



T.C.

ANKARA YILDIRIM BEYAZIT ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

CEZA HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASI

YÜKSEK LİSANS TEZİ

Yasir Emre GÜRSU

KAMU HUKUKU ANA BİLİM DALI

ANKARA, 2023

T.C.
ANKARA YILDIRIM BEYAZIT ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

CEZA HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASI

YÜKSEK LİSANS TEZİ

Yasir Emre GÜRSU

KAMU HUKUKU ANA BİLİM DALI

Dr. Öğr. Üyesi Ömer ÇELEN

ANKARA, 2023

ONAY SAYFASI

Yasir Emre Gürsu tarafından hazırlanan “CEZA HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASI” adlı tez çalışması aşağıdaki jüri tarafından oy birliği ile Ankara Yıldırım Beyazıt Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı’nda Yüksek Lisans tezi olarak kabul edilmiştir.

Jüri Üyesi	Kurumu	İmza
Dr. Öğr. Üyesi Ömer ÇELEN	Ankara Yıldırım Beyazıt Üniversitesi	
Kabul ☐ Red ☐		
Doç. Dr. Ahmet KILINÇ	Ankara Yıldırım Beyazıt Üniversitesi	
Kabul ☐ Red ☐		
Dr. Öğr. Üyesi Gülen SOYASLAN	Çankırı Karatekin Üniversitesi	
Kabul ☐ Red ☐		

Tez Savunma Tarihi: 8.05.2023

Ankara Yıldırım Beyazıt Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı’nda Yüksek Lisans tezi olması için şartları yerine getirdiğini onaylıyorum.

Sosyal Bilimler Enstitüsü Müdürü

Ünvan Ad Soyad

.....

BEYAN

Bu tez çalışmasının kendi çalışmam olduğunu, tezin planlanmasından yazımına kadar bütün aşamalarda patent ve telif haklarını ihlal edici etik dışı davranışımın olmadığını, bu tezdeki bütün bilgileri akademik ve etik kurallar içinde elde ettiğimi, bu tezde kullanılmış olan tüm bilgi ve yorumlara kaynak gösterdiğimi beyan ederim.
(4.07.2023)

Yasir Emre GÜRSU



TEŞEKKÜR

Olağanüstü yoğunluğuna rağmen fedakârlık göstererek bana vakit ayıran danışman hocam Dr. Öğr. Üyesi Ömer ÇELEN'e, jüride yer alan, kıymetli tavsiyeleri ile tezimin olgunlaşmasına ve son halini almasına katkı sunan Doç. Dr. Ahmet KILINÇ ve Dr. Öğr. Üyesi Gülen SOYASLAN hocalarıma içtenlikle teşekkürlerimi sunarım.

Tez sürecindeki destek ve dayanışmaları için Karatekin Üniversitesi Hukuk Fakültesi'ndeki kürsü arkadaşlarıma ve çalışma arkadaşlarıma ayrıca teşekkürü borç bilirim.

Son olarak yetişmemde ve bugünlere gelmemde büyük emeği olan, haklarını hiçbir zaman ödeyemeyeceğim kıymetli anne ve babama, bana her koşulda desteğini, sevgisini ve güvenini hissettiren, çalışmalarım boyunca fedakarlıkta bulunan ve beni motive eden kıymetli eşime teşekkür ederim.

Yasir Emre GÜRSU

ÖZET

Ceza Hukukunda Kişisel Verilerin Korunması

Kişisel verilerin korunması konusu anayasa hukukunu, idare hukukunu, medeni hukuku ve ceza hukukunu yakından ilgilendirmektedir. Bu çalışmanın konusu kişisel verilerin ceza hukuku kapsamında korunmasıyla sınırlıdır. Bu çalışmanın temel amacı 5237 sayılı Türk Ceza Kanunu'nda (TCK) yer alan ve kişisel verileri koruma maksadı taşıyan suç tiplerini incelemek ve bu konuda öğretiyeye katkı sunmaktır.

TCK'da yer alan suç tipleri hakkında kapsamlı bir değerlendirme yapabilmek için birinci bölümde öncelikle konuya özgü kavramsal çerçeve ele alınmış, kişisel verilerin korunması öğretisi ışığında kişisel verilerin korunması hakkının kapsamı ve hukuki niteliği açıklanmış ardından Türk Hukukundaki düzenlemelere kaynaklık teşkil eden uluslararası düzenlemeler ile diğer ülkelerin ulusal kanunlarında ve Türk Hukukunda yer alan normların tarihsel süreç içerisindeki gelişimine değinilmiştir.

Kişisel verilerin korunmasına ilişkin usul ve esasların düzenlendiği 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK), bahsi geçen suç tiplerinin uygulanmasında temel başvuru noktalarından biri olması sebebiyle ikinci bölümde özellikle ceza hukukunu ilgilendiren boyutlarıyla ele alınmıştır.

Çalışmanın üçüncü bölümünde ise TCK'da yer alan ilgili suç tipleri incelenmiştir. KVKK'nın yürürlüğe girmesinden sonra bu suç tiplerinin belirlilik ve kanunilik ilkelerine aykırı olduğu yönündeki eleştirilerin son bulduğu ancak bu suç tiplerinin fiil unsurlarına ilişkin yeni tartışmaların doğduğu tespit edilmiştir.

Verileri yok etmeme (TCK m.138) suçunun fiil unsurunun anonim hale getirmeme ve silmeme durumlarını da kapsayıp kapsamadığı konusundaki tartışmalar kanaatimizce kanuni düzenlemelerden kaynaklanmaktadır. Bu tartışmayı gidermek için verileri yok etmeme suçunu düzenleyen TCK m.138'e verileri silmeme ve anonim hale getirmeme fiilleri seçimlik hareket olarak eklenmelidir.

Öğretide aksi görüş bulunsa da kanaatimizce kişisel verileri kaydetme (TCK m.135) ile kişisel verileri verme, yayma veya ele geçirme (TCK m.136) suçlarının fiil unsurlarının gerçekleşmesi için KVKK kapsamında bir veri işleme fiilinin bulunması zorunlu değildir. Fiilin KVKK kapsamına girip girmediği ancak hukuka uygunluk sebepleri değerlendirilirken göz önünde bulundurulmalıdır.

Anahtar kelimeler: Kişisel Veri, Kişisel Verilere İlişkin Suçlar, Kişisel Verilerin Korunması Hakkı, Türk Ceza Kanunu.



ABSTRACT

Protection of Personal Data in Criminal Law

The protection of personal data is closely related to constitutional law, administrative law, civil law and criminal law. The subject of this study is limited to the protection of personal data under criminal law. The main purpose of this study is to examine the types of crimes in the Turkish Penal Code No. 5237 (TPC) that are intended to protect personal data and to contribute to the doctrine on this subject.

In order to make a comprehensive evaluation of the types of crimes under the TPC, the first part primarily discusses the conceptual framework related to the subject, explains the scope and legal nature of the right to protection of personal data in the light of the doctrine of protection of personal data, and then discusses the international regulations that constitute the source of the regulations in Turkish Law and the development of the norms in the national laws of other countries and Turkish Law in the historical process.

The Law No. 6698 on the Protection of Personal Data (LPPD), which regulates the procedures and principles regarding the protection of personal data, is discussed in the second part, especially in terms of criminal law, as it is one of the main reference points in the implementation of the aforementioned crime types.

In the third part of the study, the relevant types of crimes in the Turkish Penal Code are analyzed. It has been determined that after the enactment of the LPPD, the criticisms that these crime types are contrary to the principles of certainty and legality have come to an end, but new discussions have emerged regarding the conduct elements of these crime types.

In our opinion, the discussions on whether the conduct element of the offense of not destructing data (Article 138 of the TPC) also includes the cases of not anonymizing and not deleting data stem from the legal regulations. In order to resolve this debate, the acts of not deleting and not anonymizing data should be added as optional acts to Article 138 of the TPC, which regulates the crime of not destructing data.

Although opposite views exist in the doctrine, we believe that, it is not necessary to have a data processing act in terms of the LPPD to conclude that the conduct elements of the offences of recording personal data (Article 135 of the TPC) and giving, disseminating or obtaining personal data (Article 136 of the TPC) have been realised. Whether there is an act in terms of the LPPD is an issue that must be taken into consideration only during the evaluation of justification defenses.

Keywords: Crimes Related to Personal Data, Personal Data, Right to Protection of Personal Data, Turkish Penal Code.



İÇİNDEKİLER

ÖZET	i
ABSTRACT	iii
İÇİNDEKİLER	v
KISALTMALAR	xiii
GİRİŞ	1

BİRİNCİ BÖLÜM

KİŞİSEL VERİ KAVRAMI, KİŞİSEL VERİLERİN KORUNMASI HAKKI ve HAKKIN KORUNMASINA MAHSUS HUKUKİ DÜZENLEMELERİN GELİŞİMİ

1. KİŞİSEL VERİ KAVRAMI	7
1.1. Genel Olarak Kişisel Veri Kavramı	7
1.2. Kişisel Verinin Unsurları	9
1.2.1. Veri Unsuru	9
1.2.2. Kişi Unsuru	10
1.2.3. Verinin Kişiyeye İlişkin Olması	17
1.3. Özel Nitelikli Kişisel Veri Kavramı	18
2. KİŞİSEL VERİLERİN KORUNMASI HAKKI	20
2.1. Tarihsel Süreç İçerisinde Gelişimi	21
2.2. Önemi	24
2.3. Hukuki Niteliğine İlişkin Görüşler	26
2.3.1. Ekonomik Hak Görüşü	27
2.3.1.1. Ekonomik Hak – Mülkiyet Hakkı Görüşü	29
2.3.1.2. Ekonomik Hak – Fikri Mülkiyet Hakkı Görüşü	30

2.3.2. Temel İnsan Hakkı ve Kişilik Hakkı Görüşü	31
3. ULUSLARARASI DÜZENLEMELER	37
3.1. Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD) Rehber İlkeleri	38
3.2. Birleşmiş Milletler – Bilgisayarla İşlenen Kişisel Veri Dosyalarına İlişkin Rehber İlkeler	40
3.3. Avrupa Konseyi	41
3.3.1. 108 Sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Gerçek Kişilerin Korunması Sözleşmesi	43
3.4. Avrupa Birliği	45
3.4.1. Avrupa Parlamentosu ve Konseyinin 95/46/EC Sayılı Direktifi	46
3.4.2. Avrupa Genel Veri Koruma Tüzüğü (GVKT)	48
4. KİŞİSEL VERİLERE İLİŞKİN ULUSAL DÜZEYDEKİ NORMLARIN GELİŞİMİ.51	
4.1. Mukayeseli Hukukta	52
4.1.1. Kıta Avrupası’nda	52
4.1.1.1. Almanya’da	53
4.1.1.2. Fransa’da	55
4.1.1.3. İtalya’da	56
4.1.2. Anglosakson Ülkelerinde	57
4.1.2.1. Amerika Birleşik Devletleri’nde	57
4.1.2.2. İngiltere’de	59
4.2. Türk Hukukunda	60
4.2.1. Türk Ceza Kanunu’nun Kişisel Verilere İlişkin Hükümleri	61
4.2.2. Kişisel Verilerin Korunması Hakkının Anayasal Bir Hak Olarak Kabulü ..	62
4.2.3. 6698 Sayılı Kişisel Verilerin Korunması Kanunu’nun Kabulü	64
4.2.4. Muhtelif Kanunlarda Yer Alan Konuyla Bağlantılı Diğer Hükümler	65

İKİNCİ BÖLÜM

6698 SAYILI KVKK KAPSAMINDA KİŞİSEL VERİLERİN KORUNMASI

1. AMAÇ, KAPSAM ve TANIMLAR	67
1.1. Kanunun Amacı	67
1.2. Kanunun Kapsamı	68
1.3. Kanun Kapsamı Dışında Kalan Durumlar	70
1.4. Kavramlara İlişkin Tanımlar	72
1.4.1. Kişisel Veri	73
1.4.2. Kişisel Verilerin İşlenmesi	73
1.4.3. Açık Rıza	74
1.4.4. Anonim Hale Getirme	75
1.4.5. Veri İşleyen ve Veri Sorumlusu	76
1.4.6. Veri Kayıt Sistemi	78
2. KİŞİSEL VERİLERİN İŞLENMESİNE İLİŞKİN TEMEL İLKELER	78
2.1. Hukuka ve Dürüstlük Kuralına Uygun Olma	79
2.2. Belirli, Açık ve Meşru Amaçlar İçin İşlenme	80
2.3. İşlendikleri Amaçlarla Bağlantılı, Sınırlı ve Ölçülü Olma	81
2.4. Gerekli Olan Süre Kadar Muhafaza Edilme	83
2.5. Doğru ve Gerektiğinde Güncel Olma	84
3. KİŞİSEL VERİLERİN İŞLENME ŞARTLARI	85
3.1. Özel Nitelikli Olmayan Kişisel Verilerin İşlenme Şartları	86
3.1.1. Açık Rızanın Bulunması	87
3.1.2. Açık Rıza Şartı Aranmadan Kişisel Verilerin İşlenebileceği Haller	90

3.2. Özel Nitelikli Kişisel Verilerin İşlenme Şartları	94
4. VERİ SORUMLUSUNUN YÜKÜMLÜLÜKLERİ	97
5. İLGİLİ KİŞİNİN HAKLARI	99
6. KVKK’NIN KABAHATLERE ve SUÇLARA İLİŞKİN HÜKÜMLERİ	101
6.1. KVKK’da Kabahat Olarak Tanımlanan Fiiller ve Bunlara İlişkin Hükümler	101
6.1.1. Aydınlatma Yükümlülüğünün Yerine Getirilmemesi	103
6.1.2. Veri Güvenliğine İlişkin Yükümlülüklerin Yerine Getirilmemesi	105
6.1.3. Kurul Kararlarının Yerine Getirilmemesi	106
6.1.4. Veri Sorumluları Siciline Kayıt veya Bildirim Yükümlülüğüne Aykırı Hareket Etme	107
6.2. KVKK’nın Suçlara İlişkin Hükümleri	108
6.2.1. KVKK m.17/2 Hükmüne İlişkin Değerlendirmemiz	109

ÜÇÜNCÜ BÖLÜM

KİŞİSEL VERİLERE İLİŞKİN SUÇLAR

1. KİŞİSEL VERİLERE DOLAYLI KORUMA SAĞLAYAN SUÇ TİPLERİ	116
1.1. Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar	116
1.1.1. Haberleşmenin Gizliliğini İhlal (TCK m.132)	117
1.1.2. Kişiler Arasındaki Konuşmaların Dinlenmesi ve Kayda Alınması (TCK m.133)	118
1.1.3. Özel Hayatın Gizliliğini İhlal (TCK m.134)	119
1.2. Kişinin Hatırasına Hakaret (TCK m.130)	122
1.3. Göreve İlişkin Sırrın Açıklanması (TCK m.258)	123

1.4. Ticari Sır, Bankacılık Sırrı veya Müşteri Sırrı Niteliğindeki Bilgi ve Belgelerin Açıklanması (TCK m.239)	126
2. KİŞİSEL VERİLERİN KAYDEDİLMESİ (TCK m.135)	127
2.1. Korunan Hukuki Değer	128
2.2. Suçun Unsurları	130
2.2.1. Maddi Unsurlar	130
2.2.1.1. Suçun Maddi Konusu	130
2.2.1.2. Fail	135
2.2.1.3. Mağdur	137
2.2.1.4. Fiil	139
2.2.2. Manevi Unsur	145
2.2.3. Hukuka Aykırılık Unsuru	147
2.2.3.1. KVKK Kapsamına Giren Fiiller Bakımından Hukuka Uygunluk Sebepleri	148
2.2.3.2. Genel Hukuka Uygunluk Sebepleri	151
2.2.3.3. Hukuka Aykırı Olarak İfadesinin Anlamı	156
2.3. Nitelikli Haller	160
2.3.1. Suçun Konusuna (Özel Nitelikli Kişisel Verilere) İlişkin Nitelikli Hâl ...	160
2.3.2. Failin Sıfatı ve Fiilin İşlenme Şekliyle İlişkili Nitelikli Haller	163
2.4. Suçun Özel Görünüş Biçimleri	165
2.4.1. Teşebbüs	165
2.4.2. İştirak	166
2.4.3. İçtima	167
2.5. Soruşturma, Kovuşturma ve Yaptırım	173

3. KİŞİSEL VERİLERİ HUKUKA AYKIRI OLARAK VERME, YAYMA veya ELE	
GEÇİRME (TCK m.136)	174
3.1. Korunan Hukuki Değer	175
3.2. Suçun Unsurları	175
3.2.1. Maddi Unsurlar	175
3.2.1.1. Suçun Maddi Konusu	175
3.2.1.2. Fail	175
3.2.1.3. Mağdur	176
3.2.1.4. Fiil	176
3.2.2. Manevi Unsur	183
3.2.3. Hukuka Aykırılık Unsuru	183
3.3. Nitelikli Haller	185
3.4. Suçun Özel Görünüş Biçimleri	186
3.4.1. Teşebbüs	186
3.4.2. İştirak	186
3.4.3. İçtima	187
3.5. Soruşturma, Kovuşturma ve Yaptırım	193
4. KİŞİSEL VERİLERİ YOK ETMEME (TCK m.138)	194
4.1. Korunan Hukuki Değer	197
4.2. Suçun Unsurları	197
4.2.1. Maddi Unsurlar	197
4.2.1.1. Fail	197
4.2.1.2. Mağdur	199
4.2.1.3. Suçun Konusu	199
4.2.1.4. Fiil	200

4.2.2. Manevi Unsur	204
4.2.3. Hukuka Aykırılık Unsuru	205
4.3. Nitelikli Haller	206
4.4. Suçun Özel Görünüş Biçimleri	207
4.4.1. Teşebbüs	207
4.4.2. İştirak	207
4.4.3. İçtima	207
4.5. Soruşturma, Kovuşturma ve Yaptırım.....	208
SONUÇ	210
KAYNAKÇA	215

KISALTMALAR

ABAD	Avrupa Birliđi Adalet Divanı
AİHM	Avrupa İnsan Hakları Mahkemesi
AİHS	Avrupa İnsan Hakları Sözleşmesi
AY	Anayasa
AYM	Anayasa Mahkemesi
Bkz.	Bakınız
BM	Birleşmiş Milletler
BK	Borçlar Kanunu
C.	Cilt
c.	Cümle
C.D.	Ceza Dairesi
CMK	Ceza Muhakemesi Kanunu
Çev.	Çeviren
E.	Esas Numarası
ERÜHFD	Erciyes Üniversitesi Hukuk Fakültesi Dergisi
GVKT	Genel Veri Koruma Tüzüğü
İMHFD	İstanbul Medeniyet Üniversitesi Hukuk Fakültesi Dergisi
K.	Karar Numarası
K.T.	Karar Tarihi
KVKK	Kişisel Verilerin Korunması Kanunu
m.	Madde
MK	Medeni Kanun
OECD	Ekonomik İşbirliđi ve Kalkınma Teşkilatı
S.	Sayı
s.	Sayfa
s.e.t.	Son Erişim Tarihi
TCK	Türk Ceza Kanunu
YCGK	Yargıtay Ceza Genel Kurulu

TABLÖLAR

Tablo 1.	95
----------------------	----



GİRİŞ

Eski çağlardan bu yana insanlar, özel bilgilerinin başkaları tarafından bilinmemesi konusunda haklı bir beklenti içerisinde olmuştur. Tarihi milattan önce beşinci yüzyıla dayanan Hipokrat Yemininde yer alan hastaların özel bilgilerinin açıklanmamasına ilişkin ibare¹, kişisel bilgilerin korunması konusundaki hassasiyetin geçmiş çağlarda da var olduğunu bize göstermektedir. Ancak eski çağlarda kişisel bilgilerin gizliliğini ihlal günümüzdeki kadar sık karşılaşılan bir durum değildir. Bu sebeple yirminci yüzyıla kadar doğrudan bu bilgilerin korunmasına odaklanmış hukuki metinlere rastlamak mümkün değildir.

Son yüz yılda yaşanan teknolojik gelişmeler insan hayatını derinden etkilemiştir. Teknolojinin gelişmesi ve hayatı dönüştürmesi büyük faydalar sağlamasının yanı sıra kişilerin güvenlikleri ve özgürlükleri bakımından birtakım risklerin artmasına da sebep olmuştur. Bu risklerin başında kişisel verilerin kontrolsüz şekilde kaydedilmesi ve meşru olmayan şekillerde kullanılması gelmektedir. Zira bilgi iletişim teknolojilerinin gelişmesi ile insan hayatının büyük bir bölümü dijital alana taşınmış, gündelik işlerin pek çoğu elektronik sistemler kullanılmak suretiyle gerçekleştirilir hale gelmiştir. Bu sistemler zamanla insanların çok çeşitli bilgilerinin toplandığı ve depolandığı gözetim araçlarına dönüşmüştür. İnsan doğumundan ölümüne kadar sürekli bir gözetim altında yaşayan, geçmişi kayıt altında tutulan bir varlık halini almıştır. Veri işlemenin devasa boyutlara ulaşması çok sayıda verinin toplanmasına, çok sayıda verinin toplanması da verilerin hukuka aykırı olarak kullanılma riskinin artmasına sebep olmuştur.

Kişisel veriler üzerindeki risklerin artması devletleri bu konuda hukuki düzenlemeler yapmaya itmiştir. 1970’li yıllardan itibaren pek çok ülkede veri koruma

¹ Altuner, İlyas (2015) ‘Hipokrat Yemini’ Iğdır Üniversitesi Sosyal Bilimler Dergisi, S:7, (s.1-7), s.4.

kanunları yürürlüğe konulmaya başlamıştır². Özellikle Avrupa ülkelerinde ve Amerika Birleşik Devletleri'nde kişisel verilerin korunması hukuku hızlı bir şekilde gelişmiştir³.

İnternet ağının yaygınlaşması kişisel verilerin ülkeler arasında anlık olarak dolaşımını da beraberinde getirmiştir. Verilerin ülkeler arasında hızlı bir şekilde dolaşması ise ulusal düzenlemelerin yetersiz kalmasına ve uluslararası düzeyde adımlar atılmasına sebep olmuştur. Bu kapsamda uluslararası kuruluşlar tarafından kişisel verilerin korunmasını amaçlayan pek çok uluslararası belge kabul edilmiştir. Bu uluslararası düzenlemeler ulusal düzenlemelerin gelişimine ve yaygınlaşmasına da katkı sağlamıştır.

Ülkemizde de kişisel verilerin korunmasına ilişkin kanuni düzenlemeler bulunmaktadır. Bu konudaki ilk düzenlemeler 2005 yılında yürürlüğe giren 5237 sayılı Türk Ceza Kanunu'nda (TCK) yer almıştır. TCK'nın 135, 136 ve 138nci maddelerinde üç ayrı suç tipi ihdas edilmek suretiyle kişisel verilerin korunması hakkını ihlal eden bazı fiillerin gerçekleştirilmesi suç olarak düzenlenmiştir. Böylece kişisel verilerin korunması hakkı ceza hukuku yoluyla koruma altına alınmıştır. Kişisel verilerin ceza hukuku vasıtasıyla korunmasının bu çalışmanın ana konusunu oluşturması sebebiyle bahsi geçen suç tipleri çalışmamızda detaylı bir şekilde incelenecektir.

Kişisel verilerin korunması hukuku kendine özgü kavramlar barındıran bir alandır. Kişisel veri, anonimleştirme, veri sahibi, veri sorumlusu ve veri işleme gibi kavramlar bunlara örnek verilebilir. Bu kavramlara yüklenecek anlamlar TCK'da yer alan suç tiplerinin değerlendirilmesinde büyük önem taşımaktadır. Bu kavramların anlaşılmasında 6698 Sayılı Kişisel Verilerin Korunması Kanunu'nda (KVKK) yer alan tanımlardan ve öğretiden faydalanılması zaruridir.

KVKK yalnızca kavramlara ilişkin tanımların yer alması sebebiyle değil, aynı zamanda kişisel verilerin korunmasına ilişkin usul ve esasların burada düzenlenmiş olması sebebiyle de önem arz etmektedir. Suçun maddi unsurlarının yanı sıra hukuka aykırılık unsurunun değerlendirilmesi sırasında da KVKK hükümlerinin göz önünde bulundurulması gerekmektedir.

² **Küzeci, Elif** (2021) Kişisel Verilerin Korunması, 4. Baskı, İstanbul, On İki Levha Yayıncılık, s.118.

³ **Akgül, Aydın** (2013) Kişisel Verilerin Korunması Açısından İdarenin Hukuki Sorumluluğu ve Yargısal Denetim (Doktora), Kocaeli Üniversitesi Sosyal Bilimler Enstitüsü, s.110-111.

Çalışmamızın birinci bölümünde öncelikle kişisel veri kavramı ele alınacak, bu kavramın kapsamı unsurlarının ayrı ayrı incelenmesi suretiyle tespit edilecektir. Kişisel veri kavramının ardından kişisel verilerin korunması hakkı ele alınacaktır. Kişisel verilerin korunması hakkı bu hakkın önemi, tarihsel gelişimi ve hukuki niteliği konularının incelenmesi suretiyle açıklanacaktır. Daha sonra öğretinin gelişmesine katkı sunan ve kimi ulusal normlara kaynaklık teşkil eden uluslararası düzenlemeler hakkında genel bilgiler verilecektir. Son olarak Kıta Avrupası ülkelerinin, ABD'nin ve ülkemizin kişisel verilerin korunmasına ilişkin normlarının tarihi gelişimi ele alınacaktır.

Çalışmamızın ikinci bölümünde ceza hukuku bakımından sonuç doğuranlar başta olmak üzere KVKK hükümleri detaylı bir şekilde incelenecektir. Çalışmamızın son bölümünü teşkil eden üçüncü bölümde ise TCK'da yer alan suç tipleri birinci ve ikinci bölümlerdeki açıklamalardan da faydalanılarak detaylı bir şekilde incelenecektir.

BİRİNCİ BÖLÜM

KİŞİSEL VERİ KAVRAMI, KİŞİSEL VERİLERİN KORUNMASI HAKKI ve BU HAKKIN KORUNMASINA MAHSUS HUKUKİ DÜZENLEMELERİN GELİŞİMİ

Kişisel verilerin korunması hukuku kendine özgü kavramlar barındıran bir alandır. Kişisel veri, anonim hale getirme, veri sahibi, veri işleme ve veri sorumlusu kavramları bunlara örnek olarak zikredilebilir. Konunun daha iyi anlaşılabilmesi için öncelikle kavramsal çerçevenin çizilmesi gerekmektedir. Tezin ilerleyen bölümlerinde incelenecek konular bakımından da kavramlara atfedilecek anlamların büyük önemi bulunmaktadır. Kavramların anlam, kapsam ve sınırlarına ilişkin kabuller özel meselelerde ulaşılabilecek sonuçları etkileyebilecektir. Çalışmamızın birinci bölümünde kişisel veri kavramı detaylı şekilde ele alınacaktır. Konuya ilişkin diğer kavramlar ise ikinci bölümde 6698 sayılı Kişisel Verilerin Korunması Kanunu’nun (KVKK) ilgili hükümleri doğrultusunda açıklanacaktır.

Kişisel veri kavramı hem öğretide hem de hukuki metinlerde “*kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi*” olarak tanımlanmaktadır⁴. Bu tanım üzerinde birlik olduğunu söylemek mümkündür. Öğretide bu tanımdan yola çıkarak bir kişisel veriden söz edilebilmesi için üç unsurun bir araya gelmesi gerektiği ifade edilmektedir⁵. Bunlar bir gerçek kişinin bulunması, bir bilginin bulunması ve bilginin kişiye ilişkin olmasıdır⁶. Bilginin kişisel veri olarak kabul edilebilmesi için sır niteliğinde olması ise şart değildir.

⁴ **Küzeci**, s.10, **Dülger, Murat Volkan** (2020) Kişisel Verilerin Korunması Hukuku, 3. Baskı, İstanbul, Hukuk Akademisi, s.62.

⁵ **Yılmaz, Süleyman / Çavuşoğlu, Gökçe Filiz** (2020) Kişisel Verileri Koruma Hukuku, Yetkin Yayınları, Ankara, s.36.

⁶ **Yılmaz / Çavuşoğlu**, s.36.

Kişisel verileri özel nitelikli kişisel veriler ve özel nitelikli olmayan kişisel veriler olarak ikiye ayırmak mümkündür. Özel nitelikli verilerin neler olduğu ilgili mevzuat ile belirlenmektedir. Farklı ülke kanunlarında farklı kabuller bulunsa da genel olarak kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi, sendikal üyelikleri ve cinsel hayatı gibi konularla ilgili verileri özel nitelikli kişisel veri olarak kabul edilmektedir. Bu tür veriler üzerinde gerçekleştirilen işlemlerin hukuka uygun kabul edilebilmesi için daha sıkı şartlar aranmaktadır. Hukuka aykırı işlemlere konu edilmesi durumunda kişinin daha ciddi mağduriyetlere uğrayabileceği düşüncesi bu verilerin özel nitelikli kabul edilmesine ve ayrı bir statü sahibi kılınmasına sebep olmuştur⁷.

Çalışmamızın esas konusunu oluşturan suç tipleri kişisel verilerin korunması hakkı ile doğrudan ilişkilidir. Bu hakkın önemi ve tarihsel gelişimi konunun temeli hakkında genel bir bilgi sahibi olmak için önem arz etmektedir. Bu sebeple birinci bölümde kişisel verilerin korunması hakkı üzerinde durulacak, hakkın önemi, tarihsel gelişimi ve hukuki niteliği açıklanacaktır.

Kişisel verilerin korunması hakkının içeriği ve kapsamı zaman içerisinde gelişim göstermiştir. Kişisel verilerin korunması hakkı ortaya çıktığı 1970’li yıllarda devletlerin merkezi veri havuzları oluşturarak bireyler karşısında aşırı güçlenmesini önlemeyi hedefleyen, yani bireyi devlete karşı koruyan bir haktır⁸. Çok geçmeden özel veri bankalarının oluşması ve veri işleyen aktör sayısının artması ile aktör bazlı anlayış yerini birey bazlı anlayışa bırakmıştır. Bu anlayış değişikliği kişisel verilerin korunması hakkının temel insan hakları bağlamında özel hayatın gizliliği hakkının bir parçası ve bir alt görünüm şekli olarak nitelendirilmesini de beraberinde getirmiştir⁹. 1983 yılında Alman Anayasa Mahkemesi tarafından verilen ünlü nüfus sayım kararı hakkın gelişiminde en önemli dönüm noktası olmuş ve bu hak artık bireyin kişisel verilerinin akıbetini tayin etme hakkı olarak kabul görmeye başlamıştır¹⁰.

Kişisel verilerin korunması hakkı diğer pek çok hak ve hürriyet ile yakın ilişki içerisinde. Kişisel verilerin hukuka aykırı işlemlere konu edilmesi neticesinde veri

⁷ **Başalp, Nilgün** (2003) Kişilik Hakkının Korunması Sorunu Çerçevesinde Kişisel Verilerin Korunması ve Saklanması (Yüksek Lisans), İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, s.28.

⁸ **Küzeci**, s.117-120.

⁹ **Küzeci**, s.121.

¹⁰ **Akgül**, s.65.

sahiplerinin çok çeşitli hak ihlallerine maruz kalmaları mümkündür. Bunun yanı sıra hangi kişisel verilerinin, nerede, kim tarafından, ne maksatla muhafaza edildiğini bilmeyen, verilere erişme, verilerinin düzeltilmesini veya silinmesini isteme gibi haklara sahip olmayan bir insanın kişiliğini özgürce geliştirmesi mümkün değildir¹¹.

Kişisel verilerin korunması hakkına ilişkin bir diğer önemli konu hakkın hukuki niteliğinin tespitidir. Hakkın hukuki niteliği konusunda ekonomik hak yaklaşımı ve temel insan hakkı yaklaşımı olmak üzere temelde iki farklı yaklaşımın bulunduğu söylenebilir. Bu yaklaşımlar hakkın kapsamı, sınırlandırılması ve kullanılması konularında yola çıkılan temel hareket noktası olmaları sebebiyle önemlidir. Amerika Birleşik Devletleri'nde ekonomik hak yaklaşımı, Avrupa Birliği ülkelerinde ve ülkemizde ise temel insan hakkı yaklaşımı benimsenmiştir.

Teknolojinin gelişmesi ve internetin yaygınlaşması ile kişisel veriler sanyeler içerisinde ülke sınırları dışına aktarılmaya başlamış, bu durum kişisel verilerin korunmasına ilişkin uluslararası düzenlemeler yapılmasını mecburi kılmıştır. Uluslararası düzenlemeler dünya genelinde olduğu gibi ülkemizde de ilgili mevzuatın gelişmesinde etkili olmuştur. Bu sebeple birinci bölümde bazı uluslararası düzenlemeler hakkında genel bilgiler verilecektir.

1980'li yıllardan günümüze kadar pek çok bölgesel ve küresel örgüt nezdinde hukuki metinler kabul edilmiştir. Bu metinlerin bir kısmı taraf devletler bakımından bağlayıcı nitelikte bir kısmı ise tavsiye niteliğindedir. Bağlayıcı nitelikte olanlar taraf devletleri belirli standartlar çerçevesinde hukuki düzenlemeler yapmaya zorlaması bakımından, tavsiye niteliğinde olanlar ise kişisel verilerin korunması hukukunun yeni gelişmekte olduğu ülkelere örneklik teşkil etmesi bakımından kişisel verilerin korunması hukukuna önemli katkılar sağlamıştır.

Çalışmamızın birinci bölümünde son olarak önemli gördüğümüz bazı ülkelerin kişisel verilerin korunmasına ilişkin ulusal normlarının ve Türk Hukukundaki normların tarihi süreç içerisindeki gelişimi mukayeseli şekilde incelenecektir. Ulusal normların düzenleniş şekilleri kimi ülkelere ciddi oranda benzerlik taşırken kimi ülkelere ise

¹¹ Küzeci, s.76-77.

farklılık arz etmektedir. AB üyesi ülkelerde ve ülkemizde kişisel verilerin korunmasına ilişkin normların genel bir veri koruma kanunu içerisinde bir arada düzenlendiği göze çarpmaktadır. Bununla birlikte Kıta Avrupası'nda ve ülkemizde kişisel verilere ilişkin suç tiplerine yaptırım olarak genellikle hapis cezası öngörülmektedir. ABD'de ise genel bir veri koruma kanunu bulunmamakta, kişisel verileri korumaya yönelik normlar konu ve sektör odaklı kanunların içerisinde dağınık şekilde yer almaktadır. Yine ABD'de kişisel verilere ilişkin suçlara para cezası yaptırımları öngörülmektedir. İngiltere'de ise normların düzenleniş şekli genel olarak AB ülkelerindeki düzenlemelere benzese de suçlara karşılık ABD'dekine benzer şekilde yalnızca para cezaları öngörülmektedir.

Ülkemizde kişisel verilerin korunmasına ilişkin normlar AB ülkelerine nazaran oldukça geç gelişim göstermiştir. Doğrudan kişisel verileri korumaya yönelik ilk düzenlemeler 2005 yılında yürürlüğe giren 5237 sayılı yeni Türk Ceza Kanunu'nda yer almıştır. Kişisel verilerin korunması hakkı 2010 Anayasa değişikliği ile Anayasa'nın 20nci maddesine eklenen 3üncü fıkrada müstakil bir ifade ile yer bulmuştur. İlk veri koruma kanunu ise 2016 yılında 6698 sayılı KVKK'nın kabulü ile yürürlüğe girmiştir. Bu düzenlemelerin yanı sıra ülkemizde kişisel verilerin korunması hakkı Medeni Kanun'un kişilik haklarını koruyan hükümleri ve Borçlar Kanunu'nun haksız fiiller karşısında kişiye maddi ve manevi tazminat hakkı tanıyan hükümleri kapsamında da korunmaktadır.

1. KİŞİSEL VERİ KAVRAMI

1.1. Genel Olarak Kişisel Veri Kavramı

Kişisel verilerin korunması konusunun ele alınabilmesi için öncelikle kişisel veri kavramının ne ifade ettiğinin belirlenmesi gerekmektedir. Kişisel veri kavramını oluşturan kelimelerin sözlük anlamları kavramın çerçevesine dair fikir vermektedir. Ancak kavramın sınırlarının tam olarak belirlenebilmesi için hukuki metinlerde yer alan tanımların incelenmesi gerekmektedir.

Güncel Türkçe Sözlüğe göre veri kelimesi “*bir araştırmanın, bir tartışmanın, bir muhakemenin temeli olan ana öge, muta, done; gözlem ve deneye dayalı araştırmanın sonuçları, bilgi, data*” gibi anlamlara gelmektedir¹². Kişisel veri hukukunda veri kelimesi “*bilgi*” anlamı ile kullanılmaktadır. Uluslararası hukukta ise veri kelimesinin karşılığı olarak “*data*” kelimesi kullanılmaktadır.

Kişi kavramı ise genel olarak hak sahibi olabilen ve bu hakları kullanabilen, borç altına girebilen ve bu borçlar üzerinde tasarrufta bulunabilen, borçlarından sorumlu tutulabilen varlığı ifade etmektedir¹³. Kişiler gerçek ve tüzel kişiler olmak üzere ikiye ayrılmaktadır. Gerçek kişi tabiri yalnızca insanları ifade ederken, tüzel kişiler insanlar tarafından oluşturulan fakat onlardan bağımsız bir nitelik kazanan, hukuk düzeninin ayrı bir kişi olarak kabul ettiği mal ve kişi topluluklarını ifade eder¹⁴. Kişisel kelimesi ise Güncel Türkçe Sözlükte “*kişi ile ilgili, kişiye ilişkin*” şeklinde tanımlanmaktadır¹⁵. Dolayısıyla bu bilgilerden yola çıkarak kişisel veri kavramını gerçek veya tüzel kişiye ilişkin bilgi olarak tanımlamak mümkündür. Kişisel verilerin korunmasına ilişkin ulusal ve uluslararası hukuki metinlerde ise buna benzer bir tanım kabul edilmiş fakat tüzel kişilere ilişkin veriler genellikle kapsam dışında bırakılmıştır.

Kişisel verilerin korunmasına özgülenmiş ilk uluslararası belge niteliğini taşıyan “*Mahremiyetin Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin OECD Rehber İlkeleri*”¹⁶ 1980 yılında yayımlanmıştır ve taraf ülkeler için tavsiye niteliğindedir¹⁷. OECD (Ekonomik İşbirliği ve Kalkınma Teşkilatı) tarafından yayınlanan bu rehber ilkelerin 1-b maddesinde kişisel veri kavramı “*kimliği belirli veya belirlenebilir bir gerçek kişiye (veri sahibi) ilişkin her türlü bilgi*” olarak tanımlanmıştır. 1981 tarihinde Avrupa Konseyi tarafından yayınlanan 108 Sayılı “*Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması*” sözleşmesi¹⁸ bu alanda bağlayıcı nitelik taşıyan ilk

¹² TDK Güncel Türkçe Sözlük, (<https://sozluk.gov.tr>), s.e.t. 17.01.2023.

¹³ **Erdoğan, İhsan / Keskin, Dilşad** (2020) Türk Medeni Hukuku, 3. Baskı, Ankara, Gazi Kitabevi, s. 211.

¹⁴ **Sümer, Haluk Hadi** (2020) Hukuka Giriş, 4. Baskı, Ankara, Seçkin, s. 82.

¹⁵ TDK Güncel Türkçe Sözlük, (<https://sozluk.gov.tr>), s.e.t. 17.01.2023.

¹⁶ OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Bundan sonra OECD Rehber İlkeleri olarak anılacaktır. İngilizce tam metin için bkz. (<https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188>), s.e.t. 17.01.2023.

¹⁷ **Korkmaz, İbrahim** (2019) Kişisel Verilerin Ceza Hukuku Kapsamında Korunması, 2. Baskı, Ankara, Seçkin, s.25.

¹⁸ Bundan sonra kısaca “*108 Sayılı Avrupa Konseyi Sözleşmesi*” olarak anılacaktır, Türkçe ve İngilizce tam metin için bkz. (<http://www2.tbmm.gov.tr/d24/1/1-0966.pdf>), s.e.t. 17.01.2023.

belgedir¹⁹ ve bu belgede de kişisel veri kavramı OECD rehber ilkeleriyle aynı şekilde tanımlanmıştır. 108 Sayılı Avrupa Konseyi sözleşmesinden 14 yıl sonra 24 Ekim 1995 tarihinde Avrupa Parlamentosu ve Avrupa Birliği Konseyi tarafından kabul edilip yayınlanan 95/46/EC sayılı “*Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Direktifi*” de kişisel veri kavramı için aynı tanıımı benimsemiştir. 95/46/EC Sayılı Avrupa Birliği Direktifi 2018 yılında yürürlükten kalkmış ve onun yerine geçen Genel Veri Koruma Tüzüğü’nde (GVKT)²⁰ de kişisel veri tanımı aynıyla korunmuştur. Bazı ülke kanunlarında nispeten farklı tanımların yer aldığı görülmektedir²¹.

Türk Hukuku’nda da kişisel veri uluslararası düzenlemelere paralel olarak; “*kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi*” şeklinde tanımlanmıştır (KVKK m. 3/1-d). Dolayısıyla bu tanımın kişisel veriler için gerek uluslararası hukukta gerekse Türk hukukunda genel olarak kabul edildiğini söylemek mümkündür.

1.2. Kişisel Verinin Unsurları

Kişisel verinin varlığından söz edebilmek için kişisel veri tanımından hareketle üç unsurun bir arada bulunması gerektiğini söyleyebiliriz. Bunlar; bir verinin bulunması, gerçek bir kişinin bulunması ve verinin gerçek kişiye ilişkin olmasıdır. Aşağıda bu unsurların ayrı ayrı incelenmesi suretiyle kişisel veri kavramının kapsamı ve sınırları tespit edilecektir.

1.2.1. Veri Unsuru

Kişisel verinin varlığından söz edebilmek için öncelikle bir verinin bulunması gerekmektedir. Veri kavramı yukarıda da ifade ettiğimiz gibi kişisel veri hukukunda bilgi anlamında kullanılmaktadır. Kişisel veri tanımında yer alan “*her türlü bilgi*” ifadesinden

¹⁹ **Korkmaz**, s. 25.

²⁰ General Data Protection Regulation, Genel Veri Koruma Tüzüğü, Bundan sonra kısaca GVKT olarak anılacaktır, (<https://gdpr.eu/tag/gdpr/>), s.e.t. 17.01.2023.

²¹ Fransa, Almanya ve Avusturya veri koruma kanunlarında ufak farklılıklarla benzer tanımlara yer verilmiştir. Buna karşılık Hollanda veri koruma kanununun yukarıda ifade ettiğimiz tanımı aynen kullandığı görülmektedir. Detaylı bilgi için bkz. **Korkmaz**, s. 26-27.

de anlaşılabacağı üzere bu bilginin ne olacağı konusunda herhangi bir sınırlama bulunmamaktadır. Kişinin şahsi özellikleri, ekonomik durumu, sağlık durumu, eğitim bilgileri, çalışma bilgileri, ailevi bilgileri, dini inancı, mezhebi, etnik kökeni, alışkanlıkları, alışveriş bilgileri, kredi kartı dökümleri, banka hesap bilgileri, kimlik bilgileri, tedavi bilgileri vb. her tür bilgi bu tanımın içerisine girmektedir. Kişisel veri tanımının genişliği karşısında bilginin türü ve niteliği konusunda sınırlayıcı bir çerçeve çizmek mümkün değildir. Yukarıda saydığımız bilgi türleri yalnızca ilk anda aklımıza gelen örneklerdir.

Veri unsurunun gerçekleşip gerçekleşmediğini tespit için bilginin belirli bir kişiye ait olup olmadığının tespitine gerek yoktur. Herhangi bir bilginin varlığı bu unsur açısından yeterlidir. Gerçek bir kişiye ilişkin olma durumu kişisel verinin diğer bir unsuru olup bu unsurun gerçekleşip gerçekleşmediği ayrıca değerlendirilmelidir.

1.2.2. Kişi Unsuru

Kişisel verinin bir diğer unsuru kimliği belirli veya belirlenebilir bir kişinin bulunmasıdır. Yukarıda da belirttiğimiz üzere kişi kavramı haklara ve borçlara sahip olabilen, bunlar üzerinde tasarrufta bulunabilen varlığı ifade etmektedir. Kişiler gerçek ve tüzel kişiler olmak üzere iki kısımdır. Gerçek kişiler yalnızca insanları ifade ederken tüzel kişiler insanlar tarafından oluşturulmuş ve hukuk düzeninin kendisini müstakil bir kişi olarak tanıdığı mal ve kişi topluluklarını ifade eder. Gerçek kişilere ilişkin verilerin kişisel veri olarak kabul edilmesi konusunda herhangi bir tartışma yoktur. Fakat tüzel kişilerin kişisel verinin unsurlarından biri olan kişi unsurunu oluşturup oluşturmayacağı konusunda farklı görüşler vardır. Tüzel kişilere ilişkin verilerin kişisel veri kabul edilmesi durumunda tüzel kişilerin de kişisel verilere sağlanan özel korumadan faydalanabilmesi sonucu doğacaktır.

Bazı hukuk sistemlerinde tüzel kişilere ilişkin veriler de kişisel veri olarak kabul edilmiş ve kişisel veri hukukunun uygulama alanı genişletilmiştir. Avrupa Genel Veri Koruma Tüzüğü (GVKT) yürürlüğe girmeden önce Avrupa Birliği üyesi ülkelerden Avusturya, İtalya, Danimarka ve Lüksemburg'un veri koruma kanunlarında tüzel kişilere

ait veriler de kişisel veri olarak kabul ediliyordu²². Ancak GVKT'nin yürürlüğe girmesi ile bu ülkelerin veri koruma kanunlarında da artık yalnızca gerçek kişilere ilişkin verilerin kişisel veri olarak kabul edildiğini söylemek mümkündür.

Türk hukukunda anayasal bir hak olarak kabul edilen kişisel verilerin korunması hakkı, Anayasanın 20inci maddesinin üçüncü fıkrasında düzenlenmiştir. Bu düzenlemeye göre *“Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir.”*²³. Fıkra metninde gerçek ve tüzel kişiler arasında bir ayırım yapıp yapılmayacağına dair herhangi bir ibare bulunmamaktadır. Anayasa Mahkemesi 6475 sayılı Posta Hizmetleri Kanunu'nda yer alan bir bendin iptali istemi ile açılan davada tüzel kişilerin de bu anayasal hakka sahip olup olmadıkları konusunu değerlendirmiştir. 04.12.2014 tarihli ve 2014/183 sayılı bu kararında Anayasa Mahkemesi madde metninde ve gerekçesinde gerçek ve tüzel kişiler arasında bir ayırım yapılmadığından bahisle tüzel kişilerin de kişisel verilerin korunması hakkına sahip olduğuna hükmetmiştir²⁴. Dört AYM üyesi bu karara karşı oy kullanmıştır²⁵. Anayasa mahkemesi devam eden yıllarda pek çok kararının metninde

²² Aksoy, Hüseyin Can (2008) Kişisel Verilerin Korunması (Yüksek Lisans), Ankara Üniversitesi Sosyal Bilimler Enstitüsü, sf.26.

²³ AY m.20/3; *“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 korunmasını ilişkin esas ve usuller kanunla düzenlenir”*.

²⁴ *“...Anayasa'nın 20. maddesinde kişisel verilerin kişi bakımından korunma alanının gerçek kişiler ya da tüzel kişileri veya her ikisini içine alıp almadığı konusunda bir açıklık bulunmamaktadır. Maddenin gerekçesinde de buna ilişkin bir değerlendirme yoktur. Her ne kadar Anayasa'nın 20. maddesinde daha ziyade gerçek kişilerin özel hayatı ve bu bağlamda gerçek kişilere ilişkin kişisel verilerin korunma altında bulundurulduğu ileri sürülebilir ise de madde metninde kişisel verilerle ilgili olarak "herkes" tabirinin kullanılması dikkate alındığında, tüzel kişilere ilişkin verilerin de 20. madde kapsamında değerlendirilmesi gerekeceği açıktır ... Esasen her ne kadar 95/46/EC sayılı Avrupa Veri Koruması Direktifinde yer alan tanım, tüzel kişilere ilişkin verileri dışlamakta ve kişisel veri kapsamına yalnızca gerçek kişilere ilişkin bilgilerin gireceğini kabul etmekte ise de, gerek "Elektronik haberleşme sektöründe kişisel bilgilerin işlenmesi ve gizliliğinin korunması" hakkında 12.7.2002 gün ve 2002/58/EC sayılı Avrupa Parlamentosu ve Konsey Direktifi'nde, yalnızca elektronik haberleşme sektörüne ilişkin olarak, hem gerçek kişilerin hem de tüzel kişilerin veri sahibi kabul edileceğinin ifade edilmesi; gerekse son yıllarda kabul edilen bazı ülke kanunlarında tüzel kişilerin de kişisel verilerin korunma alanına dâhil edilmesi bir bütün olarak dikkate alındığında, Avrupa ve Dünyadaki gelişimin kişisel verilerin korunmasında tüzel kişilerin de kapsamda yer alması gerektiği yönünde olduğu görülmektedir”*. (AYM, E. 2013/84, K. 2014/183, K.T. 04/12/2014). Tam metin için bkz. (https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2014/183?Donemler_id=2&KararNo=2014%2F183) , s.e.t. 17.01.2023

²⁵ KARŞIOY: *“...kararda da belirtildiği üzere, anılan hükümde de, maddenin gerekçesinde de kişisel verilerin korunmasının tüzel kişileri kapsayıp kapsamadığı ile ilgili bir açıklık bulunmamaktadır. Diğer taraftan, Avrupa İnsan Hakları Sözleşmesinde açık bir hüküm olmamasına rağmen Avrupa İnsan Hakları Mahkemesi (AİHM)'nin kişisel verilerin korunmasını isteme hakkını kapsamında değerlendirdiği Sözleşmenin 8. maddesinde de Anayasanın 20. maddesinde olduğu gibi "herkes" kavramı kullanılmakta; ancak AİHM kararlarına da dayanılarak, maddenin temel amacının "bireyi" korumak olduğu, bu madde kapsamındaki hakkın kolektif olmaktan çok bireysel bir niteliğinin bulunduğu, maddede özne olarak "herkes"*

“...belirli veya belirlenebilir bir gerçek veya tüzel kişi hakkındaki her türlü bilgi kişisel veri olarak değerlendirilir.”²⁶ ifadesine yer vermek suretiyle tüzel kişilere ilişkin verileri de kişisel veri olarak kabul etmiştir.

Anayasa Mahkemesi’nin tüzel kişilerin de bu hakkın korumasından yararlanabileceklerine hükmetmesine karşın hem 6698 sayılı KVKK’da hem de kişisel verileri koruma maksadına matuf uluslararası sözleşme, direktif ve tüzüklerde yalnızca gerçek bir kişiye ilişkin bilgiler kişisel veri olarak kabul edilmiştir. Yukarıda kişisel veri tanımlarına yer verdiğimiz OECD Rehber İlkeleri, 108 Sayılı Avrupa Konseyi Sözleşmesi, 95/46/EC sayılı Avrupa Birliği Direktifi ve Avrupa Genel Veri Koruma Tüzüğü (GVKT) incelendiğinde yalnızca gerçek kişilere ilişkin verilerin kişisel veri kapsamına alındığı anlaşılmaktadır. 95/46/EC sayılı Avrupa Birliği Direktifi doğrultusunda hazırlanan KVKK’da da kişisel verilerin yalnızca gerçek kişilere ilişkin söz konusu olabileceği anlayışı kabul edilmiştir. Kanunun 3’üncü maddesinde kişisel veri tanımı yapılırken verinin yalnızca gerçek kişiye ilişkin olabileceği açıkça belirtilmiştir. Aynı doğrultuda ilgili kişi kavramı da “*kişisel verisi işlenen gerçek kişi*” olarak tanımlanmıştır. Dolayısıyla KVKK yalnızca gerçek kişilere ilişkin verileri koruma altına almaktadır. Bu kanun bakımından tüzel kişiler yalnızca veri işleyen ve veri sorumlusu olabilirler.

terimi tercih edildiğinden yaş, temyiz kudreti, vatandaşlık veya cinsiyet temelinde istisna olmaksızın her bireyin bu haktan yararlanabileceği, buna karşılık bu hakkın dört alt kategorisinden sadece "konuta saygı hakkının" öznesinin hem gerçek hem de tüzel kişiler olabileceği, "özel yaşama saygı hakkı", "aile yaşamına saygı hakkı" ve "haberleşmeye saygı hakkı"ndan ise doğaları gereği ancak gerçek kişilerin yararlanabileceği belirtilmektedir (Gülay Arslan Öncü, *Özel Yaşama ve Aile Yaşamına Saygı Hakkı, İnsan Hakları Avrupa Sözleşmesi ve Anayasa, Anayasa Mahkemesine Bireysel Başvuru Kapsamında Bir İnceleme*, Sibel İnceoğlu (Ed.), Ankara 2013, s.301). Kişisel veriler, "özel yaşama saygı hakkı" kapsamında korunan hukukî menfaatler arasında bulunan "bireyin mahremiyetinin korunması hakkı"nın konusu olarak ele alınmaktadır (Öncü, age., s.311-312). İncelenen kuralda kamu tüzel kişileri ile özel hukuk tüzel kişilerini kapsayacak şekilde geçen "tüzel kişiler"in ise adresleri bakımından "mahremiyet hakkı" söz konusu olmadığı gibi kuruluş gayeleri itibarıyla mümkün olduğunca aleni olmaları gerekmektedir.

Nitekim, kararın gerekçesinde atıf yapılan 95/46/EC sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Konusunda Bireylerin Korunması Hakkındaki Avrupa Direktifinin 2. maddesinde de kişisel veriler "kimliği belirli veya belirlenebilir gerçek kişilere ait bilgi" olarak tanımlanmakta ve elektronik haberleşme sektörüne ilişkin olarak tüzel kişileri de koruma kapsamında kabul eden 2002/58/EC sayılı Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Hakkındaki Avrupa Direktifinin Başlangıç kısmının 12. paragrafında bu Direktif ile üye devletlere 95/46/EC sayılı Direktifin uygulama alanını tüzel kişileri de kapsayacak şekilde genişletme yükümlülüğü getirilmediği belirtilmektedir.

...Dolayısıyla, Anayasanın 20. maddesinin son fıkrasında ayrıca düzenlenen kişisel verilerin korunmasını isteme hakkının tüzel kişileri kapsamadığını belirtmek, AIHM kararlarına da dayanılarak yapılan yukarıdaki tespitlerle çelişmeyecektir.” (AYM, E. 2013/84, K. 2014/183, K.T. 04/12/2014).

²⁶ (E.Ü., § 59; Bestami Eroğlu, § 102; Bülent Kaya [GK], B. No: 2013/2941, 11/5/2016, § 49; Fatih Saraman [GK], B. No: 2014/7256, 27/2/2019, § 57; AYM, E.2014/74, K.2014/201, 25/12/2014; 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) ayrıca bkz. (H.Ö., B. No: 2019/20473, 3/2/2022)

Türk hukukunda tüzel kişilere ilişkin verilerin açıkça kişisel veri olarak kabul edildiği tek düzenleme elektronik haberleşme sektörüne ilişkindi. 5809 sayılı Elektronik Haberleşme Kanunu'nun ilgili maddelerine dayanılarak Bilgi Teknolojileri ve İletişim Kurumu tarafından hazırlanan Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunmasına İlişkin Yönetmelik hem gerçek kişilerin hem de tüzel kişilerin verilerini kişisel veri olarak kabul etmekteydi. Söz konusu yönetmelik ile *“elektronik haberleşme sektöründe faaliyet gösteren işletmecilerin tüzel kişi abonelikleri dahil elektronik haberleşme hizmeti sunulması kapsamında elde ettikleri veriler bakımından uyacakları usul ve esaslar”*²⁷ belirlenmiştir. 2012 tarihli önceki yönetmeliğin²⁸ 3-1-h maddesinde kişisel veri *“belirli veya kimliği belirlenebilir gerçek ve tüzel kişilere ilişkin bütün bilgiler”* olarak tanımlanmıştı. 4 Haziran 2021 tarihinde eski yönetmelik yürürlükten kaldırılmış ve aynı isimle yeni yönetmelik yürürlüğe girmiştir. Yeni yönetmelikte kişisel veri tanımında değişikliğe gidilmiş ve kişisel veri kavramı KVKK'ya paralel olarak yalnızca gerçek kişileri kapsar hale getirilmiştir.

Tüzel kişilere ilişkin veriler gerçek kişiler hakkında da bilgi içeriyorsa bu verilerin koruma kapsamında olduğunu kabul etmek gerekir²⁹. Zaten bu durumda korunan gerçek kişilere ilişkin veriler olmaktadır.

Tüzel kişilere ilişkin verilerin kişisel veri kabul edilmemesi bu verilerin hiçbir suretle korunmayacağı anlamına da gelmemelidir. TMK'nın 23, 24 ve 25inci maddeleri doğrultusunda kişilik hakkının korunması kapsamında tüzel kişilerin verilerinin korunması mümkündür³⁰. Yine tüzel kişilere ait ticari sır niteliği taşıyan verilerin de ticaret hukuku kapsamında ve ceza hukuku kapsamında korunması mümkündür. Nitekim Türk Ceza Kanunu'nun 239uncu maddesinde ticari sır ve bankacılık sırlarının ifşa edilmesi suç olarak düzenlenmiştir. Tüzel kişilere ait verilerden bu kapsama girenler TCK 239'da düzenlenen suçun konusunu oluşturabilecektir.

²⁷ Yönetmelik Madde 2, tam metin için bkz. <https://www.resmigazete.gov.tr/eskiler/2020/12/20201204-13.htm>, s.e.t. 17.01.2023

²⁸ Yönetmeliğin önceki hali için bkz. <https://www.resmigazete.gov.tr/eskiler/2012/07/20120724-2.htm>, s.e.t. 17.01.2023

²⁹ **Öztürk, Bahri / Seyhan, Serkan / Altınok Çalışkan, Elif** (2022) Kişisel Verilerin Korunması Hukuku, 2. Baskı, Ankara, Seçkin, s.18.

³⁰ **Aksoy**, s.107.

Bir diğerk tartışma konusu ceninin kişisel veri süjesi olup olamayacağına ilişkindir. 6698 sayılı KVKK’da cenine dair herhangi bir hüküm bulunmamaktadır. Keza GVKT’de de ceninlere ilişkin bir hüküm yer almamaktadır. Genel hükümler çerçevesinde konuyu ele alabilmek için Medeni Kanun’un ilgili hükümlerine başvurmak gerekmektedir. TMK’nın 28inci maddesinde kişiliğin başlangıç ve bitişı düzenlenmiştir. Buna göre kişilik çocuğun tam ve sağ doğumu ile başlar ve ölüm ile sona erer. Doğum ile kişilik başlayacağına göre doğum anından itibaren her insanın tam hak ehliyetine sahip olduğunda ve dolayısıyla kişisel veri süjesi olabileceğinde tereddüt bulunmamaktadır. 28inci maddenin ikinci fıkrasında “*çocuk hak ehliyetini, sağ doğmak koşuluyla, ana rahmine düştüğü andan başlayarak elde eder*” hükmüne yer verilmek suretiyle ceninlerin durumu düzenlenmiştir. Buna göre tam ve sağ doğumun gerçekleşmesi şartıyla kişi anne karnına düştüğü andan itibaren veri süjesi olabilecektir. Anne karnındaki ceninin tam ve sağ doğumu ile veri süjesi haline geleceğı göz önünde bulundurularak cenin döneminden itibaren verilerinin korunmasına özen gösterilmelidir. Böylece ceninin gelecekte hak kaybına uğramasının önüne geçilmiş olacaktır³¹.

Ölülere ilişkin verilerin kişisel verilerin korunması mevzuatı kapsamında korunup korunmayacağı, bir diğerk deyişle ölümlerin kişisel veri süjesi olup olamayacakları da tartışma konusudur. KVKK’da ölümlerin verilerine ilişkin bir hüküm bulunmamaktadır. TMK’da da kişiliğin ölüm ile sona ereceğı düzenlenmiş fakat ölümlerin kişilik haklarının akıbeti konusunda bir düzenlemeye yer verilmemiştir. Diğerk hukuk sistemlerinde ve öğretilerde farklı görüşler bulunsa da mevzuatımızdaki mevcut hükümler doğrultusunda ölümle birlikte kişilik hakları da sona erer ve bu haklar mirasçılara devredilemez. Dolayısıyla ölenin mirasçılarının ölen kişinin kişilik hakkına dayanarak koruma talebinde bulunmaları ve bu hakları dava etmeleri mümkün değildir³². Bununla birlikte ölen kişinin şeref ve saygınlığını zedeleyecek saygısızlıkların yapılması, özel bilgilerinin ifşı edilmesi gibi olayların vuku bulması muhtemeldir. Bu gibi durumlarda ölen kişinin yakınlarının bu olaylara katlanması ve sessiz kalması beklenemez. Ölen kişinin yakınlarının ölenin hatırasına yapılacak bu saygısızlıklardan müteessir oldukları durumlarda ölenin kişilik haklarına değil kendi kişilik haklarına dayanarak kişilik haklarının korunmasını talep

³¹ **Özkan, Oğulcan** (2020) Kişisel Verilerin Korunması (Yüksek Lisans), Ankara Üniversitesi Sosyal Bilimler Enstitüsü, sf.16.

³² **Petek, Hasan** (2015) Kişilik Değerlerinin Ölümünden Sonra Korunması, 1. Baskı, Ankara, Yetkin, s.41.

etmeleri mümkündür³³. Yani ölen kişinin hatırası, o hatıraya saygısızlık edilmesi durumunda bundan müteessir olan yakınlarının kişilik hakları kapsamında korunabilecektir³⁴. Bir görüşe göre ölümlere ilişkin verilerinin ifşası gibi durumlarda da ölen kişinin hatırası bu çerçevede TMK hükümleri doğrultusunda korunabilir³⁵. KVKK ise yalnızca yaşayan gerçek kişilere ait verileri korumaktadır. KVKK hükümlerine dayanarak verilerin korunmasını talep etme hakkı yalnızca ilgili kişinin kendisine aittir. Dolayısıyla KVKK kapsamında tanınan haklar ölenin yakınları veya bir başkası tarafından kullanılamaz. Kişisel Verileri Koruma Kurumu'nun 2021/241 ve 2019/273 sayılı kararları da aynı doğrultudadır³⁶. Aynı şekilde GVKT de yalnızca hayattaki kişilere ait verileri korumaktadır. GVKT'nin 27nci paragrafında *“Bu tüzük vefat etmiş kişilerin kişisel verileri için geçerli değildir. Üye devletler ölümlerin kişisel verilerinin korunmasına ilişkin düzenlemeler yapabilirler”* ifadesi yer almaktadır. Bu ifadeden anlaşılabacağı üzere GVKT ölümlerin kişisel verilerini kapsamamakta, ölümlerin verilerine ait düzenleme yapıp yapmamak konusunda ise üye devletler özgür bırakılmaktadır.

