanarak ele geçirilmesi, birçok kişinin mağduriyetine yol açabilmektedir. Örneğin kişilerin ad, soyad, anne adı, baba adı, doğum tarihi, doğum yeri gibi kimlik bilgileri²⁸²; adres bilgileri, e-posta adres²⁸³ ve şifreleri²⁸⁴ gibi bilgilerinin elde edildiğine yönelik haberler medyada sıklıkla karşımıza çıkar olmuştur. Dolayısı ile kişisel verilerin muhafaza edilmesinin bu verilerin güvenliğini sağlamak konusunda veri

²⁷⁸ İngilizce, *anonymization*; “kişisel verilerin, belirli ya da belirlenebilir gerçek kişiyle, kişisel ya da olgusal bağımsız bilginin bağlanamamasını veya bunun ancak fahiş oranda zaman, maliyet ve emek kaybı ile bağlanabilmesini sağlayacak şekilde değiştirilmesidir.” (Federal Almanya Ver Koruma Yasası madde 3/6’dan aktaran Küzeci, 2010:206). 2016/679 sayılı Tüzüğün başlangıç bölümünün 26. maddesi uyarınca anonim veriler kişisel veri değildir ve bu nedenle tüzüğün sağladığı hukuki korumadan faydalanmazlar.

²⁷⁹ İngilizce, *pseudonymisation*; “bir kişinin adının veya diğer belirlenebilir özelliklerinin, veri öznesinin kimliğinin saptanmasını engellemek veya kimliğin saptanmasını oldukça güç duruma getirmek amacıyla bir etiket ile değiştirilmesidir.” (Federal Almanya Ver Koruma Yasası madde 3/6’dan aktaran Küzeci, 2010: 206). 2016/679 sayılı Tüzüğün başlangıç bölümünün 26. maddesi uyarınca takma ad altında toplanan kişisel verinin kimliği belirlenebilir gerçek kişiye ait bir bilgi olarak kabul edilmesi gerekir. Bunun anlamı, takma ad altında toplanan bilgilerin kişisel veri olduğu ve Tüzüğün sağladığı hukuki korumadan faydalanacağıdır.

²⁸⁰ Handbook on European Data Protection Law, 2014: 73,

https://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf (erişim tarihi:24.01.2018)

²⁸¹ Bk. KVKK 4. madde gerekçesi.

²⁸² 50 milyon Türk vatandaşının kimlik verilerinin sızdırılmasına ve ifşa edilmesine ilişkin haber için bk; “Turkish authorities ‘probing huge ID data leak’”, <http://www.bbc.com/news/technology-35978216> (erişim tarihi: 17.12.2017)

²⁸³ Yahoo’nun şirketi nezdindeki 1 milyardan fazla kullanıcı hesabında veri sızıntısı meydana geldiğini duyurduğuna ilişkin haber için bk; “Parolalarınızı değiştirin, tarihin en büyük veri sızıntısı”, <http://www.mynet.com/haber/teknoloji/parolalarinizi-degistirin-tarihin-en-buyuk-veri-sizintisi-2787884-1> (erişim tarihi:20.03.2018). Aynı yönde bk. “Yahoo, ‘mail’ skandalını doğruladı”, <http://www.trthaber.com/haber/bilim-teknoloji/yahoo-mail-skandalini-dogruladi-301852.html> (erişim tarihi: 20.03.2018).

²⁸⁴ E-posta servislerinden biri olan Gmail’in kullanıcılarına ait yaklaşık 5 milyon şifrenin yayınlanmasına ilişkin haber için bk.; “5 milyon Gmail şifresi internete düştü”, <http://www.hurriyet.com.tr/5-milyon-gmail-sifresi-internete-dustu-27181091> (erişim tarihi:20.03.2018)

sorumlusuna büyük ve zor bir sorumluluk yüklemesi karşısında ilgili mevzuatta öngörülen süre sonunda veya işlendikleri amaç için gerekli sürenin sonunda verilerin imha edilmesinin veya anonimleştirilmesinin veri sorumlusunu da potansiyel risklerden koruyacağı unutulmamalıdır.

1.3.2.6.4.6.7. Kişisel Verilerin İşlenmesinin Şartı: Açık Rıza

Kişisel veriler, kural olarak ilgisinin açık rızasının bulunması halinde hukuka uygun olarak işlenebilir²⁸⁵. Rıza, 95/46/AT sayılı Yönerge'nin 2/h. maddesinde, *“kendisine dair kişisel verilerin işlenmesi için veri öznesinin kabulüne işaret eden, özgürce ve bilgilendirme yapıldıktan sonra alınan beyan”* biçiminde tanımlanmıştır. KVKK'nın 3/a maddesinde ise kapsam bakımından daha genel bir ifade tercih edilerek; *“belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza”* şeklinde tanımlandığı görülmektedir. Kişisel verilere yönelik halihazırda en güncel hukuki metin olan 2016/679 sayılı Tüzük'te ise 4/11. maddesinde veri öznesinin rızası *“ kendisi ile ilgili kişisel verilerin işlenmesine yönelik olarak veri öznesinin bir beyan veya net bir biçimde onay ifade eden bir eylemi vasıtası ile özgürce verilmiş, spesifik, bilgilendirmeye dayalı ve açık kabul”* olarak ifade edilmiştir.

Veri öznesinin rızası, 95/46/AT sayılı Yönerge'nin 7/a maddesinde veri işlemeyi yasallaştırma kriterlerinin içerisinde diğer kriterlerden –veri öznesinin taraf olduğu bir sözleşmenin yerine getirilmesi için veya kamu menfaatine yapılan bir görevin yerine getirilmesi için gerekli olma gibi - bir üstünlüğü ya da önceliği bulunmayan bir seçenek olarak düzenlenmiş iken; KVKK'nın 5. maddesinde veri işleme faaliyetini hukuka uygun hale getiren yasal zemin ve veri öznesine tanınmış temel bir hak ve kural olarak düzenlendiği dikkat çekmektedir. Bunun yanında her ne kadar, veri öznesinin rıza göstermesi, veri işleme faaliyetini hukuka uygun hale getirirse de, bu rızanın verilmiş olması yukarıda sayılan veri işleme faaliyetine egemen olması gereken ilkelerden feragat edildiği anlamına gelmez²⁸⁶.

Kişisel verilerin korunması hakkı bağlamında geçerli bir rıza beyanından söz edilebilmesi için; veri öznesinin beyanı sırasında hiçbir baskı altında bulunmaması, veri öznesinin verilerin işleme amacı ve işleme faaliyetinin sonuçlarından tam olarak bilgilendirilmiş olması ile rıza beyanının sınırlarının makul ölçüde somutlaştırılmış olması

²⁸⁵ Başalp, 2004: 39; Toğuz, 2014: 53; Özdemir, 2009: 128.

²⁸⁶ Madde 29 Çalışma Grubu, 2011:7, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf (erişim tarihi:17.12.2017)

gerekir²⁸⁷. İlaveten, veri öznesi tarafından verilerin işlenmesine yönelik olarak verilen rıza beyanı, tereddüde yer vermeyecek şekilde açık olmalıdır²⁸⁸.

Rıza beyanının geçerliliği bakımından herhangi bir şekil şartı öngörülmemiş olmakla birlikte varlığından söz edilebilmesi için, veri öznesinin onaylama arzusunun dış dünyaya herhangi bir şekilde yansması gerekir. Bu noktada, sessiz kalma durumunun zımnî kabul anlamına gelip gelmeyeceği sorusu akla gelebilir; örneğin veri sorumlusunun iki hafta içerisinde itiraz edilmediği takdirde kişisel verilerinin üçüncü kişilere transfer edileceği yönünde veri öznelere bir bilgilendirmede bulunması halinde sessiz kalan ilgililerin, veri sorumlusunun bu işleme faaliyetine rıza gösterdiğine dair ortada hiçbir emare bulunmayacağından verilerin transfer edilmesi işlemi hukuka aykırı olacaktır²⁸⁹. KVKK'da yapılan tanımda da, belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza, ifadesine yer verilmiş ve rıza kavramının "açıklanma" biçiminde aktif yapı ile ilişkilendirilerek tanımlanmış bulunması karşısında veri sorumlusunun veri işleme faaliyetine itiraz edilmeyerek rıza gösterildiğinden bahisle kişisel verileri işleminin yasal bir temele dayandığından söz edilemez.

Rızanın kişisel verilerin işlenmesinde bir hukuka uygunluk zemini oluşturabilmesi için, hiçbir etki veya baskı altında kalmadan, özgürce ve gönüllü olarak verilmiş olması şarttır. Örneğin sağlık verileri ile işçi-işveren ilişkisine dayalı olarak işlenen veriler bakımından verilen rızanın özgür iradeye dayanıp dayanmadığının ayrıca araştırılması gerekir; zira veri öznesinin veri sorumlusunun etkisi altında bulunduğu ve verilerinin işlenmesine rıza göstermemesi halinde eksik tedavi görme ya da hiç görmeme veya salt bu nedenle önyargıya maruz kalma gibi ihtimaller dolayısı ile rıza beyanı vermesi durumunda bu iradesinin özgür olmadığı kabul edilir²⁹⁰.

Rıza beyanının genel işlem koşulları²⁹¹ içerisinde yer alan bir kloz ile alınması halinde bu rıza beyanının hukuken geçerli olup olmadığı, TBK'nın genel işlem koşullarını düzenleyen

²⁸⁷ Handbook on European Data Protection Law, 56,

https://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf (erişim tarihi:24.01.2018)

²⁸⁸ Başalp, 2015: 39; ayrıca bk. KVKK'nın 5. madde gerekçesi.

²⁸⁹ Madde 29 Çalışma Grubu, 2011: 12, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf (erişim tarihi:17.12.2017)

²⁹⁰ Madde 29 Çalışma Grubu, 2011: 13, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf (erişim tarihi:17.12.2017)

²⁹¹ Bir sözleşme, sözleşmelere hakim olan irade özgürlüğü prensibine aykırı olarak genellikle daha güçlü olan tarafının önceden ve yalnızca kendi iradesi doğrultusunda hazırlanması ile nispeten güçsüz konumda olan diğer

20. ve devamı maddeleri nazara alınarak belirlenmelidir. Buna göre, rıza beyanının genel işlem koşulu olduğu tespit edildiği takdirde veri öznesine verilerin işlenmesi konusunda açıkça bilgi verilip verilmediği verilerinin işlenmesinin kendisi açısından doğuracağı olumsuz sonuçların açıklanıp açıklanmadığı, bu beyanı değiştirme imkanının tanınıp tanınmadığı araştırılacaktır²⁹². Bu ihtimallere olumsuz cevap verilmesi halinde ise TBK'nın 21. maddesine göre rıza beyanına “yazılmamış sayılma”²⁹³ yaptırımının uygulanması gerekir.

1.3.2.6.4.6.8. Kişisel Verilerin İşlenmesinde İlgilisinin Açık Rızası Bulunması Kuralının İstisnaları

Kanun, belirli durumların varlığı halinde, kişisel verilerin ilgisinin rızasının bulunmamasına rağmen işlenebileceğini öngörmüştür. Öngörülen durumların her biri, kişisel verilerin işlenmesinde hukuka uygunluğun birer gerekçesini oluşturur. KVKK'nın 5. maddesi ile veri öznesinin rızasının bulunması kural olarak kabul edilmiş ve aynı madde içerisinde veri öznesinin rızasının bulunmasına gerek bulunmayan istisnai haller sayılmıştır. 95/46/AT sayılı Yönerge'de ve 2016/679 sayılı Tüzük'te ise bu haller rıza ile birlikte veri işlemenin hukuka uygunluk zemini olarak kabul edilmiş ve “*veri işlemeyi yasallaştıran kriterler*”²⁹⁴ ve “*veri işlemenin hukuka uygunluğu*”²⁹⁵ biçiminde ifade edilmiştir. Ancak, kişisel verinin işlenmesi bakımından dayanan yasal gerekçenin veri işlemede gözetilen farklı amaçlara göre değişkenlik göstermesi halinde bu gerekçelendirmenin veri sorumlusu tarafından ayrıca gözetilmesi gerekir. Bu durumu bir örnekle açıklamak gerekirse; veri öznesinin bir araba satın alması durumunda yapılacak satış sözleşmesi için verilerin işlenmesi, veri sorumlusuna kanunun 5/c maddesindeki istisnadan yararlanması imkanı tanırken bu verilerin veri sorumlusunun kendi pazarlama aktiviteleri kapsamında üçüncü kişilere aktarılacak olması

tarafa ise yalnızca sözleşmeyi bu haliyle tamamen kabul veya tamamen ret seçeneği sunulma biçiminde düzenlendiği takdirde genel işlem koşulları söz konusu olur (Görgeç, 2013: 406).

²⁹² Yeniocak, 2013: 82-83.

²⁹³ 6098 sayılı Türk Borçlar Kanunu

“Yazılmamış sayılma

MADDE 21- Karşı tarafın menfaatine aykırı genel işlem koşullarının sözleşmenin kapsamına girmesi, sözleşmenin yapılması sırasında düzenleyenin karşı tarafa, bu koşulların varlığı hakkında açıkça bilgi verip, bunların içeriğini öğrenme imkânı sağlamasına ve karşı tarafın da bu koşulları kabul etmesine bağlıdır. Aksi takdirde, genel işlem koşulları yazılmamış sayılır.

Sözleşmenin niteliğine ve işin özelliğine yabancı olan genel işlem koşulları da yazılmamış sayılır.”

²⁹⁴ 95/46/AT sayılı Yönerge'nin 7. madde başlığı metnin orijinalinde “Criteria for Making Data Processing Legitimate” biçimindedir.

²⁹⁵ 2016/679 sayılı Tüzük'ün 6. madde başlığı metnin orijinalinde “Lawfulness of Processing” biçimindedir.

halinde bu durum veri sorumlusunu genel kurala yönlendirerek bu işlem için veri öznesinin rızasının almasını gerektirecektir²⁹⁶.

Kanun'un 5. maddesinin 2. fıkrasında düzenlenen ve kişisel verilerin işlenmesi faaliyetinde veri öznesinin rızasının alınması zorunluluğunu ortadan kaldıran haller, 95/46/AT sayılı Yönerge'nin 7. maddesi ile benzerlik göstermektedir. Buna göre bu hallerden ilki veri işleme faaliyetinin bir kanun ile açıkça düzenlenmesidir. Örneğin; 4857 sayılı İş Kanunu'nun 75. maddesi ile işverenin işçinin kimlik bilgileri ile düzenlemek zorunda olduğu her türlü belge ve kayıtların saklandığı bir özlük dosyası tutma zorunluluğu bulunmakta olup işverenin bu veri işleme faaliyeti kanunda öngörülmüş olduğundan, işçinin rızasının alınmasına gerek bulunmamaktadır.

Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması halinde de veri öznesinin rızası aranmaz. Bu istisna 95/46/AT sayılı Yönerge'nin 7/d maddesi ve 2016/679 sayılı Tüzüğün 6/d maddesi ile benzeşmektedir. Bu duruma örnek olarak, kişinin bilincinin yerinde olmadığı bir sırada acil müdahale gerekmesi veya temyiz kudreti bulunmaması nedeni ile kişinin rızasının hukuken geçerli olmaması halinde kan grubu, geçirmiş olunan rahatsızlıklar, kullanılan ilaçlara ilişkin verilerin işlenmesi gösterilebilir²⁹⁷.

Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması halinde de veri öznesinin rızası aranmamaktadır. Bu istisna 95/46/AT sayılı Yönerge'nin 7/b maddesi ve 2016/679 sayılı Tüzük'ün 6/b maddesi ile benzeşmektedir. Bir banka ile kredi sözleşmesinin akdedilebilmesi için kişinin ödeme gücünün ve bankanın kredi alacağına ilişkin teminatın tespiti bakımından kişiye ait maaş bordrosu, tapu kayıtları, icra takibine konu edilmiş borcunun bulunup bulunmadığı gibi verilerin işlenmesi bu duruma örnek gösterilebilir²⁹⁸.

Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması halinde de kişisel verilerin işlenmesi bakımından rıza aranmaz. Bu istisna 95/46/AT sayılı Yönerge'nin 7/c maddesi ve 2016/679 sayılı Tüzüğün 6/c maddesi ile benzeşmektedir. Madde gerekçesinde bu duruma, işverenin ücretini ödeyebilmesi için işçinin banka hesap bilgilerini kayıt altında tutması hali örnek gösterilmiştir.

²⁹⁶ Madde 29 Çalışma Grubu, 2011: 8, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf (erişim tarihi:17.12.2017)

²⁹⁷ Bk. madde gerekçesi.

²⁹⁸ Bk. Madde gerekçesi.

İlgili kişinin kendisi tarafından alenileştirilmiş olması durumunda da herhangi bir şekilde kamuoyunun bilgisine sunulan kişisel veriler bakımından bu verilerin korunmasına ilişkin düzenlemeler ile amaçlanan hukuksal yararın ortadan kalktığı kabul edilir²⁹⁹.

Kişisel verilerin veri öznesinin rızası olmaksızın işlenebileceği diğer durumlar ise bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması ile ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olmasıdır.

Kanunda ayrıca 6. maddenin 3. fıkrası ile kişinin sağlığına ve cinsel hayatına ilişkin kişisel veriler yönünden açık rıza kuralına bir istisna öngörülmüş olup 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 işlenmesi mümkün kılınmıştır.

1.3.2.6.4.6.9. Veri Sorumlusunun Yükümlülükleri ile İlgili Kişinin Hakları

Kanunun 10. ve 12. maddelerinde aydınlatma yükümlülüğü ile veri güvenliğine ilişkin olmak üzere veri sorumlusunun yükümlülükleri, 11. maddesinde de ilgili kişinin yani veri öznesinin hakları düzenlenmiştir.

Veri sorumlusunun aydınlatma yükümlülüğü, kendisi veya yetkilendirdiği kişi tarafından ilgili kişilerin kişisel verilerin herhangi bir yolla elde edilmesi anında veri sorumlusunun ve var ise temsilcisinin kimliği, işleme amacı, kendisi tarafından işlenen kişisel verilerin kimlere ve hangi amaçlar doğrultusunda aktarılabilceği, kişisel verilerin hangi yöntemler ile elde edileceği ve bu yöntemin hukuki sebebi ile ilgili kişinin hakları konularını kapsamaktadır.

Kişisel hakları ihlal edilen kişilerin bu ihlalden haberdar olmadan haklarını etkin bir biçimde kullanmasının mümkün olmaması ve işleme faaliyetinin şeffaflığı bakımından aydınlatma yükümlülüğü önem taşır³⁰⁰.

Kişisel verilerin üçüncü kişiler tarafından kötüniyetli olarak kullanılması sonucunda kişiler ve kurumların maddi veya manevi pek çok zarara uğraması muhtemel olduğundan veri sorumlusunun aydınlatma yükümlülüğünün yanında işlediği verilerin güvenliğinin sağlama yükümlülüğü de bulunmaktadır. Kanun'un 12. maddesi ile öngörülen bu yükümlülük, kişisel

²⁹⁹ Bk. Madde gerekçesi.

³⁰⁰ Korkmaz, 2016: 128-129.

verilerin hukuka aykırı olarak işlenmesini, kişisel verilere hukuka aykırı olarak erişilmesini önlemeyi ve bu verilerin muhafazası için uygun güvenlik seviyesi oluşturmayı kapsar.

Kanun'un 11. maddesinde ise ilgili kişilerin hakları düzenlenmiştir. Buna göre kanun, veri sorumlusuna başvurarak kendisine ait kişisel verilerin işlenip işlenmediğini öğrenme, işlenmiş ise bu faaliyete ilişkin bilgi talep etme, işlenme amacı ile işleme faaliyetinin bu amaca uygun olarak yapılıp yapılmadığını öğrenme, kişisel verilerin aktarıldığı üçüncü kişileri bilme, kişisel verilerin eksik veya yanlış işlenmiş olması halinde bunların düzeltilmesini isteme, gerekli şartların sağlanmış olması halinde kişisel verilerin silinmesini veya yok edilmesini isteme; düzeltme, silinme ve yok etme işlemlerinin gerçekleştirilmesi halinde bu işlemlerin başlangıçta verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme, işlenen verilerin otomatik sistemler vasıtası ile analiz edilmesi suretiyle kendisi aleyhine bir sonucun ortaya çıkması durumunda buna itiraz etme ile son olarak kişisel verilerin kanuna aykırı olarak işlenmesi nedeni ile bir zararın doğması sonucunda doğan zararın tazmin edilmesini talep etme biçiminde geniş bir haklar yelpazesi öngörmüş bulunmaktadır.

1.4. Kişisel Verilerin Korunması Sorunu

Özel hayatın gizliliğinin korunması bağlamında kişisel verilerin korunması sorunu, birçok hukuk disiplini ilgilendirmekte, gerek devletle birey arası ilişkileri ve gerekse bireyler arası ilişkileri etkilemesi nedeni ile hem kamu hem de özel hukuk düzenlemelerinde yerini almış ve almaya devam etmektedir³⁰¹.

Kişisel veriler, kişinin kendisi veya yaşantısı ile ilgili bilgiler içermesi nedeni ile özel hayat kavramının bir parçası olarak kabul edilir. Nitekim kişisel verilerin işlenmesine dair usul ve esaslar, bu verilerin işlenmesine yetki veya izin verdikleri ölçüde özel hayatın gizliliği hakkının sınırlandırılmasına meşruiyet kazandırır³⁰².

Bir kimse ile ilgili özel bilgilerin onun isteği dışında bir başkası tarafından özel alanına ona ait verilerin elde edilmesi, toplanması, kaydedilmesi şeklinde haksız olarak müdahale edilmesi veya özel bilgilerin yayılması veya ifşa edilmesi sureti ile öğrenilmesi halinde o kişinin özel yaşamının gizliliği ihlal edilmiş olur. Bu durum, kişisel verilerin işlenmesinin, verileri işlenen kişi bakımından doğurduğu zararlı sonuçlardan ilki olup, diğeri ise kişi ile ilgili yanlış veya yanıltıcı bilgilerin işlenmesi halinde kişinin kimliği bakımından söz konusu olmaktadır³⁰³.

³⁰¹ Ketizmen, 2008:191; Dülger, 2016:104.

³⁰² Ketizmen, 2008:207.

³⁰³ Ross, 2006: 106-107.

Öte yandan, kişisel verilerin korunması hakkının, özel hayatın gizliliğinin korunması hakkının bir boyutu olarak değerlendirilmesi biçimindeki yaklaşımın zaman içerisinde terk edilmeye başlandığı gözlenmektedir. Nitekim 2000 tarihli AB Temel Haklar Şartı'nın 8. maddesi ile yenilikçi bir adım atılmak sureti ile kişisel verilerin korunması hakkı bağımsız bir hak olarak kabul edilmiş³⁰⁴, 2016/679 sayılı Tüzük'ün 1. maddesi ile Tüzük'ün amacının kişisel verilerin korunması temelinde kişilerin korunması olduğu vurgulanmıştır.

Gerçekten, kişisel verilerin usulsüz şekilde kullanılmasının doğurduğu sonuçlar günlük yaşamda gerçekleştirilen neredeyse her türlü işlemin çevrimiçi ortama adapte edilmesi ve bu işlemlerin güvenli bir biçimde gerçekleştirilebilmesi bakımından kişisel verilerin işlenmesini gerektirmesi karşısında oldukça yıkıcı boyutlara ulaşmıştır. Aynı şekilde, kamusal makamlar tarafından yerine getirilen kamu hizmetlerinin sağlığı ve devamlılığı, vergilendirme ile kamu düzeninin sağlanması, özel kurumlar tarafından ise kârın ve verimin yükseltilmesi bağlamında bilgiye ihtiyaç duyulmaktadır³⁰⁵. Kişisel verilerin bir kısmının “hassas” olarak nitelendirilmesinin neden olduğu, kişiye ait olup da bu kategorinin dışında kalan verilerin korunmasında kişinin menfaatinin bulunmadığı biçiminde bir yaklaşım, kişi haklarının ihlal edilmesi riskini doğuracaktır. Tek başına hiçbir şey ifade etmediği düşünülen kişisel bir bilgi, veri simsarları tarafından farklı mecralardan toplanarak veritabanlarında arşivlenmesi, birbiri ile karşılaştırılması ve kombine edilmesi sonucunda gerçek bir değer kazanmakta ve bu veriler satılarak kazanç elde edilmektedir³⁰⁶. Başlangıçta basit veya önemsiz gibi görünen bu bilgiler, teknolojinin gelişmesi ile birlikte gelecekte hayal dahi edilemeyecek ilişkilendirme ve analiz yöntemleri ile işlenerek ayrıntılı kişilik profilleri oluşturabilecek ve böylece bu veriler ilk toplandıkları andaki anlamlarının çok daha ötesinde, zararlı sonuçlar doğurabilecek bir güce ulaşabilecek, ilaveten birey verilerinin akıbetini öngöremeyecek duruma gelecektir³⁰⁷.

Bir yandan teknolojinin gelişmesi ile birlikte bilgisayar ve benzeri dijital gereçler ile internetin kullanımının artmasının sonucunda kişilere ilişkin verilerin hızla ve kolaylıkla kaydedilebilmesi, depolanabilmesi, herhangi bir amaç doğrultusunda kullanılabilmesi ve yayılabilmesi imkanının doğması, diğer yandan 1960'lı yıllardan itibaren yönetsel, ticari veya sosyal sebepler ile veri işleme faaliyetlerinde görülen artış veri mahremiyetine ve neticeten özel hayatın gizliliğine yönelik ihlal riskini arttıran etkenlerdir³⁰⁸.

³⁰⁴ Fuster ve Paepe, 2016: 136.

³⁰⁵ Mendos Kuşkonmaz, 2013: 13.

³⁰⁶ Schwartz ve Janger, 2007: 922-923.

³⁰⁷ Küzeci, 2014: 68-69.

³⁰⁸ Ketizmen, 2008: 193-194.

Bu etkenler, özel hayatın gizliliğinin; müdahale edilmezlik, yalnız kalma hakkı veya kamuyu ilgilendirmeyen konularda kişinin haksız ve istenmeyen ifşalardan uzak tutulması biçimindeki tanımlamalarını tartışmaya açmış; kişisel verileri ve bu veriler üzerindeki tasarruf hakkını da nazara alan, bu anlamda kişiye bir yetki ve talep hakkı veren kontrol merkezli tanımlamalar yapılmasına vesile olmuştur³⁰⁹.

Bu noktada ilk kez, Alman Anayasa Mahkemesi'nin 15 Aralık 1983 tarihinde verdiği Nüfus Sayımı (Census) Kararı³¹⁰'nda tanımlanan "*bilgilerin geleceğini belirleme hakkı (Informationelle Selbst-bestimmung)*"ndan bahsetmekte fayda vardır³¹¹. Pek çok Avrupa ülkesinin iç hukuk sisteminde öngördüğü veri koruma düzenlemeleri ile özellikle 95/46/AT sayılı Yönerge'yi önemli ölçüde etkileyen bu karar; Alman Parlamentosu'nda oybirliği ile kabul edilen ve nüfus sayımı sırasında vatandaşların kimlik bilgilerinin yanında gelir kaynakları, çalışma saatleri ve eğitim durumlarına ilişkin olarak da ayrıntılı bilgilerinin verilmesi zorunluluğu getiren ve birtakım amaçlarla bu bilgileri yerel yönetimlere aktarma imkanı sağlayan Nüfus Sayımı Kanunu'nda kişi hak ve özgürlüklerinin yeterince korunmadığına ilişkindir. Karara göre bilgilerin geleceğini belirleme hakkı, kişinin kendisi hakkında hangi bilgilerin, kim tarafından, ne kadar süreliğine ve hangi amaçlarla toplandığı konusunda bilgi sahibi olması ve bu bilgilerin sınırsız şekilde işlenmesinden korunmasını gerektirmekte olup bu hak, Anayasa ile güvence altına alınan insan onuru ve kişiliği serbestçe geliştirme hakkının bir parçasıdır³¹². Örnek vermek gerekirse, bir kişi herhangi bir sivil toplum örgütüne, toplantıya veya gösteriye katıldığı takdirde kendisi ile ilgili bu bilginin resmi makamlar tarafından kayıt altına alındığını düşünürse bu haklarını kullanamayacak ve neticede kişiliğini geliştirme hakkından yararlanamayacağı gibi toplumsal yaşama katılma ve burada işlev görme becerisi de geliştiremeyecektir³¹³. Kişi, kendisine ait bilgilerin ne zaman ve ne kadarının açıklanacağına kendisi karar vermelidir.

Öte yandan, bilgilerin geleceğini belirleme hakkı kişilere bilgileri üzerinde bir mülkiyet hakkı tanımlamak ya da yalnız kontrol yetkisi vermekten ziyade bireysel özerkliğin sağlanması için devlete, vatandaşlarına ait verilerin hangi şartlarla işlenebileceğini düzenleme yükümlülüğü getirmektedir.

³⁰⁹ Ketizmen, 2008: 197.

³¹⁰ (BverfGE 65, 1)

³¹¹ Küzeci, 2014: 53.

³¹² Küzeci, 2014: 56; ayrıca bk. Anayasa Mahkemesi'nin 2013/122 Esas, 2014/74 Karar sayılı ve 9.4.2014 tarihli kararı.

³¹³ Küzeci, 2014: 56-57.

İşte tüm bu sebeplerle, özel yaşamın gizliliğinin korunmasına ilişkin yasal düzenlemelerin hedefinde yer alan; kişinin, yalnızca belirli kişilerle paylaştığı özel alanın korunması düşüncesinin kişisel verilerin korunmasına ilişkin düzenlemelerin amacı ile birebir örtüşmemesi karşısında kişisel verilerin korunmasına yönelik bağımsız suç tipleri ceza kanunlarında öngörülmüş ve cezai müeyyideye tabi tutulmuşlardır. Nitekim, konusunu kişisel verilerin oluşturduğu suçların işlenmesi neticesinde kamu yararının daha fazla ihlal edildiği, hatta bu sebeple ceza kanununda kişisel verilere yönelik suçlar bakımından resen soruşturma ve kovuşturma ilkesinin benimsendiği görülmektedir³¹⁴.

1.4.1. Medeni Hukuk

Kişisel verilerin, kişilik hakkının bir parçası olması nedeni ile kişisel verilerin korunması hakkının ihlali durumunda Türk Medeni Kanunu'nun 24. maddesinde yer alan genel hüküm uyarınca bu hakkı ihlal eden kişinin sorumluluğu söz konusu olacaktır³¹⁵. Fakat burada kişilik hakkı ihlali iddiası ile sorumluluk; kişinin kişilik hakkından vazgeçtiğine dair bir irade beyanında bulunması halinde ortadan kalkar. Ancak burada dikkat edilmesi gereken, bu beyanın vazgeçmenin sonuçlarının öngörülebilmesine imkan verecek şekilde kişinin bilinçli ve özgür iradesine dayanması ile bu irade beyanının ahlaka aykırı olmamasıdır. Bunun yanında, ihlalin kamu yararı gibi üstün nitelikte bir yarara dayanması halinde veya ihlalin kanunun kişiye tanıdığı bir yetkinin kullanılmasının sonucu olması durumunda kişilik hakkı ihlalinin kaynaklanan sorumluluktan söz edilemeyecektir³¹⁶.

Kişisel verilere yönelik bir saldırı sonucunda kişilik hakkı ihlal edilen kişinin TMK'nın 25. maddesi uyarınca saldırıya son verilmesini, sona ermiş olsa bile etkilerinin halen sürmesi durumunda saldırının hukuka aykırılığının tespitini veya saldırı tehlikesinin önlenmesini talep ve dava hakkı bulunmaktadır. Öte yandan, kişilik hakkı saldırıya uğrayan kimsenin bu saldırı dolayısıyla oluşan maddi ve manevi zararların tazmini ile elde edilen kazancın vekaletsiz iş görme hükümleri uyarınca kendisine verilmesini isteme hakkı, kanunda öngörülmüş olan kişilik hakkının ve dolayısıyla kişisel verilerin korunmasına yönelik hükümlerdir. Görüldüğü üzere, TMK kişisel verilerin korunması hakkının ihlali durumunda kişilik hakkı ihlal edilen veri öznelerini güvence altına alan birtakım mekanizmalar ihtiva etmektedir.

³¹⁴ Özbek vd., 2016: 532.

³¹⁵ Özdemir, 2009: 95.

³¹⁶ Aksoy, 2010: 83-84.

1.4.2. İdare Hukuku

İdare; güvenliğin sağlanması, suçluluğun önlenmesi, planlama, sosyal devletin gereklerinin yerine getirilmesi gibi faaliyetlerini yürütebilmek adına kaçınılmaz olarak bireylerin kişisel verilerine ihtiyaç duyar³¹⁷. Bireylerin ehliyet, pasaport, ruhsatname gibi taleplerinde; vergi beyanı, evlilik gibi işlemlerinde beyan edilen, kolluk kuvvetleri tarafından yürütülen soruşturmalar kapsamında veya nüfus sayımı gibi işlemlerde elde edilen kişisel veriler bunlara örnek gösterilebilir. Fakat bu ihtiyaç kişisel verilerin hukuka uygun olarak işlenmesi konusunda idareye bir ayrıcalık bahsetmemektedir. Başka bir deyişle idare, bireylerin verilerini toplarken, kullanırken, aktarırken kişisel verilerin işlenmesine dair temel ilkelere riayet etme sorumluluğunu taşımaktadır.

Kişisel verilerin idare tarafından hukuka aykırı olarak işlenmesi sonucunda hakları ihlal edilen bireylerin hukuk devleti ilkesinin bir gereği olarak, idarenin hukuka aykırı bu işleminin durdurulmasını, kaldırılmasını, ortaya çıkan zararın giderilmesini idareden talep etme hakkı bulunmaktadır³¹⁸.

İdarenin işlem ve eylemlerinin yargı yolu ile denetimini kabul etmiş bulunan ülkelerde bu işlem ve eylemlerin dava yolu ile iptal edilmesi müessesesi, idarenin hukuka aykırı tasarruflarda bulunmasını ve kararlar almasını önlemekte; böylelikle '*idarenin hukukla bağlı olması*' ve '*hukuk devleti*' ilkelerinin güvencesini oluşturmaktadır³¹⁹. Bu bağlamda kişisel verilerin idare tarafından hukuka ve kanuna aykırı olarak kaydedilmesi ve muhafaza edilmesi, toplama amacına aykırı, yanlış veya eksik halde kullanılması, gerektiğinden uzun süre elde tutulması iptal davasına konu edilebilecek tasarruflardır.

Öte yandan, kişisel verilerin idare tarafından hukuka aykırı olarak işlenmesi, bu işleme faaliyeti sonucunda bireyin maddi veya manevi olarak zarara uğraması ve son olarak da idarenin söz konusu işlem veya eylemi ile bireyin zararı arasında illiyet bağı bulunması durumunda idarenin hukuki sorumluluğu kapsamında tazmin yükümlülüğünü gündeme getirecektir³²⁰.

Tüm bunların yanında, Türkiye'nin Avrupa Birliği üyelik sürecinde Avrupa Birliği tarafından 20. yüzyılın ikinci yarısından bu yana benimsenen kişisel verilerin korunmasının temel bir insan hakkı olduğuna ilişkin görüşün gereklerinin 108 sayılı sözleşmenin

³¹⁷ Küzeci, 2010: 318; Akgül, 2014: 275.

³¹⁸ Akgül, 2014: 263.

³¹⁹ Akgül, 2014: 264.

³²⁰ Akgül, 2014: 276.

imzalanmasından bu yana geçen yaklaşık 35 yıllık sürede yerine getirilememiş olması eleştiri konusu olmuştur.

2016 yılında yürürlüğe giren 6698 sayılı KVKK, kişisel verilerin korunmasına yönelik ihlallere karşı bireylere temel bir koruma düzeyi öngörmüş olsa da, idarenin faaliyetlerinde kişisel verilerin işlenmesine dair istisnaların kapsamının oldukça geniş tutulması nedeni ile bu mevzuatın Avrupa Birliği standartları ile uyumlu olmadığı ifade edilmektedir³²¹. Bu durum, Europol³²² ve Eurojust³²³ ile operasyonel işbirliği anlaşması yapılmasına engel teşkil etmektedir.

Anılan kanunda, veri öznesine birtakım haklar ve bu haklar ile ilişkili olarak başvuru ve şikayet usulleri öngörülmüştür.

Veri öznesinin, kanunun 11. maddesinde sayılan hakları bağlamındaki taleplerini yazılı olarak veya Kişisel Verileri Koruma Kurulu'nun belirleyeceği yöntemler vasıtası ile veri sorumlusuna iletmesinin ardından, veri sorumlusunun otuz günü geçmemek koşulu ile mümkün olan en kısa sürede bu talebi kabul etme ve gerekçesini açıklamak koşulu ile talebi reddetme yönündeki kararını yazılı olarak veya elektronik ortamda bildirmesi gerekmektedir. Bildirim bir ispat koşulu olup burada kararı içerir cevabın "bildirilmesi" ifadesinin kullanılması, veri sorumlusunun 7201 sayılı Tebligat Kanunu'na tabi olmayan gerçek kişi veya özel hukuk tüzel kişisi olması durumu ile açıklanmaktadır³²⁴. Her ne kadar madde

³²¹ "...Yeni kabul edilen Kanun, kişisel verilerin yargı birimleri ve infaz mercileri tarafından işlenmesi ile özellikle milli savunma, milli güvenlik, kamu güvenliği, kamu düzeni ve ekonomik güvenliğin kanun kapsamı dışında bırakıldığı geniş bir istisnalar listesi içermektedir. Soruşturma, kovuşturma ile yargılama ve infaz işlemleri istisna kapsamındadır. Bu konuya ilişkin hiçbir mevzuatın bulunmadığı önceki durumla kıyaslandığında bu kanun, bir ilerleme olduğuna işaret etmektedir. Ancak, bu kanun, özellikle kişisel verilerin kullanılmasını denetlemekten sorumlu makamın oluşumu ve işleyişine ilişkin hükümlerin bu kurumun tamamen bağımsız hareket etmesine yönelik güvenceler sağlamaması ve infaz mercileri ile yargı makamlarının faaliyetlerinin, kişisel verilerin korunması kurallarına riayet edilmesi yükümlülüğü çerçevesinde kapsama tam olarak dâhil edilmemesi nedeniyle hâlihazırdaki AB müktesebatı ile uyumlu değildir. Kişisel Verileri Koruma Kurumunun bağımsız bir şekilde hareket edebilmesini ve infaz mercilerinin faaliyetlerinin kanun kapsamına alınmasını sağlamak için, Türkiye, kişisel verilerin korunması mevzuatını AB müktesebatı ile uyumlu hale getirmelidir...." (Avrupa Komisyonu'nun 09.11.2016 tarihli, SWD(2016) 366 nihai sayılı AB Genişleme Politikasına İlişkin 2016 Türkiye Raporu, s. 71. - https://www.ab.gov.tr/files/pub/2016_ilerleme_raporu_tr.pdf, (erişim tarihi:19.11.2017)).

³²² Europol hakkında ayrıntılı bilgi için bk. <https://www.europol.europa.eu/about-europol> (erişim tarihi:19.11.2017).

³²³ Eurojust hakkında ayrıntılı bilgi için bk. <http://www.eurojust.europa.eu/about/background/Pages/History.aspx> (erişim tarihi:19.11.2017)

³²⁴ Bk. KVKK'nın 13. madde gerekçesi.

gerekçesinde, Tebligat Kanunu'nun 1. maddesinde³²⁵ sayılan kurum ve mercilerin bu madde bakımından yapacağı bildirimlerde Tebligat Kanunu hükümlerinin gözetileceğinin açık olduğu belirtilmiş ise de bu hususa kanunda yer verilmesinin daha doğru bir yaklaşım olacağı düşüncesindeyiz. Kararın kabul yönünde olması halinde veri öznesinin başkaca bir makama başvurusu veya işlem yapmasına lüzum bulunmayıp, talep veri sorumlusu tarafından yerine getirilecektir. Veri sorumlusuna başvuru, kurula şikayet bakımından ön koşul niteliğindedir.

Veri sorumlusuna yapılan başvurunun reddedilmesi, redde ilişkin gerekçenin yetersiz olması veya otuz günlük süre içerisinde cevap verilmemesi halinde veri öznesinin aynı hususta Kişisel Verileri Koruma Kurulu'na şikayet hakkı doğar. Ancak bu şikayet hakkının kullanılması, hak düşürücü süreye bağlanmış olup veri sorumlusunun cevabının öğrenilmesinin ardından otuz gün ve her halde başvuru tarihinden itibaren altmış gün geçtikten sonra aynı başvuruya ilişkin olarak kurula şikayette bulunulamaz. Bunun yanında kurulun görev alanına giren konularda ihlal iddiasını öğrenmesi durumunda resen inceleme yetkisi de bulunmaktadır.