Öğretideki bir görüşe göre öldükten sonra kişisel verilerinin korumasız kalacağını düşünen bir kişinin özgürce hareket etmesi mümkün olmayacağından bu durum bireyin kişiliğini serbestçe geliştirme hakkına müdahale teşkil eder³⁷. Bunun yanı sıra öğretide kişilik haklarının ölümle sona ereceği düşüncesini benimseyen İsviçre ve Türk Medeni Hukuku'ndaki yaygın kabulün aksine insan onurunun ölümden sonra da korunması gerektiği yönünde görüşler de bulunmaktadır³⁸. Bizce de doğru olan insan onurunun kişinin ölümünden sonra da korunmasıdır. Bu koruma kişinin yakınlarının kişilik hakları

³³ **Turan Başara, Gamze** (2020) ‘Kişiliğin Korunması Kapsamında Ölümden Sonra Hatıranın Korunması Teorisi’ Çankaya Üniversitesi Hukuk Fakültesi Dergisi, Cilt:5, Sayı:1, (s.341-390), s.342.

³⁴ Detaylı bilgi için bkz. **Turan Başara**, s.341-390.

³⁵ Detaylı bilgi için bkz. **Uçak, Murat** (2021) ‘Kişisel Verilerin Ölümden Sonra Korunması’ İMHFD, C:VI, S:10, (s.97-123)

³⁶ Kişisel Verileri Koruma Kurulu 18.09.2019 tarihli ve 2019/273 sayılı kararında ölen kişinin kişisel verilerine ölen kişinin yasal mirasçısı olan eşi tarafından erişim talep edilmesi şeklinde gerçekleşen olayda *“talep edilen kişisel verilerin talep eden gerçek kişiye ilişkin olmaması ve ölmüş kişiye ait olması sebebiyle talebin, Kanunun 11. maddesi kapsamında bir talep olarak değerlendirilmeyeceği kanısına varıldığından bu hususta 6698 sayılı Kanunun kapsamında yapılacak bir işlemin olmadığına”* karar vermiştir. Karar özeti için bkz. (<https://www.kvkk.gov.tr/Icerik/6710/2019-273>) s.e.t. 17.01.2023. Kurulun 18.03.2021 tarih ve 2021/241 sayılı bir diğer kararında da *“kişilik ölümle son bulduğundan ölen kişinin kişisel verilerine ilişkin talepler Kanun kapsamında değerlendirilemeyecek”* ifadesine yer verilmiştir. Bununla birlikte 21 Haziran 2019 tarihinde yayınlanarak yürürlüğe giren Kişisel Sağlık Verileri Hakkında Yönetmelik'in *“Ölünün Sağlık Verilerine Erişim”* başlıklı 11inci maddesi uyarınca *“Ölmüş bir kimsenin sağlık verilerini almaya, veraset ilamını ibraz etmek suretiyle murisin yasal mirasçıları münferit olarak yetkilidir.”* Bu hüküm ölümlerin sağlık verilerine murislerinin erişimi noktasında düzenleme alanıyla sınırlı olmak üzere bir istisna teşkil etmektedir.

³⁷ **Uçak**, s.113.

³⁸ **Uçak**, s.106.

kapsamında değil bizzat ölen kişinin kişilik hakları kapsamında sağlanmalıdır. Şayet kişilik haklarının ve dolayısıyla insan onurunun kişinin ölümünden sonra sınırlı da olsa korunabileceği anlayışı kabul edilirse kişisel verilerin de ölen kişinin kişilik hakları kapsamında ölümünden sonra korunması mümkün olacaktır. KVKK'ya bu kanun hükümlerinin ölen kişilere ait veriler için de uygulanacağına dair bir hüküm eklenmesi suretiyle ölümlere ait kişisel veriler hem kişisel verilerin korunması hukuku bakımından hem de ceza hukuku bakımından doğrudan koruma altına alınabilecektir³⁹.

Kişi unsurunu incelerken ele alınması gereken bir diğer husus kişinin kimliğinin belirli veya belirlenebilir olmasıdır. Elimizde bir veri bulunması ve bu verinin gerçek bir kişiye ilişkin olması kişisel veriden söz edebilmek için yeterli değildir. Bu kişinin kimliğinin belirli yahut belirlenebilir olması şarttır. Kişisel verilerin korunması bir kişilik hakkı olduğuna ve bu hakkın korunması ile kişilik haklarının zedelenmesinin önüne geçilmesi hedeflendiğine göre kişinin kimliğinin belirli veya belirlenebilir olması doğal olarak gereklidir. Çünkü kimliği belirsiz ve belirlenmesi de imkânsız olan bir kişiye ilişkin verilerin işlenmesi sonucu o kişinin hak ihlaline uğraması mümkün değildir.

Kişiyi doğrudan belirli kılan kimlik bilgileri ve fotoğraf gibi verilerin yanı sıra, başka bilgiler ile birlikte değerlendirildiğinde yahut bazı işlemlere tabi tutulduğunda kişiyi belirlenebilir kılan veriler de kişisel veri olarak kabul edilmelidir. İlişkin olduğu kişiyi hiçbir şekilde belirleme imkânı vermeyen verileri ise kişisel veri olarak kabul etmek mümkün değildir. Bu kıstas belirli veya belirlenebilir bir kişiye ait olmayan verilerin kişisel veri işleme şartlarını yerine getirmeden işlemeye imkân vermesi bakımından önem arz etmektedir. İstatistik hesaplamalarında, belirli bir hizmeti kullanan kişilerin kullanım verilerinden ve profil bilgilerinden istifade ederek o hizmetin geliştirilmesine yönelik yapılan çalışmalarda ve sair pek çok çalışmada veriler, kişiyi hiçbir şekilde belirlemeye imkân vermeyecek bir forma sokularak işlenmekte, böylece veri işleme şartlarına ve kanuni yükümlülöklere takılmadan veriler kullanılabilir. İlişkin olduğu kişiyi belirlemeye imkân vermeyen bu tip verilere anonim veriler denir. Verileri ilgili olduğu kişinin belirlenmesine imkân vermeyen bir forma dönüştürmeye ise verilerin anonim hale

³⁹ Fransa, Macaristan, Danimarka, Slovakya ve Bulgaristan gibi bazı ölkelerin veri koruma kanunlarında kişisel verilerin ölümünden sonra da korunmasına ilişkin hükümler yer almaktadır. Detaylı bilgi için bkz. **Uçak**, s.117-118.

getirilmesi denir. Verilerin anonim hale getirilmesi konusu ileride müstakil başlık altında tekrar ele alınacaktır.

1.2.3. Verinin Kişiyeye İlişkin Olması

Verinin kişiyeye ilişkin olması o veri ile kişi arasında bağlantı kurulabilmesini ifade eder. Kişisel veri kavramının kapsam ve sınırlarının belirlenmesi maksadıyla Veri Çalışma Grubu'nun⁴⁰ sunduğu 2007/4 sayılı görüşte verinin kişiyeye ilişkin olması unsuru detaylıca açıklanmıştır. Buna göre veriler içerik, amaç veya sonuç yönünden bir kişi ile ilişkili olabilirler. İçerik yönünden kişi ile ilgili olan veriler ile kişi arasındaki ilişki çoğu zaman kolaylıkla tespit edilebilir. Örneğin personel kayıtlarının tutulduğu ofiste bir kişinin dosyasında yer alan veriler açıkça o kişi ile ilgilidir. Yine bir hastanın tıbbi testlerinin sonuçları da o hastaya ilişkindir.

Fakat bazı durumlarda bilgilerin kişi ile ilişkisi bu kadar açık değildir. İlk bakışta başka bir nesne ile ilgili olan veriler de dolaylı olarak kişiyeye ilişkin olabilir. Kişi ile veri arasındaki ilişki amaç ve sonuç yönünden olduğunda genellikle durum böyledir. Basit bir örnek vermek gerekirse bir evin değeri o eve ilişkin bir bilgidir. Bu bilgi belirli bir bölgedeki evlerin ortalama fiyatlarını tespit etmek amacıyla kullanılırsa kişisel bir veriden söz etmek mümkün değildir. Fakat ev nihayetinde bir kişinin malıdır. Evin değeri bu kişinin ne kadar emlak vergisi ödeyeceğini belirlemek için kullanıldığında artık kişisel bir veriden söz edilecektir. Bu durumda kişi ve bilgi arasında amaç yönünden bir ilişki kurulmuştur. Bir şirket telefonunun arama kayıtlarını ele alacak olursak, bu telefonun kullandığı hat şirket adına açılmıştır ve şirketin kullanım bilgileri şirketin ne kadar telefon faturası ödeyeceğinin tespiti için kullanılabilir. Bu durumda bu veriler şirkete ilişkindir. Fakat bu telefon belirli bir personelin kullanımına tahsis edilmiş ise bu arama kayıtlarından o personelin kimler ile görüştüğü tespit edilebilir. Arama kayıtları bu amaçla

⁴⁰ Veri Çalışma Grubu 95/46/EC sayılı Avrupa Birliği Direktifinin 29 ve 30'uncu maddeleri uyarınca kurulur. Üye devletler tarafından atanan temsilcilerden oluşur. Danışma görevi görür ve bağımsız olarak hareket eder. Direktifin uygulanmasına yönelik belirsizlikleri ortadan kaldırmayı ve ulusal uygulamalara yön vermeyi hedefler.

kullanıldığında amaç yönünden ilişkiden söz edilir ve arama kayıtları o personelin kişisel verileri olarak kabul edilir⁴¹.

Verinin işlenmesi neticesinde ortaya çıkan sonuç değerlendirilerek de verinin kişiye ilişkin olup olmadığına kanaat getirilebilir. Bazı veriler içerik yönünden doğrudan kişi ile ilişkili olmasa da bu verilerin işlenmesi bir kişinin hakları ve çıkarları üzerinde etki doğurabilir. Bu etkinin büyük bir etki olması da şart değildir. Diğer insanlardan farklı bir muamele görmesi yeterlidir. İşte bu durumlarda sonuç yönünden bir ilişki olduğu kabul edilmektedir. Örneğin bir taksi şirketi tarafından şirkete bağlı taksilerin mevcut konumlarını anlık olarak izleme imkânı sunan bir uydu sistemi kurulur. Sistemin amacı taksi çağırın her müşteriye, müşterinin adresine en yakın arabayı atayarak daha iyi hizmet vermek ve yakıt tasarrufu sağlamaktır. Bu sistem için gereken veriler sürücülerle ilgili değil otomobillerle ilgili verilerdir. Sistem ile elde edilen verilerin işlenme amacı da taksi sürücülerinin performanslarını değerlendirmek değildir. Fakat bu veriler taksi sürücülerinin hız sınırlarına uyup uymadığının, uygun güzergahları kullanıp kullanmadıklarının ve direksiyon başında olup olmadıklarının kontrol edilmesini sağlar. Bunun neticesinde verilerin kişiler üzerinde önemli bir etkisi olabilir. Bu durumda verilerin taksi sürücülerine ilişkin olduğunu kabul etmek gerekir⁴².

1.3. Özel Nitelikli Kişisel Veri Kavramı

Bazı kişisel veriler, işlenmeleri durumunda nitelikleri gereği veri sahibinin daha büyük zararlara uğramasına sebep olabilirler. Bu veriler için farklı hukuki metinlerde hassas veriler, özel kategorideki veriler ve özel nitelikli veriler⁴³ gibi farklı tabirler kullanılmaktadır⁴⁴. Dini inanç, ırksal köken, sendikal üyelik, cinsel hayat vb. konulardaki bu verilerin işlenmesinin telafisi güç mağduriyetlere yol açabileceği, kişinin ayrımcılığa ve nefret söylemlerine maruz kalmasına neden olabileceği kabul edilmektedir⁴⁵. İşte bu tür

⁴¹ **Article 29 Data Protection Working Party**, Opinion 4/2007 on the concept of personal data (Veri Çalışma Grubu, Kişisel Veri Kavramına İlişkin 4/2007 Sayılı Görüş). Raporun tamamı için bkz. (https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf), s.e.t. 17.01.2023.

⁴² **Article 29 Data Protection Working Party**, Opinion 4/2007 on the concept of personal data (Veri Çalışma Grubu, Kişisel Veri Kavramına İlişkin 4/2007 Sayılı Görüş).

⁴³ Bu çalışmada 6698 sayılı KVKK'ya uygun olarak “*özel nitelikli kişisel veri*” kavramı kullanılacaktır.

⁴⁴ **Akgül**, s.12.

⁴⁵ **Başalp**, s.28.

belli başlı bazı kategorilere giren verilerin daha hassas korumaya sahip olması gerektiği fikrinden hareketle bu verilerin işlenmesi özel kurallara tabi kılınmıştır⁴⁶.

Bu kategorilerin neler olduğu hususunda hem uluslararası hukukta hem de hukukumuzda tam bir birlik olduğunu söylemek mümkün değildir. 108 sayılı Avrupa Konseyi Sözleşmesi’nde kişinin “ırksal kökeni, siyasi düşüncesi, dini veya diğer inançları, sağlık veya cinsel hayatı ve ceza mahkumiyetleri” ile ilgili veriler özel nitelikli kişisel veri kabul edilmiştir. 95/46/EC sayılı Direktifte ise bu kategorilere ek olarak “etnik köken ve sendikal üyeliğe dair veriler” de özel nitelikli veri olarak kabul edilmektedir. Son olarak GVKT’ye baktığımızda 95/46/EC sayılı Direktifte yer alan kategoriler korunmakla birlikte “genetik veriler ve biyometrik veriler ile kişinin cinsel yönelimine ilişkin verilerin” de özel nitelikli veriler olarak kabul edildiğini görmekteyiz⁴⁷.

Türk hukukunda 6698 sayılı KVKK’nın 6ncı maddesinde özel nitelikli veriler sayılmıştır. Buna göre; “Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlık, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir.” GVKT’den farklı olarak KVKK’da kişilerin “mezhebi, kılık kıyafeti, dernek ya da vakıf üyelikleri” de özel nitelikli kişisel veri olarak kabul edilmiştir. Özel nitelikli kişisel veri kategorilerinin belirlenme amaçları düşünüldüğünde, uygulanacağı toplumun kendine özgü ihtiyaçlarının bu kategorilerin belirlenmesinde etkili olması kaçınılmazdır. Türkiye’nin sosyolojisi ve yakın tarihimizde yaşanan olaylar⁴⁸ dikkate alındığında KVKK’da GVKT’ye ek olarak yukarıda bahsi geçen kategorilerin de özel nitelikli veri sayılmasının yerinde olduğunu kabul etmek gerekir.

⁴⁶ Bygrave, Lee A. (2002) Data Protection Law: Approaching Its Rationale, Logic and Limits, Hollanda, Kluwer Law International, s.67.

⁴⁷ Avrupa Genel Veri Koruma Tüzüğü (GVKT) 25 Mayıs 2018 tarihinde 95/46/EC sayılı Direktifi yürürlükten kaldırarak yürürlüğe girmiştir. Bu tarihten itibaren Avrupa Birliği’ne üye olan devletlerin tamamında veri koruma kanunu olarak GVKT uygulanmaktadır. Dolayısıyla AB üyesi ülkelerde uygulamada birliğin sağlandığını söyleyebiliriz. Buna göre bu ülkelerde “ırksal veya etnik köken, siyasi düşünce, dini veya felsefi inanç, sendikal üyelikler, ceza mahkumiyetleri, sağlık, cinsel hayat ve cinsel yönelim, genetik ve biyometrik veriler” özel nitelikli veriler olarak kabul edilmektedir.

⁴⁸ Geçmişte ülkemizde insanların mezhepleri, kılık kıyafetleri ve birtakım mensubiyetleri sebebiyle nefret ve ayrımcılığa maruz bırakıldıkları bir gerçektir. Maraş ve Sivas olayları mezhep temelli ayrımcılığa, 28 Şubat döneminde yaşanan kitlesel işten çıkarma olayları ise kılık kıyafet ve mensubiyet temelli ayrımcılığa örnek olarak gösterilebilir.

Türk Ceza Kanunu'nun 135inci maddesinde Kişisel Verilerin Kaydedilmesi suçu düzenlenmiş, aynı maddenin 2inci fıkrasında ise bazı kategorilere ilişkin verilerin hukuka aykırı olarak kaydedilmesi durumunda verilecek cezanın yarı oranında artırılacağı hükme bağlanmıştır. 135inci maddenin 2inci fıkrasında göre bunlar *“kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin”* verilerdir. 5237 sayılı TCK'nın yürürlüğe girdiği 1 Haziran 2005 tarihinden bu yana Türk Ceza Hukuku bakımından bu verilerin özel nitelikli veri sayıldığını söylemek mümkündür.

KVKK'da ve TCK'da sayılan özel nitelikli veri kategorilerinin birbiri ile uyumlu olmadığı, TCK'da daha dar bir sayımın yapıldığı göze çarpmaktadır. KVKK daha güncel bir çalışmanın ürünüdür ve TCK'nın 135inci maddesinden yaklaşık 11 sene sonra yürürlüğe girmiştir. Kişisel verilerin korunması konusunda öğretinin bu süre zarfında hızla geliştiği düşünüldüğünde özel nitelikli veri kategorilerine yenilerinin eklenmesi doğaldır. KVKK ile TCK arasındaki bu farkın özel nitelikli kişisel veri kategorilerini belirlemede ceza hukuku açısından daha dar ve sınırlayıcı bir anlayışla hareket edilmesinden kaynakladığı akla gelebilir. Fakat kanunun yapıldığı tarihte uluslararası hukukta genel kabul gören 95/46/EC sayılı Direktif ile benzer kategorilerin TCK'da benimsenmiş olması dikkate alındığında, bunun kapsamı kasten daraltmaya yönelik bir tercih değil dönemin öğretisiyle uyumlu bir düzenleme olduğu anlaşılmaktadır. KVKK'da yer alan bazı özel nitelikli veri kategorilerinin TCK'da yer almaması bu verilerin ceza hukuku kapsamında da daha üst düzey korumaya tabi tutulması gerekirken bu korumadan mahrum kalmasına yol açmaktadır. Kanaatimizce TCK m.135/2'nin, bu konuda daha güncel bir çalışmanın ürünü olan KVKK'nın özel nitelikli kişisel verileri düzenleyen 6ncı maddesine uygun hale getirilmesi yerinde olacaktır.

2. KİŞİSEL VERİLERİN KORUNMASI HAKKI

Kişisel verilerin korunması hakkı en genel anlamıyla kişilerin kendilerine ait kişisel veriler hakkında bunlara ulaşma, işlenip işlenmediğini öğrenme, hangi amaçlarla işlendiğini bilme, silinmesini talep etme, hukuka aykırı olarak kaydedilmesinin ve aktarılmasının önlenmesini isteme gibi taleplerde bulunma hakkını ifade eder. Bu hak

kişinin kendisi ile ilişkili her türlü bilginin akıbetini tayin etme imkanına sahip olmasını sağlar. Bu sayede kişi varlığını özgürce geliştirme, hak ihlaline maruz kalma tehdidi olmadan hareket etme, bir ihlal ile karşılaştığında hukuki yollara başvurarak bu ihlali sona erdirmeye olanaklarına sahip olur. Kişisel verilerin korunması hakkı özel hayatın gizliliği başta olmak üzere fikir özgürlüğü, unutulma hakkı, din ve vicdan hürriyeti gibi diğer pek çok hak ile de ilişkilidir. Kişisel verilerin korunması hakkının tarihsel gelişimi, önemi ve hukuki niteliğine ilişkin görüşler ayrı ayrı alt başlıklarda incelenecektir.

2.1. Tarihsel Süreç İçerisinde Gelişimi

Kişisel verilerin korunmasına ve dolayısıyla bu korumayı sağlayacak hukuki düzenlemelerin oluşturulmasına duyulan ihtiyaç yirminci yüzyılın ortasından itibaren gündeme gelmiş, yapılacak hukuki düzenlemelere dair tartışmalar 1960'lı yıllarda başlamış⁴⁹, ilk hukuki düzenlemeler ise 1970'li yıllarda yapılmıştır⁵⁰. Bu tarihten öncesine gidildiğinde doğrudan kişisel verilerin korunmasını amaç edinen ilke, anlaşma veya hukuki metin bulmak mümkün değildir. Bununla beraber mahremiyetin korunması ve özel hayatın gizliliğinin korunması hakkı ile sır saklamaya ilişkin yükümlülüklerin tarihi çok eskiye dayanmaktadır. Geçmiş zamanlarda kişisel verilerin de mahiyetlerine uygun düştüğü ölçüde bu hakların ve yükümlülüklerin sağladığı hukuki korumanın çatısı altında sınırlı bir korumaya sahip oldukları kabul edilmektedir.

Hipokrat yemininde geçen ve aslen hekimin sır saklama yükümlülüğüne ilişkin olan “...gördüğüm ve duyduğum fakat dışarıda konuşulmayacak olan şeyleri saklayacağım...”⁵¹ ifadesi öğretilerde bu duruma örnek olarak sıkça zikredilmektedir. Gerçekten de günümüzde hassas veriler kategorisinde kabul edilerek korunan sağlık bilgilerinin geçmişte hekimin sır saklama yükümlülüğü kapsamında sınırlı da olsa bir korumaya sahip olduğu anlaşılmaktadır. Bu noktada günümüze kıyasla sınırlı bir korumadan bahsettiğimize dikkat edilmelidir. Öyle ki günümüzde kişisel veri kavramı ortaya çıkmış, bu kavramın kapsayıcılığı sayesinde korunan veri yelpazesi geçmişe nazaran çok daha genişlemiştir. Yine 20nci asırda kişisel verilerin korunması hukukunun müstakil bir alan olarak ortaya

⁴⁹ Küzeci, s.116

⁵⁰ Küzeci, s.117

⁵¹ Altuner, s.4.

ıkması ve gelişmesi ile birlikte veri sahiplerinin bu bilgilerin akıbetini belirleme hususunda sahip olduėu hak ve imkanlar da günden güne artmıřtır. Hangi verilerinin tutulduėunu öğrenme, meřru bir sebebe dayanmadan tutulan verilerin imhasını isteme, yanlış bilgilerin düzeltilmesini talep etme, verilerin kimlerle ve hangi amaçlarla paylaşılabileceėini tayin ve takdir etme gibi haklar bunlardan bazılarıdır.

Kişisel Veri Hukuku'nun ortaya ıkıř dönemine bakıldıėında, bu dönemde kimi Avrupa devletlerinin merkezi veri tabanları oluřturma giriřimleri olduėunu görölmektedir. Bu giriřimler genelde bařarısız olsa da hukukular ve halk nezdinde tehdit algılamasının artmasına sebep olmuřtur. İkinci Dünya Savařının ve diktatörlükler döneminin yeni atlatıldıėı Avrupa'da, bu merkezi veri bankları marifetiyle devletin bireyler karřısında ařırı güçlenmesi ihtimali endişelere sebep olmuřtur. Kişisel veri hukukuna dair yapılan ilk alıřmalarda ve ortaya ıkan ilk kanunlarda bu endişenin tesirini gözlemlemek mümkündür. Verilerin korunması maksadına matuf ilk yasal düzenleme 1970 yılında Almanya'nın Hessen eyaletinde yapılmıřtır. Bu yasanın yapılmasında federe düzeyde bir veri bankasının kurulma alıřmaları etkili olmuřtur. Bu alıřmaların yol atıėı endişeler veri koruma yasasının kabul edilmesine sebep olmuřtur. Almanya'nın Hessen eyaletindeki benzer bir süreç İsve'te yařanmıř ve ulusal düzeydeki ilk Veri Koruma Yasası 1973 yılında İsve'te kabul edilmiřtir. Almanya'da ise ülkenin tamamını kapsayan Veri Koruma Yasası 1977 yılında kabul edilmiřtir⁵².

İlk hukuki düzenlemeler genellikle devletin birey karřısında enformasyon havuzunu kullanarak ařırı güçlenmesini önlemeye ve veri bankalarına iliřkin düzenlemeler getirmeye odaklanmıřtır. İlk düzenlemelerde kayıt dıřı kişisel veri arřivlerinin oluřturulmaması ve kişilerin istedikleri zaman bu verilere eriřerek gerektiėinde düzeltilmelerini talep edebilmeleri gibi bazı haklar güvence altına alınmıřtır. Bununla birlikte ilk dönem düzenlemelerinde bugün kabul edilen bazı haklar yer almamıřtır⁵³.

ok gemeden özel veri bankalarının oluřması ve veri iřleyen aktör sayısının artması ile hakkın kapsamı da genişlemiřtir. Bireylerin sadece devletin kötüye kullanımlarına karřı deėil, veri toplayan özel kişiler ve řirketler bařta olmak üzere bütün aktörlerin kötüye kullanımlarına karřı korunması gerektiėi fikrine ulařılmıřtır. Veriler tek

⁵² Küzeci, s.118

⁵³ Küzeci, s.120

bir aktör (devlet) tarafından değil pek çok aktör tarafından işlenmeye başladığında aktör bazlı düzenlemelerden veri sahibi (birey) bazlı düzenlemelere gidilmesi bir ihtiyaç halini almıştır. Böylece Kişisel Verilerin Korunması Hakkı daha çok özel hayatın gizliliği ve insan hakları bağlamında ele alınmaya başlanmıştır. Bazı Avrupa ülkelerinin anayasalarında özel hayatın gizliliğinin yanında kişisel verilerin korunması hakkı da müstakil bir hak olarak tanınmaya başlanmıştır⁵⁴.

1980’li yıllara gelindiğinde ise kişisel verilerin korunması hakkı verilerin akıbetini tayin etme hakkı olarak anlaşılmaya başlanmıştır. Bu anlayış günümüzde de kabul görmektedir. Buna göre veri sahibi veri işleme sürecinin her aşamasına aktif olarak dahil olmalı ve verilerinin kaydedilmelerinden yok edilmelerine kadar geçecek süreçte tabi tutulacakları her işlem üzerinde aktif rol oynayarak her türlü müdahalede bulunma hakkına sahip olmalıdır⁵⁵. Verilerin akıbetini tayin etme hakkı Alman Anayasa Mahkemesi’nin 1983 yılında verdiği meşhur nüfus sayım kararına dayanmaktadır. Bu karar dünya çapında geniş yankı uyandırmış ve verilerin akıbetini tayin etme hakkı kişisel verilerin korunması öğretinin temel ilkelerinden biri haline gelmiştir⁵⁶.

Teknolojideki gelişmelerle bilginin ulusal sınırlar içerisinde aktarımının yanı sıra uluslararası aktarımı da kolaylaşmış, bilgisayarlar ve internet sayesinde bilgiler uluslararası boyutta otomatik olarak işlenmeye başlamıştır. İnternet ortamında üretilen ve aktarılan verilerin pek çoğu başka bir ülkenin sınırları içerisinde bulunan serverlarda tutulmaya başlanmıştır. Bu gelişmeler dolayısıyla kişisel verilerin korunmasında ulusal düzenlemelerin yetersiz kalacağı düşüncesi 1980’li yıllarda hâkim olmaya başlamış ve ilk uluslararası düzenlemeler bu dönemde yapılmaya başlanmıştır. Uluslararası düzenlemeler genel olarak uluslararası ticari ilişkilerin sürdürülebilirliğini sağlamayı ve taraf devletleri iç hukuk düzenlemeleri yaparak kişisel verilerin korunması hukukundaki gelişmelere ayak uydurmaya zorlamayı amaçlamıştır. Çünkü hiçbir ülkenin hukuk düzeninin kendi sınırları dışarısında meydana gelecek bir hukuka aykırılıkla etkin mücadele etmeye tek başına yetemeyeceği açıktır. Bu noktada uluslararası yardımlaşma ve ihlallerle kolektif mücadele son derece önemlidir. Bu düşüncelerle yapılan uluslararası girişimler ve bu girişimlerin muhtevaları ilerleyen başlıklarda müstakil olarak ele alınacaktır.

⁵⁴ 1976 Portekiz Anayasası, İspanya Anayasası, İsveç, Avusturya ve Macaristan anayasaları bunlara örnek olarak zikredilmektedir. Bkz. **Küzeci**, s.121-122.

⁵⁵ **Küzeci**, s.123

⁵⁶ **Aksoy**, s.97.

2.2. Önemi

Kişisel verilerin korunması eski çağlardan buyana süregelen bir ihtiyaç olmakla beraber son yüzyılda dünyamızın uğradığı değişim kişisel verilerin korunmasının önemini büyük oranda artırmıştır. Dünyanın değişime uğramasında baş etkenin teknolojik gelişmeler olduğu rahatlıkla söylenebilir. Teknolojik gelişmeler her zaman toplumların yaşamını derinden etkilemiştir. Örneğin makinelerin icadı ve yaygınlaşması tarım toplumundan sanayi toplumuna geçişe sebep olmuştur. Sanayi toplumuna geçiş ile değişen ekonomik sistemin sosyal yapıya ve hukuk düzenine de büyük etkileri olmuştur. Yeni toplumsal düzen sosyal bilimler alanında da yepyeni meseleleri gündeme getirmiştir. İşçi ve işveren sınıfı arasındaki çekişme, makinelerin mülkiyeti, işçi hakları gibi pek çok konu sosyal bilimler alanında tartışılmaya başlanmıştır. Tıpkı bunun gibi bilgi iletişim teknolojilerinde yaşanan gelişmeler de sanayi toplumundan bilgi toplumuna geçişin en önemli tetikleyicisi olmuştur. Bilgi iletişim teknolojilerinin gelişmesi ile bilgi daha kolay toplanabilir, tasnif edilebilir, aktarılabilir, ulaşılabilir ve dolayısıyla daha kolay kullanılabilir hale gelmiştir. Bilginin sanayi toplumuna nazaran çok daha fazla kullanıldığı, üretimin en önemli unsurlarından biri haline geldiği ve gücün kaynağı olarak görülmeye başlandığı yeni toplumsal düzen bilgi toplumu olarak isimlendirilmeye başlanmıştır.

Bilginin gücün kaynağı olarak görülmesinin sebebini iki ayrı temelde ele alabiliriz. Birincisi; bilgi hem bilim ve teknoloji alanındaki hem de sosyal bilimler alanındaki gelişimin ve ilerlemenin en önemli yapı taşı olarak görülmektedir. Dolayısıyla bilim, teknoloji ve sosyal bilimler alanlarında gelişen bireylerin ve ülkelerin diğer bireylere ve ülkelere nazaran daha güçlü olacağına duyulan inanç bilginin güç unsuru olarak kabul edilmesine sebep olmuştur. İkincisi; bir kişi hakkında sahip olunan bilgi, o kişiyi tanımak, yönetmek ve yönlendirmek hususlarında bilgi sahibine bir güç sağlamaktadır. Tarih boyunca hem kişiler hem de devletler bu güce sahip olmak istemiştir. İstihbarat teşkilatları bu maksatla kurulmuştur.

Bilginin bir güç aracı olarak görülmesi yeni olmasa da en önemli güç unsuru olarak kabul edilmeye başlanması bilgi toplumuna geçiş ile olmuştur. Bilginin toplanması, aktarılması, depolanması ve kullanılmasının bu denli kolaylaşması eskisine nazaran çok

daha fazla bilginin kullanılmasına imkân sağlamış, daha fazla bilgi ise daha fazla güç anlamına geleceği için bilgi en önemli güç unsuru olarak kabul edilmeye başlanmıştır⁵⁷.

Bilgi iletişim teknolojilerinde büyük ilerleme kaydedilmesini takip eden ilk zamanlarda beklentiler insanların daha fazla özgürleşeceği, merkezi otoritelerin ve güç odaklarının zayıflayacağı yönünde olmuştur. İnsanların bilgiye erişimlerinin kolaylaşması, birbirleri ile daha kolay iletişim kurabilmeleri, bilgi iletişim vasıtalarının çeşitlenmesi ile bu vasıtalar üzerindeki devlet denetiminin zayıflaması gibi hususların kısmen bireylerin özgürleşmesine ortam sağladığı kabul edilebilir. Ancak bu süreçte hayatın her alanını kuşatan bilgi iletişim araçlarının birer gözetim aracına dönüşmesi beklenenin tam aksi bir netice doğurmuş ve gözetim toplumu adı verilen yeni bir toplumsal düzenin kapısı aralanmıştır⁵⁸. George Orwell'ın 1984 isimli romanında tasvir ettiği distopyanın elektronik gözetim araçları sayesinde gerçeğe dönüştüğü bir dünyaya işaret eden gözetim toplumu kavramı ilk olarak 1985'te Gary T. Marx tarafından kullanılmıştır⁵⁹. Gözetim toplumunun insanları, yaptıkları alışverişlerde, kurdukları iletişimlerde, daha doğrusu attıkları her adımda arkalarında dijital izler bırakan ve bu izler sayesinde teknolojik gücü elinde bulunduran büyük şirketler ve devletler tarafından her hareketleri takip edilebilen birer obje olarak tasvir edilmiştir. 1990'larda yapılan bu tasvirlerin ne kadar yerinde olduğu gün geçtikçe daha iyi anlaşılmıştır. Gerçekten de bugün neredeyse her cadde ve sokakta mobese ve güvenlik kameralarının bulunduğu, telefonlarımızdaki GPS sayesinde konumumuzun anlık olarak bilinebildiği, bütün alışveriş ve para transferi bilgilerimizin bankalarca saklandığı, telefon ve bilgisayar kullanarak yaptığımız her işlemin çerezler ve loglar vasıtasıyla teknoloji şirketleri ile paylaşıldığı bir dünyada yaşıyoruz. Her birimiz hayatımızı saran siber ağda attığımız her adımın kolaylıkla takip edilebilir ve kaydedilebilir olduğunun farkındayız.

Hareketlerinin takip edildiği veya en azından takip edilebilir olduğu duygusu ile yaşayan bir insanın kişiliğini özgürce gerçekleştirmesi neredeyse imkansızdır. Hakkında nerede ne kadar bilgi toplandığını bilmeyen, bu bilgilerin bir şekilde karşısına çıkarılarak

⁵⁷ Etraflı bir anlatım için bkz. **Tekgöl, Ahmet Tamer** (1997) Bilgi Toplumu ve İnternet (Yüksek Lisans), İstanbul Üniversitesi Sosyal Bilimler Enstitüsü.

⁵⁸ **Dolgun, Uğur** (2004) 'Gözetim Toplumu'nun Yükselişi: Enformasyon Toplumundan Gözetim Toplumu' Yönetim Bilimleri Dergisi, C:2, S:1, (s.55-74).

⁵⁹ **Üstün, Ezgi** (2020) Gözetim Toplumu Olgusunun Sosyal Medya Bağlamında Değerlendirilmesi (Yüksek Lisans), Pamukkale Üniversitesi Sosyal Bilimler Enstitüsü, s.60. Ayrıca bkz. **Lyon, David** (1994) The Electronic Eye, Cambridge, Polity Press, s.9.

kendisi aleyhinde kullanılmayacağından emin olamayan insanın özgürlüğü kısıtlanmış demektir. İşte tam da burada; attığımız her adımın takip edilme ve kaydedilme riski bulunan bir dünyada, kişisel verilerimizin etkin bir şekilde korunması son derece büyük önem arz etmektedir. Veri toplamanın kolaylaşması, toplanan veri sayısının artması ve siber ağın git gide hayatın daha fazla alanını kuşatması kişisel verilerimizin ihlal edilme riskini de artırmakta, bu riskin arttığı oranda kişisel verilerin korumasının önemi de artmaktadır.

Verilerinin korunması hakkındaki beklentisi kişinin mahremiyet alanını koruma hassasiyetinden doğabileceği gibi mahremiyet alanının ihlali dışında başka mağduriyetlere uğrama korkusundan da kaynaklanabilir. Zira bilgilerinin rızası olmadan başkaları tarafından kullanılması durumunda veri sahibinin pek çok açıdan mağdur olabilmesi mümkündür. Bilginin kişinin özel hayatına ilişkin olması durumunda özel hayatın gizliliği ihlal edilmiş olur. Yine kimlik bilgileri ele geçirilen bir kişinin rızası ve bilgisi olmadan bazı sözleşmelerin tarafı haline getirilmesi ve bu suretle kişinin hukuki ve ekonomik olarak pek çok yükün altına sokulması mümkündür. Böylesi bir durumda kişinin özel alanına ilişkin bir bilgi kullanılmış olmakla birlikte bu bilginin kullanılması sonucunda sadece özel alanı ihlal edilmekle kalmamış, bunun yanı sıra malvarlığı hakları da tehlikeye düşürülmüş olur. Kişisel verilerin hukuka aykırı olarak kullanılması neticesinde çok çeşitli mağduriyetlerin meydana gelebilecek olması bu verilerin korumasının önemini artıran hususlardan biridir.

2.3. Hukuki Niteliğine İlişkin Görüşler

Kişisel verilerin korunması hakkının ortaya çıktığı dönemden bugüne bu hakkın hukuki niteliği üzerinde tartışılmış ve farklı fikirler öne sürülmüştür. Hakkın hukuki niteliğinin belirlenmesi hakkın korunmasına ilişkin hukuki rejimin ve hakkı korurken kullanılacak hukuki yolların belirlenmesi bakımından son derece önemlidir. Kişisel verilerin korunması hakkının hukuki niteliğine ilişkin yaklaşımların hakkın kapsamının genişlemesinde ve içeriğinin gelişmesinde de yol gösterici bir rolünün olduğu söylenebilir.

Kişisel verilerin korunması hakkının hukuki niteliğine ilişkin görüşler ekonomik hak görüşü ve kişilik hakkı görüşü olmak üzere temelde ikiye ayrılmaktadır. Amerika Birleşik Devletleri'nde daha çok ekonomik hak anlayışı benimsenirken Kıta Avrupası'nda ve ülkemizde kişilik hakkı anlayışı benimsenmektedir.

2.3.1. Ekonomik Hak Görüşü

Ekonomik hak yaklaşımını benimseyenlerin kendi içinde iki farklı görüşe sahip oldukları söylenebilir. Bunlar mülkiyet hakkı görüşü ve fikri mülkiyet hakkı görüşüdür. Mülkiyet hakkı veya fikri mülkiyet hakkı görüşünü savunan yazarların ortak noktaları kişisel verilerin ekonomik bir değere haiz olduğunu kabul etmeleridir. Gerçekten de bilgi toplumuna geçiş ile birlikte bilginin en önemli ekonomik değer unsurlarından biri haline geldiği yadsınamaz. Kişisel veriler de bu dönemde önemi ve değeri artan, ekonomik değer kazanan bilgi türlerinden birisidir. Ekonomik hak yaklaşımını benimseyenlere göre kişisel verileri en iyi şekilde korumak verilerin günümüz piyasasında ekonomik bir değeri olduğunu göz ardı etmeyerek bu ekonomik değeri korumaya yönelik yaklaşımlar geliştirmek ile mümkündür.

Bilhassa özel şirketlerin sahip oldukları verileri pazarlama alanında etkin şekilde kullanarak bunlardan ekonomik bir değer üretmeleri kişisel verilerin ekonomik bir değer olarak görülmeye başlanmasında etkili olmuştur. İkinci Dünya Savaşının akabinde veriler genellikle devletler tarafından kamu hizmetlerinin yürütülmesi ve güvenlik maksatlarıyla işlenirken; ilerleyen süreçte şirketlerin kişisel verileri toplamak, kaydetmek ve işlemek bakımından gelişmiş teknolojiler kullanmaya başlamaları, devasa veri havuzları oluşturmaları, bu verileri yeri geldiğinde kendi ekonomik menfaatleri için kullanmaları, zaman zaman da başka şirketlere ücret karşılığı satmaları, kişisel verileri daha çok ekonomik kaygılarla işlenir hale getirmiştir. Bu gelişmeler ışığında ABD'de ve bazı ülkelerde veri sahibinin veriler üzerindeki hakkının ekonomik bir hak olduğunu varsaymanın bu verileri korumak için en etkili yol olacağı düşüncesi gelişmiştir. Aslında Amerikan Hukuku'nda da kişisel verilerin pek çok yazar tarafından özel hayatın gizliliği başlığı altında değerlendirildiği ve kişisel verileri korumakla özel hayatı koruma amacı güdüldüğü görülmektedir. Mülkiyet hakkı görüşünü savunanlar kişisel verilerin hayatın

özel alanı ile ilgisini kabul etmekte, fakat bu özel alanı korumak için en etkili yolun kişilere veriler üzerinde mülkiyet hakkı tanımak olduğunu savunmaktadırlar⁶⁰.

Ekonomik hak yaklaşımını benimseyenlere göre bu düşünce kabul edildiğinde verileri toplamak ve işlemek isteyen şirketler veri sahibinin talep ettiği bedeli ödemeyi göze almak zorunda kalacaktır. Bu sayede veri pazarının daha adil işleyeceği düşünülmektedir. Bunun yanı sıra bir karşılık ödeme yükümlülüğü şirketleri daha az veri işlemeye zorlayacaktır. Ayrıca veri sahiplerinin verilerini devretmek istememe hakları olduğu kadar bir ivaz karşılığında devredebilme hakları da olmalıdır⁶¹.

Ekonomik hak görüşünün eleştirildiği yönler de bulunmaktadır. Bu görüşü benimsemeyen yazarlar bireylerin özel şirketler karşısında pazarlık güçlerinin zayıf olduğunu, adil bir pazarlık gerçekleşmemesi durumunda mağdur olabileceklerini, dolayısıyla bireylere böyle bir hak tanımanın onlara yarardan çok zarar getirebileceğini söylemişlerdir. Bu yaklaşımın ekonomik zorluklar yaşayan veri sahiplerini verilerini korumak hususunda dezavantajlı bırakacağı, ekonomik güç sahibi şirketleri ise avantajlı bir konuma yükselteceği ifade edilmiştir. Ayrıca kişisel verilerin insanın bir ürünü değil uzantısı olduğu, bu sebeple verileri metalaştırmanın insan onuru ile bağdaşmayacağı vurgulanmıştır⁶².

Ekonomik hak yaklaşımının (bilhassa mülkiyet hakkı yaklaşımının) doğurabileceği en büyük sorunlardan biri de verilerini satan kişinin verileri üzerinde hiçbir hak iddia edemez duruma gelecek olması, satın alan kişinin ise bu veriler üzerinde mutlak bir yetkiye sahip olmasıdır. Satın alan kişinin mülkiyetine geçirdiği malı (verileri) dilediği gibi kullanma hakkının olması satım ilişkisinin doğal sonucudur. Fakat bu verilerin kullanımı sonucunda verilerin ilgili bulunduğu kişi hakkında olumsuz neticeler doğması her zaman mümkündür. Bu durumda satın alan kişinin mülkiyete bağlı kullanma ve tasarruf hakkı ile ilgili kişinin kişiliğinin ve özel hayatının korunması hakkı karşı karşıya gelecektir. Böylesi durumlarda menfaatler dengesinin nasıl kurulacağı konusu önemli bir soru işaretidir. Bunun yanı sıra veriler satın alanın mülkiyet alanına geçtiği için ilgili kişinin, verilerinin hangi maksatla kullanıldığını denetlemesi da neredeyse imkânsız hale gelecektir

⁶⁰ **Küzeci**, s.68.

⁶¹ **Küzeci**, s.69.

⁶² **Akkurt, Sinan Sami** (2020) 'Kişisel Veri Kavramının Hukuki Niteliğine İlişkin Yaklaşımlara Mukayeseli Bir Bakış' *Kişisel Verileri Koruma Dergisi*, C:2, S:1, (s.20-32), s. 23, ayrıca bkz. **Küzeci**, sf.70

2.3.1.1. Ekonomik Hak – Mülkiyet Hakkı Görüşü

Mülkiyet hakkı görüşünü savunanlara göre kişisel veriler veri sahibinin kişiliğinin bir uzantısı olmakla beraber aynı zamanda veri sahibinin bir ürünüdür⁶³. Veri sahibinin bu ürünler (veriler) üzerinde bir mülkiyet hakkı⁶⁴ olduğu kabul edilmelidir. Mülkiyet hakkı niteliği itibariyle aynî bir haktır. Herkese karşı ileri sürülebilir. Mülkiyet hakkının bu özelliği veri sahibinin haklarını herkese karşı kullanabilmesini sağlayacaktır. Mülkiyet hakkı, sahibine kullanma, yararlanma ve tasarrufta bulunma yetkisi verir. Buna göre veri sahibi kişisel verileri üzerinde istediği gibi tasarrufta bulunabilir. Verilerini kullanma hakkını bir ivaz karşılığında veya karşılıksız olarak üçüncü bir kişiye devredebilir. Üçüncü kişilere verdiği bu kullanım hakkının süresini dilediği gibi belirleyebilir, kullanım amacını tahsis edebilir ve belirli bir konuyla sınırlandırabilir. Veri sahibi kişisel verilerini satabilir, kiralayabilir veya bağışlayabilir. Bunlar mülkiyet hakkının içerisinde yer alan eşya üzerinde dilediği gibi tasarrufta bulunma hakkının doğal sonuçlarıdır.

Bu yaklaşım mülkiyet hakkının niteliği itibariyle kişisel verilere uygun düşmediği, mülkiyet hakkının sağladığı başvuru yollarının kişisel veriler bakımından kullanılmasının mümkün olmadığı gerekçeleriyle eleştirilmiştir. Gerçekten de Türk Hukuku bakımından bir değerlendirme yapmak gerekirse mülkiyet hakkının ihlali durumunda hak sahibine tanınan başvuru imkanları kişisel verilerin korunması amacına hizmet etme kabiliyetinden yoksundur. Bir veri ihlali durumunda bu ihlali önlemek için el atmanın önlenmesi davası, istihkak davası veya taşınır davası açmak kişisel verilerin niteliği ve dolayısıyla kişisel verilerin korunması hukukunun maksadı ile bağdaşmayacak, hakkın etkin şekilde korunmasına hizmet edemeyecektir⁶⁵.

⁶³ Aksoy, s.78.

⁶⁴ Mülkiyet hakkı esasen eşya hukukunun konusudur. Eşya hukukunun konusunu eşyalar oluşturur. Genel kabule göre eşya; üzerinde fiili ve hukuki hakimiyet kurulabilen, cismani ve sınırlandırılmış şeylerdir. Bu tanıma göre kişisel veriler eşya hukukundaki eşya tanımının kapsamına girmemektedir. Zira verilerin cismani bir varlığından söz edilemez. Ancak ekonomik hak yaklaşımını benimseyenlere göre kişisel veriler de eşya kavramı içerisinde değerlendirilmelidir.

⁶⁵ Akkurt, Kişisel Veri ..., s.23

2.3.1.2. Ekonomik Hak – Fikri Mülkiyet Hakkı Görüşü

Kişisel verileri ekonomik bir hak olarak kabul eden bir kısım yazarlar onun mülkiyet hakkı çerçevesinde değil fakat fikri mülkiyet hakkı çerçevesinde korunabileceği görüşüne sahiptir. Bu görüşün temelinde fikri eserler ile kişisel veriler arasında birtakım benzerlikler bulunduğu düşüncesi yatmaktadır. Hem fikir eserlerinin hem de kişisel verilerin somut bir varlıklarının bulunmaması bu benzerliklerin başında gelmektedir. Ayrıca her iki konu bakımından da ihlaller teknolojik gelişmelerle artmıştır ve genellikle internet vasıtasıyla gerçekleşmektedir. Bu benzerlikler göz önünde bulundurularak fikri mülkiyet hakkının kişisel verilerin niteliğine daha uygun düştüğü ve kişisel verilerin fikri mülkiyet hukuku yoluyla korunabileceği ifade edilmiştir.

Fikrî eserlerin korunmasındaki hedeflerden birisi de bunların kontrolsüz şekilde yayılmasını ve kullanılmasını önlemektir. Bu hedef kişisel verilerin korunması bakımından da benimsenmektedir. Kişisel verilerin de kontrol dışı yayılması ve kullanılması veri sahibinin mağduriyetine yol açmaktadır ve engellenmelidir. Ancak hemen belirtmekte fayda var ki kişisel verilerin hukuka aykırı olarak yayılması ve kullanılması durumlarında veri sahibi kişilik haklarının ihlal edilmesi ve insan onurunun zedelenmesi gibi zararlarla karşılaşacakken fikir eserleri açısından durum böyle değildir. Fikir eserlerinin izinsiz şekilde yayılması ve kullanılması durumlarında eser sahibi daha çok ekonomik bir mağduriyet yaşamaktadır. Dolayısıyla kişisel verilerin korunmasında temel maksat kişilik haklarını ve insan onurunu korumakken, fikri mülkiyetin korunmasında maksat ekonomik menfaatin ihlal edilmesini önlemektir. Farklı hukuki değerleri korumaya odaklanan bu iki hakkın bazı benzerlikler taşımaları sebebiyle aynı hukuki rejime tabi tutulmaları sağlıklı sonuçlar vermeyecektir⁶⁶.

Fikri mülkiyet hakkı bazı nitelikleri itibariyle de kişisel verilerin korunması hakkı ile bağdaşmamaktadır. Örneğin fikri mülkiyet hakkının tanıdığı koruma ülke hudutları ile sınırlıdır. Fikri mülkiyet hakkı hangi ülkede korunmak isteniyorsa hakkın o ülkede tescili kural olarak zorunludur⁶⁷. Kişisel verilerin korunması için ise tescile ihtiyaç olmadığı gibi

⁶⁶ Akkurt, Kişisel Veri ..., s.24-25

⁶⁷ Suluk, Cahit / Karasu, Rauf / Nal, Temel (2021) Fikri Mülkiyet Hukuku, 5. Baskı, Ankara, Seçkin, s. 2.

koruma alanı ülke hudutları ile sınırlı da değildir. Yine fikri mülkiyet hakları süreye tabi iken⁶⁸ kişisel verilerin korunması hakkı süreye tabi değildir.

2.3.2. Temel İnsan Hakkı ve Kişilik Hakkı Görüşü

Kıta Avrupası'nda benimsenen genel görüşe göre kişisel verilerin korunması hakkı kişinin şahıs varlığı ile doğrudan bağlantılı, sırf insan olması sebebiyle kazandığı temel insan hakları arasındadır. Bugün pek çok ülkede kişisel verilerin korunması hakkı müstakil bir anayasal düzenlemeyle korunmakta ve temel insan haklarından kabul edilmektedir. Kişisel verilerin korunması hakkının temelde insan onurunu ve bununla bağlantılı olarak insanın varlığını özgürce geliştirme hakkı ile özel yaşamın gizliliği hakkını koruduğu söylenebilir. Bunların yanı sıra yerine göre kişilerin sahip oldukları din ve vicdan hürriyeti, düşünce hürriyeti gibi diğer pek çok temel hak da kişisel verilerin korunması ile dolaylı yoldan korunabilmektedir. Kişisel verilerin insanın kişisel varlığının bir uzantısı olarak kabul edilmesi ve kişisel verilerin kullanılarak temel insan haklarının çok çeşitli şekillerde ihlal edilebilecek olması kişisel verilerin hukuk düzeni tarafından başlı başına bir kişisel değer olarak tanınmasına yol açmıştır. Kişisel verilerin korunmasının kişinin bizzat kendisinin korunması anlamına geleceği düşüncesi, kişisel verilerin korunması hakkının temel bir insan hakkı olarak kabul edilmesinde önemli rol oynamıştır⁶⁹.

Kişisel verilerin korunması hakkının müstakil bir temel insan hakkı olarak tanındığı yakın zamanlara gelene kadar bu hak özel hayatın gizliliği hakkı bağlamında değerlendirilmiştir. Kişisel verilerin korunması hakkı özel hayatın gizliliği hakkının bir alt başlığı olarak görülmüş, öğreti ve uygulama bu doğrultuda şekillenmiştir. Özel hayat kavramı sınırları keskin hatlarla belirli olmayan, sınırlayıcı bir tanım getirilemeyen, aslında sınırlayıcı bir tanım yapmaktan hukukçuların iradi olarak kaçındıkları bir kavramdır⁷⁰. Kişinin kimliği, onur ve şöhreti, fiziksel ve psikolojik bütünlüğü, cinsel hayatı ve kişisel

⁶⁸ **Suluk / Karasu / Nal**, s.2.

⁶⁹ **Bilir, Faruk** (2021) 'Kişisel Verilerin Korunması Kişinin Kendisinin Korunmasıdır' TRT Akademi Dergisi, C:6, S:11, (s.172-181)

⁷⁰ AIHM'de kararlarında özel hayat kavramını somut olayda ele alınan konu penceresinden değerlendirmiş ve pek çok farklı konunun özel hayat kavramı içerisine girebileceğine hükmetmiştir. AIHM'e göre özel hayat kavramı ayrıntılı tanımlamaya elverişli olmayan geniş bir terimdir. "*Private life is a broad term not susceptible to exhaustive definition.*" bkz. CASE OF P.G. AND J.H. v. THE UNITED KINGDOM, 25/12/2001, (<https://hudoc.echr.coe.int/eng?i=001-59665>) s.e.t. 17.01.2023

verileri gibi pek çok konu özel hayat kavramı çerçevesinde değerlendirilmektedir. Avrupa İnsan Hakları Mahkemesi (AİHM) de Avrupa İnsan Hakları Sözleşmesi'nin (AİHS) “*Özel ve Aile Hayatına Saygı*” başlığını taşıyan ve özel hayatın gizliliği hakkını düzenleyen 8inci maddesine getirdiği yorum ile kişisel verilerin bu madde çerçevesinde korunabileceğine hükmetmiştir. AİHM'ne benzer şekilde BM İnsan Hakları Komitesi de kişisel verilerin korunması hakkının BM Medeni ve Siyasal Haklar Sözleşmesi'nin özel hayatın gizliliğini düzenleyen 17. Maddesi kapsamında değerlendirilmesi gerektiğini 1988 yılında yayınlanan 16 numaralı genel yorumunda ifade etmiştir⁷¹.

Kişisel verilerin korunması ile korunan en temel alanlardan biri şüphesiz kişinin özel hayat alanıdır. Ancak kişisel verilerin korunması hakkını özel hayatın gizliliği başlığı altında değerlendiren görüş bazı durumları açıklamakta yetersiz kalması sebebiyle eleştirilmiştir. Kişisel veri hukukunun bugünkü kabullerine göre kişisel veriden söz edebilmek için verilerin kişinin özel hayat alanına ilişkin olması gerekmez. Günümüzde kabul gören kişisel veri tanımında “*özel hayat alanına ilişkin olma*” gibi bir şart yoktur. Bir verinin kişisel veri kabul edilebilmesi ve korunması için o verinin hukuka aykırı şekilde kullanılması durumunda kişinin mahremiyetine hâle gelip gelmeyeceği araştırılmamaktadır. Kişinin bizzat kendisi tarafından alenileştiren verileri kişisel veri olma özelliğini kaybetmemektedir. Sosyal medya profilinde kişinin isminin ve fotoğrafının herkese açık şekilde yer alması kişinin ismini ve fotoğrafını kişisel veri olmaktan çıkarmayacaktır. Keza bir konferansın katılım listesine imza atan kişinin listeyi gören herkese imzasını alenileştirdiği gerekçesiyle imzası kişisel veri olmaktan çıkarılamayacaktır. Yine kişinin kamuya açık şekilde düzenlenen toplantılara, gösteri yürüyüşlerine veya sendikal faaliyetlere katılması durumunda bu katılım bilgilerinin üçüncü kişiler tarafından kaydedilmesi halinde kişisel veri ihlalden söz edilecektir. Bu bilgilerin kamuya açık olmaları, başka bir deyişle özel hayat alanına ilişkin olmamaları onların isteyen herkes tarafından kaydedilebilecekleri veya kullanılabilecekleri anlamına gelmez.

Kişilerin kamuya açık verilerinin özel hayat kavramı içerisinde değerlendirilmesi ve bu suretle korunması kısmen de olsa mümkündür. Zira özel hayat kavramını açıklayan teorilerden en fazla benimsenen üç alan teorisine göre kişilerin kamusal alandaki

⁷¹ **UN Human Rights Committee** (1988) General Comment No 16 § 10 (BM İnsan Hakları Komitesi (1988) Genel Yorum No 16, § 10.)

yaşamlarının da özel hayatın gizliliği hakkı kapsamında korunması kimi durumlarda mümkündür. Kamusal alanda gerçekleşen olayların özel hayatın gizliliği hakkı kapsamına girip girmeyeceğinin kişinin bu hususu topluma açma iradesine göre belirlenmesi gerektiği kabul edilmektedir⁷². Şayet kişisel verilerin özel hayatın gizliliği hakkı çerçevesinde korunması anlayışı benimsenirse kişisel verilerin özel hayat alanına dahil olup olmadığının bu kriter göz önünde bulundurularak her olay açısından ayrı ayrı değerlendirilmesi gerekecektir. Bu ise kimi durumların kapsam dışında kalmasına yol açacaktır.

Kişisel verilerin korunması hukukunun gelişiminde en önemli dönüm noktası Alman Anayasa Mahkemesi'nin 1983 tarihli ünlü nüfus sayım kararıdır. Bu kararda mahkeme ilk kez *enformasyonel self-determinasyon* tabirini kullanmıştır⁷³. Buna göre herkes bilgilerinin geleceğini belirleme hakkına sahiptir. Kararda mahkeme verilerin geleceğini belirleme hakkının kişinin şahsiyetini özgürce geliştirme hakkı, özgür karar alma hakkı, ifade özgürlüğü ve seçme hakkı gibi pek çok hakkını garanti altına alacağını ifade etmiştir. Kendisi hakkında hangi verilerin nerede kim tarafından ne kadar saklandığını bilmeyen, bunlar üzerinde denetim ve kontrol hakkını kullanamayan bir kişinin kişiliğini özgürce geliştiremeyeceği şüphesizdir. Böylesi bir insan herhangi bir girişimde bulunacağında, siyasi veya sosyal bir ilişki geliştireceğinde, hep bir tedirginlik içerisinde olacaktır⁷⁴. Bu da kişinin sadece özel hayatın gizliliği hakkının ihlali neticesini değil, pek çok temel insan hakkını kullanamayarak onlardan mahrum kalması neticesini doğurur. Dolayısıyla Alman Anayasa Mahkemesi'nin nüfus sayım kararı bilgilerin akıbetini tayin etmek şeklinde özetlenen, hangi verilerin saklandığını ve hangi işlemlere tabi tutulduğunu öğrenme, verilerin silinmesini veya düzeltilmesini talep etme, verilerin kimlerle paylaşıldığını öğrenme gibi bugün veri sahiplerinin sahip olduğu pek çok hakkın temelini oluşturmaktadır. Bu kararın kişisel verilerin korunması hakkının özel hayatın gizliliği hakkı şemsiyesinden çıkarak müstakil bir hak olarak tanınması yolunda da bu yönleriyle etkili olduğu söylenebilir.

Özel hayatın gizliliği hakkı ile kişisel verilerin korunması hakkı birbiri ile yakın ilişkili haklar olmalarına rağmen her iki hakkın bugün geldiği konum itibarıyla bu hakları korumaya yönelik enstrümanlar birbirleriyle tam bir örtüşme içerisinde değildir. Öyle ki

⁷² Aktaş, Batuhan (2017) Özel Hayatın Gizliliğini İhlal Suçu, İstanbul, Der Yayınları, s.40.

⁷³ Yılmaz, Berrak (2019) Türk Anayasa Mahkemesi ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması (Doktora), Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü, s.120.

⁷⁴ Küzeci, s.76-77.

kişisel verilerin korunmasına ilişkin usul ve esasların düzenlendiği müstakil kanunlar kabul edilmiş bu kanunlarla veri koruma kurumları kurulmuştur. Bu kurumlar gerektiğinde ihlallere karşı idari yaptırım uygulama hakkına sahiptir. Mademki kişisel verilerin korunması hukuku kendisine has pek çok özelliği ve enstrümanı barındırmaktadır; öyleyse kişisel verilerin korunması hakkının, diğer temel haklarla ilişkili fakat müstakil varlığa sahip temel bir insan hakkı olduğunu kabul etmek gerekmektedir. AİHS'ne nazaran daha yeni bir metin olan, Avrupa Birliği tarafından hazırlanarak 2000 yılında ilan edilen Avrupa Birliği Temel Haklar Bildirgesi'nde kişisel verilerin korunması hakkı müstakil bir şekilde yer almaktadır⁷⁵. Bu durum kişisel verilerin korunması hukukunun gelişmesi ve kapsamının genişlemesi ile birlikte bu hakkın özel hayatın gizliliği hakkından bağımsız olarak tanınmaya başladığının tipik bir örneğidir.

Kişisel verilerin hukuki statüsünü açıklamada sıklıkla kullanılan bir diğer kavram kişilik hakkı kavramıdır. Aslında kişilik hakkı ve insan hakkı kavramları birbirinden tamamen bağımsız kavramlar değildir. Bu kavramlar arasında çok yakın ilişki bulunmaktadır. İnsan hakkı kavramı daha genel ve üst bir ideali ifade ederken kişilik hakkı kavramı anayasal hükümlerde korunmakla beraber daha çok medeni hukuk alanı içerisinde somutlaşır ve kişinin şahıs varlığına bağlı bazı insan haklarının toplu bir görünümünü ifade eder⁷⁶. Daha somut bir biçimde anlatmak gerekirse yaşam hakkı, maddi ve manevi varlığı koruma ve geliştirme hakkı ve özel yaşamın gizliliği hakkı gibi temel bazı insan hakları bir araya gelerek kişilik hakkını oluşturur. Kişilik hakları şahıs varlığı haklarındandır. Para ile ölçülemez, devredilemez.

Kişilik hakkı kavramını sınırlayıcı bir tanım ile ifade etmek doğru görülmemektedir. Çünkü kavramın muhtevası sürekli gelişmekte ve genişlemektedir. Ne anayasada ne de medeni kanunda kişilik hakkı kavramı net bir şekilde tanımlanmamıştır⁷⁷. Eğer mutlaka bir tanım yapmak gerekirse kişilik hakkı insanın sahip olduğu kişisel

⁷⁵ Yedinci madde özel ve aile hayatına saygıyı düzenlerken, sekizinci madde kişisel verilerin korunması hakkını düzenlemektedir. Metnin tamamı için bkz. (http://www.ceidizleme.org/ekutuphaneresim/dosya/687_1.pdf) s.e.t. 17.01.2023.

⁷⁶ İnsan hakkı ve kişilik hakkı kavramları arasındaki ilişkiye dair farklı görüşler için bkz. **Akkurt, Sinan Sami** (2020) Sosyal Medyada Gerçekleşen İhlaller Karşısında Kişilik Hakkının Korunması, 2. Baskı, Ankara, Seçkin, s.35.

⁷⁷ **Baskın, Onur** (2021) Türk Hukuku Bakımından Kişilik Hakkı Kapsamında Kişisel Verilerin Korunması, 1. Baskı, Ankara, Seçkin, s.68.

değerleri üzerindeki hakkı olarak ifadelendirilebilir⁷⁸. Bu kişisel değerler sabit ve sınırlı değildir. Zamanla değişebilir, yenileri eklenebilir veya var olanların sınırlarına ilişkin yeni yorumlar getirilebilir. Öğretide kişinin yaşam, sağlık, özgürlükler, şeref ve haysiyet, özel yaşam, kişinin adı ve resmi gibi kişisel varlıkları kişilik hakkı kapsamında değerlendirilmektedir⁷⁹. Türk Medeni Kanunu'nun 23, 24 ve 25inci maddelerinde kişilik hakkının korunmasına ilişkin genel hükümler ve genel başvuru yolları yer almaktadır. Kişilik hakları medeni hukuk bakımından bu genel hükümler vasıtasıyla korunmaktadır. Kişilik hakkı içerisinde müstakil bir kişisel değer olarak kabul edilen bazı hakları korumak için ise bu genel hükümlerin yanında bazı özel düzenlemeler yer almaktadır. Örneğin kişilik hakkı içerisinde yer alan adın korunması hakkı genel hükümlerin yanı sıra kanunun 26 ve 27nci maddelerindeki özel düzenlemeler ile de korunmaktadır⁸⁰. Bu kişisel değerler sadece medeni hukuk açısından değil ceza hukuku açısından da farklı özel düzenlemeler ile korunmaktadır.

Kişisel verilerin kişilik hakkı kapsamında korunması görüşü iki farklı fraksiyonu barındırmaktadır. Bunlar klasik kişilik hakkı görüşü ve yeni kişilik hakkı görüşüdür. Klasik kişilik hakkı görüşüne göre kişisel veriler kişilik hakkı içerisinde özel yaşamın gizliliği kapsamında korunmalıdır. Konuya veri mahremiyetinin korunması perspektifinden yaklaşan klasik görüş, kişinin özel hayat alanına ilişkin olmayan verileri veya kişi hakkındaki yanlış verileri kapsam dışında bırakması sebebiyle eleştirilmiştir⁸¹. Kişisel verilerin temel insan haklarından özel hayatın gizliliği hakkı bağlamında değerlendirilmesine karşı yapılan eleştirilere yukarıda değinmiştik. Aynı eleştiriler burada da geçerlidir. Ayrıca klasik kişilik hakkı görüşüne karşı çıkanların bir diğer gerekçesi kişisel verilerin de kendine özgü nitelikleri bulunduğu, bu hakkın korunmasının ancak hakkın niteliğine uygun özel hukuki düzenlemeler yapılması ile mümkün olduğu fikridir. Bu sebeple kişisel veriler özel hayatın gizliliği hakkı kapsamına hapsedilmemelidir. Kişisel verilerin özel hayatın gizliliği hakkı kapsamına hapsedilemeyeceği düşüncesi onu bağımsız bir temel insan hakkı olarak kabul etmenin yanında, kişilik hakkı içerisinde de bağımsız, münferit bir kişisel değer olduğunun kabul edilmesine sebep olmuştur. Kişisel verileri

⁷⁸ Öğretide kişilik hakkı pek çok yazar tarafından farklı şekillerde tanımlanmıştır. Farklı tanımlamalar ve detaylı bilgi için bkz. **Antalya, Gökhan / Topuz, Murat** (2021) Medeni Hukuk Cilt: I, 4. Baskı, Ankara, Seçkin, s.158.

⁷⁹ **Antalya / Topuz**, s.158.

⁸⁰ **Taştan, Furkan Güven** (2017) Türk Sözleşme Hukukunda Kişisel Verilerin Korunması, 1. Baskı, İstanbul, On İki Levha Yayınları, s.67

⁸¹ **Taştan**, s. 65. **Akkurt**, Kişisel Veri..., s.26.

kişilik hakkı içerisinde münferit bir kişisel değer olarak kabul eden görüşe yeni kişilik hakkı görüşü denmektedir. Bu yeni anlayışın gelişmesinde Alman Anayasa Mahkemesi'nin nüfus sayım kararının literatüre kazandırdığı enformasyonel özerklik⁸² kavramı, şüphesiz önemli bir etken olmuştur.

Netice olarak kişisel verilerin korunması hakkının temel insan haklarından biri olarak kabul edilmesinin, ayrıca insanın kişisel varlığına bağlı kişilik hakları içerisinde müstakil bir hak olarak nitelendirilmesinin, kişisel verilerin korunması hukukunun güncel kabullerine uygun en doğru yaklaşım olduğunu söylemek mümkündür.⁸³ Ülkemizde de buna benzer bir anlayışın benimsendiğini söylemek yanlış olmaz. Kişisel verilerin korunması hakkı Anayasa'nın 20/3 hükmü ile anayasal koruma altındadır. Bu anayasal hak hem kamu hukuku hem de özel hukuk alanlarında yer alan özel düzenlemelerle de korunmaktadır. Medeni hukuk alanında kişilik hakkı kapsamında korunan kişisel veriler, ceza hukuku alanında da TCK'nın 135, 136 ve 138inci maddelerinde düzenlenen suç tipleri ile de koruma altına alınmıştır. Tüm bunlar göz önünde bulundurulduğunda Türk Hukukunda kişisel verilerin temel bir insan hakkı ve kişilik haklarından birisi olarak kabul gördüğünü söylemek mümkündür.

Son olarak konuyla ilgili bir hususa açıklık getirmekte fayda vardır. Özü itibariyle mülkiyet hakkı da temel insan haklarından biridir. Fakat mülkiyet hakkı şahıs varlığı hakları arasında değil malvarlığı hakları arasında yer alır. Kişi malvarlığı hakları üzerinde istisnai durumlar hariç olmak üzere özgürce tasarrufta bulunabilir. Mülkiyet hakkı görüşünü ayrı, insan hakkı görüşünü ayrı bir başlık altında incelememiz, mülkiyet hakkı insan haklarından olmadığı için değildir. Bunun sebebi kişilik hakkı görüşünü benimseyen ekolün kişisel verileri bireyin şahsıyla doğrudan bağlantılı, onun bir uzantısı, bir parçası olarak görmesi; ekonomik hak yaklaşımını benimseyen ekolün ise kişisel verileri kişi varlığından bağımsız, devredilebilir, alım-satıma konu edilebilir bir ürün olarak görmesidir.

Günümüzde gerek iletişim sektöründe hizmet veren cep telefonu firmalarının ürünlerini kullanabilmek için, gerek sosyal medya şirketlerinin hizmetlerini kullanabilmek

⁸² Informationelle Selbstbestimmungsrecht, Informational self-determination veya enformasyonel self determinasyon

⁸³ Aynı yöndeki görüş ve konunun detaylı incelemesi için bkz. **Akkurt**, Kişisel Veri

için kullanıcılar kişisel verilerinin işlenmesine onay vermek zorunda kalmaktadır. Bu şirketler sundukları bazı ücretsiz hizmetlerin karşılığında kişisel verilerimizi işleme izni talep etmektedir. Şirketler kullanıcılardan aldıkları bu izin sayesinde verileri özellikle pazarlama alanında kullanarak maddi kazanç elde etmektedir. Bir nevi kişisel verilerimiz ücretsiz olarak aldığımız hizmetlerin ivazı, ücreti, karşılığı konumuna düşmektedir. Buradan hareketle, verilerin doğrudan bir alım satımına konu edilmesini yasaklayan kişilik hakkı görüşünün kişisel verilerin büyük bir ekonomik değere sahip olduğu günümüz piyasa gerçekleri karşısında yer yer işlevsiz kaldığını ve kişisel verilerin çeşitli şekillerde ekonomik bir metaya dönüştürüldüğünü söylemek mümkündür.

3. ULUSLARARASI DÜZENLEMELER

Kişisel verilerin korunması hakkı ile yakın ilişki içerisinde bulunan özel hayatın gizliliği hakkı eski çağlardan bu zamana kabul edilegelmiş temel haklardan birisidir. Bu durum özel hayatın gizliliği hakkına uluslararası hukuki metinlerde de sıklıkla yer verilmesine sebep olmuştur. AIHS, Birleşmiş Milletler Evrensel İnsan Hakları Bildirisi, BM Uluslararası Bireysel ve Siyasal Haklar Sözleşmesi gibi 20. Yüzyılın temel insan hakları metinleri özel hayatın gizliliği hakkının yer aldığı metinlere örnek olarak gösterilebilir⁸⁴. Kişisel verilerin korunması hukuku henüz gelişim aşamasındayken kişisel verilerin korunması hakkı bu metinlerin özel hayatın gizliliğini koruyan hükümlerinin kapsamı altında değerlendirilmiştir. Kişisel veri hukukunun gelişimi ile birlikte uluslararası metinlere kişisel verilerin korunması hakkı müstakil olarak girmeye başlamıştır⁸⁵.

Temel hak ve hürriyetleri konu alan uluslararası anlaşmaların yanı sıra münhasıran kişisel verilerin korunması konusuna odaklanmış birtakım uluslararası metinler de bulunmaktadır. Bilgi iletişim teknolojilerindeki gelişmelerin artması ve bilhassa internet ağlarının yaygınlaşması sonucunda veri işleyen bilgisayarlar birbirlerine bağlanmış, kişisel veriler anlık olarak ülkeler arasında dolaşabilen bir akışkanlığa erişmiştir. Bu durum 1980’li yıllarda kişisel verilerin korunmasında ulusal düzenlemelerin yetersiz kaldığı ve uluslararası anlaşmalara ihtiyaç duyulduğu düşüncesini doğurmuştur. Bu düşünceler

⁸⁴ Küzeci, s.128

⁸⁵ 2000 yılında yayınlanan Avrupa Birliği Temel Haklar Şartı bunun tipik örneğidir.

ışığında Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD) tarafından ilk hukuki metin kabul edilmiş⁸⁶, BM ve Avrupa Konseyi onu izleyen örgütler olmuştur.

Münhasıran kişisel verilerin korunmasını konu edinen uluslararası hukuki metinlerin bazıları tavsiye niteliğinde ve bağlayıcı değilken bazıları bağlayıcı niteliktedir. Bu metinler veri koruma hukukunun dünya çapında gelişmesine ve hukuki düzenlemelerin yaygınlaşmasına vesile olmuştur. Özellikle Avrupa Birliği tarafından kabul edilen ve belirli ulusal standartları taşımayan ülkelere veri akışını yasaklayan metinler⁸⁷ pek çok ülkeyi AB standartlarında veri koruma kanunları çıkarmaya icbar etmeleri sebebiyle son derece geniş etki oluşturmuştur⁸⁸. Aşağıda bu uluslararası metinlerden başlıcaları ele alınacaktır.

3.1. Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD) Rehber İlkeleri

Ekonomik İşbirliği ve Kalkınma Teşkilatı 14 Aralık 1960'ta imzalanan Paris Antlaşması ile Türkiye'nin de aralarında bulunduğu 20 kurucu ülke tarafından kurulmuştur. Bir süre sonra 4 ülke daha teşkilata üye olmuş ve 1973 yılında üye sayısı 24'e yükselmiştir. Bu üyeler arasında gelişmiş Avrupa ülkelerinin yanı sıra ABD, Japonya, Kanada, Avustralya gibi farklı bölgelerden ülkeler de yer almaktadır⁸⁹. OECD'nin amaçları üye ülkelerde mali istikrarın muhafaza edilmesini sağlamak, hayat standartlarının yükseltilerek sosyal refahın artırılmasını sağlamak, üye ülkeler arasında iş birliği ve yardımlaşmayı geliştirerek dünya ekonomisinin gelişmesini sağlamaktır⁹⁰. Kuruluş gayesinden de anlaşılacağı üzere OECD uluslararası insan hakları hukukuna hizmet etmekten çok ülkeler arasında ekonomik işbirliğini geliştirmeye ve dünya çapında ekonomik kalkınmayı sağlamaya odaklanmıştır. OECD tarafından "*Kişisel Verilerin Sınır Aşan Trafik ve Verilerin Korunmasına İlişkin Rehber İlkeler*" başlıklı metin (OECD Rehber İlkeleri) 23 Eylül 1980 tarihinde kabul edilmiştir. OECD Rehber İlkeleri kişisel

⁸⁶ Korkmaz, s.151.

⁸⁷ 95/46/EC Sayılı Avrupa Birliği Direktifi buna örnek verilebilir. Direktif hakkında detaylı açıklamalar ileride yapılacaktır.

⁸⁸ Küzeci, s.129.

⁸⁹ Bkz. (<https://www.oecd.org/about/>), s.e.t. 17.01.2023

⁹⁰ İktisadi İşbirliği ve Kalkınma Teşkilatı Sözleşmesi m.1, (https://www5.tbmm.gov.tr/tutanaklar/TUTANAK/KM_/d00/c002/km_00002010ss0026.pdf) s.e.t. 17.01.2023

verilerin korunmasına odaklanmış uluslararası ilk metin olma özelliğine sahiptir. Kişisel verilerin korunmasına hasredilmiş ilk uluslararası metnin ekonomik temelli bir örgüt tarafından kabul edilmiş olması kişisel verilerin ekonomik boyutunu gözler önüne sermesi bakımından önemlidir⁹¹.

OECD Rehber İlkeleri metninde sekiz temel ilke yer almaktadır. Bunlar sınırlı veri toplama ilkesi, verinin kullanılacağı amaca uygun nitelikte olması ilkesi, amacın belirliliği ilkesi, toplandığı amaçla sınırlı kullanım ilkesi, veri güvenliği ilkesi, açıklık ilkesi, bireyin katılımı ilkesi ve hesap verilebilirlik ilkesidir⁹². OECD çıkardığı bu Rehber İlkeler ile üye devletlere ulusal veri koruma kanunları çıkarırken yol gösterici olma ve veri koruma kanununa sahip olmayan ülkelerin kanun çıkarmaları için itici güç olma amacı gütmektedir.

OECD Rehber İlkeleri tavsiye niteliğindedir. Üye devletler bakımından bağlayıcı değildir ve üye devletler bu ilkeler doğrultusunda iç hukuk düzenlemeleri yapıp yapmamak konusunda özgürdürler⁹³. OECD Rehber İlkeleri'nin önsözünde konunun ekonomik boyutuna değinilmiştir. Buna göre ülkelerin ulusal düzenlemeleri arasındaki uyumsuzluklar verilerin ülkeler arası serbest dolaşımına engel olmaktadır. Bu da uluslararası ticaretin, bankacılık sektörünün ve dolayısıyla ekonominin ciddi ölçüde olumsuz etkilenmesine sebebiyet vermektedir. Önsözde yer alan bu değerlendirmelerden yola çıkarak OECD Rehber İlkelerinin insan haklarını korumaktan çok uluslararası ticareti ve ülkelerin ekonomik menfaatlerini korumaya yönelik olduğu ifade edilmiştir⁹⁴. Zaten örgütün kuruluş amacı da budur.

OECD Rehber İlkeleri'ni önemli kılan bir diğer husus metnin Avrupa ülkeleri ile ABD'nin ortak iradesini yansıttığı olmasıdır. Avrupa Konseyi tarafından ve Avrupa Birliği tarafından kabul edilen diğer metinlere ABD taraf değildir.

⁹¹ **Mendos Kuşkonmaz, Elif** (2013) Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması (Yüksek Lisans), İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, s.39

⁹² Detaylar için bkz. **Mendos Kuşkonmaz**, s.40. **Nur**, s.52. **Çokmutlu, Metin** (2014) Türk Ceza Hukukunda Kişisel Verilerin Korunması (Doktora), Kocaeli Üniversitesi Sosyal Bilimler Enstitüsü, s.76.

⁹³ **Nur, Pınar** (2022) Vergi Hukuku Açısından Kişisel Verilerin Korunması (Doktora), Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü, s.51. **Mendos Kuşkonmaz**, s.39. Korkmaz, s.153.

⁹⁴ **Mendos Kuşkonmaz**, s.39.

3.2. Birleşmiş Milletler – Bilgisayarla İşlenen Kişisel Veri Dosyalarına İlişkin Rehber İlkeler

Uluslararası hukukun en önemli aktörlerinden biri hiç şüphesiz Birleşmiş Milletler örgütüdür. Birleşmiş Milletler (BM) ikinci dünya savaşının hemen akabinde 24 Ekim 1945'te barışı, adaleti ve insan haklarını korumak iddiasıyla 51 devlet tarafından kurulmuştur. Birleşmiş Milletler'in günümüzde 193 üyesi bulunmaktadır. BM tarafından 1948 yılında İnsan Hakları Evrensel Bildirisi kabul edilmiştir. Bu bildiri temel insan haklarını ihtiva etmektedir. 1966 yılına gelindiğinde insan hakları temelli bir başka metin olan Medeni ve Siyasi Haklar Sözleşmesi BM tarafından kabul edilmiştir. Her iki metinde de kişisel verilerin korunması hakkı doğrudan yer almamakla birlikte bu hakkın temelini oluşturan özel yaşamın gizliliği hakkı yer almaktadır⁹⁵. BM İnsan Hakları Komitesi 1988 yılında kişisel verilerin korunması hakkının Medeni ve Siyasi Haklar Sözleşmesi'nin özel hayatın gizliliğini düzenleyen 17. Maddesi kapsamında korunması gerektiğini kabul etmiştir⁹⁶.

1990 yılına gelindiğinde ise Birleşmiş Milletler yalnızca kişisel verilerin korunmasına hasredilmiş yeni bir belge yayınlamıştır. *“Bilgisayarla İşlenen Kişisel Veri Dosyaları Hakkında Rehber İlkeler”* başlığını taşıyan bu metin de OECD Rehber İlkeleri gibi tavsiye niteliği taşımaktadır. Üye ülkeleri veri koruma kanunlarının çıkarılması konusunda yönlendirmekte, hükümetleri bu temel ilkelere uymaya teşvik etmektedir⁹⁷. Bu ilkeler hukuka uygunluk ve adalet ilkesi, doğruluk ilkesi, belirli ve meşru amaçlar için

⁹⁵ Özel hayatın gizliliği hakkı İnsan Hakları Evrensel Beyannamesi'nin 12. Maddesinde, Medeni ve Siyasal Haklar Şartı'nın ise 17. Maddesinde yer almaktadır.

⁹⁶ **UN Human Rights Committee** (1988) General Comment No 16 § 10 (BM İnsan Hakları Komitesi Genel Yorum No 16, § 10) Medeni ve Siyasi Haklar Sözleşmesi'nin 17. Maddesi'ne getirdiği yorumda Komite şu ifadelerle yer vermiştir; *“Kamu otoritelerinin, özel kişi veya kurumların bilgisayarlar, veri bankalarında veya benzeri cihazlarda kişisel bilgileri toplaması veya saklaması hukuki düzenlemeye tâbi olmalıdır. Devletler, bir kimsenin özel hayatına dair bilgilerin hukuken bu bilgilere sahip olma ve kullanma yetkisine sahip olmayanların eline geçmesini ve bu bilgilerin Sözleşme'nin amaçlarına aykırılık teşkil edecek şekilde kullanılmasını engellemek için etkili tedbirler almalıdır. Özel hayatın gizliliğinin en etkili şekilde korunabilmesi için, her birey kişisel dosyalarda veya veri tabanlarında kendisiyle ilgili bilgiler saklanmışsa bu bilgilerin ne tür bilgiler olduğunu ve ne amaçla saklandığı öğrenme hakkına sahiptir. Ayrıca, her birey hangi kamu otoritelerinin, özel kişilerin veya kurumların bu dosyaları kontrol altında tuttuğunu veya tutabileceğini öğrenebilmelidir. Söz konusu dosyaların, yanlış kişisel bilgilere yer vermesi halinde veya bu bilgilerin kaldırılmasını talep etme hakkına sahiptir.”* **Uyar, Lema** (2006) Birleşmiş Milletler'de İnsan Hakları Yorumları, 1. Baskı, İstanbul, Bilgi Üniversitesi Yayınları, s.36. **Çokmutlu**, s. 72. **Mendos Kuşkonmaz**, s.43.

⁹⁷ **Mendos Kuşkonmaz**, s.44.

işlenme ilkesi, veri sahibinin verilere erişiminin sağlanması ilkesi ve veri güvenliği için gerekli tedbirlerin alınması ilkesidir.

Birleşmiş Milletler Rehber İlkelerinin OECD Rehber ilkelerine nazaran daha detaylı düzenlemeler içerdiği ifade edilmektedir⁹⁸. BM Rehber İlkeleri OECD Rehber İlkeleri kadar büyük etki oluşturmaya da onu önemli kılan faktörlerden birisi bağımsız veri koruma kuruluşlarının kurulmasını öngören ilk uluslararası metin olmasıdır⁹⁹.

3.3. Avrupa Konseyi

Kişisel verilerin korunması konusunda önemli sözleşmeler yayınlayan bir diğer uluslararası kuruluş Avrupa Konseyi'dir. Avrupa Konseyi insan haklarını, demokrasiyi ve hukukun üstünlüğünü korumayı hedef ve ilke edinen devletlerin bir araya gelerek kabul ettikleri Avrupa Konseyi Statüsü¹⁰⁰ ile 5 Mayıs 1949'da kurulmuştur¹⁰¹. Türkiye kısa süre içerisinde statü belgesini kabul ederek 13 Nisan 1950'de Avrupa Konseyi¹⁰² üyeleri arasına girmiştir. Avrupa Konseyi insan haklarını geliştirmeyi ve adaleti güçlendirmeyi hedefleyen belgeler kabul etmektedir. Bunlardan en önemlisi 4 Kasım 1950 tarihinde Roma'da imzalanan Avrupa İnsan Hakları Sözleşmesi'dir (AİHS). Bu sözleşmede kişisel verilerin korunmasına ilişkin doğrudan bir hüküm bulunmamaktadır. Ancak Avrupa İnsan Hakları Mahkemesi (AİHM) sözleşmenin özel hayatın gizliliğini düzenleyen 8. Maddesi kapsamında kişisel verilerin de korunmasına ilişkin kararlar vermektedir.

AİHS'nin 8nci maddesi aşağıdaki gibidir;

“(1) Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.

⁹⁸ Çokmutlu, s.74.

⁹⁹ Mendos Kuşkonmaz, s.44.

¹⁰⁰ Avrupa Konseyi Statüsünün tam metni için bkz. (https://inhak.adalet.gov.tr/Resimler/Dokuman/2712020093815001_tur.pdf) s.e.t. 17.01.2023.

¹⁰¹ Korkmaz, s.158.

¹⁰² Avrupa Konseyi ile Avrupa Birliği birbirinden farklı yapılardır. Avrupa Birliği 1993 yılında kurulmuş, 27 ülkeden oluşan ekonomik ve siyasi bir yapıdır. Tüm üye ülkelerde geçerli ortak yasal düzenlemeler yapan, üye ülkeleri belirli hukuki standartlara uymaya zorlayan, üyeler arası ilişkinin ve merkezîyetçiliğin çok daha sıkı olduğu bir yapılandır. Türkiye Avrupa Konseyi'ne üyeyken Avrupa Birliği'ne üye değildir.

(2) Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir.”

AİHM 8nci madde kapsamındaki başvurular hakkında üç aşamalı bir değerlendirme yapmaktadır. İlk olarak başvuru konusu olayın 8nci madde ile korunan kavramlardan birinin kapsamına girip girmediği incelenmektedir¹⁰³. Bu kavramlar özel hayat, aile hayatı, konut ve haberleşmedir kavramlarıdır. Şayet olay bu hükmün kapsamına giriyorsa yapılan işlem ya da alınan önlemin bu hükümde kapsamı belirlenen hakka bir müdahale teşkil edip etmediği araştırılmaktadır¹⁰⁴. Yapılan işlem veya alınan önlemin bu maddede tanınan hakka bir müdahale teşkil ettiği anlaşılmışsa bu müdahalenin AİHS m.8/2 kapsamında meşru olup olmadığı değerlendirilmektedir¹⁰⁵.

AİHM çeşitli kararlarında kişisel verilerin resmi makamlarca toplanıp arşivlenmesi¹⁰⁶, telefon görüşmelerinin izlenmesi¹⁰⁷, verilerin toplanma amaçları dışında kullanılması¹⁰⁸, sağlık verilerinin mahremiyeti¹⁰⁹, GPS kullanımı¹¹⁰, çalışanların bilgisayar kullanımlarının izlenmesi¹¹¹, kolluk güçleri vasıtasıyla parmak izi ve fotoğraf alınması¹¹², kişisel verilere erişim¹¹³, kişisel verilerin toplanma amacı için gereken süreden fazla saklanması¹¹⁴ gibi konuların m.8/1 kapsamında olduğunu kabul etmiştir¹¹⁵.

AİHM'nin m.8/1 kapsamında kabul ettiği müdahalelerin meşru olup olmadığı m.8/2 kapsamında değerlendirilmektedir. Müdahale ancak ikinci fıkrada sınırlı sayıda

¹⁰³ Küzeci, s.156.

¹⁰⁴ Küzeci, s.156.

¹⁰⁵ Küzeci, s.156.

¹⁰⁶ Amann / İsviçre kararı, B.N. 27798/95; K.T. 16.02.2000.

¹⁰⁷ Malone / Birleşik Krallık kararı, B.N. 8691/79, K.T. 2.08.1984.

¹⁰⁸ Leander / İsviçre kararı, B.N. 9248/81, K.T. 26.03.1987.

¹⁰⁹ Z. / Finlandiya kararı, B.N. 22009/93, K.T. 25.02.1997.

¹¹⁰ Uzun / Almanya kararı, B.N. 35623/05, K.T. 2.09.2010.

¹¹¹ Barbulescu / Romanya kararı, B.N. 61496/08, K.T. 12.01.2016.

¹¹² Murray / Birleşik Krallık kararı, B.N. 14310/88, K.T. 28.10.1994.

¹¹³ Gaskin / Birleşik Krallık kararı, B.N. 10454/83, K.T. 7.09.1989.

¹¹⁴ S. ve Marper / Birleşik Krallık kararı, B.N. 30562/04, 30566/04, K.T. 4.12.2008.

¹¹⁵ Küzeci, s.159.

sayılan amaçlara uygun, kanunda açıkça öngörülmüş ve demokratik toplumun gereklerine uygun olması durumunda meşru kabul edilmektedir¹¹⁶.

Bilgi iletişim teknolojilerinde yaşanan gelişmeler karşısında kişisel verilerin korunması için 1981 yılında Avrupa Konseyi tarafından yalnızca kişisel verilerin korunmasına hasredilmiş 108 Sayılı Sözleşme kabul edilmiştir. 108 Sayılı Sözleşmenin temel amacı taraf devletlerde uyruğu ve ikametgahı ne olursa olsun bütün gerçek kişilerin kişisel verilerin otomatik işlenmesine karşı korunmasını sağlamaktır.

3.3.1. 108 Sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Gerçek Kişilerin Korunması Sözleşmesi

Tam adı 108 Sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Gerçek Kişilerin Korunması Sözleşmesi olan, kısaca 108 Sayılı Avrupa Konseyi sözleşmesi 1981 yılında kabul edilmiş, 1985 yılında yürürlüğe girmiştir¹¹⁷. Sözleşme Avrupa Konseyi'ne üye olmayan devletler tarafından da imzalanabilmektedir¹¹⁸. Sözleşmeye bugün Avrupa Konseyi üyesi 46 ülke ve konsey üyesi olmayan 10 ülke taraftır¹¹⁹. OECD Rehber İlkeleri'nden ve BM Rehber İlkeleri'nden ayrıldığı en önemli nokta taraf devletler bakımından bağlayıcı olmasıdır. Sözleşmenin 4üncü maddesinde *“Her taraf kendi iç hukukunda, işbu bölümde yer alan ilkelere işlerlik kazandırmak amacıyla gerekli önlemleri alır”* hükmü, 10uncu maddesinde ise *“ taraflar ... kuralların ihlaliyle ilgili uygun yaptırımlar ve başvuru yolları getirmekle yükümlüdür”* hükmü yer almaktadır¹²⁰. Yine sözleşmenin 3üncü maddesine göre taraf devletler sözleşme hükümlerini hem kamu sektörüne hem özel sektöre uygularlar, ancak bu sözleşme yalnızca otomatik yollarla işlenen kişisel veriler hakkında uygulanır. Hem kamunun hem de özel sektörün uygulama alanına dahil edilmesi sözleşmenin uygulama alanını genişleten olumlu

¹¹⁶ Küzeci, s.160.

¹¹⁷ Bkz. (<https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108>) s.e.t. 17.01.2023

¹¹⁸ Yılmaz, Berrak, s.131.

¹¹⁹ Sözleşmeye taraf olan ülkelerin listesi için bkz. (<https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108>) s.e.t. 17.01.2023.

¹²⁰ Türkçe tam metin için bkz. (https://inhak.adalet.gov.tr/Resimler/Dokuman/2712020140848108_tur.pdf) s.e.t. 17.01.2023

bir hükümken, otomatik yollarla işlenmeyen verilerin kapsam dışında bırakılması uygulama alanını daraltan olumsuz ve eleştiriye açık bir hükümdür.

108 Sayılı Avrupa Konseyi Sözleşmesi kişisel verilerin işlenmesine dair bazı temel ilkeler belirlemiştir. Sözleşmenin 5inci maddesinde yer alan ilkelere göre kişisel veriler;

- “a- Adil biçimde ve yasal yoldan elde edilir ve işlenir*
- b- Belirli ve meşru amaçlar için kaydedilir ve bu amaçlara aykırı şekilde kullanılamaz*
- c- Kaydedilme amaçlarına uygun ve yerinde olur, aşırı olamaz*
- d- Doğru bilgileri yansıtır ve gerektiğinde güncellenir*
- e- Kaydedilme amaçlarını gerçekleştirmek için gerekli olan süreyi aşmayacak şekilde ilgili kişilerin kimliklerini belirlemeye imkan veren bir biçimde saklanır.”*

Sözleşmenin 6ncı maddesinde özel nitelikli kişisel veri kategorileri düzenlenmiştir. Buna göre, kişinin ırksal kökenine, siyasi düşüncelerine, dini veya diğer inançlarına, sağlık veya cinsel hayatına ve ceza mahkumiyetlerine ilişkin verileri özel nitelikli verilerdir. Sözleşmenin 8inci maddesinde ise kişisel verisi işlenen ilgili kişiye tanınan bazı ek haklar yer almaktadır. Buna göre veri sahibi veri sorumlusunun kimliğini ve kendisi ile ilgili hangi verilerin işlendiğini öğrenebilir. Hakkındaki yanlış verilerin düzeltilmesini isteyebilir. Hukuka aykırı olarak toplanan ve işlenen verilerinin derhal silinmesini talep edebilir. Bu haklarını kullanırken aşırı gecikmelere veya masraflara maruz bırakılamaz.

108 Sayılı Sözleşmenin yukarıdaki hükümlerine bakarak veri koruma hukukuna önemli katkılar sunduğunu söyleyebiliriz. Özel nitelikli kişisel verilerin sayılması ve bu kategorideki veriler bakımından istisna hükümleri getirilemeyeceğinin belirtilmesi sözleşmenin imzalandığı dönem bakımından önemli bir gelişmedir. Türkiye 108 Sayılı Sözleşmeyi 28 Ocak 1981 tarihinde imzalayarak taraf olmasına rağmen sözleşmeyi iç hukukuna uzun yıllar aktarmamıştır. Bunun sebebi ülkemizde bir veri koruma kanunun bulunmamasıdır. 6698 sayılı KVKK’nın kabul edilmesinden 1 hafta önce 17 Mart 2016 tarihinde 108 Sayılı Sözleşme resmî gazetede yayınlanarak iç hukukumuza dahil edilmiştir.

2001 yılında Avrupa Konseyi 108 Sayılı Sözleşmeye ek bir protokol yayınlamıştır¹²¹. Bu ek protokol 3 maddeden oluşmaktadır ve 108 sayılı sözleşmeyi

¹²¹ 181 Sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesine Ek Denetleyici Makamlar ve Sınraşan Veri Akışına İlişkin Protokol

genişleten iki yönü vardır. Bunlardan birincisi taraf devletlere 108 sayılı sözleşme hükümlerinin uygulanmasından sorumlu denetleyici makam oluşturma yükümlülüğü yüklemesidir. Ek protokolün yenilik getiren diğer hükmü ise sözleşmeye taraf olmayan devletlere veri aktarımı yapılabilmesi için veri aktarılacak ülkede yeterli korumanın bulunması hakkındadır. Yeterli korumayı sağlamayan ülkelere veri aktarımının yasaklanması diğer ülkeler bakımından Avrupa standartlarına uygun veri koruma kanunları çıkarmaya zorlayıcı nitelikte olmuştur. Türkiye bu ek protokolü de 108 sayılı sözleşme gibi 2016 tarihinde resmî gazetede¹²² yayınlarak iç hukukuna dahil etmiştir.

3.4. Avrupa Birliği

Avrupa Birliği 7 Şubat 1992 tarihinde imzalanan, Avrupa Birliği Anlaşması olarak da bilinen Maastricht Anlaşması ile kurulmuş, ülkeler üstü bir yapıdır. Avrupa Birliği'nin, üye ülkeler nezdinde ekonomik kalkınmanın sağlanması, barışın, huzurun, güvenliğin ve adaletin tesis edilmesi, ortak pazar oluşturulması, vatandaşların ve malların üye ülkeler arasında serbest dolaşımının sağlanması gibi pek çok temel hedefi bulunmaktadır. Bunların yanı sıra Avrupa Birliği hukukun üstünlüğünü, insan haklarını, temel özgürlüklere ve demokrasiye sadakati temel ilkeleri olarak belirlemiştir. Bu değerlerin korunması ve geliştirilmesi için siyasi ve hukuki yolları kullanmayı yöntem olarak benimsemiştir¹²³.

Avrupa Birliği kurumları¹²⁴ kurucu anlaşmaya dayanarak dört farklı tipte hukuki metin üretebilirler. Bunlar tüzükler (regulations), direktifler, kararlar ve tavsiye kararlarıdır. Tüzükler, üye devletlerin iç hukukları bakımından bağlayıcı genel kanunlardır. Direktifler, üye devletlere iç hukuk kurallarını belirlenen süre içerisinde direktife uyumlu hale getirme mecburiyeti yükler. Kararlar, AB üyesi devletler hakkında veya bu devletlerin vatandaşları hakkında verilir ve bağlayıcıdır. Tavsiye kararları ise bağlayıcı değildir¹²⁵.

¹²² Bkz. (<https://www.resmigazete.gov.tr/eskiler/2016/05/20160505-1.htm>) s.e.t. 17.01.2023.

¹²³ Bkz. Avrupa Birliği Anlaşması başlangıç hükümleri, tam metin (<https://www.ab.gov.tr/files/pub/antlasmalar.pdf>) s.e.t. 17.01.2023.

¹²⁴ Bu organlar AB Komisyonu, AB Konseyi, Avrupa Parlamentosu, AB Adalet Divanı, AB Merkez Bankası ve Sayıştaydır. Anlaşmanın 14üncü maddesi doğrultusunda yasama yetkisini AB Konseyi ve Avrupa Parlamentosu ortak kullanır.

¹²⁵ Yılmaz, Berrak, s.150.

Bugüne kadar Avrupa Parlamentosu ve Konseyi tarafından çıkarılan en önemli iki düzenlemeden biri Kişisel Verilerin İşlenmesi Sırasında Gerçek Kişilerin Korunması ve Serbest Veri Trafiği Hakkında 95/46/EC sayılı Direktiftir. Bu direktif ülkemizde yürürlükte olan 6698 sayılı Kişisel Verilerin Korunması Kanunu’nun da temelini oluşturmaktadır. Bir başka deyişle 6698 sayılı KVKK hazırlanırken referans alınan temel metin 95/46/EC sayılı Direktiftir¹²⁶. Bu husus Kişisel Verileri Koruma Kurumu’nun yayınlarında da ifade edilmektedir¹²⁷. 95/46/EC sayılı Direktif Avrupa Parlamentosu tarafından 24 Ekim 1995 tarihinde kabul edilmiştir. Avrupa Birliği üyesi devletler direktifin 32nci maddesi gereği en geç 3 yıl içinde bu direktife uygun yasaları ve yönetmelikleri yürürlüğe koyacaktır. Bu hükme göre direktifin 1998 yılında tam anlamıyla uygulamaya geçtiği söylenebilir.

Avrupa Birliği ülkelerinde 1998 yılından 2018 yılına kadar 95/46/EC sayılı direktif doğrultusunda çıkarılan veri koruma yasaları uygulanmıştır. 25 Mayıs 2018 tarihine gelindiğinde ise Avrupa Parlamentosu tarafından kabul edilen General Data Protection Regulation (Genel Veri Koruma Tüzüğü – GVKT) yürürlüğe girmiştir ve 95/46/EC sayılı direktif doğrultusunda getirilen hükümler ilga edilmiştir. GVKT bir tüzük olması sebebiyle üye devletlerin iç hukuku bakımından bağlayıcıdır. Avrupa Birliği bakımından en önemli iki hukuki düzenleme olan 95/46/EC sayılı Direktif ile GVKT’nin ayrı başlıklar altında ele alınmasında fayda vardır.

3.4.1. Avrupa Parlamentosu ve Konseyinin 95/46/EC Sayılı Direktifi

95/46/EC Sayılı Direktif yayınlandığı günden bugüne hem Avrupa Birliği içerisinde hem de diğer ülkeler üzerinde çok büyük etki oluşturmuştur. Avrupa Birliği içerisinde bu kadar etkili olmasının sebebi hiç şüphesiz üye ülkeler açısından Direktifin

¹²⁶ **Yılmaz, Berrak**, s.150. **Duman, Berat** (2020) Anayasa Hukukunda Kişisel Verilerin Korunması (Doktora), Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, s.15. **Çelik, Işıl** (2022) 6698 Sayılı Kişisel Verilerin Korunması Kanunu ve 2016/679 Sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü Kapsamında Kişisel Verilerin Yurt Dışına Aktarılması (Yüksek Lisans), İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, s.5.

¹²⁷ Bkz. **Kişisel Verileri Koruma Kurumu** tarafından yayınlanan ‘Madde ve Gerekeci İle Kişisel Verilerin Korunması Kanunu (Bilgi Notu) Ve Kişisel Verilerin Korunmasına İlişkin Terimler Sözlüğü’, s.32, (<https://www.kvkk.gov.tr/Icerik/5388/Madde-ve-Gerekcesi-ile-Kisisel-Verilerin-Korunmasi-Kanunu-Bilgi-Notu-ve-Kisisel-Verilerin-Korunmasina-Iliskin-Terimler-Sozlugu>) s.e.t. 17.01.2023.

bağlayıcı olmasıdır. Direktifin 32nci maddesine göre AB üyesi ülkeler 3 yıl içerisinde kanunlarını ve yönetmeliklerini bu direktife uygun hale getirmek zorundadır¹²⁸. Direktifin Avrupa Birliği dışında da büyük etki oluşturmamasının sebebi ise üçüncü ülkelere veri transferini düzenleyen 25inci madde hükümleridir. Bu maddeye göre AB üyesi bir ülkeden üçüncü bir ülkeye veri transferi yapılabilmesi için transfer yapılacak ülkede kişisel verilere yeterli korumanın sağlanıyor olması gerekir¹²⁹. Bu madde dolayısıyla direktif, AB üyesi ülkeler ile ekonomik, sosyal ve siyasi ilişkiler içerisinde bulunan devletleri veri koruma düzenlemelerini AB ile uyumlu hale getirmek bakımından icbar edici olmuştur. Bunun yanı sıra Direktifin veri koruma hukukunun fazla gelişmediği ülkelere örneklik teşkil ettiği de ifade edilmektedir¹³⁰.

Direktifin başlangıç hükümlerine ve birinci maddesine bakarak iki temel amaca odaklandığını söyleyebiliriz. Bunların ilki tüm Avrupa ülkelerinin veri koruma kanunlarında ve uygulamalarında bir standart oluşturarak başta kişisel mahremiyet olmak üzere gerçek kişilerin temel hak ve özgürlüklerini korumaktır. Bir diğer amaç ise Avrupa Birliği'nin üye ülkeler arasında ortak pazar kurulması ve serbest ticaret ortamının sağlanması idealine uygun olarak; ülkeler arasındaki veri koruma standartlarının farklı düzeylerde olmasından kaynaklanan sebeplerle veri akışının kesilmesini önlemek ve böylece ticari ilişkilerin askıya alınması gibi ciddi ekonomik krizlerin yaşanmasının önüne geçmektir¹³¹.

95/46/EC Sayılı Direktif yedi kısımdan oluşmaktadır. Bu kısımlar sırasıyla genel hükümler, hukuka uygunluk sebepleri, yargı yolları, verilerin üçüncü ülkelere transferi, davranış kuralları, denetleme makamı ve tedbirleri uygulayan topluluk başlıklarını taşımaktadır¹³².

¹²⁸ Direktifin Türkçe tam metni için bkz. **Dülger, Murat Volkan** (2021) Bilişim, Kişisel Verilerin Korunması ve İnternet İletişimi Mevzuatı, 7. Baskı, Ankara, Seçkin.

¹²⁹ Bu hükme 26. Maddede bazı istisnalar getirilmiştir. Özetleyecek olursak veri sahibinin hayati menfaatlerinin veya bir sözleşmeden doğan menfaatlerinin korunabilmesi için veri aktarımı gerekiyorsa üçüncü ülkede yeterli koruma bulunmasa bile veri aktarımı yapılabilir.

¹³⁰ **Yılmaz, Berrak**, s.153.

¹³¹ “*Direktifin Amacı*” başlığını taşıyan birinci madde iki fıkradan oluşmaktadır ve Türkçe tercümesi şu şekildedir; “(1) Bu Direktife uygun olarak, üye devletler kişisel verilerin işlenmesine dair başta kişisel mahremiyet hakkı olmak üzere gerçek kişilerin temel haklarını ve özgürlüklerini koruyacaktır.

(2) Üye devletler birinci fıkra kapsamında sağlanan korumayla bağlantılı nedenler için üye devletler arasında kişisel verilerin akışını yasaklamayacak ya da engellemeyeceklerdir.” Bkz. **Dülger** (2021), s.535.

¹³² Bkz. **Dülger** (2021), s.522-557.

3.4.2. Avrupa Genel Veri Koruma Tüzüğü (GVKT)

Kişisel verilerin korunması hukukunda yaşanan yeni gelişmeler karşısında 95/46/EC Sayılı Direktifin yetersiz kaldığı düşüncesi ile Avrupa Birliği veri koruma hukukunda köklü bir reform yapma ihtiyacı hissetmiştir. Direktifin kabul edildiği 1995 yılından sonra bilgi iletişim teknolojilerinde büyük çaplı gelişmeler yaşanmış, veri işleme şekilleri de oldukça değişmiştir. Her şeyden önce akıllı telefonlar hayatımıza girmiştir. Bu cihazlar özellikleri gereği çalışırken aynı zamanda kullanıcının verilerini toplamaktadır. Yine 2000’li yıllarda hayatımıza giren sosyal medya platformları dünya çapında milyarlarca insanın her çeşit verisini sistemli bir şekilde toplamaktadır. Gelişmiş yapay zekâ teknolojileri otomatik veri işleme konusuna yepyeni bir boyut kazandırmıştır. Tüm bu gelişmeler beraberinde kişisel veri güvenliği bakımından yeni riskler de getirmiştir. Avrupa Birliği üyesi ülkeler bu yeni oluşan riskler karşısında yetersiz kalan düzenlemeleri ilga ederek köklü bir reform ile 14.04.2016 tarihinde GVKT’yi kabul etmiştir. GVKT, kabul edilmesinden yaklaşık iki yıl sonra 25.05.2018 tarihinde yürürlüğe girmiştir.

GVKT’nin hazırlanmasındaki bir diğer maksat üye devletler arasında veri koruma düzenlemeleri açısından birliğin sağlanmasıdır. Aslen 95/46/EC sayılı Direktif de üye devletler açısından bağlayıcıydı. Fakat bir önceki başlıkta da izah ettiğimiz üzere direktifler üye devletlerin doğrudan uyguladıkları düzenlemeler değildir. Direktifler, üye devletler bakımından belli hedefler, ilkeler, idealler ve kurallar belirleyen, bunların iç hukuka aktarılmasını icbar eden, fakat üye devletlerin bu kuralları iç hukuka aktarırken detaylarını belirlemede ilkelere sadık kalmak kaydıyla ciddi bir takdir yetkisinin de bulunduğu hukuki belgelerdir. Buna karşılık GVKT gibi tüzükler (regulations), üye devletlerin parlamentolarında herhangi bir kanunlaştırma yapmalarına gerek olmadan uygulanabilmesi sebebiyle ulusal kanunlara benzer bir nitelik taşımaktadır. Bu sebeple Avrupa Birliği kişisel veri hukukunda birliği sağlamak için direktifleri yeterli görmemiş ve bir tüzük çıkarma yoluna gitmiştir. GVKT’nin yer yer bazı detayların belirlenmesini ve uygulanmasını üye devletlere havale eden hükümleri de vardır. Bu hükümler GVKT’nin bir direktifi andırmasına sebep olduğu gerekçesiyle eleştirilmiştir. Fakat GVKT’nin bütün Avrupa’da geçerli tek bir veri koruma kanunu getirmiş olduğu göz ardı edilmemelidir¹³³. Bu bakımdan GVKT ile mevzuatta ve uygulamada birlik büyük ölçüde sağlanmıştır.

¹³³ Yılmaz, Berrak, s.171.

Avrupa Birliği Adalet Divanı (ABAD) tarafından verilen bazı kararlar da GVKT'nin oluşturulmasında ciddi oranda etkili olmuştur. Bunlardan en önemlisi 2014 tarihli İspanya/Google kararıdır. Bir İspanya vatandaşının kendisi hakkında 1998 yılında yapılan haberin artık alakasız olduğunu gerekçe göstererek haberin Google arama sonuçlarından kaldırılması talebiyle 2010 yılında İspanya Veri Koruma Kurumu'na başvurması neticesinde başlayan hukuki süreç, önce İspanya Yüksek Mahkemesi'ne taşınmış, mahkemenin ABAD'dan görüş istemesi üzerine ABAD konuya ilişkin değerlendirmede bulunmuştur. ABAD 2014 tarihli kararında Google'ı sorumlu bulmuş, verilerin arama sonuçlarından kaldırılması gerektiğini ifade etmiştir. Karara göre kişinin kişilik hakkı, özel yaşamı, veri işleyen şirketin haklı çıkarları ve kamunun bilgi edinme hakkı gibi haklar birlikte değerlendirilerek bir sonuca varılmalıdır. Eğer kişinin kişilik haklarının zedelenmesi tehlikesi varsa ve kamunun bilgi edinme hakkı gibi bir hak da söz konusu değilse kişiler arama motorlarında yer alan sonuçların kaldırılmasını talep etme hakkına sahip olmalıdır. Kişilerin çıkarları, şirketlerin ekonomik çıkarlarından ağır basmaktadır. ABAD karar metninde unutulma hakkından (right to be forgotten) açıkça bahsetmese de bu karar ile birlikte bireylerin şartları gerçekleştiği durumlarda arama motorlarından kendileri ile ilgili sonuçların kaldırılmasını isteme haklarının olduğu kabul edilmeye başlanmıştır¹³⁴. Bu kararın yayınlanmasından 2 yıl önce 2012 yılında açıklanan GVKT tasarısında unutulma hakkı açıkça zikredilmiştir¹³⁵. Karar, tasarıda zikredilen unutulma hakkının uygulamaya geçirilmesi ve daha sonra yürürlüğe girecek GVKT'deki unutulma hakkı düzenlemesine örneklik teşkil etmesi bakımından etkili olmuştur.

GVKT'nin getirdiği en önemli yeniliklerden birisi unutulma hakkının bir veri koruma kanununda açıkça düzenlenmesidir. Tüzüğün 17nci maddesi “*Silme hakkı (unutulma hakkı)*” başlığını taşımaktadır. Verisi işlenen kişi silme hakkına ilişkin şartların gerçekleşmesi halinde arama motorlarında yer alan ve aleyhine sonuç doğurma ihtimali bulunan arama sonuçlarının kaldırılmasını talep edebilir. Unutulma hakkının silme hakkını düzenleyen hükümler içerisinde mündemiç olup olmadığı daha önceleri de tartışılmaktaydı¹³⁶. Madde başlığına unutulma hakkının doğrudan eklenmesi silme

¹³⁴ Detaylı bilgi için bkz. **Soysal, Tamer** (2019) ‘Unutulma Hakkının Avrupa Birliği’nin Genel Veri Koruma Tüzüğü Çerçevesinde İncelenmesi’ Uyuşmazlık Mahkemesi Dergisi, S:13, (s. 339-422).

¹³⁵ **Soysal**, s.354.

¹³⁶ Yukarıda bahsettiğimiz İspanya Veri Koruma Kurumu ve ABAD kararı da 95/46/EC sayılı direktifin silme hakkını düzenleyen hükümlerine dayanarak verilmiştir. Bkz. **Soysal**, s.353.

hakkının unutulma hakkını da kapsayıp kapsamadığı konusundaki tartışmaları bitirmiş oldu.

Yine ABAD'ın 8 Aralık 2022 tarihinde verdiği çok yeni bir karara göre arama motorları yanlış bilgileri de sonuç listelerinden kaldırmalıdır. Bu bilgilerin yanlışlığının mahkeme kararı ile ispatlanmış olması da şart değildir. Başvurucunun bilgilerin yanlış olduğuna dair makul kanıtlar sunması verilerin kaldırılması için yeterlidir. Bu karar GVKT'nin unutulma hakkını ve silme hakkını düzenleyen 17nci maddesinin veri sahibi lehine geniş şekilde yorumlanması gerektiğini göstermesi bakımından önemlidir. Mahkemenin kişilik haklarını kamunun bilgi edinme hakkına ve şirketlerin ekonomik menfaatlerine üstün tutan yaklaşımını sürdürdüğü gözlemlenmektedir¹³⁷.

GVKT ile getirilen yeniliklerden birisi de rıza koşullarının ayrıntılı olarak düzenlenmesidir. Rıza koşulları başlığını taşıyan 7nci maddeye göre;

- “Veri sahibinin rızasının olduğunu ispat yükümlülüğü kontrolöre aittir. Veri sahibi rızasının olmadığını ispat etmek gibi bir yükümlülüğün altına sokulamaz.
- Rıza beyanı talep üzerine veriliyorsa ve talep metni kişisel verilerin işlenmesine rıza göstermek dışında başka hususları da ihtiva ediyorsa, rızaya ilişkin hususlar açık ve sade bir dil kullanılarak yazılmalı, açıkça ayırt edilebilir bir biçimde sunulmalıdır. Rıza talep formunun GVKT hükümlerine aykırılık teşkil eden hiçbir kısmı bağlayıcı değildir.
- Veri sahibinin rızasını istediği zaman geri çekme hakkı vardır. Rıza alınırken bu hususta kişiye bilgilendirme yapılır. Rızanın geri çekilmesi rıza vermek kadar kolay olmalıdır.
- Rızanın özgür bir şekilde verilip verilmediği değerlendirilirken, işlenmesine rıza gösterilen verilerin bir hizmetin yerine getirilmesi veya sözleşmenin ifası için gerekli verilerden olup olmadığı öncelikle göz önünde bulundurulmalıdır. Hizmetin yerine getirilmesi veri işlemeye rıza gösterme şartına bağlanmışsa ve bu veriler hizmetin-sözleşmenin ifası için gerekli verilerden değilse rıza özgürce verilmiş kabul edilmeyecektir.”¹³⁸

¹³⁷ ECLI:EU:C:2022:962 , Tam metin için bkz. (<https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62020CJ0460&from=EN>) s.e.t. 17.01.2023

¹³⁸ Kanuni ifadeler bire bir değil açıklayıcı bir biçimde aktarılmıştır.

GVKT ile unutulma hakkının tanınması ve rızanın güçlendirilmesinin yanında diğer bazı yenilikler de getirilmiştir¹³⁹. Özetle belirtmek gerekirse bunlar; veri işleyenlerin tamamının veri işlemekten sorumlu tutulmaları¹⁴⁰, verisi hukuka aykırı şekilde işlenen kişilere tazminat talep etme hakkının tanınması, sınır ötesi veri akışının daha sıkı kurallara bağlanması, daha sıkı yaptırımların öngörülmesi, veri sahibine verilerini bir başka yere taşıma hakkı verilmesi, hassas verilerin işlenmesinde zorunlu veri koruma görevlisinin öngörülmesi ve verilerin tasarımdan itibaren korunması yaklaşımının benimsenmesidir¹⁴¹.

4. KİŞİSEL VERİLERE İLİŞKİN ULUSAL DÜZEYDEKİ NORMLARIN GELİŞİMİ

Kişisel verilerin korunması konusunun tarihi süreç içerisinde her geçen gün daha fazla önem kazanması kişisel verileri korumaya yönelik ulusal düzeyde kanunların ve normların ihdas edilmesini mecburi kılmıştır. Ulusal düzeydeki normlar başta Kıta Avrupası ülkeleri ile İngiltere ve Amerika Birleşik Devletleri'nde yürürlüğe konmuştur. Bu ülkelerdeki gelişmeleri örnek alarak takip eden diğer dünya ülkeleri de zamanla kendi veri koruma kanunlarını oluşturmaya başlamıştır. Ulusal düzeydeki veri koruma kanunlarının yaygınlaşmasında ve bu kanunların AB standartlarına uyum arz edecek şekilde gelişmesinde Avrupa Birliği'nin 95/46/AT sayılı yönerge ile kişisel verilere yeterli koruma sağlamayan ülkelere veri transferini yasaklayan hükümler getirmesi etkili olmuştur¹⁴².

Çalışmamızın bu kısmında mukayeseli hukukta ve Türk Hukuku'nda kişisel verilere ilişkin normların tarihsel gelişimi genel hatlarıyla ele alınacaktır. Tüm dünya ülkelerindeki durumun ayrı ayrı ele alınmasının bu çalışmanın kapsamı bakımından mümkün olmadığı açıktır. Kişisel verilerin korunması hukukunun gelişimine öncülük eden ülkelerdeki normların gelişimine ilişkin genel tabloyu ortaya koymanın yeterli olduğu

¹³⁹ GVKT ile getirilen yeniliklerin tespit edilmesi ve 6698 sayılı kanun ile detaylı bir karşılaştırma yapılması için Kalkınma Bakanlığı Bilgi Toplumu Dairesi Başkanlığı tarafından bir çalışma raporu hazırlanmıştır. Detaylar için bkz. **Akıncı, Ayşe Nur** (2017) Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi, Kalkınma Bakanlığı Yayın No:2968. (http://www.bilgitoplumu.gov.tr/wp-content/uploads/2017/07/AB_Veri_Koruma_Tuzugu.pdf) s.e.t. 17.01.2023

¹⁴⁰ Bulut hizmet sağlayıcıları gibi ikincil şirketler de kanun kapsamındaki kurallara uyma yükümlülüğü altına sokulmuştur. **Akıncı**, s.14.

¹⁴¹ **Akıncı**, s.14-18.

¹⁴² **Küzeci**, s.128.

kanaatindeyiz. Bu sebeple aşağıda mukayeseli hukuk başlığı altında öncelikle Kıta Avrupası ülkelerinden Almanya, Fransa ve İtalya'daki düzenlemelerin tarihi gelişimi, ardından ise İngiltere ve ABD'deki düzenlemelerin tarihi gelişimi ele alınacaktır. Mukayeseli hukuktaki düzenlemelerden sonra ise Türk Hukuku'ndaki düzenlemelerin tarihi gelişimi incelenecektir.

4.1. Mukayeseli Hukukta

Birbirinden farklı anlayış ve sistematığe sahip olan Kıta Avrupası ve ABD hukuk sistemlerinde kişisel verilerin korunmasına ilişkin normların düzenleniş biçimleri ve gelişim süreçleri de ciddi farklılıklar arz etmektedir. Bu sebeple Kıta Avrupası ülkelerindeki ve ABD'deki normların gelişimi ayrı başlıklar altında ele alınacaktır.

4.1.1. Kıta Avrupası'nda

Kişisel verilerin korunmasına özgülenmiş ilk veri koruma kanunları Kıta Avrupası ülkeleri tarafından 1970'li yıllarda başlayıp 1990'lı yıllara kadar uzayan bir süreç içerisinde kabul edilmiş ve yürürlüğe konulmuştur¹⁴³. Bu kanunlar gelişen ihtiyaçlar ve uluslararası anlaşmalar doğrultusunda zamanla değişimlere uğramıştır.

Avrupa Birliği'nin üye ülkeler arasında belirli hukuki standartlar oluşturmayı hedefleyen yapısı ulusal kanunlar üzerinde etkili olmuştur. AB üyesi ülkelerin ulusal veri koruma kanunları önce 1995 yılında 95/46/AT sayılı AB Direktifinin kabulü ile birlikte bu direktif ile uyum arz edecek şekilde revize edilmiş, ardından 2016 yılında GVKT'nin kabulü ile köklü bir değişikliğe daha uğramıştır.

Kıta Avrupası ülkelerindeki kişisel verilerin korunmasına ilişkin normların en belirgin ortak özelliği temel kanun niteliği taşıyan bir veri koruma kanunu içerisinde

¹⁴³ Ulusal düzeydeki ilk veri koruma kanunu 1973 yılında İsveç'te kabul edilmiştir. 1977 yılında Almanya'da, 1978 yılında Fransa'da, 1996 yılında ise İtalya'da ülke genelini kapsayan veri koruma kanunları yürürlüğe girmiştir.

yekpare halde düzenlenmiş olmalarıdır. Bunun yanı sıra AB ülkelerinin veri koruma kanunları AB Direktifinin ve GVKT'nin etkisi ile birbiri ile uyumlu ve büyük ölçüde benzer düzenlemeler içermektedir.

AB üyesi ülkelerin veri koruma kanunları arasındaki uyum 2018 yılında GVKT'nin tam olarak yürürlüğe girmesi ile oldukça artmıştır. Ancak GVKT'nin bazı konulara ilişkin düzenlemeleri üye devletlerin inisiyatifine bırakmış olması sebebiyle bu ülkelerin kanunları arasında bazı farklılıklar da mevcuttur.

GVKT'nin üye devletlerin inisiyatifine bıraktığı konulardan biri de kişisel verilere ilişkin ceza hukuku alanındaki düzenlemelerdir. Tüzüğün 83üncü maddesinde idari para cezalarının uygulanacağı haller ve ceza miktarları ayrıntılı şekilde düzenlendikten sonra 84üncü maddede idari para cezalarına tabi olmayan ihlallere ilişkin cezaların üye devletler tarafından belirleneceği ifade edilmiştir. Böylece kişisel verilere ilişkin suç tanımlarının ve bunlara uygulanacak cezaların üye devletlerin ulusal kanunları tarafından belirlenmesi öngörülmüştür. Tüzüğün 84üncü maddesinde bu cezaların etkili, orantılı ve caydırıcı olması gerektiği ifade edilmiştir.

Aşağıda kişisel verilerin korunmasına ilişkin normların, özellikle suç ve cezalara ilişkin normların, Almanya, Fransa ve İtalya'daki gelişimi müstakil başlıklar halinde ele alınacaktır.

4.1.1.1. Almanya'da

Alman Anayasası'nda kişisel verilerin korunmasına ilişkin doğrudan bir hüküm bulunmamaktadır. Ancak kişisel verilerin Alman Anayasası'ndaki genel kişilik hakkı çerçevesinde korunduğu kabul edilmektedir¹⁴⁴.

Dünyada kişisel verilerin korunmasına ilişkin ilk kanun 1970 tarihinde Almanya'nın Hessen eyaletinde kabul edilmiştir. Fakat bu kanun eyalet sınırları içerisinde

¹⁴⁴ **Titrek, Gizem Büşra** (2020) Türk Ceza Hukukunda Kişisel Verilerin Korunmasına Yönelik Suçlar (Yüksek Lisans), Uludağ Üniversitesi Sosyal Bilimler Enstitüsü, s. 35.

geçerlidir. Almanya genelinde geçerli Federal Veri Koruma Kanunu (BDSG)¹⁴⁵ ise 27.01.1977 tarihinde kabul edilmiş, 1.01.1978 tarihinde yürürlüğe girmiştir.

BDSG zaman içerisinde çok defa değişikliğe uğramıştır. BDSG üzerindeki en kapsamlı değişiklik ise 2002 yılında yapılmıştır. Bu değişiklik ile BDSG 95/46/AT sayılı AB Direktifine uygun hale getirilmiştir¹⁴⁶. AB tarafından 2016 yılında kabul edilen ve 25 Mayıs 2018 tarihinde tamamen yürürlüğe giren GVKT ile birlikte Almanya’da da GVKT’ye uygun yeni bir veri koruma kanunu yapılması gerekmiştir. 27.01.1977 tarihli BDSG büyük ölçüde değiştirilerek yeni bir kanun hazırlanmış ve 25 Mayıs 2018 tarihinde GVKT ile birlikte yeni Federal Veri Koruma Kanunu (30.06.2017 tarihli BDSG)¹⁴⁷ da yürürlüğe girmiştir. Almanya’da GVKT’nin yanı sıra yeni Federal Veri Koruma Kanunu da yürürlükte.

Almanya’da kişisel verilere doğrudan koruma sağlayan suç tipleri 1977’den bu yana Federal Veri Koruma Kanunlarında yer almıştır¹⁴⁸. Suç ve cezalara ilişkin hükümler eski Federal Veri Koruma Kanunu’nun 41inci maddesinde¹⁴⁹, yeni Federal Veri Koruma Kanunu’nun ise 42nci maddesinde düzenlenmiştir. Yeni BDSG m.42/1’e göre “*Çok sayıda kişinin herkes tarafından erişilemeyen kişisel verilerini yetkisi olmaksızın, ticari bir maksatla, bilerek üçüncü kişilere aktaran ya da başka bir şekilde erişilebilir kılan kimse üç yıla kadar hapis veya adli para cezasıyla cezalandırılır.*” Yine aynı maddenin ikinci fıkrasına göre (BDSG m.42/2) “*Herkes tarafından erişilebilir olmayan kişisel verileri yetkisi olmaksızın işleyen veya hileyle elde eden kişiye bu fiilleri bir ödeme karşılığında veya kendini ya da bir başkasını zenginleştirmek veya bir başkasına zarar vermek*

¹⁴⁵ Bundesdatenschutzgesetz 27.01.1977, Almanca tam metin için bkz. (https://www.datenschutz-wiki.de/BDSG_1977) s.e.t. 1.03.2023.

¹⁴⁶ **Korkmaz**, s.260.