Kurul, kendisine 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun'un 6. maddesindeki şartları taşıyan ihbar ve şikayetlere altmış gün içerisinde cevap vermediği takdirde veri öznesinin talebi reddedilmiş olacaktır. Şikâyet üzerine veya resen yapılan inceleme sonucunda, ihlalin varlığının anlaşılması hâlinde kurul, tespit ettiği hukuka aykırılıkların veri sorumlusu tarafından giderilmesine karar vererek ilgililere tebliğ edecek, tebliğ edilen bu karar, tebliğden itibaren gecikmeksizin ve en geç otuz gün içinde yerine getirilecektir. İlgililerin kurulun kararlarına karşı idari yargı yoluna başvurmaları mümkündür³²⁶.

Kanunun 14/3. maddesi uyarınca kişisel verilerinin işlenmesi nedeni ile kişilik hakkı ihlal edilenlerin genel hükümlere göre tazminat hakkının saklı olduğu belirtilmiştir. Her ne kadar veri sorumlusuna yapılacak başvurunun kurula yöneltilecek şikayet bakımından önkoşul olduğu belirtilmiş ise de genel hükümler uyarınca talep edilecek tazminat bakımından da

³²⁵ "Tebligatın yapılması:

Madde 1 – (Değişik : 11/1/2011-6099/1 md.) Kazaî merciler, 10/12/2003 tarihli ve 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanununa ekli (I) sayılı cetvelde yer alan genel bütçe kapsamındaki kamu idareleri, (II) sayılı cetvelde yer alan özel bütçeli idareler, (III) sayılı cetvelde yer alan düzenleyici ve denetleyici kurumlar, (IV) sayılı cetvelde yer alan sosyal güvenlik kurumları ile vakıf yükseköğretim kurumları, il özel idareleri, belediyeler, köy hükûmî şahsiyetleri, barolar ve noterler tarafından yapılacak elektronik ortam da dâhil tüm tebligat, bu Kanun hükümlerine göre Posta ve Telgraf Teşkilatı Genel Müdürlüğü veya memur vasıtasıyla yapılır."

³²⁶ Korkmaz, 2016: 139.

öncelikle veri sorumlusuna başvurunun gerekli olup olmadığı konusunda kanunda bir açıklık bulunmamaktadır. Anılan maddenin gerekçesinde yer verilen;

“Başvuru yoluna gitmenin zorunlu, şikâyet yoluna gitmenin ise ihtiyari olması sebebiyle, başvurusu zımnen veya açıkça reddedilen ilgili kişinin bir yandan Kurula şikâyetle bulunabilmesi, diğer yandan doğrudan adli veya idari yargı yoluna gidebilmesi mümkün olacaktır. Ancak, ilgililerin masrafsız ve daha hızlı sonuç alınması mümkün olan şikâyet yolunu tercih edecekleri değerlendirilmektedir.”

biçimindeki görüş ile hükmün kanun sistematigi içerisindeki yeri nazara alındığında tıpkı kurula şikâyet gibi, tazminat davasının da veri sorumlusuna başvuru önkoşuluna bağlandığı söylenebilir.

Veri öznesinin, kişilik hakkı ihlali nedeni ile doğan zararının tazmini bakımından hakkı ihlal eden veri sorumlusunun gerçek veya özel hukuk tüzel kişisi olması halinde Türk Medeni Kanunu’nun ilgili hükümlerince tazminat davası açılabileceği konusunda kuşku bulunmamaktadır. Bunun yanında, idarenin işlemleri kapsamında kanuna uygun olarak gerçekleştirilmeyen veri işleme faaliyetinin ve idare eliyle işlenen kişisel verilerin güvenliğinin sağlanamaması nedeni ile kişilik hakkının ihlal edilmesi halinde tam yargı davası açılabilmesi de mümkündür³²⁷.

İdare tarafından kamu hizmetinin sağlıklı yürütülebilmesi için muhafazası gerekli olan kişisel verilerin muhafaza edilmemesi³²⁸, eksik ya da yanlış tutulması³²⁹, kişisel verilerin veri

³²⁷ Korkmaz, 2016: 138. E-devlet, MERNIS projesi gibi sistemler aracılığı ile kişisel verilerin devlet tarafından işlenmesi sonucunda TC kimlik numarası, adı, soyadı, ana adı, baba adı ve doğum tarihi bir çeşit çilingir vazifesi gördüğü ve böylelikle kişi ile ilgili devlet tarafından işlenen bütün verilere kolaylıkla ulaşılabilir olması nedeni ile güvenlik endişeleri dile getirilmektedir. (Ketizmen ve Ülküderner, 207: 190)

³²⁸ “...olayda, davacıya ait röntgenlerin hasta dosyası içerisinde yer almaması ve idare tarafından ibraz edilememesi hizmet kusurunu oluşturduğundan yapılan tıbbi müdahalenin irdelenme imkânını ortadan kaldırdığı, tıbbi müdahalenin irdelenmemesine yol açan grafiklerin saklanmaması şeklindeki hizmet kusuru sonucu davacıların mevcut belirsizlikten dolayı duyduğu üzüntü ve sıkıntıların kısmen de olsa giderilebilmesi için mahkemece takdir edilecek manevi tazminatın ödenmesi gerektiği...” Danıştay 10.D., 27.12.2011, E:2009/9151, K: 2011/5976.

³²⁹ “...davacının, hakkında uygulanan tedavileri ve zararlı sonucun sebebini öğrenmesine yarayacak tıbbi kayıtların noksan olması, dolayısıyla maddi gerçeğe (rahatsızlığının nedenine) hiçbir zaman ulaşamayacak ve ömür boyu şüphe duyacak olması nedeniyle uğradığı manevi zararının tazmini gerektiği...” Danıştay 10.D., 9.7.2012, E:2010/111, K: 2012/3358

öznesinin rızası olmaksızın üçüncü kişilere açıklanması³³⁰ tam yargı davalarına konu edilmiş ve Danıştay tarafından idarenin bu eylemleri sonucunda davacıların kişilik haklarının ihlal edilmesin durumunda hizmet kusurunun bulunduğu hükmedilmiştir³³¹.

Kanun'un 18. maddesi ile kanunda yer alan birtakım yükümlülüklerin gerçek kişi veya özel hukuk tüzel kişisi olan veri sorumluları tarafından yerine getirilmemesi hali idari yaptırıma bağlanmıştır. Söz konusu yükümlülüklerin kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları bünyesinde işlenmesi durumunda ise ilgili kamu kurum ve kuruluşunda görev yapan memurlar ve diğer kamu görevlileri ile kamu kurumu niteliğindeki meslek kuruluşlarında görev yapanların disiplin sorumluluğu gündeme gelecektir.

Buna göre idari para cezası verilmesini gerektiren ihlaller; aydınlatma yükümlülüğünün yerine getirilmemesi, veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi, kurul tarafından verilen kararların yerine getirilmemesi ile veri sorumluları siciline kayıt ve bildirim yükümlülüğünün yerine getirilmemesidir. Bu ihlaller yönünden 5.000 Türk Lirası ile 1.000.000 Türk Lirası arasında değişen idari para cezaları öngörülmüştür. İdari para cezalarının alt ve üst sınırı arasındaki farkın kabahatin haksızlık içeriği, failin ekonomik durumu ve kusurunun nazara alınarak hakkaniyetin sağlanması amacına hizmet etmesi bakımından bilinçli olarak öngörüldüğü belirtilmektedir³³². Verilen idari para cezasına ilişkin karara karşı idari yargı yoluna başvurulması mümkündür.

Kanun'un 20. maddesi ile, kişisel verilerin korunması bakımından uygulamaları ve mevzuattaki gelişmeleri takip etmek, değerlendirme ve önerilerde bulunmak, araştırma ve incelemeler yapmak veya yaptırmak; ihtiyaç duyulması hâlinde, kişisel verilerin korunması bağlamında kamu kurum ve kuruluşları, sivil toplum kuruluşları, meslek örgütleri veya üniversitelerle iş birliği yapmak; kişisel verilerle ilgili uluslararası gelişmeleri izlemek ve değerlendirmek, görev alanına giren konularda uluslararası kuruluşlarla iş birliği yapmak,

³³⁰ "...olayda, davacılar yakınının Devlet Hastanesinde yapılan ve pozitif çıkan HIV testinin sonucunun, davacıların yakını da dahil olmak üzere doğrulama testi yapılmadan hiç kimseye açıklanmaması ve ilgilinin doğrulama testi için bir üst basamak sağlık kuruluşuna sevkı gerekirken, laboratuvar teknisyeni tarafından doğrulama testi yapılmadan önceki aşamada pozitif çıkan test sonucunun açıklanmasının neden ve etkisiyle davacılar yakını intihar etmek suretiyle yaşamını yitirdiği, dava konusu olayın oluş şekli, hastalığın niteliği ve özelliği dikkate alındığında, davacılar yakınının idarenin ağır hizmet kusurunun neden ve etkisiyle intihar etmek suretiyle yaşamını yitirmesi sonucunda doğan zarar ile idari faaliyet arasında uygun nedensellik bağı bulunduğu..." Danıştay 10.D., 28.12.2005, E:2005/8407, K: 2007/6526.

³³¹ Akgül, 2013: 35.

³³² Bk. KVKK'nın 18. madde gerekçesi.

toplantılara katılmak ile yıllık faaliyet raporunu Cumhurbaşkanlığına, Türkiye Büyük Millet Meclisi İnsan Haklarını İnceleme Komisyonuna ve Başbakanlığa sunmak görevlerini yerine getirmek üzere, merkezi Ankara’da olan, idari ve mali özerkliğe sahip ve kamu tüzel kişiliğini haiz Kişisel Verileri Koruma Kurumu kurulmuştur. Kurumun Başbakanlıkla ilişkili olduğu belirtilmiştir³³³.

Kanun’un 21. maddesi ile Kişisel Verileri Koruma Kurulu düzenlenmiş olup kurulun bu Kanunla ve diğer mevzuatla verilen görev ve yetkilerini kendi sorumluluğu altında, bağımsız olarak yerine getireceği ve kullanacağı belirtilmiştir.

1.4.3. Ceza Hukuku

Kişisel verilerin işlenmesi hususunun, etkileri ve sonuçları bakımından birçok hukuk dalını ilgilendirmesi nedeni ile buna ilişkin usul ve esaslar pek çok ülkede özel bir kanunla düzenlenmiştir³³⁴. Ulusal ve uluslararası düzenlemelerde yer alan, veri işleyenin sorumluluklarına ilişkin ilkeleri oluşturan bu usul ve esaslara uyulmadan kişisel verilere yönelik olarak gerçekleştirilen kaydetme, verme, ele geçirme ve yok etmeme biçimindeki eylemler suç olarak kabul edildiğinden, ceza hukuku alanında sonuç doğurmaktadırlar. Örneğin dürüst ve hukuka uygun işleme ile amaçla bağlılık ilkelerinin ihlal edilmesi anlamına gelen, kişisel verinin hukuka aykırı olarak kaydedilmesi Türk Ceza Kanunu’nun 135. maddesinde, ele geçirilmesi, başkasına verilmesi ve yayılması 136. maddesinde suç olarak düzenlenmiştir³³⁵.

6698 sayılı KVKK’nın yürürlüğe konmasındaki öncelikli amacın bu konuda özel bir kanunun bulunmamasının TCK’da cezai müeyyideye tabi tutulan kişisel verilerin işlenmesi kapsamındaki birtakım fiillerin hangi hallerde hukuka uygun, hangi hallerde hukuka aykırı olduğunun belirlenmesinde yaşanan sorunların ortadan kaldırılması olduğu ifade edilmektedir³³⁶. Bununla birlikte, KVKK’nın kapsamı “kişisel verileri işlenen gerçek kişiler

³³³ Burada ilişkili olma kavramı, kurumun bağımsız idari otorite olma vasfına işaret etmekte ve Başbakanlıkla kurum arasında idari bütünlüğün sağlanması amacına hizmet etmekte olup “bağımsız sözcüğü organik ve işlevsel anlamda yürütme organı karşısında kurumun bağımsızlığını; idari sözcüğü ayrı kamu tüzel kişilikleri olsun olmasın idari organ niteliğinde olduklarını, “otorite sözcüğü de bunların danışma organı değil, düzenleyici veya birel idari icrai kararlar alıp uygulayan kuruluşlar olduğunu göstermektedir.” (Tan, 2002: 15)

³³⁴ Ketizmen, 2008: 191.

³³⁵ Ketizmen, 2008: 206.

³³⁶ “Ülkemizde kişisel verilerin korunmasını sağlayacak bir kanunun yürürlüğe girmesini gerektiren değişik sebepler bulunmaktadır. Öncelikle, 5237 sayılı Türk Ceza Kanununun 135 ve devamı maddelerinde, kişisel verilerin hukuka aykırı olarak elde edilmesi, kaydedilmesi veya ifşa edilmesi fiilleri suç olarak düzenlenmiş ve yaptırıma bağlanmıştır. Bununla birlikte, kişisel verilerin işlenmesine yönelik özel bir kanunun

ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler” ile sınırlandırılmıştır ve 17. maddesi ile kişisel verilere ilişkin suçlar yönünden 5237 sayılı Türk Ceza Kanunu'nun 135 ila 140. maddelerine atıf yapılmıştır. Ancak her ne kadar kişisel veri olma niteliğinin değişmemesi nedeni ile TCK'da düzenlenen kişisel verilerin hukuka aykırı olarak kaydedilmesi, verilmesi, yayılması ve ele geçirilmesi ile yok edilmemesi suçları bakımından suçun konusunu oluşturabilirler ise de KVKK'nın, bir veri kayıt sisteminin parçası olarak işlenmeyen kişisel veriler bakımından uygulama alanı bulmadığı belirtilmiştir³³⁷. Kanunkoyucunun, kişisel verilerin hukuka uygun olarak işleme ilkelerini düzenleyen bir düzenlemede dahi hukuka aykırı olduğu belirtilmeyen ve idari yaptırıma tabi tutulmayan birtakım eylemlerin ceza kanunu ile cezalandırılmasını öngören bu tutumu kendi içerisinde bir çelişki barındırmaktadır.

1.4.3.1. 5237 sayılı TCK'da Yer Alan Düzenlemeler

1.4.3.1.1. Kaydetme

Kişisel verilerin korunmasına yönelik olarak Türk Ceza Kanunu'nda yer verilen ilk düzenleme, kişisel verilerin kaydedilmesi suçudur. Kanunun 135. maddesinde yer alan suç tipi aşağıda ayrıntılı olarak açıklanmış bulunduğundan burada ayrıca değinilmemiştir.

1.4.3.1.2. Verme, Yayma veya Ele Geçirme

Türk Ceza Kanunu'nun 136. maddesi, “verileri hukuka aykırı olarak verme veya ele geçirme” suçunu düzenlemektedir. Buna göre, “*Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır.*”

Veri sözcüğü ile kişisel veri kavramı arasındaki anlam farklılığı karşısında madde başlığının madde içeriği ile örtüşmemesi³³⁸, bunun yanında madde başlığında yalnızca “verme

bulunmaması sebebiyle, bu fillerin ne zaman hukuka aykırı, ne zaman hukuka uygun olduğunun belirlenmesinde tereddütlerin yaşandığı görülmektedir.” Bk. 6698 sayılı kanunun genel gerekçesi.

³³⁷ Bk. KVKK'nın 2. madde gerekçesi.

³³⁸ Veri kelimesi, “*bir araştırmamanın, bir tartışmanın, bir muhakemenin temeli olan ana öge, muta, done*” anlamını taşımaktadır.

(http://www.tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.5b1a3ad4a0bf70.77987302 (erişim tarihi:08.06.2018)). Aynı yönde bkz.Karagülmez, 2005: 233.

ve ele geçirme” fiillerine yer verilmiş iken, madde metninde “veren, yayan ve ele geçiren” ibaresinin kullanılmış olması³³⁹ nedenleri ile söz konusu düzenleme eleştirilmektedir.

Bu suç tipi bakımından korunan hukuki yarar, tıpkı kişisel verilerin kaydedilmesi suçunda olduğu gibi, kişinin özel yaşamının gizliliğidir³⁴⁰. Kişinin kendisi hakkındaki verilerin geleceğini kontrol edebilmesi bakımından bu verilerin yetkisiz üçüncü kişilere verilmesi, yayılması veya bu kişiler tarafından ele geçirilmesi eylemleri suç olarak tanımlanmıştır³⁴¹. Suçun konusu, kişisel veridir³⁴².

Maddede suçun faili “*hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi*” olarak ifade edildiğinden, söz konusu suç herkes tarafından işlenebilir. Öte yandan, kişisel verinin, KVKK’nın 3. maddesinin 1. fıkrasının (d) bendinde “*Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi*” olarak tanımlanmış olması karşısında suçun mağduru ancak gerçek kişiler olabilir.

TCK’nın 136. maddesindeki suç tipi; vermek, yaymak ve ele geçirmek eylemlerinden ibaret olmak üzere seçimlik hareketli bir suç olup bu hareketlerin gerçekleştirilmesi ile suç tamamlanmış bulunmaktadır³⁴³. Ayrıca, bu hareketlerin gerçekleştirilmesi neticesinde herhangi bir zararın doğup doğmadığına bakılmaksızın suçun tamamlandığı kabul edilir, bu anlamda suç soyut tehlike suçudur³⁴⁴. Suçun, kişisel verilerin başkasına verilmesi seçimlik hareketi ile gerçekleştirilmesi halinde madde metninde yer alan “başkası”, gerçek veya tüzel kişi olabilecektir³⁴⁵. Vermek eylemi, *üzerinde, elinde veya yakınında olan bir şeyi birisine eriştirmek, iletme*³⁴⁶ biçiminde tanımlanmakta olup elden veya posta ve e-posta vasıta kılınmak sureti ile bir başkasına aktarılması şeklinde gerçekleşebilir³⁴⁷. Bunun yanında Yüksek Mahkeme bir kararında, kişisel verinin gerektiğinde hukuka uygun olarak o veriyi elde edebilecek bir makama verilmesi halinde bu suçun oluşmayacağına hükmetmiştir³⁴⁸.

³³⁹ Özbek vd., 2016: 579.

³⁴⁰ Özbek vd., 2016: 577; Karagülmez, 2005: 233.

³⁴¹ Ketizmen, 2008: 239.

³⁴² Özbek vd., 2016: 577.

³⁴³ Özbek vd., 2016: 578-579; Akdağ, 2013: 129.

³⁴⁴ Özbek vd., 2016: 579; Akdağ, 2013: 129.

³⁴⁵ Yargıtay CGK, 2012/12-1510 Esas, 2014/331 Karar, 17.06.2014.

³⁴⁶ http://www.tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.5a52a1da2b7375.284907 21 (erişim tarihi:07.01.2018).

³⁴⁷ Yargıtay CGK, 2012/12-1510 Esas, 2014/331 Karar, 17.06.2014.

³⁴⁸ “...incelenen dosya kapsamına göre; evli olan sanık ile katılanın boşanmalarını müteakip, katılana yoksulluk nafakası ödemeye başlayan sanığın, katılanın annesinin ölümüne bağlı olarak babasından dolayı aldığı yetim aylığında yükselme olabileceğini düşünüp, katılana ait T.C. kimlik numarası ve diğer kişisel bilgileri kullanarak,

Yaymak eylemi ise, *birçok kimseye duyurmak*³⁴⁹ olarak ifade edilir. Burada, kişisel verinin ulaşılabilir kılınması esastır³⁵⁰. Kişisel verileri bir internet sitesinde, yazılı veya görsel medyada yayınlamak, birçok kişiye elektronik posta ya da telefon aracılığı ile kısa mesaj gönderme, yayma hareketine örnek verilebilir³⁵¹. Seçimlik hareketlerden gerek vermek, gerekse yaymak biçiminde gerçekleşen fiiller esasen aktarma amacına hizmet eder ve her ne kadar kişisel verinin yayılması biçimindeki eylem, söz konusu kişisel verinin bir kişiye verilmesi eylemini de kapsamakta ise de bu durumda aynı anda gerçekleşen iki seçimlik hareket bakımından iki ayrı suç değil, tek suçun varlığı kabul edilmelidir³⁵². Fakat yayma eylemi ile gerçekleştirilen suç bakımından; kişisel verinin kulaktan kulağa aktarılmasından ziyade, bir araç kullanılmak sureti ile gerçekleştirilmesi gerektiği savunulmaktadır³⁵³. Suçun, kişisel verinin verilmesi veya yayılması suretiyle işlenmesi halinde, kişisel verinin üçüncü kişi veya kişiler tarafından öğrenilebilir hale getirilmesi yeterlidir, ayrıca bu verilerin öğrenilip öğrenilmemesi veya algılanıp algılanmamasının bir önemi bulunmamaktadır³⁵⁴.

Ceza kanununda düzenlenen bir suçun kural olarak icrai hareket ile işlenmesi öngörülmüş olsa da failin neticenin ortaya çıkmasını istemesi nedeni ile hareketsiz kalması sonucunda neticenin meydana gelmesi halinde gerçek olmayan ihmal suçları veya garantörsel ihmali suç olarak da adlandırılan ihmal sureti ile icra suçu söz konusu olur³⁵⁵.

Sosyal Güvenlik Kurumunun internet sitesine giriş yapıp, katılanın emekli aylık bilgisini sorguladığı ve sorgulama sonucunda elde ettiği internet çıktısını yoksulluk nafakasının kaldırılması talebiyle katılan aleyhine açtığı dava dosyasına delil olarak sunduğu iddia ve kabulüne konu olayda;

Şikayete konu internet çıktısını, gerektiğinde belge aslını temin edebilecek olan mahkeme dışında, üçüncü kişi ya da kişilerle paylaştığı ve/veya çoğaltarak dağıttığına ilişkin hakkında bir iddia ileri sürülmeyen sanığın, katılanın ekonomik durumunu delillendirerek, ilgili mahkeme tarafından, yoksulluk nafakasının kaldırılmasını sağlama amacını taşıyan eylemlerinde, hukuka aykırı hareket ettiği bilinciyle davrandığı kabul edilemeyeceğinden, atılı verileri hukuka aykırı olarak verme veya ele geçirme suçundan sanık hakkında CMK'nın 223/2-a maddesi gereğince beraat kararı verilmesi gerekirken, yasal ve yeterli olmayan yazılı gerekçelerle sanığın mahkumiyetine karar verilmesi, Kanuna aykırı olup..." Yargıtay 12. C.D. 2014/4939 Esas, 2014/19493 Karar, 13.10.2014.

³⁴⁹http://www.tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.5a52a1df446320.54135011 (erişim tarihi:07.01.2018)

³⁵⁰ Akdağ, 2013: 131.

³⁵¹ Yargıtay CGK, 2012/12-1510 Esas, 2014/331 Karar, 17.06.2014.

³⁵² Özbek vd., 2016: 578.

³⁵³ Özbek vd., 2016: 578; aksi görüş için bk. Akdağ, 2013:130.

³⁵⁴ Akdağ, 2013:130-131; Aydın, 2013: 20.

³⁵⁵ Hakeri, 2007: 141.

Kişisel verileri verme suçunun esasen kanunda icrai bir suç olarak düzenlenmiş olmasına karşın, ihmali olarak da işlenebileceği; örneğin hekimin hasta dosyalarını başkasının görebilmesi için özellikle açıkta bırakması halinde suçun ihmal sureti ile oluşacağı savunulmakta ise de aksi görüşte olan yazarlar da bulunmaktadır³⁵⁶.

TCK'nın 136/1. maddesinin, *“Bu madde hükmü ile hukuka uygun olarak kaydedilmiş olsun veya olmasın, kişisel verileri hukuka aykırı olarak başkalarına vermek, yaymak veya ele geçirmek, bağımsız bir suç olarak tanımlanmıştır.”* şeklindeki gerekçesinden de anlaşılacağı üzere, kişisel verilerin, “verildiği”, “yayıldığı” veya “ele geçirildiği”nin kabul edilebilmesi için, kişisel verilerin kaydedilmiş halde bulunması, kaydedilmiş haliyle başkalarına verilmesi, yayılması ya da ele geçirilmesi gerekir³⁵⁷.

Yargıtay 12. Ceza Dairesi’ne göre kişisel verilerin kaydedilmeden, hafızada tutulması sureti ile üçüncü kişiler ile paylaşılması halinde bu eylem TCK madde 136’da düzenlenen suç tipi kapsamında değerlendirilmez; ancak TCK madde 134/1’de düzenlenen özel hayatın gizliliğini ihlal suçu kapsamında incelenebilir³⁵⁸. Bu görüş, Yargıtay’ın önceki içtihatları ile uyumludur ve kişisel verinin kanunun aradığı şekilde kaydedilip kaydedilmemesinin suçun tipikliğine etkisine ilişkin bir belirlemedir; ancak somut olayın değerlendirilmesinde verinin aktarıldığı üçüncü kişinin bu veriyi kayıt altına alıp almaması gibi esasen kanun metninde yer almayan bir hususa daha yer verildiği görülmektedir: *“...somut olayda; sanık ile katılanın resmi nikahlı evli olup aralarında boşanma davası bulunduğu, sanığın kendi adına kayıtlı olan ve katılan tarafından kullanılan cep telefonu hattının geçmişe ait ayrıntılı görüşme dökümlerini içerir HTS raporlarının GSM şirketinden talep ettiği ve gönderilen bu dökümleri katılanın akrabası olan tanık Tamer'e gösterdiği iddia edilen olayda; katılanın kim ile ne zaman, hangi sıklıkla, hangi süreyle görüştüğüne ilişkin görüşme dökümlerini içerir HTS raporları kişisel veri kapsamında olup, sanığın, kişisel veri niteliğindeki HTS raporlarını hukuka uygun bir şekilde elde etmesine rağmen, tanık Tamer'e göstererek tanığın duyu organları aracılığıyla katılanın kişisel verilere vakıf olmasına neden olan sanığın eyleminin TCK'nın 134/1. maddesinin 1. cümlesinde düzenlenen özel hayatın gizliliğini ihlal suçunu oluşturduğu ve bu suçtan sorumlu tutularak cezalandırılmasına karar verilmesi gerektiği gözetilmeden, suçun nitelendirilmesinde yanılgiya düşülerek yazılı şekilde hüküm kurulması...”. Yukarıda da değinildiği üzere, kaydedilmiş halde bulunan kişisel verinin üçüncü bir kişi tarafından öğrenilmesi imkanı yaratıldığı anda kişisel verilerin verilmesi veya*

³⁵⁶ Hakeri, 2012: 760.

³⁵⁷ Ketizmen, 2008: 240. Yargıtay 12. CD. , 2013/25397 E., 2014/13374 K., 02.06.2014

³⁵⁸ Yargıtay 12. C.D. , 2017/405 Esas, 2017/9460 Karar, 27.11.2017.

yayılması biçimindeki suç tamamlanmış olacağından Daire'nin kanaatine katılmak mümkün görünmemektedir.

6698 sayılı KVKK'nın 8. ve 9. maddelerinde yer verilen "kişisel verilerin aktarılması" kavramına da kişisel verilerin hukuka aykırı olarak verilmesi ve yayılması suçları bağlamında değinmekte fayda bulunmaktadır. Zira aktarma faaliyeti, kişisel verilerin işleme biçimlerinden biri olup kural olarak yurt içinde veri öznesinin açık rızasının bulunması durumunda veya aynı kanunun 5. ve 6. maddelerinde düzenlenen, veri öznesinin açık rızasının bulunmaması durumunda dahi kişisel verilerin işlenmesinin mümkün olduğu durumlarda hukuka uygun bir şekilde gerçekleştirilebilmektedir. Söz konusu kişisel verilerin yurtdışına aktarılabilmesi için ise kişisel verilerin aktarılacağı ülkede yeterli düzeyde korumanın bulunması veya bu düzeyde koruma bulunmasa dahi Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kişisel Verileri Koruma Kurulu'nun izninin bulunması gerekir³⁵⁹. Hangi ülkelerde yeterli düzeyde koruma bulunduğu, kurul tarafından ilan edilmesi gerekmekte olup henüz bu ülkeler ilan edilmemiştir. Aktarma, kişisel verilerin üçüncü kişilere verilmesi, paylaşılması, iletilmesi, transfer edilmesi, yayılması biçiminde olabilir. Bu nedenle, kişisel verilerin yurt içinde ya da yurtdışına KVKK'da öngörülen haller dışında ve usule aykırı olarak aktarılması durumunda bu eylem TCK'nın 136. maddesinde düzenlenen kişisel verileri hukuka aykırı olarak verme ve yayma suçu kapsamında cezalandırılacaktır³⁶⁰.

Ele geçirme deyimi ise bir şeyin sahibi olmak anlamına gelir³⁶¹. Buradan hareketle, kişisel verileri ele geçirme biçimindeki seçimlik hareket, olağan koşullarda ulaşılabilir bir alanda bulunmayan kişisel verilere fail tarafından hukuka aykırı olarak hakim olunması olarak tanımlanır³⁶². Failin bu kişisel veriler üzerinde hakimiyet kurabilmek adına bir çaba göstermiş

³⁵⁹ Benzer bir düzenleme 95/46/AT sayılı Yönerge'nin 25. maddesinde de öngörülmüştür. Buna göre, kişisel verilerin Avrupa Birliği üyesi ülkelerin haricinde bir ülkeye aktarılabilmesi için aktarılabilecek ülkede de kişisel verilerin Avrupa Birliği mevzuatına uygun ve yeterli düzeyde korunması gerekmektedir. Hangi ülkelerde yeterli düzeyde koruma bulunduğu Avrupa Komisyonu karar vermektedir. Şimdiye kadar; Andora, Arjantin, Kanada, Faroe Adaları, Guernsey, İsrail, Man Adası, Jersey, Yeni Zelanda, İsviçre ve Uruguay'ın yeterli düzeyde koruma sağladığına karar verilmiştir. Ayrıntılı bilgi için bk. http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm (erişim tarihi:11.01.2018)

³⁶⁰ Korkmaz, 2016: 123.

³⁶¹ http://www.tdk.gov.tr/index.php?option=com_atasozleri&arama=kelime&guid=TDK.GTS.5a5535fb983336.45403033 (erişim tarihi: 07. 01 2018)

³⁶² Akdağ, 2013: 135. Kişisel verilerin hukuka aykırı olarak ele geçirilmesi suçuna Danıştay'ın 21.04.2015 tarihli kararına konu olan olay örnek gösterilebilir: "*Dava dosyasının incelenmesinden, Trabzon İli Sürmene İlçe Adliyesi'nde zabıt katibi olarak görev yapan davacı tarafından eşi ile ilgili bir takım şüpheleri üzerine eşinin cep*

olması gerekmektedir³⁶³. Öğretide, kişisel verilerin yalnızca içeriğinin öğrenilmesi durumunda da suçun oluşacağı savunulmakta³⁶⁴ ise de Yargıtay'ın kişisel verilerin hukuka aykırı olarak ele geçirilmesi suçunu

*“...kişisel verilerin, üzerinde yazılı olduğu belgenin bulunduğu yerden alınması ya da kaydedilmiş haliyle başka bir nesne üzerine taşınarak (örneğin; yazının başka bir kağıt, defter vb. nesne üzerine geçirilmesi, taşınabilir belleğe veya CD'ye aktarılması gibi işlemlerle) sabitlenmesi, böylece istenildiğinde tekrar kullanılabilmesi olanağını sağlayan her türlü faaliyet, kişisel verileri “ele geçirme” kapsamında değerlendirilebilir”*³⁶⁵

biçiminde tanımlaması karşısında yalnızca verinin öğrenilmesi ile suçun tamamlanmış kabul edilemeyeceği görüşünde olduğu anlaşılmaktadır.

1.4.3.1.3. Yok Etmeme

Türk Ceza Kanunu'nda kişisel verilere ilişkin yer verilen diğer bir düzenleme ise “verileri yok etmeme” suçudur. 138. maddede bulunan söz konusu düzenlemeye göre; “kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde bir yıldan iki yıla kadar hapis cezası verilir.”

Madde metni ile madde başlığı arasında tıpkı 136. maddede olduğu gibi terimsel olarak bir uyumsuzluk söz konusudur. Zira madde içeriği sistem içerisinde bulunan kişisel verilerin yok edilmemesi iken başlığında yalnızca “verileri yok etmeme” ifadesi kullanılmıştır. Öte yandan, 135. ve 136. maddelerde suçun konusu olan kişisel veriler bakımından otomatik işleme ile otomatik olmayan işleme arasında herhangi bir ayırım yapılmamıştır. Oysa yok etmeme biçiminde gerçekleşen suç bakımından kişisel verinin “sistem içinde” bulunmasının bu verilerin otomatik işleme usulü ile yani bilişim sistemi içerisinde yer alması anlamına geldiğinin kabulü halinde diğer maddeler ile arasında çelişki

telefonuyla yaptığı görüşmeleri tespit etmek amacıyla gerçek olmayan bir soruşturma numarası vererek 09.06.2008 ve 11.06.2008 tarihlerinde Telekomünikasyon İletişim Başkanlığı'na müzekkere yazdığı, yazmış olduğu bu müzekerelerin Cumhuriyet Savcısı tarafından imzalandığı ve telefon görüşmelerinin bu suretle temin edildiği;” (Danıştay 16. D., 2015/9697 Esas, 2015/1941 Karar).

³⁶³ Akdağ, 2013: 135.

³⁶⁴ Akdağ, 2013: 136.

³⁶⁵ Yargıtay 12. C.D. 2015/10737 Esas, 2016/13557 Karar, 21.12.2016.

ortaya çıkmaktadır³⁶⁶. Bu durum, otomatik olmayan yollarla işlenen kişisel verilerin kişisel verilerin işlenmesine egemen olan *ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme* prensibinin bir gereği olarak öngörülen bu cezai yaptırımın sağladığı hukuki korumadan mahrum kalması sonucu doğurmaktadır.

Kişisel verilerin işlenmesi faaliyeti belirli bir amaç doğrultusunda gerçekleştirilmekte olup bu faaliyetin hizmet ettiği amacın ortadan kalkması halinde artık veri işlemenin meşruiyetinden de söz edilemez³⁶⁷. Başlangıçta hukuka uygun halde işlenen (kaydedilen, depolanan, üçüncü kişilere aktarılan, vs.) kişisel verilerin yok edilmesi bakımından kanunda öngörülen süreler içerisinde yok edilmemesi halinde kişisel verileri yok etmeme suçu oluşur³⁶⁸. Burada korunan hukuki değer, kişinin özel hayatının gizliliğidir³⁶⁹. Konusu sistem içerisinde kayıtlı bulunan kişisel veriler olan söz konusu suçu, kamu görevlisi olup olmamasına bakılmaksızın yalnızca verileri sistem içerisinde yok etmekle yükümlü olan kişi işleyebilir. Başka bir anlatımla kişisel verileri yok etmeme suçu bir özgü suçtur³⁷⁰. Suçun mağduru ise ancak sistemde kayıtlı verisi bulunan kişiler olabilir³⁷¹.

Kişisel verileri yok etmeme suçu, kanunun belirli bir hareketin gerçekleştirilmemesi durumunu müeyyideye tabi tuttuğu hallerde söz konusu olan, ihmali suçlardandır³⁷². Yok etmek; imha etmek, silmek, ortadan kaldırmak biçiminde olabileceği gibi³⁷³, anonimleştirme şeklinde de gerçekleştirilebilir³⁷⁴. Fakat verilerin takma adlar altında toplanması (*pseudonymisation*) ile yok etme yükümlülüğünün ortadan kalktığı söylenemez. Zira kişisel verilerin yok edilmesi suçunun kişinin özel hayatının gizliliğinin korunması amacına hizmet ettiği nazara alındığında, yok etme eyleminin verinin tümüyle erişilemez ve tekrar kullanılamaz hale getirilmesinin yanında veri ile veri öznesi arasındaki bağlantının koparılması, o verinin kullanılarak veri öznesinin kimliğinin belirlenebilme ihtimalinin ortadan kaldırılması olarak anlaşılması gerekir. Ancak burada yok etme yükümlülüğünün doğması için kanunda öngörülmüş sürenin dolması gerektiği ve buradaki kanun ifadesinden

³⁶⁶ Ketizmen, 2008: 242; Yaşar, Gökcan ve Artuç, suçun otomatik olmayan yollarla işlenen kişisel veriler bakımından da söz konusu olabileceği kanaatindedirler, bk. Yaşar ve diğerleri, 2014: 4464.

³⁶⁷ Ketizmen, 2008: 240.

³⁶⁸ Bk. madde gerekçesi.

³⁶⁹ Özbek vd., 2016: 582.

³⁷⁰ Akdağ, 2013: 144; Özbek vd., 2016: 582.

³⁷¹ Özbek vd., 2016: 582.

³⁷² Akdağ, 2013: 145; Özbek vd., 2016: 582.

³⁷³ Yaşar vd., 2014: 4463.

³⁷⁴ Ketizmen, 2008: 241; Akdağ, 2013: 148.

gerek maddi ve gerekse şekli hukuk kurallarının kast edildiği unutulmamalıdır; bu durumda, yok etme yükümlülüğü idarenin düzenleyici işlemi ile de kişisel verilerin yok edilmesi yükümlülüğü yüklenebilir³⁷⁵. Verileri yok etmekle yükümlü kişinin kanunun belirlediği sürenin geçmiş olduğu anda kişisel verileri yok etmemiş olması ile suç tamamlanmakla suçun oluşumu için herhangi bir zarar doğması da şart olmadığından suç, soyut tehlike suçudur³⁷⁶.

KVKK'nın 7. maddesi ile “kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesi” düzenlenmiş bulunmaktadır³⁷⁷. O halde kişisel verilerin yok edilmesine ilişkin diğer kanunlarla getirilen özel hükümler yanında kişisel verilerin işlenmesini gerektiren sebeplerin ortadan kalkması halinde veri sorumlusuna kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğü yüklenmektedir. Aynı kanunun 17. maddesinin 2. fıkrasında, bu kanunun 7. maddesi hükmüne aykırı olarak; kişisel verileri silmeyen veya anonim hâle getirmeyenlerin TCK'nın 138. maddesine göre cezalandırılacağı öngörülmüştür. Hal böyle iken, kişisel verilerin kanunlarda belirli bir sürenin dolması halinde silinmesi yükümlülüğü yanında, kişisel verinin işlenme amacının ortadan kalkmış olması durumu da bu suçun kapsamına alınmış bulunmaktadır. Bununla birlikte, kişisel verilerin yok edilmesi, silinmesi ve anonim hale getirilmesine ilişkin usul ve esasları düzenleyen “Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik³⁷⁸”, 28.10.2017 tarihli ve 30224 sayılı Resmi Gazete’ de yayınlanarak 01.01.2018 tarihi itibarıyla yürürlüğe girmiştir.

TCK'nın 138. maddesine 21.02.2014 tarihli 6526 sayılı Kanun'un 5. maddesi ile eklenen 2. fıkra ile suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması hâli, ağırlaştırıcı neden olarak düzenlenmiştir. Bu duruma kişisel veri niteliğindeki; CMK'nın 75. ve 76. maddeleri uyarınca bir suça ilişkin delil elde etme amacı ile şüpheli, sanık veya mağdurun üzerinde iç beden

³⁷⁵ Akdağ, 2013: 146; Özbek vd., 2016: 583.

³⁷⁶ Özbek vd., 2016: 584.

³⁷⁷ *Kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesi*

MADDE 7- (1) Bu Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir.

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

(3) Kişisel verilerin silinmesine, yok edilmesine veya anonim hâle getirilmesine ilişkin usul ve esaslar yönetmelikle düzenlenir.

³⁷⁸ [http://www.resmigazete.gov.tr/main.aspx?home=http://www.resmigazete.gov.tr/eskiler/2017/10/20171028.htm](http://www.resmigazete.gov.tr/main.aspx?home=http://www.resmigazete.gov.tr/eskiler/2017/10/20171028.htm&main=http://www.resmigazete.gov.tr/eskiler/2017/10/20171028.htm) (erişim tarihi: 10.01.2018)

muayenesi yapılması ya da vücuttan kan veya benzeri biyolojik örneklerle saç, tükürük, tırnak gibi örnekler alınması üzerine 78. madde uyarınca yapılan genetik inceleme sonuçlarının kovuşturmaya yer olmadığı kararına itiraz süresinin dolması, itirazın reddi, beraat veya ceza verilmesine yer olmadığı kararı verilip kesinleşmesi hâllerinde yok edilmesi zorunluluğu örnek gösterilebilir³⁷⁹. Devamla, aynı kanunun 81. maddesi uyarınca şüpheli veya sanığın kimliğinin tespiti için gerekli olması halinde; fotoğrafı, beden ölçüleri, parmak ve avuç içi izi, bedeninde yer almış olup tespitini kolaylaştıracak diğer özellikleri ile sesi ve görüntülerinin kovuşturmaya yer olmadığı kararına itiraz süresinin dolması, itirazın reddi, beraat veya ceza verilmesine yer olmadığı kararı verilip kesinleşmesi hâllerinde derhal yok edilmesi gerekir. Yine CMK'nın 135. maddesine göre yapılan iletişimin tespiti ile dinlenmesi sonucunda kayda alınan bilgiler kişisel veri niteliğinde olduğundan şüpheli ve sanığın tanıklıktan çekinebilecek kişilerle arasındaki iletişime dair olduğunun anlaşılması veya kararın uygulanması sırasında şüpheli hakkında kovuşturmaya yer olmadığına dair karar verilmesi ya da aynı maddenin birinci fıkrasına göre hâkim onayının alınamaması halinde yapılan tespiti ve dinlemeye ilişkin kayıtlar yok edilmek zorundadır³⁸⁰.

³⁷⁹ Genetik inceleme sonuçlarının gizliliği

Madde 80 – (Değişik: 25/5/2005 – 5353/4 md.)

(1) 75, 76 ve 78 inci madde hükümlerine göre alınan örnekler üzerinde yapılan inceleme sonuçları, kişisel veri niteliğinde olup, başka bir amaçla kullanılamaz; dosya içeriğini öğrenme yetkisine sahip bulunan kişiler tarafından bir başkasına verilemez. (2) Bu bilgiler, kovuşturmaya yer olmadığı kararına itiraz süresinin dolması, itirazın reddi, beraat veya ceza verilmesine yer olmadığı kararı verilip kesinleşmesi hâllerinde Cumhuriyet savcısının huzurunda derhâl yok edilir ve bu husus dosyasında muhafaza edilmek üzere tutanağa geçirilir.

³⁸⁰ İletişimin tespiti, dinlenmesi ve kayda alınması

Madde 135 – (3) Şüpheli veya sanığın tanıklıktan çekinebilecek kişilerle arasındaki iletişimi kayda alınamaz. Kayda alma gerçekleşikten sonra bu durumun anlaşılması hâlinde, alınan kayıtlar derhâl yok edilir.

Kararların yerine getirilmesi, iletişim içeriklerinin yok edilmesi

Madde 137 – (3) 135 inci maddeye göre verilen kararın uygulanması sırasında şüpheli hakkında kovuşturmaya yer olmadığına dair karar verilmesi ya da aynı maddenin birinci fıkrasına göre hâkim onayının alınamaması halinde, bunun uygulanmasına Cumhuriyet savcısı tarafından derhâl son verilir. Bu durumda, yapılan tespit veya dinlemeye ilişkin kayıtlar Cumhuriyet savcısının denetimi altında en geç on gün içinde yok edilerek, durum bir tutanakla tespit edilir. (4) Tespit ve dinlemeye ilişkin kayıtların yok edilmesi halinde soruşturma evresinin bitiminden itibaren, en geç onbeş gün içinde, Cumhuriyet Başsavcılığı, tedbirin nedeni, kapsamı, süresi ve sonucu hakkında ilgisine yazılı olarak bilgi verir.

İKİNCİ BÖLÜM

KİŞİSEL VERİLERİ KAYDETME SUÇUNUN UNSURLARI VE ÖZEL GÖRÜNÜŞ BİÇİMLERİ

Kişisel verileri kaydetme suçu, 765 sayılı TCK'da yer almamakta olup ilk kez 5237 sayılı Türk Ceza Kanunu'nun özel hükümlere ilişkin ikinci kitabının kişilere karşı suçları düzenleyen ikinci kısmının özel hayata ve hayatın gizli alanına karşı suçlar başlıklı dokuzuncu bölümü altında 135. maddesinde öngörülmüştür. Söz konusu madde, iki fıkradan ibaret olup; birinci fıkrasında hukuka aykırı olarak kişisel verileri kaydetme, ikinci fıkrasında ise kaydedilen bu kişisel verilerin kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması daha fazla ceza tayini gerektiren nitelikli hal olarak düzenlenmiştir³⁸¹.

³⁸¹ Madde gerekçesi:

Çağımızda kişilerle ilgili kayıtların bilgisayar ortamlarına geçirilip muhafaza edilmesi uygulamasına bazı kurum ve kuruluşlar tarafından başvurulmaktadır; hastanelerde hastalara, sigorta şirketlerinde sigortalılara, bankaların ve kredili alışveriş yapılan mağazaların müşterilerine ilişkin kayıtlar, böylece tutulmaktadır. Bu bilgilerin amaçları dışında kullanılmasından veya herhangi bir şekilde üçüncü şahısların eline geçerek hukuka aykırı olarak yararlanılmasından dolayı hakkında bilgi toplanan kişiler büyük zararlara uğrayabilmektedirler. Bu bakımdan, kişilerle ilgili bilgilerin hukuka aykırı olarak kayda alınması suç olarak tanımlanmıştır. Suçun konusu, kişisel verilerdir. Gerçek kişiyle ilgili her türlü bilgi, kişisel veri olarak kabul edilmelidir. Söz konusu suç tanımında kişisel verilerin bilgisayar ortamında veya kağıt üzerinde kayda alınması arasında bir ayırım gözetilmemiştir. Bu bakımdan, söz konusu suç tanımı ile Avrupa Konseyi bünyesinde hazırlanan Türkiye'nin de 28 Ocak 1981 tarihinde imzalamakla taraf olduğu "Kişisel Nitelikteki Verilerin Otomatik İşleme Tâbi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme"nin ilgili hükümlerine geçerlilik tanınmıştır. Bu suçun oluşabilmesi için, kişisel verilerin hukuka aykırı bir şekilde kayda alınması gerekir. Kişinin rızası ile kendisiyle ilgili bilgilerin kayda alınmasının suç oluşturmayacağı muhakkaktır. Belirli nitelikteki kişisel verilerin kayda alınması kanun hükmünün gereği olarak yapılmaktadır. Bu bakımdan, çeşitli kamu kurumlarında verilen kamu hizmetinin gereği olarak kişilerle ilgili bazı bilgiler ilgili kanun hükümlerine istinaden kayda alınmaktadır. Bu durumlarda, söz konusu suç oluşmayacaktır. Maddenin ikinci fıkrasında, kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine, ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kayda almak, suç olarak tanımlanmıştır. Ancak, bunlardan kişilerin ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgilerin kayda alınmasına kanunlarda özellikle suçlulukla mücadele

2.1. Korunan Hukuki Değer

Suçun işlenmesi sonucunda ihlal edilen değer ya da menfaat, esasen söz konusu fiilin suç olarak tanımlanmasına sebep olan, başka bir deyişle kanunkoyucuyu tipi düzenlemeye sevk eden ve sonuç olarak bu suç tipi ile korunan hukuki değerdir³⁸². Dolayısıyla, "kişisel verilerin kaydedilmesi" suçu bakımından korunan hukuki değer, bu suç tipinin kanunun "özel hayata ve hayatın gizli alanına karşı suçlar" başlığı altında düzenlenmiş olması karşısında kişinin özel hayatı olduğu sonucuna varmak mümkündür³⁸³.

Kişinin özel hayatı, hayatının başkalarının gözü önünde olmayan ve kamuya kapalı alanıdır³⁸⁴. Özel hayat kavramı esasen ayrıcalıklarına önem veren burjuva sınıfının bu ayrıcalıkları nedeni ile komşularından uzak durmaya çalıştığı bir dönemde ortaya çıkmıştır³⁸⁵. Günümüzde ise özel hayatın gizliliği kişi özgürlüğünün bir parçası olup insanın maddi ve manevi varlığının korunması ve geliştirilmesi için vazgeçilmezdir³⁸⁶.

Kişisel verilerin korunması hususu, 1970'li yıllardan itibaren özel hayatın gizliliği kapsamında tartışılmaya başlanmış ve kişisel veriler, özel hayatın parçası olarak kabul edilmiştir³⁸⁷. Türk hukukunda ise Anayasa Mahkemesi'nin 1996/68 Esas, 1991/1 Karar sayılı ve 6.1.1999 tarihli kararında³⁸⁸ kişisel verilerin korunması hakkı, Anayasa'nın 20. maddesinde öngörülen özel hayatın gizliliğinin korunması hakkı bağlamında tartışılmıştır. Anayasa Mahkemesi'nin bu kararı ile kişisel verilerin kaydedilmesi eyleminin hukuki sonucunun özel hayatın gizliliğinin korunması hakkı kapsamında değerlendirilmesi gerektiği ve bunun doğal bir sonucu olarak Anayasanın özel hayatın gizliliğine ilişkin sınırlandırma rejimine tabi olacağı teyit edilmiştir³⁸⁹.

7.5.2010 tarihli Anayasa değişikliği ile Anayasa'nın 20. maddesine,

bağlamında, suç ve suçluların ortaya çıkarılmasını sağlamak amacıyla belli ölçüde izin verilebilir. Bu durumlarda söz konusu suç oluşmayacaktır.

³⁸² Özgenç, 2016: 199; Özbek vd., 2017: 196.

³⁸³ Özbek vd., 2016: 565; Soyaslan, 2016: 349; Aydın, 2015: 125; Ergün, 2008: 115; Karagülmez, 2005: 230; Dülger, 2016: 120.

³⁸⁴ Hafızogulları ve Özen, 2009: 17.

³⁸⁵ Özbek vd., 2016: 555.

³⁸⁶ Özbek vd., 2016: 556.

³⁸⁷ Ketizmen, 2008: 207.

³⁸⁸ Karar metni için bk. <http://www.kararlaryeni.anayasa.gov.tr/Karar/Content/9f7b3df0-e060-4c61-9dc8-f9e43a52adf4?excludeGerekce=False&wordsOnly=False> /(erişim tarihi:20.09.2017).

³⁸⁹ Ketizmen, 2008: 210.

“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.”

fıkrası eklenmiş ve son olarak da KVKK'nın "amaç" başlıklı 1. maddesinde, *"Bu Kanunun amacı, kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektir."* ifadesine yer verilmiş olup kişisel verilerin korunması bağlamında kişisel verinin kaydedilmesi suçu ile korunan hukuki değerin özel hayatın gizliliği olarak kabul edildiği konusunda tereddüt kalmamıştır.

2.2. Tipiklik (Tipe Uygunluk)

Tipiklik, işlenen fiilin ceza kanunundaki suç tanımına birebir uygun olup olmadığının tespiti ile ilgilidir; başka bir deyişle bu fiilin ceza normundaki soyut tasviridir³⁹⁰. Bir eylemin suç olduğunun kabulü için dış dünyada değişiklik yaratan hareketin ceza kanunundaki tanıma veya tipe uygun olması gerekir³⁹¹. Kanunkoyucunun cezalandırılması kanaatinde olduğu davranış şekillerinin haksızlık içeriğini somutlaştıran unsurlar, suçun kanuni tipini ya da tarifini oluşturur³⁹².

TCK'nın kabul ettiği suç teorisi uyarınca; suç tipinde yer alan fail, mağdur, suçun konusu, hareket gibi objektif unsurlara tipikliğin maddi unsurları, kast ve taksir gibi subjektif unsurlara ise tipikliğin manevi unsurları adı verilmektedir³⁹³.

³⁹⁰ Artuk vd., 2013: 204. Bu unsuru, "yasallık" veya "suç kalıbına uygunluk" olarak adlandıran yazarlar da bulunmaktadır. Bk. Centel vd., 2014: 219.

³⁹¹ Artuk vd., 2013: 203; Koca ve Üzülmöz, 2017: 104.

³⁹² Koca ve Üzülmöz, 2017: 105.

³⁹³ Koca ve Üzülmöz, 2017: 110-111. Özbek/Doğan/Bacaksız/Tepe de benzer şekilde, suçun unsurlarından tipe uygun eylemin içeriğini objektif nitelikteki unsurlar, subjektif nitelikteki unsurlar ile yaptırım olarak sınıflandırmaktadır. Bk. Özbek vd., 2017: 214 vd. Ancak Artuk/Gökçen/Yenidünya, suçun unsurlarını tipiklik, maddi unsurlar, manevi unsurlar ve hukuka aykırılık biçiminde bir tasnifle incelemektedir. Bk. Artuk vd., 2013:210.

2.2.1. Suçun Maddi Unsurları

2.2.1.1. Fiil – Hareket

Fiil, suçun varlığına ilişkin birincil koşul olup (nullum crimen sine actione) insanın dış dünyada bir şeyi yapmak ya da yapmamak biçiminde ortaya çıkan iradi davranışıdır³⁹⁴. Birinci durumda icrai, ikinci durumda ise ihmali bir hareket söz konusudur. Ceza hukuku bakımından ise suç tanımına uyan ve bu tanımdaki neticeyi doğurmaya elverişli, iradi davranıştır³⁹⁵.

TCK 135. maddede düzenlenen kişisel verilerin kaydedilmesi suçu bakımından hareket, kişisel nitelikteki verinin kaydedilmesidir. Kaydetme kelimesi; yazmak, bazı önemli noktaları tespit etmek; hatırlamak için yazmak, not etmek; sesi veya resmi manyetik bant üzerine geçirmek; elektronik veya sayısal araçlarda bilgiyi korumaya almak anlamlarına gelmekte olup³⁹⁶ kanunda kişisel verilerin kaydedilmesi suçu bakımından kaydetme eyleminin bu anlamlarından hangisini kapsadığı belirtilmemiştir³⁹⁷. Bunun sebebinin söz konusu suça ilişkin düzenlemenin Fransız Ceza Kanunu'nda bulunan düzenlemeden örnek alındığı ve bu kanunda ilgili suça ilişkin maddenin eksik norm³⁹⁸ olarak düzenlenmesi olduğu savunulmaktadır³⁹⁹. Burada kaydetme fiilinden anlaşılması gerekenin, verilerin gerektiğinde kullanılmak üzere hazır edilmesi olduğu; bu anlamda verilerin yazılması, depolanması, muhafaza edilmesi veya şerh düşülmesi gerekliliğinin bulunduğu ifade edilmektedir⁴⁰⁰.

³⁹⁴ Artuk vd., 2013: 212.

³⁹⁵ Centel vd., 2014: 222.

³⁹⁶ http://www.tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.59c409241ecae3.899768
73 / (erişim tarihi:21.09.2017)

³⁹⁷ "...Ülkemizde kişisel verilerin korunmasını sağlayacak bir kanunun yürürlüğe girmesini gerektiren değişik sebepler bulunmaktadır. Öncelikle, 5237 sayılı Türk Ceza Kanunu'nun 135 ve devamı maddelerinde kişisel verilerin hukuka aykırı olarak elde edilmesi, kaydedilmesi veya ifşa edilmesi eylemleri suç olarak düzenlenmiş ve yaptırma bağlanmıştır. Bununla birlikte, kişisel verilerin işlenmesine yönelik özel bir kanunun bulunmaması sebebiyle, bu fiillerin ne zaman hukuka aykırı, ne zaman hukuka uygun olduğunun belirlenmesinde tereddütlerin yaşandığı görülmektedir..." (KVKK genel gerekçesinden).

³⁹⁸ "Eksik ceza normları, kural olarak, hüküm veya müeyyideden meydana gelen bir bütünün, yalnız bir kısmını içeren hükümlerdir. Bu tür hükümler, ya sadece davranış kuralı olan hükmü, ya da sadece müeyyideyi içermektedir. Burada, eksik kalan kısımlarını birleştirerek normu oluşturmak yorumcunun görevidir. Kanunun, ör., 257. maddesinde, hüküm eksiktir. Burada "görevinin gereklerine aykırı hareket etmek" veya "görevinin gereklerini yapmakta ihmal veya gecikme göstermek" ancak kamu görevlisinin görevini düzenleyen mevzuata gidilerek belirlenebilmekte, böylece hüküm tamamlanmaktadır." (Hafızoğulları ve Özen, 2010: 66).

³⁹⁹ Ketizmen, 2008: 235.

⁴⁰⁰ Yaşar vd., 2014: 4437.

İlaveten, kişisel verinin kaydedilmesi sonucunda mağdurun bir zarara uğrayıp uğramadığının bir önemi bulunmamaktadır⁴⁰¹. Bu bakımdan suç, tehlike suçu olarak kabul edilmektedir⁴⁰². Her ne kadar kişisel verinin kaydının ağırlıklı olarak bilgisayar aracılığı ile dijital ortamda yapılması kolay ve yaygın olsa da esasen söz konusu kaydın bilgisayar ortamında veya kağıt üzerinde gerçekleştirilmesinin bu suç bakımından bir farkı yoktur⁴⁰³. Bu anlamda kişisel verilerin kaydedilmesi suçu, serbest hareketli bir suç olup bu suçun her türlü fiille, bilgisayarın ana belleği, CD, USB bellek vs. herhangi bir dijital materyal üzerinde veya kalem, fotokopi, tarama gibi kağıt üzerinde işlenebilmesi mümkündür⁴⁰⁴. Suç, kayıt etme fiilinin tamamlanması ile birlikte gerçekleşmiş olmakta⁴⁰⁵, bu verilerin kullanılması veya fayda sağlanması gerekmemektedir⁴⁰⁶. KVKK, kişisel verilere yönelik tüm eylemler açısından "işleme" terimini kullanmış olup kaydetme de bir tür kişisel verinin işlenmesi faaliyetidir⁴⁰⁷.

Bu noktada, hukuka uygun bir şekilde kaydedilen kişisel verinin kaydedilme amacının dışında kullanılmasının, başka bir deyişle işlenmesinin bu suç kapsamında değerlendirilip değerlendirilmeyeceği sorusu akla gelebilir. Kişisel verinin işlenmesinde uyulması gereken ilkelerden biri olan amaçla bağlılık ilkesinin meşru amaç dışında başka bir amaç için işlenmesini önlemeye yönelik misyonu, 135. maddede dikkate alınmamış olup⁴⁰⁸ kişisel verinin kaydedilme anında hukuka uygun olması durumunda kaydedilen verinin amacı dışında kullanılması 135. maddedeki suçun kapsamı dışındadır⁴⁰⁹.

⁴⁰¹ Karagülmez, 2005: 231; Yaşar vd., 2014: 4438.

⁴⁰² Taşkın, 2008: 102; Dülger, 2016:129.

⁴⁰³ Bk. maddenin gerekçesi. Aynı yönde bk. Ergün, 2008: 114; Karagülmez, 2005: 231.

⁴⁰⁴ Taşkın, 2008: 101; Karagülmez, 2005:231; Ketizmen, 2008: 231; Dülger, 2016: 128.

⁴⁰⁵ Karagülmez, 2005: 231.

⁴⁰⁶ Yaşar vd., 2014: 4438.

⁴⁰⁷ Bk. KVKK madde 3-e.

⁴⁰⁸ Ketizmen, 2008: 238. Yazara göre, maddenin gerekçesinde yer alan "...Bu bilgilerin amaçları dışında kullanılmasından veya herhangi bir şekilde üçüncü şahısların eline geçerek hukuka aykırı olarak yararlanılmasından dolayı hakkında bilgi toplanan kişiler büyük zararlara uğrayabilmektedirler" ifadesi kişisel verilerin işlenmesine ilişkin bir gerçeği yansıtmakla birlikte gerekçe madde içeriği ile örtüşmemektedir.

⁴⁰⁹ Hukuka uygun olarak kaydedilen kişisel verinin kaydedilme amacının dışında kullanılması durumunun her ne kadar kişisel verilerin kaydedilmesi suçu kapsamında değerlendirilmesi mümkün olmasa da; örneğin bir kamu görevlisinin hukuka uygun olarak kaydedilmiş kişisel veriyi görevinin gereklerine aykırı hareket etmek suretiyle kaydedilme amacının dışında kullanarak kişilerin mağduriyetine veya kamunun zararına neden olması ya da kişilere haksız bir menfaat sağlaması halinde bu fiili görevi kötüye kullanma suçu olarak nitelendirilebilir.

Verileri kaydetmeden öğrenme, salt duyu organları aracılığı ile vakıf olunması ve akılda tutma halinde kişisel verileri kaydetme suçundan söz edilemez⁴¹⁰. Yine, veri ile kişi arasındaki bağlantı ortadan kaldırıldığında, yani kişisel veri anonim hale getirildiğinde bu verinin kaydedilmesi veya alenileşmiş ve herkes tarafından erişilebilir bir verinin kaydedilmesi kişisel verileri kaydetme suçunu oluşturmayacaktır; zira bu durumlarda veri süjesinin özel hayatının ihlal edilmesi söz konusu olmayacak ve bu verinin gizli kalmasından makul bir beklentisinin varlığından söz edilemeyecektir⁴¹¹.

Kişisel verilerin hukuka aykırı olarak kaydedilmesi suçunun ihmal sureti ile işlenmesi mümkün değildir⁴¹².

2.2.1.2. Konu

Fiilin konusu, tipe uygun hareketin üzerinde gerçekleştiği; eşya veya şahsın fiziki yapısı, maddi varlığıdır⁴¹³. Bu durumda, kişisel verilerin kaydedilmesi suçunun konusu, kişisel veridir⁴¹⁴.

Kişisel veri kavramından ne anlaşılması gerektiği, çalışmamızın başında "Kişisel Veri Kavramı" başlığı altında tartışılmış olduğundan burada tekrar edilmesine gerek görmemekle

⁴¹⁰ "...Kişisel verilerin kaydedilmeden önce öğrenilmesi, hafızada tutulan kişisel verilerin başkalarına açıklanması, kişisel verilere salt duyu organları aracılığıyla vakıf olunması, ancak TCK'nın 134/1. maddesinin 1. cümlesinde düzenlenen özel hayatın gizliliğini ihlal suçu kapsamında değerlendirilebilir. Bu açıklamalar ışığında incelenen dosyada, elektronik mühendisi olan sanığın, teknik servis elemanı olarak çalıştığı sırada, Turgut Özal Tıp Merkezi psikiyatri anabilim dalında tedavi gören mağdure hemşirenin, Corteks adlı bilgi sisteminde bulunan muayene bilgilerini okuyup, hastane çalışanlarına, mağdurenin intihar girişiminde bulunduğunu anlattığı olayda, Dairemizin değişen görüşüne göre; Mağdurenin kişisel verilerini, kaydedilmiş haliyle ele geçirip, bu haliyle başkalarına verdiği veya yaydığına dair hakkında bir delil bulunmayan sanığın, mağdurenin özel yaşam alanındaki sağlık bilgilerini okuyup, içeriğini öğrendiği mağdureye ait kişisel verileri başkalarına açıklaması eyleminin, TCK'nın 134/1-1. maddesinde tanımlanan özel hayatın gizliliğini ihlal suçunu oluşturacağı gözetilmeden, suç vasfında yanılığa düşülerek, sanık hakkında, verileri hukuka aykırı olarak verme veya ele geçirme suçundan mahkumiyet kararı verilmesi..." Yargıtay 12. CD. 2014/3107 E., 2014/20959 K. 27.10.2014.

⁴¹¹ Ketizmen, 2008: 238.

⁴¹² Özbek vd., 2016: 571; Hafizoğulları ve Özen, 2009: 20. Kural olarak icrai bir hareketle gerçekleştirilebilecek bir neticenin ihmali bir tutumla gerçekleştirilmesi biçiminde ifade edilen ihmal suretiyle icra suçlarına ilişkin bir düzenlemeye TCK'nın genel hükümlerinde yer verilmemiş olması nedeni ile bu ihtimalin, bu konuya dair özel birer düzenleme niteliğindeki TCK m. 83, m. 88 ve m. 94 hükümleri dışında cezalandırılması mümkün değildir. Bk. Koca ve Üzülmüş, 2017: 391.

⁴¹³ Özbek vd., 2017:196; Özgenç, 2016: 198.

⁴¹⁴ Özbek vd., 2016: 565; Dülger, 2016: 125.

birlikte, kişinin kendisine ait telefonu ile yaptığı görüşme detayları⁴¹⁵; ad, soyad, kimlik numarası, telefon numarası⁴¹⁶, ⁴¹⁷, ⁴¹⁸, fotoğraf ve sesi⁴¹⁹, e- posta adresi ve adreste kayıtlı

⁴¹⁵ "...Sanık Gönül'ün, 23.02.2011 tarihinde boşandığı eski eşi katılan Mustafa'nın kimlerle görüştüğünü öğrenmek amacıyla, 04.09.2012 tarihinde, kimliği belirlenemeyen bir erkek şahsa, kendi adına kayıtlı olan telefon hattından, T... A.Ş.'nin müşteri temsilcisini arattırdığı, söz konusu erkek şahsın, kendisini katılan olarak tanıtır, işlem güvenliği için gerekli olan sorulara doğru cevaplar verdikten sonra, katılana ait GSM hattının 25.06.2012, 25.07.2012 ve 25.08.2012 düzenleme tarihli faturalarına ilişkin kullanım detaylarının, sanığın adresine gönderilmesi için adres değişikliği talebinde bulunduğu ve işlemlerin tamamlanmasının ardından katılanın abonesi olduğu telefon hattının geçmişe ait görüşme detay bilgileri adresine gelen sanığın, bu belgelerde yazılı numaraları arayıp, katılanın telefonla görüştüğü kişileri tespit etmeye çalıştığı olayda, Haberleşme sürecinin taraflarını ve zamanını gösteren bilgiler, "kişisel veri" kapsamında olup, katılanın ne zaman kiminle hangi sıklıkla ve ne kadar süreyle görüştüğüne ilişkin kişisel verilerinin yazılı olduğu belgeleri hukuka aykırı olarak ele geçiren sanık hakkında, TCK'nın 136/1. maddesinde tanımlanan verileri hukuka aykırı olarak verme veya ele geçirme suçundan mahkumiyet hükmü kurulması gerekirken, suç vasfında yanılıya düşülüp, yasal ve yeterli olmayan gerekçelere dayalı olarak, sanığın TCK'nın 134/1. maddesinde düzenlenen özel hayatın gizliliğini ihlal suçundan mahkumiyetine karar verilmesi..." (Yargıtay 12. CD, 2014/11621 E, 2015/568 K, 19.01.2015).

⁴¹⁶ "...Sanığın...mağdurun ad ve soyadı, fotoğrafı ve telefon numaraları ile "E. O. Dansöz" şeklinde kartvizit bastırarak mağdurun bulunduğu yerdeki esnaflara ve baro temsilciliğine göndermek suretiyle kişisel veri niteliğindeki bilgilerini yaydığı, atılı suçların bu şekilde sübut bulduğu anlaşılmakla..." Yargıtay 12. CD. 2014/11879 E., 2015/22 K., 12.01.2015.

⁴¹⁷ Yargıtay 12. CD., 2014/11861E., 2015/19 K., 12.01.2015.

⁴¹⁸ Yargıtay 12. CD., 2014/11758 E., 2015/16 K., 12.01.2015

⁴¹⁹ Kişinin fotoğrafının ve sesinin kişisel verilerin kaydedilmesi suçunun konusunu oluşturup oluşturmayacağı meselesinin her somut olay bakımından ayrı ayrı ve titizlikle irdelenmesi gerekmektedir. "...Bir özel hayat görüntüsü ya da sesinin, "kişisel veri" olduğunda kuşku bulunmamakta ise de, kişinin özel hayatına ilişkin görüntüsü ya da sesinin, bilgisi dışında, resim çekme veya kaydetme özelliğine sahip aletle belli bir elektronik, dijital, manyetik yere sabitlenmesi TCK'nın 134/1. maddesinin 2. cümlesinde; rızası dışında ifşa edilmesi, yani; yayılması, açığa vurulması, afişe edilmesi, ilan edilmesi, kamuoyuna duyurulması, aleniyet kazandırılması, özetle; içeriğini öğrenme yetkisi bulunmayan kişi veya kişilerin bilgisine sunulması TCK'nın 134/2. maddesinde özel hayatın gizliliğini ihlal suçu kapsamında düzenlendiğinden, kişinin özel hayatına ilişkin görüntüsü, fotoğrafı ya da sesi, yasal anlamda, TCK'nın 135 ve 136. maddeleri kapsamında kişisel veri olarak değerlendirilemez...." - Yargıtay 12. CD. 2013/30368 E. , 2014/16607 K., 07.07.2014; "...Katılanın internette yer alan günlük kıyafetleriyle poz vermiş şekilde çektiği resminin, özel yaşam alanına ilişkin ve özel hayatının gizliliğini ihlal edecek nitelikte olmaması karşısında, sanığa isnat edilen özel hayatın gizliliğini ihlal suçunun yasal unsurlarının somut olayda gerçekleşmediği ve katılanın kişisel veri niteliğindeki resmini hukuka aykırı olarak yayımlayan sanığın eyleminin TCK'nın 136. maddesinde tanımlanan verileri hukuka aykırı olarak verme veya ele geçirme suçunu oluşturacağı gözetilmeden, aynı eylemden dolayı sanık hakkında kişisel verilerin kaydedilmesi suçundan beraat hükmü kurulup, yasal ve yeterli olmayan gerekçelere dayalı olarak, TCK'nın 134/2. maddesinde

arkadaş bilgileri⁴²⁰, yerleşim yeri, eğitim durumu, mesleği, özgeçmişi⁴²¹, arabasının plakası⁴²², banka hesap bilgileri, telefon numarası, elektronik posta adresi, IP adresi⁴²³, kan grubu, medeni hali, parmak izi, DNA'sı, saç, tükürük, tırnak gibi biyolojik örnekleri⁴²⁴, vergi kayıtları⁴²⁵, kredi kartı bilgileri⁴²⁶, GBT (Genel Bilgi Toplama) ve mahkumiyetlere ilişkin Adli Sicil kayıtları⁴²⁷, herhangi bir hastalığın seyri, teşhisi, tedavisi ve yapılan tetkikler konusunda bilgiler içeren belgeler veya kayıtlar⁴²⁸ kişisel verilere örnek gösterilebilir.

düzenlenen özel hayatın gizliliğini ihlal suçundan mahkumiyet kararı verilmesi..." - Yargıtay 12. CD. 2013/27724 E., 2014/16601 K., 07.07.2014); ayrıca bk. KVKK, 3. madde gerekçesi.

⁴²⁰ "...Sanığın, şikayetçinin elektronik posta adresini ele geçirdiği ve bilahare adrese erişimini engellediği, sistemi engelleme, bozma, verileri yok etme veya değiştirme suçunun bu şekilde sübut bulunduğu anlaşıldığından, mahkumiyetine karar verilmesinde isabetsizlik görülmemiş; şikayetçinin elektronik posta adresindeki kişisel veri niteliğindeki arkadaş bilgilerini ele geçiren sanığın eyleminin TCK'nın 44. maddesi gereğince fikri içtima kapsamında değerlendirilemeyeceği..." Yargıtay 12. CD. 2014/11398 E., 2014/17253 K., 08.09.2014.

⁴²¹ bk. KVKK, 3. madde gerekçesi.

⁴²² Ergün, 2008: 114.

⁴²³ *Scarlet v. SABAM* davasında Avrupa Birliği Adalet Divanı, kullanıcısını açıkça belirleyebilme imkanını haiz olması sebebi ile IP adresinin korunan kişisel verilerden olduğu hükmetmiştir. ([http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62010CJ0070:EN:HTML/\(erişim tarihi:22.10.2017\).](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62010CJ0070:EN:HTML/(erişim tarihi:22.10.2017).))

⁴²⁴ Yargıtay 12. CD. 2014/9544 E., 2015/46 K., 12.01.2015.

⁴²⁵ Yargıtay 12. CD. 2014/7209 E., 2014/20326 K., 20.10.2014.

⁴²⁶ "...Oluşa ve kabule göre; katılanın müdürü ve temsilcisi olduğu firmada, teknik servis elemanı olarak çalışmakta olan sanığın, son bir hafta iş yerine gelmeyip, telefonla iş yeri arkadaşlarını arayarak, servise çıkarken kullanmak üzere verilen çantanın, ısrarla kendisine gönderilmesini istemesi üzerine, hal ve hareketlerinden şüphelenilerek, 06.06.2005 günü, katılan ve iş yeri çalışanları tarafından söz konusu çantanın açılıp, içerisinde bulunan veri depolama aygıtının incelenmesi sonucunda, şirkete ait birtakım mali bilgiler ve programlar ile katılana ait kredi kartının ön ve arka yüzünün kaydedilmiş olduğunun tespit edildiği olayda, gerek soruşturma aşamasında düzenlenen 09.11.2006 tarihli bilirkişi raporuna, gerek katılan ve iş yeri çalışanlarınca tanzim edilen tutanak ekine göre, "kişisel veri" olarak kabul edilen bilgilerin, 13.05.2005 ve 14.05.2005 tarihlerinde kayıt altına alındığının belirlenmesi ve ele geçirilme tarihi itibarıyla 01 Haziran 2005 tarihinden önce yürürlükte bulunan 765 sayılı TCK'da iddia konusu eylemin suç olarak tanımlanmamış olması nedeniyle, 5271 sayılı CMK'nın 223/2-a maddesi gereğince sanık hakkında beraat kararı verilmesi gerekirken, bahse konu bilgilerin, sanık tarafından ele geçirilip, herkes tarafından kolaylıkla ulaşılabilen ve iş yeri çalışanlarının müdahalesine açık olan çanta içerisindeki veri depolama aygıtına yüklendiğine dair, savunmanın aksine delil bulunmadığı gibi, 5237 sayılı TCK'da, gerçek kişiye ait bilgilerin, "kişisel veri" olarak düzenlenmesi karşısında, katılana ait kredi kartı bilgileri hariç, şirkete ait mali bilgilerin ve programların "kişisel veri" olarak kabul edilemeyeceği de gözetilmeden, yasal olmayan ve dosya kapsamına uygun düşmeyen yetersiz gerekçelerle, sanığın mahkumiyetine karar verilmesi..." Yargıtay 12. CD., 2013/10672 E., 2013/15772 K., 10.06.2013.

⁴²⁷ "...Dosya kapsamına göre, ege postası gazetesinin imtiyaz sahibi ve yazı işleri müdürü olan sanığın, gazetenin 23.02.2011 ve 26.02.2011 tarihli internet sayfasındaki yazısında, Bayraklı belediyesinin AKP'li

Yine, 5271 sayılı Ceza Muhakemeleri Kanunu'nun 75. maddesi uyarınca şüpheli veya sanık üzerinde; 76 maddesi uyarınca mağdurun üzerinde bir suça ilişkin delil elde etmek amacı ile yapılan iç beden muayenesi, vücuttan alınan kan veya biyolojik örneklerle saç, tükürük, tırnak gibi örnekler üzerinde yapılan tahliller ile aynı kanunun 80. maddesi uyarınca bu örnekler üzerinde belirli amaçlar doğrultusunda⁴²⁹ yapılan moleküler genetik incelemeler sonucu elde edilen bulguların kişisel veri niteliğinde olduğu ayrıca ve açıkça ifade edilmiştir⁴³⁰.

Yargıtay, kişinin çıplak halde çekilmiş fotoğraflarının veya buna benzer şekilde cinsel arzuların tatmini maksadı ile çekilmiş videolarının ise cinsel ve fiziksel mahremiyetine ilişkin olduğundan bahisle kişisel veri kapsamında değerlendirilmesinin mümkün olmadığı ve failin bu eyleminin özel hayatın gizliliğini ihlal suçunu oluşturacağı görüşündedir⁴³¹. Yargıtay'ın bu

belediye meclis üyesi olan katılan hakkında Boztepe'nin şok eden sicili başlığı altında "...İzmir İl Emniyet Müdürlüğü Bayraklı Belediyesinin partili Meclis üyesi H.B.'yi sakıncalı buldu... Sicili bozuk çıktı.." biçimindeki ifadeler ile katılanın birçok suçtan mahkemelerde yargılanmış olduğu, silah ruhsatı yenileme talebinin İzmir Emniyet Müdürlüğü'nce "sicili bozuk" olduğu gerekçesi ile reddedildiği ve elindeki silahlara el konulması yönünde karar verdiği, Emniyet Müdürlüğü'nün ortaya epeyce kabarık bir suç dökümü çıkardığını yazarak katılanın 1989, 1996 ve 1997 yılında yargılandığı ve bazıları beraat ve ortadan kaldırma ile sonuçlanan suçlara ilişkin kişisel veri niteliğindeki GBT kayıtları ve silinme koşulları oluşmuş eski mahkumiyetlere ilişkin adli sicil kayıtlarını yayımladığı..." Yargıtay 12. CD. 2013/30385 E., 2014/14157 K., 09.06.2014.

⁴²⁸ *"...Hastanın başka bir doktora veya hastaneye gittiğinde hasta hakkında yeni doktoruna bilgi verilmesi, böylece tedavisi için daha hızlı ve daha doğru kararlar alınmasını sağlamak amacıyla, uygulamada bir örneği taburcu olan hasta veya yakınlarına verilen, ilgili doktor tarafından doldurularak imzalanan, hastanın kimlik bilgileri, hastalığın seyri, teşhisi, tedavisi ve yapılan tetkikler konusunda bilgiler içeren epikriz raporu düzenlenerek katılanın taburcu edildiği, bir süre sonra, katılanın oğlu tarafından, eşi A... aleyhine, Hepatit B hastası olduğunu gizleyip, kendisini aldatarak evlendiği iddiasıyla boşanma davası açılması üzerine, A...'un vekilliğini üstlenen sanık avukatın, 06.06.2006 tarihli cevap dilekçesinde, davacı tarafın iddialarının soyut olduğunu, davacının eşiyle olan geçimsizliklerinin asıl sebebinin, oğluna aşırı düşkün olan kayınvalidesinin, oğlunun geliniyle evli kalmasını kabullenemeyişi olup, bu nedenle intihara teşebbüs ettiğini belirterek, müvekkili A...'dan temin ettiği katılan hakkında düzenlenen konsültasyon kağıdı ve epikriz raporu fotokopilerini iddiaya ispat olarak dilekçesine ekli olarak vermesi şeklinde gelişen olayda;...sanığın, kişisel veri niteliğindeki katılanın intihar teşebbüsü ile ilgili belge örneklerini, suç işleme kastıyla hareket ederek üçüncü kişi ya da kişilere verdiğine dair dosya kapsamında bir bilgi ve belge de bulunmadığı anlaşılmakla..." Yargıtay 12. CD. 2012/32354 E. , 2013/18659 K., 08.07.2013.*

⁴²⁹ Bu amaçlar, soybağının veya elde edilen bulgunun şüpheli veya sanığa ya da mağdura ait olup olmadığının tespiti için.

⁴³⁰ Bk. CMK madde 80.

⁴³¹ *"...Sanıkların, mağdurla arkadaşlık kurdukları ve mağdurun, internet ortamından rızası ile gönderdiği çıplak fotoğraflarını flash diske kaydedip, babası M...'e vermek suretiyle ifşa ettiklerinin iddia edildiği olayda;*

kanaati; özel hayata ve hayatın gizli alanına karşı suçlar başlığı altında yer verilen, özel hayatın gizliliğini ihlal ile kişisel verilerin kaydedilmesi suçlarının düzenlenmesindeki amaçsal farklılık bağlamında değerlendirilmelidir. TCK'nın 134. maddesinde düzenlenen özel hayatın gizliliğini ihlal suçu⁴³², kanunun gerekçesinde “gizli yaşam alanına girerek veya başka suretle başkaları tarafından görülmesi mümkün olmayan bir özel yaşam olayının saptanması ve kaydedilmesi” biçiminde tarif edilmiştir. Gerçekten, kişinin özel hayatının temelini, davranışlarını özgürce belirleyebilme anlamına gelen bağımsızlık ile bireysel veya ailevi alanını paylaşmak istediği kişileri kendisinin belirleyebilmesi hakkına işaret eden gizlilik unsurları oluşturur⁴³³. Buna göre bireyin, özel hayatını yalnızca kendisinin uygun gördüğü kişiler ile uygun gördüğü ölçüde ve zamanda paylaşma hakkı bulunmaktadır⁴³⁴. Dolayısı ile kanunkoyucunun özel hayatın gizliliğini ihlal suçu düzenlemesi ile amacının, bireyin yaşamının gizli ve dokunulmaz kalmasını arzuladığı alanına müdahale edilmesini cezalandırmak olduğu sonucuna varılmaktadır. Oysa kanunun 135. maddesinde yer alan kişisel verilerin kaydedilmesi suçu düzenlemesi ile amaçlanan, kişiye ait olup onun kimliğini belirlemeye yarayan her türlü bilginin, kişinin dokunulmazlık beklentisi bulunup bulunmadığına bakılmaksızın hukuka aykırı olarak kaydedilmesinin önlenmesidir. Bu bağlamda, kişinin görüntüsünün de onun kimliğini belirlemeye imkan verdiği takdirde kişisel veri olduğunda kuşku bulunmadığından Yargıtay'ın kişinin çıplak görüntülerinin kişisel veri olarak değerlendirilemeyeceği görüşüne katılmamakla birlikte; bu mahiyetteki görüntüleri kişinin yalnızca uygun gördüğü kişiler ile paylaşması hakkı ve bu görüntüler yönünden haklı bir dokunulmazlık beklentisinin bulunduğu gerçeği karşısında kişinin çıplak görüntülerinin kaydedilmesinin özel hayatın gizliliğini ihlal suçunu oluşturacağı görüşünün yerinde olduğu kanaatindeyiz.