¹⁴⁷ Bundesdatenschutzgesetz 30.06.2017, İngilizce tam metin için bkz. (https://www.gesetze-im-internet.de/englisch_bdsge/englisch_bdsge.pdf) s.e.t. 1.03.2023

¹⁴⁸ Alman Ceza Kanunu’nda (StGB) ise kişisel verilere dolaylı koruma sağlayan bazı suç tipleri yer almaktadır. StGB m.201’de düzenlenen aleni olmayan konuşmaların gizliliğini ihlal suçu, m.201a’da düzenlenen fotoğraf veya görüntülerin kaydedilmesi suretiyle mahremiyeti ihlal suçu, m.202a’da düzenlenen veri casusluğu suçu, m.202b’de düzenlenen kimlik hırsızlığı suçu, 202d’de düzenlenen çalınmış verilerin işlenmesi suçu ve m.203’de düzenlenen özel sırların ihlali suçu kişisel verilere dolaylı koruma sağlayan suçlara örnek olarak sayılabilir. Madde 202a’da ve m.202d’de bahsi geçen veri kavramı kişisel veri niteliği taşımayan verileri de kapsamaktadır. Saydığımız suç tiplerinin tamamı şikâyet tabidir. Bu suç tipleri hakkında detaylı bilgi için bkz. **Korkmaz**, s.264-268.

¹⁴⁹ 1978 yılında yürürlüğe giren eski Federal Veri Koruma Kanunu’nun 41inci maddesinde de kişisel verilere karşı bazı seçimlik hareketler suç olarak düzenlenmiştir. Buna göre, bu kanun ile korunan ve herkese açık olmayan kişisel verileri yetkisiz olarak aktaran, değiştiren veya ele geçiren kişiye 1 yıla kadar hapis veya adli para cezası verilir. Suçun maddi menfaat temin etmek veya kişiye zarar vermek maksadıyla işlenmesi halinde ise cezanın üst sınırı iki yıldır.

amacıyla işlemesi halinde 2 yıla kadar hapis veya adli para cezası verilir.” Bu suçların takibi şikâyetle bağlıdır. Ancak veri sahibinin yanı sıra veri sorumlusu, Verilerin Korunması ve Bilgi Edinme Hürriyeti Federal Temsilcisi ile Federal Denetim Kurulu ve eyaletlerin denetim kurulları da şikâyet hakkına sahiptir¹⁵⁰.

4.1.1.2. Fransa’da

Halen yürürlükte olan 1958 tarihli Fransa Anayasası’nda özel hayatın gizliliği hakkı ve kişisel verilerin korunması hakkı açıkça belirtilmemiştir¹⁵¹.

1978 yılında kabul edilen Bilgi Teknolojisi, Veri Dosyaları ve Bireysel Özgürlükler Kanunu¹⁵² Fransa’nın ilk veri koruma kanunudur. Fransız Veri Koruma Kurumu (CNIL) bu kanun ile kurulmuştur¹⁵³. Bu kanun GVKT’nin yürürlüğe girmesinden sonra 1 Haziran 2019 tarihinde köklü bir değişime uğramış ve GVKT’ye uygun hale getirilmiştir.

Kişisel verileri korumaya yönelik suçlar Bilgi Teknolojisi, Veri Dosyaları ve Bireysel Özgürlükler Kanunu’nda değil Fransız Ceza Kanunu’nun¹⁵⁴ 226-16 ila 226-24 maddeleri arasında düzenlenmiştir. Kişisel verilere ilişkin ilk suç tipleri Fransız Ceza Kanunu’na 1992 yılında girmiş olup zamanla bu suç tiplerinin sayısı artmış ve var olanlar revize edilerek geliştirilmiştir.

¹⁵⁰ **Kangal, Zeynel Temel** (2019) Kişisel Verilerin Ceza ve Kabahatler Hukukunda Korunması, 1. Baskı, İstanbul, On İki Levha Yayınları, s.93.

¹⁵¹ **Korkmaz**, s.253.

¹⁵² Loi informatique et libertés, Fransız Veri Koruma Kanunu, son halinin Fransızca tam metni için bkz. (<https://www.cnil.fr/fr/la-loi-informatique-et-libertes>) s.e.t. 1.03.2023

¹⁵³ **Korkmaz**, s.254.

¹⁵⁴ Fransızca tam metin için bkz. (<https://www.legifrance.gouv.fr/codes/id/LEGITEXT000006070719>) s.e.t. 1.03.2023

4.1.1.3. İtalya’da

İtalya’da kişisel verilerin korunmasına ilişkin ilk kanun olan 675 sayılı Bireylerin ve Diğer Kişilerin Kişisel Verilerinin İşlenmesine Karşı Korunması Kanunu¹⁵⁵ 31 Aralık 1996’da kabul edilmiştir. Bu kanun aynı zamanda 95/46/AT sayılı AB Direktifinin iç hukuka aktarılması anlamına gelmektedir¹⁵⁶. Kişisel verilere ilişkin suçlar ilk olarak bu kanunun 34 ila 37nci maddeleri arasında düzenlenmiştir. Buna göre veri koruma kurumuna yanlış veya eksik bildirimde bulunmak (m.34), kişisel verileri hukuka aykırı olarak işlemek (m.35), veri güvenliği için gerekli önlemleri almamak (m.36) ve kurul tarafından alınan tedbirlere uymamak (m.37) en fazla 3 yıl olmak üzere değişen miktarlarda hapis cezalarını gerektiren suçlar olarak düzenlenmiştir.

1 Ocak 2004 tarihinde yeni İtalyan Veri Koruma Kanunu (Il Codice in materia di protezione dei dati personali)¹⁵⁷ yürürlüğe girmiş ve kişisel verilerin korunmasına ilişkin bütün kanuni düzenlemeler bu kanunda birleştirilmiştir¹⁵⁸. Tüm Avrupa’da olduğu gibi İtalya’da da GVKT’nin yürürlüğe girmesiyle birlikte veri koruma kanununda ciddi değişiklikler yapılmıştır¹⁵⁹.

Kişisel verilere ilişkin suç ve cezaları ihtiva eden ve halen yürürlükte olan hükümler İtalyan Veri Koruma Kanunu’nun 167 ila 170nci maddelerinde yer almaktadır. Buna göre kişisel verileri hukuka aykırı olarak işlemek (m.167), büyük ölçekte işlenen kişisel verileri hukuka aykırı olarak vermek veya yaymak (m.167-a), büyük ölçekte işlenen kişisel verileri hileli yollarla elde etmek (m.167-b), kurula gerçek dışı beyanda bulunmak veya kurulun görevlerini yerine getirmesini engellemek (m.168) ve kurul tarafından verilen kararlara uymamak (m.170) suç olarak düzenlenmiştir.

¹⁵⁵ İngilizce tam metin için bkz. (<https://www.ics.uci.edu/~kobsa/privacy/Italian-privacy-law.html>) s.e.t. 1.03.2023.

¹⁵⁶ **Korkmaz**, s.268.

¹⁵⁷ Güncel halinin İngilizce tam metni için bkz. (<https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9740796>) s.e.t. 1.03.2023.

¹⁵⁸ **Korkmaz**, s.268.

¹⁵⁹ Bu değişiklikler 10 Ağustos 2018 tarihinde 101 sayılı KHK ile yapılmıştır. Bkz. (<https://www.gdpd.it/codice>) s.e.t. 1.03.2023.

4.1.2. Anglosakson Ülkelerinde

Kişisel verilerin korunmasına ilişkin normların gelişimi bakımından önem arz eden Anglosakson ülkeler İngiltere ve Amerika Birleşik Devletleridir. İngiltere kişisel verilerin korunması hakkının hızlı geliştiği bir ülke olması sebebiyle, ABD ise AB üyesi ülkelerden farklılaşan yaklaşımı sebebiyle incelenecektir.

ABD'nin ve İngiltere'nin kişisel verilerin korunması hukukuna yaklaşımları birbirlerinden tamamen farklıdır. İngiltere yakın zamana kadar AB üyesi olması sebebiyle Kıta Avrupası ülkelerindekine benzer bir yaklaşıma ve benzer kanuni düzenlemelere sahiptir. ABD'deki yaklaşım ve normların sistematığı ise AB ülkelerinden tamamen farklıdır. İngiltere'deki ve ABD'deki düzenlemelerin ortak noktası ise kişisel verilere ilişkin suçlara yalnızca para cezalarının öngörölmüş olmasıdır.

4.1.2.1. Amerika Birleşik Devletleri'nde

Amerikan Anayasasında özel hayatın gizliliğini ve kişisel verilerin korunmasını konu alan açık bir hüküm bulunmamaktadır¹⁶⁰. Amerikan Yüksek Mahkemesi Haklar Bildirgesi hükümlerini yorumlamak suretiyle kişisel mahremiyet hakkının Anayasada mündemiç olarak bulunduğu hükmetmiştir¹⁶¹. Kişisel verilerin de mahremiyet hakkı çerçevesinde korunduğu ifade edilmektedir¹⁶².

Kişisel verilerin korunmasına ilişkin hükümler ABD'de temel bir veri koruma kanununda değil, federal düzeydeki ve eyaletler düzeyindeki pek çok farklı kanunun konu ve sektör bazlı düzenlemelerinde dağınık bir şekilde yer almaktadır¹⁶³. ABD'deki normların düzenleniş şekli bu yönüyle AB ülkelerindeki düzenlemelerden oldukça farklıdır. ABD'deki normların kimi federal düzeyde kimi eyaletler düzeyinde olmak üzere

¹⁶⁰ Korkmaz, s.274.

¹⁶¹ Ersoy, Uğur (2009) Bir İnsan Hakları Kavramı Olarak Kişisel Verilerin Korunması (Yüksek Lisans), Gazi Üniversitesi Sosyal Bilimler Enstitüsü, s.79.

¹⁶² Ersoy, s.79.

¹⁶³ Korkmaz, s.274.

yüzlerce farklı hukuki düzenlemede dağınık bir biçimde yer almasının kişisel verilerin korunmasını zayıflattığı ifade edilmektedir¹⁶⁴.

Kişisel verilerin korunmasına ilişkin ilk federal kanun 27 Eylül 1975 yılında yürürlüğe giren Mahremiyet Kanunu'dur¹⁶⁵. Bu kanun halen kişisel verilerin korunmasına ilişkin en kapsamlı düzenlemelerin yer aldığı federal kanun konumundadır¹⁶⁶. Ancak bu kanun hükümleri yalnızca federal kurumlar tarafından kaydedilen ve işlenen kişisel veriler hakkında uygulanmaktadır¹⁶⁷. Özel sektör kuruluşları ve eyalet çapında faaliyet gösteren devlet ve hükümet organları bu kanunun hükümlerine tabi değildir¹⁶⁸.

Mahremiyet Kanunu yalnızca bazı durumlarda cezai yaptırımlara imkân tanımaktadır. Kişisel verilerin hukuka aykırı olarak işlenmesi bu kanunda kabahat olarak tanımlanmış ve fiili gerçekleştiren memur hakkında beş bin dolara kadar para cezası verilebileceği öngörülmüştür¹⁶⁹.

ABD'de kişisel verilerin korunmasına ilişkin hükümler ihtiva eden kanunlardan bir kısmı verilerin devlete karşı korunmasına odaklanmışken bir kısmı ise verilerin özel sektöre karşı korunmasını düzenlemektedir. Verileri devlete karşı korumaya yönelik hükümlerin yer aldığı kanunlara Mahremiyet Kanunu, Elektronik İletişimde Özel Hayatın Korunması Kanunu¹⁷⁰, Özel Hayatın Korunması Kanunu¹⁷¹ ve Aile Öğrenim Hakları ve Özel Hayat Kanunu¹⁷² örnek verilebilir. Verilerin özel sektöre karşı korunmasına yönelik hükümler içeren kanunlara ise Adil Kredi Bildirim Kanunu¹⁷³, Finansal Modernizasyon

¹⁶⁴ **Korkmaz**, s.274.

¹⁶⁵ Privacy Act, İngilizce tam metin için bkz. (<https://www.archives.gov/about/laws/privacy-act-1974.html>) s.e.t. 1.03.2023

¹⁶⁶ **Korkmaz**, s.276.

¹⁶⁷ Bkz. (<https://www.justice.gov/opcl/privacy-act-1974>)

¹⁶⁸ **Ersoy**, s.80-81.

¹⁶⁹ **United States Department of Justice**, Overview of The Privacy Act of 1974, 2020 Edition, (ABD Adalet Bakanlığı, 1974 Mahremiyet Kanunu'na Genel Bakış, 2020 Edisyonu), s.335. İngilizce tam metin için bkz. (<https://www.justice.gov/media/1122281/dl?inline>) s.e.t. 1.03.2023.

¹⁷⁰ Electronic Communications Privacy Act of 1986, İngilizce tam metin için bkz. (<https://www.law.cornell.edu/uscode/text/18/part-I/chapter-119>) s.e.t. 1.03.2023.

¹⁷¹ Privacy Protection, İngilizce tam metin için bkz. (<https://www.law.cornell.edu/uscode/text/42/chapter-21A>), s.e.t. 1.03.2023.

¹⁷² The Family Educational Rights and Privacy Act, İngilizce tam metin için bkz. (<http://www.law.cornell.edu/uscode/text/20/1232g>) s.e.t. 1.03.2023.

¹⁷³ The Fair Credit Reporting Act, İngilizce tam metin için bkz. (<http://www.law.cornell.edu/uscode/text/15/1681b>) s.e.t. 01.03.2023

Kanunu¹⁷⁴, Kimlik Hırsızlığı ve Gaspını Önleme Kanunu¹⁷⁵, Kablolı İletişimin Düzenlenmesi Kanunu¹⁷⁶, Video Bilgilerinin Korunması Kanunu¹⁷⁷, Sağlık Sigortası Taşınabilirliği ve Sorumluluğu Kanunu¹⁷⁸, Çocukların Kişisel Verilerinin İnternette Korunması Kanunu¹⁷⁹ örnek verilebilir¹⁸⁰.

ABD’de kişisel verilerin korunmasına ilişkin hükümlere uyulmaması genellikle para cezası yaptırıma tabi tutulmaktadır. Ancak kimlik hırsızlığı¹⁸¹ gibi bazı istisnai durumlarda hapis cezası öngörülmüştür. Hapis cezasının öngörüldüğü durumlarda kişisel verilerin korunması hakkının yanı sıra bu haktan daha üstün bir hukuki menfaatin de ihlal edildiği göze çarpmaktadır.

4.1.2.2. İngiltere’de

İngiltere’de kişisel verilere ilişkin hükümlerin toplu halde ve kapsamlı bir şekilde yer aldığı ilk kanun 1984 tarihli Veri Koruma Kanunu’dur¹⁸². Bu kanun 1998 yılına kadar yürürlükte kalmıştır. 95/46/AT sayılı AB Direktifinin kabulünden sonra 1998 yılında İngiltere’de yeni bir veri koruma kanunu kabul edilmiştir. 1998 tarihli Veri Koruma Kanunu¹⁸³ ile İngiltere AB Direktifinin hükümlerini iç hukukuna aktaran ilk ülkelerden biri olmuştur. Bu kanun 2018 yılında yerini 2018 tarihli yeni Veri Koruma Kanunu’na¹⁸⁴

¹⁷⁴ Financial Modernization Act, İngilizce tam metin için bkz. (<https://www.govinfo.gov/content/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf>), s.e.t. 1.03.2023.

¹⁷⁵ The Identity Theft and Assumption Deterrence Act, İngilizce tam metin için bkz. (<http://www.ftc.gov/node/119459>) s.e.t. 01.03.2023

¹⁷⁶ The Cable Communications Policy Act, İngilizce tam metin için bkz. (<http://www.law.cornell.edu/uscode/text/47/chapter-5/subchapter-V%E2%80%9393A>) s.e.t. 1.03.2023.

¹⁷⁷ The Videotape Privacy Protection Act, İngilizce tam metin için bkz. (<http://www.law.cornell.edu/uscode/text/18/2710>) s.e.t. 1.03.2023.

¹⁷⁸ The Health Insurance Portability and Accountability Act of 1997, İngilizce tam metin için bkz. (<http://www.law.cornell.edu/uscode/text/42/chapter-7/subchapter-XI/part-C>) s.e.t. 1.03.2023.

¹⁷⁹ The Children’s Online Privacy Protection Act of 1998, İngilizce tam metin için bkz. (<http://www.ftc.gov/ogc/coppa1.htm>) s.e.t. 1.03.2023.

¹⁸⁰ Detaylı bilgi için bkz. **Korkmaz**, s.276-291.

¹⁸¹ Kimlik hırsızlığı kimlik bilgilerinin suç işlemek amacıyla kullanılması durumudur. Kimlik Hırsızlığı ve Gaspını Önleme Kanunu’nda düzenlenmiştir.

¹⁸² Data Protection Act 1984, İngilizce tam metin için bkz. (<https://www.legislation.gov.uk/ukpga/1984/35/enacted/data.pdf>) s.e.t. 1.03.2023

¹⁸³ Data Protection Act 1998, İngilizce tam metin için bkz. (<http://www.legislation.gov.uk/ukpga/1998/29/contents>) s.e.t. 1.03.2023

¹⁸⁴ Data Protection Act 2018, İngilizce tam metin için bkz. (<https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>) s.e.t. 1.03.2023

bırakmıştır. GVKT hükümlerini uygulama maksadıyla yürürlüğe koyulan 2018 tarihli Veri Koruma Kanunu İngiltere'nin AB'den ayrılmasına rağmen hâlâ yürürlüktedir.

Kişisel verilerin korunmasına ilişkin ilk suç tipi 1984 tarihli Veri Koruma Kanunu'nun 15inci maddesinde düzenlenmiştir. Buna göre kişisel verilerin bilgisayar bürosu tarafından izinsiz ifşa edilmesi suç olarak kabul edilmiştir. 1984 yılından bugüne kadar İngiliz hukukunda kişisel verilere ilişkin suçlar veri koruma kanunlarında yer almıştır. Kişisel verilere ilişkin suçlar bugün yürürlükte olan 2018 tarihli Veri Koruma Kanunu'nun 170 ila 173üncü maddeleri arasında yer almaktadır.

2018 tarihli Veri Koruma Kanunu'nun 170nci maddesinde kişisel verileri hukuka aykırı olarak elde etme, ifşa etme, ifşasını sağlama, muhafaza etme, satma ve satmayı teklif etme fiilleri suç olarak düzenlenmiştir¹⁸⁵. 171nci maddede anonimleştirilmiş verilerin anonimliğinin kaldırılması fiili ve anonimliği kaldırılmış verilerin işlenmesi fiili¹⁸⁶, 173üncü maddede ise veri sahibinin bilgi edinme hakkını kullanmasını engellemek maksadıyla verilerin silinmesi, değiştirilmesi veya tahrip edilmesi fiilleri suç olarak düzenlenmiştir¹⁸⁷.

İngiltere'de kişisel verilere ilişkin suç tipleri için hapis cezası öngörülmemiştir. Veri Koruma Kanunu'nun 196ncı maddesine göre yukarıda bahsi geçen suç tipleri için mahkeme sanığın durumuna göre takdir edilmek üzere bir üst sınıra bağlı kalmaksızın para cezaları verebilmektedir.

4.2. Türk Hukukunda

Kişisel verilerin korunmasına ilişkin normları doğrudan ve dolaylı normlar olarak ikiye ayırmak mümkündür. Kişisel verilerin korunması hakkı ülkemizde Medeni Kanun'un ve Borçlar Kanunu'nun genel hükümleri nezdinde dolaylı olarak korunmaktadır. Kişisel verilerin korunması hakkının gerek özel hayatın gizliliği başlığı altında değerlendirildiği

¹⁸⁵ **Maden, Mehmet** (2021) Ceza Hukukunda Kişisel Verilerin Korunması, 1. Baskı, Ankara, Adalet Yayınları, s.31.

¹⁸⁶ **Maden**, s.33.

¹⁸⁷ **Maden**, s.34.

dönemde gerekse kişilik hakkının bağımsız bir görünüm şekli olarak nitelendirilmeye başlandığı yakın dönemde, bu verilerin kişilik hakkı kapsamında korunabileceği kabul edilmiştir. Kişisel verilerinin hukuka aykırı şekilde kullanılması suretiyle kişilik hakları ihlal edilen ilgili kişiler Medeni Kanun'un kişilik haklarını saldırılara karşı korumayı konu alan 24 ve 25inci maddelerine dayanarak dava açabilirler.

Kişisel verilerin hukuka aykırı olarak işlenmesi Borçlar Hukuku bakımından haksız fiil teşkil etmektedir¹⁸⁸. Yine ilgili kişiler Borçlar Kanunu hükümlerine dayanarak haksız fiilden kaynaklanan maddi ve manevi tazminat haklarını dava konusu edebilirler. Kişilik haklarını haksız müdahalelere karşı korumayı hedefleyen bu genel hükümler kişisel verilerin korunması açısından önemli olmasına karşın yetersizdir. Bunun en büyük sebebi bu hükümlerin önleyici nitelikte olmamalarıdır. Bu hükümler ancak ve ancak kişilik haklarına haksız bir müdahalenin gerçekleşmesinden sonra uygulama alanı bulacaktır¹⁸⁹.

Kişisel verilerin etkin bir şekilde korunması doğrudan kişisel verilerin korunması maksadına matuf normların yürürlüğe konmasıyla mümkündür. Türk Hukuku'nda doğrudan kişisel verileri koruma maksadına matuf ilk hukuki düzenlemeler 2005 yılında yürürlüğe giren 5237 sayılı TCK'da yer almıştır. 2010 yılında kişisel verilerin korunması hakkı Anayasa'da müstakil bir ifadeye kavuşmuştur. 2016 yılında ise kapsayıcı bir veri koruma kanunu olan 6698 sayılı KVKK kabul edilmiş ve yürürlüğe konmuştur.

4.2.1. Türk Ceza Kanunu'nun Kişisel Verilere İlişkin Hükümleri

Kişisel verilerin korunması hakkı Avrupa'da ve Amerika'da 1960'lı yıllarda tartışılmaya başlanmış ve 1970'li yıllarda ilk veri koruma kanunları çıkarılmıştır. 1980'li yıllara gelindiğinde ilk uluslararası sözleşmeler imzalanmaya başlanmıştır. Türkiye 1981 yılında Avrupa Konseyi tarafından kabul edilen 108 Sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Gerçek Kişilerin Korunması Sözleşmesi'ni imzalayan ilk ülkelerden biridir. Fakat 108 Sayılı sözleşme 2016 yılına kadar iç hukukumuza dahil

¹⁸⁸ Korkmaz, s.333.

¹⁸⁹ Korkmaz, s.334.

edilmemiştir. Bunun sebebi ülkemizde kişisel verilerin korunması hakkına ilişkin usul ve esasları düzenleyen bir veri koruma kanununun bulunmamasıdır.

Ülkemizde kişisel verilerin bu hakkı korumaya hasredilmiş doğrudan hükümlerle korunmaya başlanması Avrupa'ya nazaran çok geç olmuştur. Doğrudan kişisel verileri koruma maksadına matuf ilk hükümler 1 Haziran 2005 yılında yürürlüğe giren Türk Ceza Kanunu'nun 135, 136 ve 138inci maddelerinde yer almıştır. Buna göre kişisel verilerin hukuka aykırı olarak kaydedilmesi, verilmesi, yayılması, ele geçirilmesi veya yok edilmemesi suç olarak düzenlenmiştir. TCK'nın 135inci maddesinin gerekçesinde bu suç tipleri ile 108 Sayılı Sözleşmede öngörülen hükümlere geçerlilik tanındığı ifade edilmiştir.

Kişisel verilerin korunması hakkına yönelik tipe uygun ihlallerin suç olarak tanımlanması ve cezai yaptırıma bağlanması elbette son derece önemli bir gelişmedir. Lakin kişisel verilerin korunması hukuku bazı teknik tanımlar içeren, kendine özgü gereklilikleri bulunan kapsamlı bir alandır. Kişisel verilerin etkili bir biçimde korunması öncelikle bu hakkın Anayasa'da tanınmasına ve çağın gerekliliklerine uygun kapsamlı düzenlemeler içeren bir veri koruma kanununun yürürlüğe konmasına bağlıdır. Nitekim TCK'nın ilgili hükümleri yürürlüğe konduğu ilk yıllarda bazı eleştirileri de beraberinde getirmiştir. Bu eleştirilerin başında kişisel veri tanımının kanunlarda açıkça yapılmamış olması sebebiyle bu hükümlerin belirsizlik taşıması ve buna bağlı olarak kanunilik ilkesine aykırı oldukları iddiası yer almaktadır. Bu tartışmalar bir veri koruma kanunu yapılmasının gerekliliğini tekrar hatırlatmıştır.

4.2.2. Kişisel Verilerin Korunması Hakkının Anayasal Bir Hak Olarak Kabulü

12 Eylül 2010 tarihinde yapılan referandum ile Anayasa'nın Özel Hayatın Gizliliği başlığını taşıyan 20nci maddesine yeni bir fıkra eklenmiş ve kişisel verilerin korunması hakkı Anayasa'da müstakil bir hak olarak kabul edilmiştir. Bu fıkraya göre *“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”.

Kişisel verilerin korunması hakkının Anayasa’da müstakil bir düzenleme olarak yer alması devlete bazı yükümlülükler yüklemektedir. Devlet kişisel verilerin korunması hakkının sınırlandırılmasında belirli kriterler ile bağlıdır. Bu kriterler Anayasa’nın 13üncü maddesinde sayılmıştır. Buna göre kişisel verilerin korunması hakkı ancak kanun ile sınırlandırılabilir. İdarenin düzenleyici işlemleri ile bu hakka bir sınırlama getirilmesi mümkün değildir. Yine bu sınırlamalar Anayasa’nın sözüne ve ruhuna, demokratik düzenin ve laik cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz. Bu sınırlamalar getirilirken hakkın özüne dokunulamaz¹⁹⁰. Anayasal hakların sınırlandırılması hakkında bazı maddelerde öngörülen özel sınırlama sebepleri 20nci maddede öngörülmemiştir. Buradan yasama organının hakkı sınırlandırıcı düzenlemeler yaparken belirli sebeplerle bağlı kalmak zorunda olmadığı sonucuna ulaşmak mümkündür. Ancak yasama organı tarafından ihdas edilen hakkı sınırlandırıcı hükümler her halükârda yukarıda belirttiğimiz 13üncü maddede yer alan kriterlere uymak zorundadır.

Kişisel verilerin korunması hakkının Anayasa’da yer almasının bir diğer sonucu da kanunların Anayasa’ya uygun olma zorunluluğu bakımındandır. Anayasa’nın normlar hiyerarşisinin en üstünde yer almasının doğal bir sonucu olarak kişisel verilerin korunması hakkına aykırı bir kanun çıkarılamaz. Böylesi bir durumda Anayasa Mahkemesi ilgili hükmü iptal yaptırımına tabi tutacaktır.

Kişisel verilerin korunması hakkının Anayasa’ya müstakil bir fıkra olarak eklenmesinden önce kişisel verilerin diğer bazı Anayasa maddeleri vasıtasıyla korunduğundan söz edilebilir. 2010 Anayasa değişikliğinden önce Anayasa Mahkemesi kişisel verilerin korunması hakkını tıpkı AİHM gibi özel yaşamın gizliliği hakkı altında değerlendirmekteydi¹⁹¹. Doğrudan özel yaşam alanına dahil kabul edilen kişisel veriler özel yaşam hakkının yanı sıra diğer bazı anayasal hakların da dolaylı koruması altındaydı. Maddi ve manevi varlığı serbestçe geliştirme hakkı, insan onurunun korunması, haberleşme özgürlüğü, konut dokunulmazlığı, fikir özgürlüğü, din ve vicdan özgürlüğü

¹⁹⁰ AY m. 13.

¹⁹¹ AYM, E: 1996/68, K: 1999/1, K. T. 06.01.1999.

gibi haklar kişisel verilere dolaylı koruma sağlayan diğer haklar arasında değerlendirilebilir¹⁹².

Anayasa Mahkemesi 2010 değişikliğinden sonra 30.12.2015 tarihli bir kararında kişisel verilerin korunmasını isteme hakkının niteliğine ve diğer haklarla ilişkisine dair bir yorumda bulunmuş ve bundan sonraki kararlarında bu ifadesine atıf yapmayı sürdürmüştür. AYM'ne göre “*Kişisel verilerin korunması hakkı, kişinin insan onurunun korunmasının ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak, bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır.*”¹⁹³. Anayasa Mahkemesi'nin ifadesinden de anlaşılacağı üzere kişisel verilerin korunması hakkı her ne kadar özel yaşamın gizliliği başlığı altında düzenlenmiş olsa da insan onuru ve kişiliği serbestçe geliştirme hakkı ile doğrudan ilişkilidir. Bunun yanında kişisel verilerin korunması hakkı kişinin pek çok temel hak ve özgürlüğünün korunmasına hizmet etmektedir. Gerçekten de kişisel verilerin korunması hakkının ihlali neticesinde kişilerin diğer pek çok hakkı yönünden de mağdur olabilmeleri mümkündür. Kişisel verilerinin açıklanma tehdidi kişiyi ifade hürriyeti, din ve vicdan hürriyeti gibi pek çok hakkını gereği gibi kullanmaktan yoksun bırakabilir.

4.2.3. 6698 Sayılı Kişisel Verilerin Korunması Kanunu'nun Kabulü

7 Nisan 2016 tarihinde resmî gazetede yayımlanarak yürürlüğe giren 6698 Sayılı KVKK ile Türk Hukuku uzun yıllar beklenen veri koruma kanununa kavuşmuştur. Kişisel verilerin korunmasına ilişkin usul ve esasların kanunla düzenleneceğini ifade eden Anayasa'nın 20/3 maddesinin son cümlesinin gereği yerine getirilmiştir. Kanun ile literatüre ait tanımlar yapılmış, veri işleme şartları ve bu verileri işlerken uyulacak temel ilkeler belirlenmiş, veri sahibinin hakları sayılmış, veri sahibine hak ihlali durumunda kurula şikâyet hakkı verilmiş ve veri sorumlusunun yükümlülükleri belirlenmiştir. Ayrıca idari ve mali özerkliğe sahip bir veri koruma kurumu kurulmuştur.

¹⁹² Kişisel verilerin korunması hakkına dolaylı koruma sağlayan anayasal haklar konusunda daha detaylı bir değerlendirme için bkz. **Yüzbaşı Tobaz, Firdevs** (2021) Uluslararası İnsan Hakları Hukukunda ve Türk Hukukunda Kişisel Verilerin Korunması (Doktora), Trabzon Üniversitesi Lisansüstü Eğitim Enstitüsü, s.288.

¹⁹³ AYM, E: 2014/122, K: 2015/123, K.T. 30.12.2015.

Kanunun yürürlüğe girmesi Türk Ceza Hukuku bakımından da önemli sonuçlar doğurmuştur. Bilhassa tipikliğin maddi unsurlarının ve hukuka aykırılık unsurunun değerlendirilmesinde 6698 sayılı kanun hükümleri önem arz etmektedir. Kişisel veri tanımının yapıldığı 3üncü madde, veri işlerken uyulması gereken temel ilkeleri belirleyen 4üncü madde ve veri işleme şartlarını (hukuka uygunluk sebeplerini) düzenleyen 5inci ve 6ncı madde ilgili suçların değerlendirilmesinde göz önünde bulundurulması gereken hükümlerin başta gelenleridir. 6698 Sayılı KVKK'da yer alan hükümler ikinci bölümde detaylı şekilde ele alınacaktır.

4.2.4. Muhtelif Kanunlarda Yer Alan Konuyla Bağlantılı Diğer Hükümler

Anayasa, Türk Ceza Kanunu, Medeni Kanun, Borçlar Kanunu ve Kişisel Verilerin Korunması Kanunu kişisel verileri korumaya matuf düzenlemelerin yer aldığı başlıca kanunlardır. Fakat bunların yanında diğer bazı kanunlarda da kişisel verilere ilişkin hükümler bulunmaktadır. Ceza Muhakemesi Kanunu (m. 75, 80, 134-138, 140), İş Kanunu (m. 75), Bankacılık Kanunu (m. 73), Vergi Usul Kanunu (m. 5, 148), Karayolları Trafik Kanunu (m. 5), PVSK (m. 5, ek m. 7), Devlet İstihbarat Hizmetleri ve Milli İstihbarat Kanunu (m. 4, 6), Elektronik İmza Kanunu (m. 12), Noterlik Kanunu (sır saklama yükümlülüğüne ilişkin 54üncü madde), Yabancılar ve Uluslararası Koruma Kanunu (m. 99), Adli Sicil Kanunu (m. 11), İstatistik Kanunu (m. 14, 53), Fikir ve Sanat Eserleri Kanunu (m. 19, 70, 83-86), Nüfus Hizmetleri Kanunu (m. 9, 45), Elektronik Haberleşme Kanunu (m. 51-52), İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun (m. 9) ve Sporda Şiddet ve Düzensizliğin Önlenmesine Dair Kanun'da (m. 5) kişisel verilerin korunması konusuna ilişkin bazı hükümler bulunmaktadır¹⁹⁴.

Farklı konulara odaklanmış çok sayıda kanunda kişisel verilerin korunmasını ilgilendiren düzenlemelerin bulunması çağımızda kişisel verilerin hayatın her alanında kullanıldığının bir göstergesidir. Konumuzla doğrudan bağlantılı olmadığı için bu düzenlemelerin her birine ayrı ayrı değinmeye ihtiyaç bulunmamaktadır. Fakat şunu

¹⁹⁴ Bu kanunlarda yer alan hükümler hakkında detaylı değerlendirme için bkz. **Korkmaz**, s.335-360. **Duman**, s.277-283.

belirtmekte fayda var ki bu kanunların ilgili hükümlerinde veya başka bir kanunda kişisel verilerin belirli amaçlar için işlenmesine izin verildiği durumlarda ceza hukuku bakımından bir hukuka uygunluk sebebinin varlığı gündeme gelecektir. Hukuk düzeni bir bütündür ve bir kanunda kişiye hak veya görev olarak yüklenmiş bir fiilin gerçekleştirilmesinin başka bir kanuna göre suç oluşturması kabul edilemez. Bu husus, Türk Ceza Kanunu’nun 24/1 maddesinde açıkça belirtilmiştir. Buna göre “*Kanunun hükmünü yerine getiren kimseye ceza verilmez*”. Kişisel verilerin işleme şartlarının yer aldığı KVKK’nın 5inci maddesinin 2-a bendi de kanunlarda açıkça öngörülen hallerde verilerin işlenebileceğini düzenlemiştir.



İKİNCİ BÖLÜM

6698 SAYILI KVKK KAPSAMINDA KİŞİSEL VERİLERİN KORUNMASI

1. AMAÇ, KAPSAM ve TANIMLAR

1.1. Kanunun Amacı

6698 Sayılı Kanunu’nun amacı “*Amaç*” başlığını taşıyan m.1’de düzenlenmiştir. Buna göre “*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*”.

Kişisel verilerin kamu ve özel sektör tarafından yoğun bir şekilde işlendiği günümüz dünyasında sektör bazlı bazı özel düzenlemeler ve genel hükümler kapsamında kişisel verilerin korunması artık mümkün değildir. İhlal gerçekleşikten sonra devreye giren Medeni Kanun (MK) ve Borçlar Kanunu (BK) hükümleri de verilerin korunmasını değil ancak ihlallerin durdurulmasını ve zararların giderilmesini temin etme kabiliyetine haizdir. Ancak kişisel verilerin korunması öğretisinin ulaştığı güncel anlayış kişiye henüz kişilik hakları zedelenmeden birtakım haklar ve yetkiler sunarak bu suretle ihlaller karşısında kişiyi korumayı esas almaktadır. Verilerin geleceğini belirleme hakkı olarak da ifade edilen bu anlayışın uygulamaya geçirilmesi ancak veri sahibine verilerinin var olduğu andan yok olduğu ana kadar belirli haklar tanıyan, bu hakları kullanması için etkili mekanizmaları hayata geçiren ve veri işleyenlere de birtakım yükümlülükler getiren kapsamlı bir kanun ile mümkündür. Anayasa’da yer alan temel hak ve özgürlüklerin kişisel verilerin hukuka aykırı şekilde işlenmesi suretiyle gadre uğratılmasının engellenmesi de ancak bu şekilde mümkün olabilir.

Kanunun amacı düzenlenirken “*özel hayatın gizliliği hakkının ve diğer temel hakların korunması*” ifadesinin kullanılması, buna karşılık kişisel verilerin korunmasını isteme hakkı ifadesine açıkça yer verilmemesi eleştirilere sebep olmuştur¹⁹⁵. Bizce de bu eleştirilerde haklılık payı vardır. Zira kişisel verilerin korunması hakkının özel hayatın gizliliği şemsiyesinden çıkarılarak bu haklar ile bağlantılı fakat müstakil bir hak olarak kabul edilmesinde ve kanunlarda müstakil olarak zikredilmesinde yarar vardır.

Kanunun amaç başlıklı 1inci maddesinde açıkça değinilmemiş olsa da ilgili kişilerin sahip oldukları hakların düzenlenmesi, ihlaller karşısında gidebilecekleri başvuru yollarının belirlenmesi ve bağımsız bir veri koruma kurumunun kurulması da kanunun amaçları arasındadır. Nitekim ilerleyen maddelerde bu konulara yönelik düzenlemeler getirilmiştir.

1.2. Kanunun Kapsamı

“*Kapsam*” başlığını taşıyan 2nci maddeye göre “*Bu Kanun hükümleri, 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 uygulanır.*” Bu maddeden hareketle verisi işlenenler bakımından sadece gerçek kişiler kanun kapsamına girmektedir. Verisi işlenen tüzel kişiler ise açıkça kanun kapsamı dışında bırakılmıştır. Tüzel kişilere ilişkin veriler işlenirken ancak bu verilerin bir başka gerçek kişiye ilişkin olması durumunda işleme faaliyeti bu kanun kapsamında değerlendirilebilecektir¹⁹⁶. Bu durumda da zaten korunan tüzel kişinin verisi değil gerçek kişinin verisidir.

Madde metninden hareketle veri işleyen hem gerçek kişilerin hem de tüzel kişilerin kanun kapsamında olduğu anlaşılmaktadır. Kamu ve özel sektör bakımından da bir ayrım yapılmamıştır. Dolayısıyla hem kamu sektöründe hem de özel sektörde yürütülen veri

¹⁹⁵ Dülger (2020), s.114.

¹⁹⁶ Öztürk / Seyhan / Altınok, s.26.

işleme faaliyetleri bu kanun kapsamında değerlendirilecektir¹⁹⁷. Ancak kanun veri işleyenlerin bu kanun kapsamında değerlendirilebilmesi için belirli özellikleri taşımalarını aramaktadır. Veri işleyenlerin kanun kapsamına girmesi bu verilerin tamamen veya kısmen otomatik olan yollarla işlenmesine veya bir veri kayıt sisteminin parçası olarak işlenmesine bağlı kılınmıştır. Derli toplu bir şekilde ifade etmek gerekirse;

- Tamamen veya kısmen otomatik yollarla veri işleyen gerçek ve tüzel kişiler,
- Verilerin otomatik yollarla işlenip işlenmediğine bakılmaksızın; verileri bir veri kayıt sisteminin parçası olarak işleyen gerçek ve tüzel kişiler,

kanun kapsamında değerlendirilmelidir. Bu açıklamalardan anlaşılacağı üzere verilerin otomatik olmayan yollarla ve bir veri kayıt sisteminin parçası da olmadan işlenmesi hali kanun kapsamına alınmamıştır. Böylesi bir durumda 6698 Sayılı Kanun hükümlerine başvurulamayacaktır. Ancak diğer kanunlarda yer alan hükümlerin uygulanmasına bu tür durumlarda da devam edilmelidir¹⁹⁸. Zira KVKK'nın kapsamını düzenleyen bu hüküm yalnızca bu kanun bakımından bağlayıcıdır. Otomatik olmayan yollarla ve bir veri kayıt sisteminin de parçası olmadan işlenen veriler Türk Ceza Kanunu kapsamına girmeye devam edecektir¹⁹⁹. TCK'da yer alan suç tiplerinin oluşması için KVKK kapsamına giren bir fiilin şart olduğunu söylemek TCK'nın uygulama alanını hukuki bir dayanak olmaksızın daraltmak olacaktır. Yine MK ve BK hükümlerinin uygulanması bakımından da bu şartın aranmayacağı söylenmelidir.

Veri kayıt sisteminin ne olduğu ilk etapta tam olarak anlaşılamayabilir. Kanunun üçüncü maddesinin h bendinde veri kayıt sistemi *“kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi”* şeklinde tanımlanmıştır. Sistem ifadesi her ne kadar dijital ortamı çağırırsa da veri kayıt sisteminden söz edebilmek için dijital bir ortama ihtiyaç yoktur. Verilerin ulaşmayı kolaylaştıracak şekilde belirli kriterlere göre yapılandırılmış olması yeterlidir. Fiziki bir dosya da bu anlamda veri kayıt sistemi olarak kabul edilebilir. Bu husus ikinci maddenin gerekçesinde de açıkça ifade edilmiştir.

¹⁹⁷ Öztürk / Seyhan / Altınok, s.26.

¹⁹⁸ Öztürk / Seyhan / Altınok, s.27.

¹⁹⁹ Gerekçede bu hususa şu şekilde yer verilmiştir; *“Bu kapsamda, otomatik olmayan yollarla işlenen kişisel veriler bir veri kayıt sisteminin parçası değilse Kanun kapsamında değerlendirilmeyecektir. Ancak, bu hüküm anılan verilerin kişisel veri niteliğini etkilemeyeceğinden, bu tür verilere ilişkin hukuka aykırı eylemler 5237 sayılı Türk Ceza Kanunu uyarınca suç teşkil etmeye devam edecektir.”* Gerekçenin tam metni için bkz. (<https://www5.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf>) s.e.t. 17.01.2023.

1.3. Kanun Kapsamı Dışında Kalan Durumlar

Kanunun kapsamını düzenleyen ikinci maddenin mefhumu muhalifinden hareketle tüzel kişilere ait verilerin kanun kapsamı dışında olduğu sonucuna varmak gerektiğini ifade etmiştik. Yine ikinci maddeden hareketle otomatik olmayan yollarla ve bir veri kayıt sisteminin parçası da olmadan işlenen verilerin de kanun kapsamı dışında olduğunu söylemiştik. Kanunun kapsamına dair ifadelerin yer aldığı ikinci maddedeki tarife girmekle birlikte kanun kapsamı dışında tutulan bazı istisna halleri de bulunmaktadır. Bunlar kanunun istisnaları düzenleyen 28inci maddesinde iki fıkra halinde belirlenmiştir. Birinci fıkra tamamen kanun kapsamı dışında kalan halleri düzenlerken ikinci fıkra esasen kanun kapsamında olmakla birlikte kanunun bazı hükümlerinden istisna tutulacak halleri düzenlemektedir. Birinci fıkraya göre (m.28/1) aşağıdaki hallerde KVKK hükümleri uygulanmaz;

“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.”

Ana muhalefet partisi milletvekilleri tarafından bu fıkroda yer alan a ve ç bentlerinin Anayasa’ya aykırı oldukları iddiasıyla iptali istenmiştir. A bendinde yer alan ve aile fertlerinin birbirleri ile ilgili kişisel verileri belirli şartlar altında işleminin kanun

kapsamında yer almayacağını düzenleyen ifadenin özel hayatın gizliliğini ve kişisel verilerin korunmasını isteme hakkını orantısız şekilde sınırladığı iddia edilmiştir. İptal isteminde kişinin aile fertlerine karşı da özel bir alanının bulunması gerektiği, özellikle velayet ilişkisinin çocuğun kişiliğini, maddi ve manevi bütünlüğü ile bunlardan doğan haklarını tamamen ortadan kaldırmaması gerektiği ifade edilmiştir. Buna karşılık Anayasa Mahkemesi yaptığı değerlendirmede a bendinde yer alan ifadelerin hakkın özüne dokunacak şekilde orantısız sonuçlara yol açmayacağını, kanun koyucunun bu bentte yer alan hükümleri koyarken hayatın olağan akışı içerisinde aile fertleri arasında sıklıkla yaşanması muhtemel veri işleme durumlarını göz önünde bulundurduğunu, gerek velayet ilişkisinden gerek aile içi diğer ilişkilerden kaynaklanan sebeplerle aile fertlerinin birbirlerinin kişisel verilerine erişme-kullanma durumlarının oluşabileceğini ifade etmiştir. Bu düzenlemelerin hakkın özüne dokunmadığına, demokratik toplumun gereklerine ve ölçülülük ilkesine aykırı olmadıklarına ve iptal isteminin reddine karar vermiştir²⁰⁰. Aile fertleri arasındaki birbirleri ile birlikte yaşamaktan kaynaklanan zaruri günlük ilişkiler göz önünde bulundurulduğunda bunlar arasındaki veri işleme hallerinin kanun kapsamı dışında tutulması yerinde olmuştur. Ancak bu veri işleme faaliyetleri sırasında veri güvenliğine ilişkin yükümlülöklere uymanın şart olduđu ve aile fertlerine ilişkin bilgilerin üçüncü kişilerle paylaşılmasının istisna kapsamında olmadığı kanunda açıkça ifade edilmiştir.

Anayasa'ya aykırılığı iddia edilen bir diğör bent bazı kamu kurumlarının önleyici, koruyucu ve istihbari faaliyetleri çerçevesinde veri işlemelerini kanun kapsamı dışında tutan ç bendidir. Anayasa mahkemesi bu bent ile ilgili yapılan iptal istemini de reddetmiştir²⁰¹. Kamu düzeni, kamu güvenliği, ekonomik güvenlik gibi içeriğı net bir şekilde belirli olmayan, yoruma açık kavramların kullanılması bu bende yöneltlen eleştirilerden biridir. Ancak bu maksatlarla yapılacak işleme faaliyetlerinin sadece kanun tarafından kendisine bu görev verilmiş kurumlar tarafından yapılması öngörülmektedir. Bu görevlerle mesul kılınmış bazı kamu kurumlarının görevlerini yapabilmeleri için bazı kişisel verileri işlemeye mecbur bulundukları kesindir. Kolluk teşkilatları ve Millî İstihbarat Teşkilâtı kanunla kendisine bu görevler verilen kurumlardır. Bu kurumların görevleri ile doğrudan bağlantılı faaliyetler yürütürken KVKK engeline takılmaları görevleri ile bağdaşmayacaktır. Kanunun düzenleniş şeklinden de anlaşılacağı üzere bu kurumlar tarafından yapılacak veri işleme faaliyetlerinin milli güvenliği, kamu güvenliğini,

²⁰⁰ AYM, E. 2016/125, K. 2017/143, K.T. 28.9.2017.

²⁰¹ AYM, E. 2016/125, K. 2017/143, K.T. 28.9.2017.

kamu düzenini ve ekonomik güvenliği ilgilendirmeyen, siyasi, ideolojik ve sair, kanunla tanınmayan amaçlar için gerçekleştirilmesi durumunda bu faaliyetler istisna kapsamına girmeyecektir. Devlet ve ilgili devlet görevlileri hukuk önünde sorumlu olacaktır. Düzenleme bu yönüyle ölçülüdür. Fakat kişiler hakkında bu görevlerle bağdaşmayan kayıtların tutulması halinde bu durumun tespiti ve ispatı zor olacaktır. Tespitin ve ispatın zor oluşunun kişi güvenliği bakımından risklere sebep olduğu bir gerçektir. Bu riskler ile kamu güvenliğinin sağlanması menfaati arasında bir denge kurulması zaruridir.

Bir diğer istisna halleri 28/2’de düzenlenmiştir. Buna göre belirli bazı durumlarda²⁰² “*veri sorumlusunun aydınlatma yükümlülüğünü düzenleyen 10uncu madde, zararın giderilmesini talep etme hakkı hariç, ilgili kişinin haklarını düzenleyen 11inci madde ve Veri Sorumluları Siciline kayıt yükümlülüğünü düzenleyen 16ncı madde uygulanmaz*”. Ancak bu kısmi istisnanın uygulanabilmesi için veri işleme faaliyetlerinin bu kanunun temel ilkelerine uygun ve orantılı olması gerekir. Temel ilkelere uygunluk şartının gözetilmesi istisnaların kötüye kullanılmasının önüne geçmektedir. Zira temel ilkelerin başında hukuka ve dürüstlük kuralına uygunluk²⁰³ gelmektedir.

1.4. Kavramlara İlişkin Tanımlar

6698 Sayılı Kanun’da yer alan kavramların ne ifade ettiği kanunun üçüncü maddesinde tanımlanmıştır. Kavramların gelişim süreçlerine ve bu kavramlar üzerindeki tartışmalara fazla değinmeden, tanımlar ve hukukumuzdaki yansımaları hakkında kısa bilgiler vermek konumuz açısından yeterli olacaktır.

²⁰² Bu durumlar a, b, c, ç bentlerinde şu şekilde sayılmıştır; “a) Kişisel veri işlemenin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması. b) İlgili kişinin kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi. c) Kişisel veri işlemenin 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 işlemenin bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olması.”

²⁰³ KVKK m. 4/2-a.

1.4.1. Kişisel Veri

Kişisel veri kavramı kanunda “*kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi*” olarak tanımlanmıştır²⁰⁴. Birinci bölümde kişisel veri kavramını açıklarken bu kavramın ne ifade ettiğini detaylı şekilde ele almıştık. Orada ele aldığımız detaylar tekrara düşmemek için burada yeniden zikredilmemiştir. Tanımdan anlaşılabileceği üzere KVKK bakımından yalnızca gerçek kişilere ilişkin veriler kişisel veri olarak kabul edilmiş, tüzel kişilerin verileri kişisel veri olarak kabul edilmemiştir.

Kişisel verisi işlenen gerçek kişi ise kanunda “*ilgili kişi*” kavramı ile ifade edilmiştir. Öğretide ilgili kişiyi ifade etmek için bu tabirin dışında veri sahibi, veri öznesi, veri süjesi gibi ifadeler de kullanılmaktadır.

1.4.2. Kişisel Verilerin İşlenmesi

Kişisel verilerin işlenmesi kavramının tanımı kanunda oldukça geniş tutulmuştur. Kanunda “*Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem*” veri işleme olarak tanımlanmıştır. Kanun burada kaydetme, depolama, yeniden düzenleme, aktarma, sınıflandırma gibi örnek bazı işlemler saymıştır. Bunların her biri tek başına veri işlemenin gerçekleşmesi için yeterlidir. Kişisel veriler üzerinde bu işlemlerden herhangi

²⁰⁴ Üçüncü maddenin gerekçesinde kişisel veri kavramının içeriğine dair fikir oluşturma için şu ifadelere yer verilmiştir; “*Kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade etmektedir. Bu bağlamda sadece bireyin adı, soyadı, doğum tarihi ve doğum yeri gibi onun kesin teşhisini sağlayan bilgiler değil, aynı zamanda kişinin fiziki, ailevi, ekonomik, sosyal ve sair özelliklerine ilişkin bilgiler de kişisel veridir. Bir kişinin belirli veya belirlenebilir olması, mevcut verilerin herhangi bir şekilde bir gerçek kişiyle ilişkilendirilmesi suretiyle, o kişinin tanımlanabilir hale getirilmesini ifade eder. Yani verilerin; kişinin fiziksel, ekonomik, kültürel, sosyal veya psikolojik kimliğini ifade eden somut bir içerik taşıması veya kimlik, vergi, sigorta numarası gibi herhangi bir kayıtlı ilişkilendirilmesi sonucunda kişinin belirlenmesini sağlayan tüm halleri kapsar. İsim, telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler gibi veriler dolaylı da olsa kişiyi belirlenebilir kılabilecek özellikleri nedeniyle kişisel verilerdir.*” **Tasarı**, s.7. Tam metin için bkz. (<https://www5.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf>) s.e.t. 1.04.2023

biri yapıldığında veri işlemeden söz edilecektir. Ancak burada kanunun bu işlemleri sınırlayıcı bir şekilde saymadığına, örnek kabilinden saydığına dikkat etmek gerekmektedir. Kanun koyucu bu işlemleri saydıktan sonra “*gibi*” ifadesini kullanmak suretiyle başka işlemlerin de veri işleme tabirinin kapsamına girebileceğine dikkat çekmiştir. O halde veri işlemenin varlığından söz edebilmek için kişisel veriler üzerinde herhangi bir işlemin yapılmış olması yeterlidir.

Veri işlemeden söz edebilmek için söz konusu işlemlerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla gerçekleştirilmesi gerekmektedir. Otomatik olmayan yollarla ve veri kayıt sisteminin bir parçası olmadan kişisel veriler üzerinde yapılacak işlemler veri işleme olarak kabul edilmemiştir. Burada kanun koyucu kanunun kapsamı başlığını taşıyan ikinci maddede koyduğu kriterin bir benzerini getirmiştir. Verilerin otomatik olmayan yollarla veri kayıt sistemiyle ilişkili olmadan işlenmesi durumunda bu kanunun uygulanmayacağı bu tanım ile de pekiştirilmek istenmiştir.

1.4.3. Açık Rıza

Açık rıza kişisel verilerin korunması hukukunun en önemli kavramlarından birisidir. Kişisel verilerin işlenmesinin hukuka uygun hale gelebilmesi açık rızanın varlığına ya da diğer veri işleme şartlarının gerçekleşmesine bağlıdır. Anayasa’nın kişisel verilerin korunması hakkını düzenleyen 20/3 fıkrasında kişisel verilerin yalnızca kişinin açık rızası ile veya kanunda öngörülen hallerde işlenebileceği ifade edilmiştir. Uluslararası belgelerde ve veri koruma kanunlarında da kişisel verilerin işlenmesi genel olarak açık rıza şartına bağlanmıştır.

95/46/EC Sayılı Direktif’e, GVKT’ye ve Anayasa’daki hükme paralel olarak 6698 Sayılı Kanun’da da açık rıza kavramına yer verilmiştir. Kanunda açık rıza “*belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanan rıza*” olarak

tanımlanmıştır²⁰⁵. Bu tanımdan yola çıkarak açık rızanın meydana gelebilmesi için şu üç unsurun gerçekleşmesi gerektiği söylenebilir;

- Rıza belirli bir konuya ilişkin olmalıdır. Konusu, içeriği ve kapsamı tam olarak belirli olmayan bir şeye verilen rıza KVKK bakımından açık rıza olarak değerlendirilemeyecektir.
- Rıza bilgilendirmeye dayalı olarak verilmelidir. Rızayı verecek olan kişi rızanın kapsamı hakkında tamamen, açık ve net şekilde bilgilendirilmiş olmalıdır.
- Rıza kişinin özgür iradesini yansıtmalıdır. Bu unsur öncelikle kişinin rıza vermeye herhangi bir şekilde icbar edilmemiş olmasını kapsamakla birlikte diğer iki unsur ile de yakın ilişki içerisindedir. Bilgilendirmeye dayanmayan ve belirli bir konuya özgülenmemiş rızanın kişinin özgür iradesini ne kadar yansıttığı şüphelidir.

Kişisel verilerin işleme şartları başlığında açık rıza konusunu tekrar ele alacağımız için burada bu kadar bilgi vermenin yeterli olduğu kanaatindeyiz.

1.4.4. Anonim Hale Getirme

Kişisel verilerin anonim hale getirilmesi bu verilerin başka verilerle eşleştirilerek veya başka birtakım yollar kullanılarak dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir. Kişi ile veri arasındaki bağlantı koparılmaktadır. “*Kimliği belirli veya belirlenebilir*” bir kişiye ilişkin olan kişisel veri “*kimliği belirsiz ve belirlenemez*” bir kişiye ilişkin hale gelmekte, anonimleştirilmiş veriye dönüşmektedir. Anonim hale getirilen veriler aslında bir gerçek kişiye ilişkin bilgi sunmaya devam etmektedir. Fakat bu gerçek kişinin kim olduğunun tespit edilmesi imkansızlaştırılmakta, veri ile kişi arasındaki bağ sonsuza kadar koparılmaktadır.

Anonim hale getirmede kullanılacak yöntemlerin belirlenmesi oldukça teknik bir konudur. Kişisel Verileri Koruma Kurumu da anonim hale getirme yöntemleri konusunda

²⁰⁵ Kanunun üçüncü maddesinin gerekçesinde 95/46/EC sayılı direktif esas alınarak bir tanım yapıldığı ifade edilmiştir. Gerekçe: “*Açık rıza, 95/46 EC sayılı Direktif dikkate alınarak tanımlanmaktadır. Buna göre, açık rıza ilgili kişinin kendisiyle ilgili veri işlenmesine, özgürce, konuyla ilgili yeterli bilgi sahibi olarak, tereddüde yer bırakmayacak açıklıkta ve sadece o işlemle sınırlı olarak verdiği onay beyanı şeklinde anlaşılmalıdır.*” **Tasarı**, s.7.

yol gösterici olması için bu teknik ayrıntıları ihtiva eden bir rehber yayınlamıştır²⁰⁶. Bu rehberde verilerin nasıl anonim hale getirilebileceğine ilişkin örnekler verilmiştir. Fakat bu yöntemler kullanılarak anonim hale getirilmiş verilerin de zaman zaman anonimliğini kaybetmesi söz konusu olabilmektedir. Anonimleştirme işlemi yapılırken uygulanan adımları tersine uygulayarak veya anonim halde yayınlanan bilgileri başka bilgilerle birlikte değerlendirilerek kimlik tespiti yapılması zaman zaman mümkün olabilmektedir. Bugün eldeki verilerden hareketle kimliğinin tespit edilmesi mümkün olmayan birisi yarın yeni üretilen bir yazılım sayesinde kimliği belirlenebilir hale gelebilmektedir. Dolayısıyla verilerin anonim hale getirilmesi işlevsel bir yöntem olsa da bazı riskleri de içerisinde barındırmaktadır. Verileri anonim hale getirerek kullanma yoluna giden veri sorumlusu verilerin anonimliğini herhangi bir şekilde kaybetmesi riskinden de sorumlu tutulmalıdır.

1.4.5. Veri İşleyen ve Veri Sorumlusu

Kanuna göre veri sorumlusu kavramı “*Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi*” ifade eder.

Veri sorumlusunun kim olduğunun tespit edilmesi kişisel verilerin korunması hukukunda son derece önemlidir. Çünkü kanun veri sorumlusuna pek çok yükümlülükler yüklemektedir. Onuncu maddede düzenlenen aydınlatma yükümlülüğü ve yedinci maddede düzenlenen verileri silme, yok etme, anonim hale getirme yükümlülüğü ve on ikinci maddede düzenlenen veri güvenliğini sağlama yükümlülükleri bunlara örnek gösterilebilir. Ayrıca veri sahibi 11inci maddede düzenlenen haklarını veri sorumlusuna başvurmak suretiyle kullanabilmektedir. Veri sahibinin haklarını kullanabilmesi bakımından da veri sorumlusunun kim olduğunu tespit etmek önemlidir.

²⁰⁶ **Kişisel Verileri Koruma Kurumu**, Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi, tam metin (<https://www.kvkk.gov.tr/yayinlar/K%C4%B0%C5%9E%C4%B0SEL%20VER%C4%B0LER%C4%B0N%20S%C4%B0L%C4%B0NMES%C4%B0,%20YOK%20ED%C4%B0LMES%C4%B0%20VEYA%20ANON%C4%B0M%20HALE%20GET%C4%B0R%C4%B0LMES%C4%B0%20REHBER%C4%B0.pdf>) s.e.t. 17.01.2023

Veri sorumlusunun kim olduğunun tespit edilmesi TCK m.138’de düzenlenen suçun failinin tespit edilmesi bakımından da son derece önemlidir. Keza KVKK’nın 7nci maddesinde yer alan verileri silme, yok etme veya anonim hale getirme yükümlülüğüne uymayan veri sorumluları TCK m.138’de düzenlenen suçtan sorumlu tutulabilmektedir.

Veri sorumlusu veri kayıt sisteminin ve veri işleme faaliyetlerinin yönetimini sağlayan kişidir. Veri sorumlusunu tespit için öğretide ve Kişisel Verileri Koruma Kurulu kararlarında bazı kriterler zikredilmiştir. Hangi verilerin, hangi amaçla, ne kadar süre depolanacağı, kimlere aktarılacağı, bu verileri korumak için ne gibi tedbirler alınacağı gibi konularda karar vermeye yetkili bulunan kişi veri sorumlusu olarak kabul edilmelidir²⁰⁷. Her ne kadar veri sorumlusu tanımında gerçek veya tüzel kişi ifadesi kullanılmış olsa da Kişisel Verileri Koruma Kurulu bir kararında tüzel kişiliğe sahip olmayan apartman kat malikleri kurulunun da veri sorumlusu olabileceğini ifade etmiştir. Kurula göre veri sorumlusunun kim olduğu tespit edilirken her somut olayın şartlarına göre özel bir değerlendirme yapılmalıdır. Bu değerlendirme sırasında veri kayıt sistemini kuran, uhdesinde bulunduran ve yöneten birim ve yetkili kişi tespit edilmelidir²⁰⁸.

Veri işleyen tabiri ise kanuna göre “*veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi*” ifade eder. Veri işleyen kendisine verilen yetkinin sınırları içerisinde hareket edebilir, karar alabilir ve uygulayabilir²⁰⁹. Veri işleyen daha çok işlemleri yürüten pozisyonundayken, veri sorumlusu veri işleme faaliyetlerinden hukuken sorumlu olan ve bu faaliyetler üzerinde yönetici pozisyonunda bulunan kişidir. Bununla birlikte veri sorumlusu bazı yetkilerini veri işleyene devretmiş olabilir. Devredilen bu yetkiler daha çok teknik konularla ilgilidir. Bunlar genellikle verilerin nasıl depolanacağı, nasıl yok edileceği, verilerin muhafazası için alınabilecek önlemlere dair teknik ayrıntıların tespiti gibi hususlardır. Bu tür teknik hususları ve yürütülecek işlemleri bir şahsa devretmiş olması veri işleyeni sorumluluktan kurtarmayacak, veri sorumlusunun yükümlülükleri devam edecektir²¹⁰. Veri işleyen de işleme faaliyetleri sırasında veri güvenliğine ilişkin tedbirleri almak konusunda veri sorumlusu ile birlikte müştereken sorumludur.

²⁰⁷ Öztürk / Seyhan / Altınok, s.40-41.

²⁰⁸ Öztürk / Seyhan / Altınok, s.39.

²⁰⁹ Öztürk / Seyhan / Altınok, s.42.

²¹⁰ Uyarer, Sinem Göçmen (2020) Kişisel Verilerin Korunması, 2. Baskı, Ankara, Seçkin, s. 122.

1.4.6. Veri Kayıt Sistemi

Veri kayıt sistemi kanunda “*kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi*” olarak tanımlanmıştır. Veri kayıt sistemi elektronik veya fiziksel olabilir. Veri kayıt sistemleri verilere ulaşmayı ve verileri kullanmayı kolaylaştıran sistemlerdir. Örneğin kişilerin kredi kartı borcunu ödeme durumu, öğrenim durumu, tuttukları takım, üye oldukları sendika gibi herhangi bir bilgi türü üzerinden tasnif edildiği, kişiler hakkında bir veya birden fazla veriye daha kolay ve toplu bir şekilde ulaşmayı sağlayan herhangi bir sistem veya fiziki bir dosya, klasör veya kâğıt veri kayıt sistemi olarak kabul edilebilir.

Günümüzde veri kayıt sistemleri daha çok elektronik ortamda oluşturulmaktadır. Bu sistemlere entegre olarak çalışabilen belirli işlevlere sahip programlar ile veriler otomatik yollarla işlenmektedir.

2. KİŞİSEL VERİLERİN İŞLENMESİNE İLİŞKİN TEMEL İLKELER

Kişisel verilerin korunmasına mahsus diğer pek çok hukuki belgede olduğu gibi²¹¹ KVKK’da da verilerin işlenmesi sırasında uyulması gereken bazı genel ilkeler sayılmıştır. Kanunun 4üncü maddesinin birinci fıkrasında kişisel verilerin ancak bu kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun şekilde işlenebileceği ifade edilmiştir. Birinci fıkrada kişisel verilerin korunmasının esas olduğu ve işlemenin ancak istisnai olarak ve kanunla düzenlenen durumlarda yapılabileceği teyit edilmiştir. İkinci fıkrada ise veri işleme süreçlerine hâkim olması gereken ilkeler sayılmıştır. Bunlar “*hukuka ve dürüstlük kuralına uygun olma, doğru ve gerektiğinde güncel olma, belirli, açık ve meşru amaçlar için işlenme, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma, gerekli olan süre kadar muhafaza edilme*” ilkeleridir. Bu temel ilkelere verilerin yok edildiği ana kadar gerçekleştirilen bütün işleme faaliyetlerinde uyulması zorunludur. Bu ilkelere aykırı

²¹¹ OECD Rehber İlkeleri İkinci Bölüm, 108 Sayılı Avrupa Konseyi Sözleşmesi 5inci madde, 95/46/EC Sayılı AB Direktifi 6ncı madde, GVKT 5inci madde.

hareket edilmesi işlemin hukuka uygunluğunu ortadan kaldıracaktır ve veri işleyenin sorumluluğu doğacaktır²¹².

Bu ilkeler birbirlerinden tamamen ayrı muhtevalara sahip değildir. Daha çok birbirini ve kanunun diğer hükümlerini tamamlayıcı niteliktedir. Bu ilkelerin ekseriyeti veri koruma hukukunun yeni ortaya çıkmaya başladığı dönemlerde kabul edilmiş ve günümüzde de hukuki metinlerde yer almaya devam etmiştir. Bu ilkelerin işaret ettiği hususlarda zamanla ayrıntılı düzenlemeler yapılmıştır. Veri koruma hukukunun bu ilkeler doğrultusunda geliştiği göz önünde bulundurulduğunda bu ilkelerin kanunda yer alan diğer hak ve yükümlülüklerin ve veri işleme şartlarının özünü oluşturduğu söylenebilir.

2.1. Hukuka ve Dürüstlük Kuralına Uygun Olma

Bu ilkeye göre veri işleme faaliyetleri hukuka ve dürüstlük kuralına uygun olarak yürütülmelidir. Bu ilke diğer ilkelerin temelini oluşturmaktadır. Çünkü hukuka ve dürüstlük kuralına uygun olma ilkesi diğer ilkeleri saran, kapsayan ve onların özünü meydana getiren bir ilkedir. Bu sebeple veri koruma hukukunun temel ilkesi olarak kabul edilebilir²¹³. İlkeyi, hukuka uygunluk ve dürüstlük kuralına uygunluk olarak iki kısımda incelemek mümkündür.

Hukuka uygunluk genel olarak hukuk düzenine uygunluğu ifade eder. Veri işleme faaliyetlerinin başta Anayasa'ya olmak üzere 6698 sayılı KVKK'ya, diğer kanunlara ve ilgili yönetmeliklere uygun olarak gerçekleştirilmesi anlamına gelir. Dürüstlük kuralına uygunluk ifadesini ise tarif etmesi nispeten daha zordur. Dürüstlük kuralına uygunluk genellikle öğretide veri işleyenin ilgili kişinin çıkarlarını ve makul beklentilerini dikkate alması olarak açıklanmaktadır²¹⁴. Dürüstlük kuralını veri işleyenin iyiniyetli hareket etmesi olarak da tanımlamak mümkündür. Bazen veri işleme faaliyeti açık rızanın alınmış olması veya diğer veri işleme şartlarının gerçekleşmiş olması sebeplerinden biriyle hukuka uygun kılınmış olabilir. Ancak veri işleyenin kötü niyetli ya da özensizce gerçekleştirdiği bazı davranışlar verisi işlenen kişi aleyhine bazı sonuçların doğmasına sebep olabilir. İşte bu tip

²¹² Korkmaz, s.119.

²¹³ Bygrave, s.58.

²¹⁴ Küzeci, s.228-229.

durumlarda veri işleyenin hareketlerinin hukuka uygun olmasına rağmen dürüstlük kuralına uygun olmadığı söylenebilecektir. Veri işleyenin ilgili kişiyi yanıltarak rızasını alması, bilgisizliğinden faydalanması, topladığı verileri amacı dışında kullanması gibi durumlarda da dürüstlük kuralı elbette ihlal edilmiş olacaktır. Fakat bu durumlar zaten diğer ilkeler ve veri işleme şartları kapsamında korunmaktadır.

2.2. Belirli, Açık ve Meşru Amaçlar İçin İşlenme

Veri işleme faaliyetinin bu ilkeye uygun olabilmesi için iki şartın yerine gelmiş olması gerekmektedir. Birinci şart verilerin belirli ve açık amaçlar için işlenmesidir. İkinci şart ise bu amaçların meşru olmasıdır. Bu iki şartı ayrı ayrı ele almak gerekmektedir.

Veri işlemenin belirli ve açık amaçlar doğrultusunda yürütülmesi, kişisel verilerin sadece toplanması aşamasında değil yok edilmesine kadar uygulanacak bütün işlemlerde amacın belirli ve açık olmasını ifade eder. Bu ilkeye göre veri işleyenin amacı herhangi bir tereddüde mahal bırakmayacak biçimde tam ve net olarak belirli olmalıdır. Bu ilke veri sorumlusunun ilgili kişiyi bilgilendirme yükümlülüğünün de temelini oluşturmaktadır. Veri sorumlusu veri sahibini verilerinin hangi amaçlarla işleneceği konusunda açık ve net bir şekilde aydınlatmakla yükümlüdür.

Veri işleme süreçlerinde belirliliğin ve açıklığın sağlanması her şeyden önce konuyla ilgili hukuki düzenlemelerde belirsiz ifadelerden kaçınılmasıyla mümkündür. Ayrıca kişisel verilerin olur da bir gün gerekirse mantığı ile toplanması da amacın belirliliği ve açıklığı ilkesine terstir²¹⁵.

Amacın belirli ve açık olması tek başına yeterli değildir. Aynı zamanda bu amacın veya amaçların meşru da olmaları gerekir. Meşruluk, öğretide genellikle veri işleme faaliyetlerinin hukuki düzenlemelerde belirtilen usul ve esaslara uygun yürütülmesi olarak ifade edilmektedir. KVKK'nın veri işleme şartlarını düzenleyen 5 ve 6ncı maddelerine atıf yapılmaktadır²¹⁶. Ancak bu ifadeler amacın meşruiyeti kavramını kuşatmakta yetersiz

²¹⁵ **Küzeci**, s.231.

²¹⁶ Bkz. **Küzeci**, s.232 ve 386.

kalmaktadır. İşlenmesine açık rıza verilmiş veya alenileştirilmiş verilerin işlenmesi dışında, diğer veri işleme şartlarına dayanarak yapılan işleme faaliyetleri bakımından amaç, hukuka uygunluğun temelini oluşturduğu için bir beis yoktur. Fakat açık rızaya dayanarak yapılan işleme faaliyetlerinde veya kişinin kendisi tarafından alenileştirilmiş veriler üzerindeki veri işleme faaliyetlerinde veri işleyeninin gayri meşru bir amaç ile veri işlemesi imkân dahilindedir. Yani amacın meşruiyeti için veri işleme faaliyetinin hukuka uygunluk sebeplerinden birine dayanması tek başına yeterli görülmemelidir. Gerçekten de kimi zaman kişinin kendisi tarafından alenileştirilmiş bazı veriler gayri meşru amaçlar için kullanılabilir. Örneğin herkese açık sosyal medya profilinde paylaşılan bir fotoğrafın alınıp bir online arkadaşlık sitesinde profil oluştururken kullanılmasında durum böyledir. Dolayısıyla diğer hususların yanında amacın da özel olarak hukuka uygunluğu değerlendirilmelidir. Bazı yazarlar meşruiyet kavramını daha geniş yorumlayarak bunun yalnızca hukuka uygunluğu değil sosyal kabul edilebilirliği de kapsadığını ifade etmiştir²¹⁷.

2.3. İşlendikleri Amaçlarla Bağlantılı, Sınırlı ve Ölçülü Olma

Bu ilke yukarıda ele aldığımız belirli, açık ve meşru amaçlar için işlenme ilkesiyle doğrudan bağlantılıdır. Bu iki ilkenin sınırlarını birbirinden ayırmak zordur. Bu ilkeler birbirini tamamlar ve teyit eder niteliktedir. Belirli, açık ve meşru olan amaç ile bağlantılı olmayan verilerin işlenmesi, veri işleme faaliyeti sırasında amacın sınırlarının dışına çıkılması yasaktır. Gerekçede bu ilke “*Kişisel verilerin, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması ilkesi, işlenen verilerin, belirlenen amaçların gerçekleştirilebilmesine elverişli olmasını, amacın gerçekleştirilmesiyle ilgili olmayan veya ihtiyaç duyulmayan kişisel verilerin işlenmesinden kaçınılmasını gerektirmektedir.*” ifadeleriyle açıklanmıştır²¹⁸. Bizce de bu açıklama yerindedir. Ancak bazı örneklerle desteklenmesinde fayda vardır.

Örneğin yakın çevredeki restoranlardan online olarak sipariş vermenizi sağlayan bazı platformlar bulunmaktadır. Bu platformlara üye olurken kullanıcılar tarafından isim, adres ve telefon numarası gibi bazı bilgiler verilmektedir. Sipariş oluşturulduğunda bu

²¹⁷ Bygrave, s.61.

²¹⁸ Tasarı, s.8.

bilgiler siparişi hazırlayacak restorana iletilmekte, restoranın kuryesi elindeki bilgilere göre teslimatı gerçekleştirmektedir. Ülkemizde de bu tür platformlar yaygın olarak kullanılmaktadır. Ancak sınırlı ve ölçülü veri işleme prensibine uygun hareket eden firmalar olduğu gibi bu prensibe uymayan firmalar da bulunmaktadır. Somut bir biçimde açıklamak gerekirse; A platformu sipariş veren kişinin telefon numarası, adı soyadı gibi bilgilerinin tamamını restoran ve kurye ile paylaşırken B platformu soyadını gizlemekte, yalnızca isim ve adres bilgisi paylaşmaktadır. B platformunda sipariş verenin soyadı ve telefon numarası yalnızca platform yetkilisi tarafından görüntülenebilmektedir. Kurye adres yanlışlığı veya kapının açılmaması gibi sorunlarla karşılaştığında platformun sağladığı uygulamadan sipariş sahibini ara seçeneğini kullanarak sipariş sahibini arayabilmektedir. Bu arama kuryenin telefonundan platformunun santraline yönelmekte, kurye ile müşteri arasındaki bağlantı santral tarafından numaranın yönlendirilmesi ile sağlanmaktadır. Böylece kurye müşterinin, müşteri de kuryenin telefon numarasını öğrenmemektedir. Bu durum amaca ulaşmak için gereken miktarda verinin işlenmesine güzel bir örneklik teşkil etmektedir. Amaca ulaşmak için zaruri olmayan verilerin işlenmesi veri sahibinin haksızlığa uğrama riskini artıracaktır. Keza ülkemizde de bu ilkeye dikkat edilmemesi sebebiyle hak ihlallerinin yaşandığı bir gerçektir²¹⁹.

Kişisel verilerin rıza ile alındığı durumlarda genellikle ölçülülük sorunu gündeme gelmemektedir. Çünkü kişi kendi rızası ile verilerini paylaşmaktadır. Ancak veri sahibinin bir hizmetten ya da bir haktan faydalanabilmek için verilerini paylaştığı bazı durumlarda ölçülülük konusunda problemler oluşabilmektedir. Sözleşmeden doğan sorumluluğun veya hizmetin yerine getirilebilmesi veya bir ilişkinin kurulabilmesi için verilerin alındığı durumlarda amacın gerektirdiğinden daha fazla veri toplanıyorsa bu ilkenin ihlal edildiğinden söz edilebilecektir. İş sözleşmeleri bunun tipik bir örneğidir. İş başvurularında başvuru sahiplerinden pek çok belge istenmektedir. İş başvurusunda bulunan kişiler başvurularının reddedilmesi korkusuyla normalde paylaşmak istemeyecekleri verileri de

²¹⁹ Kuryelerin sipariş götördükleri müşterilere daha sonra rahatsız edici mesajlar atmaları, aramaları gibi olaylar sıklıkla yaşanmaktadır. Özellikle ülkemizde bir firmada yıllardır aynı sorunun yaşanıyor olması ve halen bir önlem alınmamış olması KVKK hükümlerinin ne kadar etkin uygulandığı konusunu sorgulatmaktadır. Haberlere yansıyan örnek olaylar için bkz. Olay 1 – (<https://www.hurriyet.com.tr/ekonomi/siparis-veren-kadini-taciz-etti-isinden-kovuldu-28285941>) s.e.t. 17.01.2023. Olay 2 – (<https://www.sabah.com.tr/yasam/tacizcisini-randevuyla-polislere-yakalatti-6233362>) s.e.t. 17.01.2023. Olay 3 – (<https://www.gercekgundem.com/guncel/153772/yemek-siparisi-verdi-kurye-tarafindan-tacize-ugradi>) s.e.t. 17.01.2023

paylaşmak zorunda kalmaktadır. Böylesi bir durumda bu ilkenin ihlal edildiği kabul edilebilir²²⁰.

2.4. Gerekli Olan Süre Kadar Muhafaza Edilme

Amaç ile sınırlılık, hukuka uygunluk ve dürüstlük ilkelerinin yansımalarından birisi de verilerin gerekli olan süre kadar muhafaza edilmesidir. Bu ilkeye göre kişisel veriler *“ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar”* muhafaza edilmelidir. Bu ilke de iki ayrı duruma işaret etmektedir. Birincisi verilerin ne kadar süre tutulacağına ilişkin mevzuatta belirli bir sürenin öngörülmüş olması durumudur. Bazı kişisel verilerin tutulacağı süre kanunlar veya yönetmelikler tarafından belirlenmiş, bu sürelerin sonunda veri sorumlusuna verileri imha etme yükümlülüğü yüklenmiştir. Bazı veriler açısından ise hukuki düzenlemelerde net bir süre öngörülmemiştir. Bu tür verilerin saklanacağı süre işlendikleri amaca göre belirlenir. Eğer işleme amacı ortadan kalkmışsa, daha önceden belirlenmiş amaç ile ilgili olarak artık işlenmesine gerek kalmamışsa bu verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi gerekir.

Kanunda belirlenen sürelerin dolmasından ya da işleme amacının ortadan kalkmasından sonra ne kadar süre içerisinde verilerin imha edilmesi gerektiği yönetmelik ile belirlenmiştir. Kişisel Verileri Koruma Kurumu 28 Ekim 2017 tarihinde Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik başlığıyla bir yönetmelik yayınlamıştır²²¹. Bu yönetmeliğin 11inci maddesinde kişisel verileri resen silme, yok etme veya anonim hale getirme süreleri düzenlenmiştir. Buna göre kişisel veri saklama ve imha politikası²²² hazırlamakla yükümlü olan veri sorumluları, verileri imha yükümlülüğünün doğduğu tarihten sonraki ilk periyodik imha işleminde bu işlemlerden birini (silme, yok etme, anonim hale getirme) yapmakla yükümlüdür. Bu süre her halde 6 ayı geçemez. Saklama ve imha politikası hazırlamakla yükümlü olmayan veri

²²⁰ Küzeci, s.238.

²²¹ Tam metin için bkz. (<https://www.resmigazete.gov.tr/eskiler/2017/10/20171028-10.htm>) s.e.t. 17.01.2023

²²² Kişisel veri saklama ve imha politikası veri sorumlularının, kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi belirleme işlemi ile silme, yok etme ve anonim hale getirme işlemi için dayanak yaptıkları politikayı ifade eder. (Yönetmelik m. 4/1-f) Veri Sorumluları Siciline kayıt olmakla yükümlü olan veri sorumluları, kişisel veri işleme envanterine uygun olarak kişisel veri saklama ve imha politikası hazırlamakla yükümlüdür. (Yönetmelik m. 5)

sorumluları ise verileri imha etme yükümlülüğünün doğmasından itibaren 3 ay içinde bu işlemlerden birini yapmakla yükümlüdür.

Verilerin silinmesi ve yok edilmesi kavramları benzer manalar ifade etmektedir. Anonim hale getirme ise kavramlar başlığında açıkladığımız üzere *“kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesini”* ifade etmektedir. Bu işlemlerden herhangi birinin yapılması KVKK tarafından veri sorumlusuna yüklenen yükümlüğün yerine gelmesi için yeterlidir. Veri sorumlusu bu yükümlülüğünü yerine getirmemesi halinde KVKK 17/2’ye ve TCK 138’e göre sorumlu olur. Bu konuya ilişkin detaylar ileride verileri yok etmeme suçu başlığı altında ele alınacaktır.

2.5. Doğru ve Gerektiğinde Güncel Olma

Kişisel verilerin işlenmesi sürecine hâkim olan bir diğer ilkeye göre veriler doğru ve gerektiğinde güncel olarak tutulmalıdır. Verilerin doğru ve güncel olmasını sağlamak veri sorumlusuna yüklenmiş bir yükümlülüktür. Veriler bir amaç doğrultusunda işlenmektedir. Bu amaç kimi zaman bir kamu hizmetinin görülmesi, kimi zaman sözleşmenin gereklerinin yerine getirilmesi, kimi zaman bir hizmetin sunulması, kimi zaman da veri işleyenin ticari menfaatler elde etmesidir. Verilerin hukuka uygun olarak işlendiği durumların çoğunda hem ilgili kişinin hem de veri işleyenin menfaatleri söz konusudur. Dolayısıyla verilerin yanlış işlenmesi halinde genellikle hem ilgili kişinin hem de veri işleyenin menfaatleri zedeleneyecektir. Bu ilke doğru olmayan verilerin işlenmesi sebebiyle meydana gelebilecek zararlardan hem veri işleyeni hem de ilgili kişiyi koruma amacı gütmektedir.

Verilerin doğru ve güncel olarak tutulması kişisel veri hukukunun ilk zamanlarında ortaya çıkmış ilkelerden biridir. İlk zamanlarda verilerin daha çok kamu sektörü tarafından işlendiğini ve bu işlemenin daha çok kamusal hizmetlerin görülmesi ile kamu güvenliğinin sağlanması maksatlarına odaklandığı dikkate alındığında, geçmişte ilkenin birey ve toplum menfaatine hizmet eden yönünün ağır bastığı söylenebilir. Öğretide de ilkeye dair açıklamaların genellikle ilkenin birey menfaatini koruyan yönü öncelenerek yapıldığı göze

çarpmaktadır²²³. Ancak günümüzde verilerin genellikle özel sektör tarafından birtakım ekonomik menfaatler elde etme maksadıyla işlendiği göz önünde bulundurulduğunda bu ilkenin daha çok veri işleyenin menfaatlerine koruma sağlayacağını söylemek yanlış olmaz. Müşteri tercihlerinin saptanması, doğru kişilere doğru ürünlerin pazarlanması, kullanıcı hareketleri göz önünde bulundurularak ürünlerin geliştirilmesi gibi, veri işleyenin menfaatlerine hizmet eden veri işleme faaliyetleri bugünün dünyasında veri işleme faaliyetlerinin büyük kısmını oluşturmaktadır. Bunların yanında elbette kişisel verilerin ilgili kişilerin menfaatine işlendiği pek çok durum da varlığını korumaktadır.

Kişisel verilerin doğru ve gerektiğinde güncel olarak tutulması veri sorumlusuna yüklenmiş bir yükümlülük olmakla birlikte veri sorumlusunun bu yükümlülüğü tek başına yerine getirmesi çoğu zaman mümkün değildir. Çünkü verilerin doğru olup olmadığını bilebilecek en iyi kişi aslında veri sahibidir. Fakat veri sorumlusunun bilgilerin güncelliğini veya doğruluğunu teyit etmek için sık sık veri sahibine bildirim göndermesi de uygun değildir. Veri sahibinin bilgilerinde bir değişiklik olması durumunda veri sorumlusunu bilgilendirmesi daha doğru bir yol olacaktır. Veri sorumlusunun veri sahibine istediği zaman zahmetsiz bir şekilde bilgilerine ulaşabilme, yanlışları düzeltebilme ve güncellemeleri yapabilme imkânı sunması bu yükümlülüğü yerine getirmesi için işlevsel bir yöntemdir. Bugün internet sitelerinde kullanıcıların üyelik bilgilerini güncellemelerine imkân tanıyan arayüzlerin yer alması buna örnek olarak gösterilebilir. Böylece ilgili kişinin verilerine erişim hakkı da sağlanmış olacaktır²²⁴. Bunun yanı sıra veri sorumlusu verilerin yanlışlığını kendi imkânlarıyla tespit etmişse, veri sahibinin talebini beklemeden bu yanlışlığı ortadan kaldırmakla yükümlüdür. Bu yükümlülüğünü yanlış düzelterek veya yanlış veriyi imha ederek yerine getirebilir.

3. KİŞİSEL VERİLERİN İŞLENME ŞARTLARI

Kişisel verilerin korunması hakkını düzenleyen Anayasa'nın 20/3 maddesi hükmünde kişisel verilerin ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebileceği ifade edilmiştir. Kişisel verilerin korunması kural işlenmesi ise istisnadır. Bu

²²³ Küzeci, s.243, 244. Yılmaz, Berrak, s. 99. Korkmaz, s.124.

²²⁴ Küzeci, s.243, 244.

istisnanın ilki kişisel verilerin işlenmesinin kanunda açıkça öngörölmüş olmasıdır. Kişisel veriler kanunda belirtilen hallerde kanunun izin verdiği kadarıyla sınırlı olmak üzere işlenebilir. Böylesi bir durumda veri işleme fiili hukuka uygundur. Veri işleme fiilini hukuka uygun hale getiren bir diğer durum ise ilgili kişinin açık rızasının varlığıdır.

Anayasa’da yer alan, kişisel verilerin yalnızca kanunlarda öngörölen hallerde işlenebileceği hükmü doğrultusunda, 6698 Sayılı Kanun’un 5inci ve 6ncı maddelerinde kişisel verilerin işlenme şartları düzenlenmiştir. 6ncı maddede özel nitelikli veri kategorileri sayılmış ve bu kategorilerdeki verilerin işlenmesi için diğer verilere nazaran daha sıkı şartlar öngörölmüştür. 6ncı maddede sayılan özel nitelikli veri kategorilerine girmeyen verilerin işlenmesi bakımından aranacak şartlar ise 5inci maddede düzenlenmiştir.

3.1. Özel Nitelikli Olmayan Kişisel Verilerin İşlenme Şartları

Özel nitelikli kişisel verilerin²²⁵ dışında kalan diğer kişisel veri türlerinin işlenme şartları kanunun 5inci maddesinde iki fıkra halinde düzenlenmiştir. Birinci fıkrada kişisel verilerin kişinin açık rızası bulunmadan işlenemeyeceği belirtilmiş, ikinci fıkrada ise açık rızanın bulunmadığı hallerde de kişisel verilerin işlenebileceği istisnai haller sayılmıştır. Bu düzenleme şekli açık rıza dışında kalan diğer veri işleme şartlarını açık rıza kuralının bir istisnası konumuna getirmiştir. Fakat Anayasa’da kişisel verilerin işlenme şartlarını belirleyen düzenleme açık rızanın varlığını ve kanunda öngörölen diğer hallerin varlığını eşdeğer kabul etmektedir²²⁶. Anayasa’ya göre kanunda öngörölen haller açık rıza şartının istisnası değildir. Birinci fıkranın “*Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez*” yerine “*Kişisel veriler ilgili kişinin açık rızasının varlığı durumunda işlenebilir.*” şeklinde düzenlenmesi, kişisel verilerin işlenebileceği diğer durumların ise

²²⁵ Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir. Bu kategorilerdeki veriler açısından 6ncı maddede yer alan işleme şartları aranmaktadır. Bu kategorilerin dışındaki veriler için ise 5inci madde hükümleri geçerlidir.

²²⁶ AY m.20/3; “.....*Kişisel veriler, ancak kanunda öngörölen hallerde veya kişinin açık rızasıyla işlenebilir....*”

devam eden fıkralarda düzenlemesi yerinde olurdu. Böylesi bir düzenleme Anayasa'daki formülasyona da daha uygun olurdu²²⁷.

3.1.1. Açık Rızanın Bulunması

6698 Sayılı Kanun kişisel verilerin açık rıza olmaksızın işlenmesini yasaklamıştır (m.5/1 & m.6/2). Açık rıza kavramı ise kanunun 3üncü maddesinde tanımlanmıştır. Bu tanıma göre açık rıza *“belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza”* anlamına gelir. Bu tanımdan yola çıkarak açık rızanın belirli bir konuya ilişkin olma, bilgilendirmeye dayanma ve özgür iradeyle açıklanma şeklinde üç unsurunun bulunduğu anlaşılmaktadır. Bu üç unsurun hepsi gerçekleşmeden açık rızanın varlığından söz etmek mümkün değildir.

Belirli bir konuya ilişkin olma şartı kişisel veriler hakkında açık uçlu genel rızaların geçersiz olduğunu ifade etmektedir. Rıza veren kişi hangi verilerinin, hangi konularla ilgili olarak işleneceğini bilmelidir²²⁸. Rıza veren kişi beyanında bu hususları açıkça ifade etmelidir. Rıza beyanının bir istemin onaylanması şeklinde gerçekleştirildiği durumlarda da ilgili kişiye sunulan açık rıza istem metninde hangi verilerin hangi konularla ilgili olarak işleneceği açıkça belirtilmelidir. *“Bütün kişisel verilerimin işlenmesine rıza gösteriyorum”* şeklindeki rıza beyanları Kurul tarafından *“battaniye rıza”* olarak tabir edilmekte ve geçersiz sayılmaktadır²²⁹. İlgili kişi birden fazla kategorideki verisinin işlenmesine açık rıza verecekse rıza beyanında bu kategorilerin neler olduğu ve verilerin hangi amaçlar doğrultusunda işleneceği açıkça yer almalıdır.

Bilgilendirmeye dayalı olma şartı ise ilgili kişinin, veriler üzerinde ne tür işlemlerin gerçekleştirileceği ve hangi amaçlarla verilerinin işleneceği gibi konularda veri sorumlusu tarafından detaylı şekilde aydınlatılması anlamına gelir. Bu aydınlatma açık rıza verilmeden önce gerçekleştirilmelidir. Rıza verildikten sonra yapılan bilgilendirme rızayı

²²⁷ Benzer görüş için bkz. **Koca, Mahmut / Üzülmaz, İlhan** (2020) Türk Ceza Hukuku Özel Hükümler, 7. Baskı, Ankara, Adalet Yayınevi, s.563

²²⁸ **Uyarer**, s.112.

²²⁹ **Kişisel Verileri Koruma Kurulu**, Açık Rıza Alınırken Dikkat Edilecek Hususlar, (<https://www.kvkk.gov.tr/Icerik/2037/Acik-Riza-Alirken-Dikkat-Edilecek-Hususlar>) s.e.t. 17.01.2023

hukuka uygun hale getirmez. Veri sorumlusu bu yükümlülüğünü aydınlatma metni marifetiyle yerine getirir. Aydınlatma metnindeki ifadeler açık, sade, net ve anlaşılır olmalıdır²³⁰.

Özgür irade ile açıklanma şartı ise öncelikle iradenin hile, korkutma ve aldatma gibi herhangi bir yolla sakatlanmamış olmasını ifade eder. Bu etkenlerden biri ile irade sakatlanmışsa zaten geçerli bir rızadan bahsedilemeyecektir. Bu durum sadece açık rıza için değil her türlü rıza için geçerlidir. Gerek medeni hukuk gerekse ceza hukuku böylesi bir rızayı hukuka uygun verilmiş geçerli bir rıza olarak kabul etmemektedir.

Kişisel Verilerin Korunması hukukunda açık rızanın özgür irade ile verilme şartının gerçekleşmediği kabul edilen bazı durumlar vardır. Bunlardan ön önemlisi açık rızanın bir hizmetten faydalanabilmek için şart koşulması durumudur. Bir hizmet ilişkisi kurulurken o hizmetin yerine getirilmesi ile doğrudan ilişkili bulunmayan, alakasız kişisel verilerin talep edilmesi halinde, açık rızanın verilmesi hizmetten faydalanabilmenin şartı olarak sunulmuşsa açık rıza geçersizdir. Zira böylesi bir rızanın özgür irade ile verildiğini söylemek mümkün değildir²³¹. Açık rıza talep eden ile açık rıza veren arasında hiyerarşik ilişkinin bulunduğu hâllerde da buna benzer bir durum söz konusudur. Hiyerarşik ilişkinin bulunması elbette açık rızanın her durumda geçersiz olduğu anlamına gelmez. Fakat böylesi durumlarda rızanın özgür irade ile verilip verilmediğini hassasiyetle araştırmak gerekir.

Kişisel verilerin işlenmesi maksadıyla açık rıza alınması sırasında aynı rıza metnine kişisel verilerin yurtdışına aktarılabilceği ibaresinin de konulması durumunda yurt dışına aktarım için açık rıza verildiği kabul edilemez. Yurt dışına aktarım için kişinin ayrıca açık rıza vermesi gerekir. Yurt dışına aktarım için verilecek rızanın da açık rızada aranan şartları sağlaması gerekir²³².

Kişisel Verileri Koruma Kurulu'nun Whatsapp hakkında verdiği bir kararda verilerin işlemesine dair rıza ile yurtdışına aktarımına ilişkin rızanın tek onay ile verilmesinin mümkün olmadığı, kullanıcılara verilerin işlenmesi ve yurtdışına aktarımı

²³⁰ Öztürk / Seyhan / Altınok, s.68.

²³¹ Öztürk / Seyhan / Altınok, s.69.

²³² Açık Rıza Rehberi, s.4, Tam metin için bkz. (<https://kvkk.gov.tr/yayinlar/A%C3%87IK%20RIZA.pdf>) s.e.t. 17.01.2023

konusunda ayrı ayrı karar verme imkanının sunulması gerektiği, ayrıca hizmetten faydalanmanın açık rıza verme şartına bağlı kılınmasının kabul edilemeyeceği ve Whatsapp tarafından kullanıcılara dayatılan sözleşmenin hukuka aykırı olduğu ifade edilmiştir²³³. Sonuç olarak Whatsapp'ın 1.950.0000 TL idari para cezasına çarptırılmasına ve hukuka aykırılıkların giderilmesi için üç ay süre verilmesine hükmedilmiştir.

Özellikle elektronik ortamda açık rıza genellikle veri sorumlusunun talebi üzerine verilmektedir. Girdiğiniz çoğu internet sitesinde açılan bir uyarı penceresi vasıtasıyla size çerezleri kabul edip etmediğiniz sorulmaktadır. İlk ekranda karşınızda iki seçenek yer almaktadır. Genellikle bunlardan birisi “*kabul ediyorum*” seçeneği iken diğeri “*çerezleri yönet*” veya “*özelleştir*” seçeneğidir. Çerezleri kabul etmek istemiyorsanız önce çerezleri yönet seçeneğine basmanız, ardından çerezlerin her birini ayrı ayrı reddetmeniz, sonra onayla tuşuna basmanız gerekmektedir. Çerezleri kabul etmek tek tık kadar kolayken reddetmek o kadar da kolay değildir. Bu durumla karşılaşan internet kullanıcıları genellikle çerezleri kabul etmek istememesine rağmen bu zahmete katlanmamak için zoraki bir şekilde kabul et seçeneğine tıklamaktadır. Bu durumda açık rızanın özgür irade ile verildiğinden söz edilemeyeceği için rıza geçersiz sayılmalıdır. Tarif ettiğimiz sistemin bir benzerini uygulayan Google hakkında Fransız Veri Koruma Otoritesi (CNIL) tarafından verilen bir kararda bu durumun veri koruma kanununa aykırı olduğuna hükmedilmiş ve Google 150.000.000 euro para cezasına çarptırılmıştır²³⁴. CNIL benzer bir kararı Facebook için de vermiş ve bu firmayı da 60.000.000 euro para cezasına çarptırmıştır²³⁵.

Açık rıza ilgili kişinin olumlu irade beyanı ile verilmelidir. Kişinin sessiz kalması açık rızanın varlığı anlamına gelmez. Rızanın ilgili kişi tarafından aktif bir davranış ile verilmesi gerekir. Rıza şekil şartına bağlı değildir. Yazılı veya sözlü olması arasında, fiziki ortamda veya elektronik ortamda verilmesi arasında fark yoktur. Açık rızanın varlığı ve içeriği konusunda her türlü ispat yükü veri sorumlusuna aittir²³⁶.

²³³ Whatsapp Kararı, tam metin için bkz. (<https://www.kvkk.gov.tr/Icerik/7045/WHATSAPP-UYGULAMASI-HAKKINDA-YURUTULEN-RESEN-INCELEMEYE-ILISKIN-KAMUOYU-DUYURUSU>) s.e.t. 17.01.2023

²³⁴ **Öztürk / Seyhan / Altınok**, s.70-71. CNIL Google kararı için bkz. (https://www.cnil.fr/sites/default/files/atoms/files/deliberation_of_the_restricted_committee_no._san-2021-023_of_31_december_2021_concerning_google_llc_and_google_ireland_limited.pdf) s.e.t. 17.01.2023

²³⁵ CNIL Facebook kararı için bkz. (https://www.cnil.fr/sites/default/files/atoms/files/deliberation_of_the_restricted_committee_no._san-2021-024_of_31_december_2021_concerning_facebook_ireland_limited.pdf) s.e.t. 17.01.2023

²³⁶ Açık Rıza Rehberi, s.3.

Başka bir veri işleme şartının gerçekleşmesi ile hukuka uygun hale gelmiş veri işleme faaliyetleri için ayrıca bir de açık rızanın istenmesinin hukuka aykırı olduğu kabul edilmektedir. Açık rıza ancak başka bir veri işleme şartının gerçekleşmediği durumlarda alınmalıdır. Çünkü başka bir veri işleme şartının bulunduğu durumlarda açık rızası alınan kişi bu açık rızaya dayanılarak veri işleme faaliyetinin yürütüldüğünü düşünecektir. Bir süre sonra açık rızasını geri çektiğinde veri işleme faaliyetinin durduğuna, artık verilerinin işlenmediğine kanaat getirecektir. Veri sahibinin verilerinin işlenmesine rağmen işlenmediği düşüncesine sevk edilmesine yol açacağı için diğer veri işleme şartlarının varlığı halinde açık rıza alınmasının dürüstlük kuralına aykırı bir hareket olduğu kabul edilmektedir²³⁷.

3.1.2. Açık Rıza Şartı Aranmadan Kişisel Verilerin İşlenebileceği Haller

Özel nitelikli olmayan kişisel verilerin açık rıza şartı aranmadan işlenebileceği haller m.5/2'de yedi bent halinde sayılmıştır.

- a. *“Kanunlarda açıkça öngörülmesi”* durumunda kişisel veriler açık rıza şartı aranmadan işlenebilir. Bu hüküm Anayasa'nın kişisel verilerin kanunlarda öngörülen hallerde işlenebileceğine dair hükmüne paralel olarak kanuna alınmıştır. Ancak bazı yazarlar tarafından kendisi de bir kanun olan 6698 Sayılı Kanun'da böyle bir ifadeye yer verilmesi eleştirilmiş, bu kanunun öngördüğü hallerin sayılmasının yeterli olduğu ifade edilmiştir²³⁸.
- b. *“Füili 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”* durumunda açık rıza şartı aranmadan kişisel verileri işlenebilir. Burada dikkat edilmesi gereken husus verilerin yalnızca insanın hayatını veya beden bütünlüğünü korumak maksadıyla işlenebileceğidir. Bu hükmün altında yatan düşünce insan hayatının ve beden bütünlüğünün korunması hakkının kişisel verilerin korunması hakkından daha üstün

²³⁷ **Kişisel Verileri Koruma Kurumu**, Kişisel Verilerin İşlenme Şartları, s.2-3, tam metin için bkz. (<https://www.kvkk.gov.tr/Icerik/4190/Kisisel-Verilerin-Islenme-Sartlari>) s.e.t. 17.01.2023.

²³⁸ **Koca / Üzülmaz** (2020), s.563.

nitelikli bir hak olduğudur. Gerçekten de kişilerin hayatı ve beden bütünlüğü söz konusu olduğunda kişisel veri işleme yasağı sebebiyle gerekli işlemlerin yapılamaması kabul edilebilir bir şey değildir. Madde gerekçesinde rızasını açıklayamayacak durumda olan kişiye yaralı ve bilinci kapalı kişiler, rızasına geçerlilik tanınmayan kişiye ise akıl hastası kişiler örnek verilmiştir.

- c. *“Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması”* durumunda bu veriler açık rıza şartı aranmaksızın işlenebilir. Sözleşmeden doğan ilişki vesilesiyle elde edilmiş veriler yalnızca sözleşmeden doğan yükümlülüklerin ifası ile doğrudan alakalı olan durumlar kapsamında işlenebilir. Bu verilerin farklı amaçlar için ya da gerek olmayan durumlarda işlenmesi hâlinde veri işleme hukuka aykırı olacaktır.
- d. *“Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması”* durumunda kişisel veriler açık rıza şartı aranmaksızın işlenebilir. Madde gerekçesinde bu şarta ilişkin şu örnekler zikredilmiştir. *“Bir şirketin çalışanına maaş ödeyebilmesi için, banka hesap numarası, evli olup olmadığı bakmakla yükümlü olduğu kişiler, eşinin çalışıp çalışmadığı, sosyal sigorta numarası gibi verileri işlemesi bu bendin verdiği yetkiye istinaden olacaktır.”*
- e. *“İlgili kişinin kendisi tarafından alenileştirilmiş olması”* durumunda da kişisel veriler açık rıza aranmaksızın işlenebilir. Kanun gerekçesinde bu bende gerekçe olarak ilgili kişinin kendisi tarafından alenileştirilmiş verilerin korunmasında hukuki yarar bulunmadığı ifade edilmiştir. Fakat bazı durumlarda veriler kişinin kendisi tarafından alenileştirilmiş olsa bile bu verilerin hukuka aykırı amaçlarla kullanılması suretiyle kişi zarara uğratılabilmektedir. Dolayısıyla kişinin kendisi tarafından alenileştirilmiş verilerin korunmasında da zaman zaman hukuki yarar bulunabileceği, bu verilerin işlenmesinin hukuka uygun olması genel kural olmakla birlikte kimi durumlarda aleni verileri işlemenin hukuka aykırılık teşkil edebileceği kabul edilmelidir. Kişisel Verileri Koruma Kurumu da alenileştirilmiş verilerin kişinin alenileştirme iradesi ve alenileştirme amacıyla yakın ilişki içerisinde olduğunu kabul etmektedir. Kurum tarafından yayınlanan kamuoyu duyurusunda bu konu detaylı şekilde ele alınmıştır²³⁹. Alenileştirilmiş bir veriden söz edebilmek için öncelikle

²³⁹ **Kişisel Verileri Koruma Kurumu**, Alenileştirme Hakkında Kamuoyu Duyurusu, (<https://www.kvkk.gov.tr/Icerik/6843/-ALENILESTIRME-HAKKINDA-KAMUOYU-DUYURUSU>) s.e.t. 17.01.2023

ilgili kişide alenileştirme iradesinin bulunması gerekir. Kişinin iradesi dışında kamuya açıklanmış ya da herkes tarafından görünür hale gelmiş bir veri alenileştirilmiş veri olarak kabul edilemez. Dolayısıyla ilgilinin alenileştirme iradesinin bulunmadığı durumlarda bu verilerin işlenmesi hukuka aykırıdır.

Kişinin kendi iradesi ile alenileştirilen veriler bakımından ise alenileştirme amacının dikkate alınması gerekmektedir. Bir kişisel verinin alenileştirilme amacının dışında kullanılması halinde bu kullanım hukuka uygun kabul edilemez. Örneğin aracını satmak için bir internet sitesine ilan veren ve iletişim bilgilerini orada paylaşan bir kişinin iletişim bilgileri kullanılmak suretiyle kişiye reklam mesajları gönderilmesi alenileştirilmiş verilerin amaç dışı kullanımını teşkil eder. Çünkü kişi araç ile ilgili bilgi alınabilmesi ve talipler ile iletişim kurulabilmesi için bu bilgilerini alenileştirmiştir²⁴⁰.

Kişinin herkese açık sosyal medya profilinde paylaştığı bilgiler alenileştirilmiş veriler olarak kabul edilebilir. Ancak bu bilgiler ve fotoğraflar kullanılarak sahte hesap oluşturulması, buradan kişinin onurunu zedeleyici hukuka ve ahlaka aykırı yayınlar yapılması durumunda kişisel verilerin hukuka uygun olarak işlendiği söylenemez. Yine bir gazetecinin köşe yazılarıyla birlikte basılan fotoğrafının alınarak bir evlilik sitesinde kullanılması durumunda hukuka uygun veri işlemeden söz edilemez²⁴¹. Çünkü bu durumlarda amaç dışı kullanım söz konusudur.

Kişinin kamusal alandaki davranışları izlenerek hangi derneklere gittiğinin, hangi toplantı ve gösteri yürüyüşlerine katıldığının kaydedilmesi de hukuka uygun olmayacaktır. Burada kişinin bu bilgileri alenileştirme iradesinin olup olmadığı şüphelidir. Çünkü kişinin bu hareketlerinin kamuya açık alanda gerçekleşmesi bir mecburiyettir. Kişinin kendi iradesiyle ve belli amaçlarla kullanılması için bu bilgileri alenileştirdiğinden söz etmek mümkün olmayacaktır.

Alenileştirilmiş veriler üzerinde gerçekleştirilen veri işleme faaliyetlerinin hukuka uygun olabilmeleri için dürüstlük kuralına da uygun olmaları gerekir. Veri işleme faaliyeti sırasında verisi işlenen gerçek kişinin makul beklentilerine uygun hareket edilmelidir²⁴².

²⁴⁰ Benzer bir olay hakkında verilen kurul kararı için bkz. K.S. 2019/331, K.T. 07/11/2019, Karar Özeti (<https://kvkk.gov.tr/Icerik/6623/2019-331>) s.e.t. 17.01.2023

²⁴¹ Yargıtay da önüne gelen bir olayda kişinin aleni verisinin amaç dışı kullanılmasını suç olarak kabul etmiştir. Yargıtay 12. Ceza Dairesi, 2011/20072 E., 2012/12126 K., 15.05.2012 K.T.

²⁴² **Dölger** (2020), s.406

- f. *“Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması”* durumunda kişisel veriler açık rıza şartı aranmaksızın işlenebilir. Bu şart genellikle mahkemelerde savunma hakkı kullanırken gerçekleşmektedir. Madde gerekçesinde de savunma hakkı bağlamında bir örnek verilmiştir. Bir işçinin işverenine karşı açtığı davada işveren tarafından işçiye ait bazı bilgilerin savunma maksadıyla kullanılmasında durum böyledir. Savunma hakkı kullanıldığı için veri işleme hukuka uygun hale gelecektir. Ancak madde metninden de anlaşılacağı üzere somut olayda veri işlemenin zorunlu olması gerekir. Başka bir şekilde ispatlanması mümkün durumların verilerin ele geçirilmesi suretiyle ispatlanmaya çalışılması hukuka uygun kabul edilemez. Madde gerekçesinde zikredilen bir diğer örneğe göre *“kısıtlı bir kişinin haklarının korunması amacıyla vasiinin veya kayyımın, kısıtlının mali bilgilerini tutması”* durumunda bu şart gerçekleşmiş olacak ve veri işleme hukuka uygun kabul edilecektir.
- g. *“İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması”* durumunda kişisel veriler açık rıza şartı aranmaksızın işlenebilir. Burada veri sorumlusunun meşru menfaati ile ilgili kişinin kişisel verilerinin korunması menfaati arasında bir yarış vardır. Kanun bu yarışan iki menfaatten veri sorumlusunun menfaatini ilgili kişinin menfaatine üstün tutmuştur²⁴³. Fakat bu üstünlük her durumda kabul edilmemiş, bazı şartlara bağlanmıştır. Buna göre veri işleme faaliyeti sırasında ilgili kişinin temel hak ve özgürlüklerine zarar verilmemeli, veri işleme zorunlu olmalı ve veri sorumlusunun menfaati meşru bir menfaat olmalıdır. Madde gerekçesinde örnek olarak *“bir şirket sahibinin, çalışanlarının temel hak ve özgürlüklerine zarar vermemek kaydıyla, onların terfileri, maaş zamları yahut sosyal haklarının düzenlenmesinde ya da işletmenin yeniden yapılandırılması sürecinde görev ve rol dağıtımında esas alınmak üzere çalışanların kişisel verilerini işleyebileceği”* zikredilmiştir.

²⁴³ Yüzbaşı Tobaz, s.351.

3.2. Özel Nitelikli Kişisel Verilerin İşlenme Şartları

KVKK'nın 6ncı maddesinin birinci fıkrasında “*Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri*” özel nitelikli kişisel veriler olarak sayılmıştır. Kanun burada özel nitelikli veri kategorilerini teker teker saymıştır. Dolayısıyla bu kategoriler sınırlı sayıdadır ve yorum yoluyla çoğaltılmaları mümkün değildir.

Uygulamada bazen verilerin özel nitelikli veri kategorisine girip girmedikleri konusunda tereddüt oluşabilmektedir. Örneğin bir kişinin yüzünü net bir biçimde gösteren görüntüsü biyometrik veri olarak kabul edilmektedir. Güvenlik kamerası görüntülerinde kişilerin yüzleri genellikle görünmektedir. Yine kamera görüntülerinden kişinin gözlük, koltuk değneği, tekerlekli sandalye gibi araçlar kullandığı da görülebilmekte, haliyle bu görüntüler kişinin sağlık durumuna ilişkin bir bilgi de içermektedir. O halde güvenlik kamerası görüntüleri özel nitelikli veri kategorisinde mi yoksa sıradan veriler kategorisinde mi değerlendirilecek sorusu gündeme gelmektedir. Bunun sonucu olarak bu tür durumlarda sıradan kişisel verilere ilişkin hükümlerin mi yoksa özel nitelikli kişisel verilere ilişkin hükümlerin mi uygulanacağı tartışma konusu olmaktadır. Bu konuya ilişkin AB hukukundaki yaklaşımın Türk Hukuku'nda da genel kabul gördüğü söylenebilir. Buna göre somut olayda eğer söz konusu veri onu özel nitelikli kılan unsuru bakımından işleniyorsa özel nitelikli verilere ilişkin hükümler uygulanmalıdır²⁴⁴. Veriyi özel nitelikli kılan sebebe ilişkin bir işlem gerçekleştirilmiyorsa sıradan verilere ilişkin hükümler uygulanmalıdır. Somutlaştıracak olursak; güvenlik kamerası görüntüleri sadece güvenlik amacıyla kaydedilmekte ise görüntülerdeki kişilerin gözlük kullanması gibi hususlar tek başına bu verileri kişilerin sağlığına ilişkin veriler kılmaya yetmez. Yine bu görüntüler bir yüz tanıma sistemi tarafından işleme tabi tutulup biyometrik görüntüler/kayıtlar elde edilmiyorsa bu durumda özel nitelikli verilere ilişkin hükümleri uygulamaya gerek yoktur.

Özel nitelikli verilerin işlenmesine ilişkin şartlar 6ncı maddenin 2, 3 ve 4üncü fıkralarında düzenlenmiştir. İkinci fıkrada yer alan hükme göre “*özel nitelikli kişisel verilerin ilgilinin açık rızası olmaksızın işlenmesi yasaktır.*” Bu fıkradan anlaşılabacağı üzere

²⁴⁴ Küzeci, s.407.

kural özel nitelikli kişisel verilerin açık rıza ile işlenmesidir. Üçüncü fıkra da ise açık rıza olmadan özel nitelikli kişisel verilerin işlenmesine ilişkin yasağa bazı istisnalar getirilmiştir. Başka bir deyişle açık rızanın bulunmadığı durumlarda da özel nitelikli kişisel verilerin işlenebileceği bazı durumlar belirlenmiştir.

İstisnaları düzenleyen bu üçüncü fıkra da kanun ikili bir ayırım yapmaktadır. Sağlık ve cinsel hayata ilişkin veriler için farklı şartlar öngörülmüş, diğer özel nitelikli veriler için farklı şartlar öngörülmüştür. Üçüncü fıkraya göre “sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir.”

Tablo 1. Özel nitelikli kişisel verilerin işlenme şartları²⁴⁵

Özel Nitelikli Kişisel Veri Türü	İşlenme Şartları
<i>“Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri”</i>	Kural: İlgilinin açık rızasının bulunması halinde veriler işlenebilir. İstisna: Veri İşlemenin kanunlarda öngörülmüş olması halinde veriler açık rıza aranmaksızın işlenebilir.
Sağlık ve cinsel yaşama ilişkin kişisel veriler	Kural: İlgilinin açık rızasının bulunması halinde veriler işlenebilir. İstisna: Verilerin 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 durumunda veriler açık rıza aranmaksızın işlenebilir.

²⁴⁵ Tablo hazırlanırken faydalanılan kaynak için bkz. **Küzeci**, s.405.

Özel nitelikli kişisel verilerin işlenmesine ilişkin bir diğer şart dördüncü fıkrada düzenlenmiştir. Buna göre özel nitelikli kişisel verilerin işlenmesinin hukuka uygun hale gelebilmesi için kurul tarafından belirlenen önlemlerin alınması şarttır. Yukarıda değindiğimiz açık rıza ile işleme, kanunda öngörülme gibi veri işlemeyi hukuka uygun hale getiren durumlardan her birinde ayrıca kurul tarafından belirlenen önlemlerin de alınması gerekmektedir.

Kurul kanunun m.6/4 ve m.22/1-ç hükümleri ile kendisine verilen yetki ve görev doğrultusunda bir karar yayınlamış ve özel nitelikli kişisel veriler işlenirken alınması gereken önlemleri belirlemiştir. Karara göre veri sorumluları özel nitelikli kişisel verilerin güvenliğine yönelik ayrı bir politika ve prosedür belirlemelidir. Bu prosedür sistemli, kuralları net bir biçimde belli, yönetilebilir ve sürdürülebilir olmalıdır. Özel nitelikli kişisel verilerin işlenme süreçlerinde yer alan çalışanlara eğitimler verilmelidir. Kararda elektronik ortamda işlenen veriler için ayrı, fiziki ortamda işlenen veriler için ayrı tedbirler öngörülmüştür²⁴⁶.

²⁴⁶ Kararda öngörülen önlemler özel nitelikli kişisel verilerin işlenmesi faaliyetlerinin hukuka uygun gerçekleşip gerçekleşmediğinin belirlenmesi bakımından önem arz ettiği için kararın tamamına burada yer vermek gerekmektedir. Kurul kararına göre alınması gereken önlemler aşağıda sıralanmıştır;

- “1- Özel nitelikli kişisel verilerin güvenliğine yönelik sistemli, kuralları net bir şekilde belli, yönetilebilir ve sürdürülebilir ayrı bir politika ve prosedürün belirlenmesi,*
- 2- Özel nitelikli kişisel verilerin işlenmesi süreçlerinde yer alan çalışanlara yönelik,*
 - a) Kanun ve buna bağlı yönetmelikler ile özel nitelikli kişisel veri güvenliği konularında düzenli olarak eğitimler verilmesi,*
 - b) Gizlilik sözleşmelerinin yapılması,*
 - c) Verilere erişim yetkisine sahip kullanıcıların, yetki kapsamlarının ve sürelerinin net olarak tanımlanması,*
 - ç) Periyodik olarak yetki kontrollerinin gerçekleştirilmesi,*
 - d) Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkilerinin derhal kaldırılması. Bu kapsamda, veri sorumlusu tarafından kendisine tahsis edilen envanterin iade alınması,*
- 3- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, elektronik ortam ise*
 - a) Verilerin kriptografik yöntemler kullanılarak muhafaza edilmesi,*
 - b) Kriptografik anahtarların güvenli ve farklı ortamlarda tutulması,*
 - c) Veriler üzerinde gerçekleştirilen tüm hareketlerin işlem kayıtlarının güvenli olarak loglanması,*
 - ç) Verilerin bulunduğu ortamlara ait güvenlik güncellemelerinin sürekli takip edilmesi, gerekli güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,*
 - d) Verilere bir yazılım aracılığı ile erişiliyorsa bu yazılıma ait kullanıcı yetkilendirmelerinin yapılması, bu yazılımların güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,*
 - e) Verilere uzaktan erişim gerekiyorsa en az iki kademeli kimlik doğrulama sisteminin sağlanması,*
- 4- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, fiziksel ortam ise*
 - a) Özel nitelikli kişisel verilerin bulunduğu ortamın niteliğine göre yeterli güvenlik önlemlerinin (elektrik kaçağı, yangın, su baskını, hırsızlık vb. durumlara karşı) alındığından emin olunması,*
 - b) Bu ortamların fiziksel güvenliğinin sağlanarak yetkisiz giriş çıkışların engellenmesi,*
- 5- Özel nitelikli kişisel veriler aktarılacaksa*
 - a) Verilerin e-posta yoluyla aktarılması gerekiyorsa şifreli olarak kurumsal e-posta adresiyle veya Kayıtlı Elektronik Posta (KEP) hesabı kullanılarak aktarılması,*

4. VERİ SORUMLUSUNUN YÜKÜMLÜLÜKLERİ

6698 sayılı kanun veri sorumlusunun kim olduğunu tanımlamış²⁴⁷ ve veri sorumlusuna pek çok yükümlülük yüklemiştir. Bu yükümlülükler kanunun muhtelif maddelerinde dağınık şekilde yer almaktadır. İlgili kişi veya kişileri aydınlatmak (m.10), gerektiğinde verileri silmek, yok etmek veya anonim hâle getirmek (m.7), ilgili kişilerin haklarını kullanmak üzere yaptığı başvuruları yanıtlamak (m.11, m.13), gerekli tedbirleri alarak veri güvenliğinin sağlamak (m.12), kurulun inceleme için istediği bilgi ve belgeleri göndermek (m.15) ve şartları sağlıyorsa veri sorumluları siciline kaydolmak (m.16) veri sorumlusunun başlıca yükümlülükleridir.

Kanunun 17 ve 18inci maddelerini ihtiva eden beşinci bölümünde suçlar ve kabahatler düzenlenmiştir. Buna göre veri sorumlusunun verileri silme, yok etme veya anonim hale getirme yükümlülüğünü düzenleyen 7nci madde hükmüne aykırı hareket etmesi suç olarak tanımlanmıştır²⁴⁸. Veri sorumlusunun kanunun 10, 12, 15 ve 16ncı maddelerine aykırı hareketleri ise kabahat olarak tanımlanmış ve bu kabahatler için değişen miktarlarda idari para cezaları öngörülmüştür. KVKK'nın suçlara ve kabahatlere ilişkin maddeleri ileride ayrı başlıklarda ele alınacaktır.

Veri sorumlusunun aydınlatma yükümlülüğü 10uncu maddede düzenlenmiştir ve en sık uygulanan yükümlülüktür. Çünkü veri sorumlusu her veri toplama işleminden önce veri sahibini aydınlatmak ile yükümlüdür. Veri sahipleri ve veri sorumluları arasında doğan her kişisel veri işleme ilişkisinin başında yerine getirilmesi gereken bir yükümlülük olması ve veri sahibinin haklarını kullanabilmesi gerekli olması gibi hususlar aydınlatma yükümlülüğünü önemli kılmaktadır. Kanuna göre veri sahibinin ilgili kişiyi “veri

b) Taşınabilir Bellek, CD, DVD gibi ortamlar yoluyla aktarılması gerekiyorsa kriptografik yöntemlerle şifrelenmesi ve kriptografik anahtarın farklı ortamda tutulması,

c) Farklı fiziksel ortamlardaki sunucular arasında aktarma gerçekleştiriliyorsa, sunucular arasında VPN kurularak veya sFTP yöntemiyle veri aktarımının gerçekleştirilmesi,

ç) Verilerin kağıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemlerin alınması ve evrakın “gizlilik dereceli belgeler” formatında gönderilmesi gerekir.

6- Yukarıda belirtilen önlemlerin yanı sıra Kişisel Verileri Koruma Kurumunun internet sitesinde yayımlanan Kişisel Veri Güvenliği Rehberinde belirtilen uygun güvenlik düzeyini temin etmeye yönelik teknik ve idari tedbirler de dikkate alınmalıdır.”

²⁴⁷ KVKK m. 3/1-1: “Veri sorumlusu kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi ifade eder.”

²⁴⁸ KVKK m. 17/2 & TCK m. 138.

sorumlusunun ve varsa temsilcisinin kimliği, işlenen kişisel verilerin kimlere ve hangi amaçlarla aktarılabileceği, kişisel veri toplamanın yöntemi ve hukuki sebebi, ilgili kişinin 11inci maddede sayılan hakları” konularında bilgilendirmesi aydınlatma yükümlülüğünün kapsamına girmektedir. Bilgilendirme açık, sade, net ve anlaşılır bir şekilde yapılmalıdır. Gereksiz şekilde uzun olmamalıdır. İlgiliyi yeterince aydınlatmayacak kadar kısa da olmamalıdır. Somut olayın gerekliliğine uygun bir uzunlukta ve yine somut olayın gerekliliklerine uygun bir içerik ile sade ve öz bir biçimde kişiye aktarılmalıdır. Bilgilendirme herhangi bir şekil şartına tabi değildir. Fakat bilgilendirmenin yapıldığını ve içeriğinin mevzuata uygun olduğunu ispat etme yükümlülüğü veri sorumlusuna aittir. İspatın sağlanabilmesi bakımından veri sorumlusunun bilgilendirmeyi yazılı bir şekilde yapması, eğer başka yollarla yapıyorsa bunu kayıt altına alması lehine olacaktır.

Aydınlatma yükümlülüğü şekil şartına tabi olmadığı için elektronik ortamda da yerine getirilebilir²⁴⁹. Aydınlatma yükümlülüğünün detayları ve bu yükümlülük yerine getirilirken uyulacak usul ve esaslar Kurum tarafından yayınlanan bir tebliğ ile açıklanmıştır²⁵⁰.

Veri sorumlusunun en temel yükümlülüğü gerekli önlemleri alarak veri güvenliğini sağlamaktır. Kanunun 12nci maddesine göre “*veri sorumlusu kişisel verilerin hukuka aykırı olarak işlenmesini önlemekle, kişisel verilere hukuka aykırı bir şekilde erişilmesini önlemekle ve kişisel verilerin muhafazasını sağlamakla*” yükümlüdür²⁵¹. Veri sorumlusunun bu yükümlülükleri yerine getirmiş sayılması için bu amaçlara uygun güvenlik düzeyini sağlaması gerekir. Bu güvenlik düzeyinin sağlanması için her türlü teknik ve idari tedbirin alınması veri sorumlusunun yükümlülüğüdür. Veri sorumlusu işlediği kişisel verilere hukuka aykırı bir erişimin gerçekleşmesi durumunda bu durumu en kısa sürede veri sahibine ve Kişisel Verileri Koruma Kurulu’na bildirir. Kurul gerek görmesi halinde bu durumu internet sitesinde veya başka yollarla ilan edebilir²⁵².

Veri sorumlusunun bir diğer yükümlülüğü verileri silmek, yok etmek veya anonim hale getirmektedir. Bu yükümlülük kanunun 7nci maddesinde düzenlenmiştir. Buna göre

²⁴⁹ Detaylar için bkz. **Yüzbaşı Tobaz**, s.358-361.

²⁵⁰ **Kişisel Verileri Koruma Kurumu**, Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ, Resmi Gazete, Sayı: 30356, Tarih: 10.03.2018, (<https://www.resmigazete.gov.tr/eskiler/2018/03/20180310-5.htm>) s.e.t. 17.01.2023.

²⁵¹ KVKK m.12/1.

²⁵² KVKK m.12/5.

bu kanunun veya ilgili diğer kanunların hükümlerine uygun olarak gerçekleştirilen veri işleme faaliyetlerinde, verilerin işlenmesini gerektiren hukuki sebep ortadan kalktığı takdirde veri sorumluları kişisel verileri silmekle, yok etmekle veya anonim hale getirmekle yükümlüdür. Bu yükümlülüğe aykırı hareketler TCK'nın “*Verileri Yok Etmeme*” başlıklı 138inci maddesi kapsamında suç teşkil etmektedir. Bu suç için 1 yıldan 2 yıla kadar hapis cezası öngörülmüştür. Veri sorumlularının bu yükümlülüğe aykırı hareket etmelerinin suç olduğu KVKK'nın 17/2 hükmü ile de teyit edilmiştir.

6698 Sayılı Kanun'un 7nci maddesinin 3üncü fıkrasında “*kışisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin usul ve esaslar yönetmelikle düzenlenir*” hükmü yer almaktadır. Veri sorumlusunun yükümlülüğüne ilişkin detayların belirlenmesi bakımından ve verileri yok etmeme suçunun unsurlarının hangi durumlarda gerçekleşeceğinin tespiti bakımından bu yönetmelik oldukça önemlidir²⁵³. Üçüncü bölümde kişisel verilerin korunması hakkını ihlal eden suçlar incelenirken bu konu detaylı şekilde ele alınacağı için şimdilik bu kadar bilgi vermeyi yeterli görüyoruz.