*mağdurun, cinsel ve fiziksel mahremiyetine ilişkin çıplak görüntüleri kişisel veri kapsamında değerlendirilemeyeceğinden, eylemin, kişisel verilerin kaydedilmesi suçunu değil, TCK'nın 134/1. maddesinin 2. cümlesi ve 134/2. maddesine uyan özel hayatın gizliliğini ihlal suçlarını oluşturacağı...”*Yargıtay 12. CD., 2014/11530 E., 2015/584 K., 19.01.2015.

⁴³² Özel hayatın gizliliğini ihlal

Madde 134- (1) Kişilerin özel hayatının gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Gizliliğin görüntü veya seslerin kayda alınması suretiyle ihlal edilmesi halinde, verilecek ceza bir kat artırılır.

(2) (Değişik: 2/7/2012-6352/81 md.) Kişilerin özel hayatına ilişkin görüntü veya sesleri hukuka aykırı olarak ifşa eden kimse iki yıldan beş yıla kadar hapis cezası ile cezalandırılır. Ifşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur.

⁴³³ Yurtsever, 2015: 10; Geçmez, 2014: 14.

⁴³⁴ Geçmez, 2014:14.

Her ne kadar kişisel verinin kişinin kimliğini belirleyen ve belirlenebilir kılan, kişiyi toplumda yer alan diğer bireylerden ayıran ve onun niteliklerini ortaya koymaya elverişli, gerçek kişiye ait her türlü bilgi olarak anlaşılması gerekir ise de, bu düzenlemenin uygulama alanının amaçlanandan fazla genişletilerek, uygulamada belirsizlik ve hemen her eylemin suç oluşturması gibi olumsuz sonuçların doğmaması için, maddenin uygulamasında, somut olayın özellikleri dikkate alınarak titizlikle değerlendirme yapılması, olayda herhangi bir hukuk dalı tarafından kabul edilebilecek bir hukuka uygunluk nedeni veya bu kapsamda nazara alınabilecek bir hususun bulunup bulunmadığının saptanması ve sanığın eylemiyle hukuka aykırı hareket ettiğini bildiği ya da bilebilecek durumda olduğunun da ayrıca tespit edilmesi gerektiği kabul edilmiştir⁴³⁵.

⁴³⁵ "... "Kişisel veri" kavramından, kişinin, yetkisiz üçüncü kişilerin bilgisine sunmadığı, istediğinde başka kişilere açıklayarak ancak sınırlı bir çevre ile paylaştığı nüfus bilgileri (T.C. kimlik numarası, adı, soyadı, doğum yeri ve tarihi, anne ve baba adı gibi), adli sicil kaydı, yerleşim yeri, eğitim durumu, mesleği, banka hesap bilgileri, telefon numarası, elektronik posta adresi, kan grubu, medeni hali, parmak izi, DNA'sı, saç, tükürük, tırnak gibi biyolojik örnekleri, cinsel ve ahlaki eğilimi, sağlık bilgileri, etnik kökeni, siyasi, felsefi ve dini görüşü, sendikal bağlantıları gibi kişinin kimliğini belirleyen veya belirlenebilir kılan, kişiyi toplumda yer alan diğer bireylerden ayıran ve onun niteliklerini ortaya koymaya elverişli, gerçek kişiye ait her türlü bilginin anlaşılması gerekir. Herkes tarafından bilinen ve/veya kolaylıkla ulaşılması ve bilinmesi mümkün olan kişisel bilgiler de, yasal anlamda "kişisel veri" olarak kabul edilmekte ise de, anılan maddenin uygulama alanının amaçlanandan fazla genişletilerek, uygulamada belirsizlik ve hemen her eylemin suç oluşturması gibi olumsuz sonuçların doğmaması için, maddenin uygulamasında, somut olayın özellikleri dikkate alınarak titizlikle değerlendirme yapılması, olayda herhangi bir hukuk dalı tarafından kabul edilebilecek bir hukuka uygunluk nedeni veya bu kapsamda nazara alınabilecek bir hususun bulunup bulunmadığının saptanması ve sanığın eylemiyle hukuka aykırı hareket ettiğini bildiği ya da bilebilecek durumda olduğunun da ayrıca tespit edilmesi gerekir. Bu açıklamalar ışığında incelenen dosya kapsamına göre; çeşitli televizyon programlarının sunuculuğunu yapan, aynı zamanda sinema ve tiyatro oyuncusu olup, kamuoyu tarafından tanınan katılanın, yaklaşık 25 yıl önce, özel bir proje için çektiğini beyan ettiği yarı çıplak resminin, sanığın sahibi olduğu eğlence amaçlı bir internet sitesinde, bir başka internet sitesine link verilerek yayımlandığı iddia ve kabulüne konu olayda, Dosyada mevcut delillere göre; şikayete konu resmin; Haftasonu adlı haftalık magazinaktüel gazetesinin 15.11.1995 tarihli nüshasında, "Vay Vay Vay Kraliçeye Bak!"; "Tecrübesiz, Saf ve Güzel..." ibareleriyle beraber yayımlandığı, asgari 10 yıldır da çeşitli internet sitelerinde yayımlanmakta olup, erişiminin engellenmediği; ayrıca, katılanın, gerek şikayete konu resmi çektiği dönemde, gerek bu dönemden sonra, rızası dahilinde yayımlanan çok sayıda görüntüsü olup, bu şekilde magazin basınının ve toplumun dikkatini çektiği, şöhretinin de devam ettiği nazara alındığında, sanığın, farklı bir internet sitesinde paylaşılan ve orijinal haline müdahalede bulunmadığı ünlü bir kişiye ait resme, kendi sitesi üzerinden bağlantı kurulmasını sağlamaktan ibaret eyleminde, hukuka aykırı hareket ettiği bilinciyle davrandığı kabul edilemeyeceğinden, sanık hakkında CMK'nın 223/2-a maddesi gereğince beraat kararı verilmesi gerekirken, yasal ve yeterli olmayan gerekçelere dayalı olarak, sanığın TCK'nın 136/1. maddesinde tanımlanan verileri hukuka aykırı olarak verme

Kişisel verilerin kaydedilmesi suçu bakımından, suçun konusu olan kişisel verinin hukuka aykırı olarak kaydedilmesi gerekmekte olup söz konusu verilerin sır olarak nitelendirilen ve veri sahibinin diğer kişilerin erişimine izin vermediği veri niteliğinde olması aranmamaktadır⁴³⁶.

Buna karşın Yargıtay 12. Ceza Dairesi, 05.05.2014 tarihli bir kararında;

"...kişisel veri kavramından, kişinin, yetkisiz üçüncü kişilerin bilgisine sunmadığı, istediğinde başka kişilere açıklayarak ancak sınırlı bir çevre ile paylaştığı, herkes tarafından bilinmeyen ve/veya kolaylıkla ulaşılması ve bilinmesi mümkün olmayan, kişinin kimliğini belirleyen veya belirlenebilir kılan, kişiyi toplumda yer alan diğer bireylerden ayıran ve onun niteliklerini ortaya koymaya elverişli, gerçek kişiye ait her türlü bilginin anlaşılması gerektiği..."

biçiminde bir kanaate yer vermiştir.⁴³⁷

Yargıtay'ın kişisel verileri; kişinin, yetkisiz üçüncü kişilerin bilgisine sunmadığı, istediğinde başka kişilere açıklayarak ancak sınırlı bir çevre ile paylaştığı, herkes tarafından bilinmeyen ve/veya kolaylıkla ulaşılması ve bilinmesi mümkün olmayan bilgiler olarak tarif ettiği bu tanım, kavramın gerek mevzuat içerisindeki ve gerekse öğreti ve içtihatlar ile benimsenen tanımı ile çelişmektedir. Zira kararda geçen bu nitelendirme, bireyin hayatının aleniyetten dokunulmazlığa doğru ortak hayat alanı, özel hayat alanı ve sır alanı olarak birbiri ile iç içe geçmiş halde bulunan yaşam alanlarına ayrıldığı görüşü ile ilk kez Alman hukukçu Hubmann tarafından ortaya atılan "üç alan teorisi" bağlamında bireyin özel hayat alanını ifade etmektedir⁴³⁸. Oysa kanunkoyucu, kişisel verilerin dahil olduğu hayat alanına ilişkin olarak herhangi bir sınırlama getirmeksizin kanunda kimliği belirli veya belirlenebilir gerçek kişiye ilişkin olduğu sürece her türlü bilgi yönünden koruma mekanizması öngörmüştür. Bu nedenle Yüksek Mahkeme'nin bu içtihadı ile ortaya koyduğu görüşe katılmamaktayız.

2.2.1.3. Fail

5237 sayılı Türk Ceza Kanunu'nun 135. maddesinde, hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verileceği öngörülmüştür.

veya ele geçirme suçundan mahkumiyetine karar verilmesi..." Yargıtay 12. CD. 2014/9544 E., 2015/46 K., 12.01.2015.

⁴³⁶ Dülger, 2013: 574.

⁴³⁷ Yargıtay 12. CD.,2013/26191 E., 2014/10756 K., 05.05.2014. Aynı yönde bk. Yargıtay 12. CD. 2014/9544 E., 2015/46 K., 12.01.2015.

⁴³⁸ Yurtsever, 2015: 11; Geçmez, 2014: 7.

Kanun koyucunun suçun failine ilişkin olarak "kimse" ifadesini kullanmış olması karşısında, bu suçun herkes tarafından işlenebileceği sonucuna varılmaktadır⁴³⁹.

Bununla birlikte, Kanun'un 137. maddesinde suçun kamu görevlisi tarafından görevinin verdiği yetkiyi kötüye kullanmak sureti ile veya belli bir meslek veya sanatın sağladığı kolaylıktan yararlanmak sureti ile işlenmiş olması halinde verilecek cezanın yarı oranında arttırılacağı düzenlenmiştir. Bu durumda, suçun failinin kamu görevlisi veya meslek ya da sanat sahibi olması suç tipini görünüşte özgü suç haline getirmektedir⁴⁴⁰.

2.2.1.4. Mağdur

Suçun konusunun ait olduğu kişi, suçun mağduru olarak kabul edilmektedir⁴⁴¹. TCK'da hukuka aykırı olarak kaydedilmesinin cezai müeyyideye bağlandığı veriler bakımından kanun metninde herhangi bir ayrıma yer verilmemiş olmasına karşın, gerekçedeki tanıma bakıldığında cezai himaye yönünden tüzel kişilere ait verilerin bu suçun konusu oluşturamayacağı sonucuna varılmaktadır⁴⁴². Nitekim KVKK'nın konusunu oluşturan kişisel veri, gerçek kişiye ait her türlü bilgi olarak tanımlanmıştır. Hal böyle iken, suçun mağduru verileri hukuka aykırı olarak kayıt altına alınan kişilerdir.

Kural olarak tüzel kişilerin bir suçun mağduru olmaları mümkün olmayıp suçun işlenmesinden dolayı bir zarara uğramaları halinde "suçtan zarar gören" olarak nitelendirilirler⁴⁴³. Ancak kişisel verilerin kaydedilmesi suçu ile korunan hukuksal menfaatin kişinin özel hayatı olarak kabul edilmesi ve özel hayat kavramının gerçek kişiye özgü bir değer olması karşısında bu suç tipi açısından tüzel kişilerin suçtan zarar gören konumunda olması mümkün görünmemektedir⁴⁴⁴.

2.2.1.5. Nitelikli Unsurlar

2.2.1.5.1. Özel Nitelikli (Hassas) Kişisel Verilerin Kaydedilmesi

2.2.1.5.1.1. Genel Olarak

KVKK 'nın 6. maddesinde "özel nitelikli veriler"; kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili

⁴³⁹ Özgenç, 2016: 191; Koca ve Üzülmüş, 2017: 113; Akdağ, 2013: 94; Aydın, 2015: 127.

⁴⁴⁰ Koca ve Üzülmüş, 2017: 113.

⁴⁴¹ Özgenç, 2016: 202; Koca ve Üzülmüş, 2017: 114.

⁴⁴² Hafızogulları ve Özen, 2009: 19.

⁴⁴³ Koca ve Üzülmüş, 2017: 115; Özgenç, 2016: 192.

⁴⁴⁴ Aksi yönde bk. Aydın, 2015: 131; Gültekin, 2012: 129.

verileri ile biyometrik ve genetik verileri olarak belirtilmiş bulunmaktadır. İşlenmeleri durumunda verinin ilgili olduğu kişinin herhangi bir şekilde ayrımcılığa tabi tutulması tehlikesi doğuran bu veriler, özel nitelikli veri grubunu oluşturmaktadır^{445, 446}.

Doktrinde ve ilgili düzenlemelerde "hassas veri (sensitive data)"⁴⁴⁷ olarak da adlandırılan özel nitelikli veriler, 07.04.2016 tarihinde Resmi Gazete'de yayımlanarak yürürlüğe giren bu kanunda oldukça geniş tutulmuş olmasına karşın, Türk Ceza Kanunu'nun 135/2. maddesinde bu veri kategorilerinden yalnızca siyasi, felsefi veya dini görüşler, ırki köken, ahlaki eğilim, cinsel yaşam, sağlık durumu ve sendikal bağlantılara yer verildiği görülmektedir.

Şu halde, KVKK'da her ne kadar kişilerin kılık ve kıyafeti, dernek ve vakıf üyeliği, ceza mahkumiyetleri, güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel veri kategorileri arasında sayılmış, başka bir deyişle hassas veri olarak kabul edilmiş ise de, bu tip veriler Türk Ceza Kanunu'nun özel veri kategorilerinin kaydedilmesi bakımından öngördüğü nitelikli cezai yaptırım ile korunamayacaktır. Yine, maddenin ikinci fıkrasında belirtilen bu özel nitelikteki veriler sınırlı sayıda olduğundan, örneğin kişinin herhangi bir derneğe olan üyeliğine ilişkin veri bu fıkra kapsamında değerlendirilemeyecektir⁴⁴⁸. Zira aksinin kabulü, TCK'nın 2. maddesinde düzenlenen *kıyas yasağını* ihlal edecektir.

2.2.1.5.1.2. Siyasi Görüş

Türk Dil Kurumu'nun Büyük Türkçe Sözlüğünde siyasi kelimesi "siyasetle ilgili, siyasal, politik"; görüş kelimesi ise "bir olay, varlık veya düşünce üzerinde varılan yargı, fikir" ifadeleri ile tanımlanmıştır. O halde, siyasi görüş kavramının neyi ifade ettiğinin anlaşılabilmesi için siyaset veya onunla eş anlamlı olan politika kavramını açıklığa kavuşturmak gerekmektedir. Politikanın eski çağlardan bugüne yapılan tanımlarında onun iki farklı yönünden hareket edildiği görülür; buna göre *"Politika, gerçekte hem bir çatışma ve iktidar kavgasıdır, hem de - hiç değilse bir ölçüde - toplumun bütün üyelerinin yararına*

⁴⁴⁵ Kişisel Verileri Koruma Kurumu, 6698 Sayılı Kişisel Verilerin Korunmasına Yönelik Soru ve Cevaplar, s. 20, <http://www.kvkk.gov.tr/yayinlar/6698%20SAYILI%20K%C4%B0%C5%9E%C4%B0SEL%20VER%C4%B0LER%C4%B0N%20KORUNMASI%20KANUNUNUN%20UYGULANMASINA%20Y%C3%96NEL%C4%B0K%20SORU%20VE%20CEVAPLAR.pdf> (erişim tarihi:05.11.2017); Dülger, 2016: 109.

⁴⁴⁶ Örneğin nüfus kayıtlarının ayrıntılı ve kişilerin etnik kökeni ve dini görüşü gibi hassas verilerini içerir biçimde tutulmasının Yahudi soykırımında etkili olduğu ifade edilmektedir. (Dülger, 2016: 109).

⁴⁴⁷ Dülger, 2016: 109.

⁴⁴⁸ Taşkın, 2008: 100.

olabilecek bir düzen yaratma aracıdır"⁴⁴⁹. Dolayısı ile siyasi veya politik görüş, iktidar kavgası temelinde kişinin devletin etkinliklerini düzenleme ve gerçekleştirme biçimine dair vardığı yargı ya da fikirdir. Özel veri kategorileri içerisinde bulunan bu kavram, 1992 tarihli İsviçre Federal Veri Koruma Kanunu'nda "ideolojik görüş ve faaliyetler" olarak ifade edilmiştir⁴⁵⁰.

2.2.1.5.1.3. Felsefi ve Dini Görüş

Gerek 95/46/AT sayılı Yönerge'de ve gerekse 2016/679 sayılı Tüzük'te özel veri kategorileri arasında sayılan felsefi ve dini inançlara ilişkin veriler, 5237 sayılı Türk Ceza Kanunu'nun 135. maddesinin 2. fıkra düzenlemesinde inanç (belief) kelimesi yerine görüş kelimesi tercih edilerek *'felsefi görüş ve dini görüşlere ilişkin veri'* olarak belirtilmiştir. Felsefi inanç kavramının uygulama açısından tanımlanması ve içeriği doldurulması zor bir nitelik taşıması nedeni ile bu kavrama hukuksal metinde yer verilmesi eleştirilmiş olmasına karşın⁴⁵¹ TCK'da "inanç" kelimesi yerine çok daha geniş kapsamlı ve sınırlarının çizilmesi zor olan "görüş" kelimesi kullanılmıştır. AIHM, İnsan Hakları ve Temel Özgürlüklerin Korunmasına İlişkin Sözleşme'ye Ek 1 Nolu Protokol'ün 2. maddesinin⁴⁵² ihlal edildiği iddiasına ilişkin bir başvuruyu incelediği kararında, dini ve felsefi bağlamda kullanılan "inançlar" kelimesinin Sözleşme'nin "ifade özgürlüğü"nü düzenleyen 10. maddesinin koruması altında olan "fikirler" ve "düşünceler" kelimeleri ile eş anlamlı olmadığını, "din ve vicdan özgürlüğü"nü düzenleyen 9. maddesi bağlamında değerlendirilmesi gerektiği kanaatine varmıştır⁴⁵³. Burada dikkat edilmesi gereken, kavramın belirli bir ölçüde inandırıcılık, ciddiyet, tutarlılık ve önem taşıyan görüşleri ifade etmesidir⁴⁵⁴.

⁴⁴⁹ Kapani, 2007: 18.

⁴⁵⁰ Kaya, 2011: 319.

⁴⁵¹ Article 29 Data Protection Working Party, Advice Paper On Special Categories of Data ("sensitive data"), Ref. Ares(2011)444105 - 20/04/2011, s. 10. http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf (erişim tarihi:30.12.2017)

⁴⁵² Madde 2 - Eğitim hakkı

Hiç kimse eğitim hakkından yoksun bırakılamaz. Devlet, eğitim ve öğretim alanında yükleneceği görevlerin yerine getirilmesinde, ana ve babanın bu eğitim ve öğretimin kendi dini ve felsefi inançlarına göre yapılmasını sağlama haklarına saygı gösterir.

⁴⁵³ Campbell ve Cosans/İngiltere kararı, başvuru no: 7511/76; 7743/76;25.02.1982 (parg.:36; [https://hudoc.echr.coe.int/eng#{"itemid":\["001-57455"\]}](https://hudoc.echr.coe.int/eng#{)) (erişim tarihi:30.12.2017).

⁴⁵⁴ Doğru ve Nalbant, 2013: 766.

Felsefi kelimesi bakımından ise sınırlayıcı bir tanım yapılması hayli güç olup felsefi inancı, insan onuru ile bağdaşmaz olmayan ve demokratik bir toplumda saygıyı hak eden inanç ve kanaat olarak tanımlamak gerekir⁴⁵⁵. TCK bakımından da bu kanunda yer alan felsefi ve dini görüş kavramlarının kişinin ayrımcılığa uğratılması riski barındırması kriteri göz önünde bulundurularak, Ateizm, Deizm, Hinduizm, Brahmanizm, Yahudilik, Hristiyanlık, İslamiyet gibi kişide inanç seviyesine ulaşmış kabullere işaret ettiği yerinde olarak savunulmaktadır⁴⁵⁶. Felsefi ve dini görüş kavramları anlamları ve esasları bakımından birlikte değerlendirilmelidir. Zira varolanların varlığı, anlamı ve varoluş nedeni üzerine gerçekleştirilen düşünme faaliyeti başlangıçta dini temeller üzerinde gerçekleştirilirken eleştirel düşünce ve gözlemin konusu haline gelince felsefenin doğumu söz konusu olmuştur⁴⁵⁷.

Bir kişinin uçak yolculuğu esnasında yemek tercihinin Yahudi inancına uygun (kosher) veya Müslüman inancına uygun (helal) yemeklerden yana kullanması durumunda Havayolu şirketi tarafından kaydedilecek bu veri dini inanç biçimindeki özel veri kategorisindedir⁴⁵⁸. Yine, Birleşik Krallık'ta bir mahkeme, küresel ısınmaya dair inancı, felsefi inanç olarak kabul etmiştir⁴⁵⁹.

2.2.1.5.1.4. Irki Köken

İrk, kalıtsal olarak ortak fiziksel ve fizyolojik özelliklere sahip insanlar topluluğu olarak tanımlanmakta⁴⁶⁰ olup bir kişinin irki kökeninin bilgisi kimi zaman onun salt bu nedenle ayrımcılığa tabi tutulması riskini doğurmaktadır. Bu nedenle AİHS'nin 14. maddesi⁴⁶¹ ile ayrımcılık yasaklanmış olup AİHM, kişilerin irki kökenleri nedeni ile

⁴⁵⁵ *Campbell ve Cosans/İngiltere kararı*, başvuru no: 7511/76; 7743/76; 25.02.1982; parag.:36.

⁴⁵⁶ Akdağ, 2013: 33.

⁴⁵⁷ http://tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.5a4775ae9a7ff0.20230552 (erişim tarihi:30.12.2017).

⁴⁵⁸ Handbook on European Data Protection Law, 87,

https://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf (erişim tarihi:24.01.2018)

⁴⁵⁹ Madde 29 Çalışma Grubu, 2011: 8, http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf (erişim tarihi:30.12.2017)

⁴⁶⁰ http://tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.5a482e93401a29.08983880 (erişim tarihi:31.12.2017)

⁴⁶¹ Madde 14

ayrımcılığa uğradıkları iddiasını incelediği kararlarında ırk ayrımcılığını ve devletin ırk ayrımcılığına karşı üstlenmesi gerektiği rolü aşağıdaki gibi belirlemiştir:

*"Bir kişiye, diğerlerinin yanı sıra etnik kökeni nedeniyle yapılan ayrımcılık, bir tür ırk ayrımcılığıdır. Irk ayrımcılığı, ayrımcılığın insanları özellikle inciten bir türü olup, tehlikeli sonuçları nedeniyle yetkililerin özel önem vermesini ve güçlü bir şekilde tepkide bulunmasını gerektirmektedir. Bu nedenle yetkililerin kendilerine elverişli olan her türlü imkânı kullanarak ırkçılıkla mücadele etmeleri ve farklılıkların bir tehdit olarak değil, bir tür zenginlik kaynağı olarak görüldüğü demokratik toplum vizyonunu güçlendirmeleri gerekmektedir."*⁴⁶².

*"Mahkeme ayrıca, tamamen ya da büyük oranda kişinin etnik kökenini temel alan muamele farkının, çoğulculuk ve farklı kültürlerle saygı ilkeleri üzerine kurulu olan çağdaş demokratik toplumlarda nesnel olarak gerekçelendirilemeyeceğine hükmetmiştir"*⁴⁶³.

Irki kökene ait veriler, kişilerin siyah, beyaz, Afrika kökenli, Asya kökenli⁴⁶⁴, Roman⁴⁶⁵, Çeçen⁴⁶⁶, Türk⁴⁶⁷ olması gibi bilgiyi içermekte olup kişilerin irki ve etnik kökene göre sınıflandırılması tarihsel olgular ile medeni haklar hareketi ve yasama faaliyetlerine dayanmaktadır⁴⁶⁸.

Bu Sözleşme'de tanınan hak ve özgürlüklerden yararlanma, cinsiyet, ırk, renk, dil, din, siyasal veya diğer kanaatler, ulusal veya toplumsal köken, ulusal bir azınlığa aidiyet, servet, doğum başta olmak üzere herhangi başka bir duruma dayalı hiçbir ayrımcılık gözetilmeksizin sağlanmalıdır.

⁴⁶² *Nachova ve Diğerleri/Bulgaristan*, Başvuru no: 43577/98 ve 43579/98, 6.7.2005,

[https://hudoc.echr.coe.int/eng#{\"tabview\":\"document\", \"itemid\":\"001-69630\"}](https://hudoc.echr.coe.int/eng#{\) (erişim tarihi:31.12.2017);

Timishev/Rusya, Başvuru no: 55762/00 ve 55974/00, 13.12.2005,

[https://hudoc.echr.coe.int/eng#{\"tabview\":\"document\", \"itemid\":\"001-71627\"}](https://hudoc.echr.coe.int/eng#{\), (erişim tarihi:31.12.2017);

Adalet Bakanlığı Uluslararası Hukuk ve Dış İlişkiler Genel Müdürlüğü İnsan Hakları Daire Başkanlığı, 2013:5-6, http://www.echr.coe.int/Documents/FS_Racial_discrimination_TUR.pdf (erişim tarihi:31.12.2017).

⁴⁶³ *Timishev/Rusya*, Başvuru no: 55762/00 ve 55974/00, 13.12.2005, Adalet Bakanlığı Uluslararası Hukuk ve Dış İlişkiler Genel Müdürlüğü İnsan Hakları Daire Başkanlığı, 2013:6, http://www.echr.coe.int/Documents/FS_Racial_discrimination_TUR.pdf (erişim tarihi:31.12.2017).

⁴⁶⁴ Amerika Nüfus Bürosu, 2002:100.

⁴⁶⁵ *Nachova ve Diğerleri/Bulgaristan*, Başvuru no: 43577/98 ve 43579/98, 6.7.2005.

⁴⁶⁶ *Timishev/Rusya*, Başvuru no: 55762/00 ve 55974/00, 13.12.2005.

⁴⁶⁷ *Turan Çakır/Belçika*, başvuru no: 44256/06, 10.3.2009, [https://hudoc.echr.coe.int/eng#{\"itemid\":\"001-111151\"}](https://hudoc.echr.coe.int/eng#{\), (erişim tarihi:31.12.2017)

⁴⁶⁸ Idler, 2007:37.

Irki köken kavramına bir yasa metninde yer verilmesi eleştirilmektedir⁴⁶⁹. Zira son bilimsel gelişmelere göre, homo sapiens yani insan türü farklı ırklara ya da alt türlere ayrılmadığı kanaatine varılmış, 1970’lerden bu yana moleküler biyoloji ve nüfus genetiği bu tür sistematik ayrımların ortadaki muazzam çeşitliliği açıklayamamakta ve esasen insanlar arasındaki genetik çeşitlilik coğrafi ve iklimsel farklılıklardan kaynaklanmaktadır⁴⁷⁰; bu sebeplerle yasa metninde yer alan ırki köken kavramının belirsiz olduğu ve belirli bir etnik kökene ait verilere işaret ettiği savunulmaktadır⁴⁷¹. 2016/679 sayılı Tüzük’ün 9. maddesinde düzenlenen özel veri kategorilerinde “ırksal menşei” kavramına yer verilmiş olmakla birlikte, metnin başlangıç kısmının 51. maddesinde, tüzükte bu kavrama yer verilmesinin Birliğin farklı insan ırklarının varlığını kabul ettiği anlamına gelmediği vurgulanmıştır.

2.2.1.5.1.5. Ahlaki Eğilim

Kanunkoyucu, TCK’nın 135. maddesinde cezanın artırım nedeni olarak öngördüğü özel veri kategorileri içerisinde ahlaki eğilim kavramına da yer vermiş bulunmaktadır. Bir kişinin, hangi verilerinin ahlaki eğilimine ilişkin olduğunun belirlenmesi oldukça güçtür. Zira kanunun gerekçesinde bu kavramdan ne anlaşılması gerektiği açıklanmadığı gibi KVKK’nın 6. maddesinde de ahlaki eğilim kavramı özel veri kategorileri içerisinde sayılmamıştır. Aynı şekilde kişisel verilerin korunmasına dair uluslararası düzenlemelerde de ahlaki eğilim biçiminde bir hassas veri grubuna rastlanmamaktadır.

Kişinin ahlaki eğilimine ilişkin verilerinin neleri kapsadığının anlaşılabilmesi için “ahlak” kavramının tanımlanması gerekir. Türk Dil Kurumu’na göre ahlak, “*belli bir dönemde belli insan topluluklarınca benimsenmiş olan, bireylerin birbirleriyle ilişkilerini düzenleyen törel davranış kurallarının, yasalarının, ilkelerinin toplamı*”dır. Bu tanımdan, ahlakın zamana ve yere göre değişiklik gösteren bir olgu olduğu ve değer yargıları ile

⁴⁶⁹ Madde 29 Çalışma Grubu, 2011: 10, http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf (erişim tarihi: 31.12.2017)

⁴⁷⁰ Madde 29 Çalışma Grubu, 2011: 10; Somersan, 2012:5 <http://secbir.org/images/haber/2011/01/17-semra-somersan.pdf> (erişim tarihi:31.12.2017)

⁴⁷¹ Madde 29 Çalışma Grubu, 2011: 10, http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf (erişim tarihi: 31.12.2017)

davranış kurallarından meydana geldiği anlaşılmaktadır⁴⁷². Eğilim ise “*bir şeyi sevmeye, istemeye veya yapmaya içten yönelme, meyil, temayül*” olarak tanımlanmıştır⁴⁷³.

TCK’da ahlak kavramına 135. maddenin yanında; 225. ve devamı maddelerde düzenlenen; alenen cinsel ilişkide bulunma ve teşhircilik yapma biçiminde hayasızca hareketler, müstehcenlik, fuhuşa teşvik ve aracılık, kumar oynanması için yer ve imkan sağlama, çocukları ve beden veya ruh bakımından kendini idare edemeyecek kişileri dilencilikte araç olarak kullanmak suçlarının “*genel ahlaka karşı suçlar*” başlığı altında toplanmak sureti ile değinilmiştir. Yine, aile hukukundan kaynaklanan yükümlülüğünün ihlali başlıklı 233. maddenin 3. fıkrası⁴⁷⁴ ile itiyadi sarhoşluk ile uyuşturucu ve uyarıcı maddelerin kullanılmasının ahlak kavramı ile ilişkilendirildiği görülmektedir. Hal böyle iken, bir kişinin fuhuş, kumar, dilencilik, itiyadi sarhoşluk ile uyuşturucu ve uyarıcı maddeler ile olan ilişkisini gösterir verilerin ahlaki eğilimine işaret ettiği söylenebilir⁴⁷⁵. Ancak kanun temelinde yapılacak böyle bir yorum dahi ahlaki eğilim kavramını netleştirememekte ve sınırlarını çizememektedir. Örneğin; bir kişinin borçlarını devamlı olarak ödememesi, dindarlığı ya da bir sporcunun doping kullandığına ilişkin verinin ahlaki eğilime işaret edip etmediği belirsizdir ve bu hususta yapılacak seçim görecelidir. Bunun yanında kişiye ilişkin birtakım bilgilerin sınıflandırılması bakımından ahlaki eğilim ile madde metninde ağırlaştırıcı neden olarak öngörülen diğer veri kategorileri arasında seçim yapmak oldukça zordur. Örneğin; bir kişinin pedofili, nekrofil veya kleptomani olduğu bilgisi kişinin ahlaki eğilimine ilişkin kişisel veri olarak kabul edilebileceği gibi sağlık durumu olarak da nitelendirilebilir.

Esasen ahlaki eğilim kavramının, TCK madde 135’te düzenlenen suç bakımından ağırlaştırıcı neden olarak öngörülmüş olması, kanunilik ilkesi bakımından problemli görünmektedir. Kanunilik ilkesinin en önemli sonucu belirlilik prensibi olmakla, bir suçun maddi unsurunun mümkün olduğunca açık bir biçimde kanunda gösterilmesi ceza hukukunun

⁴⁷² Kuçuradi, 2009: 31,33’ten aktaran; Eryılmaz, 2015: 12.

⁴⁷³ http://tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.5ae303f5f30fe6.85073425 (erişim tarihi: 31.12.2017)

⁴⁷⁴ “*Velayet hakları kaldırılmış olsa da, itiyadi sarhoşluk, uyuşturucu veya uyarıcı maddelerin kullanılması ya da onur kırıcı tavır ve hareketlerin sonucu maddi ve manevi özen noksanlığı nedeniyle çocuklarının ahlak, güvenlik ve sağlığını ağır şekilde tehlikeye sokan ana veya baba, üç aydan bir yıla kadar hapis cezası ile cezalandırılır.*”

⁴⁷⁵ Aynı yönde bk. Akdağ, 2013: 33-34.

güvence fonksiyonunun gereğidir⁴⁷⁶. Ceza kanununda suç oluşturan eylemler, kapsamının belirlenmesinde tereddüt yaratmayacak ölçüde net olarak tanımlanmalıdır⁴⁷⁷.

2.2.1.5.1.6. Cinsel Yaşam

Cinsellik, Dünya Sağlık Örgütü tarafından şu şekilde tanımlanmıştır:

“Cinsellik, hayat boyunca insan olmanın merkezi bir yanını oluşturur ve cinsiyeti, cinsel kimlikleri ve rolü, cinsel uyumu, erotizmi, cinsel ilişki ve üremeyi kapsar. Cinsellik, düşüncede fantazilerde, arzulara, inançlarda, tutumlarda, değerlerde, davranışlarda, uygulamalarda, rollerde ve ilişkilerde tecrübe ve ifade edilir. Cinselliğin tüm bu boyutları içermesine rağmen, her zaman bunların hepsinin tecrübe veya ifade edildiği anlamına gelmez. Cinsellik biyolojik, psikolojik, sosyal, ekonomik, politik, kültürel, etik, yasal, tarihsel, dini ve ruhani faktörlerin etkisi altındadır.”⁴⁷⁸

Cinselliğin yukarıda açıklanan çok yönlü niteliği sonucunda kanunda yer alan “cinsel yaşam” ifadesi de oldukça kapsamlıdır ve kimliği belirli veya belirlenebilir bireyin cinselliği ile ilgili bütün verilerin cinsel yaşamına ait kişisel veri olduğu kabul edilebilir. Ancak kişinin cinsel yaşamına ilişkin olup da ayrımcılığa tutulması riskinin en yüksek olduğu verilerinin cinsel yönelime dair bilgiler olduğu görülmektedir⁴⁷⁹. Cinsel yönelim kişinin cinsel his ve tutumunun belirli bir cinsiyete olan çekimi olarak ifade edilmekte olup bunlardan eşcinsellik, biseksüellik veya transseksüellik biçimindeki yönelimlere sahip (lgbt⁴⁸⁰) kişilerin eğitim, sağlık, iş ortamı ve askerlik gibi süreçlerde zorluklarla karşılaştığı, önyargıya ve ayrımcılığa maruz kaldığı bilinen bir durumdur⁴⁸¹. Bu kişiler birçok toplumda, toplumsal cinsiyet⁴⁸²

⁴⁷⁶ Artuk vd., 2013: 110; Hakeri, 2012: 14; Koca ve Üzülmmez, 2017: 59 - 60.

⁴⁷⁷ Hafizoğulları ve Özen, 2010: 19; Koca ve Üzülmmez, 2017: 57.

⁴⁷⁸ Dünya Sağlık Örgütü, 2006: 5,

http://www.who.int/reproductivehealth/publications/sexual_health/defining_sexual_health.pdf?ua=1 (erişim tarihi:24.12.2017)

⁴⁷⁹ Akdağ, 2013: 34.

⁴⁸⁰ Lezbiyen, gey, biseksüel, transseksüel kelimelerinin baş harflerinin bir araya getirilmesi ile oluşan ve bu şekilde cinsel yönelimleri olan bireyleri ifade etmek için kullanılan kısaltmadır.

⁴⁸¹ Hekimoğlu, 2017: 109.

⁴⁸² “Kadınlar ve erkekler için yaygın olarak kabul edilen düşünce ve beklentileri (normları) ifade eder. Bunlar “tipik” olarak dişi (ya da feminen) ve erkeksi (maskülen ya da eril) özellikleri ve yetileri ve çeşitli durumlar karşısında kadınların ve erkeklerin nasıl davranması gerektiği konusunda genelin paylaştığı beklentileri içerir.” (Bozdemir ve Özcan, 2011: 38, <http://dergipark.ulakbim.gov.tr/tjfmmpc/article/viewFile/5000055970/5000053179> (erişim tarihi:25.12.2017))

kalıplarına tehdit olarak algılanarak saygınlığı hak etmeyen ve hasta bireyler olarak kabul görmektedirler⁴⁸³.

Lgbt bireylerin, yalnızca cinsel yönelimleri nedeni ile ayrımcılığa tabi tutulduğu, AİHM tarafından karara bağlanan *X/Türkiye*⁴⁸⁴ davasında somutlaşmıştır. Mahkemenin önüne gelen başvuruya konu olan olay, eşcinsel olan başvurunun tutuklu olarak cezaevinde bulunduğu sırada, cinsel eğilimi nedeni ile diğer mahpusların taciz ve sindirme eylemlerine maruz kalması sonucunda eşcinsel mahpusların bulunduğu bir koğuşa nakledilmesini istemesinin ardından cezaevi yönetiminin onu sekiz ay on gün boyunca diğer mahpuslar ile her türlü temas ve sosyal aktiviteden mahrum bırakarak ve açık havaya çıkma imkanı vermeyerek, tek kişilik 7 m² büyüklüğünde, pis, aydınlatması yetersiz, lavabosuz ve içinde farelerin bulunduğu bir koğuştaki tecrit etmesi biçiminde cereyan etmiştir⁴⁸⁵. Olayda dikkat çeken husus, süreçteki yazışmalarda başvurunun, kendisine ait dilekçede dahi “eşcinsellik hastalığına yakalanan kişi” olarak tabir edilmesidir. Bu durum, başvurunun kendisine yönelen fiziksel ve psikolojik tacize karşı korunmanın tek yolunun eşcinselliğini bir hastalık olarak kabul etmesi ile mümkün olabileceğine inandığını göstermektedir⁴⁸⁶. Bu olay, kişinin cinsel yaşamına ilişkin kişisel verilerinin özel nitelikli veri olarak kabul edilmesinin yerindeliğinin somut bir örneğidir.

2.2.1.5.1.7. Sağlık Durumu

KVKK'nın 6. maddesinde özel nitelikli kişisel veriler kategorisinde "kişinin sağlığı" biçiminde ifade edilmiş bulunmakla 20.10.2016 tarihli ve 29863 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren "*Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik*"ın 4. maddesinde "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü sağlık bilgisi" olarak tanımlanmıştır. Avrupa Birliği'nin 2016/679 sayılı Tüzük'ün 4. maddesinde ise "*sağlığa ilişkin veri*" kavramı kullanılmış ve görece ayrıntılı bir tanım yapılmış bulunmaktadır. Buna göre sağlığa ilişkin veri, gerçek bir kişinin sağlık durumu hakkında bilgi ortaya koyan sağlık hizmetleri kayıtları dahil olmak üzere kişinin

⁴⁸³ Şah, 2012:24.

http://193.255.56.45:8080/xmlui/bitstream/handle/123456789/272/Sah%2c%20Umut_2012.pdf?sequence=1&isAllowed=y (erişim tarihi:25.12.2017).

⁴⁸⁴ *X/Türkiye*, Başvuru no:24626/09, 9.10.2012, [https://hudoc.echr.coe.int/eng#{"itemid":\["001-120280"\]}](https://hudoc.echr.coe.int/eng#{) (erişim tarihi:30.12.2017)

⁴⁸⁵ *X/Türkiye*, Başvuru no:24626/09, 9.10.2012, par. 42.