5. İLGİLİ KİŞİNİN HAKLARI

6698 Sayılı Kanun veri sorumlusuna belirli yükümlölükler yüklerken ilgili kişiye de belirli haklar tanımıştır. İlgili kişinin hakları kanunun 11inci maddesinde düzenlenmiştir. Buna göre ilgili kişi;

- Verilerinin işlenip işlenmediğini öğrenme,
- Verileri işlenmiş ise hangi verilerinin ne kadar işlendiği gibi detaylar hakkında bilgi alma,
- Kışisel verilerinin işlenme amaçlarını öğrenme ve verilerinin bu amaçlar dışında işlenip işlenmediğini öğrenme,
- Kışisel verilerinin yurt içinde veya yurt dışında kimlere hangi maksatlarla aktarıldığını öğrenme,

²⁵³ Bu yönetmelik 28.10.2017 tarihli ve 30224 sayılı Resmî Gazetede yayımlanarak yürürlüğe girmiştir. Tam metin için bkz. (<https://mevzuat.gov.tr/mevzuat?MevzuatNo=24038&MevzuatTur=7&MevzuatTertip=5>) s.e.t. 17.01.2023

- Kişisel verilerinin yanlış veya eksik işlenmiş olması durumunda yanlışların düzeltilmesini veya eksiklerin giderilmesini talep etme,
- Kanunun yedinci maddesindeki şartların gerçekleşmiş olması durumunda kişisel verilerinin silinmesini veya yok edilmesini isteme,
- Kişisel verilerin düzeltilmesi veya silinmesi taleplerinin verilerin aktarıldığı üçüncü kişilere de iletilmesini isteme,
- Otomatik işlemlerin yol açtığı aleyhine sonuçlara itiraz etme,
- Verilerinin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması halinde uğradığı zararların giderilmesini isteme

haklarına sahiptir. Tüm bu haklar göz önünde bulundurulduğunda kanunun “*verilerin geleceğini belirleme hakkı*” yaklaşımını esas alarak, ilgili kişiye verileri üzerinde tam bir hakimiyet sağlamayı amaçladığı anlaşılmaktadır.

KVKK 11inci maddede sayılan bu hakların yanı sıra ilgili kişiye genel bir güvence de sağlamaktadır. Bu güvence kişisel verilerin korunmasını isteme hakkının etkin şekilde korunması için öngörülen usul ve esasların belirlenmesi suretiyle hukuki belirliliğin sağlanmış olmasıdır. İlgili kişi bu kanun ve kanun doğrultusunda çıkarılan yönetmelikler nezdinde hukuka aykırılık teşkil eden her durumda kişisel verilerine yapılan hukuka aykırı müdahaleye karşı başvuru yollarına sahip olmuştur. İlgili kişi veri sorumlusuna başvurarak hukuka aykırılığın giderilmesini isteyebilir²⁵⁴. Veri sorumlusundan tatmin edici bir cevap alamadığı veya bu cevabı yetersiz bulduğu durumlarda Kişisel Verileri Koruma Kurumu’na başvurabilir²⁵⁵. İlgili kişinin başvurusu üzerine yapılacak inceleme sonucunda 18inci maddede yer alan kabahatlerden birini işlediği tespit edildiğinde veri sorumlusu idari para cezasına çarptırılabilir. Kişilik hakları zedelenen ilgili kişi Borçlar Kanunu’nun maddi ve manevi tazminatı konu alan genel hükümlerinin uygulanması suretiyle uğradığı zararların giderilmesini hukuk mahkemelerinden talep edebilir²⁵⁶. Hukuka aykırı olarak verilerini kaydeden, aktaran, yayan, ele geçiren ve yok etmeyenler hakkında suç duyurusunda bulunabilir²⁵⁷.

²⁵⁴ KVKK m.13.

²⁵⁵ KVKK m.14.

²⁵⁶ KVKK m.14/3.

²⁵⁷ KVKK m.17.

6. KVKK’NIN KABAHATLERE ve SUÇLARA İLİŞKİN HÜKÜMLERİ

Kişisel verilerin KVKK’da yer alan düzenlemelere aykırı olarak işlenmesi durumunda ihlalin niteliğine göre veri sorumlularına ve veri işleyenlere idari veya cezai yaptırım uygulanması mümkündür. İdari ve cezai yaptırımlara ilişkin hükümler KVKK’nın beşinci bölümünü teşkil eden 17nci ve 18inci maddelerinde düzenlenmiştir. Suçlar başlığını taşıyan 17nci maddede suçlara ilişkin hükümler, kabahatler başlığını taşıyan 18inci maddede ise kabahatlere ilişkin hükümler yer almaktadır.

KVKK’nın 17nci maddesinde kişisel verilere ilişkin suçlar bakımından TCK’nın 135 ila 140ncı maddelerinde yer alan hükümlerin uygulanacağı ifade edilmiş, yeni bir suç tanımı yapılmamıştır²⁵⁸. Buna karşılık 18inci maddede KVKK hükümlerine aykırılık teşkil eden bazı fiiller kabahat olarak tanımlanmış ve bunlara uygulanacak yaptırımlar belirlenmiştir.

Kişisel verilerin korunması hakkını ihlal eden bazı fiillerin suç olarak bazı fiillerin ise kabahat olarak tanımlanması bu fiillerin korunan hukuki değeri ihlal dereceleri ile ilgilidir. Kanun koyucu kişisel verilerin korunması hakkını daha ağır şekilde ihlal ettiğine kanaat getirdiği fiilleri suç olarak tanımlamış ve bunlara cezai yaptırımlar öngörmüş, kişisel verilerin korunması hakkını daha hafif şekilde ihlal ettiğine kanaat getirdiği fiilleri ise kabahat olarak tanımlamış ve bunlara idari yaptırım uygulanmasını yeterli görmüştür²⁵⁹.

6.1. KVKK’da Kabahat Olarak Tanımlanan Fiiller ve Bunlara İlişkin Hükümler

6698 Sayılı KVKK’nın 18inci maddesi üç fıkradan oluşmaktadır. Maddenin 1inci fıkrasının a, b, c ve ç bentlerinde her bentte bir kabahat olmak üzere dört farklı kabahat

²⁵⁸ Öğretide bir görüşe göre KVKK m.17/2 hükmü ile yeni bir suç tanımı yapılmıştır. Ancak bizim de katıldığımız diğer görüşe göre bu fıkra ile yeni bir suç tanımı yapılmamış, KVKK m.7 hükmüne aykırı olarak verilerin silinmemesi ve anonim hale getirilmemesi hallerinde de TCK m.138 hükmünün uygulanacağı teyit edilmek istenmiştir. Bu konu aşağıda 6.2.1. numaralı başlıkta detaylı olarak ele alınmıştır.

²⁵⁹ Kangal, s.177.

tanımlanmıştır. Bunlar aydınlatma yükümlülüğünün yerine getirilmemesi (m. 18/1-a), veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi (m. 18/1-b), kurul tarafından verilen kararların yerine getirilmemesi (m. 18/1-c) ve veri sorumluları siciline kayıt veya bildirim yükümlülüğüne aykırı hareket edilmesidir (m. 18/1-ç). Bu kabahatlere değişen miktarlarda idari para cezaları öngörülmüştür²⁶⁰.

Bu kanunda öngörülen idari para cezaları veri sorumlusu olan gerçek kişilere ve özel hukuk tüzel kişilerine uygulanabilir (KVKK m.18/2). Bu fiillerin kamu kurumları ve kamu kurumu niteliğindeki meslek kuruluşları bünyesinde işlenmesi halinde idari para cezası uygulanamaz. Bu fiillerin *“kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları bünyesinde işlenmesi hâlinde, Kurulun yapacağı bildirim üzerine, ilgili kamu kurum ve kuruluşunda görev yapan memurlar ve diğer kamu görevlileri ile kamu kurumu niteliğindeki meslek kuruluşlarında görev yapanlar hakkında disiplin hükümlerine göre işlem yapılması ve sonucunun Kurula bildirilmesi”* öngörülmüştür (m.18/3).

KVKK m.18’de yer alan hükümlerin yanı sıra Kabahatler Kanunu’nda (KK) yer alan genel hükümler bu kabahatler için de uygulanacaktır. Genel hükümlerden yola çıkarak bu kabahatlerin kasten işlenebilecekleri gibi taksirle de işlenebilecekleri söylenebilir (KK m.9). Aksi bir hüküm bulunmadığı için bu kabahatlere teşebbüs cezalandırılmayacaktır (KK m.13).

Kabahatler Kanunu’nun 14üncü maddesinde iştirake ilişkin hükümler düzenlenmiştir. Buna göre *“kabahatin işlenişine birden fazla kişinin iştirak etmesi halinde bu kişilerden her biri hakkında fail olarak idari para cezası verilir”* (KK m.14/1). *“Özel faillik niteliğinin arandığı durumlarda, kabahate iştirak eden ve bu niteliği taşımayan kişi hakkında da fail olarak idarî para cezası verilir”* (KK m.14/2). Kabahate iştirakin söz konusu olabilmesi için hem iştirak edilen fiilin hem de iştirakin kasten gerçekleştirilmesi gerekir²⁶¹. Bu hükümlerden yola çıkarak KVKK m.18/1’de düzenlenen kabahatlere

²⁶⁰ Bu miktarlar Kabahatler Kanunu m.17/7 hükmü gereğince her takvim yılı başında yeniden değerlendirilerek oranında artırılmaktadır.

²⁶¹ **Karınçu, Sümeýra** (2019) Kişisel Verilerin Korunması Kanunu Kapsamında Aydınlatma Yükümlülüğünün Yerine Getirilmemesi Kabahati (Yüksek Lisans), İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, s.94.

iştirakin mümkün olduğu söylenebilir²⁶². Öğretideki bir görüşe göre ise Kabahatler Kanunu karşısında özel norm niteliği taşıyan KVKK m.18/2 hükmü öncelikle uygulanacağından, Kabahatler Kanunu’nun iştirake ilişkin mezkûr hükümlerinden yola çıkarak veri sorumlusu dışında herhangi bir kişiye idari para cezası verilmesi mümkün değildir²⁶³.

Kabahatler dolayısıyla uygulanan idari para cezalarına karşı başvuru yolu Kabahatler Kanunu’nun 17nci maddesinde düzenlenmiştir. Buna göre bu kabahatlere ilişkin verilecek idari para cezalarına karşı kararın tebliği veya tefhiminden itibaren on beş gün içinde sulh ceza mahkemesine başvurulabilir (KK m.27/1).

KVKK m.28’in birinci fıkrasında belirtilen istisna hallerinde KVKK hükümleri uygulanmayacağı için bu istisnalar kapsamındaki veri işleme faaliyetleri neticesinde söz konusu kabahatlerin oluşması mümkün değildir. 28nci maddenin ikinci fıkrasında belirtilen kısmi istisna hallerinde ise aydınlatma yükümlülüğünü yerine getirmeme ve veri sorumluları siciline kayıt veya bildirim yükümlülüğüne aykırı davranma kabahatleri oluşmayacak, diğer kabahatlere ilişkin hükümlerin uygulanmasına devam edilecektir.

6.1.1. Aydınlatma Yükümlülüğünün Yerine Getirilmemesi

Veri sorumlusunun ilgili kişiyi aydınlatma yükümlülüğü kanunun 10uncu maddesinde düzenlenmiştir. Aydınlatma yükümlülüğünün yerine getirilmesi sırasında uyulacak usul ve esaslar ise bu konuda Kişisel Verileri Koruma Kurumu tarafından yayınlanan bir tebliğ ile belirlenmiştir²⁶⁴. Buna göre veri sorumlusu veya veri sorumlusunun yetkilendirdiği kişi ilgili kişilere “*veri sorumlusunun ve varsa temsilcisinin kimliği, kişisel verilerin hangi amaçla işleneceği, işlenen kişisel verilerin kimlere ve hangi amaçlarla aktarılabilirliği, kişisel veri toplamanın yöntemi ve hukuki sebebi, ilgili kişinin 11nci maddede sayılan hakları*” konularında bilgi vermekle yükümlüdür. Aydınlatma yükümlülüğünün 10uncu maddede ve ilgili tebliğde bahsi geçen tüm bu hususları

²⁶² Karınçu, s.94.

²⁶³ Kangal, s.183-184.

²⁶⁴ Bahsi geçen “Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ” 10 Mart 2018 tarihinde Resmî Gazete’de yayımlanmıştır. Tam metin için bkz. (<https://www.resmigazete.gov.tr/eskiler/2018/03/20180310-5.htm>) s.e.t. 1.03.2023.

kapsayacak şekilde yerine getirilmesi gerekir²⁶⁵. Aydınlatma yükümlülüğünün 10uncu maddede tarif edildiği şekilde yerine getirilmemesi KVKK m.18/1-a hükmü ile kabahat olarak tanımlanmıştır. Aydınlatma yükümlülüğünü yerine getirmeme kabahatini işleyen veri sorumlusuna Kişisel Verileri Koruma Kurulu tarafından 5.000 Türk lirasından 100.000 Türk lirasına kadar idari para cezası verileceği ifade edilmiştir (m. 18/1-a & m. 18/2).

İlgili kişinin verilerin elde edilmesi sırasında aydınlatılması mecburidir. Veriler KVKK m.5 ve m.6'da yer alan veri işleme şartlarından hangisine dayanılarak elde ediliyor olursa olsun aydınlatma yükümlülüğü doğmaktadır²⁶⁶. Aydınlatma yükümlülüğü veriler elde edilmeden önce veya verilerin elde edildiği esnada yerine getirilmelidir. Aydınlatma yükümlülüğü yerine getirilmeden veriler elde edildiği takdirde verilerin elde edildiği an bu kabahat oluşur. Veriler elde edildikten sonra aydınlatma yükümlülüğünün yerine getirilmesi kabahatin oluşmasını engellemez²⁶⁷. Kişisel verilerin ilgili kişinin kendisinden değil de başka bir kişiden elde edilmesi durumunda ise aydınlatma yükümlülüğünün “*verilerin elde edilmesinden itibaren makul bir süre içerisinde*” yerine getirilmesi gerektiği kabul edilmiştir²⁶⁸.

Kişisel verilerin açık rızaya dayalı olarak işlendiği durumlarda aydınlatma yükümlülüğünün yerine getirilmemesi rızayı geçersiz kılacağı için aynı zamanda kişisel verilerin hukuka aykırı olarak kaydedilmesi (TCK m.135) suçunun oluşması da söz konusu olacaktır. Bu durumda bu fiil hem kabahat hem de suç teşkil ettiği için içtima hükümleri gereği yalnızca suçtan dolayı yaptırım uygulanacaktır²⁶⁹.

Kişisel verilerin açık rıza dışında diğer veri işleme şartlarına dayalı olarak işlendiği durumlarda aydınlatma yükümlülüğü yerine getirilmeden verilerin elde edilmesi suç oluşmasına sebebiyet vermez. Çünkü aydınlatma yükümlülüğünün yerine getirilmemesi veri işleme şartının geçerliliğini etkilemeyecek ve dolayısıyla verileri kaydetme fiili hukuka aykırı hale gelmeyecektir. Bu durumda yalnızca kabahat oluşacaktır.

²⁶⁵ Kangal, s.189.

²⁶⁶ Tebliğ m.5/1-a: “İlgili kişinin açık rızasına veya Kanundaki diğer işleme şartlarına bağlı olarak kişisel veri işlendiği her durumda aydınlatma yükümlülüğü yerine getirilmelidir.”

²⁶⁷ Kangal, s.189.

²⁶⁸ Tebliğ m.6/1-a.

²⁶⁹ Kabahatler Kanunu m.15/3: “Bir fiil hem kabahat hem de suç olarak tanımlanmış ise, sadece suçtan dolayı yaptırım uygulanabilir. Ancak, suçtan dolayı yaptırım uygulanamayan hallerde kabahat dolayısıyla yaptırım uygulanır.”

Diğer kabahatlere uygulanan idari para cezaları gibi KVKK'da düzenlenen kabahatlere uygulanan idari para cezaları da her takvim yılının başında yeniden değerlendirilme oranında artırılmaktadır. Yeniden değerlendirme oranında artırılmış haliyle 2023 yılı içerisinde bu kabahati işleyenlere verilecek idari para cezasının alt sınırı 29 bin 852 lira, üst sınırı ise 597 bin 191 liradır²⁷⁰.

6.1.2. Veri Güvenliğine İlişkin Yükümlülüklerin Yerine Getirilmemesi

Veri güvenliğine ilişkin yükümlülükler KVKK'nın 12nci maddesinde düzenlenmiştir. Buna göre;

“(1) Veri sorumlusu;

a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,

b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,

c) Kişisel verilerin muhafazasını sağlamak,

amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.

(2) Veri sorumlusu, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, birinci fıkrada belirtilen tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumludur.

(3) Veri sorumlusu, kendi kurum veya kuruluşunda, bu Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorundadır.

(4) Veri sorumluları ile veri işleyen kişiler, öğrendikleri kişisel verileri bu Kanun hükümlerine aykırı olarak başkasına açıklayamaz ve işleme amacı dışında kullanamazlar. Bu yükümlülük görevden ayrılmalarından sonra da devam eder.

(5) İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul,

²⁷⁰ Kişisel Verileri Koruma Kurumu KVKK kapsamındaki kabahatlere uygulanacak idari para cezalarını her yıl yeniden değerlendirme oranı dikkate alınarak artırılmış şekilde internet sitesinde yayınlamaktadır. Güncel miktarlar kurumun resmi internet sitesinden alınmıştır. Detaylar için bkz. (<https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/fcbcf082-1c32-4e53-af98-b90ac7aa298e.pdf>) s.e.t. 1.03.2023

gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.”

12nci madde yer alan bu yükümlölüklerin yerine getirilmemesi KVKK m.18/1-b bendinde kabahat olarak tanımlanmış ve bu yükümlölükleri yerine getirmeyenlere kurul tarafından 15.000 Türk lirasından 1.000.000 Türk lirasına kadar idari para cezası verileceği ifade edilmiştir. Yeniden değerlendirme oranında artırılmış haliyle 2023 yılı içerisinde bu kabahati işleyenlere verilecek idari para cezasının alt sınırı 89 bin 579 lira, üst sınırı ise 5 milyon 972 bin 40 liradır.

Bu kabahat seçimlik hareketli bir kabahattir. 12nci maddede sayılan yükümlölüklerden birinin yerine getirilmemesi kabahatin oluşması için yeterlidir. Dördüncü fıkrada yer alan yükümlölüğe aykırı şekilde kişisel verileri başkasına açıklayan veri sorumlusu bu kabahatin yanı sıra TCK m.136’da düzenlenen kişisel verileri hukuka aykırı olarak verme, yayma veya ele geçirme suçunu da işlemiş olabilir. Şayet veri sorumlusu tek fiil ile hem bu kabahati hem de TCK m.136’da tanımlanan suçu işlemişse yalnızca suçtan dolayı yaptırım uygulanabilecektir (KK m.15/3).

6.1.3. Kurul Kararlarının Yerine Getirilmemesi

KVKK m. 18/1-c’de Kişisel Verileri Koruma Kurulu’nun kanunun 15inci maddesi uyarınca verdiği kararların yerine getirilmemesi kabahat olarak düzenlenmiştir. Kanunun 15inci maddesinde Kurulun ihlal iddiaları hakkında şikâyet üzerine veya resen inceleme yapabileceği düzenlenmiştir. Kurul inceleme yapabilmek için veri sorumlusundan konuyla ilgili bilgi ve belgeleri talep edecektir. Veri sorumlusu bu bilgi ve belgeleri kurula göndermek zorundadır. Kurul inceleme sonucunda verilerin işlenmesinin veya yurt dışına aktarımının durdurulmasına karar verebilir. Tespit ettiği hukuka aykırılıkların giderilmesine karar verebilir. Kurulun talep ettiği bilgi ve belgelerin gönderilmemesi veya kurul kararlarına uyulmaması hallerinde bu kabahat oluşacaktır²⁷¹.

²⁷¹ Kangal, s.225-228.

Kurul yaygın bir ihlal tespit ettiği durumlarda genel nitelikte ilke kararlar da yayımlayabilmektedir. Ancak bu kabahatin ilke kararlara uyulmaması durumunda değil yalnızca bireysel kararlara uyulmaması durumunda oluşmayacağı kabul edilmektedir²⁷².

Bu kabahati işleyen veri sorumlusu hakkında 25.000 Türk lirasından 1.000.000 Türk lirasına kadar idari para cezası verileceği ilgili fıkra da ifade edilmiştir. Yeniden değerlendirme oranında artırılmış haliyle 2023 yılı içerisinde bu kabahati işleyenlere verilecek idari para cezasının alt sınırı 149 bin 285 lira, üst sınırı ise 5 milyon 971 bin 989 liradır.

6.1.4. Veri Sorumluları Siciline Kayıt veya Bildirim Yükümlülüğüne Aykırı Hareket Etme

Kanunun 16ncı maddesinde veri sorumluları siciline kayıt ve bildirim yükümlülüğü düzenlenmiştir. Buna göre veri işleyen her gerçek ve tüzel kişi veri işleme faaliyetleri hakkında detaylı bilgi içeren bir bildirimde bulunmak suretiyle bu sicile kaydolmak zorundadır. *“Ancak, işlenen kişisel verinin niteliği, sayısı, veri işlemenin kanundan kaynaklanması veya üçüncü kişilere aktarılma durumu gibi Kurulca belirlenecek objektif kriterler göz önüne alınmak suretiyle, Kurul tarafından, Veri Sorumluları Siciline kayıt zorunluluğuna istisna getirilebilir”* (KVKK m.16/2). Kurul bu yetkisini kullanarak bazı veri sorumlularını bu yükümlülükten ayrı tutmuştur²⁷³. Otomatik olmayan yollarla veri işleyen veri sorumluları, avukatlar, noterler ve yıllık çalışan sayısı 50’den az olan veri sorumluları gibi küçük çaplı veri işleme faaliyetinde bulunan pek çok veri sorumlusu istisna kapsamına alınmıştır²⁷⁴.

Veri sorumluları siciline kayıt ve bildirim yükümlülüğüne aykırı hareket etmek kabahat olarak tanımlanmıştır (KVKK m.18/1-ç). Bu kabahat yalnızca sicile kayıt yükümlülüğü bulunan veri sorumluları tarafından işlenebilecektir. Bu kabahati işleyen veri sorumlularına 20.000 Türk lirasından 1.000.000 Türk lirasına kadar idari para cezası

²⁷² Kangal, s.228.

²⁷³ 2018/32, 2018/68, 2018/75 ve 2018/87 sayılı Kurul Kararları ile bu istisnalar belirlenmiştir.

²⁷⁴ Detaylar için Kişisel Verileri Koruma Kurumu tarafından yayımlanan Sorularla VERBİS isimli kitapçığın 10uncu sayfasına bakınız. Online erişim için bkz. (https://verbis.kvkk.gov.tr/UploadedFiles/SORULARLA_VERB%C4%B0S.pdf) s.e.t. 1.03.2023

verileceği ifade edilmiştir. Yeniden değerlendirme oranında artırılmış haliyle 2023 yılı içerisinde bu kabahati işleyenlere verilecek idari para cezasının alt sınırı 119 bin 428 lira, üst sınırı ise 5 milyon 971 bin 989 liradır.

Bu kabahat seçimlik hareketli bir kabahattir. Veri sorumluları siciline hiç kayıt olmayarak veya kayıt bildiriminde eksik bilgi vererek bu kabahatin işlenmesi mümkündür²⁷⁵. Kayıt bildiriminde yer alması gereken bilgiler KVKK m.16/3’de düzenlenmiştir²⁷⁶.

6.2. KVKK’nın Suçlara İlişkin Hükümleri

Suçlara ilişkin hükümler KVKK’nın suçlar başlıklı 17nci maddesinde yer almaktadır. Bu madde iki fıkradan oluşmaktadır. Birinci fıkrada kişisel verilere ilişkin suçlar bakımından 5237 sayılı Türk Ceza Kanunu’nun 135 ila 140ıncı madde hükümlerinin uygulanacağı ifade edilmiştir. Atıf yapılan Türk Ceza Kanunu’nun 135inci maddesi kişisel verilerin hukuka aykırı olarak kaydedilmesini, 136ncı maddesi verileri hukuka aykırı olarak verme, yayma ve ele geçirme fiillerini, 138inci maddesi ise kişisel verilerin yok edilmemesini suç olarak düzenlemiştir. 137nci madde nitelikli halleri, 139uncu madde bu suçların şikâyeteye tabi olmadıklarını, 140ıncı madde ise tüzel kişilere uygulanacak güvenlik tedbirlerini düzenlemektedir. Yani birinci fıkranın atıf yaptığı TCK’nın 135 ila 140ıncı maddeleri arasında üç farklı suç tipi yer almaktadır. Bu suç tiplerine ilişkin detaylı açıklamalar üçüncü bölümde yapılacaktır.

17nci maddenin ikinci fıkrası ise kişisel verilerin silinmemesi ve anonim hale getirilmemesi fiillerine ilişkindir. Bu fıkrada yer alan hükmün ifade ettiği anlam tartışma konusu olmuştur. Kanaatimizce 17nci maddenin ikinci fıkrasındaki ifade ile kişisel verileri silmeyenler ve anonim hale getirmeyenler hakkında da TCK m.138 hükmünün

²⁷⁵ Kangal, s.238.

²⁷⁶ Buna göre bildirimde “a) Veri sorumlusu ve varsa temsilcisinin kimlik ve adres bilgileri. b) Kişisel verilerin hangi amaçla işleneceği. c) Veri konusu kişi grubu ve grupları ile bu kişilere ait veri kategorileri hakkındaki açıklamalar. ç) Kişisel verilerin aktarılabilmesi için alıcı veya alıcı grupları. d) Yabancı ülkelere aktarımı öngörülen kişisel veriler. e) Kişisel veri güvenliğine ilişkin alınan tedbirler. f) Kişisel verilerin işlendikleri amaç için gerekli olan azami süre” yer almalıdır.

uygulanacağı teyit edilmiştir. Bu maddenin ifade ettiği anlama ilişkin görüşümüz aşağıda detaylı şekilde açıklanmıştır.

6.2.1. KVKK m.17/2 Hükmüne İlişkin Değerlendirmemiz

Kanunun 17nci maddesinin ikinci fıkrasında “*Bu Kanunun 7nci maddesi hükmüne aykırı olarak; kişisel verileri silmeyen veya anonim hâle getirmeyenler 5237 sayılı Kanunun 138 inci maddesine göre cezalandırılır*” ifadesi yer almaktadır. Bu fıkra ne kadar ihtiyacı duyulduğu, kanun koyucunun bu fıkra hükmü ile tam olarak ne amaçladığı öğretide tartışma konusu olmuştur. Kimi yazarlar bu fıkra ile yeni bir suç tipi ihdas edildiğini ifade etmiştir²⁷⁷. Yeni bir suç tipi ihdas edildiğini iddia eden yazarlardan bazılarının göre TCK m.138 “*Verileri Yok Etmeme*” suçunu düzenlerken, KVKK m.17/2 “*Kişisel Verileri Silmeme veya Anonim Hale Getirmeme*” suçunu düzenlemektedir²⁷⁸. Bizim de katıldığımız diğer görüşe göre ise²⁷⁹ KVKK m.17/2’de yeni bir suç tipi ihdas edilmemiş, verilerin silinmemesi ve anonim hale getirilmemesi fiilleri bakımından da TCK m.138 hükmünün uygulanacağı teyit edilmek istenmiştir.

KVKK m.17/2 hükmünün hangi amaç ile getirildiğini tespit edebilmek için bu hükmün yanında KVKK m.7’de ve TCK m.138’de yer alan hükümleri de incelemek gerekmektedir. TCK m.138 “*Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde bir yıldan iki yıla kadar hapis cezası verilir*” hükmünü içermektedir. Bu ifadeye göre kanunların belirlediği sürelerin geçmiş olmasına rağmen verileri “*yok etmekle*” görevli kişilerin görevlerini yerine getirmemeleri suç olarak düzenlenmiştir.

KVKK’nın 7nci maddesi işleme sebepleri ortadan kalktığı takdirde veri sorumlularına verileri “*silme, yok etme veya anonim hale getirme*” görevini yüklemekte, bu seçimlilik hareketlerden birinin yapılmasını yükümlülüğün yerine getirilmesi için

²⁷⁷ Koca / Üzülmaz (2020), s.587, Maden, s.131-142. Dülger (2020), s.764.

²⁷⁸ Maden, s.121. Dülger (2020), s.764.

²⁷⁹ Sağlam, Tuğba (2020) Türk Ceza Hukukunda Kişisel Verilerin Korunması (Yüksek Lisans), Ankara Üniversitesi Sosyal Bilimler Enstitüsü, s.120. Yıldız, Gamze (2022) Kişisel Verilerin Korunması Bağlamında Verileri Yok Etmeme Suçu (Yüksek Lisans), Ankara Üniversitesi Sosyal Bilimler Enstitüsü, s.86.

yeterli kabul etmektedir²⁸⁰. Veri işleme sebepleri ortadan kalkmış olmasına rağmen bu seçimlik hareketlerden biri veri sorumlusu tarafından yerine getirilmemişse, veri sorumlusu verileri “*yok etme, silme veya anonim hale getirme*” görevini yerine getirmemiş olacaktır.

Kişilere kanunlar tarafından yok etme görevi verilen hallerde görev yerine getirilmemişse yok etmeme söz konusudur. Bu durumda TCK m.138’de tanımlanan verileri yok etmeme suçunun gündeme geleceğinde tereddüt yoktur. Fakat kanunlarda kişilere yüklenen görev silme veya anonim hale getirme şeklinde tanımlandığında bu yükümlülüklerin yerine getirilmemesi “*silmeme*” veya “*anonim hale getirmeme*” hareketi olarak tanımlanabilir. “*Silmeme*” ve “*anonim hale getirmeme*” hareketlerinin de TCK m.138’de tanımlanan “*yok etmeme*” hareketinin kapsamına girip girmediği konusunda tereddütler oluşmuştur. Kanaatimizce bu konuda bir tereddüde gerek yoktur. TCK m.138’de yer alan yok etme ifadesi silme ve anonim hale getirme fiillerini de kapsamaktadır²⁸¹. Dolayısıyla veri sorumlularının KVKK m.7’ye aykırı olarak verileri silmemesi, yok etmemesi veya anonim hale getirmemesi durumunda TCK m.138’de tanımlanan yok etmeme fiilini gerçekleştirdiklerini kabul etmek gerekir. Yani KVKK m.7 hükmüne aykırı hareket etmek başka herhangi bir kanun hükmünün göndermesine ihtiyaç olmadan TCK m.138 kapsamında değerlendirilebilecektir.

Kanun koyucu silmeme ve anonim hale getirmeme hareketlerinin TCK 138 kapsamına girip girmeyeceği konusunda bir tereddüt oluşabileceğini düşünerek KVKK m.17/2 hükmünde m.7’ye atıf yaparak kişisel verilerin silinmemesi ve anonim hale getirilmemesi durumunda kişilere TCK 138 uyarınca ceza verileceğini ifade etmiştir. Bu fıkra KVKK m.7’ye atıf yapıldıktan sonra yalnızca silmeme ve anonim hale getirmeme hareketlerinden bahsedilmesi, m.7’de yer alan yok etmeme hareketine yer verilmemesi, yok etmeme hareketinin TCK 138 kapsamında değerlendirileceği konusunda bir şüphenin bulunmamasından kaynaklanmakta ve fıkranın şüpheleri gidermek amacıyla kanuna

²⁸⁰ Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik m.7/5: “*Veri sorumlusu, Kurul tarafından aksine bir karar alınmadıkça, kişisel verileri resen silme, yok etme veya anonim hale getirme yöntemlerinden uygun olanını seçer.*”

²⁸¹ Aynı yönde görüş için bkz. **Koca / Üzülmaz** (2020), s.588, Yine KVKK’nın kabulünden önce “*Verileri Yok Etmeme*” suçunu “*Kişisel Verilerin Silinmemesi*” suçu olarak isimlendirenlerin olduğu göze çarpmaktadır. Bu durum silme ve yok etme kavramlarının birbiriyle eş anlamlı kabul edildiğine bariz bir örnektir. Örneğin Hale Akdağ TCK m.138’i “*Kişisel Verilerin Silinmemesi Suçu*” başlığıyla ele almaktadır. Bkz. **Akdağ, Hale** (2013) Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması, 1. Baskı, Ankara, Adalet Yayınevi, s.144.

konulduğuna delil oluşturmaktadır. Ancak bu hüküm tereddütleri ortadan kaldırmamış, bilakis daha fazla tartışmanın ve farklı düşüncenin ortaya çıkmasına yol açmıştır.

Suçlar başlıklı 17nci madde düzenlenirken KVKK m.7 ile TCK m.138 arasındaki uyumsuzluk dikkat çekmiş, m.17/2 hükmü de bu uyuşmazlığı ortadan kaldırmak için getirilmiştir. Fakat sorunun bu hüküm ile çözülmeye çalışılması kanaatimizce kanun yapma tekniği açısından problemlidir ve başka tartışmalara zemin hazırlamıştır. TCK 138’de yer alan yok etmeme suçunun fiil unsurunun hangi durumlarda oluşacağına ilişkin tartışmalar yaşanacağı düşünülüyorsa KVKK’da yok etme kavramı tanımlanmak suretiyle bu tartışmaların önüne geçilebilirdi. KVKK yok etmeyi silme ve anonim hale getirme kavramlarını da kapsayan bir kavram olarak tanımlamış olsa karışıklık giderilmiş olurdu.

Silme, yok etme ve anonim hale getirme kavramlarına ilişkin tanımlara Kurum tarafından yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik’te ayrı ayrı yer verilmiştir. Bu yönetmelikte ayrıca “*imha*” kavramına yer verilmiştir. Verilerin imha edilmesi kavramı silme, yok etme ve anonim hale getirme kavramlarının üçünü de kapsayacak şekilde tanımlanmıştır. Koca / Üzülmaz’e göre TCK m.138’de yer alan yok etme ifadesi yönetmelikte tanımlanan imha etme ifadesiyle eş anlamlı olarak düşünülmelidir²⁸². Biz de bu görüşe katılmaktayız. Koca / Üzülmaz’e katılmadığımız nokta yazarların KVKK m.17/2’nin yeni bir suç ihdas ettiği görüşüdür. Koca / Üzülmaz kanun koyucunun silme ve anonim hale getirme kavramlarının yok etme kavramı içinde kabul edilemeyeceği kanaatinde olduğunu, bu sebeple bu eksikliği yeni bir suç ihdas ederek kapatmaya çalıştığını savunmaktadır. Biz ise kanun koyucunun silme ve anonim hale getirme kavramlarını aslen yok etme kavramı içerisinde değerlendirdiğini, fakat uygulamada tereddüde mahal bırakmamak ve bu durumlarda da TCK m.138’in uygulanacağını teyit etmek için bu hükmü getirdiğini düşünmekteyiz²⁸³.

Kanaatimizce m.17/2 hükmünün bu hüküm ile yeni bir suç ihdas edildiği şeklinde yorumlanması uygulamada bazı problemlere yol açabilecek niteliktedir. Şöyle ki; verileri yok etmeme durumunda suçun unsurlarının gerçekleşip gerçekleşmediği TCK m.138 kapsamında belirlenecekken, verileri silmeme ve anonim hale getirmeme durumunda

²⁸² Koca / Üzülmaz (2020), s.588.

²⁸³ KVKK’nın gerekçesinde de kanun koyucunun yeni bir suç ihdas etme niyetinde olduğunu düşündürecek bir ifade bulunmamaktadır.

suçun unsurlarının gerçekleşip gerçekleşmediği KVKK m.17/2'ye göre belirlenmeye çalışılacaktır²⁸⁴. KVKK ile yeni bir suç ihdas edildiğini kabul edersek KVKK'nın istisna hükümlerinin bu suç için de geçerli olduğunu kabul etmek gerekecektir²⁸⁵. Verileri yok etmeme fiili bakımından geçerli olmayan istisna hükümlerinin silmeme ve anonim hale getirmeme fiilleri bakımından geçerli olduğunu kabul etmek doğru olmayacaktır²⁸⁶. Ayrıca verileri silmeme veya anonim hale getirmeme suçunun KVKK'nın kapsamına girmeyen hiçbir durumda oluşamayacağını kabul etmek gerekecektir. Açıkladığımız sebeplerle kanun koyucunun iradesinin yeni suç ihdas etmeye yönelik değil, tereddütleri gidermeye yönelik olduğunu kabul etmenin daha doğru olduğu kanaatindeyiz. Bu kabulün hükmün düzenleniş şeklindeki emareler, madde gerekçesi ve oluşacak sonuçlar birlikte değerlendirildiğinde daha yerinde olduğu kanaatindeyiz.

Yeni bir suç ihdas etme amacı gütmeyen KVKK'nın suçlar başlıklı 17nci maddesi kanaatimizce gereksiz olmuştur²⁸⁷. Bu maddeye kanunda hiç yer verilmemiş olsa zaten TCK'nın ilgili hükümleri şartları gerçekleştiği takdirde uygulanmaya devam edecektir.

²⁸⁴ Koca / Üzülmöz de böyle bir karmaşaya sebebiyet verdiği için kanun koyucuyu eleştirmektedir. Bkz. **Koca / Üzülmöz** (2020), s.587

²⁸⁵ KVKK'nın istisnalar başlıklı 28inci maddesi ile bu kanunun uygulanmayacağı bazı istisnai haller sayılmıştır. Bu istisnalar oldukça geniş bir alandaki veri işleme faaliyetlerini bu kanun hükümlerinden muaf tutmaktadır.

²⁸⁶ Koca / Üzülmöz TCK 135-140 arasında düzenlenen suçlar bakımından fiil unsurunun gerçekleşmesi için *“tamamen veya kısmen otomatik olan yollarla veya bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla”* veri işlenmesini şart koşmaktadır. Dolayısıyla KVKK kapsamına girmeyen bir fiilin TCK kapsamına girmesi bu yazarlara göre mümkün değildir. Onların benimsedikleri görüşe göre istisna hükümleri bakımından bir ikilik de oluşmayacaktır. Fakat üçüncü bölümde detaylarını açıklayacağımız üzere biz TCK'daki suç tiplerinin oluşması için fiillerin KVKK'daki veri işleme tanımına mutabık şekilde gerçekleşmesinin şart olmadığı kanaatindeyiz. Yani otomatik olmayan yollarla ve bir veri kayıt sisteminin de parçası olmadan gerçekleştirilen kaydetme, verme, yayma ve yok etmeme fiilleri TCK bakımından suç teşkil edebilecektir.

²⁸⁷ Aynı yöndeki görüş için bkz. **Koca / Üzülmöz** (2020), s.588.

ÜÇÜNCÜ BÖLÜM

KİŞİSEL VERİLERE İLİŞKİN SUÇLAR

Kişisel verilerin hukuka aykırı olarak işlenmesi veri sahibi için ciddi riskler oluşturmaktadır. Bu risklerin başında kişinin özel hayat alanının ihlal edilmesi gelmektedir. Kişisel verilerin hukuka aykırı olarak işlenmesi suretiyle başta özel hayat alanının ihlal edilmesi olmak üzere karşılaşılabilecek pek çok riske karşı kişilerin korunması için, Türk Ceza Kanunu'nun "*Kişilere Karşı Suçlar*" başlıklı ikinci kısmının "*Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar*" başlıklı dokuzuncu bölümünde 135, 136 ve 138nci maddelerinde doğrudan kişisel verilerin korunmasına odaklanmış bazı suç tipleri düzenlenmiştir. Kanun koyucu bu suç tipleri ile kişisel veriler üzerinde gerçekleştirilecek bazı hukuka aykırı fiilleri suç olarak tanımlamıştır. Bunlar kişisel verilerin hukuka aykırı olarak kaydedilmesi (m.135), hukuka aykırı olarak verilmesi, ele geçirilmesi veya yayılması (m.136) ve hukuken zorunlu olmasına rağmen yok edilmemesi (m.138) fiilleridir.

Doğrudan kişisel verilerin korunmasına odaklanmış bu suç tipleri 2005 yılında 5237 sayılı TCK ile yürürlüğe girmiştir. Bu suç tiplerinin yürürlüğe girdiği tarihte Türk Hukukunda kişisel verilerin korunmasına ilişkin başka hukuki düzenleme bulunmamaktadır. Türk Hukukunda kişisel verileri korumaya yönelik ilk hükümler 5237 sayılı TCK'da yer almıştır. Diğer yandan Avrupa ülkelerinde yapılan hukuki düzenlemelere bakıldığında önce veri koruma kanunlarının yürürlüğe konduğu, bu kanunlar ile eş zamanlı olarak veya bu kanunların yürürlüğe girmesinden kısa bir süre sonra kişisel verilere ilişkin suç tiplerinin düzenlendiği göze çarpmaktadır²⁸⁸.

²⁸⁸ Kişisel verilerin korunması hakkı ilk dönemlerde genellikle özel hayatın gizliliği kapsamında değerlendirildiğinden Anayasal düzenlemeler genellikle veri koruma kanunlarından sonra fakat ona yakın zamanda yapılmıştır. Detaylı değerlendirmelerimiz için bkz. birinci bölüm 4.1.1. numaralı başlık.

Ülkemizde kişisel verilerin korunmasına ilişkin hiçbir pozitif hukuk normu yokken bu konunun doğrudan ceza kanununda yeni suç tipleri ihdas etmek suretiyle düzenlenmesi bazı problemlere yol açmıştır. Konu ile ilgili kavramların ve bu alana hâkim ilkelerin tam olarak bilinmiyor oluşu bu problemlerin temelini oluşturmuştur. Özellikle kişisel veri kavramının çerçevesinin hukuk normlarıyla çizilmemiş olması suçun maddi unsurlarından biri olan suçun maddi konusunun hangi durumlarda var olduğu konusunda ciddi tartışmalara yol açmıştır. Bu tartışmalar suçun maddi konusu başlığında detaylı şekilde ele alınacaktır.

Kişisel verilerin korunması hakkı Anayasa Hukuku, Medeni Hukuk ve İdare Hukuku'nu yakından ilgilendirmektedir. Hakkın korunması öncelikle bu alanlarda yapılacak düzenlemelerle mümkündür. Ceza Hukuku ise doğası gereği diğer hukuk alanlarının korumasının yetersiz kaldığı durumlarda devreye girmektedir. Dolayısıyla diğer hukuk alanları tarafından hiçbir pozitif düzenlemeye konu edilmemiş bir konunun doğrudan Ceza Kanunu'nda suç olarak düzenlenmesinin hukuk mantığına uygun olmadığı söylenebilir. Konuya ilişkin usul ve esasların düzenlendiği ana kanun olan 6698 sayılı KVKK ile, suçların düzenlendiği 5237 sayılı TCK arasındaki diğer uyumsuzlukların²⁸⁹ temelinde de TCK'nın KVKK'dan çok önce yürürlüğe girmesi, dolayısıyla bu hükümlerin oturmuş bir öğreti ve birikim üzerine inşa edilmemiş olması yatmaktadır.

KVKK, yürürlüğe girdiği 2016 yılından beri TCK'daki hükümlerin uygulanması sırasında başvurulacak esas kanun haline gelmiştir. KVKK'nın kapsamına giren durumlarda, bu kanunda yer alan tanımlar, ilkeler, yükümlülükler ve veri işleme şartları bu suçların oluşup oluşmadığının değerlendirilmesi bakımından son derece önemlidir. Ancak KVKK'nın kapsamına girmeyen bazı durumlar da TCK'nın kapsamına girebilecektir. KVKK'ya göre veri işlemeden söz edebilmek için veriler üzerinde yapılan işlemin *“tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla”* gerçekleşmesi gerekir. Diğer bir ifadeyle veriler üzerinde otomatik olmayan yollarla ve bir veri kayıt sisteminin parçası da olmadan gerçekleştirilmiş işlemler veri işleme kapsamına girmez ve KVKK kapsamındaki

²⁸⁹ Bu uyumsuzluklar sırası geldikçe detaylarıyla ele alınacaktır. Şimdi birkaç örnek vermek gerekirse; KVKK'da düzenlenen özel nitelikli kişisel veri kategorileri ile TCK'da suçun konusuna ilişkin nitelikli hali oluşturan veri kategorileri arasında uyumsuzluk vardır. KVKK ve ilgili alt yönetmeliklerinde *“verileri imha etme”* olarak tanımlanan kavram, TCK'da *“verileri yok etme”* şeklinde kullanılmıştır ve bu durum ikinci bölümün *“KVKK'nın suçlara ilişkin hükümleri”* başlığında ele aldığımız üzere öğretide ciddi tartışmalara sebebiyet vermiştir.

düzenlemeler bu tür durumlarda uygulanmaz. Fakat KVKK'nın gerekçesinde de açıkça zikredildiği üzere bu durumlarda TCK'daki hükümler uygulanmaya devam edecektir²⁹⁰. Dolayısıyla TCK'daki suç tiplerine ilişkin değerlendirmelerde bulunurken KVKK'ya sadece KVKK kapsamına giren durumlar için başvurulabilecektir. KVKK kapsamına girmeyen durumlar için ise bilhassa hukuka uygunluk sebepleri bakımından TCK'da ve diğer kanunlarda yer alan düzenlemelere göre uygulama yapılmalıdır²⁹¹.

Öğretide bir yazar verilerin korunmasına ilişkin suç tiplerinin KVKK yerine TCK'da düzenlenmiş olmasını eleştirmiştir²⁹². KVKK ile TCK arasındaki uyumsuzlukların giderilmesi için en etkili yolun suç tiplerinin KVKK'da düzenlenmesi olduğunu, şayet bu yöntem izlenmeyecekse TCK'nın ilgili hükümlerinde değişiklikler yapılması suretiyle uyumsuzlukların giderilmesi gerektiğini ifade etmiştir²⁹³. Almanya ve İtalya gibi bazı Avrupa ülkelerinde kişisel verilere ilişkin suçlar veri koruma kanunlarında düzenlenmiştir²⁹⁴. Ancak ülkemizde bu suç tiplerinin TCK'da düzenlenmesi kanaatimizce yasama organının bilinçli bir tercihidir. KVKK'nın gerekçesinde de açıkça ifade edildiği üzere kanun koyucu KVKK kapsamına girmeyen durumlarda da TCK'daki hükümlerin uygulanabilmesini istemektedir²⁹⁵. Şayet suç tipleri KVKK'da düzenlenmiş olsaydı KVKK kapsamına girmeyen durumlarda bu suçların oluşmayacağını kabul etmek gerekirdi. Kanaatimizce suç tiplerinin KVKK'da düzenlenmesi bu suçların kapsamlarının daralmasına yol açacaktır. Dolayısıyla KVKK ve TCK arasındaki uyumsuzlukların giderilmesi için uyumsuzluğa sebep olan TCK hükümleri ile KVKK hükümlerinin yeniden düzenlenmesi daha doğru bir çözüm olacaktır.

Kişisel verilerin diğer bazı suç tipleri vasıtasıyla dolaylı olarak da korunduğu söylenebilir. Bu suç tiplerinin başında TCK'nın “*Özel Hayata ve Hayatın Gizli Alanına*

²⁹⁰ Madde 2 Gerekçesi: “Bu kapsamda, otomatik olmayan yollarla işlenen kişisel veriler bir veri kayıt sisteminin parçası değilse Kanun kapsamında değerlendirilmeyecektir. Ancak, bu hüküm anılan verilerin kişisel veri niteliğini etkilemeyeceğinden, bu tür verilere ilişkin hukuka aykırı eylemler 5237 sayılı Türk Ceza Kanunu uyarınca suç teşkil etmeye devam edecektir.” **Tasarı**, s.7 (<https://www5.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf>) s.e.t. 1.04.2023

²⁹¹ KVKK'nın kapsamını daraltan bir diğer hükme kanunun istisnalar başlıklı 28inci maddesinde yer verilmiştir. Bu konuya ilişkin detaylar ikinci bölümde ele alındığı için burada tekrar değinilmemiştir. 28inci maddede istisna olarak düzenlenmiş hallerde KVKK uygulanmayacağı için bu tür durumlarda da TCK'ya ve diğer kanunlara göre değerlendirme yapılmalıdır.

²⁹² **Orhan, Uğur** (2021) ‘Kişisel Verilerin Korunmasına İlişkin Türk Ceza Hukuku Düzenlemeleri Üzerine Değerlendirme’ Ankara Üniversitesi Hukuk Fakültesi Dergisi, C:70, S:4, (s.1359-1384), s.1359.

²⁹³ **Orhan**, s.1381.

²⁹⁴ Detaylı bilgi için birinci bölümde yer alan 4.1.1.1. ve 4.1.1.3. numaralı başlıklara bakınız.

²⁹⁵ **Tasarı**, s.7 (<https://www5.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf>) s.e.t. 1.04.2023.

Karşı Suçlar” başlıklı bölümünde yer alan Haberleşmenin Gizliliğini İhlal (TCK m.132), Kişiler Arasındaki Konuşmaların Dinlenmesi ve Kayda Alınması (TCK m.133) ve Özel Hayatın Gizliliğini İhlal (TCK m.134) suçları gelmektedir. Bunların yanı sıra Kişinin Hatırasına Hakaret (m.130), Ticari Sır, Bankacılık Sırrı veya Müşteri Sırrı Niteliğindeki Bilgi ve Belgelerin Açıklanması (m.239), Göreve İlişkin Sırrın Açıklanması (m.258) suçları da yerine göre kişisel verilere dolaylı koruma sağlamaktadır.

Çalışmamızın bu bölümünde öncelikle kişisel verilere dolaylı koruma sağlayan suç tipleri hakkında genel bilgiler verilecek, daha sonra doğrudan kişisel verileri korumaya özgülenmiş suç tipleri detaylı şekilde incelenecektir. Doğrudan kişisel verileri korumaya özgülenmiş suç tipleri tipleri incelenirken KVKK kapsamına giren fiiller için ikinci bölümde açıkladığımız KVKK hükümlerinden de yararlanılacaktır.

1. KİŞİSEL VERİLERE DOLAYLI KORUMA SAĞLAYAN SUÇ TİPLERİ

Türk Ceza Kanunu’nda yer alan bazı suç tipleri esasen başka bir hukuki menfaati korumaya odaklanmış olmalarına rağmen kişisel verilere de dolaylı olarak koruma sağlamaktadır. Bu suçların konusu doğrudan kişisel veriler değildir. Ancak yerine göre bu suçların maddi konuları kişisel veri niteliği de taşıyabilmektedir. Bu suçların konularının kişisel verilerden oluşması durumunda kişisel veriler de dolaylı şekilde korunmuş olmaktadır.

1.1. Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar

Kişisel verilere dolaylı yoldan koruma sağlayan suçların başında TCK’nın özel hayata ve hayatın gizli alanına karşı suçlar başlıklı bölümünde düzenlenen suçlar gelmektedir. Bu bölümde yer alan suçlardan doğrudan kişisel verilerin korunmasına özgülenmiş suç tipleri haricindeki suçlar kişisel verilere dolaylı koruma sağlamaktadır.

1.1.1. Haberleşmenin Gizliliğini İhlal (TCK m.132)

Haberleşmenin Gizliliğini İhlal Suçu Türk Ceza Kanunu'nun 132nci maddesinde düzenlenmiştir. Suç ile Anayasa'nın 22nci maddesinde yer alan haberleşme hürriyeti kapsamında haberleşmenin mahremiyeti korunmaktadır²⁹⁶. Haberleşmenin mahremiyeti haberleşmenin başkalarının denetim ve gözetiminden uzak bir şekilde gerçekleştirilmesi hakkını ifade eder²⁹⁷.

Bu suç 132nci maddede üç fıkra halinde düzenlenmiştir. Her bir fıkroda ayrı bir suç tanımı yapılmıştır²⁹⁸. Birinci fıkranın birinci cümlesinde haberleşmenin gizliliğini ihlal eden kişiye 1 yıldan 3 yıla kadar hapis cezası verileceği ifade edilmiştir. Birinci fıkranın ikinci cümlesinde ise ihlalin haberleşme içeriklerinin kaydı suretiyle gerçekleşmesi nitelikli hal olarak düzenlenmiş, faile verilecek cezanın bir kat artırılacağı ifade edilmiştir. İkinci fıkroda haberleşme içeriklerinin hukuka aykırı olarak ifşa edilmesi hali düzenlenmiş, bu fiili gerçekleştiren kimseye 2 yıldan 5 yıla kadar hapis cezası verileceği ifade edilmiştir. Üçüncü fıkroda ise haberleşmenin taraflarından birinin diğer tarafın rızası olmadan haberleşme içeriğini ifşa etmesi suç olarak düzenlenmiş, bu fiili gerçekleştiren kişiye 1 yıldan 3 yıla kadar hapis cezası verileceği ifade edilmiştir. Bu üç suç tanımının ortak özelliği suçun konusunu haberleşme içeriklerinin oluşturması ve suç ile haberleşmenin mahremiyetinin korunmasıdır.

Birinci ve ikinci fıkradaki fiilleri ancak haberleşmenin tarafı olmayan bir kişi işleyebilir. Haberleşmenin tarafı olan bir kişinin birinci ve ikinci fıkradaki fiili işlemesi mümkün değildir. Üçüncü fıkroda düzenlenen fiili ise ancak haberleşmenin tarafı olan bir kişi işleyebilir.

132nci maddede düzenlenen bu suçun oluşabilmesi için öncelikle kişiler arasında gerçekleşen bir haberleşmenin bulunması gerekir²⁹⁹. Bu haberleşmenin en az iki kişi arasında, başkalarıyla paylaşmadan özel bir şekilde, bir haberleşme vasıtası (telefon,

²⁹⁶ Koca / Üzülmöz (2020), s.516.

²⁹⁷ Koca / Üzülmöz (2020), s.517.

²⁹⁸ Koca / Üzülmöz (2020), s.516.

²⁹⁹ Koca / Üzülmöz (2020), s.518.

bilgisayar, mektup, faks gibi araçlar) kullanılarak gerçekleştirilmesi şarttır³⁰⁰. Suçun konusunu bu haberleşme vasıtaları ile gönderilen haberleşme içerikleri oluşturmaktadır. Kişiler arasında herhangi bir vasıta kullanmadan gerçekleştirilen konuşmalar ise bu suçun konusunu oluşturmaz.

Bu suçun oluşabilmesi için haberleşmenin taraflarından en az birisinin gerçek kişi olması şarttır³⁰¹. Tüzel kişiler arasındaki haberleşme içeriklerinin suçun konusunu oluşturması mümkün değildir. Tüzel kişiler arasındaki haberleşme içeriklerinin ticari sırlara ilişkin olması durumunda şartları oluşmuşsa TCK m.239 kapsamında korunmaları mümkündür.

Haberleşme içerikleri kişilerin birbirlerine duygu, düşünce veya herhangi bir bilgiyi iletme için kullandıkları ses, yazı veya sembol gibi unsurlardan oluşabilir. Kanaatimizce kişiler arasındaki haberleşme içerikleri aynı zamanda kişisel veri niteliği taşımaktadır. Kişinin haberleşme araçları vasıtasıyla bir başkasına özel olarak ne söylediğine ne gönderdiğine ilişkin bilgiler de o kişiye ilişkin bilgi olarak kabul edilmelidir. Bu suçun işlenebilmesi için haberleşme içeriklerinin gizli olması gerekmektedir³⁰². Kamunun erişimine açık bir şekilde gerçekleştirilen bir haberleşmenin içeriği bu suçun konusunu oluşturamaz. Bu suçun gerçekleştiği her durumda fiilin işleniş şekline göre TCK m.135 veya 136 ile ıçtima ilişkisi oluşacaktır. TCK m.135 ve m.136 incelenirken bu suç ile ıçtima ilişkilerine ıçtima başlıkları altında yer verilmiştir.

1.1.2. Kişiler Arasındaki Konuşmaların Dinlenmesi ve Kayda Alınması (TCK m.133)

Kişiler Arasındaki Konuşmaların Dinlenmesi ve Kayda Alınması Suçu TCK'nın 133üncü maddesinde üç fıkra halinde düzenlenmiştir. Esasen her fıkrada ayrı bir suç tanımı yapılmak suretiyle üç farklı suç tipinin düzenlendiğini söylemek mümkündür³⁰³.

³⁰⁰ **Yokuş Sevük, Handan** (2009) 'Haberleşmenin Gizliliğini İhlal Suçu' Dicle Üniversitesi Hukuk Fakültesi Dergisi, C:12-13, S:16-17-18-19, (s.159-195), s.169. **Koca / Üzülmöz** (2020), s.518.

³⁰¹ **Korkmaz**, s.378.

³⁰² Detaylı bilgi için bkz. **Yokuş Sevük**, s.169-170.

³⁰³ **Koca / Üzülmöz** (2020), s.529.

133üncü maddenin birinci fıkrasında “*kişiler arasındaki aleni olmayan konuşmaları, taraflardan herhangi birinin rızası olmaksızın bir aletle dinlemek veya bunları bir ses alma cihazı ile kaydetmek*” suç olarak düzenlenmiş, bu fiili işleyen kişiye 2 yıldan 5 yıla kadar hapis cezası verileceği ifade edilmiştir. İkinci fıkrada “*kişinin katıldığı aleni olmayan bir söyleşiyi, diğer konuşanların rızası olmadan ses alma cihazı ile kayda alması*” suç olarak düzenlenmiş ve bu fiili işleyen kişiye 6 aydan 2 yıla kadar hapis veya adli para cezası verileceği ifade edilmiştir. Üçüncü fıkrada ise “*kişiler arasındaki aleni olmayan konuşmaların kaydedilmesi suretiyle elde edilen verilerin hukuka aykırı olarak ifşa edilmesi*” suç olarak düzenlenmiş, bu fiili işleyen kişilere 2 yıldan 5 yıla kadar hapis ve dört bin güne kadar adli para cezası verileceği ifade edilmiştir.

133üncü maddede düzenlenen suçlar ile özel hayatın gizliliğinin bir parçası olarak kabul edilen sözün mahremiyeti korunmaktadır³⁰⁴. Bu suçların maddi konusunu kişiler arasındaki aleni olmayan ve bir vasıta kullanmadan yüz yüze yapılan konuşmalar oluşturmaktadır³⁰⁵. Bir araç vasıtasıyla gerçekleştirilen konuşmalar ise haberleşme niteliği taşıyacağı için bu suçun değil TCK m.132’de düzenlenen suçun konusunu oluşturur³⁰⁶.

Kişiler arasındaki konuşmalar aynı zamanda kişisel veri niteliği taşımaktadır. Dolayısıyla TCK m.133 ile m.135 ve 136’da düzenlenen suçlar arasında içtima ilişkisi oluşması kaçınılmazdır. Bu suçun kişisel verilere karşı suçlar ile içtima ilişkileri ileride ilgili suç tiplerinin içtima başlıkları altında incelenecektir.

1.1.3. Özel Hayatın Gizliliğini İhlal (TCK m.134)

Özel Hayatın Gizliliğini İhlal Suçu TCK’nın 134ncü maddesinde iki fıkra halinde düzenlenmiştir. Birinci fıkranın birinci cümlesinde “*kişilerin özel hayatının gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır*” ifadesine yer verilmiştir. Bu cümlede oldukça geniş kapsamlı bir suç tanımı yapılmıştır. Özel hayatın gizliliğinin herhangi bir şekilde ihlal edilmesi bu suçun oluşması için yeterlidir.

³⁰⁴ Özbek, Veli Özer / Doğan, Koray / Bacaksız, Pınar (2022) Türk Ceza Hukuku Özel Hükümler, 17. Baskı, Ankara, Seçkin, s.573.

³⁰⁵ Korkmaz, s.380.

³⁰⁶ Korkmaz, s.380.

Suç ile korunan hukuki menfaat özel hayatın gizliliği hakkıdır³⁰⁷. Suçun maddi konusunu ise kişinin özel hayat alanına giren her türlü unsur oluşturabilir. Özel hayat alanına nelerin dahil olduğunu tespit için farklı teoriler geliştirilmiştir. Bunlardan en çok kabul gören üç alan teorisidir. Bu teoriye göre kişinin hayat alanı kamuya açık hayat alanı, özel hayat alanı ve gizli hayat alanı olmak üzere üçe ayrılır³⁰⁸. Gizli hayat alanı kişinin kimseyle paylaşmadığı, kendisine mahsus kıldığı, kimsenin bilmesini istemediği, ancak çok güvendiği ve en yakın gördüğü bazı kişilere açtığı hayat alanıdır³⁰⁹. Özel hayat alanı kişinin gizli hayat alanından biraz daha fazla kişi ile paylaştığı, ailesi, arkadaşları ve yakın çevresinden dilediği sınırlı sayıdaki kişiye açtığı hayat alanıdır³¹⁰. Kamuya açık alan ise kişinin herhangi bir gizliliği bulunmayan hayat alanıdır. Özel hayat alanı ve gizli hayat alanı özel hayatın gizliliği hakkı kapsamında korunmaktadır. Kamusal hayat alanı ise esasen herhangi bir gizliliği bulunmadığı için koruma altında değildir. Fakat öğretide ve yargı kararlarında genel olarak kabul edilen görüşe göre kişinin kamusal hayat alanındaki hayatı da büsbütün koruma kapsamı dışında tutulmamalıdır³¹¹. Kişinin kamusal alandaki yaşamına dair makul beklentileri göz önünde bulundurulmalıdır³¹².

Birinci fıkranın birinci cümlesinde yer alan suç tanımında özel hayatın gizliliğinin ne şekilde ihlal edileceği belirtilmemiştir. Öğretide bu ihlalin kişinin beş duyusu vasıtasıyla başkalarının özel hayatlarını algılaması ile gerçekleşeceği ifade edilmiştir³¹³. Oldukça soyut ve genel bir şekilde tanımlanmış olan bu suçu somutlaştırmak için öğretide bazı

³⁰⁷ Koca / Üzülmaz (2020), s.544.

³⁰⁸ Koca / Üzülmaz (2020), s.545.

³⁰⁹ Koca / Üzülmaz (2020), s.545.

³¹⁰ Koca / Üzülmaz (2020), s.545.

³¹¹ "TCK'nın 134. maddesinde düzenlenen özel hayatın gizliliğini ihlal suçunun konusunu oluşturan özel hayat kavramı; kişinin sadece gözlerden uzakta, başkalarıyla paylaşmadığı, kapalı kapılar ardında, dört duvar arasındaki yaşantısı ve mahremiyetinden ibaret değil, herkesin bilmediği veya bilmemesi gereken, istenildiğinde başka kişilere açıklanabilen, tamamen kişiye özel hayat olayları ve bilgilerin tamamını içerir. Bu nedenle, kamuya açık alanda bulunulması, bu alandaki her görüntü veya sesin dinlenilmesine, izlenilmesine, kaydedilmesine, sürekli ve izinsiz olarak elde bulundurulmasına rıza gösterildiği anlamına gelmez. Kamuya açık alanda bulunulduğunda dahi, "kalabalığın içinde dikkat çekmezlik, tanınmazlık, bilinmezlik" prensibi geçerli olup, kamuya açık alandaki kişinin, gün içerisinde yaptıkları, gittiği yerler, kiminle niçin, nasıl, nerede ve ne zaman görüştüğü gibi hususları tespit etmek amacıyla sürekli denetim ve gözetim altına alınması sonucu elde edilmiş bilgileri ya da onun başkalarınca görülmesi ve bilinmesini istemeyeceği, özel yaşam alanına girdiğinde şüphe bulunmayan faaliyetleri özel hayat kavramı kapsamına dahildir; ancak, süreklilik içermeyen ve özel yaşam alanına dahil olmayan olay ve bilgiler ise bu kapsamda değerlendirilemez. Sonuç olarak, bir olay ya da bilginin, özel hayat kavramı kapsamına girip girmediği belirlenirken, sadece içinde bulunulan fiziki çevrenin özelliklerine bakılmamalı, kişinin toplum içindeki konumu, mesleği, görevi, kamuoyu tarafından tanınıp tanınmadığı, dışa yansıyan davranışları, rıza ve öngörülere, sosyal ilişkileri, müdahalenin derecesi gibi ölçütler de göz önüne alınmalıdır." Yargıtay 12. Ceza Dairesi, E. 2015/9708, K. 2016/10986, K.T. 29.06.2016. Akyürek, Güçlü (2021) Özel Hayatın Gizliliğini İhlal Suçu, 3. Baskı, Ankara, Seçkin, s.218.