⁴⁸⁶ Canveren ve Özeren, 2014: 81.

fiziksel veya akıl sağlığına ilişkin olan verilerdir⁴⁸⁷. Dolayısı ile hastalığın türü, hastanın ve hastalığın öyküsü, teşhis, tedavi, psikolojik belirtiler, uzuv eksiklikleri, muayene sonuçları, tıbbi tahlil sonuçları, görüntüleme filmleri sağlığa ilişkin verilere örnek gösterilebilir⁴⁸⁸. Tıbbi veriler olarak da adlandırılabilir bu veriler, mahiyeti itibari ile tıp mesleği mensuplarınca edinilebilecek bilgilerden olup kötüye kullanılmaları halinin ilgisine vereceği zararın boyutu nazara alındığında özel veri kategorisi olarak kabul edilmesi ve kaydedilmelerinin özel bir usule tabi tutulması yerindedir⁴⁸⁹. AIDS hastalığını taşıyan bir kişinin sağlık durumunu gösteren bilgilerin işlenmesi halinde bu kişinin toplumsal yaşamda veya iş yaşamında ayrımcılığa maruz kalması bu duruma örnek olarak gösterilebilir.

Bir İngiliz gazetesi tarafından uyuşturucu bağımlılığına yönelik bir rehabilitasyon merkezinin çıkışında çekilen fotoğraflarının gazetede uyuşturucu bağımlısı olduğuna dair yayınlanan haberde kullanılması nedeni ile veri öznesi tarafından açılan davada⁴⁹⁰, veri öznesinin gördüğü tedaviye ilişkin detayları içeren bu fotoğraf ve haber, kişinin fiziksel veya ruhsal sağlık durumu ile ilgili olduğundan hassas veri olarak kabul edilmiştir⁴⁹¹.

2.2.1.5.1.8. Sendikal Bağlantı

6356 sayılı Sendikalar ve Toplu İş Sözleşmesi Kanunu uyarınca sendika, “İşçilerin veya işverenlerin çalışma ilişkilerinde, ortak ekonomik ve sosyal hak ve çıkarlarını korumak ve geliştirmek için en az yedi işçi veya işverenin bir araya gelerek bir işkolunda faaliyette bulunmak üzere oluşturdukları tüzel kişiliğe sahip kuruluşlar”ı ifade eder. 4688 sayılı Kamu Görevlileri Sendikaları ve Toplu Sözleşme Kanunu’nda ise “Kamu görevlilerinin ortak ekonomik, sosyal ve meslekî hak ve menfaatlerini korumak ve geliştirmek için oluşturdukları tüzel kişiliğe sahip kuruluşları” biçiminde tanımlanmıştır.

Temsil ettikleri grubun ortak çıkarlarını koruma ve geliştirme gayesinde olan sivil toplum kuruluşları sendikalar, bu gayelerini hayata geçirebilmek için sendikacılığın ekonomik ve sosyal yönünün yanı sıra siyasal fonksiyonundan da yararlanmak zorundadır; zira siyasi partiler de örgütlü güç niteliğindeki sendikalara oy oranlarını artırmak için siyasi partilerle

⁴⁸⁷ http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf (erişim tarihi:06.11.2017).

⁴⁸⁸ Akgül, 2013: 11.

⁴⁸⁹ Yokuş Sevil, 2008: 784.

⁴⁹⁰ Campbell/ Mirror Group Newspapers Ltd., House of Lords, Birleşik Krallık, 2004 ([2002] EWHC 499 (QB); [2002] EMLR 617); Akrivopoulou ve Garipidis, 2014: 227.

⁴⁹¹ İtişgen, 2015: 183.

ilişki kurma yoluna gitmektedirler⁴⁹². Başka bir anlatımla; karşılıklı fayda öngören bu sistemde, sendika açısından üyelerinin menfaatlerinin korunması bağlamında talep edilen haklar çoğu zaman yasal bir düzenleme gerektirdiğinden sendikaların siyasi ortama dahil olarak siyasal faaliyette bulunmaları kaçınılmazdır⁴⁹³. Sendikaların siyasi faaliyetleri ve siyasi partiler ile olan ilişkisi, bulunduğu ülkenin çalışma ilişkilerine ilişkin mevzuatına, siyasal rejiminin özelliğine –çoğulcu demokratik veya totaliter gibi- ;kültürel, tarihsel birikimine ve son olarak sendikaların siyaset yapma eğilimine göre farklılık arz etmekle, sendikaların siyasi rolü bu kriterlere göre şekillenmektedir⁴⁹⁴.

Türkiye’de sendika kurma ve sendikaya üye olma, Anayasa’nın 51. maddesinde sosyal ve ekonomik haklar kapsamında öngörülmüş temel bir insan hakkıdır⁴⁹⁵. Ancak sendika üyeliği, sendikaların yukarıda sözü edilen siyasi karakteri nedeni ile ilgisinin ayrımcılığa tabi tutulma riskini de beraberinde getirir. Bu nedenledir ki, 6356 sayılı Sendikalar ve Toplu İş Sözleşmesi Kanunu’un 25. maddesinde işverenin, işçinin sendikal özgürlüğünü kısıtlayan ayrımcılık niteliğindeki faaliyetleri sendikal tazminat yaptırımına bağlanmıştır⁴⁹⁶. İşte bu

⁴⁹² Mahiroğulları, 2004: 350, <http://dspace.marmara.edu.tr/bitstream/handle/11424/1817/5000007359-5000012160-1-SM.pdf?sequence=1>. (erişim tarihi:24.12.2017)

⁴⁹³ Mahiroğulları, 2004: 352, <http://dspace.marmara.edu.tr/bitstream/handle/11424/1817/5000007359-5000012160-1-SM.pdf?sequence=1>. (erişim tarihi:24.12.2017)

⁴⁹⁴ Sendikacılığın siyasi partilerle olan ilişkisinin Türkiye açısından tarihsel gelişimi konusunda bk. Mahiroğulları, 2003: 43-46.

⁴⁹⁵ *Sendika kurma hakkı*

Madde 51 – (Değişik: 3/10/2001-4709/20 md.) Çalışanlar ve işverenler, üyelerinin çalışma ilişkilerinde, ekonomik ve sosyal hak ve menfaatlerini korumak ve geliştirmek için önceden izin almaksızın sendikalar ve üst kuruluşlar kurma, bunlara serbestçe üye olma ve üyelikten serbestçe çekilme haklarına sahiptir. Hiç kimse bir sendikaya üye olmaya ya da üyelikten ayrılmaya zorlanamaz.

Sendika kurma hakkı ancak, millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâk ile başkalarının hak ve özgürlüklerinin korunması sebepleriyle ve kanunla sınırlanabilir.

Sendika kurma hakkının kullanılmasında uygulanacak şekil, şart ve usuller kanunda gösterilir.

(Mülga dördüncü fıkra: 7/5/2010-5982/5 md.)

İşçi niteliği taşımayan kamu görevlilerinin bu alandaki haklarının kapsam, istisna ve sınırları gördükleri hizmetin niteliğine uygun olarak kanunla düzenlenir.

Sendika ve üst kuruluşlarının tüzükleri, yönetim ve işleyişleri, Cumhuriyetin temel niteliklerine ve demokrasi esaslarına aykırı olamaz.

⁴⁹⁶ *Sendika özgürlüğünün güvencesi*

MADDE 25 – (1) İşçilerin işe alınmaları; belli bir sendikaya girmeleri veya girmemeleri, belli bir sendikadaki üyeliği sürdürmeleri veya üyelikten çekilmeleri veya herhangi bir sendikaya üye olmaları veya olmamaları şartına bağlı tutulamaz.

ayrımcılık riski, kişilerin sendikal bağlantılarını gösteren kişisel verilerinin kişinin siyasi inanç veya yakınlığının güçlü bir göstergesi olması hasebiyle özel veri kategorisi olarak kabul edilmesini gerektirmiştir⁴⁹⁷.

Sendikal bağlantıya ilişkin kişisel verinin işlenmesinin yasal düzenleme ile öngörülmüş olması halinde hukuka uygun kabul edileceğinde bir tartışma bulunmamaktadır. Örneğin, 4688 sayılı Kamu Görevlileri Sendikaları ve Toplu Sözleşme Kanunu'nun "Üyelik Ödentisi" başlıklı 25. maddesindeki,

"Kamu görevlileri sendikasına, kamu görevlisinin ödeyeceği üyelik ödentileri, 14 üncü madde çerçevesinde doldurulan üyelik başvuru formuna ve sendika tüzüğünde belirtilen aylık ödenti tutarına göre kamu işverenince aylığından kesilerek beş gün içinde sendikaların banka hesaplarına yatırılır ve ödenti listesinin bir örneği ilgili sendikaya gönderilir. Kamu işvereni, sendikaya üye olan ve üyelik ödentisi kesilen kamu görevlilerinin listesini her ayın son haftasında, işyerinde herkesin görebileceği yerde ve kurumsal düzeyde duyurulabilecek diğer araçlarla ilan eder."

(2) İşveren, bir sendikaya üye olan işçilerle sendika üyesi olmayan işçiler veya ayrı sendikalara üye olan işçiler arasında, çalışma şartları veya çalıştırmaya son verilmesi bakımından herhangi bir ayırım yapamaz. Ücret, ikramiye, prim ve paraya ilişkin sosyal yardım konularında toplu iş sözleşmesi hükümleri saklıdır.

(3) İşçiler, sendikaya üye olmaları veya olmamaları, iş saatleri dışında veya işverenin izni ile iş saatleri içinde işçi kuruluşlarının faaliyetlerine katılmaları veya sendikal faaliyette bulunmalarından dolayı işten çıkarılamaz veya farklı işleme tabi tutulamaz.

(4) İşverenin (...) (1) yukarıdaki fıkralara aykırı hareket etmesi hâlinde işçinin bir yıllık ücret tutarından az olmamak üzere sendikal tazminata hükmedilir. (1)

(5) Sendikal bir nedenle iş sözleşmesinin feshi hâlinde işçi, 4857 sayılı Kanunun (...) (2) , 20 ve 21 inci madde hükümlerine göre dava açma hakkına sahiptir. İş sözleşmesinin sendikal nedenle feshedildiğinin tespit edilmesi hâlinde, 4857 sayılı Kanunun 21 inci maddesine göre işçinin başvurusu, işverenin işe başlatması veya başlatmaması şartına bağlı olmaksızın sendikal tazminata karar verilir. Ancak işçinin işe başlatılmaması hâlinde, ayrıca 4857 sayılı Kanunun 21 inci maddesinin birinci fıkrasında belirtilen tazminata hükmedilmez. İşçinin 4857 sayılı Kanunun yukarıdaki hükümlerine göre dava açmaması ayrıca sendikal tazminat talebini engellemez. (2)

(6) İş sözleşmesinin sendikal nedenle feshedildiği iddiası ile açılacak davada, feshin nedenini ispat yükümlülüğü işverene aittir. Feshin işverenin ileri sürdüğü nedene dayanmadığını iddia eden işçi, feshin sendikal nedene dayandığını ispatla yükümlüdür.

(7) Fesih dışında işverenin sendikal ayrımcılık yaptığı iddiasını işçi ispat etmekle yükümlüdür. Ancak işçi sendikal ayrımcılık yapıldığını güçlü biçimde gösteren bir durumu ortaya koyduğunda, işveren davranışının nedenini ispat etmekle yükümlü olur.

(8) Yukarıdaki hükümlere aykırı olan toplu iş sözleşmesi ve iş sözleşmesi hükümleri geçersizdir.

(9) İşçinin iş kanunları ve diğer kanunlara göre sahip olduğu hakları saklıdır.

⁴⁹⁷

düzenlemesi uyarınca, kamu kurumlarının bu vesileyle kamu görevlilerinin sendikal bağlantılarını gösteren kişisel verilerini internet sitelerinde yayınladığı görülmektedir. Burada sendikal bağlantıya ilişkin kişisel verilerin işlenmesi dayanağını her ne kadar kanuni düzenlemeden alıyor olsa da bu verilerin işlenmesine KVKK'ın 4. maddesinin ve özellikle “ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme” ile “doğru ve gerektiğinde güncel olma” ilkelerinin gözetilmesi gerektiği, aksi takdirde TCK'nın 135. maddesinde düzenlenen suça konu olabileceği unutulmamalıdır.

2.2.1.5.2. Suçun Kamu Görevlisi Tarafından ve Görevinin Verdiği Yetkinin Kötüye Kullanılması Suretiyle İşlenmesi

TCK'nın 137/1-a maddesine göre kişisel verileri hukuka aykırı olarak kaydedilmesi suçunun bir kamu görevlisi tarafından ve görevinin verdiği yetkinin kötüye kullanılması suretiyle işlenmesi halinde verilecek cezanın yarı oranında arttırılmaktadır.

Fail hakkında suçun söz konusu nitelikli hali uyarınca cezaya hükmolunabilmesi için kamu görevlisi kavramının açıklığa kavuşturulması, bu kapsamda failin kamu görevlisi olup olmadığının belirlenmesi ile bu görevin ona verdiği yetkinin kötüye kullanılması suretiyle işlenip işlenmediğinin tespit edilmesi gereklidir. Öğretide söz konusu nitelikli halin, TCK'nın 257. maddesinde düzenlenen görevi kötüye kullanma suçunun birinci fıkrasının özel bir halini teşkil ettiği savunulmakta ise de⁴⁹⁸, bu düşüncenin görevi kötüye kullanma suçu yönünden kişilerin mağduriyetine veya kamunun zararına neden olunması veya kamu görevlisinin haksız bir menfaat temin etmesinin gerekmesi, oysa kişisel verilerin kaydedilmesi suçunun bir tehlike suçu olması nedeni ile kabulü mümkün görünmemektedir.

Kamu görevlisi kavramı TCK'nın 6/1-c maddesinde “*kamusal faaliyetin yürütülmesine atama veya seçilme yoluyla ya da herhangi bir surette sürekli, süreli veya geçici olarak katılan kişi*” biçiminde tanımlanmıştır. Maddenin gerekçesi incelendiğinde ise, bir kimsenin kamu görevlisi olduğunun kabulünde temel kıstasın görevinin kamusal faaliyet olduğunun belirtildiği görülür⁴⁹⁹. Ancak karşılığı idare hukukunda dahi bulunmayan kamusal

⁴⁹⁸ Özbek vd., 2016: 571; Yaşar vd., 2014: 4458.

⁴⁹⁹ Madde gerekçesi; “765 sayılı Türk Ceza kanunundaki memur tanımının doğrultusunda sakıncaları aynen devam ettirecek nitelikte olan tanım, Tasarı metninden çıkarılarak; memur kavramını da kapsayan “kamu görevlisi” tanımına yer verilmiştir. Yapılan yeni tanıma göre kişinin kamu görevlisi sayılması için aranacak yegane ölçüt gördüğü işin kamusal faaliyet olmasıdır. Bilindiği üzere kamusal faaliyet, Anayasa ve kanunlarda belirlenmiş olan usullere göre verilmiş olan bir siyasal kararla, bir hizmetin kamu adına yürütülmesidir. Bu faaliyetin yürütülmesine katılan kişilerin maaş, ücret veya sair bir maddi karşılık alıp almamalarının, bu işi sürekli, süreli veya geçici olarak yapmalarının bir önemi bulunmamaktadır. Bu bakımdan örneğin mesleklerinin icrası

faaliyet kavramından ne anlaşılması gerektiği hususuna kanunda yer verilmemiş olması, kamu görevlisi kavramını ceza hukuku bağlamında tartışmaya açmıştır⁵⁰⁰. Bu bağlamda, kamusal faaliyetin devlet ve diğer kamu tüzel kişilerinin asli faaliyetleri kapsamında, bizzat kendisinin yürüttüğü veya denetimi altında yürütülen faaliyet olarak tanımlanması gerektiği ifade edilmektedir⁵⁰¹. Dolayısı ile sözleşmeli personel, kamu iktisadi teşebbüsü personeli⁵⁰², kooperatif yönetim kurulu üyeleri ve memurları⁵⁰³ ile kamu kurumu niteliğindeki meslek örgütlerinin üyeleri de TCK anlamında kamu görevlisi olarak kabul edilmektedir⁵⁰⁴. Kamusal faaliyet kavramının anlamı itibariyle kamu görevlisi kavramının kapsamını ceza hukukunun belirlilik ve son çare olma gibi ilkelerini zedeler biçimde genişleteceğinden bahisle, kamu görevi ve kamu hizmeti yürütenleri ifade ettiği, kamuya yararlı bir faaliyetin yürütülmesine katılanları ise kapsam dışında bıraktığı şeklinde yorumlanması gerektiği savunulmaktadır⁵⁰⁵. Kişinin kamu görevlisi olarak kabul edilmesinde görevin kamusal faaliyete ilişkin olmasının yanında kişinin bu kamusal faaliyete katılma biçimi, faaliyetin niteliği ve son olarak kişinin yönetim ile özel hukuk ilişkisi içerisinde bulunmaması kriterleri önem taşımaktadır⁵⁰⁶. Hal

bağlamında avukat veya noterin kamu görevlisi olduğu hususunda bir tereddüt bulunmamaktadır. Keza kişi, bilirkişilik, tercümanlık ve tanıklık faaliyetinin icrası kapsamında bir kamu görevlisidir. Askerlik görevi yapan kişiler de kamu görevlisidirler. Bu bakımdan örneğin bir suç vakasına müdahil olan bir tutuklu veya hükümlünün naklini gerçekleştiren jandarma subay veya erleri de kamu görevlisidirler. Buna karşılık, kamusal bir faaliyetin yürütülmesinin ihaleye dayalı olarak özel hukuk kişilerince üstlenilmesi durumunda bu kişilerin kamu görevlisi sayılmayacağı açıktır.”

⁵⁰⁰ Kaplan, 2015: 64; Özen ve Tozman, 2009: 43.

⁵⁰¹ Kaplan, 2015: 68; Özen ve Tozman, 2009: 45.

⁵⁰² 399 sayılı KHK

Teşebbüs Personelinin Yükümlülük ve Sorumlulukları

Madde 11/ d) (Değişik: 2/12/1999 - 4483/17 md.) Teşebbüs genel müdürü ve yönetim kurulu üyelerinin görevlerini icra sırasında işledikleri suçlardan dolayı yargılanmaları, ilgili bakanın iznine bağlı olup; bu konuda Memurlar ve Diğer Kamu Görevlilerinin Yargılanması Hakkında Kanun hükümleri uygulanır.

⁵⁰³ 1163 sayılı Kooperatifler Kanunu

Üyelerin titizlik derecesi ve sorumlulukları:

Madde 62/ cümle 3 –Yönetim Kurulu üyeleri ve kooperatif memurları, kendi kusurlarından ileri gelen zararlardan sorumludurlar. Bunların suç teşkil eden fiil ve hareketlerinden ve özellikle kooperatifin para ve malları bilanço, tutanak, rapor ve başka evrak, defter ve belgeleri üzerinde işledikleri suçlardan dolayı kamu görevlisi gibi cezalandırılır.

⁵⁰⁴ Kaplan, 2015: 70-73. Kamu kurumu niteliğindeki meslek örgütlerinin üyelerinin kamu görevlisi olarak kabul edilmeleri gerektiği yönünde ayrıca bk. Gökcan, 2015: 154.

⁵⁰⁵ Özen ve Tozman, 2009: 45; Demren Dönmez, 2011: 120.

⁵⁰⁶ Demren Dönmez, 2011: 114-115.

böyle iken, bilirkişilik, tanıklık, tercümanlık, noterlik veya avukatlık görevi üstlenen kişiler de bu faaliyetleri kapsamında TCK bakımından kamu görevlisidirler. Bunun yanında her ne kadar TCK'nın 6/1-d maddesinde ayrı bir başlık altında tanımlanmış olsalar da yargı görevi ifa eden yüksek mahkemeler ve adli, idarî ve askerî mahkemeler üye ve hakimleri ile Cumhuriyet savcılarının da yargı görevinin kamusal faaliyet olması nedeni ile kamu görevlisi kabul edilecekleri konusunda kuşku bulunmamaktadır⁵⁰⁷.

Failin kamu görevlisi olmasının yanında, kişisel verilerin hukuka aykırı olarak kaydedilmesinin görevinin verdiği yetkinin kötüye kullanılması ile gerçekleşmesi gerekmektedir. Bu durumda, fail tarafından kötüye kullanılan yetkinin failin görevi ile ilişkili olması gerekmekte olup görevin kapsamı mevzuata ve genel uygulamaya göre belirlenecektir⁵⁰⁸. Örneğin, görevi gereği kişisel verilere erişim yetkisi bulunan vergi dairesi görevlilerinin görevlerine aykırı olarak kişilerin malvarlıkları, vergi borçları gibi hususları kayıt altına almaları durumunda cezai sorumlulukları gündeme gelecektir. Devamla, şüpheli veya sanığın iç beden muayenesi, vücudundan alınan kan ve benzeri biyolojik örnekler ile saç, tükürük, tırnak gibi örnekler üzerinde yapılan inceleme sonuçları kişisel veri niteliğinde olup CMK'nın 75/5. maddesi uyarınca üst sınırı iki yıldan daha az hapis cezasını gerektiren suçlar bakımından bu tür bir inceleme yapılması kanunen mümkün olmadığından, üst sınırı iki yıldan daha az hapis cezasını öngören bir suç nedeni ile yapılan soruşturmada şüpheliden alınan örnekler veya muayene neticesinde elde edilen sonuçlar bakımından TCK'nın 137/1. maddesindeki nitelikli hal söz konusu olacaktır.

2.2.1.5.3. Suçun Belli Bir Meslek ve Sanatın Sağladığı Kolaylıktan Yararlanmak Suretiyle İşlenmesi

TCK madde 137/1-b'ye göre kişisel verilerin hukuka aykırı olarak kaydedilmesi suçunun belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenmesi halinde verilecek cezanın yarı oranında arttırılmaktadır.

Meslek, *“belli bir eğitim ile kazanılan sistemli bilgi ve becerilere dayalı, insanlara yararlı mal üretmek, hizmet vermek ve karşılığında para kazanmak için yapılan, kuralları belirlenmiş iş”* biçiminde tanımlanmaktadır⁵⁰⁹. Sanat ise farklı anlamlar barındırmakta olup incelenen madde bağlamında “zanaat” anlamı ile kullanıldığı düşünülmektedir⁵¹⁰. Zanaat,

⁵⁰⁷ Demren Dönmez, 2011: 114.

⁵⁰⁸ Özbek vd., 2016: 571; Yaşar vd., 2014: 4458.

⁵⁰⁹ http://www.tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.5a5a24cbdc431.804884 33 (erişim tarihi:13.01.2018)

⁵¹⁰ Özbek vd., 2016: 572.

“insanların maddeye dayanan gereksinimlerini karşılamak için yapılan, öğrenimle birlikte deneyim, beceri ve ustalık gerektiren iş” anlamına gelir⁵¹¹.

Bu düzenleme bakımından önemli olan husus, meslek ve sanatının failin suçu işleminde kolaylık yaratması ve suçun işlendiği anda failin o meslek ve sanatını icra ediyor olmasıdır⁵¹². Meslek ve sanatın sağladığı kolaylık ise failin, mağdurun kişisel verilerine ulaşmasına fayda sağlaması, elverişli olması veya aracılık etmesidir⁵¹³. Örneğin, banka memurlarının müşterilerine, sağlık çalışanlarının hastalara ait kişisel verileri hukuka aykırı olarak kaydetmeleri halinde bu verilere erişmelerinde meslek ve sanatlarının sağladığı kolaylıktan yararlandıkları söylenebilir⁵¹⁴.

2.2.2. Manevi Unsur

Gerçekleştirilen eylem ile fail arasındaki manevi bağ, suçun manevi unsuru olarak adlandırılır. Bir suçun kanundaki düzenlemesinde aranan manevi unsur -kast veya taksir- somut durumda mevcut olmadığı takdirde suç oluşturan bir haksızlıktan söz edilemeyecektir⁵¹⁵.

Kişisel verilerin kaydedilmesi suçu ancak kastla işlenebilir⁵¹⁶. Kast, suçun kanuni tanımındaki unsurların bilinmesi ve istenmesidir. Kaydedilen bilginin, kişisel veri olduğunun bilinmesi ve bu kişisel verinin kaydedilmesinin istenmesi durumunda suçun manevi unsuru tamamlanmış olur⁵¹⁷. Fakat suçun olası kasta işlenip işlenemeyeceği konusunda öğretide farklı görüşler bulunmaktadır. TCK'nın 21. maddesinin 2. fıkrasına göre, *“kişinin, suçun kanuni tanımındaki unsurların gerçekleşebileceğini öngörmesine rağmen, fiili işlemesi halinde”* varlığı kabul edilen olası kast; *“kişinin bir davranışına bağlı olarak ortaya çıkabilecek, ihtimal dahilindeki neticenin meydana gelme tehlikesini, davranışını gerçekleştirirken kabullenmesidir”⁵¹⁸*. Manevi unsur bakımından kastın arandığı suçların kural olarak olası kasta işlenmesi de mümkündür⁵¹⁹. Öte yandan, madde metninde kaydetme

⁵¹¹http://www.tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.5a5a29bb765825.342286 38 (erişim tarihi:13.01.2018)

⁵¹² Soyaslan, 2016: 357.

⁵¹³ Soyaslan, 2016: 357; Özbek vd., 2016:572.

⁵¹⁴Özbek vd., 2016: 573.

⁵¹⁵ Özgenç, 2016: 221.

⁵¹⁶ Özbek vd., 2016:576.

⁵¹⁷ Akdağ, 2013: 105.

⁵¹⁸ Karakehya, 2006: 29.

⁵¹⁹ Özbek vd., 2016: 576; Karakehya, 2006: 26.

eyleminin hukuka aykırı olarak gerçekleştirilmesinin aranmasının manevi unsur bakımından failin doğrudan kast ile hareket etmesi gerektiği şeklinde yorumlanmasının doğal bir sonucu olarak suçun olası kastla işlenemeyeceği savunulmaktadır⁵²⁰.

Bir suçun taksirle işlenebileceğinin kabulü, istisnai bir hal olup kanunda özel olarak düzenlenmiş olmasına bağlıdır. Kişisel verilerin kaydedilmesi suçunun kanunda taksirli biçimi düzenlenmemiş olduğundan bu suç bakımından taksirli sorumluluk söz konusu olmaz.

2.3. Hukuka Aykırılık

Fail tarafından gerçekleştirilen fiilin hukuk düzenince sakıncalı kabul edilmesi, başka bir deyişle kanunkoyucu tarafından öngörülen emir ve yasağa aykırı davranılması o fiilin hukuka aykırılığına işaret eder⁵²¹. Hukuka aykırılık, haksızlık olarak ortaya çıkan eylemin bir vasfıdır⁵²². Hukuka aykırılık vasfını tipikliğin maddi bir unsuru olarak değil, suçun genel bir unsuru olarak kabul etmek gerekir⁵²³. Haksızlık teşkil eden ve kanunda suç olarak tanımlanmış bu eylemin cezai müeyyideye tabi tutulabilmesi için hukuka aykırılık vasfını ortadan kaldıran bir sebep somut olayda bulunmamalıdır⁵²⁴.

Bazı suç tanımlarında -tıpkı kişisel verilerin kaydedilmesi suçunda olduğu gibi- "hukuka aykırı olarak", "hukuka aykırı yollarla", "hukuka aykırı başka bir davranışla" gibi ifadelere yer verilmiş olup suç olarak tanımlanan eylemin hukuka aykırılığına vurgu yapıldığı görülmektedir. Bu durum öğretide *hukuka özel aykırılık* olarak ifade edilmektedir⁵²⁵. Bu ifadelerin ne anlama geldiği doktrinde tartışma konusu olmuştur.

Bir kısım yazarlara göre bu durum, failin işlediği fiilin hukuka aykırı olduğunun bilincinde olmasını, başka bir deyişle doğrudan kastla hareket etmiş olmasına işaret etmektedir⁵²⁶. Buna göre bu suç tiplerinde hukuka aykırılık, tipikliğin bir unsuru olma özelliğini kazanır⁵²⁷. Failin kastının özel olarak belirtilen hukuka aykırılık durumunu da kapsaması, "hukuka aykırılığı bildiğinin ayrıca ispat edilmesi" gerekir⁵²⁸. Hal böyle iken,

⁵²⁰ Aydın, 2015: 140.

⁵²¹ Özgenç, 2016: 287; Özbek vd., 2017: 258; Artuk vd., 2013: 368.

⁵²² Özgenç, 2016: 287.

⁵²³ Artuk vd., 2013: 372.

⁵²⁴ Özgenç, 2016: 292.

⁵²⁵ Katoğlu, 2003: 122; Özbek vd., 2017: 262; Akdağ, 2013: 106.

⁵²⁶ Özgenç, 2016: 294; Artuk vd., 2013: 372; İçel vd. 2000: 110; Karagülmez, 2005: 231; İtişgen, 2015: 191.

⁵²⁷ Artuk vd., 2013: 373.

⁵²⁸ İçel vd., 2000: 111; Akbulut, 2014: 286.

kişisel verileri kaydetme suçunun ancak doğrudan kastla işlenebileceği sonucuna varılmaktadır.

Diğer bir görüşe göre ise, bu durumda bir eylemin tipe uygun olması halinde o fiilin doğrudan hukuka da aykırı olduğu söylenemeyecektir. O halde hakimın söz konusu eylemin hukuka aykırı olduğunu tespit etme zorunluluğu bulunmaktadır⁵²⁹. Esasen hukuka aykırılık unsuruna ceza normunda özel olarak yer verilmesinin sebebi suç tipindeki eylemin hukuka uygun da olabileceğini belirtmek içindir⁵³⁰. Dolayısı ile kişisel verileri kaydetme suçunu düzenleyen TCK madde 135'te "hukuka aykırı olarak" ifadesine yer verilmiş olmasının anlamı, kişisel verilerin kaydedilebilme koşullarının bir hukuk kuralı ile belirlenmiş olması karşısında kaydetme fiili bu mevzuata uygun olduğu sürece bu fiilin cezalandırılmasının mümkün olmadığıdır^{531, 532}.

Bir kısım yazarlara göre ise, kanun maddesinde "hukuka aykırı olarak" ifadesine yer verilmiş olmasının, hukuka özel aykırılığa işaret ettiği iddiasının kabulü mümkün değildir; zira hukuka aykırılık failin eylemi ile hukuk normu arasındaki çatışma anlamına gelmekte olup niteliği itibari ile özel-genel hukuka uygunluk nedeni gibi bir sınıflandırmaya tabi tutulamaz⁵³³.

Kanaatimizce, kanunkoyucunun ceza normunda hukuka aykırılığa ayrıca vurgu yapması sebepsiz değildir. Bu durum eylemin tipe uygun olmasının hukuka aykırılığın karinesini oluşturduğu kuralına istisna getirmekte ve hakime tipe uygun eylemin hukuka

⁵²⁹ Önder, 1992: 139.

⁵³⁰ Özbek vd., 2016: 538.

⁵³¹ Özbek vd., 2016: 574; Akdağ, 2013: 111.

⁵³² Kişisel Verilerin Korunması Kanunu Tasarısı'na ilişkin olarak Adalet Komisyonu'nda gerçekleştirilen 26. Dönem 1. Yasama yılının 27.01.2016 tarihli görüşmesinde Adalet Bakanı tarafından "*Türk Ceza Kanunu'nun 135 ve devamı maddelerinde kişisel verilerin hukuka aykırı olarak işlenmesi suç olarak düzenlenmekte, ancak hukuka aykırılığa sebep olabilecek unsurlar kanunda belirtilmediğinden ve bu konuda özel bir kanun da olmadığından, diğer bir ifadeyle, hukuka uygunluk hâli düzenlenmediğinden uygulamada çok ciddi sorunlar yaşanmaktadır.*" sözleri ile Kişisel Verilerin Korunması Kanunu'nun gerekliliğine ve bu kanunun TCK'nun 135. maddesinde suç olarak düzenlenen kişisel verilerin kaydedilmesi eyleminin hangi hallerde hukuka uygun olacağının belirlenmesine hizmet edeceğine işaret edilmiştir (https://www.tbmm.gov.tr/develop/owa/komisyon_tutanaklari.mv_goruntule?pTutanakId=6269 , erişim tarihi:23.12.2017).

⁵³³ Delitala, 1930: 39'dan aktaran Katoğlu:2003: 124; Hafizoğulları ve Özen, 2010: 220.

aykırı olup olmadığını özel olarak araştırma görevi yüklemektedir. Nitekim maddenin gerekçesi de bu görüşü destekler niteliktedir⁵³⁴.

Maddenin ikinci fıkrasında, kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine ait verilerin kaydedilmesi durumunda "hukuka aykırı olarak" ifadesine yer verilmediği; fıkranın ikinci bölümünde ise diğer durumlar için hukuka aykırı olma durumuna tekrar vurgu yapıldığı dikkat çekmektedir. Bu durumdan, fıkranın ilk bölümündeki bilgilerin kişisel veri olarak kaydedilmesi halinin her zaman mutlak olarak hukuka aykırı olduğu sonucuna varılmaktadır⁵³⁵. Dolayısıyla kişilerin siyasi, felsefi ve dini görüşleri ile ırki kökenlerine ait verilerin *mutlak dokunulmaz* olduğu ve bu verilerin kaydedilebileceğini öngören bir hukuk kuralının düzenlenemeyeceği ifade edilmektedir⁵³⁶. Ancak kanunun anılan fıkranın ilk bölümündeki verileri diğerlerinden niçin ayırık tuttuğu anlaşılamamakta, gerekçede ve hazırlık çalışmalarında da bu konuya ilişkin bir açıklama bulunmamaktadır. Bir kısım yazarlarca, kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine ait verilerin kaydedilmesinin her halde hukuka aykırı kabul edilip cezaya hükmolunması gerektiği biçimindeki bir yorumun; kaydedilen verinin kişinin mesleğine, dini görüşüne veya ahlaki eğilimine ilişkin olması arasında bir fark bulunmadığı ve maddenin esasen kişisel veri kabul edilen bütün bilgilerin hukuka aykırı olarak kaydedilmesinin suç olduğu düzenlemesine yer verdiği ve hukuka aykırılığın suçun konusu olan her tür veriye ilişkin olduğu gerekçeleriyle kabulünün mümkün olmadığı düşünülmektedir⁵³⁷.

Kişisel verileri kaydetme suçu yönünden kanunda sınırlı sayıda düzenlenmiş bulunan hukuka uygunluk nedenlerinin söz konusu olup olamayacağını tespit edebilmek için her bir hukuka uygunluk sebebini ayrı ayrı incelemekte fayda vardır:

**Hakkın kullanılması* biçimindeki hukuka uygunluk nedeni, 5237 sayılı TCK'nun 26/1 maddesinde *"Hakkını kullanan kişiye ceza verilmez."* sözleri ile ifade edilmiştir. Bir kişiye hukuk düzeni tarafından bir hak bahşedildiğinde bu hakkın kullanılması, başkalarının

⁵³⁴ "Bu suçun oluşabilmesi için, kişisel verilerin hukuka aykırı bir şekilde kayda alınması gerekir. Kişinin rızası ile kendisiyle ilgili bilgilerin kayda alınmasının suç oluşturmayaacağı muhakkaktır. Belirli nitelikteki kişisel verilerin kayda alınması kanun hükmünün gereği olarak yapılmaktadır. Bu bakımdan, çeşitli kamu kurumlarında verilen kamu hizmetinin gereği olarak kişilerle ilgili bazı bilgiler ilgili kanun hükümlerine istinaden kayda alınmaktadır. Bu durumlarda, söz konusu suç oluşmayacaktır. " (TCK madde 135 gerekçesi, parç. 4).

⁵³⁵ Hafizoğulları ve Özen, 2009: 20; Ketizmen, 2008: 235; Taşkın, 2008: 103. Madde gerekçesi de bu kanaati destekler niteliktedir.

⁵³⁶ Özbek vd., 2016: 567.

⁵³⁷ Yaşar vd., 2014: 4437.

menfaati ile çatışsa bile hakkını kullanan kişinin fiiline üstünlük tanınır ve hukuka uygun kabul edilir⁵³⁸.

Hakkın kullanılmasının hukuka uygunluk sebebi olarak kabul edilmesi için, Türk doktrin ve uygulamasında dört şartın varlığı aranmaktadır⁵³⁹;

-Hukuk düzeni tarafından kabul edilmiş bulunan bir hakkın varlığı,

-Bu hakkın yine hukuk düzeni tarafından belirlenen sınırlar içerisinde kullanılması, başka bir anlatımla hakkın suiistimal edilmemesi⁵⁴⁰,

-Bu hakkı kullanan kimsenin hakkını doğrudan doğruya, herhangi bir merciin aracılığına ya da muvafakatine bağlı olmaksızın kullanabilmesi⁵⁴¹,

-Hakkın kullanılması ile işlenen suç arasında nedensellik bağının bulunması⁵⁴².

Mevzuatımızda hakkın kullanılması niteliğindeki hukuka uygunluk sebebi bir hayli çoktur⁵⁴³. Kişisel verilerin kaydedilmesi eyleminin hakkın kullanılması biçimindeki hukuka uygunluk sebebine dayalı olarak gerçekleştirilmesine işverenin yönetim hakkı kapsamında işçilerin çeşitli metotlarla izlenmesi ve denetlenmesi örnek gösterilmektedir⁵⁴⁴. Bunların yanında, basın özgürlüğü kapsamında haber verme hakkının kullanılması kişisel verilerin kaydedilmesinin hukuki zeminini oluşturabilir. Anayasal şikayet hakkının kullanılması bağlamında isnadın dayanağını oluşturan somut vakalarla ilişkili olarak kişisel verilerin kaydedilmesinin de hukuka uygun olduğu ifade edilmektedir⁵⁴⁵.

4857 sayılı İş Kanunu'nun 8. maddesinde iş sözleşmesinin, *"bir tarafın (işçi) bağımlı olarak iş görmeyi, diğer tarafın (işveren) da ücret ödemeyi üstlenmesinden oluşan sözleşme"* olarak tanımlanmış olması nedeni ile işverenin yönetim hakkı bu tanımda yer alan "bağımlılık" unsurunun doğal bir sonucu olarak karşımıza çıkmaktadır⁵⁴⁶. İşverenin yönetim hakkı, emir ve talimat verebilme ile işyerinin düzenini sağlamak adına gözetim, kontrol,

⁵³⁸ Artuk vd.,2013: 396.

⁵³⁹ İçel vd., 2000: 167-168; Artuk vd., 2013: 297

⁵⁴⁰ Özbek vd., 2017: 296.

⁵⁴¹ " Bir hakkı kullanan kimsenin hukuka aykırı bir şekilde hareket etmiş sayılamayacağı, bilinen bir gerçektir. Bir hak, kanun, tüzük, yönetmelik, genelge gibi nizamlara dayanabilir ve hukuken tanınmış ve düzenlenmiş olmak kaydıyla, bir mesleğin icrasın-dan da doğabilir. Burada hakkın doğrudan doğruya kullanılabilir olması aranacaktır. Eğer hak, bir mercie başvurarak kullanılabilirse, artık buradaki hak kap-samında kabul olunmayacaktır." (Madde gerekçesi).

⁵⁴² Özbek vd.; 2017: 296.

⁵⁴³ Artuk vd.; 2013: 396.

⁵⁴⁴ Aydın, 2015: 157.

⁵⁴⁵ Özen, 2009: 17.

⁵⁴⁶ Balkır, 2005: 198.

denetimde bulunma ve işçilerin işyerinde gerçekleştirecekleri davranışlar bakımından kurallar koyabilme yetkisini bünyesinde barındırır⁵⁴⁷. Teknolojinin gelişmesi ve internetin birçok alanda iş ilişkilerinin vazgeçilmez bir parçası haline gelmesi ile birlikte işçilerin bu olanakları kendilerine boş vakit yaratmaya yönelik veya işveren açısından bilgi güvenliğini tehlikeye düşürebilecek, hukuki ve cezai sorumluluğa yol açabilecek şekillerde kullanımı birtakım yeni problemler de ortaya çıkarmıştır. Bu nedenle, işverenin yönetim hakkına dayanarak işletmesini ve kendisini korumak maksadı ile işçinin iş görme borcunu ve faaliyetlerini denetleme aracı olarak işçinin elektronik postaları, telefon görüşmeleri, internet kullanımı ve işyerindeki davranışlarının gözlenmesi sık karşılaşılabir bir durum haline gelmiştir⁵⁴⁸.

İşverenin dayanağını iş sözleşmesinin bağımlılık unsurundan alan yönetim ve denetim hakkının kabulü, bu hakka dayanılarak işçilerin özel hayatlarının gizliliği ile kişisel verilerinin korunması hakkının bir kenara bırakılacağı anlamına gelmemektedir. Bu nedenle işçilerin yönetim hakkına bağlı olarak kişisel verilerinin kaydedilmesi birtakım şartlarla sınırlandırılmış bulunmaktadır. Buna göre işçiler, izlenmeye başlamadan önce bunun nedenleri, zamanı, vasıtaları ve kapsamından haberdar edilmeli, bunun yanında işçilerin özel hayatlarının gizliliği ile kişisel verilerinin korunması hakkına mümkün olan en az derecede müdahale edecek metotlara başvurulmalı ve işverenin menfaatleri ile işçinin hakları arasında denge kurulmalıdır⁵⁴⁹.

Temelini Avrupa İnsan Hakları Sözleşmesinin 10. maddesi ile Anayasa'nın 28. vd. maddelerinden alan ve 5187 sayılı Basın Kanununun 3. maddesinde düzenlenen basın özgürlüğü ve bu kapsamda bilgi edinme, yayma, eleştirme, yorumlama ve eser ortaya koyma hakkının hukuka uygunluk nedeni olarak kabul edilebilmesi için; haberin gerçek ve güncel olması, haberin kamuyu ilgilendirmesi yani kamuoyunun haberi öğrenmekte menfaatinin bulunması ve haber ile haberin veriliş şeklinin uyumlu olması gereklidir⁵⁵⁰. Burada dikkat edilmesi gereken husus, basın özgürlüğü ve haber verme hakkının kötüye kullanılarak kişilik haklarına saldırıda bulunulmaması ve kişisel verilerin korunması hakkının ihlal edilmemesidir⁵⁵¹.

**Görevin ya da kanun hükmünün yerine getirilmesi biçimindeki hukuka uygunluk nedeni, TCK'nın 24. maddesinin birinci fıkrasında düzenlenmiş bulunmakla, kanunun belirli bir davranışta bulunmak hususunda belirli durumdaki kişilere yetki vermiş olması durumunda*

⁵⁴⁷ Balkır, 2005: 198-199.

⁵⁴⁸ Savaş, 2009: 98.

⁵⁴⁹ Savaş, 2009: 101; Aydın, 2015: 158.

⁵⁵⁰ Yargıtay CGK, 2012/12-1510 Esas, 2014/331 Karar, 17.06.2014; Özbek vd., 2017: 309-310.

⁵⁵¹ Aydın, 2015: 159.

söz konusu olur⁵⁵². Kanun hükmünün yerine getirilmesini hakkın icrasından ayıran husus, kanun hükmünün yerine getirilmesinin bir yetki ya da görev niteliğinde olmasıdır⁵⁵³.

Kişisel verilerin kaydedilmesi suçu bakımından kanun hükmünün yerine getirilmesi bir hukuka uygunluk nedeni olarak kabul edilmektedir⁵⁵⁴. Anayasa'nın 20. maddesi ile kişisel verilerin ancak kanunda öngörülen hallerde ve ilgisinin rızasının bulunması halinde işlenebileceği düzenlenmiştir. Madde gerekçesinde de; *"Belirli nitelikteki kişisel verilerin kayda alınması kanun hükmünün gereği olarak yapılmaktadır. Bu bakımdan, çeşitli kamu kurumlarında verilen kamu hizmetinin gereği olarak kişilerle ilgili bazı bilgiler ilgili kanun hükümlerine istinaden kayda alınmaktadırlar. Bu durumlarda, söz konusu suç oluşmayacaktır. "* ifadesine yer verilmek sureti ile bu hukuka uygunluk nedenine vurgu yapıldığı görülmektedir. Fakat önemli olan, kişisel verilerin işlenmesinin kural olarak yasaklanması ve kişisel verilerin işlenmesinin zorunlu olduğu durumları ise istisnai bir şekilde ve titizlikle düzenlenmeli, işleme nedeni ile kişilerin temel hak ve özgürlüklerinin sınırlandırılmasının mümkün olduğunca asgari düzeyde tutulmasına özen gösterilmelidir⁵⁵⁵.

Mevzuatımızda kişisel verilerin kaydedilmesini öngören pek çok düzenleme bulunmaktadır:

-5271 Sayılı Ceza Muhakemesi Kanunu'nda yer alan düzenlemeler:

Kanun'un 80. maddesi ile bir suça ilişkin delil elde etmek için şüpheli, sanık veya mağdur üzerinde iç beden muayenesi yapılması ya da vücuttan kan veya benzeri biyolojik örneklerle saç, tükürük, tırnak gibi örnekler üzerinde yapılan genetik incelemeler ya da soybağının veya elde edilen bulgunun şüpheli veya sanığa ya da mağdura ait olup olmadığının tespiti için yapılan incelemeler sonucunda elde edilen bilgilerin kişisel veri niteliğinde ve gizli olduğu belirtilmiştir⁵⁵⁶.

⁵⁵² Artuk vd.; 2013: 377.

⁵⁵³ Özbek vd., 2017: 266.

⁵⁵⁴ Soyaslan, 2016: 351.

⁵⁵⁵ Akdağ, 2013: 120.

⁵⁵⁶ Madde 80 – (Değişik: 25/5/2005 – 5353/4 md.) (1) 75, 76 ve 78 inci madde hükümlerine göre alınan örnekler üzerinde yapılan inceleme sonuçları, kişisel veri niteliğinde olup, başka bir amaçla kullanılamaz; dosya içeriğini öğrenme yetkisine sahip bulunan kişiler tarafından bir başkasına verilemez.

(2) Bu bilgiler, kovuşturmayla yer olmadığı kararına itiraz süresinin dolması, itirazın reddi, beraat veya ceza verilmesine yer olmadığı kararı verilip kesinleşmesi hâllerinde Cumhuriyet savcısının huzurunda derhâl yok edilir ve bu husus dosyasında muhafaza edilmek üzere tutanağa geçirilir.

Yine, Kanun'un 135. maddesi uyarınca verilen iletişimin tespiti, dinlenmesi ve kayda alınmasına ilişkin kararlar sonucunda elde edilen veriler kişisel verilerdir⁵⁵⁷.

-2559 Sayılı Polis Vazife ve Selahiyet Kanunu'nda yer alan düzenlemeler:

Kanun'un 5. maddesi ile kişisel verilerden sayılan parmak izi ve fotoğrafların hangi koşullarda kayda alınabileceği düzenlenmiştir⁵⁵⁸.

⁵⁵⁷ Kararların yerine getirilmesi, iletişim içeriklerinin yok edilmesi

Madde 137 – (1) 135 inci maddeye göre verilecek karar gereğince Cumhuriyet savcısı veya görevlendireceği adli kolluk görevlisi, telekomünikasyon hizmeti veren kurum ve kuruluşların yetkililerinden iletişimin tespiti, dinlenmesi veya kayda alınması işlemlerinin yapılmasını ve bu amaçla cihazların yerleştirilmesini yazılı olarak istediğinde, bu istem derhâl yerine getirilir; yerine getirilmemesi hâlinde zor kullanılabilir. İşlemin başladığı ve bitirildiği tarih ve saat ile işlemi yapanın kimliği bir tutanakla saptanır.

(2) 135 inci maddeye göre verilen karar gereğince tutulan kayıtlar, Cumhuriyet Savcılığınca görevlendirilen kişiler tarafından çözümlenerek metin hâline getirilir. Yabancı dildeki kayıtlar, tercüman aracılığı ile Türkçe'ye çevrilir.

(3) 135 inci maddeye göre verilen kararın uygulanması sırasında şüpheli hakkında kovuşturmaya yer olmadığına dair karar verilmesi ya da aynı maddenin birinci fıkrasına göre hâkim onayının alınamaması halinde, bunun uygulanmasına Cumhuriyet savcısı tarafından derhâl son verilir. Bu durumda, yapılan tespit veya dinlemeye ilişkin kayıtlar Cumhuriyet savcısının denetimi altında en geç on gün içinde yok edilerek, durum bir tutanakla tespit edilir.

(4) Tespit ve dinlemeye ilişkin kayıtların yok edilmesi halinde soruşturma evresinin bitiminden itibaren, en geç onbeş gün içinde, Cumhuriyet Başsavcılığı, tedbirin nedeni, kapsamı, süresi ve sonucu hakkında ilgisine yazılı olarak bilgi verir.

⁵⁵⁸ Parmak izi ve fotoğrafların kayda alınması

Madde 5- (Değişik: 2/6/2007-5681/2 md.)

Polis;

a) Gönüllü,

b) Her çeşit silah ruhsatı, sürücü belgesi, pasaport veya pasaport yerine geçen belge almak için başvuruda bulunan,

c) Başta polis olmak üzere, genel veya özel kolluk görevlisi ya da özel güvenlik görevlisi olarak istihdam edilen,

ç) Türk vatandaşlığına başvuruda bulunan,

d) Sığınma talebinde bulunan veya gerekli görülmesi halinde, ülkeye giriş yapan sair yabancı,

e) Gözaltına alınan, kişilerin parmak izini alır. Birinci fıkraya göre alınan parmak izi, ait olduğu kişinin kimlik bilgileri ile birlikte, ne zaman ve kim tarafından alındığı belirtilmek suretiyle, bu amaca özgü sisteme kaydedilerek saklanır. Ancak, parmak izinin hangi sebeple alındığı sisteme kaydedilmez.

Olay yerinden elde edilen ve kime ait olduğu henüz tespit edilemeyen parmak izleri, kime ait olduğu tespit edilmeye kadar, ilgili soruşturma dosya numarası ile birlikte sisteme kaydedilir.

5271 sayılı Ceza Muhakemesi Kanununun 81 inci maddesi ile 5275 sayılı Ceza ve Güvenlik Tedbirlerinin İnfazı Hakkında Kanunun 21 inci maddesi hükümlerine göre alınan parmak izleri de bu sisteme kaydedilir.

Anılan kanunda kişisel verilerin kayıt altına alınmasına ilişkin bir başka düzenleme ise, sanal ortamda işlenen suçlar bakımından internet abonelerine ilişkin kimlik bilgilerine ulaşma konusunda kolluk kuvvetlerine verilen yetkidir⁵⁵⁹.

-5549 Sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun'da yer alan düzenleme:

İşbu Kanun'un 19. maddesi ile Maliye Bakanına bağlı olan Mali Suçları Araştırma Kurulu Başkanlığı'na suç gelirlerinin aklanması ve terörün finansmanının önlenmesi amacı ile veri toplamak ile kamu kurum ve kuruluşları, gerçek ve tüzel kişiler, tüzel kişiliği olmayan kuruluşlardan her türlü bilgi ve belgeyi istemek yetkisi verilmiştir⁵⁶⁰.

-213 Sayılı Vergi Usul Kanunu'nda yer alan düzenleme:

(a) bendi hariç birinci fıkra ile dördüncü fıkra kapsamına giren kişilerin ayrıca fotoğrafları alınarak, ikinci fıkra da belirlenen esaslara uygun olarak parmak izi ile birlikte sisteme kaydedilir.

Bu sistemde yer alan bilgiler, kimlik tespiti, suçun önlenmesi veya yürütülmekte olan soruşturma ve kovuşturma kapsamında maddî gerçeğin ortaya çıkarılması amacıyla mahkeme, hâkim, Cumhuriyet savcısı ve kolluk tarafından kullanılabilir.

Kolluk birimleri, kimlik tespiti yapmak ya da olay yerinden alınan parmak izini karşılaştırmak amacıyla doğrudan bu sistemle bağlantı kurabilir.

Sistemde kayıtlı bilgilerin hangi kamu görevlisi tarafından ve ne amaçla kullanıldığının denetlenebilmesine imkân tanıyan bir güvenlik sistemi kurulur.

Sistemde yer alan kayıtlar gizlidir; altıncı ve yedinci fıkralarda belirlenen amaçlar dışında kullanılamaz.

Sisteme kayıtlı olan parmak izi ve fotoğraflar, kişinin ölümünden itibaren on yıl ve her halde kayıt tarihinden itibaren seksen yıl geçtikten sonra sistemden silinir.

Parmak izi ile fotoğrafların sistemde kaydedilmesi ve saklanması ile bu kayıtlardan yararlanmaya ilişkin diğer esas ve usûller, İçişleri Bakanlığı tarafından Adalet Bakanlığının görüşü alınarak çıkarılacak yönetmelikle düzenlenir.

⁵⁵⁹ Adli görev ve yetkiler

Ek Madde 6 – (Ek: 16/6/1985 - 3233/7 md.; Değişik: 2/6/2007-5681/5 md.)

(Ek fıkra: 2/1/2017-KHK-680/27 md.) Polis, sanal ortamda işlenen suçlarda, yetkili Cumhuriyet başsavcılığının tespiti amacıyla, internet abonelerine ait kimlik bilgilerine ulaşmaya, sanal ortamda araştırma yapmaya yetkilidir. Erişim sağlayıcıları, yer sağlayıcıları ve içerik sağlayıcıları talep edilen bu bilgileri kolluğun bu suçlarla mücadele için oluşturduğu birimine bildirir.

⁵⁶⁰ Başkanlığın görev ve yetkileri

MADDE 19 – (1) Mali Suçları Araştırma Kurulu Başkanlığı doğrudan Maliye Bakanına bağlı olup görev ve yetkileri şunlardır:

...e) Suç gelirlerinin aklanması ve terörün finansmanının önlenmesi kapsamında veri toplamak, şüpheli işlem bildirimlerini almak, analiz etmek ve değerlendirmek.

...j) Kamu kurum ve kuruluşları, gerçek ve tüzel kişiler ile tüzel kişiliği olmayan kuruluşlardan her türlü bilgi ve belgeyi istemek

Kanunun 5. maddesi ile vergi mahremiyetine değinilmiş olup vergi muameleleri ve incelemeleri ile uğraşan memurlara, vergi mahkemeleri, bölge idare mahkemeleri ve Danıştay'da görevli olanlara, vergi kanunlarına göre kurulan komisyonlara iştirak edenler ile vergi işlerinde kullanılan bilirkişilere kişisel verilerden sayılan; mükellefin ve mükellefle ilgili kimselerin şahıslarına, işlem ve hesap durumlarına, işlerine, işletmelerine, servetlerine veya mesleklerine dair bilgilerin işlenmesi yetkisi tanınmış olup bu kişilerin sayılan verileri ifşa etmeme ve üçüncü kişiler yararına kullanmama yükümlülüğü bulunmaktadır⁵⁶¹.

-5352 Sayılı Adli Sicil Kanunu'nda yer alan düzenlemeler:

Kişiler hakkında verilmiş ve kesinleşmiş mahkûmiyet hükümleri kişisel verilerden olup Türk mahkemeleri tarafından vatandaş veya yabancı hakkında verilen bu hükümler adli sicile kaydedilmektedir. Sicile kaydedilen bu bilgiler kullanılış amacı belirtilmek sureti ile vekâletnamede açıkça belirtilmek koşuluyla vekili, kamu kurum ve kuruluşları, kamu kurumu niteliğindeki meslek kuruluşları tarafından temin edilerek kayıt altına alınabilir⁵⁶². Bu veriler, Cumhuriyet Başsavcılıklarından, kaymakamlıklardan ve yurt dışında elçilik ve konsolosluklardan temin edilebilir olduğundan bu makamların verileri işleminin de hukuka uygun olduğunda tartışma bulunmamaktadır⁵⁶³.

⁵⁶¹ Vergi mahremiyeti:

Madde 5 – Aşağıda yazılı kimseler görevleri dolayısıyla, mükellefin ve mükellefle ilgili kimselerin şahıslarına, muamele ve hesap durumlarına, işlerine, işletmelerine, servetlerine veya mesleklerine mütaallik olmak üzere öğrendikleri sırları veya gizli kalması lazım gelen diğer hususları ifşa edemezler ve kendilerinin veya üçüncü şahısların nefine kullanamazlar;

- 1. Vergi muameleleri ve incelemeleri ile uğraşan memurlar;*
- 2. (Değişik : 23/6/1982 - 2686/1 md.) Vergi mahkemeleri, bölge idare mahkemeleri ve Danıştayda görevli olanlar;*
- 3. Vergi kanunlarına göre kurulan komisyonlara iştirak edenler;*
- 4. Vergi işlerinde kullanılan bilirkişiler. Bu yasak, yukarıda yazılı kimseler, bu görevlerinden ayrılışları dahi devam eder.*

⁵⁶² Adli sicil bilgileri verilebilecek olanlar

Madde 7- (1) Adli sicil bilgileri, kullanılış amacı belirtilmek suretiyle;

- a) İlgili kişiye veya vekâletnamede açıkça belirtilmek koşuluyla vekiline,*
 - b) Kamu kurum ve kuruluşlarına, kamu kurumu niteliğindeki meslek kuruluşlarına,*
- Verilebilir.*

(2) Yabancı devletler tarafından istenilen adli sicil bilgileri mütekabiliyet esasına göre verilir.

⁵⁶³ Adli sicil bilgilerini verebilecek merciler

Madde 8- (1) Adli sicil bilgileri; mahalli adli sicillerde Cumhuriyet başsavcılıklarınca,

(...)(2) kaymakamlıklarca yurt dışında elçilik ve konsolosluklarca, merkezi adli sicilde ise Adalet Bakanlığı Adli Sicil ve İstatistik Genel Müdürlüğüne verilir.

-2000/284 Sayılı Güvenlik Soruşturması ve Arşiv Araştırması Yönetmeliği⁵⁶⁴,’nde yer alan düzenleme:

Yönetmeliğin 8. maddesi uyarınca güvenlik soruşturması ve arşiv araştırması; gizlilik dereceli birim ve kısımlar ile askeri, emniyet, istihbarat teşkilatlarında ve ceza infaz kurumları ve tutukevlerinde çalıştırılacak personel hakkında yapılmakta iken⁵⁶⁵, 657 sayılı Devlet Memurları Kanunu’nun 48. maddesine 03.10.2016 tarihli ve 676 sayılı Kanun Hükmünde Kararname’nin 74. maddesi ile eklenen 8 fıkra hükmü uyarınca devlet memurluğuna alınacak kişiler için de yapılmasının yasal dayanağı oluşturulmuştur. Milli İstihbarat Teşkilatı Müsteşarlığı, Emniyet Genel Müdürlüğü ve mahalli mülki idare amirlikleri tarafından yapılan güvenlik soruşturması ve arşiv araştırmasında kimlik kontrolü, kimlik kayıtlarının doğruluk derecesi, uyrukluğ, geçmişte yabancı bir devletin uyrukluğuna girip girmediği, kolluk kuvvetleri tarafından halen aranıp aranmadığı, kolluk kuvvetlerinin ve istihbarat ünitelerinin arşivlerinde bilgiler bulunup bulunmadığı, adli sicil kaydının ve hakkında bir tahdidin olup olmadığı, yıkıcı faaliyetlerde bulunup bulunmadığı ve 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanuna ve Atatürk ilke ve inkılaplarına aykırı davranıp davranmadığı, şeref

⁵⁶⁴ Bakanlar Kurulu Karar Tarihi:14.2.2000; Dayandığı Kanunun Tarihi:26.10.1994, Dayandığı Kanunun Sayısı:4045.

⁵⁶⁵ *Hakkında güvenlik soruşturması ve arşiv araştırması yapılacak personel*

Madde 8 – Güvenlik soruşturması ve arşiv araştırması; gizlilik dereceli birim ve kısımlar ile askeri, emniyet, istihbarat teşkilatlarında ve ceza infaz kurumları ve tutukevlerinde çalıştırılacak personel hakkında yapılır. Emniyet Genel Müdürlüğü ve mahalli mülki idare amirlikleri, güvenlik soruşturması ve arşiv araştırmasını; bakanlıklar, kamu kurum ve kuruluşlarının gizlilik dereceli birim ve kısımları ile yurtdışı teşkilatında ve askeri, emniyet, istihbarat teşkilatlarında ve ceza infaz kurumu ve tutukevlerinde çalıştırılacak personel hakkında yapar. Milli İstihbarat Teşkilatı Müsteşarlığı; Emniyet Genel Müdürlüğü ve mahalli mülki idare amirliklerinin görev ve yetkileri saklı kalmak kaydıyla, güvenlik soruşturmasını Milli İstihbarat Teşkilatında çalışacak personel, Türk Silahlı Kuvvetlerinin kadro ve kuruluşlarında çalışacak subay adayları ve Türk Silahlı Kuvvetlerinin belirleyeceği diğer personel ile bakanlıklar ve kamu kurum ve kuruluşlarının gizlilik dereceli birim ve kısımlarının hiyerarşik olarak bağlı bulunduğu üst kademe yöneticilerinden müsteşar, genel müdür, vali, büyükelçi ve müstakil birim amirleri ile bunların yardımcıları ve ayrıca yurtdışı teşkilatında sürekli görevlendirilecek bütün personel hakkında, arşiv araştırmasını ise sadece gizlilik dereceli birim ve kısımlarda görev alacaklar ile bunların bu fıkra da sayılanlar dışında kalan yöneticileri ve ceza infaz kurumları ve tutukevlerinde çalışacak personel hakkında yapar.

(Ek fıkra: 28/9/2000-2000/1391 K.) Ayrıca, müşterek kararname ile atanacak personelden hakkında güvenlik soruşturması yapılmamış olanlar için Başbakanlıkça arşiv araştırması yaptırılır. Milli İstihbarat Teşkilatı Müsteşarlığı ile Emniyet Genel Müdürlüğü’nün birbirlerinin personeli hakkında yapacakları güvenlik soruşturması ve arşiv araştırmasının esas ve usulleri ile bu Yönetmeliğin uygulanmasında kullanılacak bilgi ve belgelerin karşılıklı değişimi Başbakanın onayıyla yürürlüğe konulacak esaslar ile düzenlenir.

ve haysiyetini ihlal edecek ve görevine yansıyacak şekilde kumara, uyuşturucuya, içkiye, paraya ve aşırı bir şekilde menfaatine düşkün olup olmadığı, ahlak ve adaba aykırı davranıp davranmadığı, yabancılarla, özellikle hasım ve hasım olması muhtemel Devlet mensupları ve temsilcileriyle ilgili derecesinin iç yüzü ve nedeni, sır saklama yeteneğinin olup olmadığı araştırılmaktadır.

Güvenlik soruşturması ile arşiv araştırması sonucunda kayıt altına alınan veriler, kişinin kimliğini belirleyebilme yeteneğine sahip olduğu müddetçe kişisel veri olarak kabul edileceğinden, bu verilerin anılan Yönetmelikte sayılan merciler dışında herhangi bir kişi veya kurum tarafından kaydedilmesi suç oluşturur.

-5490 Sayılı Nüfus Hizmetleri Kanunu'nda yer alan düzenlemeler:

Kişinin doğumundan ölümüne kadar kişisel ve medenî durumuna, uyrukluğuna ve bunlarda meydana gelebilecek değişikliklere ait doğal ve hukukî olayların belirlenip saptanması ile elektronik ortamda ulusal adres veri tabanının oluşturulması amacı ile İçişleri Bakanlığı'nın merkez ve taşra teşkilatı ile dış temsilcilikler tarafından aile kütükleri oluşturulmaktadır. Aile kütükleri kişilerin Türkiye Cumhuriyeti kimlik numarası, kayıtlı bulunduğu il, ilçe, köy veya mahalle adı ile cilt, aile ve birey sıra numarası, adı ve soyadı, cinsiyeti, baba ve ana adı ile soyadları, evli kadınların önceki soyadları, doğum yeri ile gün, ay ve yıl olarak doğum tarihi ve kütüğe kayıt tarihi, evlenme, boşanma, soybağının kurulması veya reddi, ölüm, vatandaşlığın kazanılması veya kaybedilmesi gibi kişisel durumda meydana gelen değişiklik veya yetkili makamlarca yapılan düzeltmeler, dini, medenî hali, yerleşim yeri adresi⁵⁶⁶, fotoğrafı, biyometrik verisi, velayete ve vesayete ilişkin bilgileri ile bir kısmı özel veri kategorilerinden oluşan kişisel verilerini içermektedir.

Kişinin aile kütüğünde yer alan bilgilerinin dökümü nüfus kayıt örneği⁵⁶⁷ olarak adlandırılmaktadır. Bu bilgileri doğrudan almaya yetkili olan İçişleri Bakanlığı, dış temsilcilikler, asker alma işlemleri için Milli Savunma Bakanlığı, adlî makamlar, adlî işlemlerle sınırlı olmak üzere kolluk kuruluşları, evlenme işlemleri için evlendirme işlemini yapmaya yetkili olanlar, ölüm işlemleri için resmî sağlık kuruluşları, kaydın sahiplerinin eşleri

⁵⁶⁶ Yerleşim yeri adresi ve diğer adres bilgilerinin verilmesi kişinin rızasına bağlı olduğu düzenlenmiştir.

⁵⁶⁷ Nüfus kayıt örneği verilmesi

MADDE 43- (1) Kişinin aile kütüğündeki kaydının çıkarılması ve aslına uygunluğunun nüfus müdürlüğünce onanması ile elde edilen nüfus kayıt örnekleri, aksi ispat edilene kadar geçerlidir. Nüfus kayıt örneği, istenme nedeni ve hangi amaçla kullanılacağını belirtildiği yazılı istek olmadan verilemez. Ancak kişinin kimliğini kanıtlayan resmî bir belge ile şahsen başvurması halinde yazılı müracaat aranmaz. Nüfus kayıt örneklerinde, bunları istemeye yetkili olanlar tarafından açıkça ve gerekçeli olarak istenmediği takdirde, kimlik bilgileri dışında kişisel bilgilere yer verilmez. Bu belgeler üzerinde silinti ve kazıntı yapılamaz.

ile veli, vasi, alt ve üst soyları ya da bu kişilere ait vekâletnameyi ibraz edenlerin kişisel verileri hukuka uygun olarak kaydettiği kabul edilmektedir. Bunların dışında kalan kurumlar ve tüzel kişiler, yazılı olarak başvurmak ve istem nedenini açıkça belirtmek suretiyle Bakanlık veya mülkî idare amirinin emri ile nüfus kayıt örneğini alabilirler.

Kanunun 45. maddesi ile İçişleri Bakanlığı'nın kimlik verilerini hangi kurum ve kuruluşlarla paylaşabileceği ayrıca düzenlenmiş olup bu kapsamda kaydedilen kişisel veriler bakımından da hukuka uygunluk söz konusu olacaktır⁵⁶⁸.

-4857 Sayılı İş Kanunu'nda yer alan düzenleme:

İşverenin çalıştırdığı her işçi için düzenlemek zorunda olduğu işçi özlük dosyalarında işçilerin kimlik bilgileri ile birlikte İş Kanunu ve diğer kanunlar uyarınca düzenlemesi ve muhafaza etmesi zorunlu olduğu belgeler yönünden işçiye ait olup bunların muhteviyatında yer alan kişisel verilerin hukuka uygun olarak kaydedildiği kabul edilecektir⁵⁶⁹.

-6098 Sayılı Türk Borçlar Kanunu'nda yer alan düzenleme:

İşçinin kişiliğinin korunması kapsamında Kanun'un 419. maddesi ile işçiye ait kişisel verilerin işveren tarafından kullanımının kapsamı belirlenmiş ve kaydın hukukiliği işçinin işe yatkınlığı ile ilgili veya hizmet sözleşmesinin ifası için zorunlu olduğu durumlar ile sınırlandırılmıştır⁵⁷⁰.

⁵⁶⁸ Kimlik Paylaşımı Sisteminin kullanılması

MADDE 45- (Değişik: 19/10/2017-7039/11 md.) (1) Bakanlık, merkezî veri tabanında tutulan verileri bu Kanunda belirtilen usul ve esaslar çerçevesinde kurumlarla; kimlik verilerini, kamu hizmeti sunan tüzel kişilikler, 3/6/2007 tarihli ve 5684 sayılı Sigortacılık Kanunu çerçevesinde faaliyette bulunan sigorta ve emeklilik şirketleri, 19/10/2005 tarihli ve 5411 sayılı Bankacılık Kanunu çerçevesinde faaliyette bulunan bankalar, Risk Merkezi ve 5411 sayılı Kanunun 73 üncü maddesinin son fıkrası uyarınca bilgi paylaşımı amacıyla kurulmuş şirketler, 21/11/2012 tarihli ve 6361 sayılı Finansal Kiralama, Faktoring ve Finansman Şirketleri Kanunu kapsamındaki finansal kiralama şirketleri ile finansman şirketleri; yerleşim yeri ve diğer adres bilgilerini ise Bakanlıkça belirlenen adrese dayalı kamu hizmeti sunan kuruluşlar, 5684 sayılı Kanun çerçevesinde faaliyette bulunan sigorta ve emeklilik şirketleri, 5411 sayılı Kanun çerçevesinde faaliyette bulunan bankalar, Risk Merkezi ve 5411 sayılı Kanunun 73 üncü maddesinin son fıkrası uyarınca bilgi paylaşımı amacıyla kurulmuş şirketler, 6361 sayılı Finansal Kiralama, Faktoring ve Finansman Şirketleri Kanunu kapsamındaki finansal kiralama şirketleri ve finansman şirketleri ile paylaşabilir.

⁵⁶⁹ İşçi özlük dosyası

Madde 75 - İşveren çalıştırdığı her işçi için bir özlük dosyası düzenler. İşveren bu dosyada, işçinin kimlik bilgilerinin yanında, bu Kanun ve diğer kanunlar uyarınca düzenlemek zorunda olduğu her türlü belge ve kayıtları saklamak ve bunları istendiği zaman yetkili memur ve mercilere göstermek zorundadır.

⁵⁷⁰ 3. Kişisel verilerin kullanılmasında

MADDE 419- İşveren, işçiye ait kişisel verileri, ancak işçinin işe yatkınlığıyla ilgili veya hizmet sözleşmesinin ifası için zorunlu olduğu ölçüde kullanabilir.

-5502 Sayılı Sosyal Güvenlik Kurumu Kanunu'nda yer alan düzenleme:

Sosyal Güvenlik Kurumu'nun, yalnızca kendisine 5502 sayılı Kanun⁵⁷¹ ve diğer kanunlar ile verilen görevleri yerine getirmek amacı ile kişisel verileri kaydedebileceği Kanun'un 35. maddesinde öngörülmüştür⁵⁷².

-5070 Sayılı Elektronik İmza Kanunu'nda yer alan düzenleme:

Elektronik sertifika hizmet sağlayıcısının elektronik sertifika talep eden kişinin yalnızca elektronik sertifika vermek için gerekli bilgileri kayıt altına alabileceği, kanunun "Bilgilerin korunması" başlıklı 12. maddesinde düzenlenmiştir⁵⁷³.

-5429 Sayılı Türkiye İstatistik Kanunu'nda yer alan düzenleme:

Türkiye İstatistik Kurumu'nun görev alanına giren konularla ilgili sayım ve araştırmalarda, istatistik üretimi için gerekli gördüğü her türlü ortamdaki veri ve bilgiyi, tüm istatistikî birimlerden isteme ve kaydetme yetkisi Kanun'un 7. maddesinde düzenlenmiştir⁵⁷⁴.

Özel kanun hükümleri saklıdır.

⁵⁷¹ Kurumun amacı ve görevleri

MADDE 3- Kurumun temel amacı; sosyal sigortacılık ilkelerine dayalı, etkin, adil, kolay erişilebilir, aktüeryal ve malî açıdan sürdürülebilir, çağdaş standartlarda sosyal güvenlik sistemini yürütmektir. Kurumun görevleri şunlardır:

- a) Ulusal kalkınma strateji ve politikaları ile yıllık uygulama programlarını dikkate alarak sosyal güvenlik politikalarını uygulamak, bu politikaların geliştirilmesine yönelik çalışmalar yapmak.*
- b) Hizmet sunduğu gerçek ve tüzel kişileri hak ve yükümlülükleri konusunda bilgilendirmek, haklarının kullanılmasını ve yükümlülüklerinin yerine getirilmesini kolaylaştırmak.*
- c) Sosyal güvenliğe ilişkin konularda; uluslararası gelişmeleri izlemek, Avrupa Birliği ve uluslararası kuruluşlar ile işbirliği yapmak, yabancı ülkelerle yapılacak sosyal güvenlik sözleşmelerine ilişkin gerekli çalışmaları yürütmek, usûlüne göre yürürlüğe konulmuş uluslararası antlaşmaları uygulamak.*
- ç) Sosyal güvenlik alanında, eğitim, araştırma ve danışmanlık faaliyetleri yapmak ve yaptırmak, kamu idareleri arasında koordinasyon ve işbirliğini sağlamak.*
- d) Bu Kanun ve diğer kanunlar ile Kuruma verilen görevleri yapmak.*

⁵⁷² MADDE 35

(Değişik altıncı fıkra: 4/4/2015-6645/43 md.) Kurum (Sosyal Güvenlik Kurumu), bu Kanun ve diğer kanunlarla verilen görevleri yerine getirmek amacıyla işlediği kişisel veriler ile ticari sır niteliğinde olan verileri, veri sahibinin noter onaylı muvafakati olmadan gerçek veya tüzel kişilerle paylaşamaz.

⁵⁷³ Madde 12- Elektronik sertifika hizmet sağlayıcısı;

- a) Elektronik sertifika talep eden kişiden, elektronik sertifika vermek için gerekli bilgiler hariç bilgi talep edemez ve bu bilgileri kişinin rızası dışında elde edemez.*

⁵⁷⁴ Bilgi isteme, bilgilerin doğruluğunu araştırma, kontrol ve saklama

Madde 7- Başkanlık, Kurumun (Türkiye İstatistik Kurumu) görev alanına giren konularla ilgili sayım ve araştırmalarda, istatistik üretimi için gerekli gördüğü her türlü ortamdaki veri ve bilgiyi, tüm istatistikî birimlerden, Başkanlıkça belirlenen şekil, süre ve standartlarda doğrudan isteme yetkisine sahiptir.

-5809 Sayılı Elektronik Haberleşme Kanunu'nda yer alan düzenlemeler:

Kanun'un 51. maddesi ile kişisel verilerin işlenmesi ve gizliliğin korunması hususu düzenlenmiş; buna göre elektronik haberleşmenin sağlanması faaliyeti kapsamında trafik verilerinin; trafiğin yönetimi, arabağlantı, faturalama, usulsüzlük/dolandırıcılık tespitleri ve benzeri işlemleri gerçekleştirmek veya tüketici şikâyetleri ile arabağlantı ve faturalama anlaşmazlıkları başta olmak üzere, uzlaşmazlıkların çözümü amacıyla sadece işletmeci tarafından yetkilendirilen kişilerle sınırlı kalmak kaydıyla kaydedilebileceği öngörülmüştür⁵⁷⁵. Aynı Kanun'un 60. maddesi⁵⁷⁶ ile de Bilgi Teknolojileri ve İletişim Kurumu'nun görevi

Başkanlık, gerektiğinde verilen veri veya bilgilerin doğruluğunu araştırmaya, kontrol etmeye, ilgililerden ek bilgi ve belge istemeye, araştırma ve kontroller sonucu düzenlenecek belgelerle gerçek veri ve bilgiyi belirlemeye yetkilidir.

Başkanlığın veri ve bilgi derleme ve yayımlama işlemleri dâhil her türlü faaliyetleri elektronik ortamda yapılabilir, arşivlenebilir ve elektronik imza kullanılabilir.

Elektronik ortamda tutulan bilgilere ilişkin belgeler, bu veri ve bilgilerin kesinleşip kullanıma açık hâle gelmesine kadar saklanır ve bu sürenin sonunda imha edilir.

⁵⁷⁵ 1) Kişisel verilerin işlenmesi ve gizliliğin korunması

MADDE 51

(7) Trafik verileri; trafiğin yönetimi, arabağlantı, faturalama, usulsüzlük/dolandırıcılık tespitleri ve benzeri işlemleri gerçekleştirmek veya tüketici şikâyetleri ile arabağlantı ve faturalama anlaşmazlıkları başta olmak üzere, uzlaşmazlıkların çözümü amacıyla sadece işletmeci tarafından yetkilendirilen kişilerle sınırlı kalmak kaydıyla işlenir ve bu uzlaşmazlıkların çözüm süreci tamamlanıncaya kadar gizliliği ve bütünlüğü sağlanarak saklanır.

(8) İşletmeciler konum verilerinin işlenmesinde abonelere/kullanıcılara bu verilerin işlenmesini reddetme imkânı sağlar. İlgili mevzuatın ve yargı kararlarının öngördüğü durumlar haricinde ancak acil yardım çağrıları ile 29/5/2009 tarihli ve 5902 sayılı Afet ve Acil Durum Yönetimi Başkanlığının Teşkilat ve Görevleri Hakkında Kanunda tanımlanan afet ve acil durum hâllerinde abonelerin/kullanıcıların açık rızası aranmaksızın konum verileri ve ilgili kişilerin kimlik bilgileri işletmeci tarafından yetkilendirilen kişilerle sınırlı olmak kaydıyla işlenebilir.

(9) Abone/kullanıcı şikâyetlerinin incelenmesi ve denetim faaliyetleri kapsamında trafik ve konum verileri ile kişisel veriler, belirtilen faaliyetlerle sınırlı olmak kaydıyla işlenebilir.

(11) İşletmeciler, tahsilata ilişkin riskin yönetilmesi ve kötü niyetli kullanımların önlenmesi amacıyla abonelerin elektronik haberleşme hizmetlerine yönelik fatura tutarı ve ödeme bilgilerini diğer işletmecilerle paylaşabilir veya işleyebilir

⁵⁷⁶ 2) Kurumun yetkisi ve idarî yaptırımlar

MADDE 60

(11) (Ek: 15/8/2016-KHK-671/25 md.; Aynen kabul: 9/11/2016-6757/22 md.) Kurum, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerin siber saldırılara karşı korunması ve bu saldırılara karşı caydırıcılık sağlamak için her türlü tedbiri alır veya aldırır.

kapsamında ilgili yerlerden bilgi, belge, veri ve kayıtları alabileceği düzenlenmiş olup bu kapsamda kişisel verileri kaydetme yetkisi bulunmaktadır.

-6563 Sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun'da yer alan düzenleme:

Kanun'un 10. maddesi ile hizmet sağlayıcıların ve aracı hizmet sağlayıcının kişisel verilerin korunması yükümlülüğü düzenlenmiş, aynı madde aile bu kişilerin kanun çerçevesinde yürüttüğü faaliyetler⁵⁷⁷ nedeni ile kişisel verileri kaydedebileceği de öngörülmüştür.

**Meşru savunma* biçimindeki hukuka uygunluk nedeni ise TCK'nun 25. maddesinin birinci fıkrasında *"Gerek kendisine ve gerek başkasına ait bir hakka yönelmiş, gerçekleşen, gerçekleşmesi veya tekrarı muhakkak olan haksız bir saldırıyı o anda hal ve koşullara göre saldırı ile orantılı biçimde defetmek zorunluluğu ile işlenen fiillerden dolayı faile ceza verilmez."* şeklinde düzenlenmiştir.

Meşru savunma, kişinin kendisini savunması, kendisinin veya bir başkasının meşru haklarına yönelen saldırılara kuvvet kullanarak karşı çıkması olarak tanımlanmaktadır⁵⁷⁸.

Bir fiilin meşru savunma olarak nitelendirilebilmesi için; saldırıya ve savunmaya ilişkin olmak üzere belirli şartların varlığı aranmaktadır⁵⁷⁹. Saldırıya ilişkin olarak; öncelikle bir saldırının bulunması, bu saldırının haksız (hukuka aykırı) olması ve bir hakka yönelmiş olması ile halen mevcut olması gerekir. Savunmaya ilişkin olarak ise savunmanın bir zorunluluk olması, saldırıya ve saldırana karşı yapılması ile savunmanın tecavüz ile orantılı olması gerekir.

(12) (Ek: 15/8/2016-KHK-671/25 md.; Aynen kabul: 9/11/2016-6757/22 md.) Kurum, görevi kapsamında ilgili yerlerden bilgi, belge, veri ve kayıtları alabilir ve değerlendirmesini yapabilir; arşivlerden, elektronik bilgi işlem merkezlerinden ve iletişim altyapısından yararlanabilir, bunlarla irtibat kurabilir ve bu kapsamda diğer gerekli önlemleri alabilir veya aldırabilir. Kurum, bu fıkra da belirtilen görevlerin ifasında bakanlıklar, kurum ve kuruluşlar ile işbirliği içerisinde çalışır. Bu kapsamda Kurum tarafından istenen her türlü bilgi ve belge talebi; ilgili bakanlık, kurum ve kuruluşlar tarafından gecikmeksizin yerine getirilir. Bu fıkra ya göre bilgi ve belge talebinde bulunulması ve bu taleplerin yerine getirilmesine ilişkin usul ve esaslar ile diğer hususlar Başbakanlıkça belirlenir.