³¹² Bu konuda detaylı bilgi için bkz. Aktaş, s.149-150 ve 40.

³¹³ Soyaslan, Doğan (2020) Ceza Hukuku Özel Hükümler, 13. Baskı, Ankara, Yetkin Yayınları, s.354.

örnekler de zikredilmektedir. Odasında giyinen bir kişiyi kapı deliğinden gözetlemek, ağaca çıkarak komşusunun evinin içini gözetlemek, bir kişinin çantasını veya çekmecesini izinsiz karıştırmak, eşler arasındaki tartışmayı özel bir çaba göstererek dinlemek özel hayatın gizliliğinin ihlali suçunu oluşturur³¹⁴.

Birinci cümlede tanımlanan suç bu bölümde düzenlenen diğer suçlar bakımından genel norm niteliğindedir. Özel hayata ve hayatın gizli alanına karşı suçlar bölümünde düzenlenen diğer suç tiplerinin gerçekleşmediği durumlarda bu suç meydana gelecektir. İhlal eyleminin kişiler arasındaki haberleşme içerikleri, kişiler arasındaki konuşmalar veya kişisel veriler dışında özel hayat alanına dahil başka bir maddi konu üzerinde gerçekleştirilmesi halinde genel norm niteliğindeki m.134/1-c.1 hükmü uygulanacaktır.

Birinci fıkranın ikinci cümlesinde ise “*gizliliğin görüntü veya seslerin kayda alınması suretiyle ihlal edilmesi*” suçun nitelikli hali olarak düzenlenmiştir³¹⁵. Bu durumda birinci fıkraya göre verilecek ceza bir kat artırılabacaktır. İkinci cümlede yer alan hükmün uygulanabilmesi için görüntü ve seslerin kişinin özel hayat alanına ilişkin olması gerekmektedir.

İkinci fıkra ise “*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*” hükmüne yer verilmiştir. Bu fıkra tanımlanan suçun işlenebilmesi için kişinin özel hayat alanına ilişkin görüntü ve seslerin hukuka aykırı bir şekilde elde edilmiş olması şart değildir³¹⁶. Fıkra geçen “*hukuka aykırı olarak*” ifadesi tipik haksızlığın tamamını nitелеmektedir ve m.135 ile m.136’daki ifade ile aynı fonksiyonu görmektedir³¹⁷.

Kişilere ait ses ve görüntülerin kişisel veri niteliği taşıdığında şüphe yoktur. Dolayısıyla birinci fıkranın ikinci cümlesi ile TCK m.135 arasında, ikinci fıkra ile de TCK m.136 arasında sık sık içtima ilişkisi gündeme gelmektedir. Özel Hayatın Gizliliğini İhlal

³¹⁴ **Hafizoğulları, Zeki / Özen, Muharrem** (2010) Türk Ceza Hukuku Özel Hükümler: Kişilere Karşı Suçlar, Ankara, U S-A Yayınları, s.263-264. **Soyaslan** (2020), s.354.

³¹⁵ **Koca / Üzülmüş** (2020), s.543.

³¹⁶ **Soyaslan** (2020), s.356.

³¹⁷ Bu ifadenin anlamı ileride Kişisel Verilerin Kaydedilmesi Suçu incelenirken detaylı şekilde açıklanacaktır.

Suçu ile kişisel verilere ilişkin suçlar arasındaki içtima ilişkisi ileride ilgili suçların içtima başlıkları altında ayrıca incelenecektir.

1.2. Kişinin Hatırasına Hakaret (TCK m.130)

Kişinin Hatırasına Hakaret Suçu TCK'nın 130uncu maddesinde iki fıkra halinde düzenlenmiştir. Ceset ve kemiklere karşı tahkir edici fiilleri suç olarak düzenleyen ikinci fıkranın kişisel verileri ilgilendiren herhangi bir yönü bulunmamaktadır. Konumuzla ilgili olan ve kişinin hatırasına hakareti düzenleyen birinci fıkra hükmü ise aşağıdaki gibidir;

“(1) Bir kimsenin öldükten sonra hatırasına en az üç kişiyle ihtilat ederek hakaret eden kişi, üç aydan iki yıla kadar hapis veya adli para cezası ile cezalandırılır. Ceza, hakaretin alenen işlenmesi halinde, altıda biri oranında artırılır.”

Hakaret fiili somut bir fiil veya olgu isnat edilerek, sövme veya yakıştırmalarda bulunarak işlenebilir³¹⁸. Hakaret fiilinin ölüye karşı üç kişi ile ihtilat ederek işlenmesi bu suçun oluşması için yeterlidir. Suç ile ölünün devam edegelen insanlık değerinin korunduğu ifade edilmektedir³¹⁹. Ancak suçun takibinin şikâyetle bağlı olması ve şikâyet hakkının ölenin ikinci dereceye kadar üstsoy ve altsoyu, eş veya kardeşleri tarafından kullanılabilir olması suç ile ölenin devam eden insanlık değerinden ziyade ölenin yakınlarının korunduğu izlenimini vermektedir. Ölen kişi ile yakınları arasında bir husumet bulunması durumunda ölenin yakınları hakarettten müteessir olmayabilir ve dolayısıyla şikâyetle de bulunmayabilir. Yine hakaret fiilinin bizzat ölenin yakını tarafından işlenmiş olması durumunda da kişinin kendisinden şikayetçi olmayacağı açıktır. Şayet korunmak istenen hukuki menfaat doğrudan ölen kişinin saygınlığı, onuru veya insanlık değeri ise kanaatimizce suçun takibinin şikâyetle bağlı olmaması gerekirdi³²⁰.

³¹⁸ Koca / Üzülmöz (2020), s.506.

³¹⁹ Koca / Üzülmöz (2020), s.506.

³²⁰ Madde gerekçesinde yer alan “Genel olarak hakaret suçu ancak hayatta bulunan kişilere karşı işlenebilir. Çünkü, onur ve şeref, ancak yaşayan kişiler açısından söz konusudur” ifadesi de bu kanaatimizi destekler niteliktedir. Gerekçe için bkz. Özbek, Veli Özer (2008) Yeni Türk Ceza Kanunu’nun Anlamı (TCK İzmir Şerhi), 1.Baskı, Ankara, Seçkin, Cilt:2, s.853.

Kişisel verilerin korunması hukukundaki genel kabule göre ölmüş bir kişinin verileri kişisel veri olarak kabul edilmemektedir³²¹. Dolayısıyla ölümlere ait verilerin yayılması durumunda kişisel verileri hukuka aykırı olarak verme ve yaymadan söz edilemeyeceği için failin TCK m.136 nezdinde sorumluluğu bulunmamaktadır. Ancak ölmüş bir kişinin verilerinin ifşa edilmesi suretiyle hem ölünün hatırasının zedelenmesi hem de yakınlarının mağdur edilmesi mümkündür. Ölmüş bir kişinin ceza mahkumiyetine ilişkin verilerin yayılması suretiyle saygınlığının zedelenmeye çalışılması durumunda kişinin hatırasına hakaret suçu oluşacaktır. Evli ve çocuk sahibi bir adamın çocuk sahibi olmasının aslında mümkün olmadığını gösteren sağlık raporunun öldükten sonra yayınlanması örneğinde de durum böyledir. Bu raporun yayınlanması suretiyle hem ölen kişinin hem de ailenin diğer fertlerinin saygınlığının zedelenmesi kaçınılmazdır. Bu durumda da kişinin hatırasına hakaret suçu meydana gelecektir.

Ölmüş bir kişinin verilerinin doğrudan kişisel verileri korumaya özgülenmiş suçlar vasıtasıyla korunmaması, yalnızca diğer bazı suçların dolaylı korunması altında olması kanaatimizce yeterli değildir. Çünkü TCK m.130 yalnızca yayınlanması halinde kişinin hatırasına hakaret oluşturabilecek verilere bir koruma sağlamaktadır. Yayılması hakaret teşkil etmeyen veriler ise bu madde nezdinde korunamamaktadır. Ayrıca bu fiilin ölenin yakınları tarafından işlenmesi durumunda veya ölenin yakınlarının bu fiili umursamamaları durumunda kişinin hatırasına hakaret de cezasız kalmaktadır. Kişinin yaşarken kişiliğini özgürce geliştirmesinin ancak öldükten sonra da verilerinin korunacağına duyacağı güven ile sağlanabileceği göz önünde bulundurulmalı, ölümlerin verileri de hem KVKK nezdinde hem de TCK m.136 nezdinde korunmalıdır. Kanaatimizce ölümlere ait verilerin kişisel veri olarak kabul edilmesine imkân tanıyacak bir hüküm ile bu koruma sağlanabilir.

1.3. Göreve İlişkin Sırrın Açıklanması (TCK m.258)

Göreve İlişkin Sırrın Açıklanması Suçu TCK'nın 258inci maddesinde aşağıdaki şekilde düzenlenmiştir;

³²¹ Bu konudaki detaylı açıklamalarımız için birinci bölümün 1.2.2. numaralı başlığına bakabilirsiniz.

“(1) Görevi nedeniyle kendisine verilen veya aynı nedenle bilgi edindiği ve gizli kalması gereken belgeleri, kararları ve emirleri ve diğer tebligatı açıklayan veya yayınlayan veya ne suretle olursa olsun başkalarının bilgi edinmesini kolaylaştıran kamu görevlisine, bir yıldan dört yıla kadar hapis cezası verilir.

(2) Kamu görevlisi sıfatı sona erdikten sonra, birinci fıkra yazılı fiilleri işleyen kimseye de aynı ceza verilir.”

Bu suç yalnızca kamu görevlileri tarafından işlenebilmektedir. Dolayısıyla özgü suçtur. Kamu görevlisi sıfatının sona ermesinden sonra da kamu görevi sırasında görevi nedeniyle edindiği bilgilerle ilgili olarak yukarıdaki fiilleri işleyen kişilere de bu hüküm uygulanmaya devam edecektir.

Birinci fıkra hükmü ile genel olarak kamu görevlisinin görevi nedeniyle kendisine verilen ya da görevi nedeniyle bilgi edindiği ve gizli kalması gereken belgeleri, kararları, emirleri ve diğer tebligatı açıklaması suç olarak düzenlenmiştir. Madde metninden suçun maddi konusunun belge, karar, emir veya tebligat olması gerektiği anlaşılmaktadır. Ancak belge, karar, emir veya tebligatın doğrudan yayınlanması veya verilmesinin şart olmadığı, bunların içerisinde mündemiç olarak bulunan bilgilerin açıklanmasının yeterli olduğu kabul edilmektedir³²². Bu bilginin kamu görevlisi tarafından görevi nedeniyle edinilmiş olması ve gizli kalması gereken bir bilgi olması gerekmektedir.

Göreve İlişkin Sırrın Açıklanması Suçunun kapsamına ilişkin öğretide farklı görüşler bulunmaktadır. Bizim de katıldığımız görüşe göre bu suç çeşitli kanun ve yönetmeliklerle kamu görevlilerine yüklenmiş meslek sırrının saklanmasına yönelik yükümlülüklerin ihlali durumunda meydana gelecek genel bir normdur³²³. Meslek sırrının ifşasının başkaca bir suç oluşturmadığı durumlarda genel norm niteliğindeki 258nci madde uygulanacaktır³²⁴. Avukatlık Kanunu’nun 36ncı maddesinde³²⁵, Bankacılık Kanunu’nun

³²² Bayraktar, Köksal / Evik, Vesile Sonay / Kangal, Zeynel T. / Yıldız, Ali Kemal / Zafer, Hamide ve diğerleri (2021) Özel Ceza Hukuku Cilt IX – Kamu İdaresinin Güvenilirliğine ve İşleyişine Karşı Suçlar, 1. Baskı, İstanbul, On İki Levha Yayınları, s.280.

³²³ Özen, Muharrem / Köksal, Atacan (2020) ‘Göreve İlişkin Sırrın Açıklanması Suçu’ Ankara Üniversitesi Hukuk Fakültesi Dergisi, C:69, S:1, (s.189-232), s.194. Aynı yöndeki görüş için ayrıca bkz. Alşahin, Mehmet Emin (2014) ‘Göreve İlişkin Sırrın Açıklanması Suçu’ Marmara Üniversitesi Hukuk Fakültesi Dergisi, C:20, S:2, (s.219-250), s.225-226.

³²⁴ “Bu itibarla ancak kamu görevlisinin gördüğü fonksiyon sebebiyle öğrendiği bir sırrı açıklaması başka herhangi bir maddenin uygulanmasına yol açmadığı hallerde, genel ve tamamlayıcı nitelikte olan göreve ilişkin sırrın açıklanması hükmünün uygulanması mümkün olacaktır.” Özen / Köksal, s.194., Alşahin, s.226.

73üncü maddesinde³²⁶, Serbest Muhasebeci Mali Müşavir ve Yeminli Mali Müşavirlerin Çalışma Usul ve Esasları Hakkında Yönetmeliğin 7nci maddesinde³²⁷ ve Hasta Hakları Yönetmeliğinin 23ncü maddesinde³²⁸ mesleğin icrası sırasında öğrenilen bilgilerin hukuka aykırı şekilde açıklanması yasaklanmıştır. Bu yükümlülöklere aykırı hareketlerin başka bir suç teşkil etmediğı durumlarda suça ilişkin diğör şartlar da gerçekleşmiş ise TCK m.258 hükmü uygulanacaktır.

Bu suçun maddi konusunu oluşturan bilgilerin kişisel veri içermesi ve TCK m.258 kapsamında kişisel verilere dolaylı bir koruma sağlanması mümkündür. Ancak kişisel verilerin hukuka aykırı olarak verilmesi veya yayılması öncelikle TCK m.136 kapsamında değerlendirilecek, şayet bu suç bir sebepten oluşmamış ise TCK m.258 hükmü uygulanacaktır. Ölmüş bir kişiye ait verilerin hukuka aykırı olarak verilmesi ve yayılması olayında kanaatimizce bu durum gerçekleşir. Ölümlere ait verilerin TCK m.136'nın konusunu oluşturması mevzuatımıza göre mümkün değildir. Ancak mesleki sırların saklanması ile ilişkin yükümlölüklerin kişinin ölümü ile birlikte de devam edeceği kanaatindeyiz³²⁹. Dolayısıyla ölen kişinin verilerinin diğör şartların da varlığı halinde m.258 kapsamında korunması mümkündür.

TCK m.258 hükmünün kapsamına ilişkin bir diğör görüşe göre bu suçun maddi konusu dar bir şekilde tanımlanmıştır³³⁰. Hasta bilgileri gibi kişisel veriler kamu görevi

³²⁵ 1136 sayılı Avukatlık Kanunu m.36: “Avukatların, kendilerine tevdi edilen veya gerek avukatlık görevi, gerekse, Türkiye Barolar Birliği ve barolar organlarındaki görevleri dolayısıyla öğrendikleri hususları açığa vurmaları yasaktır.”

³²⁶ 5411 sayılı Bankacılık Kanunu m.73: “Sıfat ve görevleri dolayısıyla bankalara veya müşterilerine ait sırları öğrenenler, söz konusu sırları bu konuda kanunen açıkça yetkili kılınan mercilerden başkasına açıklayamazlar. Bu yükümlölük görevden ayrıldıktan sonra da devam eder.”

³²⁷ Yönetmelik m.7: “Meslek mensupları ve bunların yanlarında çalışanlar mesleki faaliyetleri dolayısıyla öğrendikleri bilgi ve sırları mesleki faaliyetlerine son verseler bile ifşa edemezler....” Tam metin için bkz. (<https://www.mevzuat.gov.tr/anasayfa/MevzuatFihristDetayIframe?MevzuatTur=7&MevzuatNo=4650&MevzuatTertip=5>) s.e.t. 1.04.2023

³²⁸ Yönetmelik m.23: “Sağlık hizmetinin verilmesi sebebiyle edinilen bilgiler, kanun ile müsaade edilen haller dışında, hiçbir şekilde açıklanamaz.” Tam metin için bkz. (<https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=4847&MevzuatTur=7&MevzuatTertip=5>) s.e.t. 1.04.2023.

³²⁹ Hekimlik Meslek Etiğı Kurallarının sır saklama yükümlölüğüne ilişkin 9ncu maddesinde “Hekim, hastasından mesleğini uygularken öğrendiğı sırları açıklayamaz. Hastanın ölmesi ya da o hekimle ilişkisinin sona ermesi, hekimin bu yükümlölüğünü ortadan kaldırmaz” ifadesi yer almaktadır. Bkz. Türk Tabipler Birliği Yayınları, Hekimlik Meslek Etiğı Kuralları, (https://www.ttb.org.tr/kutuphane/h_etikkural.pdf) s.e.t. 1.04.2023. Sır saklama yükümlölüğünün ilgili kişinin ölmesinden sonra da devam edeceğinin bir hukuk kurallıyla açıkça ifade edilmediğı durumlarda da kanaatimizce mesleğe ilişkin sırrın korunmasına devam edilmelidir.

³³⁰ **Hakeri, Hakan** (2022) Tıp Ceza Hukuku, 2. Baskı, Ankara, Seçkin, s.284. Yargıtay da bir kararında “göreve ilişkin sırrın açıklanması suçunda ifade edilen sırrın kamu idaresinin yürütölmesi ve işleyişine

nedeniyle gizliliği haiz belgelerden olmadığı için kişisel verilerin verilmesi ve yayılması eylemleri m.258 kapsamında değerlendirilemeyecektir³³¹. Kişisel verilerin hukuka aykırı şekilde verilmesi ve yayılması fiilleri bakımından yalnızca TCK m.136 hükmü uygulanabilecektir³³².

1.4. Ticari Sır, Bankacılık Sırrı veya Müşteri Sırrı Niteliğindeki Bilgi ve Belgelerin Açıklanması (TCK m.239)

Bu suç TCK'nın 239uncu maddesinde dört fıkra halinde düzenlenmiştir. Konumuzla ilgili olan birinci fıkra hükmü aşağıdaki gibidir;

“(1) Sıfat veya görevi, meslek veya sanatı gereği vakıf olduğu ticari sır, bankacılık sırrı veya müşteri sırrı niteliğindeki bilgi veya belgeleri yetkisiz kişilere veren veya ifşa eden kişi, şikayet üzerine, bir yıldan üç yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır. Bu bilgi veya belgelerin, hukuka aykırı yolla elde eden kişiler tarafından yetkisiz kişilere verilmesi veya ifşa edilmesi halinde de bu fıkraya göre cezaya hükmolunur.”

Söz konusu suç ile ekonomik istikrar, güven ilişkisi, kamu düzeni ve müşterilerin özel hayatlarının gizliliği gibi birden fazla hukuki yararın korunduğu kabul edilmektedir³³³. Suçun ekonomi, sanayi ve ticarete ilişkin suçlar bölümünde düzenlenmiş olması dikkate alındığında suç ile korunan hukuki yararın daha çok ekonomik ve sınaî haklar olduğu, özel hayatın gizliliğinin korunmasının ise ikinci planda yer aldığı ifade edilebilir.

Suçun maddi konusunu ticari sır, bankacılık sırrı veya müşteri sırrı niteliğindeki bilgi ve belgeler oluşturmaktadır. Failin bu bilgilere mesleği, görevi, sıfatı veya sanatı gereği sahip olmuş olması gerekir. Ticari sırlar ve bankacılık sırları genelde tüzel kişilere ilişkin bilgiler içermektedir. Dolayısıyla suçun konusunun ticari sırlardan veya bankacılık

ilişkin bilgi ve belgeleri kapsadığı” ibaresine yer vermek suretiyle suçun maddi konusunu dar şekilde tanımlamıştır. Yargıtay 5. C.D., E. 2014/6781, K.2016/8476.

³³¹ **Hakeri**, s.284

³³² **Hakeri**, s.284

³³³ **Çırak, Ezgi** (2022) ‘Ticari Sırrın İfşasından Doğan Ceza Sorumluluğuna İlişkin Türk ve Alman Hukuk Sistemlerindeki Güncel Durumun Değerlendirilmesi’ Ticaret ve Fikri Mülkiyet Hukuku Dergisi, C:8, S:1, (s.179-206), s.185.

sırlarından oluşması durumunda suç ile tüzel kişilere ait verilerin korunduğu kabul edilmektedir³³⁴. Suçun konusunun müşteri sırrı niteliğindeki bilgilerden oluşması halinde ise gerçek kişilere ait veriler, yani kişisel veriler korunmaktadır³³⁵.

2. KİŞİSEL VERİLERİN KAYDEDİLMESİ (TCK m.135)

Kaydetme işlemi kişisel veriler üzerinde gerçekleştirilen işlemlerin en önemlilerinden biridir. Çünkü kaydetme işlemi genellikle veri işleme sürecinin ilk adımını teşkil eder. Verilerin kullanılabilmesi için öncelikle kaydedilmesi veya ele geçirilmesi gerekir. Kamu hizmetlerinin görülmesi, ticari ilişkilerin kurulması, bir hizmetin sağlanması, resmî veya özel kurum ve kuruluşların faaliyetlerinin yerine getirilmesi, genel sağlığın, güvenliğinin ve kamu düzeninin korunması gibi pek çok meşru amaç için kişisel veriler kaydedilmektedir. Kişisel verilerin kaydedilmesi hayatın devam edebilmesi için adeta bir zorunluluk halini almıştır. Verilerin hukuka uygun olarak kaydedilmesinde hem veri sahibinin hem veri işleyeninin hem de kamunun menfaati olduğu şüphesizdir. Ancak verilerin hukuka aykırı olarak kaydedilmesi durumunda verileri kaydedilen kişinin başta kişisel verilerin korunması hakkı olmak üzere bu hak ile ilişkili pek çok temel hak ve hürriyetinin tehlikeye düşmesi de söz konusudur. Veri işleme sürecinin ilk ve en önemli adımını oluşturan verilerin kaydedilmesi fiilinin hukuka aykırı olarak gerçekleştirilmesi durumunda kanun koyucu failin cezai yaptırıma tabi tutulmasını gerekli görmüş ve kişisel verilerin kaydedilmesi suçu ihdas edilmiştir.

Suç “*Kişisel Verilerin Kaydedilmesi*” başlığını taşıyan m.135’in birinci fıkrasında aşağıdaki gibi tanımlanmıştır;

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

135inci maddenin ikinci fıkrasında suçun konusuna ilişkin nitelikli hâl tanımlanmıştır³³⁶. Bu fıkra da yer alan ve suçun konusuna ilişkin olan nitelikli haller

³³⁴ Korkmaz, s.206.

³³⁵ Korkmaz, s.206.

yalnızca bu suç tipi için geçerlidir. Hem “*kişisel verilerin kaydedilmesi*” suçunu hem de “*verileri hukuka aykırı olarak yayma ve ele geçirme*” suçunu kapsayan diğer nitelikli haller ise “*Nitelikli haller*” başlığını taşıyan m.137’de düzenlenmiştir³³⁷. Nitelikli hallere ilişkin detaylı değerlendirme ilgili başlıkta yapılacaktır.

2.1. Korunan Hukuki Değer

Yukarıda da belirttiğimiz üzere kişisel verilerin kaydedilmesi suçuna ilişkin hükümler yeni TCK ile birlikte 2005 yılında yürürlüğe girmiştir. TCK’nın yürürlüğe girdiği tarihte henüz kişisel verilerin korunması hakkı Anayasa’da ayrı bir fıkra olarak tanınmamıştır. Kişisel verilerin korunması hakkı o dönemde Anayasa m.20/1’de düzenlenen özel hayatın gizliliği hakkının bir alt görünüm şekli olarak kabul edilmekte ve bu çerçevede korunmaktadır. O dönemin kabullerine uygun olarak kişisel verilere ilişkin suç tipleri de TCK’nın “*Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar*” bölümünde düzenlenmiştir. Suçun düzenlendiği bölümü ve kişisel verilerin korunması hakkının özel hayatın gizliliği hakkı içerisinde değerlendiriliyor oluşunu nazar-ı itibara alarak öğretide bazı yazarlar bu suç tipi ile korunan hukuki değerın özel hayatın gizliliği hakkı olduğunu ifade etmiştir³³⁸.

2010 Anayasa değişikliğinden ve KVKK’nın yürürlüğe girmesinden sonra ise bu suçlar ile korunan hukuki menfaatin kişisel verilerin korunması hakkı olduğu kabul edilmeye başlanmıştır. Bazı yazarlar korunan hukuki menfaatin doğrudan kişisel verilerin korunması hakkı olduğunu savunurken³³⁹ diğer bazı yazarlar ise suç ile özel yaşamın

³³⁶ TCK m.135/2: “*Kişisel verinin, kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması durumunda birinci fıkra uyarınca verilecek ceza yarı oranında artırılır.*”

³³⁷ TCK m.137/1: “*Yukarıdaki maddelerde tanımlanan suçların; a) Kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle, b) Belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle, İşlenmesi halinde, verilecek ceza yarı oranında artırılır.*”

³³⁸ Bu yöndeki görüş için bkz. **Özbek / Doğan / Bacaksız** (2022), s.597. **Ketizmen**, s.258. **Akdağ**, s.38-39. **Gültekin, Nil Melek** (2012) *Kişisel Verilerin Ceza Hukuku Yönünden Korunması* (Yüksek Lisans) Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü, s.124.

³³⁹ **Korkmaz**, s.381. **Şimşek, Sıla Türkan** (2020) *Kişisel Verilerin Kaydedilmesi Suçu* (Yüksek Lisans), Bahçeşehir Üniversitesi Sosyal Bilimler Enstitüsü, s.49.

gizliliği hakkının bir alt görünüm şekli olan kişisel verilerin korunması hakkının korunduğunu savunmaktadır³⁴⁰.

Bu görüşü³⁴¹ savunanların hareket noktası kişisel verilerin korunması hakkına Anayasa’da ayrı bir madde ve başlık altında değil, özel hayatın gizliliği hakkını düzenleyen 20nci maddede yer verilmiş olmasıdır. TCK’daki suç tiplerinin de özel hayata ve hayatın gizli alanına karşı suçlar bölümünde düzenlenmiş olması bu yorumun yapılmasına sebep olmaktadır. Gerçekten de hukuki düzenlemelerin yapılış şekli dikkate alındığında Türk hukukunda kişisel verilerin korunması hakkının özel hayatın gizliliği hakkının özel bir görünüm biçimi olarak kabul edildiği sonucuna ulaşmak gerekir. Ancak bu anlayış kişisel verilerin korunması hukuku öğretisinin güncel kabulleriyle örtüşmemektedir. Birinci bölümde gerekçelerini detaylı şekilde açıkladığımız üzere kişisel verilerin korunması hakkı müstakil bir temel insan hakkı olarak kabul edilmelidir. Bu kabul, hakkın özel hayatın gizliliği, insan onuru, bireysel özerklik gibi diğer temel haklarla yakın ilişki içerisinde olduğu gerçeğini değiştirmez. Diğer hak ve hürriyetlerle yakın ilişki içerisinde fakat müstakil bir varlığı olan kişisel verilerin korunması hakkı Anayasa’da da ayrı bir madde ve başlık altında düzenlenmelidir. TCK’daki suç tipleri de “*Kişisel Verilere Karşı Suçlar*” başlığı ile ayrı bir bölüm altında ele alınmalıdır.

Her ne kadar kanunun düzenleniş şeklinden hareketle korunan hukuki yararın özel hayatın gizliliği hakkının özel bir görünüm şekli olarak kişisel verilerin korunması hakkı olduğu söylenebilirse de kanaatimizce kişisel verilerin korunması hakkını özel hayatın gizliliği çatısı altında değil müstakil olarak ifade etmek daha doğrudur. Aslında kanuni tanımların açıklığı karşısında bu iki ifade ediş şeklinin pratikte farklı sonuçlar doğurmaması gerekir. Ancak suçun maddi konusu bahsinde de göreceğimiz üzere kişisel verileri kişinin özel hayat alanı içerisinde değerlendirme gayreti uygulamacıları zaman zaman yanlış yorumlara sevk etmektedir. Bu yanlış yorumlarla kişisel veri tanımı öğretiye ve mevzuata aykırı olarak daraltılmaya çalışılmaktadır.

Sonuç olarak katıldığımız görüş bu suçlar ile korunan hukuki menfaatin temel insan haklarından biri olan kişisel verilerin korunması hakkı olduğudur. Halihazırda öğretilerde de

³⁴⁰ **Hafizoğulları / Özen**, s.268. **Koca / Üzülmöz** (2020), s.556.

³⁴¹ Özel hayatın gizliliği hakkının özel bir görünüm şekli olan kişisel verilerin korunması hakkı görüşü

ağırlıklı görüş bu yöndedir³⁴². Kişisel verilerin korunması hakkının diğer haklar ile olan yakın ilişkisi sebebiyle bu suçlar ile diğer pek çok hakkın da yerine göre korunabildiği söylenebilir. İnsan onuru, bireyin kişiliğini özgürce geliştirme hakkı, özel hayat hakkı, ifade hürriyeti, din ve vicdan hürriyeti, sendikal faaliyetlerde bulunma özgürlüğü dolaylı olarak korunan haklardan bazılarıdır³⁴³.

2.2. Suçun Unsurları

Suçun unsurları maddi unsur, manevi unsur ve hukuka aykırılık unsuru olmak üzere üç başlıkta incelenecektir.

2.2.1. Maddi Unsurlar

Maddi unsurlar suçun maddi konusu, fail, mağdur ve fiil olmak üzere dört başlık altında incelenecektir.

2.2.1.1. Suçun Maddi Konusu

Suçun maddi konusu kanuni tanımında yer alan fiilin üzerinde icra edildiği kişi veya şeydir³⁴⁴. Bu suç tipi bakımından kaydetme fiilinin üzerinde icra edildiği şey kişisel verilerdir. Dolayısıyla suçun maddi konusunu kişisel veriler oluşturur³⁴⁵.

Kişisel veri kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgidir.³⁴⁶ Bu tanımdan yola çıkarak kişisel veri kavramının üç unsurun bir araya

³⁴² Korkmaz, s.381.

³⁴³ Kişisel verilerin korunması hakkının hukuki niteliğine ve diğer hak ve hürriyetlerle ilişkisine dair detaylı açıklamalar için birinci bölümde yer alan ilgili başlıklara bakınız.

³⁴⁴ Koca, Mahmut / Üzülmüş, İlhan (2022) Ceza Hukuku Genel Hükümler, 15. Baskı, Ankara, Seçkin, s.118.

³⁴⁵ Kişisel veri kavramının kapsamına dair detaylı değerlendirmelerimizi birinci bölümde yapmıştık. O sebeple kavramın kapsamı hakkında uzun tartışmalara burada yer vermeyeceğiz. Kavramın kapsamına ilişkin önemli noktaları kısaca hatırlatıp Ceza Hukuku öğretisinde ve Yargıtay kararlarında tartışılan hususları inceleyecek, bu konulara ilişkin görüşlerimizi belirteceğiz.

gelmesiyle oluřtuđu sylenebilir. Bunlar bir bilginin bulunması, bir kiřinin bulunması ve bilginin bu kiřiye iliřkin olmasıdır³⁴⁷.

Kiřisel veriden sz edebilmek iin kiřinin kimlięi belirli veya belirlenebilir olmalıdır. Kimlięi belirli bir gerek kiřiye iliřkin her trl bilgi kiřisel veridir. Kimlięi belirli olmayan bir gerek kiřiye iliřkin bilginin ise kiřisel veri olarak kabul edilebilmesi iin kiřinin kimlięinin belirlenebilir olması gerekir. *“Bařka verilerle eřleřtirilerek dahi hibir surette kimlięi belirli veya belirlenebilir bir gerek kiřiyle iliřkilendirilemeyecek”* veriler ise anonim verilerdir. Anonim veriler kiřisel veri olarak kabul edilemez. Aslında anonim veriler de bir gerek kiři hakkında bilgi sunmaktadır fakat bu kiřinin kim olduęu belirli deęildir ve belirlenmesi de mmkn deęildir. Kiři ile veri arasındaki baę sonsuza dek kopmuřtur. Dolayısıyla bu tr veriler artık kiřisel veri olarak kabul edilmemektedir.

Kiřisel veriden sz edebilmek iin gereken bir dięer řart kiřinin gerek bir kiři olmasıdır. Tzel kiřilere iliřkin veriler kiřisel veri olarak kabul edilmemektedir. ęretide tzel kiřilerin verilerinin kiřisel veri olarak kabul edilmesi gerektięini savunanlar³⁴⁸ bulunsa da bu artık ok cılız kalmıř bir grřtr. Hem Avrupa’da hem de lkemizde genel kabul tzel kiřilere ait verilerin kiřisel veri olamayacaęı ynndedir. KVKK’daki kiřisel veri tanımı, TCK m.135’in gerekesindeki ifade ve Yargıtayın yerleřik uygulaması bu yndedir.

Kiřisel verilere iliřkin su tiplerinin en ok tartıřmaya konu olan unsurlarından biri suun maddi konusudur. ęretideki bir grře gre TCK’nın 135 vd. maddelerinde yer alan kiřisel verilere iliřkin suların kaynaęı Fransız Ceza Kanunu’ndaki dzenlemelerdir³⁴⁹. Fransız Ceza Kanunu’nda bu sular eksik norm olarak dzenlenmiřtir ve bu suların unsurlarının oluřup oluřmadıęının deęerlendirilmesi bakımından Fransız Veri Koruma Kanunu’na bařvurulmaktadır³⁵⁰. Fransa’da bir veri koruma kanununun

³⁴⁶ KVKK m.3/1-d hkmnde ve TCK m.135’in gerekesinde bu tanım benimsenmiřtir.

³⁴⁷ Kiřisel veri kavramının kapsamı ve unsurları hakkında detaylı deęerlendirmeler iin birinci blmn ilgili bařlıklarına bakabilirsiniz.

³⁴⁸ Bkz. **Bk, Alaattin** (2018) Biliřim Alanında Kiřisel Verilerin Korunması, 1. Baskı, Ankara, Sekin, s.204.

³⁴⁹ **Ketizmen, Muammer** (2006) Trk Ceza Hukukunda Biliřim Suları (Doktora), Ankara niversitesi Sosyal Bilimler Enstits, s.271-272

³⁵⁰ Yargıtay Ceza Genel Kurulu da KVKK’nın yrrlęe girmesinden nceki bir kararında TCK’daki hkmlerin eksik norm olduęunu ifade etmiřtir. Bkz. *“Bugne kadar kiřisel verilerin neler olduęuna dair kanunun ıkarılmaması nedeniyle TCK’ndaki 135 ve 136. maddelerindeki hukuka aykırılıęın hangi hallerde*

bulunması dolayısıyla bu düzenleme onlar için sorun teşkil etmemektedir. Fakat Türkiye’de mevzubahis ceza normları veri koruma kanunundan önce yürürlüğe girdiği için problem oluşmuştur³⁵¹. Öğretide bazı yazarlar tarafından TCK’da yer alan bu suç tiplerinin içeriğindeki kavramların belirsizlik taşıdıkları, dolayısıyla kanunilik ilkesine aykırılık teşkil ettikleri, veri koruma kanununun çıkarılmasına kadar bu hükümlerin yürürlüğünün ertelenmesi gerektiği savunulmuştur³⁵².

Bir diğer görüşe göre³⁵³ kişisel veri kavramı ve bu konuya ilişkin diğer kavramlar öğretide ve uluslararası metinlerde açık şekilde yer almaktadır. Belirlilik ve kanuniliğin gerçekleşmesi için kavramların kanunla tanımlanması şart değildir. Kavramların yorumlanmasının uygulamacılara bırakılmasında bir sakınca yoktur. Anayasa Mahkemesi de somut norm denetimi yaptığı bir davada benzer gerekçelerle TCK 136’nın kanunilik ilkesine aykırı olmadığına hükmetmiştir³⁵⁴.

Bu suçun ihdas edildiği 2005 yılından bu yana tartışılan hususlardan biri ise her türlü bilginin kişisel veri olarak kabul edilip edilmeyeceğidir. Öğretideki genel kabul ve TCK’nın gerekçesi kişisel verinin gerçek kişi hakkındaki her türlü bilgi olduğuna yönelik ise de öğretide bazı yazarlar her türlü bilginin kişisel veri olarak kabul edilmesine karşı çıkmıştır³⁵⁵. Bu görüşe göre suç tipi ile korunmak istenen hukuki değer kişinin özel yaşam

oluşturduğuna ilişkin başvurulabilecek kapsayıcı bir kaynak ya da norm olmaması nedeniyle bu iki madde eksik norm sayılırlar” YCGK, E. 2012/1510, K. 2014/331, K.T 17.06.2014.

³⁵¹ **Ketizmen**, s.271-272.

³⁵² **Yaşar, Osman / Gökcan, Hasan Tahsin / Artuç, Mustafa** (2010) Yorumlu Uygulamalı Türk Ceza Kanunu, 1. Baskı, Ankara, Adalet Yayınevi, Cilt 3, s.4116. Bu suç tiplerinin KVKK’nın kabulünden önce kanunilik ilkesine aykırı olduğu görüşü için ayrıca bkz. **Şen, Ersan** (2006) Yeni Türk Ceza Kanunu Yorumu, İstanbul, Vedat Kitapçılık, Cilt:1, s.601.

³⁵³ **Özbek**, s.948.

³⁵⁴ “Kuralda yer alan “kişisel veri” kavramı teknolojik gelişmelere bağlı olarak çok farklı şekillerde ortaya çıkabileceğinden bu kapsama giren tüm verilerin kanun koyucu tarafından önceden öngörülebilmesi ve tek tek sayılabilmesi mümkün değildir. Bununla birlikte gerek ulusal ve uluslararası mevzuat gerekse yargı içtihatları çerçevesinde “kişisel veri” kavramının, belirli veya kimliği belirlenebilir olmak şartıyla, bir kişiye ilişkin bütün bilgileri ifade ettiği kabul edilmektedir. “Kişisel veri” kavramının bu çerçevede doktrin, uygulama ve yargı kararlarında belirlenerek anlam ve içeriğinin gelişip değişeceğinde kuşku yoktur. Dolayısıyla başvuru kararında her ne kadar ceza mevzuatında “kişisel veri” ile ilgili bir tanım ve sınırlandırmanın yapılmadığı, bu nedenle itiraz konusu kuralın belirsiz olduğu ileri sürülmüş ise de ulusal ve uluslararası mevzuat ile yargı içtihatları dikkate alındığında kuralın belirsiz olduğundan söz edilemeyeceği açıktır. Ayrıca itiraz söz konusu kuralla “kişisel verileri hukuka aykırı olarak bir başkasına verme, yayma veya ele geçirme” eylemi suç olarak kabul edilmekte ve bu eylem nedeniyle verilecek ceza kuralda açıkça belirlendiğinden kuralla hangi somut eylem ve bu olguya hangi hukuksal yaptırımın bağlandığı açıkça ortaya konulmaktadır. Dolayısıyla itiraz konusu kuralda suçta ve cezada kanunilik ilkesi ile özel hayatın gizliliği ilkesine aykırılık bulunmamaktadır. Açıklanan nedenlerle kural, Anayasanın 20. Ve 38. maddelerine aykırı değildir.” AYM E. 2015/32, K. 2015/102, K.T 12.11.2015.

³⁵⁵ **Aydın, Sedat Erdem** (2015) AİHM İçtihatları Bağlamında Kişisel Verilerin Kaydedilmesi Suçu, 1. Baskı, İstanbul, On İki Levha Yayınları, s.130.

hakkıdır. Dolayısıyla kişinin gizli tutulması noktasında bir beklentisinin olmadığı, kendisi tarafından alenileştirilmiş verileri veya herkes tarafından bilinebilecek nitelikteki bilgileri bu suçun maddi unsuru olarak kabul edilmemelidir³⁵⁶. Kişisel veri ilgili kişinin sır alanına ilişkin bir bilgi olmalıdır³⁵⁷. Yargıtay ceza dairelerinin eski bazı kararlarında da kişisel veri kavramının kapsamına ilişkin benzer görüşlere yer verilmiş, her türlü bilginin kişisel veri kabul edilmesi halinde ceza sorumluluğunun amaçlanandan çok fazla genişleyeceği, hemen her eylemin suç oluşturabileceği ifade edilmiştir³⁵⁸. Ceza Genel Kurulu ise daire kararlarının aksine kimliği belirli veya belirlenebilir gerçek bir kişiye ilişkin her türlü bilginin kişisel veri kabul edilmesi gerektiğini, bir verinin kişisel veri olabilmesi için gizli olmasının şart olmadığını, herkes tarafından bilinebilen bilgilerin de kişisel veri olarak kabul edilmesi gerektiğini ve hukuka aykırı fiillere karşı korunması gerektiğini ifade etmiştir³⁵⁹. Yargıtay dairelerinin ve Ceza Genel Kurulu'nun güncel görüşü her türlü bilginin kişisel veri olarak kabul edilmesi yönündedir.

Herkes tarafından bilinebilecek nitelikteki verilerin veya kişinin kendisi tarafından alenileştirilmiş verilerin kişisel veri olarak kabul edilmesi maddenin uygulama alanını amaçlanandan fazla genişletmeyecektir. Bir şeyin suçun konusunu oluşturabilecek nitelikte olması mutlak anlamda cezalandırılabilir bir durumun varlığı anlamına gelmez. Verilerin kişinin kendisi tarafından alenileştirilmiş olması KVKK'da bir hukuka uygunluk sebebi olarak kabul edilmiştir. Kişinin kendisi tarafından alenileştirilmiş bir verinin alenileştirilme amacına uygun ve kişinin makul beklentilerini göz ardı etmeyecek şekilde kaydedilmesi durumunda KVKK'da yer alan hukuka uygunluk sebebi dolayısıyla fiil hukuka uygun kabul edilecektir³⁶⁰. Herkes tarafından bilinebilir nitelikteki bir verinin kaydedilmesi durumunda ise yerine göre hukuka aykırılığı veya kusurluluğu kaldıran hata hallerinden

³⁵⁶ **Özbek / Doğan / Bacaksız** (2022), s.597.

³⁵⁷ **Aydın**, s.130.

³⁵⁸ "... suçun maddi konusunu oluşturan "kişisel veri" kavramından, kişinin, yetkisiz üçüncü kişilerin bilgisine sunmadığı, istediğinde başka kişilere açıklayarak ancak sınırlı bir çevre ile paylaştığı bilgiler anlaşılmalıdır." Yargıtay 12. Ceza Dairesi, 2012/20543 E., 2012/20422 K., 2.10.2012 K.T. Benzer yöndeki bir diğer kararda "ancak, herkes tarafından bilinen ve/veya kolaylıkla ulaşılması ve bilinmesi mümkün olan kişisel bilgiler, yasal anlamda "kişisel veri" olarak değerlendirilemez, aksinin kabulü; anılan maddenin uygulama alanının amaçlanandan fazla genişletilerek, uygulamada belirsizlik ve hemen her eylemin suç oluşturması gibi olumsuz sonuçlar doğurur, bu nedenle, bir kişisel bilginin, açıklanan anlamda "kişisel veri" kabul edilip edilmeyeceğine karar verilirken, somut olayın özellikleri dikkate alınarak titizlikle değerlendirme yapılması, sanığın eylemiyle hukuka aykırı hareket ettiğini bildiği ya da bilebilecek durumda olduğunun da tespit edilmesi gerekir." İfadelerine yer verilmiştir. Bkz. Yargıtay 12. Ceza Dairesi, 2013/9669 E., 2014/3760 K., 17.02.2014 K.T.

³⁵⁹ Yargıtay Ceza Genel Kurulu, E. 2012/1510, K. 2014/331, K.T. 17.06.2014.

³⁶⁰ KVKK'da yer alan hukuka uygunluk sebepleri yalnızca KVKK kapsamında giren durumlarda uygulanabileceğini hatırlatmak isteriz. Konuya ilişkin detaylar hukuka aykırılık unsuru başlığında ele alınacaktır.

bahsedilebilecektir. Dolayısıyla kişisel veri kavramının sınırlarını daraltmayı mecbur kılacak bir durum mevcut değildir.

Kişisel veri kavramının sınırlarının daraltılarak yorumlanması kimi zaman bazı suçların cezasız kalmasına ve veri sahiplerinin mağdur olmasına yol açabilir. Örneğin kişinin herkese açık sosyal medya profilinde paylaştığı bir gönderiyi alıp paylaşılma amacına aykırı şekilde kullanan bir kişi veri sahibinin mağduriyetine sebep olabilir. Başkasının fotoğrafıyla sahte hesap açılması durumunda kişisel verinin hukuka aykırı şekilde kullanıldığında bir şüphe yoktur. Yargıtay önüne gelen benzer olaylarda çelişkili kararlar vermiştir. Örneğin bir gazetecinin köşe yazılarıyla birlikte yayınlanan fotoğrafını alıp bir flört sitesinde profil oluşturan sanığın eylemlerinin kişisel verileri verme, yayma veya ele geçirme suçunu oluşturduğuna hükmedilmiştir³⁶¹. Başka bir olayda ilgi duyduğu kişiyle konuşmak için sahte Facebook profili açan sanık ilgili kişiyle bir süre konuşmuştur. Sanığın hesabının sahte olduğunu anlayan kişi bu hesabı arkadaş listesinden çıkarmıştır. Bunun üzerine sanık ilgili kişinin Facebook profilinden aldığı fotoğrafları kendi sahte profilinde yayınlamıştır. Yargıtay fotoğrafların herkese açık oluşunu ve özel hayata ilişkin olmayışını gerekçe göstererek fiilin suç oluşturmadığına hükmetmiştir³⁶². Gazeteci olayında da gazete köşesinde yayınlanan fotoğraf herkese açıktır ve özel hayata ilişkin değildir. Fakat yargıtay o olayda kişisel verileri yayma suçunun oluştuğuna hükmetmiştir. Yargıtay'ın KVKK'nın kabulünden önceki kararlarında somut olayda eylemin oluşturduğu mağduriyet düzeyine göre kişisel veri kavramının kapsamını esnetme yoluna gittiği gözlemlenmektedir. Kanaatimizce bu uygulama tarzı hatalıdır. Kişisel veri kavramı geniş şekilde yorumlanmalı, somut olaydaki fiilin cezalandırılabilir olup olmadığı ise hukuka aykırılık ve kusurluluk bağlamında değerlendirilmelidir. Yargıtay Ceza Genel Kurulu'nun 2014 yılında kişisel veri kavramının geniş yorumlanması yönünde verdiği karardan³⁶³ ve 2016 yılında KVKK'nın kabul edilmesinden sonra zamanla 12. Ceza Dairesi'nin de bu uygulamadan vazgeçtiği ve kişisel veri kavramını geniş yorumlamaya başladığı gözlemlenmektedir³⁶⁴.

³⁶¹ Yargıtay 12. Ceza Dairesi, 2011/20072 E., 2012/12126 K., 15.05.2012 K.T.

³⁶² Yargıtay 12. Ceza Dairesi, 2015/4349 E., 2016/5349 K.

³⁶³ Yargıtay Ceza Genel Kurulu, 2012/1510 E., 2014/331 K., 17.06.2014 K.T.

³⁶⁴ Aynı yöndeki tespit için bkz. **İçel, Kayıhan** (2020) 'Ceza Hukuku Açısından Kişisel Verilerin Korunmasında "Kişisel Veri" ve "Hukuka Aykırılık" Kavramları' İstanbul Barosu Dergisi, C:94, S:2, (s.15-23), s.18. Örnek karar için bkz. 12. Ceza Dairesi, 2018/8466 E., 2019/9054 K., 18.09.2019 K.T

Veri kelimesi her ne kadar elektronik ortamda tutulan bir bilgiyi çağrışırsa da suçun konusunun varlığı bakımından kişisel verinin fiziki ortamda veya elektronik ortamda bulunması arasında bir fark yoktur³⁶⁵.

Ölmüş bir kişiye ait veriler ise kişisel veri olarak kabul edilmediği için suçun maddi konusunu oluşturamayacaktır. Kanaatimizce KVKK'ya eklenecek bir hüküm ile ölümlere ait verilerin de kişisel veri olarak kabul edilmesi, kişilerin öldükten sonra da ihlallere karşı korunması gerekmektedir. Çünkü öldükten sonra verilerinin korunmayacağını düşünen bir kişi sağlığında kişiliğini özgürce geliştiremez. Ayrıca insan onurunun ölümle sona ermeyen bir değer olduğunu kabul etmek ve ölen kişinin de haklarını korumak gerekmektedir³⁶⁶. Esasen ölümlerin verilerinin kişisel veri olarak kabul edilmesini engelleyen ya da yasaklayan herhangi bir norm bulunmamaktadır. Ancak kişisel verilerin korunması hukukunda yaygın kabul ölümlere ait verilerin kişisel veri olarak kabul edilemeyeceği yönündedir³⁶⁷. Öğretideki genel kabulün aksine bir yorum geliştirmek suretiyle bu suçun maddi konusunu ölümlere ait verilerin de oluşturabileceğini kabul etmek ceza sorumluluğunu genişletici bir nitelik taşıyacağı için doğru olmayacaktır. Bu sebeple eksikliğin genişletici yorumda bulunmak suretiyle değil KVKK'ya ölmüş kişilerin verilerinin kişisel veri niteliğini koruyacağına dair bir hüküm eklemek suretiyle giderilmesinin yerinde olacağı kanaatindeyiz.

2.2.1.2. Fail

Suç tanımında fail için “*kişisel verileri kaydeden kimse*” ifadesi kullanılmıştır. “*Kimse*” ifadesinden anlaşılabileceği üzere suçun temel şeklinde fail için herhangi bir özellik aranmamıştır. Herkes bu suçun faili olabilir. Ancak m.137’de suçun “*a) Kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle, b) Belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle*” işlenmesi durumları nitelikli hâl olarak kabul edilmiştir³⁶⁸. Suçun temel şeklinin herkes tarafından, nitelikli halinin ise yalnızca belirli özellikleri taşıyan kişiler tarafından işlenebildiği suçlar görünüşte özgü suç

³⁶⁵ Maden, s.46

³⁶⁶ Bu konuda detaylı açıklamalar için birinci bölümün 1.2.2. numaralı başlığına bakabilirsiniz.

³⁶⁷ Bkz. birinci bölüm 1.2.2. numaralı başlık.

³⁶⁸ TCK m.137.

olarak ifade edilmektedir³⁶⁹. Kişisel verilerin kaydedilmesi suçu da bu kapsamda görünüşte özgü suç olarak nitelendirilebilir³⁷⁰.

Türk Ceza Kanunu'nun benimsediği anlayışa uygun olarak diğer suçlarda olduğu gibi bu suç bakımından da yalnızca gerçek kişiler fail olarak kabul edilebilir³⁷¹. Tüzel kişiler suçun faili olamaz³⁷². Ancak suçun tüzel kişinin temsilcileri tarafından tüzel kişi menfaatine işlendiği durumlarda tüzel kişilik hakkında bunlara özgü güvenlik tedbirlerine hükmedilir³⁷³. Tüzel kişilik yararına bu suçları işleyen gerçek kişiler ise suçun faili olarak cezalandırılabilir.

³⁶⁹ Koca / Üzülmaz (2022), s.115.

³⁷⁰ Maden, s.68. Korkmaz, s.337. Kangal, s.61.

³⁷¹ TCK m.20/2'de "Tüzel kişiler hakkında ceza yaptırımı uygulanamaz. Ancak, suç dolayısıyla kanunda öngörülen güvenlik tedbiri niteliğindeki yaptırımlar saklıdır." düzenlemesi bulunmaktadır. Bu maddenin gerekçesinde de tüzel kişilerin fail olarak kabul edilemeyeceği açık ve net bir şekilde ifade edilmiştir. Gerekçe şu şekildedir: "Özel hukuk tüzel kişilerinin suç faili sayılıp sayılmaması ile işlenen bir suçtan dolayı bunlar hakkında bir yaptırıma hükmedilmesi sorununun birbirinden ayırmak gerekir. Suç ve ceza politikası gereği olarak ancak gerçek kişiler suç faili olabilir ve sadece gerçek kişiler hakkında ceza yaptırımına hükmedilebilir. Bu anlaşılış, Anayasamızda da güvence altına alınan ceza sorumluluğunun şahsiliği kuralının bir gereğidir. Ancak, işlenen suç dolayısıyla özel hukuk tüzel kişileri hakkında güvenlik tedbiri niteliğinde yaptırımlara hükmedilebilecektir. Para cezasının uygulamasındaki kolaylık, tüzel kişiler hakkında da ceza yaptırımına hükmedilebileceği düşüncesine haklılık kazandırmaz. Tüzel kişiler için ancak idari yaptırım niteliğinde "para cezası" öngörülebilir. Çünkü, idari yaptırımlarla, ceza yaptırımları arasında neden, amaç ve sonuçları bakımından farklılıklar bulunmaktadır. Örneğin, şirket niteliğindeki bir tüzel kişinin faaliyeti ile ilgili olarak doğan vergi borcunun zamanında ve tam olarak ödenmemesi dolayısıyla, tüzel kişi hakkında da "para cezası" verilebilmektedir. Ancak, bu yaptırımın asıl amacı, verginin zamanında ve eksiksiz olarak ödenmemesi dolayısıyla kamu maliyesinin uğradığı zararın giderilmesi ve vergi düzeninin etkinliğinin sağlanmasıdır. Bu tür yaptırımların bir ceza hukuku yaptırımı olmadığı açıktır. Vergi borcunun gerçeğe uygun bir şekilde doğmasının önüne geçebilmek amacıyla sahte belge düzenlenmiş olması durumunda ayrıca bu sahteciliği gerçekleştiren gerçek kişiler hakkında ceza yaptırımına hükmedilebilecektir. Bu durumda bile tüzel kişi hakkında verilen "para cezası", bir idari yaptırım olma özelliğini korur. Yapılan bu yeni düzenlemeyle, tüzel kişiler hakkında da özellikle "para cezası" bağlamında ceza yaptırımına hükmedilebileceği yönündeki hukukî temelden yoksun anlayışın önüne geçilmek amaçlanmıştır."

³⁷² Soyaslan Ceza Hukuku Genel Hükümler kitabında teorik olarak tüzel kişilerin de suç faili olabileceklerini savunmaktadır. Fakat özel hükümler kitabında bu suç tipini incelerken yalnızca gerçek kişilerin fail olabileceklerini ifade etmiştir. Bunun sebebi TCK'nın tüzel kişileri fail olarak kabul etmeyen net tutumudur. Bkz. Soyaslan, Doğan (2022) Ceza Hukuku Genel Hükümler, 10. Baskı, Ankara, Yetkin Yayınları, s.232. Soyaslan (2020), s.361.

³⁷³ TCK m.60'ta tüzel kişilere uygulanacak güvenlik tedbirlerine hangi şartlar altında başvurulacağı ve bu güvenlik tedbirlerinin neler olduğu düzenlenmiştir. Yine bu maddenin dördüncü fıkrasında bu madde hükümlerinin uygulanabilmesi kanunda bunun açıkça belirtilmesi şartına bağlanmıştır. TCK m.140'ta ise m.132 ile m.140 arasındaki hükümler kastedilerek "Yukarıdaki maddelerde tanımlanan suçların işlenmesi dolayısıyla tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükümler" ifadesine yer verilmiştir. Dolayısıyla TCK 135, 136 ve 138'de düzenlenen suç tiplerinin tüzel kişilerce işlenmesi durumunda TCK m.60 hükümlerine başvurulacak ve bunlara özgü güvenlik tedbirleri uygulanacaktır.

2.2.1.3. Mağdur

Mağdur en basit ifadesiyle kendisine karşı suç işlenmiş kişiyi ifade eder. Mağdur hukuki bir kavramdır ve suçun maddi unsurlarından biri olması sebebiyle mağdurun doğru tespit edilmesi son derece önemlidir. Mağduru daha doğru tespit edebilmek için öğretide sözlük tanımlarının ötesinde bazı hukuki tanımlar yapılmıştır. En çok kabul gören tanımlardan birine göre mağdur kavramı “suçun konusunun ait olduğu kişiyi” ifade eder³⁷⁴. Öğretide sıkça kullanılan diğer bir tanıma göre ise mağdur “suçla korunan hukuki değerın sahibini” ifade eder³⁷⁵. Biz de bu iki muteber tanım üzerinden değerlendirmelerimizi yapacağız.

Suç ile korunan hukuki değerin kişisel verilerin korunması hakkı olduğunu, suçun maddi konusunun ise kişisel veriler olduğunu ifade etmiştik. Dolayısıyla bu suçun mağduru kişisel verileri kaydedilerek kişisel verilerin korunması hakkı ihlal edilen kişidir. Daha açık bir ifadeyle suçun mağduru kişisel verisi kaydedilen herhangi bir kimsedir.

Suçun maddi konusunu oluşturan kişisel veri kavramından yola çıkarak mağdur hakkında bazı tespitlerde bulunmak mümkündür. Öğretide genel kabule göre sadece gerçek kişilerin verileri kişisel veri olarak kabul edilmektedir. Kişisel veri kavramının tanımlandığı KVKK m.3/1-d hükmünde ve TCK m.135’in gerekçesinde tüzel kişilere ait veriler kişisel veri olarak kabul edilmemiştir. Dolayısıyla tüzel kişilerin bu suçun mağduru olabilmesi mümkün değildir³⁷⁶. Maddenin ikinci fıkrasında kişisel veriler sıralanırken kişinin “cinsel yaşamına, sağlığına, ırkı kökenlerine, ahlaki eğilimlerine” ilişkin verilerden bahsedilmesi de kanunun gerçek kişileri korumayı amaçladığına delil olarak gösterilmiştir³⁷⁷. Ancak bu delillendirme şeklinin doğru olmadığı kanaatindeyiz. Bahsedilen türlerin dışında da veri türleri vardır. Örneğin adres bilgisi bir kişisel veri olarak kabul edilebilir. Tüzel kişilerin de pekâlâ adresi bulunmaktadır. KVKK’daki

³⁷⁴ **Özgenç, İzzet** (2022) Türk Ceza Hukuku Genel Hükümler, 15. Baskı, Ankara, Seçkin, s.223. **Koca / Üzülmaz** (2022), s.116,

³⁷⁵ **Soyaslan** (2022), s.233. **Özbek, Veli Özer / Doğan, Koray / Bacaksız, Pınar**, Türk Ceza Hukuku Genel Hükümler, 13. Baskı, Ankara, Seçkin, s.213.

³⁷⁶ Aynı yönde görüşler için bkz. **Koca / Üzülmaz** (2020), s.557. **Gültekin**, s.129. **Aydın**, s.131. **Korkmaz**, s.338. **Yıldız**, s.98. **Börekçi, Eşref Barış** (2020) Kişisel Verileri Verme, Yayma veya Ele Geçirme Suçu, 1. Baskı, İstanbul, On İki Levha Yayınları, s.73. **Şimşek**, s.66. **Maden**, s.71-73. **Kangal**, s.62. **Dülger** (2020), s.690. Esasen öğretide neredeyse bütün yazarlar tüzel kişilerin bu suçun mağduru olamayacağını kabul etmektedir. Aksi görüş ise oldukça azınlıktadır.

³⁷⁷ **Gültekin**, s.129.

tanımdan ve madde gerekçesinden hareketle suçun mağdurunun yalnızca gerçek kişiler olabileceğini söylemek yeterlidir. Tüzel kişiler suçun mağduru olamasalar da suçtan zarar gören olabilirler³⁷⁸.

Öğretide tüzel kişilerin de suçun mağduru olabileceği yönünde görüş beyan edenler olmuştur³⁷⁹. KVKK'nın ilk tasarılarında tüzel kişilerin de kişisel veri öznesi olarak kabul edilmesi, kişisel verilerin korunması hakkına ilişkin Anayasa'da yer alan hükümde tüzel kişiler ile gerçek kişiler arasında bir ayrım yapılmamış olması, Anayasa Mahkemesi'nin bazı kararlarında kişisel verilerin korunması hakkına tüzel kişilerin de sahip olduğunu ifade etmesi gibi hususlar bu görüşe delil olarak sunulabilir. Bu görüşteki bir yazar TCK'da suç tipi düzenlenirken mağdur bakımından bir özellik zikredilmemiş olması sebebiyle tüzel kişilerin de mağdur olabileceğini, gerekçedeki yorumun kanun ile çeliştiğini ve amacını aştığını savunmuştur³⁸⁰. Aynı yazara göre KVKK'nın tüzel kişileri kapsam dışında bırakan düzenlemesi de yanlıştır ve değiştirilmelidir. Ancak KVKK'da yer alan tanım, TCK m.135'in gerekçesi, öğretideki baskın görüş ve Yargıtay'ın bu yöndeki uygulamaları³⁸¹ dikkate alındığında tüzel kişilerin bu suçun mağduru olamayacağını kabul etmek kanaatimizce daha isabetlidir.

Gerçek kişinin suçun mağduru olabilmesi için sağ olması gerekir. Ölümle birlikte kişilik sona erdiği için ölümlerin suçun mağduru olamayacağı kabul edilmektedir³⁸². Ölümlerin kişisel verilerinin işlendiği durumlarda koşullarının gerçekleşmesi halinde TCK m.130/1'de düzenlenen “*Kişinin Hatırasına Hakaret*” suçu veya TCK m.258'de düzenlenen “*Göreve İlişkin Sırrın Açıklanması*” suçu oluşabilir³⁸³.

³⁷⁸ **Kangal**, s.62. **Maden**, s.73. **Dülger** (2020), s.690. Öğretide genel kabul tüzel kişilerin suçtan zarar gören olabileceği şeklindedir. Fakat tüzel kişilerin bu suç için mağdur olamayacağı gibi suçtan zarar gören de olamayacağı şeklinde bir görüş de bulunmaktadır. Bkz. **Koca / Üzülmaz** (2020), s.557.

³⁷⁹ **Yılmaz, Sacit** (2016) Türk Ceza Hukuku Sisteminde Siber Suçlar, 1. Baskı, Ankara, Adalet Yayınları, s.257. **Soyaslan** (2022), s.361.

³⁸⁰ **Bük**, s.204.