⁵⁷⁷ Tanımlar

MADDE 2 – (1) Bu Kanunun uygulanmasında;

a) Elektronik ticaret: Fiziki olarak karşı karşıya gelmeksizin, elektronik ortamda gerçekleştirilen çevrim içi iktisadi ve ticari her türlü faaliyeti... ifade eder.

⁵⁷⁸ Demirbaş, 2017: 286; Artuk vd.; 2013: 379.

⁵⁷⁹ Artuk vd.; 2013: 383; Hafizoğulları ve Özen, 2010: 243.

765 sayılı TCK'da saldırının meşru savunma kapsamında değerlendirilebilmesi için nefse veya ırza yönelik olması aranmakta idi. 5237 sayılı TCK'da ise meşru savunma, kişinin kendisine veya başkasına ait bir hakka karşı gerçekleşen, gerçekleşmesi veya tekrarı muhakkak olan bir saldırıyı savuşturmak olarak nitelendirilerek kapsamı genişletilmiştir. Her ne kadar, bu düzenleme ile hakkın niteliği hususunda bir açıklama yapılmamış olsa da, yalnızca bireysel nitelikteki hukuki menfaatlere yönelik saldırılar bakımından meşru savunmanın mümkün olabileceği savunulmaktadır⁵⁸⁰. Bu durumda, kişinin yaşamı, vücut bütünlüğü, şerefi, hürriyeti, mülkiyet hakkı, özel hayatının gizliliğine yönelik eylemlere karşı meşru savunmada bulunabileceği söylenebilir.

Bunun yanında, savunma eyleminin hukuka uygun kabul edilebilmesi için, saldırıdan başka türlü kurtulma imkanının bulunmaması yani savunmanın zorunlu olması gerekmektedir. Burada savunmanın zorunluluğu, saldırıya uğrayan hakka yönelik tehlikeyi kesin olarak ve derhal ortadan kaldırma yeteneğinde bulunup bulunmadığına göre değerlendirilir⁵⁸¹.

Kişisel verilerin kaydedilmesi suçu bakımından hukuka uygunluk nedeni olarak meşru savunmanın kabul edilmesi mümkün değildir. Kişinin kendisine veya başkasına bir saldırının gerçekleştirileceğini öğrenmesi halinde yetkili makamlara bildirmek amacı ile saldırıyı gerçekleştirecek kişiler ile ilgili verileri kaydettiği takdirde bu eyleminin meşru savunma kapsamında hukuka uygun olacağı savunulmaktadır⁵⁸². Ancak kanaatimizce meşru savunmanın niteliği itibarı ile bu durumda dahi kişisel verilerin kaydedilmesi suçu ile bağdaşamaz. Zira burada kaydetme eyleminin kişinin kendisine yönelen saldırıyı defetmeye matuf olduğundan ve saldırının defedilmesi için zorunlu olduğundan söz edilemez⁵⁸³.

**İlgilisinin rızasının bulunması*, suç tipine uygun bir fiili hukuka uygun hale getiren durumlardan bir diğeridir. Hukuka uygunluk sebebi olarak ilgilinin rızası, TCK'nun 26. maddesinin 2. fıkrasında, *"Kişinin üzerinde mutlak surette tasarruf edebileceği bir hakkına ilişkin olmak üzere, açıkladığı rızası çerçevesinde işlenen fiilden dolayı kimseye ceza verilmez."* ifadesi ile düzenlenmiştir.

Buna göre ilgilinin rızasının eylemi hukuka uygun hale getirebilmesi için söz konusu rızanın kişinin mutlak surette tasarruf edebileceği bir hakka ilişkin olarak verilmiş olması⁵⁸⁴,

⁵⁸⁰ Artuk vd.;2013: 388.

⁵⁸¹ Koca ve Üzülmüş, 2017: 280; Artuk vd.; 2013: 392; Demirbaş, 2017: 294.

⁵⁸² Özen, 2009: 17.

⁵⁸³ Aydın, 2015: 159.

⁵⁸⁴ İlgilinin rızası her durumda ihlali hukuka uygun hale getirmeyecek, rızanın eylemi hukuka uygun hale getirebilmesi için hareketin yönelik olduğu suç tipinde belirtilen konunun kişiye ait olması gerekecektir. (Özbek vd.; 2017: 316-317.)

rıza gösterenin rıza beyanına ehil olması⁵⁸⁵ ve rızanın açıkça veya zımni, yazılı ya da sözlü olarak açıklanmış olması⁵⁸⁶ koşullarını birlikte taşıması gerekir⁵⁸⁷. Bu durumda kişinin hakkına zarar veren veya risk altına alan eylemi kabul etmesi ile söz konusu eylem hukuka uygun kabul edilecektir⁵⁸⁸.

İlgilinin rızası, öğretide tipikliği kaldıran rıza ve hukuka aykırılığı kaldıran rıza olmak üzere ikili bir tasnife tabi tutulmuştur⁵⁸⁹. Bu tasnifin temeli, ceza kanununda düzenlenen suç tiplerine dayanmaktadır⁵⁹⁰. Suçun kanuni tanımında eylemin hak sahibinin rızası hilafına işlenmesine bir unsur olarak yer verilmiş ise ilgilinin rızasının bulunması tipikliği ortadan kaldırmaktadır⁵⁹¹. Diğer hallerde ilgilinin rızası hukuka aykırılığı ortadan kaldırır. Kişisel verilerin kaydedilmesi suçu bakımından suçun kanuni tanımına eylemin veri öznesinin rızasına rağmen gerçekleştirilmesine bir unsur olarak yer verilmediğinden veri öznesinin rızası eylemin hukuka aykırılığını ortadan kaldıracaktır⁵⁹².

Kural olarak ilgilinin rızasının hukuka uygunluk nedeni olarak kabul edilmesinde herhangi bir şekil şartı öngörülmemiş olup rıza açıklaması açık veya örtülü olabilir⁵⁹³. İlgilinin rıza gösterdiğine dair emarelerin bulunması veya hal ve tutumundan rıza gösterdiğinin anlaşılması yeterlidir⁵⁹⁴. Bunun yanında, rıza göstermeye ehil olan kimsenin rıza gösterilmesi gereken anda şuurunun yerinde olmaması ya da başka türlü bir nedenle rıza beyanında bulunamayacağı bir halde olması durumunda, söz konusu engeller bulunmasa idi eyleme rıza göstereceği kabul edilebilir ise bu duruma varsayılan (mefruz) rıza adı verilmektedir⁵⁹⁵. Varsayılan rızanın hukuka uygunluk sebebi olarak kabul edilmesinin sebebi mağdurun korunan menfaatinin zarara uğratılan hakkından üstün olmasına dayanmasıdır⁵⁹⁶.

Kişisel verilerin kaydedilmesi suçu açısından veri öznesinin rızasının hukuka uygunluk nedeni olarak kabul edilmesi için rıza açıklamasının örtülü olarak gerçekleştirilmesi

⁵⁸⁵ Eyleme rıza gösteren hak sahibinin temyiz kudretine sahip olması gerekir.(Özbek vd.; 2017:325.)

⁵⁸⁶ "Ceza sorumluluğunu kaldıran bir se-bep olarak rıza, suçun oluşumu açısından fiilin işlenmesinden önce ve en geç işlendiği sırada açıklandığında etkili olur. " (Madde gerekçesi).

⁵⁸⁷ Artuk vd.; 2013:434-439.

⁵⁸⁸ Ekici Şahin, 2012: 7.

⁵⁸⁹ Koca ve Üzülmmez, 2017: 286.

⁵⁹⁰ Ekici Şahin, 2012: 103.

⁵⁹¹ Koca ve Üzülmmez, 2017: 286.

⁵⁹² Aydın, 2015: 145.

⁵⁹³ Demirbaş, 2017: 330.

⁵⁹⁴ Ekici Şahin, 2012: 177.

⁵⁹⁵ Ekici Şahin, 2012: 223; Kangal, 2011: 224.

⁵⁹⁶ Koca ve Üzülmmez, 2017: 294; Kangal, 2011: 233.

KVKK'nın 5/1. maddesi ile kişisel verilerin ancak veri öznesinin açık rızası ile işlenebileceğinin belirtilmiş olması karşısında mümkün görünmemektedir⁵⁹⁷. Açık rızanın tanımı ve hangi hallerde eylemi hukuka uygun hale getirdiğine ilişkin olarak yukarıdaki açıklamalara bakılmalıdır. Öte yandan, KVKK'nın 5/2-b maddesinde *“Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması”* halinde kişisel verinin veri öznesinin rızası olmaksızın işlenebileceği belirtilmiş olmakla, varsayılan rızaya geçerlilik tanındığı görülmektedir.

Veri öznesinin veri işleme faaliyetine rıza göstermiş olmasının veri işlemede uyulması gereken temel ilkelere riayet edilmesi yükümlülüğünü ortadan kaldırmadığı yukarıda belirtilmiş idi. Başka bir anlatımla, veri öznesinin rıza göstermesi, verilerin dürüstlük kuralına uygun, doğru ve gerektiğinde güncel olarak, belirli, açık ve meşru amaçlar için, işlendikleri amaçlarla bağlantılı, sınırlı ve ölçülü olarak işleme ile işlendikleri amaç için gerekli olan süre kadar muhafaza etme ilkelerinden feragat ettiği anlamına gelmez. KVKK'nın 17. maddesinde TCK'nın 135 ila 140 maddelerine yapılan atıfla veri sorumlularının kanuna aykırı eylemlerinin TCK kapsamında cezalandırılacağı düzenlenmiştir. O halde, veri öznesinin kişisel verilerinin kaydedilmesine rıza göstermiş olması durumunda kişisel verilerinin örneğin yanlış ya da belirsiz, müphem ve gayrimeşru amaçlar için kaydedilmesi halinde bu rıza beyanı kaydetme eylemini hukuka uygun hale getirmeyecektir. Nitekim ilgilinin rızasının konusu kanun, ahlak ve adaba aykırı olamaz⁵⁹⁸.

Bir eylemin gerçekleştirilmesine ilişkin gösterilen ve eylemi hukuka uygun hale getiren rıza, eylem tamamlanıncaya kadar her an geri alınabilir⁵⁹⁹.

2.4. Suçun Özel Görünüş Biçimleri

2.4.1. Teşebbüs

Ceza kanunlarında yer verilen suçların işlenmesi süreci; failin o suçlardan birini işlemeye karar vermesi, bunun için hazırlık yapması ve son olarak icra hareketlerin gerçekleştirilmesi ile neticenin doğması üzerine suçun tamamlanması biçiminde cereyan etmektedir⁶⁰⁰. TCK'nın 35. maddesinde düzenlenen teşebbüs, elverişli hareketler ile icrasına başlanan suçun failin elinde olmayan herhangi bir nedenle tamamlanamaması durumunu ifade

⁵⁹⁷ Aydın, 2015: 146; Akdağ, 2013: 113-114.

⁵⁹⁸ İçel vd., 2000: 185.

⁵⁹⁹ Demirbaş, 2017: 331.

⁶⁰⁰ Koca ve Üzülmüş, 2017: 407.

eder⁶⁰¹. Toplumsal barışın, suçun kanuni tanımında öngörülen neticenin suçun teşebbüs aşamasında kalmış olması nedeni ile ortaya çıkmaması halinde dahi bozulması, suça teşebbüsün cezalandırılmasını gerektirir⁶⁰².

Öğretide bir kısım yazarlar tarafından, kişisel verilerin kaydedilmesi suçunun neticesi harekete bitişik bir suç olması gerekçesi ile teşebbüse elverişli olmadığı, kişisel verilerin hukuka aykırı olarak ele geçirilmesi suçunun bağımsız olarak düzenlenmiş olması karşısında kişisel verilerin ele geçirilmesi ile birlikte henüz kaydedilmemiş olmasının da teşebbüs olarak kabul edilemeyeceği ifade edilmektedir⁶⁰³.

Bizim de katıldığımız diğer görüşe göre ise, hareketin parçalara bölünebilmesi durumunda teşebbüsün söz konusu olabileceği; örneğin kişisel verilerin kaydedilmesinden ibaret fiil bakımından, kayıt işleminin başlaması ile tamamlanması arasında failin yakalanması veya teknik birtakım problemler yaşanması nedeni ile icra hareketi başlamış fakat failin elinde olmayan sebeplerle suç tamamlanamamış olacağından failin eyleminin suça teşebbüs olarak değerlendirilmesi mümkündür⁶⁰⁴.

2.4.2. İştirak

Suç tipinin, tek kişi tarafından gerçekleştirilmeye elverişli olmasına karşın birden fazla kişinin önceden yapılan bir işbirliği içerisinde birlikte işlenmesi durumuna suça iştirak adı verilir⁶⁰⁵.

Kişisel verilerin kaydedilmesi suçunun birden fazla fail tarafından birlikte işlenmesi halinde suça iştirake ilişkin genel hükümlerin uygulanması söz konusu olacaktır⁶⁰⁶. Bu anlamda özellik arz eden husus, TCK'nın 137. maddesinde öngörülen, kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle ve belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenmesi biçimindeki nitelikli unsurlar özgü suç niteliği taşıdığından suça iştirakin değerlendirilmesinde bu durumun dikkate alınmasını gerektirmesidir⁶⁰⁷.

⁶⁰¹ Koca ve Üzülmüş, 2017: 407; Özbek vd., 2017: 430.

⁶⁰² Demirbaş, 2017: 457.

⁶⁰³ Özbek vd., 2016: 576.

⁶⁰⁴ Soyaslan, 2016: 352; Hafızoğulları ve Özen, 2009: 20; Yaşar vd., 2014: 4440; Akdağ, 2013: 123; Aydın, 2015: 161; Özen, 2009: 18.

⁶⁰⁵ Demirbaş, 2017: 492.

⁶⁰⁶ Soyaslan, 2016: 352; Yaşar vd., 2014: 4440.

⁶⁰⁷ Aydın, 2015: 162.

2.4.3. İçtima

Birden fazla hukuki menfaatin tek bir fiille veya aynı hukuki menfaatin birden fazla fiille ihlal edilmesine suçların içtimaı adı verilir⁶⁰⁸. Suçların içtimaı, failin birden çok suç işlenmesi halinde sorumluluğun kapsamını belirlemektedir⁶⁰⁹. TCK'daki suçların içtimaı halleri; 42. maddede yer verilen “bileşik suç”, 43. maddede yer verilen “zincirleme suç” ile 44. maddede yer verilen “fikri içtima”dır.

Ceza kanununda yer alan normların aynı fiille ilgili görünmesine rağmen, esasen bu normlardan yalnızca birinin somut olaya uygulanabiliyor olması durumu ise görünüşte içtima (birleşme) olarak ifade edilir⁶¹⁰. Görünüşte birleşme, özel norm-genel norm ilişkisi yönünden söz konusu olabilir. Buna göre, gerek özel norm ve gerekse genel norm, aynı hukuksal değere ilişkin olmalıdır ve özel normun, genel normun nitelikleri ile birlikte genel norma nazaran bünyesinde birtakım ek nitelikleri kendine özgü olarak barındırması halinde somut olayda özel norm uygulama alanı bulacaktır⁶¹¹.

TCK'nın 132. ve devamı maddelerinde özel hayata ve hayatın gizli alanına karşı suçlar başlığı altında haberleşmenin gizliliğini ihlal, kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması, özel hayatın gizliliğini ihlal, kişisel verilerin kaydedilmesi, kişisel verileri hukuka aykırı olarak verme, yama ve ele geçirme ile kişisel verileri yok etmeme suçları öngörülmüştür. Bu suçların tamamı bakımından korunan hukuki menfaat kişinin özel hayatıdır. Burada, haberleşmenin gizliliğini ihlal veya kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması durumunda haberleşme içeriğinin ya da kişiler arasındaki konuşmaların kaydedilmesi sırasında kişisel verilerin de kayıt altına alınması halinde fail hakkında fikri içtima hükümlerinin uygulanacağı ve TCK madde 44 uyarınca en ağır cezayı gerektiren suçun cezasına hükmedileceği savunulmaktadır⁶¹².

Kişisel verilerin kimliği belirli veya belirlenebilir kişiye ait her türlü bilgi olarak tanımlandığı ve bu kapsamda kişinin görüntüsünün ve sesinin kişisel veri niteliğinde olduğu yukarıda ifade edilmiş idi. Bu nedenle özel hayata karşı suçlar içerisinde düzenlenen ve kişisel verilerin kaydedilmesi, verilmesi, yayılması, ele geçirilmesi ile yok edilmemesi biçimindeki suçlar haricindeki düzenlemelerin hukuki konusunu oluşturan kişiye ait ses ve görüntülerin, kayıt altına alınması halinde aynı zamanda 135. maddedeki suçu oluşturacağı

⁶⁰⁸ Özbek vd., 2017: 531; Koca ve Üzülmöz, 2017: 498.

⁶⁰⁹ Koca ve Üzülmöz, 2017: 498.

⁶¹⁰ İçel, 2008: 36.

⁶¹¹ İçel, 2008: 37.

⁶¹² Gültekin, 2012: 152.

aşıkardır⁶¹³. Ancak burada özel norm - genel norm ilişkisinden kaynaklanan görünüşte içtima durumu nazara alınmalıdır ve somut olaya genel norm niteliğindeki kişisel verilerin kaydedilmesi düzenlemesi değil, olayın özelliğine göre diğer düzenlemelerin uygulanması gerekir⁶¹⁴. Bu durumda, kişiler arasındaki haberleşme içeriklerinin kaydedilmesi durumunda TCK'nın 132. maddesi, kişiler arasındaki aleni olmayan konuşmaların kaydedilmesi veya kişinin kendi katıldığı aleni olmayan bir söyleşiyi kaydetmesi durumunda TCK'nın 133. maddesi uygulama alanı bulacaktır.

Bunun yanında, 134. maddede düzenlenen özel hayatın gizliliğini ihlal suçunun TCK'nın 9. bölümünde düzenlenen suçlar içerisinde genel norm niteliğini haiz olduğu savunulmaktadır⁶¹⁵. Zira kanunda özel hayat kavramı tanımlanmamış olmakla birlikte bu suçun konusunu, kişinin yalnızca kendisinin bildiği ve veya dar bir çevre ile paylaştığı bilgiler veya olayların oluşturduğu belirtilmekte ve bu belirleme suçun kapsamını oldukça genişletmektedir⁶¹⁶. Ancak özel hayatın gizliliğini ihlal suçunun kişisel verilerin kaydedilmesi suçu ile ilişkisi, aynı bölümdeki diğer suçlara göre farklılık arz etmektedir.

Her ne kadar, kişisel verilerin kaydedilmesi suçu ile korunan hukuki menfaat kişinin özel hayatı olsa da bu suçun konusunu kanunkoyucunun benimsediği üç alan teorisine göre kişinin özel hayat alanı ile sır hayat alanı dışında kalan ortak hayat alanına ait veriler de oluşturabilir. Bu kapsamda, kişinin kimliğini belirlemeye imkan vermesi halinde herhangi bir sınırlama olmaksızın kişiye ait her türlü bilgi kişisel veridir. Oysa özel hayatın gizliliğini ihlal suçu düzenlemesi, kişinin yalnızca uygun gördüğü kişiler ile uygun gördüğü ölçüde paylaştığı ve dolayısı ile makul bir dokunulmazlık beklentisinin olduğu hayat alanına müdahale edilmesini önlemeyi amaçlamaktadır. Bu nedenle kaydedilen kişisel verinin kişinin hayatının dışarıdan gizlediği ve başkaları tarafından öğrenilmesini istemediği bölümüne dahil olması halinde kişisel verilerin kaydedilmesi suçuna göre özel norm niteliğinde olan özel hayatın gizliliğin ihlal suçu oluşacaktır⁶¹⁷. Yargıtay da bilhassa eylemin bu özelliğini suçu kişisel verilerin kaydedilmesi suçundan ayıran kıtas olarak kabul etmektedir⁶¹⁸.

⁶¹³ Akdağ, 2013: 125.

⁶¹⁴ Akdağ, 2013: 125, Özen, 2009: 18.

⁶¹⁵ Tezcan vd., 2017: 639.

⁶¹⁶ Tezcan vd., 2017: 641.

⁶¹⁷ Aynı yönde bk. Aydın, 2015: 163.

⁶¹⁸ "...Sanığın aşamalarındaki, koridorda önünde yürüten mağdurun bacağındaki dövme figürü ilgisini çektiği için çekim yaptığına ilişkin ikrar içeren beyanları, sanığı daha önceden tanımayan ve kendi onur ve namusunu ilgilendiren bir konuda iftira atması için geçerli sebep bulunmayan mağdurun, sanığın cep telefonundan elde edilen video görüntülerine ait fotoğraflardan, siyah-beyaz elbiseli bayanın arkadan çekilmiş görüntülerinin

Kişisel verilerin kaydedilmesi suçunun zincirleme suç biçiminde gerçekleştirilmesi mümkündür⁶¹⁹. Konusu kişisel veriler olan suçlar bakımından ise fikri içtima söz konusu olabilir⁶²⁰. Bu duruma, kişisel verinin herkesçe ulaşılabilir bir şekilde sosyal medya sitesine kaydedilmesinin akabinde yayma fiili de gerçekleşmiş olacağından TCK'nın 135. maddesi ile 136. maddesi bakımından fikri içtima hükmü uygulanacaktır⁶²¹.

Öğretide, kişisel verilerin hukuka aykırı olarak kaydedilmesi suçunun bilişim sisteminde yer alan veriler bakımından gerçekleştirilebilmesi öncelikle söz konusu bilişim sistemine girilmesi ve orada hukuka aykırı olarak kalmayı gerektireceğinden TCK'nın 243. maddesinde yer alan “bilişim sistemine girme suçu” kişisel verilerin kaydedilmesi suçu bakımından geçit suçu⁶²² olarak kabul edileceği savunulmaktadır⁶²³. Oysa bir suçun başka bir suç bakımından geçit suçu olarak kabul edilebilmesi için her iki suçun da aynı hukuki menfaati korumaya yönelmesi, suçun her ikisinin de faili ile mağdurunun aynı olması gerekmektedir⁶²⁴. Bu nedenle her ne kadar bilişim sistemine girme suçu ile kişisel verileri kaydetme suçu arasında bir geçit ilişkisi varmış gibi görünse de, bu iki suçun korudukları hukuki değer, fail ve mağdur açısından farklılık arz etmeleri nedeni ile bu suçların birlikte işlenmesi halinde bağımsız olarak varlıklarını sürdürecekleri ve gerçek içtima kurallarına tabi olacağı sonucuna varılmaktadır.

kendisine ait olduğuna ilişkin anlatımı, adliye kamera kayıtlarının incelenmesinde, sanığın, koridorda mağduru arkadan takip ederek cep telefonu ile çekim yaptığının tespit edilmesi, bilirkişi raporunda, sanığın cep telefonunda, mağdurun özellikle arka kısımdan bel, kalça ve bacak kısımlarına yoğunlaşan ve herhangi bir konuşma içeriği bulunmayan görüntü kayıtları ve bu görüntü kayıtlarının dışında telefonun hafıza kartında ayrıca kimlikleri anlaşılamayan ve farklı tarihlerde oluşturulduğu anlaşılan başka bayanlara ait benzer nitelikte görüntülerin bulunduğu belirtilmesi karşısında, sanığın, cinsel arzu ve isteklerini tatmin maksadıyla mağduru takip ederek fiziksel mahremiyetini içeren görüntülerini çekerek kaydettiğinin anlaşıldığı, mağdurun fiziksel mahremiyetine ilişkin görüntüleri yasal anlamda kişisel veri kapsamında değerlendirilemeyeceğinden...”
Yargıtay 12. CD. 2014/7518 E., 2014/23588 K., 24.11.2014.

⁶¹⁹ Özbek vd., 2016: 576; Özen, 2009: 18.

⁶²⁰ Özbek vd., 2016: 576.

⁶²¹ Özen, 2009: 19.

⁶²² “Failin bir suçu işlemek için aynı hukuki değeri koruyan daha hafif bir suçtan geçmek zorunda olduğu hallerde geçit suçu söz konusu olur.” (İçel, 2008: 46)

⁶²³ Soyaslan, 2016: 352.

⁶²⁴ İçel, 2008: 47.

2.5. Yaptırım ve Muhakeme

2.5.1. Yaptırım

Kişisel verilerin kaydedilmesi suçunun bir yıldan üç yıla kadar hapis cezası ile cezalandırılacağı öngörülmüştür. Ancak kaydedilen kişisel verilerin kişinin siyasi, felsefi veya dini görüşlerine, ırki kökenine, ahlaki eğilimlerine, cinsel yaşamına, sağlık durumuna veya sendikal bağlantılarına ilişkin olması durumunda ceza yarı oranında arttırılacaktır.

Madde metni, yaptırım bakımından birkaç kez değişikliğe uğramış bulunmaktadır. Bu değişikliklerin ilki; 21.02.2014 tarihli ve 6526 sayılı kanunun 3. maddesi ile maddenin birinci fıkrasında gerçekleştirilmekle, cezanın alt sınırını altı aydan bir yıla çıkarmıştır. İkinci değişiklik ise maddenin ikinci fıkrasında yapılmış olup 24.03.2016 tarihli ve 6698 sayılı KVKK'nın 30. maddesi ile bu kanun bakımından özel nitelikli kişisel veri olarak adlandırılan ve istisnai birkaç durum dışında işlenmesi yasak olan; kişinin siyasi, felsefi veya dini görüşlerine, ırki kökenine, ahlaki eğilimlerine, cinsel yaşamına, sağlık durumuna veya sendikal bağlantılarına dair verilerin kaydedilmesi halinin verilecek cezada bir artırım nedeni olarak kabul edilmesine ilişkindir. Bu durumda verilecek ceza yarı oranında arttırılacak olup failin bir yıl altı ay ile dört yıl altı ay arasında değişen bir süre hapis cezası ile cezalandırılması mümkündür.

Suçun yaptırımına ilişkin olarak değinilmesi gereken bir diğer husus ise Kanun'un 137. maddesi uyarınca suçun kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle veya belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenmesi durumlarının nitelikli hal kapsamında düzenlendiği ve bu nedenle faile isnat edilen suçun sabit olması halinde verilecek cezanın yine yarı oranında arttırılması gerektiğidir.

Kanunun 140. maddesi uyarınca kişisel verilerin kaydedilmesi suçunun işlenmesi dolayısı ile tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunacaktır.

5271 sayılı Ceza Muhakemesi Kanunu'nun 253. ve devamı maddelerinde düzenlenen "uzlaştırma" kurumunun suçun takibinin şikayete bağlı olmayışı ve anılan maddelerde, suçun şüpheli ile mağdur veya suçtan zarar gören kişinin uzlaştırılması girişiminde bulunulacak suç tipleri arasında sayılmamış olması nedeni ile uygulanması söz konusu değildir.

2.5.2. Muhakeme

TCK'nın 139. maddesi uyarınca kişisel verilerin kaydedilmesi suçunun soruşturulması ve kovuşturulması şikayete bağlı olmayıp re'sen takip edilecektir.

Öngörülen yaptırımın üst sınırı nazara alındığında görevli mahkemenin asliye ceza mahkemesi olduğu anlaşılmaktadır.

5271 sayılı Ceza Muhakemesi Kanunu'nun 12. maddesi uyarınca yetkili mahkeme suçun işlendiği, yani kişisel verilerin kaydedildiği yer mahkemesidir⁶²⁵. Ancak bu suçun maddi unsuru olan kaydetme fiilinin bilişim sistemleri vasıtası ile gerçekleştirilmesi ihtimali yüksek olduğundan icra hareketlerinin bir kısmının Türkiye'de bir kısmının başka bir ülkede veya Türkiye'nin farklı yerlerinde gerçekleştirilmesi halinde mesafe suçu söz konusu olmakla; TCK'nın 8. maddesi uyarınca ilk durumda suç Türkiye'de gerçekleştirilmiş kabul edilecek; ikinci durumda ise fiilin gerçekleştiği yer, bunun tespit edilememesi halinde ise CMK'nın 13. maddesinde yer alan özel yetki kuralları nazara alınarak yetkili mahkeme belirlenecektir⁶²⁶.

Kişisel verilerin kaydedilmesi suçunun kamu görevlisinin görevi sebebiyle işlenmesi durumunda 4483 sayılı Memurlar ve Diğer Kamu Görevlilerinin Yargılanması Hakkında Kanun hükümleri uyarınca bu kişiler hakkında soruşturma yapılabilmesi izin koşuluna bağlanmış olup soruşturma izni alındıktan sonra soruşturma yapılması gerekmektedir⁶²⁷.

Suçun kural olarak dava zamanaşımı süresi TCK'nun 66/1-e maddesi uyarınca sekiz yıldır.

⁶²⁵ Yaşar vd., 2014: 4441.

⁶²⁶ Gültekin, 2012: 159.

⁶²⁷ Yaşar vd., 2014: 4441.

SONUÇ

Tarih boyunca, bilgiye sahip olma güç ile eşdeğer kabul edilmiştir. Bu nedenle bireyler birbirileri hakkında elde ettikleri bilgileri her ne amaçla olursa olsun gerektiği takdirde kullanmak üzere kaydetme, muhafaza etme, aktarma eğiliminde olmuşlardır. Teknolojinin gelişimi, bu eğilimi adeta bir veri açlığına çevirmiş, geleneksel bilgi işleme yöntemlerinin yerini oldukça kolay ve hızlı veri işleme faaliyetine bırakması kişiye ilişkin bilgileri birer meta haline getirmiştir. Kişilerin isim ve soyisminden aile bireylerine, geçirdiği hastalıklardan cinsel eğilimlerine, eğitim bilgilerinden ekonomik durumlarına kadar kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi olarak tanımlanan kişisel veriler; hem devletin hem de özel kişi ve kurumların işleme faaliyetlerine konu olmaktadır. Böylesine yoğun bir gözetime maruz kalan bireyin kişiliğinin giderek şeffaflaşması ve davranışlarını otokontrol süzgecinden geçirme mecburiyeti duyması madalyonun bir yüzüdür. Diğer yüzü ise kamu güvenliği, kamu düzeni, hizmetlerin devamlılığı ve sıhhati gibi gerekçeler ile bireylerin kişisel verilerinin işlenmesine rıza gösterme mecburiyetinde bırakılmasıdır. “Saklayacak bir şeyin yoksa korkacak bir şeyin de yok demektir” düşüncesi ile temel hak ve özgürlüklerinden adım adım ödün veren bireyin kişiliğini özgürce geliştirme hakkına sahip olabileceğinden de söz edilemez.

Kişisel verilerin işlenmesi hususuna hukuksal bir çerçeve çizme düşüncesi ilk kez, kişisel bilgilerin denetlenmeksizin kaydedilerek muhafaza edilmesinin sonuçlarını, II. Dünya Savaşı sırasında acı bir şekilde tecrübe eden Avrupa’da filizlenmiştir. Bu düşünce uluslararası anlamda ilk meyvesini 28 Ocak 1981 tarihli “Kişisel Verilerin Otomatik İşleme Tabi Tutulması Sırasında İnsanın Korunmasına İlişkin Sözleşme” ile vermiş, onu 24 Ekim 1995 tarihli “Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımında Bireylerin Korunmasına İlişkin 95/46/AT sayılı Avrupa Parlamentosu ve Konseyi Yönergesi” izlemiştir. Bu düzenlemeler, bireyin kişisel verilerinin korunması hakkını bütüncül ve yeknesak bir biçimde korumayı amaçlamıştır. Buna rağmen ülkeler bağlamında eşit koruma düzeyi sağlanamaması ve hızla gelişen teknolojinin getirdiği yenilikler sonucunda mevcut düzenlemelerin ihtiyaca cevap veremediğinin anlaşılması üzerine Avrupa Birliği üye ülkeler nezdinde doğrudan bağlayıcılık etkisini haiz olan 2016/679 sayılı Genel Veri Koruma Tüzüğü, 25 Mayıs 2018 tarihinde yürürlüğe girmek üzere kabul edilmiştir. Genel Veri Koruma Tüzüğü, Avrupa veri koruma hukukunu temelinden etkileyecek bir reform niteliğindedir.

Başlangıçta özel hayatın gizliliğinin korunması hakkının bir parçası olarak kabul edilen kişisel verilerin korunması hakkı, Avrupa İnsan Hakları Mahkemesi'nin içtihatlarına Avrupa İnsan Hakları Sözleşmesi'nin özel ve aile hayatına saygı başlıklı 8. maddesi bağlamında konu olmuş, uluslararası düzenlemeler amaç bakımından özel hayatın gizliliği kavramına atıf yapmıştır. Türkiye'de de gerek 2010 yılında gerçekleştirilen değişiklik ile kişisel verilerin korunması hakkının Anayasa'nın "özel hayatın gizliliği" başlıklı 20. maddesine eklenmesi ve gerekse Türk Ceza Kanunu'nda kişisel verilerin kaydedilmesi, verilmesi, ele geçirilmesi, yayılması ve yok edilmemesi suçlarının "özel hayata ve hayatın gizli alanına karşı suçlar" başlığı altında düzenlenmesi, Türk hukukunda da kişisel verilerin özel hayat kapsamında değerlendirildiğini göstermektedir.

Kişisel verilerin kişinin özel hayatı ile yakın ilişki içerisinde olduğu aksi inkar edilemez bir olgudur. Ancak kişisel verilerin korunması hakkının özel hayatın gizliliğinin korunması hakkından ayrılan yönleri, onun hukuk dünyasında bağımsız ve kendine özgü bir hak alanı olarak tanımlanmaya başlamasına sebep olmuştur. Bu yönler, kişisel verilerin hukuka ve dürüstlük kuralına uygun olarak, yalnızca belirli amaçlar dahilinde ve veri öznesinin rızası ya da veri işlemeyi yasallaştıran bir sebebe dayanarak işlenmesi zorunluluğu; veri öznesine işlenen verilerine erişim ve düzeltme hakkı verilmesi ile veri işleme faaliyetinin bağımsız bir otorite tarafından denetlenmesi zorunluluğudur. Nitekim kişisel verilerin korunması hakkı, 2000 tarihli Temel Haklar Şartı'nda bağımsız bir temel hak olarak kabul edilmiş, 2016/679 sayılı Genel Veri Koruma Tüzüğü'nde ise tüzüğün amacının kişisel verilerin korunması temelinde kişilerin korunması olduğu belirtilmiştir.

Kişisel verilerin korunmasına yönelik olarak ilk bağlayıcı hukuksal düzenleme olma niteliğini taşıyan 28 Ocak 1981 tarihli ve 108 sayılı Avrupa Konseyi Sözleşmesi, Türkiye tarafından 28 Ocak 1981 tarihinde imzalanmış olmasına karşın sözleşmede yer alan ilkelerin iç hukukun bir parçası haline getirilmesi şartı yerine getirilemediğinden, başka bir deyişle kişisel verilerin korunmasına ilişkin temel bir yasal düzenlemenin yürürlüğe konulamamış olması nedeni ile sözleşmenin onaylanması ve yürürlüğe konulması uzun bir süre mümkün olamamıştır. Bir yanda Avrupa Birliği'nin kişisel verilerin korunması hususunun yasal bir düzenlemeye kavuşturulması konusundaki ısrarlı talebi; diğer yanda özellikle 2005 yılında yürürlüğe giren 5237 sayılı Türk Ceza Kanunu'nda suç tipi olarak yer verilen birtakım eylemlerin hangi durumlarda hukuka aykırı olduğunu tespit etmeye esas oluşturacak özel bir kanunun bulunmaması nedeni ile uygulamada sorunlar yaşanması sonucunda 6698 sayılı Kişisel Verilerin Korunması Kanunu 24 Mart 2016 tarihinde kabul edilerek yürürlüğe konmuştur. Bu düzenleme, kişisel verilerin korunması hususunu yasal bir zemine

kavuşturması nedeni ile Türk hukuku için önemli bir adımdır; ancak kanunda yer verilen geniş istisnalar listesi düzenlemeyi esaslı eleştirilere maruz bırakmıştır. Zira bu istisnalar, bireylere kişisel verilerinin korunması hakkından yararlanabilecekleri oldukça kısıtlı bir alan bırakmaktadır. Bunun yanında, kanunun 2012 yılında teklifi yayınlanan 25 Mayıs 2018 tarihinde yürürlüğe girecek Genel Veri Koruma Tüzüğü yerine onun mülga edeceği 95/46/AT sayılı Yönerge esas alınarak hazırlanması diğer bir eleştiri konusudur.

Çalışmamızda, kişisel verilerin korunması hususu Türk Ceza Kanunu bağlamında ele alınmış, kanunun 135. maddesinde yer verilen “kişisel verileri kaydetme suçu” ayrıntıları ile incelenmiştir. TCK’nın 136. maddesinde düzenlenen, kişisel verilerin ele geçirilmesi, verilmesi ve yayılması ile 138. maddesinde düzenlenen kişisel verilerin yok edilmemesi suçlarına ise ana hatları ile yer verilmiştir.

Buna göre, kişisel verilerin kaydedilmesi suçu ile korunması amaçlanan hukuki değer; kanunun sistematigi, Anayasa ve içtihatlar karşısında kişinin özel hayatı olduğu sonucuna varılmıştır. Suçun maddi unsurlarından fiil, kişisel verinin herhangi bir yol ile herhangi bir formatta kaydedilmesidir. Burada mağdurun suç nedeni ile zarara uğrayıp uğramamasının bir önemi bulunmamaktadır. Bu nedenle kişisel verilerin kaydedilmesi suçu bir tehlike suçudur.

Kişisel verilerin kaydedilmesi suçunun konusu kişisel nitelikteki her tür veridir. Ancak kanunkoyucu, birtakım kişisel verilerin kaydedilmesinin bireylerin hak ve özgürlüklerinin önemli ölçüde ihlal edilmesi riski doğurması nedeni ile bu tür verilerin kaydedilmesini suçun nitelikli unsuru olarak kabul etmiştir. Hassas veya özel nitelikli olarak da adlandırılan bu veriler kanunda kişilerin siyasi, felsefi veya dini görüşlerine, ırkı kökenlerine, ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına ve sendikal bağlantılarına ilişkin olmak üzere sınırlı olarak yer almaktadır. Ancak bu kavramların soyut yapısı, zamansal ve bölgesel açıdan göreceli oluşu nedeni ile içeriğinin belirlenmesi ve sınırlarının çizilmesindeki güçlükler, ceza hukukunun kanunilik prensibine aykırılık teşkil etmektedir.

Kişisel verilerin korunmasına yönelik düzenlemelerinin hiçbirinin amacı, kişisel verilerin işlenmesine bütünü ile engel olunması değildir. Zira bireyin toplum içerisinde birtakım hizmetlerden faydalanabilmesi, güvenliğinin sağlanabilmesi ve ticari faaliyetlerin sağlıklı bir biçimde yürütülebilmesi gibi sebeplerle kişisel verilerin işlenmesi zorunludur. Bu kapsamda, kanunkoyucunun, kanunun 135. maddesinde kişisel verilerin kaydedilmesi suçu bakımından suçun konusunu oluşturan kişisel verinin “hukuka aykırı olarak” kaydedilmesi gerektiğine, başka bir deyişle hukuka özel aykırılık haline vurgu yapması;

kişisel verilerin kaydedilebilme koşullarının bir hukuk kuralı ile belirlenmiş olması karşısında kaydetme fiili bu mevzuata uygun olduğu sürece bu fiilin cezalandırılmasının mümkün olmadığına işaret etmektedir.

Kişisel verilerin kaydedilmesi suçu, TCK'nın “özel hayata ve hayatın gizli alanına karşı suçlar” başlığı altında düzenlenen 9. bölümündeki haberleşmenin gizliliğini ihlal, kişiler arasındaki konuşmaların kayda alınması, ve özel hayatın gizliliğini ihlal suçlarına göre genel norm niteliğindedir. Dolayısı ile failin kişisel veri niteliğindeki görüntü ve sesleri hukuka aykırı olarak kayıt altına alması halinde özel norm - genel norm ilişkisinden kaynaklanan görünüşte içtima durumu nazara alınmalıdır ve somut olaya genel norm niteliğindeki kişisel verilerin kaydedilmesi düzenlemesi değil, olayın özelliğine göre diğer düzenlemelerin uygulanması gerekir.

6698 sayılı KVKK'nın gerekçesinde, bu kanunun yürürlüğe konmasındaki öncelikli amacın bu konuda özel bir kanunun bulunmamasının TCK'da cezai müeyyideye tabi tutulan kişisel verilerin işlenmesi kapsamındaki birtakım fiillerin hangi hallerde hukuka uygun, hangi hallerde hukuka aykırı olduğunun belirlenmesinde yaşanan sorunların ortadan kaldırılması olduğu ifade edilmiştir. Ancak, KVKK, bir veri kayıt sisteminin parçası olarak işlenmeyen kişisel verileri kapsam dışı bırakmıştır. Bu durum, özel kanunda hukuka aykırı olduğu belirtilmeyen ve idari yaptırıma tabi tutulmayan birtakım eylemlerin ceza kanunu ile cezalandırılması sonucunu doğurduğundan kendi içerisinde bir çelişki barındırmaktadır.

Çalışmamızda, kişisel verilerin kaydedilmesi suçu özelinde kişisel verilerin korunması hukuku incelenmiştir. Türkiye’de uzun yıllar boyunca kişisel verilerin korunmasına yönelik özel bir düzenlemenin yürürlüğe konması ihtiyacı vurgulanmış, nihayet 2016 yılında bu ihtiyaca cevap vermesi beklentisi ile 6698 sayılı Kişisel Verilerin Korunması Kanunu Türk mevzuatına dahil edilmiştir. Bu oldukça büyük ve önemli bir adım olarak değerlendirilmekle birlikte, bireylerin kişiliğini serbestçe geliştirme, özel yaşamın gizliliği ve kişisel verilerin korunması hakları konusunda bilinçlenmeleri bu haklarının korunması talebini gerek devlete gerekse özel kişi ve kurumlara yöneltmelerinin de aynı derecede önem arz ettiği unutulmamalıdır.

KAYNAKÇA

- Akbulut, B. (2014). *Türk Ceza Kanunu ile Kabahatler Kanunu Genel Hükümleri Dışında Özel Olarak İncelenmesi*. Adalet Yayınevi, Ankara.
- Akdağ, H. (2013). *Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması*. Adalet Yayınevi, Ankara.
- Akgül, A. (2016). “Kişisel Verilerin Korunmasında Yeni Bir Hak: “Unutulma Hakkı” ve AB Adalet Divanı’nın “Google Kararı””. *Türkiye Barolar Birliği Dergisi*, 116: 11-38.
- Akgül, A. (2013). “Danıştay Kararları Işığında Kişisel Sağlık Verilerinin Korunması”. *Danıştay Dergisi*, 133: 21-45.
- Akgül, A. (2014). *Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması*. Beta Yayınevi, İstanbul.
- Akgül, A. (2015). “Kişisel Verilerin Korunması Bağlamında Biyometrik Yöntemlerin Kullanımı ve Danıştay Yaklaşımı”. *Türkiye Barolar Birliği Dergisi*, 118: 199-222.
- Akıncı, A. N. (2017). *Avrupa Birliği Genel Veri Koruma Tüzüğü’nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi*. TC Kalkınma Bakanlığı İktisadi Sektörler ve Koordinasyon Genel Müdürlüğü, Ankara.
- Akipek, J. ve Akıntürk, T. (2007). *Türk Medeni Hukuku Başlangıç Hükümleri*. Beta Yayınevi, İstanbul.
- Akrivopoulou, C. M. ve Garipidis, N.(2014): *Human Rights and the Impact of ICT in the Public Sphere: Participation, Democracy and Political Autonomy*. IGI Global, ABD.
- Aksoy, H. C. (2010). *Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması*. Çakmak Yayınevi, Ankara.
- Artuk, M. E., Gökçen, A., Yenidünya, C.(2013). *Ceza Hukuku Genel Hükümler*. Adalet Yayınevi, Ankara.
- Atak S. (2010). “Avrupa Konseyi’nin Kişisel Veriler Açısından Sağladığı Temel Güvenceler”. *Türkiye Barolar Birliği Dergisi*, Ankara, 87: 90-120.
- Avrupa Parlamentosu, (2015). *A Comparison Between US and EU Data Protection Legislation for Law Enforcement Purposes*. Avrupa Parlamentosu, Brüksel.
- Aydın N. (2013). “Tıp Ceza Hukukunda Verileri Hukuka Aykırı Olarak Verme ve Ele Geçirme Suçu (TCK m. 136)”. *Selçuk Üniversitesi Hukuk Fakültesi Dergisi*, 21(2):7-30.
- Aydın, S. E. (2015). *AIHM İçtihatları Bağlamında Kişisel Verilerin Kaydedilmesi Suçu*. On İki Levha Yayıncılık, İstanbul.

- Balkır, Z. G. (2005). “İşverenin Yönetim Hakkının Kullanılmasında Etik Sınırlar”. 2. Siyasette ve Yönetimde Etik Sempozyumu, 18-19 Kasım 2005, Sakarya Üniversitesi, s.197-209.
- Başalp, N. (2004). *Kişisel Verilerin Korunması ve Saklanması*. Yetkin Yayınları, Ankara.
- Başalp, N. (2015). “Avrupa Birliği Veri Koruması Genel Regülasyonu’nun Temel Yenilikleri”. *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, 21(1):77-105.
- Börding, A. (2017). “Safe Harbour: The Decision of the European Court of Justice”. *Big Data in Context, Legal, Social and Technological Insights*, Springer Open, 37-45.
- Bygrave, L. A. (2003). “Digital Rights Management and Privacy – Legal Aspects in the European Union”. E. Becker, W. Buhse, D. Günnewig, N. Rump Ed.). *Digital Rights Management*. Lecture Notes in Computer Science, vol 2770. Springer, Berlin, Heidelberg, s. 418-446
- Canveren Ö., Özeren E. (2014) “Avrupa İnsan Hakları Mahkemesi’nin X/Türkiye Kararı Temelinde Türkiye’de LGBT Mahkûmlara Yönelik Bir İnceleme”. *Kadın/Woman* 2000, 15 (1) 71-96.
- Centel N., Zafer H., Çakmut Ö. (2014). *Türk Ceza Hukukuna Giriş*. Beta Yayınevi, İstanbul.
- Demirbaş, T. (2017). *Ceza Hukuku Genel Hükümler*. Seçkin Yayınevi, Ankara.
- Demren Dönmez, B. (2011). “Türk Ceza Kanunu’nda ‘Kamu Görevlisi’ Kavramı”. *Türkiye Barolar Birliği Dergisi*, 94: 95-130.
- Díaz E. D. (2016). “The new European Union General Regulation on Data Protection and the legal consequences for institutions”. *Church, Communication and Culture*, 1(1): 206-239.
- Dix, A. (2013). “The Commission’s Data Protection Reform After Snowden’s Summer”. *Intereconomics, Leibniz Information Center for Economics, Forum on EU Data Protection Reform: Opportunities and Concerns*, 5: 268 – 271.
- Doğru O.; Nalbant A. (2013). *İnsan Hakları Avrupa Sözleşmesi Açıklama ve Önemli Kararlar*, 2. Cilt. Yüksek Yargı Kurumlarının Avrupa Standartları Bakımından Rollerinin Güçlendirilmesi Ortak Projesi, Avrupa Konseyi-T.C. Yargıtay Başkanlığı.
- Dülger M. V. (2013). *Bilişim Suçları ve İnternet İletişim Hukuku*. Seçkin Yayınevi, Ankara.
- Dülger, M. V. (2016). “Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması”. *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi*, 3(2): 101-167.
- Ekici Şahin, M. (2012). *Ceza Hukukunda Rıza*. On İki Levha Yayıncılık, İstanbul.

- Ergün, İ. (2008). *Siber Suçların Cezalandırılması ve Türkiye’de Durum*. Adalet Yayınevi, Ankara.
- Eryılmaz, K. (2015). “Türkiye Yargısının Ahlâkla İmtihani: “Doğal Olmayan” İlişki”. *Hukuk Kuramı*, 2 (5): 11-19.
- Fuster, G. G. ve Paepe, P. (2016). “Reflexive Governance and the EU Third Pillar: Analysis of Data Protection and Criminal Law Aspects”. E. Guild ve F. Geyer (Ed.). *Security versus Justice?*. Routledge Taylor&Francis Group, Londra ve New York, s.129-148.
- Geçmez, T. (2014). *Haberleşmenin Gizliliğini İhlal ve Özel Hayatın Gizliliğini İhlal Suçları* (TCK m. 132-134). Yayımlanmamış Yüksek Lisans Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.
- Gökcan, H. T. (2015). “Türk Ceza Kanunu Uygulamasında Kamu Görevlisi Kavramı”. *Ceza Hukuku ve Kriminoloji Dergisi*, 3 (2): 147-160.
- Görgeç, B. (2013). “Genel İşlem Koşullarının Kişilik Hakkı Kapsamında Değerlendirilmesi”. *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, 19 (1): 403-440.
- Gültekin, N. M. (2012). *Kişisel Verilerin Ceza Hukuku Yönünden Korunması*. Yayımlanmamış Yüksek Lisans Tezi, Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.
- Hafizoğulları Z. ve Özen M. (2009). "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar". *Ankara Barosu Dergisi*, 67/4:9-22.
- Hafizoğulları, Z., Özen, M. (2010). *Türk Ceza Hukuku Genel Hükümler*. US-A Yayıncılık, Ankara.
- Hakeri, H. (2007). “İhmalî Suçlar”. *Ceza Hukuku Dergisi*, 4:137-169.
- Hakeri, H. (2012). *Tıp Hukuku*. Seçkin Yayıncılık, Ankara.
- Hekimoğlu, F. M. (2017). “Psikiyatri Araştırmalarında ve Klinik Uygulamalarda Etik Standartların Önemi: Gey, Lezbiyen, Biseksüel ve Transgender Popülasyonu”. *Türkiye Klinikleri Journal of Medical Ethics-Law and History*, 25(3): 108-115.
- Idler, J. E. (2007) ,”Federal Classification and Ethno-Racial Identity”. *Public Affairs Quarterly*, 21(1) : 37-59
- İçel K., Sokullu-Akinci F., Özgenç İ., Sözüer A., Mahmutoglu F. S., Ünver Y. (2000). *İçel Suç Teorisi 2. Kitap*. Beta Yayınevi, İstanbul.
- İçel, K. (2008). “Görünüşte Birleşme (İçtima) İlkeleri ve Yeni Türk Ceza Kanunu”. *İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi*, 7(14):35-49.
- İtişgen, R. (2015). “Türk Ceza Hukukunda Kişisel Verileri Hukuka Aykırı Olarak Verme Veya Ele Geçirme Suçu”. *Türkiye Adalet Akademisi Dergisi*, 6 (23):179-202.

- Kangal, Z. T. (2011). “Ceza Hukukunda Varsayılan Rıza”. *Gazi Üniversitesi Hukuk Fakültesi Dergisi*, 15 (4): 223-251.
- Kapani, M. (2007). *Politika Bilimine Giriş*. Bilgi Yayınevi, Ankara.
- Kaplan, M. (2015). “Türk Ceza Hukukunda Kamu Görevlisi Kavramı”. *Akdeniz Üniversitesi Hukuk Fakültesi Dergisi*, 5 (2): 49-77.
- Karagülmez, A. (2005). *Bilişim Suçları ve Soruşturma – Kovuşturma Evreleri*. Seçkin Yayınevi, Ankara.
- Karakehya, H. (2006). “Olası Kast”. *Ceza Hukuku Dergisi*, 2:19-46.
- Katoğlu, T. (2003). *Ceza Hukukunda Hukuka Aykırılık*. Seçkin Yayınevi, Ankara.
- Kaya M. (2010). “Telekomünikasyon Alanında Kişilik Haklarının Korunması”, *Ankara Barosu Dergisi*, 68 (4) :279-334.
- Kaya, C. (2011). “Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi”. *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, LXIX(1 -2): 317-334.
- Ketizmen, M, (2008), *Türk Ceza Hukukunda Bilişim Suçları*. Adalet Yayınevi, Ankara.
- Ketizmen, M. Ve Ülküderner Ç. (2007). “E-Devlet Uygulamalarında Kişisel Verilerin Korun(ma)ması”. *XII. “Türkiye’de İnternet” Konferansı*, 8-10 Kasım 2007, Ankara, 189-193.
- Kılınç, D. (2012). “Anayasal Bir Hak Olarak Kişisel Verilerin Korunması”. *AÜHFD Dergisi*, 61(3), 1089-1169.
- Koca, M, Üzülmüş, İ. (2017). *Türk Ceza Hukuku Genel Hükümler*. Seçkin Yayınevi, Ankara.
- Korff, D. (1998). *Study On The Protection Of The Rights And Interests Of Legal Persons With Regard To The Processing Of Personal Data Relating To Such Persons (Final Report)*. Commission of the European Communities, Cambridge.
- Korff, D. (2002). *EC Study on Implementation of Data Protection Directive, Comparative Summary of National Laws*. Human Rights Center University of Essex, Cambridge.
- Korkmaz, İ. (2016). “Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme”. *Türkiye Barolar Birliği Dergisi*, 124: 81-152.
- Küzeci, E. (2010). *Kişisel Verilerin Korunması*. Turhan Kitabevi Yayınları, Ankara.
- Küzeci, E. (2014) “İstatistikî Birimler ve Bilgilerin Geleceğini Belirleme Hakkı”. *İnsan Hakları Yıllığı*, 32: 53-75.
- Lloyd, I. (2014). *Information Technology Law*. Oxford University Press, Oxford.
- Mahiroğulları, A. (2003). “Türkiye’de Sendika-Siyasi Parti İlişkileri”. *Sosyal Siyaset Konferansları Dergisi*, Sayı:46, 43-88.

- Mäkinen, J. (2015) “Data Quality, Sensitive Data And Joint Controllershship As Examples Of Grey Areas in The Existing Data Protection Framework For The Internet Of Things” *Information & Communications Technology Law*, 24:3, 262-277.
- Manav, A. E. (2015). “İş İlişkisinde İşçinin Kişisel Verilerinin Korunması”. *Gazi Üniversitesi Hukuk Fakültesi Dergisi*, XIX (2):95-136.
- Mendos Kuşkonmaz E. (2013). *Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması*. Yayımlanmamış Yüksek Lisans Tezi. İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.
- Önder, A. (1992). *Ceza Hukuku Genel Hükümler, Cilt:II-III*. Beta Yayınevi, İstanbul.
- Özbek, V. Ö., Doğan, K., Bacaksız, P., Tepe, İ. (2016). *Türk Ceza Hukuku Özel Hükümler*. Seçkin Yayınevi, Ankara.
- Özbek, V. Ö., Doğan, K., Bacaksız, P., Tepe, İ. (2017). *Türk Ceza Hukuku Genel Hükümler*. Seçkin Yayınevi, Ankara.
- Özdemir, H. (2009). *Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması*. Seçkin Yayınları, Ankara.
- Özen, M. ve Tozman, Ö. (2009). “Türk Ceza Hukukunda Kamu Görevlisi Kavramı”. *Amme İdaresi Dergisi*, 42 (4): 25-57.
- Özen, M. (2009). “Kişisel Verilerin Kaydedilmesi, Verilmesi veya Ele Geçirilmesi ve Yok Edilmemesi Suçları (TCK m. 136, 137, 138)”. *Kamu Hukuku Arşivi*, 12(1):13-28.
- Özgenç İ. (2016). *Türk Ceza Hukuk Genel Hükümler*. Seçkin Yayınevi, Ankara.
- Peretti, K. K. (2008). “Data Breaches: What the Underground World of Carding Reveals”. *Santa Clara Computer & High Tech. L.J.* 25: 375-413.
- Room, S. (2007). *Data Protecion & Compliance in Context*. The British Computer Society Publishing and Informatio Product, Swindon, Birleşik Krallık.
- Roos, A. (2006). “Core Principles Of Data Protection Law”. *The Comparative and International Law Journal of Southern Africa*, 39 (1) : 102-130
- Samuelson, P. (2000). “Privacy As Intellectual Property?”, *Stanford Law Review*, 52 (5): 1128-1129
- Savaş, B. (2009). “İş Hukukunda Siber Gözetim”. *Çalışma ve Toplum Ekonomi ve Hukuk Dergisi*, 3 (22):97-132.
- Schwartz, P. M. ve Janger, E. J. (2007). “Notification of Data Security Breaches”. *Michigan Law Review*, 105 (5): 913-984.
- Simonius, A. (Çev. Arık, F.). (1955). “Şahsiyet Hakları”. *AÜSBF Dergisi*, 1:186-198.
- Soyaslan, D. (2016). *Ceza Hukuku Özel Hükümler*. Yetkin Yayınları, Ankara.

- Stute, D. J. (2015). "Privacy Almighty? The CJEU's Judgment in Google Spain SL v. AEPD". *Michigan Journal of International Law*, 36(4):649-680.
- Şen, E. (2011). "Kişisel Verileri Koruma Kanunu Tasarısı'nın Anayasa ve Türk Ceza Kanunu Hükümleri Çerçevesinde Değerlendirilmesi". *Yorumluyorum*, Seçkin Yayıncılık, Ankara.
- Şık E. (2012). *İşverenin Özlük Dosyası Düzenleme Borcu*. Yayımlanmamış Yüksek Lisans Tezi. Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü, İzmir.
- Şimşek, O. (2008). *Anayasa Hukukunda Kişisel Verilerin Korunması*. Beta Yayınevi, İstanbul.
- Tan, T. (2002) "Bağımsız İdari Otoriteler veya Düzenleyici Kurullar". *Amme İdaresi Dergisi*, 35 (2):11-37.
- Taşkın, Ş. C. (2008). *Bilişim Suçları*. Beta Yayınevi, Bursa.
- Tezcan, D. (1991). "Bilgisayar Karşısında Özel Hayatın Korunması", Anayasa Yargısı 8, Anayasa Mahkemesinin 29.Kuruluş Yıldönümü Sempozyumu, 25 – 27 Nisan 1991, Ankara, s. 385-392.
- Tezcan, D., Erdem, M. H., Önok, M. (2017). *Teorik ve Pratik Ceza Özel Hukuku*. Seçkin Yayınevi, Ankara.
- Toğuz, Ö. (2014). *Avrupa Birliği ve Türkiye’de Fikri Mülkiyet ve Veri Koruması*. Legal Yayıncılık, İstanbul.
- Amerika Nüfus Bürosu. (2002). *Measuring America: The Decennial Censuses from 1790 to 2000*. U.S Census Bureau, ABD.
- Uncular, S. (2014). *İş İlişkisinde İşçinin Kişisel Verilerinin Korunması*. Seçkin Yayınevi, Ankara.
- United Nations. (2016). *Data Protection Regulations And International Data Flows: Implications For Trade And Development*. United Nations, İsviçre.
- Uygun, M. (2010). *Avrupa Birliğinin 95/46 Sayılı Veri Koruma Yönergesi Işığında Kişisel Verilerin Korunması*. Yayımlanmamış Yüksek Lisans Tezi. Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.
- Ünver, Y. (2008). "Kişisel Verilerin Korunması". *Galatasaray Üniversitesi Hukuk Fakültesi Dergisi*, 2008(1):163-196.
- Waele H. D. (2014). "Veri Koruma Direktifi'nin Tüzük İle Değiştirilmesinin Sonuçları". (Çev. N. Tekin). *Küresel Bakış Çeviri Hukuk Dergisi*, 4(13):75-79.

- Warren S. D. ve Brandeis L. D. (2007). “Mahremiyet Hakkı”. (Çev. G. Arslan) K, İçel ve Y. Ünver (Ed.). *Özel Yaşam, Medya ve Ceza Hukuku*. Seçkin Yayınevi, Ankara, s. 19-42.
- Wong, R. (2013). *Data Security Breaches and Privacy in Europe*. Springer-Verlag, Londra.
- Yaşar O., Gökcan H.T., Artuç M. (2014). *Yorumlu-Uygulamalı Türk Ceza Kanunu, 3. Cilt*. Adalet Yayınevi, Ankara.
- Yeniocak, U. (2013). “Borçlar Kanunu Hükümlerine Göre Genel İşlem Koşullarının Yargısal Denetimi”. *Türkiye Barolar Birliği Dergisi*, 107: 75-96.
- Yenisey, F. ve Plagemann G. (2015) *Alman Ceza Kanunu Strafgesetzbuch (Açıklamalar, Almanca Metin, Türkçe Çeviri ve Sözlük)*, Beta Yayınevi, İstanbul.
- Yılmaz, S. S. (2014). *Tıp Alanında Kişisel Verilerin Açıklanması Suçu*. Seçkim Yayınevi, Ankara.
- Yokuş Sevik, H. (2008). “Tıp Ceza Hukukunda Kişisel Verilerin Açıklanması”. V.Türk – Alman Tıp Hukuku Sempozyumu, Tıp Ceza Hukukunun Güncel Sorunları, 28 Şubat – 1 Mart 2008, Ankara, 782-811.
- Yurtsever, M. (2015). *Özel Hayatın Gizliliğini İhlal Suçu*. Yayımlanmamış Yüksek Lisans Tezi, Bahçeşehir Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.
- Yüksel Civelek, D. (2011). *Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi*. Bilgi Toplumu Dairesi Başkanlığı, Ankara.

İnternet Kaynakları

- <https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded> (erişim tarihi:16.01.2018)
- <http://www.bbc.com/news/av/world-asia-china-42248056/in-your-face-china-s-all-seeing-state> (erişim tarihi:16.01.2018)
- <https://www.hrw.org/news/2017/12/13/china-minority-region-collects-dna-millions> (erişim tarihi:16.01.2018)
- http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx (erişim tarihi:16.01.2018).
- http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf (erişim tarihi: 09.11.2017).
- Madde 29 Çalışma Grubu’nun 4/2007 sayılı görüşü, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf (erişim tarihi:09.11.2017).

- Avrupa Birliği'nin 2016/679 sayılı Genel Veri Koruma Tüzüğü, http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf (erişim tarihi: 06.11.2017)
- Madde 29 Çalışma Grubu'nun 3/2005 sayılı, biyometrik verilerin Birlik üyesi devletler tarafından düzenlenen pasaport ve vizelerde kullanılmasına ilişkin görüşü, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp112_en.pdf (erişim tarihi:15.11.2017)
- https://www.legislation.gov.uk/ukpga/1998/29/pdfs/ukpga_19980029_en.pdf (erişim tarihi: 02.01.2018)
- https://www.legifrance.gouv.fr/affichCode.do;jsessionid=41ED3CB20161448EBD6835FDAE939576.tplgfr25s_1?idSectionTA=LEGISCTA000006165313&cidTexte=LEGITEXT000006070719&dateTexte=20180102 (erişim tarihi:02.01.2018)
- OECD, <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprivacyandtransborderflowsofpersonaldata.htm>. (erişim tarihi: 09.04.2017)
- OECD, http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (erişim tarihi:16.01.2018).
- United Nations, <http://hrlibrary.umn.edu/instate/q2grcpd.htm> (erişim tarihi: 23.04.2017)
- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, <http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37>. (erişim tarihi:23.04.2017).
- http://www.uhdigm.adalet.gov.tr/sozlesmeler/coktarafilsoz/ak/turkce/108_tur.pdf. (erişim tarihi:23.04.2017)
- Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine*, <http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168007cf98> (erişim tarihi: 23.04.2017)
- Convention on Cybercrime*, <http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561> (erişim tarihi: 23.04.2017)
- Leander/İsveç*, Başvuru no:9248/81, 26.03.1987, [https://hudoc.echr.coe.int/tur#{"fulltext":\["leander"\],"documentcollectionid2":\["GRANDCHAMBER"\],"CHAMBER":\["CHAMBER"\],"itemid":\["001-57519"\]}](https://hudoc.echr.coe.int/tur#{) (erişim tarihi:15.01.2018)
- Klass ve diğerleri/Almanya*, başvuru no: 5029/71, 6.9.1978 - [https://hudoc.echr.coe.int/tur#{"fulltext":\["klass"\],"documentcollectionid2":\["GRANDCHAMBER"\],"CHAMBER":\["CHAMBER"\],"itemid":\["001-57510"\]}](https://hudoc.echr.coe.int/tur#{) (erişim tarihi:15.01.2018)

- Amann/İsviçre*, Başvuru no: 27798/95, 16.2.2000 -
[http://hudoc.echr.coe.int/tur#{\"fulltext\":\[\"amann\"\],\"documentcollectionid2\":\[\"GRANDCHAMBER\",\"CHAMBER\"\],\"itemid\":\[\"001-58497\"\]}](http://hudoc.echr.coe.int/tur#{\) (erişim tarihi:07.05.2017)
- S. *Ve Marper/Birleşik Krallık*, başvuru no:30562/04, 4.12.2008 -
[https://hudoc.echr.coe.int/tur#{\"fulltext\":\[\"marper\"\],\"documentcollectionid2\":\[\"GRANDCHAMBER\",\"CHAMBER\"\],\"itemid\":\[\"001-90051\"\]}](https://hudoc.echr.coe.int/tur#{\) (erişim tarihi: 15.01.2018)
- Gaskin/ Birleşik Krallık, başvuru no: 10454/83, 7.7.1989 -
[http://hudoc.echr.coe.int/tur#{\"fulltext\":\[\"gaskin\"\],\"documentcollectionid2\":\[\"GRANDCHAMBER\",\"CHAMBER\"\],\"itemid\":\[\"001-57491\"\]}](http://hudoc.echr.coe.int/tur#{\) (erişim tarihi: 07.05.2017)
- 108 sayılı Sözleşmenin 15.01.2018 tarihi itibariyle güncel imza ve onay durumu,
https://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/treaty/108/signatures?p_auth=cOAvxJNk (erişim tarihi:15.01.2018)
- Avrupa Konseyi, Bilimsel Araştırma ve İstatistiki Amaçlar İçin Kişisel Verilerin Korunmasına İlişkin Tavsiye (<https://rm.coe.int/16804bc647>, erişim tarihi: 28.05.2017)
- Avrupa Konseyi, Doğrudan Reklam Amacıyla Kullanım Sırasında Kişisel Verilerin Korunması Hakkında Tavsiye (<https://rm.coe.int/16804bd336>, erişim tarihi: 28.05.2017)
- Avrupa Konseyi, Sosyal Güvenlik Amacıyla Kullanım Sırasında Kişisel Verilerin Korunması Hakkında Tavsiye (<https://rm.coe.int/16804dd352>, erişim tarihi: 28.05.2017)
- Avrupa Konseyi, Polisiye Faaliyetler Alanında Kişisel Verilerin Korunması Hakkında Tavsiye (<https://rm.coe.int/16804e7a3c>, erişim tarihi: 28.05.2017)
- Avrupa Konseyi, İş İlişkisi Amacıyla Kullanılan Kişisel Verilerin Korunması Hakkında Tavsiye (<https://rm.coe.int/1680500b15>, erişim tarihi:28.05.2017)
- Avrupa Konseyi, Ödeme İlişkisi ve Bununla Bağlantılı İşlemler İçin Kullanılan Kişisel Verilerin Korunmasına İlişkin Tavsiye (<https://rm.coe.int/16804e15cd>, erişim tarihi: 28.05.2017)
- Avrupa Konseyi, Tıbbi Verilerin Korunması Hakkında Tavsiye (<https://rm.coe.int/16804f0ed0> , erişim tarihi: 28.05.2017),
- Avrupa Konseyi, İstatistiki Amaçlar İçin Toplanan Kişisel Verilerin Korunması Hakkında Tavsiye (<https://rm.coe.int/1680508d7e>, erişim tarihi:28.05.2017)
- Avrupa Konseyi, Sigorta Amacıyla Toplanan ve İşlenen Kişisel Verilerin İşlenmesi Hakkında Tavsiye (<https://rm.coe.int/16804d9ddd> , erişim tarihi: 28.05.2017).

Avrupa Konseyi üyesi ülkelerin 108 sayılı sözleşmeyi imzaladıkları ve yürürlüğe koydukları tarihler, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=MIAxQjzm (erişim tarihi:30.11.2017)

Avrupa Birliği Bakanlığı, <http://www.ab.gov.tr/105.html> , (erişim tarihi:04.06.2017).

Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector (<http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1496587871952&uri=CELEX:31997L0066> , erişim tarihi:04.06.2017)

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (<http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1496588313140&uri=CELEX:32002L0058> , erişim tarihi:04.06.2017)

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (<http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1496574544000&uri=CELEX:31995L0046> (erişim tarihi: 04.06.2017).

ABAD, <http://curia.europa.eu/juris/document/document.jsf?docid=48382&doclang=en> (erişim tarihi:21.01.2018).

http://ec.europa.eu/justice/dataprotection/document/review2012/com_2012_11_en.pdf (erişim tarihi:23.11.2017).

Avrupa Birliği'nin İşleyişi Hakkında Antlaşma, <https://www.ab.gov.tr/files/pub/antlasmalar.pdf> (erişim tarihi:25.11.2017)

EU Press Release: Data Protection Reform – Frequently Asked Questions, 4.11.2010 - http://europa.eu/rapid/press-release_MEMO-10-542_en.htm?locale=EN (erişim tarihi:26.11.2017)

ABAD,<http://curia.europa.eu/juris/document/document.jsf?jsessionid=9ea7d0f130d5a87cc50a1c8b478399a7d411c2280f12.e34KaxiLc3eQc40LaxqMbN4PaNiPe0?text=&docid=152065&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=99126> (erişim tarihi:27.11.2017)

<http://www.anayasa.gov.tr/icsayfalar/basin/kararlarailiskinbasinduyurulari/bireyselbasvuru/de-tay/pdf/2013-5653.pdf> (erişim tarihi:27.11.2017)

APEC, <https://www.apec.org/About-Us/About-APEC/History> (erişim tarihi: 19.03.2018)

APEC, <https://www.apec.org/Publications/2005/12/APEC-Privacy-Framework> (erişim tarihi: 19.03.2018)

ABAD, <http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=2294770> (erişim tarihi: 18.11.2017)

Avrupa Komisyonu, <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016D1250&from=EN> (erişim tarihi: 11.01.2018)

Federal (Alman) Veri Koruma Kanunu, <http://www.legislationline.org/topics/country/28/topic/3> (erişim tarihi: 24.01.2018)

İngiltere Veri Koruma Kanunu, https://www.legislation.gov.uk/ukpga/1998/29/pdfs/ukpga_19980029_en.pdf (erişim tarihi: 25.01.2018)

İngiltere Kişisel Verilerin Korunması Kanunu Taslağı, <https://publications.parliament.uk/pa/bills/cbill/2017-2019/0153/18153.pdf> (erişim tarihi: 27.01.2018)

İngiltere Parlamentosu, <https://services.parliament.uk/bills/2017-19/dataprotection.html> (erişim tarihi: 27.01.2018)

Avrupa Komisyonu'nun 09.11.2016 tarihli, SWD(2016) 366 nihai sayılı AB Genişleme Politikasına İlişkin 2016 Türkiye Raporu, https://www.ab.gov.tr/files/pub/2016_ilerleme_raporu_tr.pdf, (erişim tarihi: 17.01.2018)

Veri Sorumluları Sicili Hakkında Yönetmelik, <http://www.resmigazete.gov.tr/main.aspx?home=http://www.resmigazete.gov.tr/eskiler/2017/12/20171230.htm&main=http://www.resmigazete.gov.tr/eskiler/2017/12/20171230.htm> (erişim tarihi: 17.01.2018)

Handbook on European Data Protection Law, 73 https://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf (erişim tarihi: 24.01.2018)

Peck/Birleşik Krallık, B.No: 44647/98, 28.01.2003, [https://hudoc.echr.coe.int/tur#{\"fulltext\":\[\"CASEOFPECKv.THEUNITEDKINGDOM\"\],\"documentcollectionid2\":\[\"GRANDCHAMBER\",\"CHAMBER\"\],\"itemid\":\[\"001-60898\"\]}](https://hudoc.echr.coe.int/tur#{\) (erişim tarihi: 24.01.2018)

- 50 milyon Türk vatandaşının kimlik verilerinin sızdırılmasına ve ifşa edilmesine ilişkin haber, “Turkish authorities ‘probing huge ID data leak’”, <http://www.bbc.com/news/technology-35978216> (erişim tarihi: 17.12.2017)
- Yahoo’nun şirketi nezdindeki 1 milyardan fazla kullanıcı hesabında veri sızıntısı meydana geldiğini duyurduğuna ilişkin haber, “Parolalarınızı değiştirin, tarihin en büyük veri sızıntısı”, <http://www.mynet.com/haber/teknoloji/parolalarinizi-degistirin-tarihin-en-buyuk-veri-sizintisi-2787884-1> (erişim tarihi:20.03.2018).
- “Yahoo, ‘mail’ skandalını doğruladı”, <http://www.trthaber.com/haber/bilim-teknoloji/yahoo-mail-skandalini-dogruladi-301852.html> (erişim tarihi: 20.03.2018).
- E-posta servislerinden biri olan Gmail’in kullanıcılarına ait yaklaşık 5 milyon şifrenin yayınlanmasına ilişkin haber, “5 milyon Gmail şifresi internete düştü”, <http://www.hurriyet.com.tr/5-milyon-gmail-sifresi-internete-dustu-27181091> (erişim tarihi:20.03.2018)
- Madde 29 Çalışma Grubu, 2011:7, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf (erişim tarihi:17.12.2017)
- Avrupa Komisyonu'nun 09.11.2016 tarihli, SWD(2016) 366 nihai sayılı AB Genişleme Politikasına İlişkin 2016 Türkiye Raporu, s. 71. - https://www.ab.gov.tr/files/pub/2016_ilerleme_raporu_tr.pdf, (erişim tarihi:19.11.2017)
- Europol, <https://www.europol.europa.eu/about-europol> (erişim tarihi:19.11.2017).
- Eurojust, <http://www.eurojust.europa.eu/about/background/Pages/History.aspx> (erişim tarihi:19.11.2017)
- http://www.tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.5a52a1da2b7375.28490721 (erişim tarihi:07.01.2018).
- http://www.tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.5a52a1df446320.54135011 (erişim tarihi:07.01.2018)
- Avrupa Komisyonu, http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm (erişim tarihi:11.01.2018)
- http://www.tdk.gov.tr/index.php?option=com_atasozleri&arama=kelime&guid=TDK.GTS.5a5535fb983336.45403033 (erişim tarihi: 07. 01 2018)
- http://www.tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.5b1a3ad4a0bf70.77987302 (erişim tarihi:08.06.2018)

Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik, <http://www.resmigazete.gov.tr/main.aspx?home=http://www.resmigazete.gov.tr/eskiler/2017/10/20171028.htm&main=http://www.resmigazete.gov.tr/eskiler/2017/10/20171028.htm> (erişim tarihi:10.01.2018)

Anayasa Mahkemesi, <http://www.kararlaryeni.anayasa.gov.tr/Karar/Content/9f7b3df0-e060-4c61-9dc8-f9e43a52adf4?excludeGerekce=False&wordsOnly=False> (erişim tarihi:20.09.2017)

http://www.tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.59c409241ecae3.89976873 / (erişim tarihi:21.09.2017)

https://www.gesetze-im-internet.de/englisch_bdsge/englisch_bdsge.pdf (erişim tarihi:08.06.2018)

ABAD, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62010CJ0070:EN:HTML>, (erişim tarihi:22.10.2017).)

Kişisel Verileri Koruma Kurumu, 6698 Sayılı Kişisel Verilerin Korunmasına Yönelik Soru ve Cevaplar, <http://www.kvkk.gov.tr/yayinlar/6698%20SAYILI%20K%C4%B0%C5%9E%C4%B0SEL%20VER%C4%B0LER%C4%B0N%20KORUNMASI%20KANUNUNUN%20UYGULANMASINA%20Y%C3%96NEL%C4%B0K%20SORU%20VE%20CEVAPLAR.pdf> (erişim tarihi:05.11.2017)

Article 29 Data Protection Working Party, Advice Paper On Special Categories of Data ("sensitive data"), Ref. Ares(2011)444105 - 20/04/2011, s. 10. http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf (erişim tarihi:30.12.2017)

Campbell ve Cosans/İngiltere kararı, başvuru no: 7511/76; 7743/76; 25.02.1982 (parg.:36; [https://hudoc.echr.coe.int/eng#{\"itemid\":\[\"001-57455\"\]}](https://hudoc.echr.coe.int/eng#{\)) (erişim tarihi:30.12.2017).

http://tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.5a4775ae9a7ff0.20230552 (erişim tarihi:30.12.2017).

http://tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.5a482e93401a29.08983880 (erişim tarihi:31.12.2017)

Nachova ve Diğerleri/Bulgaristan, Başvuru no: 43577/98 ve 43579/98, 6.7.2005, [https://hudoc.echr.coe.int/eng#{\"tabview\":\[\"document\"\],\"itemid\":\[\"001-69630\"\]}](https://hudoc.echr.coe.int/eng#{\) (erişim tarihi:31.12.2017)

- Timishev/Rusya*, Başvuru no: 55762/00 ve 55974/00, 13.12.2005,
[https://hudoc.echr.coe.int/eng#{\"tabview\":\[\"document\"\],\"itemid\":\[\"001-71627\"\]},](https://hudoc.echr.coe.int/eng#{\)
 (erişim tarihi:31.12.2017)
- Adalet Bakanlığı Uluslararası Hukuk ve Dış İlişkiler Genel Müdürlüğü İnsan Hakları Daire Başkanlığı, 2013:5-6,
http://www.echr.coe.int/Documents/FS_Racial_discrimination_TUR.pdf (erişim tarihi:31.12.2017).
- Turan Çakır/Belçika*, başvuru no: 44256/06,10.3.2009,
[https://hudoc.echr.coe.int/eng#{\"itemid\":\[\"001-111151\"\]},](https://hudoc.echr.coe.int/eng#{\) (erişim tarihi:31.12.2017)
- Somersan, S. (2012). “İrkların Olmadığı Bir Dünyada Irkçılık”, *Ayrımcılık: Çok Boyutlu Yaklaşımlar*. Bilgi Üniversitesi Yayınları, İstanbul, s. 1-13,
<http://secbir.org/images/haber/2011/01/17-semra-somersan.pdf> (erişim tarihi:31.12.2017)
- http://tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.5ae303f5f30fe6.85073425 (erişim tarihi: 31.12.2017)
- Dünya Sağlık Örgütü, 2006: 5,
http://www.who.int/reproductivehealth/publications/sexual_health/defining_sexual_health.pdf?ua=1 (erişim tarihi:24.12.2017)
- Bozdemir N, Özcan S. (2011). “Cinsellik Ve Cinsel Sağlığa Genel Bakış”. *Turkish Journal Of Family Medicine And Primary Care*; 5 (4): 37-46,
<http://dergipark.ulakbim.gov.tr/tjfmpe/article/viewFile/5000055970/5000053179>
 (erişim tarihi:25.12.2017)
- Şah, U. (2012). “Eşcinselliğe, Biseksüelliğe ve Transeksüelliğe İlişkin Tanımlamaların Homofobi ve LGBT Bireylerle Tanışıklık Düzeyi İle İlişkisi”. *Psikoloji Çalışmaları Dergisi*, 32(2): 23-48,
http://193.255.56.45:8080/xmlui/bitstream/handle/123456789/272/Sah%2c%20Umut_2012.pdf?sequence=1&isAllowed=y (erişim tarihi:25.12.2017).
- Mahiroğulları, A. (2004). “Teorik Çerçevesi ve Dünyadaki Uygulamalarıyla Sendika-Siyaset, Sendika- Siyasal Parti İlişkisi”. *T.C. Marmara Üniversitesi İ.I.B.F. Dergisi*, XIX (I): 349-371.
<http://dspace.marmara.edu.tr/bitstream/handle/11424/1817/5000007359-5000012160-1-SM.pdf?sequence=1>. (erişim tarihi:24.12.2017)
- X/Türkiye*, Başvuru no:24626/09, 9.10.2012, [https://hudoc.echr.coe.int/eng#{\"itemid\":\[\"001-120280\"\]},](https://hudoc.echr.coe.int/eng#{\) (erişim tarihi:30.12.2017)

Avrupa Birliđi, http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf
(eriřim tarihi:06.11.2017)

http://www.tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.5a5a24cbdc431.80488433 (eriřim tairihi:13.01.2018)

http://www.tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.5a5a29bb765825.34228638 (eriřim tarihi:13.01.2018)

https://www.tbmm.gov.tr/develop/owa/komisyon_tutanaklari.mv_goruntule?pTutanakId=6269 , (eriřim tarihi: 23.12.2017)



Ö Z G E Ç M İ Ş

Adı ve SOYADI	Melike KÖSE AYSUN
Doğum Yeri - Tarihi	Baykan – 31.03.1990
EĞİTİM DURUMU	
Mezun Olduğu Lise	Antalya Anadolu Lisesi
Lisans Diploması	Ankara Üniversitesi Hukuk Fakültesi
Yabancı Dil / Diller	İngilizce
İŞ DENEYİMİ	
Stajlar	Antalya Barosu Avukatlık Stajı
Çalıştığı Kurumlar	Serbest Avukat
E-Posta	av.melikekose@gmail.com