³⁸¹ Yargıtay bir kararında özel hukuk tüzel kişisi olan bir şirketin mağdur olamayacağını ifade etmiştir. “*Kişisel veri kavramından gerçek kişiye ait her türlü bilginin anlaşılması gerektiği nazara alındığında, sanıklara atılı verileri hukuka aykırı olarak verme veya ele geçirme suçunun koruduğu hukuki yarar ve iddianamenin kapsamına göre davaya katılmasına karar verilen şikâyetçi TTNET Anonim Şirketinin sanıklara yüklenen suçun mağduru olmadığı*” 12. Ceza Dairesi 2019/12443 E., 2019/11106 K. Ayrıca Yargıtay kararlarının pek çoğunda kişisel verilerin KVKK'daki tanıma uygun olarak “*kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi*” şeklinde tanımlandığı görülmektedir.

³⁸² **Korkmaz**, s.399.

³⁸³ **Kangal**, s.62.

2.2.1.4. Fiil

Kanunda suçun fiil unsuru kişisel verileri kaydetmek olarak tanımlanmıştır. Kaydetmek bir bilgiyi istenildiğinde yeniden ulaşılabilir ve kullanılabilir bir formda saklamak demektir. Suç tanımında kaydetmek fiiliyle ilgili sınırlayıcı bir kriter³⁸⁴ getirilmediği için her türlü kaydetme fiili suçun fiil unsurunu oluşturabilir. Bu sebeple kişisel verilerin kaydedilmesi suçu serbest hareketli bir suçtur³⁸⁵.

Kaydetme eylemi pek çok farklı şekilde gerçekleştirilebilir. Önemli olan bu eylem sonunda verinin tekrar ulaşılabilir ve kullanılabilir bir biçimde muhafaza edilecek hale getirilmiş olmasıdır. Bilgiyi bir kâğıda yazmak, DVD, USB, bilgisayar hafızası, telefon hafızası gibi herhangi bir dijital ortamda depolamak, video görüntüsünü veya sesi manyetik bant üzerine geçirmek gibi hareketler kaydetme fiili olarak kabul edilebilir.

Verilerin dijital ortamda kaydedilmesi ile fiziksel ortamda kaydedilmesi arasında herhangi bir fark yoktur³⁸⁶. Her iki durumda da fiil unsuru gerçekleşmiştir. Kişisel verilere salt duyu organları vasıtasıyla vakıf olunması ve bunların ezberlenerek akılda tutulması ise kaydetme anlamına gelmez. Kaydetme fiilinin bir araç kullanarak yapılması gerekir³⁸⁷.

Kişisel verilerin kaydedilmesi suçu sırf hareket suçudur. Kaydetme hareketinin gerçekleşmesi ile suç tamamlanır. Ayrıca bir neticenin gerçekleşmesine gerek yoktur³⁸⁸. Öğretide bazı yazarlar ise bu suçun neticeli suç olduğunu savunmaktadır³⁸⁹.

³⁸⁴ Örneğin madde metninde “*kişisel verilerin veri kayıt sistemine kaydedilmesi*” ifadesi yer almış olsaydı veri kayıt sistemi dışında herhangi bir yere yapılan kaydetme fiilinin bu kapsamda değerlendirilemeyeceğini kabul etmek gerekirdi.

³⁸⁵ **Maden**, s.51. **Dülger** (2020), s.697. Suçun bağlı hareketli bir suç olduğu yönündeki karşı görüş için bkz. **Özbek / Doğan / Bacaksız**, Ceza Özel, s.598.

³⁸⁶ Gerekçede bu durum şu şekilde ifade edilmiştir: “*Söz konusu suç tanımında kişisel verilerin bilgisayar ortamında veya kâğıt üzerinde kayda alınması arasında bir ayırım gözetilmemiştir.*” **Özbek**, s.946.

³⁸⁷ **Kangal**, s.66. **Köse Aysun, Melike** (2021), *Kişisel Verilerin Kaydedilmesi Suçu*, 2. Baskı, Ankara, Seçkin, s.120. **Özbek / Doğan / Bacaksız**, Özel Hükümler, s.598.

³⁸⁸ **Koca / Üzülmaz** (2020), s.561. **Maden**, s.53. **Hafizoğulları / Özen**, s.269.

³⁸⁹ Kişisel verilerin kaydedilmesi suçunun neticeli suç olduğunu savunan yazarlardan Dülger kayıt etme hareketinin tıpkı adam öldürme gibi neticeyi de içinde barındırdığını, hareket ile neticenin genellikle eş zamanlı olarak gerçekleşiyor oluşunun suç tipinde bir netice aranmadığı şeklinde yorumlanmaması gerektiğini ifade etmektedir. Bkz. **Dülger** (2020), s.698. **Özbek / Doğan / Bacaksız** ise suçun neticesi harekete bitişik bir suç olduğunu ifade etmektedir. Bkz. **Özbek / Doğan / Bacaksız**, Ceza Özel, s.599

Kişisel verilerin kaydedilmesi suçunun gerçekleşmesi için verilerin veya veri sahibinin bir zarara uğraması şartı aranmamaktadır. Dolayısıyla bu suç bir tehlike suçudur. Tehlike suçları da kendi içerisinde somut tehlike suçu ve soyut tehlike suçu şeklinde ikiye ayrılmaktadır. Suçun cezalandırılabilmesi için somut bir tehlikenin oluşması şartının aranmadığı durumlarda soyut tehlike suçundan söz edilir. Kişisel verilerin kaydedilmesi suçunun oluşması için de tipe uygun ve hukuka aykırı hareket yeterlidir. Suç konusu bakımından somut bir tehlikenin oluşması gerekmez. Bu sebeple kişisel verilerin kaydedilmesi suçu bir soyut tehlike suçudur³⁹⁰.

Bu suçun meydana gelmesi için verilerin ilk defa kaydediliyor olması gerekmez. Daha önce hukuka uygun olarak kaydedilmiş verilerin hukuka aykırı olarak bir başka yere daha kaydedilmesi suretiyle de bu fiil gerçekleştirilebilir³⁹¹. Örneğin personel işlerinde görevli bir memurun personellerin özlük bilgilerini içeren dosyaları hukuka aykırı olarak kendi USB belleğine kaydetmesi, kaydetmek amacıyla kendisine mail olarak göndermesi suç oluşturur³⁹². Bu personelin bilgisi, izni ve onayı doğrultusunda üçüncü bir kişinin verileri hukuka aykırı olarak kendi USB belleğine kaydetmesi durumunda ise personel açısından kişisel verileri hukuka aykırı olarak verme fiili, üçüncü kişi açısından verileri hukuka aykırı olarak ele geçirme fiili vardır. Dolayısıyla bu durumda kişisel verileri kaydetme suçu (TCK m.135) değil verileri verme, yayma veya ele geçirme suçu (TCK m.136) oluşacaktır.

Hukuka aykırı olarak kaydedilmiş verilerin tekrar kaydedilmesi, başka bir depolama cihazına veya dosyaya aktarılması gibi durumlar ise iki farklı şekillerde gerçekleşebilir. Kişisel verileri hukuka aykırı olarak bilgisayarına kaydetmiş bir kişinin aynı verileri yedeklemek maksadıyla USB belleğe aktarması, Google Drive, I Cloud, Yandex Disk gibi online yedekleme hizmeti veren sitelerdeki hesabında yedeklemesi gibi kaydetme fiillerinin her biri için artık yeni bir suç oluşmaz. Çünkü bu fiiller aynı veriler üzerinde gerçekleşmektedir³⁹³. Fakat fail farklı bir zamanda aynı kişinin farklı bir verisini

³⁹⁰ **Koca / Üzülmaz** (2020), s.561. **Özbek / Doğan / Bacaksız**, Ceza Özel, s.599. **Dülger** (2020), s.699. **Maden**, s.54. **Korkmaz**, s.395.

³⁹¹ **Koca / Üzülmaz** (2020), s.561.

³⁹² Burada ele geçirme suçunun oluştuğu da söylenebilir. Fakat biz kaydetme suçunun oluştuğu kanaatindeyiz. Aslen bu iki kavram birbirine çok yakındır ve kanun bunların ayırt edilebilmesi için bir kriter getirmemiştir. Bu iki fiil arasındaki ayrım ileride kişisel verileri ele geçirme suçunun fiil unsuru başlığı altında ele alınacaktır.

³⁹³ **Kangal**, s.67.

daha kaydettiğinde yeni bir suç oluşabilecektir³⁹⁴. Hukuka aykırı olarak kaydedilmiş veriyi üçüncü bir kişi kaydettiğinde ise verileri ele geçirme suçu (TCK m.136) oluşacaktır.

6698 sayılı KVKK'nın yürürlüğe girmesinden sonra fiil unsuru ile ilgili ciddi bir tartışma ortaya çıkmıştır. Öğretide bazı yazarlar TCK'da yer alan suç tiplerinin fiil unsurlarının meydana gelebilmesi için KVKK'da tanımlanan veri işleme kavramının kapsamına giren bir fiilin bulunması gerektiği görüşündedir³⁹⁵. KVKK'da veri işleme kavramı *"Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem"* olarak tanımlanmıştır. Kişisel verilerin otomatik olmayan yollarla ve bir veri kayıt sisteminin parçası da olmadan kaydedilmesi, ele geçirilmesi, verilmesi veya yayılması durumunda KVKK'ya göre veri işlemeden söz edilemez. Bu tür durumlarda TCK'da yer alan suçların oluşup oluşmayacağı tartışma konusudur. Bizim de katıldığımız görüşe göre TCK'da yer alan suç tipleri bakımından fiil unsurunun gerçekleşmesi için KVKK'da yer alan veri işleme tanımına uygun bir fiilin bulunması şart değildir³⁹⁶. Diğer bir deyişle kişisel verilerin otomatik olmayan yollarla, bir veri kayıt sisteminin de parçası olmadan kaydedilmesi kişisel verilerin kaydedilmesi suçunun fiil unsurunu oluşturabilir. Öğretide zikredilen bir örnekle somutlaştırmak gerekirse; başkasının telefon numarasının herhangi bir hukuka uygunluk sebebine dayanmadan cepten çıkarılan bir kâğıda yazılması durumunda KVKK kapsamında veri işlemeden söz edilemeyecektir³⁹⁷. Zira bu olayda otomatik yollarla işlemeden ve bir veri kayıt sisteminin parçası olarak işlemeden söz

³⁹⁴ Farklı bir zamanda aynı kişinin farklı bir verisinin kaydedildiği durumda şartlarının oluşması durumunda zincirleme suç hükümleri uygulanabilecektir. Burada failin bir suç işleme kararının icrası kapsamında hareket edip etmediğine göre bir değerlendirme yapmak gerekecektir.

³⁹⁵ **Koca / Üzülmaz** (2020), s.61. **Korkmaz**, s.393. **Uyarer**, s.200.

³⁹⁶ **Kangal**, s.65. **Maden**, s.55-62. **Sarıusta, Kader** (2018) Kişisel Verilerin Ceza Hukuku Yoluyla Korunması (Yüksek Lisans), Gaziantep Üniversitesi Sosyal Bilimler Enstitüsü, s.124. **Sert, Şeyma** (2019) Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması, 1. Baskı, Ankara, Seçkin, s.103. **Titrek**, s.72. Atıf yapılan yazarlar bu konuyu ele almış ve KVKK'da yer alan, tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla fiillerin gerçekleştirilmesi şartının bu suç tiplerinde aranmayacağını açıkça ifade etmiştir. Öğretide bu suç tiplerini inceleyen diğer pek çok yazar ise bu konuda herhangi bir değerlendirmeye yer vermemiştir. Herhangi bir değerlendirmede bulunmayan yazarların da bu suç tipleri açısından yukarıda zikrettiğimiz şartı aramadıkları sonucuna ulaşmak mümkündür.

³⁹⁷ **Koca / Üzülmaz** (2020), s.561.

edilemeyecektir. Böylesi bir fiil KVKK kapsamına girmese de kanaatimizce TCK kapsamına girecektir.

Kişisel verilerin kaydedilmesi suçunun oluşması için verilerin tamamen veya kısmen otomatik olan yollarla veya veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla kaydedilmesi gerektiğini savunan yazarlar, TCK m.136'nın fiil unsurunu incelerken aynı şarttan bahsetmemektedir. Dolayısıyla bu yazarların anlatımından kişisel verileri verme, ele geçirme veya yayma (TCK m.136) suçu için böyle bir şart aranmayacağı sonucu çıkmaktadır. Ancak KVKK'da veri işleme kavramı kişisel veriler üzerindeki her türlü işlem olarak tanımlanmıştır ve TCK m.136'da seçimlik hareketler olarak düzenlenen verme, ele geçirme ve yayma fiilleri de veri işleme kapsamına girebilecek nitelikte hareketlerdir³⁹⁸. Dolayısıyla TCK m.135'in fiil unsuru için yukarıda zikrettiğimiz şart aranacaksa TCK m.136 bakımından da aynı şartın aranması gerekir. Bunun zaten açık bir durum olması sebebiyle yazarların gereksiz tekrardan kaçınmak adına TCK m.136'yı ele alırken bu şarta değinmemiş olması ihtimali akla gelebilir. Fakat Koca / Üzülmüş tarafından TCK m.136'nın fiil unsuru anlatılırken verilen bir örnekte hastayı tedavi eden bir hekimin hasta ile ilgili bilgileri ilgisiz bir kişiye sözle açıklaması durumunda bu suçun oluşacağı ifade edilmiştir³⁹⁹. Bu örnekte ne otomatik bir veri işlemeyen ne de bir veri kayıt sisteminden söz edilemeyeceğine göre yazarların TCK m.136 için böyle bir şart aramadıkları anlaşılmaktadır. TCK m.135 ile 136 bakımından farklı yaklaşımlar sergilenmesinin kendi içerisinde tutarlı olmadığını söylemek gerekir.

Kişisel verilere ilişkin suçlar bakımından iki ihtimalli bir durumun olduğu söylenebilir. Birinci ihtimal bu suçlarının fiil unsurunun KVKK kapsamına girmeyecek bir şekilde gerçekleşmesidir. Bu durumda KVKK hükümleri uygulanmayacaktır. Dolayısıyla hukuka uygunluk sebepleri bakımından genel hükümlere başvurulacaktır. İkinci ihtimal ise bu suçların fiil unsurunun KVKK kapsamına da girecek şekilde gerçekleştirilmesidir. Bu durumda KVKK hükümleri uygulama alanı bulacağından KVKK'da yer alan veri işleme

³⁹⁸ Öğretide Eşref Barış Börekçi de verme, ele geçirme ve yayma fiillerinin otomatik yollarla veya veri kayıt sisteminin parçası olarak gerçekleştirilmesi halinde KVKK'da tanımlanan veri işleme kavramının kapsamına girdiğini ifade etmektedir. Esasen bu konuda bir şüphe yoktur. Bkz. **Börekçi**, s.90-92.

³⁹⁹ Bahsi geçen örnek için bkz. **Koca / Üzülmüş** (2020), s.578.

şartları ve veri işleme ilkeleri göz önünde bulundurulacak, hukuka aykırılık unsuru buna göre değerlendirilecektir⁴⁰⁰.

KVKK'daki veri işleme kavramının kapsamına giren fiillerden ancak TCK'daki suç tiplerinde düzenlenen fiillerin kapsamına girenler cezalandırılabilir. TCK'da tanımlanan fiillerin geniş şekilde yorumlanması suretiyle KVKK'daki veri işleme kavramının kapsamına giren her halin cezalandırılmaya çalışılması mümkün değildir. Böylesi bir tutum kıyas anlamına gelir ve kıyas TCK m.2/3 hükmü ile açıkça yasaklanmıştır.

Öğretide bir yazar veri işleme kavramının kapsamına giren bütün durumların cezalandırılması gerektiğini, fakat bu durumun KVKK ve TCK'nın birbiri ile uyumsuz olması sebebiyle kanunilik ilkesine aykırılık teşkil ettiğini, bu uyumsuzluğun giderilmesi için TCK m.135'te yer alan kaydetme fiilinin işleme olarak değiştirilmesi gerektiğini savunmaktadır⁴⁰¹. Bu görüşe katılmıyoruz. TCK kişisel veriler üzerindeki farklı eylemleri farklı suç başlıkları altında düzenlemiş ve bunlara farklı oranlarda cezalar ve farklı nitelikli haller öngörmüştür. Kişisel verilerin hukuka aykırı olarak kaydedilmesi fiiline öngörülen ceza 1 yıldan 3 yıla kadar iken verilerin hukuka aykırı olarak verilmesi, ele geçirilmesi ve yayılması fiillerine öngörülen ceza 2 yıldan 4 yıla kadardır. Bu fark kanun koyucunun TCK m.135 ve m.136'daki fiillerin haksızlık oranını birbiri ile aynı kabul etmemesinden kaynaklanmaktadır. Yazar kişisel veriler üzerindeki bazı fiillerin cezasız kalmasını da bu

⁴⁰⁰ Ancak şunu belirtmekte fayda var ki KVKK'daki veri işleme tanımının kapsamına giren bir fiilin gerçekleştirilmesi durumunda söz konusu fiil KVKK'nın istisnalar başlıklı 28inci maddesi kapsamına giriyorsa KVKK hükümleri uygulanmayacaktır. Öğretide bir görüşe göre KVKK m.28'deki istisnalar halleri hukuka uygunluk sebepleridir. (Bkz. **Korkmaz**, s.422) Fakat biz bu görüşe katılmıyoruz. İstisna hallerinin varlığı durumunda KVKK hükümleri uygulanmazken diğer kanunlarda yer alan hükümler, dolayısıyla TCK hükümleri uygulanmaya devam edecektir.

⁴⁰¹ Korkmaz'ın bu konudaki açıklamaları şu şekildedir; “TCK ile Kişisel Verilerin Korunması Kanunu arasında kişisel verilerin korunmasına yaklaşım açısından farklılıklar bulunmaktadır. Daha önceki bölümlerde belirtildiği gibi kişisel verilerin işlenmesi 6698 sayılı Kanun'da “Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem” olarak geniş bir şekilde tanımlanmış olmasına rağmen TCK'da bu eylemlerden sadece kaydedilmesi, verilmesi, yayılması, ele geçirilmesi, yok edilmemesi eylemleri suç olarak düzenlenmiştir. Bunun sonucunda kişisel veriler hukuka uygunluk sebepleri olmadan 6698 sayılı Kanun'da kişisel verilerin işlenmesi olarak sayılan; depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi eylemlerle işlenirse, bu eylemlerin TCK'da suç sayılan eylemlerle bağlantılı olması durumunda cezalandırılacaklar, aksi taktirde kanunilik ilkesi gereği TCK'da suç olarak düzenlenmediklerinden yaptırımsız kalacaklar ve bu da kişisel verileri bu eylemlere karşı korunmasız bırakacaktır. TCK'nun 6698 sayılı Kişisel Verilerin Korunması Kanunu ile uyumlu hale getirilerek kişisel veriler üzerinde ceza hukuku kapsamında etkin bir koruma sağlanabilmesi için TCK'nun 135. Maddesinde düzenlenen kişisel verilerin kaydedilmesi eyleminin, kişisel verilerin işlenmesi olarak değiştirilmesi gerekmektedir.” **Korkmaz**, s.396-397

değişikliğin yapılması için bir gerekçe olarak sunmuştur. Veri işleme kavramının tanımında örnek kabilinden sayılan “*değiştirme*” ve “*yeniden düzenleme*” gibi bazı fiillerin TCK kapsamında cezalandırılmadığı doğrudur. Fakat bu fiillerin suç olarak kabul edilmesi bizce gerekli değildir. Bu fiillerin haksızlık içeriği TCK’da tanımlanan fiiller kadar ağır değildir.

Veri işleme kavramının TCK’ya taşınması durumunda sorun teşkil edecek bir diğer husus veri işleme kavramının sınırlarının belirsiz oluşudur. Zira KVKK’da bu kavram tanımlanırken sayılan fiiller örnek kabilindendir ve sınırlayıcı değildir. KVKK veriler üzerinde gerçekleştirilecek her türlü işlemi veri işleme olarak kabul etmektedir. Veriler üzerinde gerçekleştirilecek her işlemin suç olarak tanımlanmasında hukuki yarar bulunmadığını, bunun ceza sorumluluğunu gereksiz ölçüde genişleteceğini düşünmekteyiz. Ayrıca bu değişiklik yapıldığında yalnızca KVKK’nın kapsamına giren durumlarda (yukarıda bahsettiğimiz verileri değiştirme gibi kimi hafif ihlal durumlarında da) suç oluşacaktır. KVKK kapsamına girmeyen durumlarda suç oluşmayacak, kimi önemli hak ihlalleri cezasız kalacaktır. Yani KVKK kapsamına giren kimi nispeten önemsiz ihlallerin cezalandırılması, KVKK kapsamına girmeyen kimi önemli ihlallerin ise cezalandırılmaması gibi istenmeyen sonuçlar doğacaktır. Bu sebeplerle TCK m.135’teki kaydetme ifadesinin işleme olarak değiştirilmesi gerektiği fikrine katılmıyoruz.

Son olarak kaydetme fiilinin ihmali hareketle işlenebilmesi de mümkündür. Örneğin hukuka uygunluk sebeplerinden birine dayanarak otomatik yollarla veri kaydeden bir kişi hukuka uygunluk sebepleri ortadan kalktığında veri kaydetmeyi durdurmak zorundadır. Hukuka uygunluk sebebinin kalktığını ve artık veri kaydetmenin haksızlık teşkil edeceğini bilmesine rağmen otomatik işlemlere müdahale etmeyen, bu suretle verilerin kaydedilmesini sağlayan kişi ihmali hareketle suçu işlemiş olur.

Madde metninde suç tanımı “*hukuka aykırı olarak*” kişisel verilerin kaydedilmesi şeklinde yapılmıştır. Buradaki hukuka aykırı olarak ifadesinin ne anlama geldiği hukuka aykırılık unsuru başlığında açıklanacaktır.

2.2.2. Manevi Unsur

Kişisel verilerin kaydedilmesi suçu ancak kasten işlenebilir. Suçun taksirli hali kanunda düzenlenmemiştir.

Kast kanunda “suçun kanuni tanımındaki unsurların bilerek ve istenerek gerçekleştirilmesi” şeklinde tanımlanmıştır. Madde gerekçesinde ise kastın varlığı için “suçun kanuni tanımındaki **maddi** unsurların bilerek ve istenerek gerçekleştirilmesi” gerektiği ifade edilmiştir. Öğretideki genel kabule göre kastın varlığından söz edebilmek için failin suçun maddi unsurlarını bilmesi ve istemesi gerekir. Hukuka aykırılık unsuru ise kastın kapsamına dahil değildir. Kişisel verilerin kaydedilmesi suçunun kanuni tanımında düzenlenen maddi unsurlar kaydetme fiili ve kişisel veridir.

Kanuni tanımda geçen kişisel veri unsuru normatif bir unsurdur. Yani bu unsurun ifade ettiği anlam ve bu anlamın kapsamı-sınırları normal bir kişinin günlük hayat bilgisi, somut gözlem ve müşahedesi ile tam olarak anlaşılamaz. Kişisel veri kavramının ne ifade ettiğini tespit edebilmek için hukuki bir değerlendirmeye ihtiyaç vardır. Böylesi normatif unsurlar bakımından failin kastının varlığının kabul edilebilmesi için failin bu unsur hakkında genel bir anlam bilgisine sahip olması gerekir. Failin gerçek kişiye ilişkin, onun şahsı bakımından fonksiyon gören bir bilgiyi kaydettiğini bilmesi⁴⁰² ve iradesini bu doğrultuda kullanarak kaydetme fiilini gerçekleştirmesi durumunda kast vardır. Ancak failin somut olaydaki bilginin (verinin) kanunen kişisel veri olarak tanımlandığını bilmesi kastın varlığı için şart değildir⁴⁰³.

⁴⁰² Koca / Üzülmaz (2020), s.562.

⁴⁰³ Koca / Üzülmaz (2020), s.562. Gökhan Ölmez bu konuyu şu ifadelerle izah etmiştir: “Suçun değerlendirilebilir (normatif) unsurları ise algılanan dışsallığın bir norm ya da üzerinde daha önce toplumda fikir birliğine varılmış ve bu suretle kurumsallaşmış bir uzlaşma ekseninde anlamlandırılmasını gerekli kılar. ... İşte failin söz konusu sosyal anlam bilgisine sahip olmadığı hallerde kasten hareket ettiğinden bahsedilemez. Kendisinden bir suç tanımında yer verilen kavramların hukuki anlamını ve kapsamını bilmesi beklenmeyen failin, düzenlemede yer alan kavramların işaret ettiği gerçekliğin bir parçasını oluşturan unsurların sosyal anlam bilgisine sahip olması halinde kastı mevcut bulunmaktadır. Değerlendirilebilir (normatif) unsurların sosyal anlamına dair “paralel muhakeme”; kanun koyucu tarafından ilgili suç tanımından yer verilen kavramın anlamının somut olayda failde yansıma bulup bulmadığını ifade etmektedir. Failin, paralel muhakeme sonucunda somut olaydaki unsura ilişkin sosyal anlam bilgisine sahip olduğu hallerde kastı bulunmaktadır. Paralel muhakemenin başarısız olduğu hallerde ise değerlendirilebilir unsur bilgisinin bulunmaması dolayısıyla kastın varlığından bahsedilemez. Bu itibarla, failin unsurun anlam bilgisine sahip olması önem arz etmekte olup; kavram bilgisinin bulunmaması kastın varlığını etkilemez. Dolayısıyla kapsam hatası olarak ifade ettiğimiz hata türünün kastın varlığına herhangi bir etkisi bulunmaz.” Ölmez, Gökhan (2020) Suçun Tanımlanabilir ve Değerlendirilebilir Unsurları (Doktora), Ankara Hacı Bayram Veli Üniversitesi Lisansüstü Eğitim Enstitüsü, s.267-268.

Suçun kanuni tanımında herhangi bir saik aranmamıştır. Failin hangi maksatla verileri kaydettiğinin bir önemi yoktur. Suçun manevi unsuru değerlendirilirken failin ne maksatla hareket ettiğine bakılmayacaktır.

Suçun olası kast ile işlenip işlenemeyeceği tartışma konusudur. Bazı yazarlar suçun olası kast ile de işlenebileceğini savunmaktayken⁴⁰⁴, bazı yazarlar yalnızca doğrudan kast ile işlenebileceğini savunmaktadır⁴⁰⁵. Suçun yalnızca doğrudan kast ile işlenebileceğini savunan yazarlar madde metninde yer alan “*hukuka aykırı olarak*” ifadesinden yola çıkmaktadır. Fakat bu yazarların birbirinden farklı iki görüş ile bu sonuca ulaştığını söylemek gerekir. Birinci görüşteki yazarlar bu ifade sebebiyle hukuka özel aykırılığın aranacağını, kastın hukuka aykırılığı da kapsaması gerektiğini, bu sebeple suçun sadece doğrudan kastla işlenebileceğini savunmaktadır⁴⁰⁶. İkinci görüşteki yazarlar ise kastın hukuka aykırılığı kapsamasının gerekmediğini, fakat tipteki bu ifadenin haksızlık bilinci konusunda bir bağlantı noktası oluşturacağını, bu sebeple suçun yalnızca doğrudan kastla işlenebileceğini savunmaktadır⁴⁰⁷. “*Hukuka aykırı olarak*” ifadesinin özel hukuka aykırılık anlamına gelmediğini düşündüğümüz için birinci görüşe katılmıyoruz. İkinci görüşe ise teorik olarak katılmakla birlikte TCK bakımından uygulanmasının mümkün olmadığı kanaatindeyiz. TCK’da suçun yalnızca doğrudan haksızlık bilinci ile işlendiği durumlarda failin cezalandırılmasını, olası haksızlık bilinci ve haksızlık yanılığı hallerinde ise faile ceza verilmemesini sağlayacak hukuki bir dayanak bulunmamaktadır. Dolayısıyla suç yalnızca doğrudan haksızlık bilinciyle işlenmesi durumunda değil, olası haksızlık bilinciyle ve kaçınılabilir haksızlık yanılığı altında işlenmesi durumlarında da cezalandırılacaktır. Haksızlık yanılığı veya olası haksızlık bilinci durumundaki failin ise olası kastla hareket etmesi mümkün olduğundan suçun olası kastla işlenmesi mümkün gözükmektedir⁴⁰⁸.

⁴⁰⁴ Özbek / Doğan / Bacaksız, Ceza Özel, s.607. Kangal, s.71.

⁴⁰⁵ Koca / Üzülmöz (2020), s.562. Maden, s.79.

⁴⁰⁶ Maden, s.79.

⁴⁰⁷ Koca / Üzülmöz (2020), s.562.

⁴⁰⁸ Bu konuda detaylı açıklamalara ileride 1.2.3.3. numaralı başlıkta yer verilmiştir.

2.2.3. Hukuka Aykırılık Unsuru

Suçun oluşması için gereken unsurlardan bir diğeri hukuka aykırılık unsurudur. Kişisel verilerin kaydedilmesi fiilini hukuka uygun hale getiren bir hukuka uygunluk sebebinin bulunmadığı durumlarda hukuka aykırılık unsuru da gerçekleştiği için suç oluşacaktır. Bir hukuka uygunluk sebebinin bulunması durumunda ise fiil hukuka uygun hale gelecek ve suç oluşmayacaktır.

Anayasa m.20/3'te kişisel verilerin ancak kanunla öngörülen hallerde veya kişinin açık rızası ile işlenebileceği düzenlenmiştir. Veri işleme ise KVKK m.3/1-e hükmünde *“Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem”* olarak tanımlanmıştır. Dolayısıyla *“veri işleme”* tanımının kapsamına giren durumlarda verilerin ancak veri sahibinin açık rızasının bulunduğu durumlarda veya kanunlarda açıkça öngörülmüş olması halinde işlenebileceği kabul edilmelidir.

Fiil başlığı altında bu suçun fiil unsurunun iki şekilde gerçekleşebileceğinden bahsetmiştik. Fiilin gerçekleşme şekli olayda hangi hukuka uygunluk sebeplerinin gündeme gelebileceğinin tespiti bakımından son derece önemlidir.

Kişisel verilerin kaydedilmesi suçunun fiil unsuru gerçekleşme şekline göre iki kategoride ele alınabilir. Birincisi KVKK'nın kapsamına giren bir kaydetme fiilidir. İkincisi ise KVKK kapsamına girmeyen, sıradan bir kaydetme fiilidir. Birinci durumda KVKK hükümleri uygulanacağı için KVKK'da yer alan hukuka uygunluk sebepleri gündeme gelebilecekken, ikinci durumda KVKK'da yer alan hukuka uygunluk sebeplerine başvurulamayacak, yalnızca genel hukuka uygunluk sebepleri söz konusu olabilecektir.

Kaydetme fiilinin KVKK'nın kapsamına girebilmesi için öncelikle veri işleme kavramının kapsamına girmesi gerekir. Veri işleme kavramının tanımını yukarıda vermiştik. Buna göre kaydetme fiilinin *“tamamen veya kısmen otomatik olan veya*

herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla” gerçekleştirilmesi durumunda veri işlemeden söz edilecektir. Veri işlemeden söz edildiği durumlarda ise KVKK uygulama alanı bulacaktır. Ancak kanunun 28inci maddesindeki istisna hükümlerinin kapsamına giren bir veri işleme fiilinin varlığı halinde KVKK hükümlerinin uygulanmayacağını hatırlatmak gerekir. Somut olayda KVKK hükümlerinin uygulanması için bir veri işleme faaliyetinin var olması ve bu faaliyetin 28inci maddede istisna olarak düzenlenmemiş olması gerekir. 28inci maddenin ikinci fıkrasındaki kısmî istisna hallerinde ise KVKK’da yer alan hukuka uygunluk sebepleri gündeme gelebilecektir. Çünkü bu durumlarda kanunun veri işleme şartlarını ve genel ilkeleri düzenleyen maddeleri istisna kapsamına alınmamıştır. KVKK kapsamına giren durumlarda KVKK hükümleri ile çelişmemesi şartıyla diğer kanunların hükümleri de uygulanabilecek, diğer kanunlarda yer alan hukuka uygunluk sebepleri de gündeme gelebilecektir.

Otomatik olmayan yollarla ve bir veri kayıt sisteminin de parçası olmadan gerçekleştirilen kişisel verilerin kaydedilmesi eylemi veri işleme kavramının kapsamında olmadığı için KVKK kapsamına girmeyecektir. Yine veri işleme kavramının kapsamına girmesine rağmen KVKK m.28/1’de belirtilen tam istisna hallerinden biri ile kanunun uygulanmasından bağışık tutulmuş bir kaydetme fiili de KVKK kapsamına girmeyecektir. İşte bu tür kaydetme fiilleri bakımından yalnızca genel hukuka uygunluk sebepleri uygulanacaktır.

2.2.3.1. KVKK Kapsamına Giren Fiiller Bakımından Hukuka Uygunluk Sebepleri

6698 sayılı KVKK’nın 5inci maddesinde kişisel verilerin işleme şartları düzenlenmiştir. Bu işleme şartları özel nitelikli olmayan kişisel verilerin hangi durumlarda işlenebileceğini belirlemektedir. Kanunun 6ncı maddesinde ise özel nitelikli kişisel verilerin işleme şartları düzenlenmiştir. Özel nitelikli kişisel veriler ancak 6ncı maddede düzenlenen şartların varlığı halinde işlenebilecektir. 5nci ve 6ncı maddelerde yer alan veri işleme şartlarının varlığı veri işleme fiilini hukuka uygun hale getireceği için kişisel verilerin kaydedilmesi suçu bakımından hukuka uygunluk sebebi olarak kabul edilecektir. Ancak şunu belirtmekte fayda var ki KVKK nezdinde veri işlemenin hukuka uygun hale

gelebilmesi için veri işleme faaliyetinin 4üncü maddede düzenlenen genel ilkelere de uygun şekilde yürütülmesi gerekmektedir. Genel ilkelere ve veri işleme şartlarına ilişkin detaylı açıklamalar ikinci bölümde yapıldığı için burada aynı açıklamaları tekrar yapmaya lüzum görmüyoruz. Ancak toplu bir görünümün sağlanması amacıyla 4, 5 ve 6ncı maddeleri kanuni ifadeler şeklinde zikretmeyi gerekli ve yeterli görüyoruz.

Kişisel verilerin işlenmesinde uyulması zorunlu olan ilkeler m.4'te şöyle sıralanmıştır; “

- i. *Hukuka ve dürüstlük kurallarına uygun olma.*
- ii. *Doğru ve gerektiğinde güncel olma.*
- iii. *Belirli, açık ve meşru amaçlar için işlenme.*
- iv. *İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma.*
- v. *İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme.”*

“Doğru ve gerektiğinde güncel olma” ilkesi aslen veri işleme şartları ile değil veri sorumlusunun yükümlülükleriyle alakalı bir ilkedir. Bu sebeple veri işleme şartlarından birinin varlığı halinde bu ilkeye aykırı hareketin tek başına hukuka uygunluk sebebini ortadan kaldırmayacağı kanaatindeyiz. Diğer ilkelere aykırı davranışlar ise veri işleme şartlarından biri var olsa dahi veri işlemeyi hukuka aykırı hale getirecektir⁴⁰⁹.

Özel nitelikli olmayan kişisel verilerin işleme şartları m.5'te şu şekilde düzenlenmiştir; “

- a) *İlgili kişinin açık rızasının bulunması*
- b) *Veri işlemenin kanunlarda açıkça öngörülmesi*
- c) *Veri işlemenin 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.*
- d) *Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.*
- e) *Veri işlemenin veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.*

⁴⁰⁹ İlkelerle ilişkin detaylı açıklamalar için ikinci bölüme bakınız.

- f) Verilerin ilgili kişinin kendisi tarafından alenileştirilmiş olması.
- g) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.
- h) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.”

Özel nitelikli olmayan kişisel verilerin KVKK kapsamında kaydedilmesi durumunda bu şartlardan birinin bulunması halinde veri işleme fiili hukuka uygun olacağı için suç oluşmayacaktır⁴¹⁰.

Özel nitelikli kişisel verilerin işlenme şartları KVKK m.6’da dört fıkra halinde düzenlenmiştir. Özel nitelikli kişisel verilerden birinin KVKK kapsamında kaydedilmesi durumunda aşağıdaki şartlar aranacaktır. Bu şartlardan birinin bulunması halinde veri işleme fiili hukuka uygun olacağı için suç oluşmayacaktır.

Özel Nitelikli Kişisel Veri Türü	İşlenme Şartları
“Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri”	Kural: Bu tür veriler ilgilinin açık rızası olmadan işlenemez İstisna: Bu tür veriler veri işlemenin kanunlarda öngörülmüş olması durumunda açık rıza olmasa da işlenebilir.

⁴¹⁰ Beşinci maddede yer alan veri işleme şartlarına ilişkin detaylı değerlendirmeler için ikinci bölümün ilgili başlığına bakınız.

Sağlık ve cinsel yaşama ilişkin kişisel veriler	Kural: Bu tür veriler ilgilinin açık rızası olmadan işlenemez İstisna: Verilerin 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 halinde bu tür veriler açık rıza aranmaksızın işlenebilir.
---	--

Özel nitelikli kişisel verilerin işlenme şartlarına ilişkin detaylı değerlendirmelerimiz için ikinci bölümün ilgili başlığına bakabilirsiniz.

Kişisel verilerin KVKK kapsamında işlenmesi durumunda ayrıca genel hukuka uygunluk sebeplerinin varlığı ile de fiil hukuka uygun hale gelebilir. Ancak iki farklı hükmün bulunması durumunda özel kanun olması sebebiyle KVKK hükümleri uygulanması gerektiğine dikkat edilmelidir. Örneğin KVKK’da açık rıza aranırken TCK açısından rızanın zımnî olması yeterlidir. Değerlendirme konusu somut olayda fiil unsuru KVKK kapsamında bir veri işleme teşkil ediyorsa açık rıza aranacak, KVKK kapsamına girmiyorsa zımnî rıza yeterli olacaktır.

2.2.3.2. Genel Hukuka Uygunluk Sebepleri

TCK’da yer alan genel hukuka uygunluk sebepleri kişisel verilerin kaydedilmesi suçu bakımından da uygulanacaktır. Kişisel veriler ister KVKK kapsamında kaydedilmiş olsun ister KVKK kapsamına girmeyecek bir şekilde kaydedilmiş olsun TCK’da yer alan genel hukuka uygunluk sebepleri uygulanabilir. Ancak KVKK kapsamına giren durumlar için KVKK hükümleri ile diğer kanun hükümleri arasında çelişki bulunması durumunda özel normun önceliği ilkesi gereği KVKK hükümlerinin uygulanması gerekecektir. Bu durum rıza hukuka uygunluk sebebinde karşımıza çıkmaktadır. Rıza hem TCK’da hem de

KVKK da düzenlenmiş bir hukuka uygunluk sebebidir. Fakat KVKK’da rızanın geçerli olması daha sıkı şartlara bağlanmıştır. KVKK kapsamına giren bir veri işleme faaliyetinde rızanın geçerli olabilmesi için açık rıza şartlarına uyulması gerekecektir.

TCK’da düzenlenen genel hukuka uygunluk sebepleri kanunun hükmünün yerine getirilmesi, meşru müdafaa, hakkın kullanılması ve ilgilinin rızasıdır. Zorunluluk halinin ve hukuka aykırı fakat bağlayıcı emrin yerine getirilmesinin hukuka uygunluk sebeplerinden mi yoksa kusurluluğu ortadan kaldıran hallerden mi olduğu öğretilerde tartışmalıdır. Biz bu durumları kusurluluğu ortadan kaldıran hallerden kabul ettiğimiz için bu başlık altında yer vermeyeceğiz.

Kanun hükmünün yerine getirilmesi TCK m.24/1 hükmünde bir hukuka uygunluk sebebi olarak düzenlenmiştir. Söz konusu fıkrada “*Kanunun hükmünü yerine getiren kimseye ceza verilmez*” ifadesi yer almaktadır. Hukuka ve usulüne uygun şekilde verilmiş emirler de kanunun hükmünü icra sebebiyle hukuka uygundur. Çünkü bu tür durumlarda emri veren ve emri alan kanun tarafından kendilerine verilmiş olan görevleri ifa etmektedir. Bu hukuka uygunluk sebebi, hukuk düzeninin bir kişiye kanun ile bir görev veya yetki vermesi durumunda bu doğrultuda hareket eden kişinin başka bir kanun hükmü tarafından suçlu addedilmesinin mümkün olmayacağı düşüncesine dayanmaktadır⁴¹¹. Kanunun hükmünün usulüne uygun olarak yerine getirilmesi durumunda kişinin fiili tipe uygun olsa dahi hukuka aykırılıktan söz edilemez.

Kişisel verilerin işlenmesi konusunda en çok gündeme gelebilecek hukuka uygunluk sebeplerinden biri kanunun hükmünü icradır. Kamu hizmetlerinin yerine getirilmesi, güvenliğin sağlanması, olası uyuşmazlıkların önüne geçilmesi gibi pek çok sebebe dayalı olarak kanunlar tarafından kişilere kişisel verileri işleme⁴¹² görevi, yükümlülüğü veya hakkı tanınmaktadır. Bu hükümler doğrultusunda sınırlara da riayet ederek kişisel verileri kaydeden kişiler kanunun hükmünü yerine getirdikleri için veri kaydetme fiilleri hukuka uygun hale gelecektir.

⁴¹¹ “*Kanun bir taraftan kişiden görevini yapmasını isterken, diğer taraftan görevini yapan kimseyi cezalandıramaz.*” Soyaslan (2022), s.380.

⁴¹² Buradaki işleme tabiri veriler üzerindeki her türlü işlemi ifade etmek için kullanılmıştır. KVKK’da yer alan kavramsal manası ile kullanılmamıştır.

Öğretide kanunun hükmünün yerine getirilmesi ifadesinde geçen kanun kavramının geniş yorumlanması gerektiği, tüzük, yönetmelik ve kararların da bu kapsamda değerlendirilebileceği kabul edilmektedir⁴¹³. Bununla birlikte kişisel verilerin korunması hakkına ilişkin Anayasa’da yer alan hükümde bu hakkın korunmasına ilişkin usul ve esasların kanunla düzenleneceği ve kişisel verilerin ancak açık rıza halinde veya kanunda öngörülen durumlarda işlenebileceği ifade edilmektedir. Anayasa’nın bu hükmü karşısında kişisel verilere ilişkin suçlarda kanun ifadesinden TBMM tarafından çıkarılan yasama tasarrufunun anlaşılması gerektiği savunulmaktadır⁴¹⁴. Kanaatimizce kişisel verilerin korunması hakkının sınırlanması anlamına gelecek durumların kanunlarda açıkça düzenlenmesi gereklidir. Kanunda sınırlamanın amacı ve konusu açıkça belirlendikten sonra uygulamaya ilişkin detayların yönetmelik ve tüzük gibi düzenleyici işlemlerle belirlenmesinde sakınca yoktur.

Kanunun hükmünü icra hukuka uygunluk sebebine dair bazı örnekler vermek gerekirse; 5271 sayılı Ceza Muhakemesi Kanunu’nun (CMK) 75, 76, ve 78inci maddelerinde bir suça ilişkin delil elde etmek amacıyla şüpheli ve sanıklardan kan, saç, tükürük, tırnak gibi biyolojik örneklerin alınabileceği hüküm altına alınmıştır. 80inci maddede ise alınan bu örneklerin kişisel veri niteliğinde olduğu, amacı dışında kullanılamayacağı, yetkisiz kişilere verilemeyeceği ve ne zaman yok edileceği düzenlenmiştir⁴¹⁵. Yine CMK m.81’de parmak izinin alınması, m.135’te iletişimin tespiti, m.140’da sanığın ses ve görüntülerinin kayda alınması hükme bağlanmıştır. Kişisel verilerin kaydedilmesine izin veren hükümler bunlarla da sınırlı değildir. İş Kanunu (m. 75), Bankacılık Kanunu (m. 73), Vergi Usul Kanunu (m. 5, 148), Karayolları Trafik Kanunu (m. 5), PVSK (m. 5, ek m. 7), Devlet İstihbarat Hizmetleri ve Milli İstihbarat Kanunu (m. 4, 6), Elektronik İmza Kanunu (m. 12) gibi pek çok kanunda bu konuya ilişkin hükümler yer almaktadır. Bu hükümlere uygun olarak gerçekleştirilen kişisel veri kaydetme fiilleri kanunun hükmünü icra hukuka uygunluk sebebi vesilesiyle hukuka uygun hale gelecektir.

⁴¹³ Soyaslan (2022), s.381. Koca / Üzülmmez (2022), s.276.

⁴¹⁴ Koca / Üzülmmez (2020), s.563.

⁴¹⁵ TCK m.80; “(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”.

Meşru müdafaa TCK'da düzenlenen bir diğer genel hukuka uygunluk sebebidir. Niteliğine uygun düştüğü ölçüde bütün suç tipleri için uygulanabilecektir⁴¹⁶. Kişisel Verilerin Kaydedilmesi suçunun gerçekleşme şekli dikkate alındığında bu suç açısından uygulamada meşru müdafaa hukuka uygunluk sebebiyle karşılaştırılması pek olası değildir. Bu suç açısından meşru müdafaanın uygulanmasının mümkün olduğunu savunanlar⁴¹⁷ olmakla birlikte mümkün olmadığını savunanlar⁴¹⁸ da vardır. İstisnai de olsa bazı durumlarda meşru müdafaaya ilişkin şartların gerçekleşmesinin mümkün olduğu kanaatindeyiz. Somutlaştırmak gerekirse; trafiğin sıkışık olduğu bir yerde yaşanan bir anlaşmazlık olduğunu düşünelim. Bir magandanın aracından inerek kadın bir sürücüye tehdit ve hakaretler savurmaya başladığını, aracına saldırarak zarar verdiğini ve saldırılarını şiddetini artırarak sürdürdüğünü varsayalım. Sıkışık trafik nedeniyle olay yerinden aracıyla uzaklaşma imkânı bulamayan kadının telefonunu çıkararak olanları kayda almaya başladığını varsayalım. Saldırganın kayda alındığını fark ettiğinde cezai yaptırıma uğrama, haber olma ve itibar kaybı yaşama gibi çeşitli korkularla saldırılarını durdurması mümkündür. Esasen rızası olmayan bir kişiyi kamera ile video kaydına almak kişisel verileri kaydetme suçunu teşkil edecektir. Fakat böyle bir olayda failin kendisine yönelmiş bir saldırıyı def etmek için bu kaydı almasının zaruri ve orantılı olduğu kabul edilebilir. Dolayısıyla bu tür istisnai durumlarda meşru müdafaa hükmünün bu suç bakımından uygulanabileceği kabul edilmelidir.

Hakkın kullanılması TCK'da düzenlenen bir diğer genel hukuka uygunluk sebebidir. TCK m.26/1'de hakkını kullanan kimseye ceza verilmeyeceği ifade edilmiştir. Fail kişisel verilerin kaydedilmesi fiilini bir hakkın kullanılması kapsamında gerçekleştiriyor olabilir ve bu durumda fiil hukuka uygun hale gelebilir. Somutlaştırmak gerekirse; kişisel veri kaydetmenin bilimsel çalışmalar için gerekli olması durumunda bilim ve sanat hürriyeti (AY m.27), haber içeriğinde kullanılması durumunda haber alma ve verme hürriyeti (AY m.26), mahkemede savunma yaparken gerekli olması durumunda savunma hakkı (AY m.36) bağlamında kişisel verilerin kaydedilmesi olasıdır. Uygulamada da bu durumlarla sıkça karşılaşılmaktadır. Örneğin kamuyu ilgilendiren bir konuda,

⁴¹⁶ Meşru müdafaa TCK m.25/1'de şu şekilde tanımlanmıştır. “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.”

⁴¹⁷ **Erdoğan, Yavuz** (2013) ‘Kişisel Verilerin Korunması Bakımından Türk Ceza Kanunu Hükümlerinin Değerlendirilmesi’ ERÜHFD, C:8, S:2, Doğan Soyaslan Armağanı, (s.569-632), s.599.

⁴¹⁸ **Köse Aysun**, s.162.

hakkında güncel, doğru ve haber verme hakkının sınırlarını aşmayan bir yayın yapılan kişi, haber içeriğinde şahsına ait bazı bilgilerin (mesleği, yaşı vs.) bulunması sebebiyle kişisel verilerinin hukuka aykırı olarak kaydedildiğini ve yayıldığını iddia etse de haberi yapan kişinin fiili hukuka uygundur.

İlgilinin rızası TCK’da düzenlenen bir diğer genel hukuka uygunluk sebebidir. TCK m.26/2’ye göre “*Kişinin üzerinde mutlak surette tasarruf edebileceği bir hakkına ilişkin olmak üzere, açıkladığı rızası çerçevesinde işlenen fiilden dolayı kimseye ceza verilmez*”. Kişisel verilerin korunması hakkını kişinin üzerinde mutlak surette tasarruf edebileceği bir hak olarak kabul etmek gerekir⁴¹⁹. Anayasa’da ve KVKK’da kişisel verilerin rıza ile işlenebilecek olmasının hüküm altına alınması bu hak üzerinde kişinin tasarruf yetkisi olduğunu göstermektedir.

Genel bir hukuka uygunluk sebebi olan rızanın geçerliliği için bazı şartlar vardır. Öncelikle rıza kişinin üzerinde mutlak suretle tasarrufta bulunabileceği bir hakka ilişkin verilmiş olmalıdır. Kişisel verilerin korunması hakkı böyle bir haktır. Beyanda bulunan kişinin rızaya ehil olması gerekir. Kişinin rızaya ehil kabul edilebilmesi için temyiz kudretine haiz olması, fiilin hukuki anlam ve sonuçlarını kavrama ve davranışlarını yönlendirme yeteneğine sahip olması gerekir⁴²⁰. Rıza fiilin işlenmesinden önce veya en geç işlenme sırasında verilmiş olmalıdır. Sonradan verilen rıza fiili hukuka uygun hale getirmez. TCK’da düzenlenen rıza için bir şekil şartı yoktur. Açık veya örtülü, yazılı veya sözlü olması fark etmez⁴²¹.

Kişisel verilerin işlenmesi için Anayasa’da ve KVKK’da **açık rıza** aranmıştır. Anayasa’da ve KVKK’da yer alan açık rıza şartı, veri işleme tanımının ve dolayısıyla KVKK’nın kapsamına giren durumlarda aranmalıdır. KVKK kapsamına girmeyen kişisel veri kaydetme fiillerinin hukuka uygunluğu için genel hukuka uygunluk sebebi olan rızaya ilişkin şartların gerçekleşmiş olması yeterlidir. Açık rıza için kişisel verilerin korunması hukukunda sıkı şartlar öngörülmüştür. Sıradan (KVKK kapsamına girmeyen) bir veri kaydetme fiili için bu şartların aranması fiilen imkansızdır. Örneğin arkadaşının rızası ile telefon numarasını alan ve bir kâğıda yazan kişinin yaptığı eylem kişisel verilerin

⁴¹⁹ Kangal, s.77.

⁴²⁰ Soyaslan (2022), s.378.

⁴²¹ Koca / Üzülmöz (2022), s.298.

kaydedilmesidir. Eğer bu olayda rızanın geçerliliği için veri sahibinin verinin kullanılma amaçlarına ilişkin aydınlatılmasını, açık bir irade beyanı ile bu işlemi onaylamasını, bu aydınlatma ve onamın ispatı gerektiğinde ispat yükünün numarayı kaydedene yüklenmesini, şartlarına uygun bir açık rızayı temin ettiğini ispat edemediği durumlarda rızayı geçersiz sayarak kişiyi cezalandırmayı kabul edersek, bu kabul hiç şüphesiz sosyal hayatın gerçekleri ile bağdaşmaz. Açık rıza dahil olmak üzere, KVKK’da yer alan ve veri işleme sürecini sıkı bir şekilde tanzim etme maksadı güden düzenlemeler, otomatik yollarla veya veri kayıt sistemleri içerisinde gerçekleştirilen geniş kapsamlı veri işleme faaliyetlerini kapsamakta, bu alanı disiplinize etmeyi amaçlamaktadır. KVKK kapsamına giren bir veri işleme faaliyeti için açık rızaya ilişkin şartlar aranmalı, KVKK kapsamına girmeyen bir veri işleme için ise genel rıza yeterli kabul edilmelidir⁴²². Açık rızaya ilişkin detaylı açıklamalara çalışmamızın ikinci bölümündeki ilgili başlıkta ulaşılabilir.

2.2.3.3. Hukuka Aykırı Olarak İfadesinin Anlamı

Değerlendirilmesi gereken bir diğer husus kanuni tanımda yer alan hukuka aykırı olarak ifadesinin ne anlama geldiğidir⁴²³. Bu konuda öğretide farklı görüşler vardır. Türk Ceza Hukuku öğretisinde hâkim olan görüşe göre hukuka aykırılığın kanuni tanımda özel olarak zikredilmesi durumunda özel hukuka aykırılıktan söz edilir ve hukuka aykırılık tipiklik içerisinde bir unsur özelliği kazanır⁴²⁴. Bu durumda kastın hukuka aykırılığı da kapsamı gerekir. Suçun maddi unsurlarının yanında failin hukuka aykırılığın bilincinde olarak hareket ettiğinin de ayrıca araştırılması ve kanıtlanması gerekir. Aksi takdirde kasttan söz edilemez⁴²⁵.

Hukuka aykırılık ifadesinin anlamına yönelik bir diğer görüşe göre ise bu ifade her zaman aynı fonksiyonu görmez. Bazı durumlarda tipiklik içerisinde yer alırken bazı

⁴²² Aynı yönde açıklamalar; “KVKK açısından veri ilgisinin “açık rızası” aranırken, KVKK’ya tabi olmayan kişisel veriler bakımından aynı husus bu suç tipi açısından aranmaz.... KVKK’ya tabi olmayan kişisel veriler açısından zımî rıza geçerli olacaktır.” **Dülger** (2020), s.711-712.

⁴²³ TCK’da hukuka aykırılığın suç tipinde özel olarak zikredildiği pek çok suç tipi bulunmaktadır. Bu suç tiplerinde “Hukuka aykırı olarak”, “hukuka aykırı yollarla”, “hukuka aykırı şekilde”, “haksız bir menfaat” gibi farklı ifadeler kullanılmıştır.

⁴²⁴ **Artuk, Mehmet Emin / Gökçen, Ahmet / Alaşahin, Mehmet Emin / Çakır, Kerim** (2019) Ceza Hukuku Genel Hükümler, 13. Baskı, Ankara, Adalet Yayınları, s.398.

⁴²⁵ **Özgenç**, s.310.

durumlarda tipikliğe dahil değildir. İfadenin yer aldığı her suç tipi için ayrı bir değerlendirme yapılması ve fonksiyonunun buna göre tespit edilmesi gerekir⁴²⁶. Şayet bu ve benzeri ifadeler suç tipinde yer alan maddi unsurlardan birinin niteliğini ifade ediyorsa bu ifadenin tipikliğe dahil olduğunu kabul etmek gerekir⁴²⁷. Failin bunu bilmemesi ise unsur yanılığı oluşturacağı için kastı ortadan kaldırır (TCK m.30/1)⁴²⁸. Bu tip suçlar ancak doğrudan kastla işlenebilir⁴²⁹. Örnek vermek gerekirse TCK m.91/5’de yer alan “*Hukuka aykırı yollarla elde edilmiş olan organ veya dokuyu saklayan, nakleden veya aşıl原因an kişi, iki yıldan beş yıla kadar hapis cezası ile cezalandırılır*” hükmünde durum böyledir. Hukuka aykırı yollarla elde edilmiş olmak suçun maddi unsurlarından biri olan organ ve dokuyu nitelemektedir. Dolayısıyla bu ifade suçun unsuruna dahildir. Failin organ veya dokunun hukuka aykırı yollarla elde edilmiş olduğunu bilmesi kastın varlığı için şarttır⁴³⁰.

Suçun kanuni tanımında yer alan hukuka aykırılık ifadesi maddi unsurlardan birinin değil de tipik haksızlığın tamamının değerlendirilmesine yönelikse bu ifade hukuka aykırılık unsurunun ayrıca vurgulanması anlamına gelir ve tipikliğe dahil değildir. Kanun koyucu bu ifadeye yer vermekle hâkimi somut olayda bir hukuka uygunluk sebebinin bulunabileceği konusunda uyarmakta, bu konunun üzerinde titizlikle durulmasını sağlamaya çalışmaktadır. Bu hususu biraz daha açmakta fayda vardır. Suç kanuni tanımdaki maddi ve manevi unsurların “*hukuka aykırı olarak*” gerçekleştirilmesidir. Hukuka aykırılık her suç için bulunması gereken bir unsurdur ve çoğu zaman suçun kanuni ifadesinde ayrıca zikredilmez. Suçun kanuni tanımındaki unsurların tamamını niteleyecek şekilde hukuka aykırılığın ayrıca zikredilmesi suçun unsurları açısından yeni bir durum doğurmaz. Hukuka aykırılık unsuruna dikkat çekerek hâkimi somut olayda bir hukuka uygunluk sebebinin bulunabileceği konusunda uyarma fonksiyonu görür. Bu durumda hâkim tipe uygun fiilin gerçekleşmesini hukuka aykırılığa bir karine olarak kabul etmemeli, somut olayda bir hukuka uygunluk sebebinin gerçekleşip gerçekleşmediğini ayrıca araştırmalı ve hükümde bu hususa açıkça yer vermelidir⁴³¹.

⁴²⁶ Dülger (2020), s.704. Koca / Üzülmmez (2022), s.269. Göktürk, Neslihan (2016) ‘Suçun Yasal Tanımında Yer Alan Hukuka Aykırılık İfadesinin İcra Ettiği Fonksiyon’ İnönü Üniversitesi Hukuk Fakültesi Dergisi, C:7, S:1, (s.407-450), s.427.

⁴²⁷ Koca / Üzülmmez (2022), s.269.

⁴²⁸ Göktürk (2016), s.427.

⁴²⁹ Koca / Üzülmmez (2022), s.269., Göktürk (2016), s.427.

⁴³⁰ Göktürk (2016). s.427

⁴³¹ Göktürk (2016), s.432., Demirbaş, Timur (2022) Ceza Hukuku Genel Hükümler, 17. Baskı, Ankara, Seçkin, s.291.

Failin icra ettiği fiilin hukuka aykırı olduğunun bilincinde olması suçun unsurları ile alakalı bir durum değil, failin kınanabilirliğine ilişkin olan kusurluluk alanıyla ilgili bir konudur ve buna haksızlık bilinci denir. Öğretide, “*hukuka aykırı olarak*” ifadesinin, kast ve tipiklik bağlamında değerlendirilemese bile failin taşıdığı haksızlık bilincine bir atıf olarak yorumlanabileceği ifade edilmektedir⁴³². Bizce de bu tür ifadelerin haksızlık bilinci kapsamında değerlendirilmesi daha doğrudur.

Failin hukuka aykırı olarak hareket ettiğinin bilincinde olması doğrudan haksızlık bilinci ile hareket etmesi anlamına gelir. Doğrudan haksızlık bilinci failin fiilinin kesin olarak hukuka aykırı olduğunu bilmesidir ve bu durumda fail tam kusurludur. Fail fiilinin hukuka aykırılığı konusunda şüphe içinde ise olası haksızlık bilincinden söz edilmektedir. Bu durumda failin tam kusurlu olup olmadığı konusunda farklı fikirler olmakla beraber Alman öğretisinde hâkim olan görüş failin tam kusurlu olduğu yönündedir⁴³³. Ancak Göktürk’e göre suç tipinde yer alan “*hukuka aykırı olarak*” ifadesi olası haksızlık bilinci içerisinde bulunan failin kusurlu addedilmesine engel olmaktadır⁴³⁴. Bizce de doğru olan budur.

Haksızlık bilincinin bulunmadığı (failin fiilinin haksızlık oluşturmadığını düşünerek hareket ettiği) durumlarda ise haksızlık yanılığı söz konusudur. Haksızlık yanılığı TCK m.30/4’te düzenlenmiştir. Bu hükme göre işlediği fiilin haksızlık oluşturduğu hususunda kaçınılmaz bir hataya düşen kişi kusurlu değildir ve cezalandırılmaz. TCK kaçınılmaz haksızlık yanılığı halinde faile ceza verilmeyeceğini kabul ederek “*kusursuz ceza olmaz*” prensibine ve kusurlu sorumluluk anlayışına uygun bir düzenleme getirmiştir. Ancak haksızlık yanılığının kaçınılabilir olduğu durumlar için TCK’da bir düzenleme yer almamaktadır. Gerekçedeki ifadeye göre hatanın kaçınılabilir olması halinde kişi kusurlu sayılacak fakat bu husus temel cezanın belirlenmesinde göz önünde bulundurulacaktır. Kişinin haksızlık yanılığı içerisinde bulunmasının temel cezanın belirlenmesinde göz önünde bulundurulması kanaatimizce failin kusuruyla orantılı ceza verilmesini sağlamak bakımından işlevsel değildir⁴³⁵. Alman Ceza Kanunu’nun 17nci paragrafında kaçınılabilir haksızlık yanılığı halinde cezada indirimle gidilebileceği hükmü

⁴³² “Tipteki bu ifade haksızlık bilinci bakımından bir bağlantı noktası oluşturur.” Koca / Üzülmöz (2020), s.562. “Bu suçlarda failin kusuru hukuka aykırılığı da kapsamalıdır.” Özbek / Doğan / Bacaksız, Ceza Genel, s.284.

⁴³³ Detaylı bilgi için bkz. Göktürk (2016), s.432-433.

⁴³⁴ Göktürk (2016), s.432-433.

⁴³⁵ Öbek / Doğan / Bacaksız, Ceza Genel, s.457.

yer almaktadır⁴³⁶. Şayet indirim sonucu ortaya çıkan ceza da failin kusuru ile orantısız şekilde fazla ise failin beraatine karar verilmesi gerektiği kabul edilmektedir⁴³⁷. Buna benzer bir düzenlemeye Türk Ceza Hukuku'nda da ihtiyaç bulunmaktadır. TCK m.30/4 hükmüne kaçınılabilir haksızlık yanılığının varlığı durumunda hâkime cezada indirim yapma ve bazı durumlarda ceza vermeme olanağı tanıyacak bir hüküm getirilmesi gerektiğini düşünmekteyiz. Böylesi bir düzenleme hâkime kusurluluk bağlamında geniş kapsamlı bir değerlendirmede bulunma imkânı sağlayacak, hâkimin somut olaydaki kusur oranını dikkate alarak ceza adaletini sağlamasına imkân tanıyacaktır. Suçun kanuni tanımında “*hukuka aykırı olarak*” ifadesinin yer aldığı durumlarda failin doğrudan haksızlık bilinci ile hareket etmesinin kusurlu addedilebilme şartı olarak kabul edilmesi yine bu sayede mümkün olabilecektir⁴³⁸. Böylesi durumlarda suçun doğrudan haksızlık bilinci ile işlenmesi gerektiği kabul edildiğinde olası kast ile işlenemeyeceği de söylenebilecektir. Esasen öğretide bu görüşü savunan yazarlar bulunmasına rağmen⁴³⁹ TCK'nın mevcut haliyle bu yönde bir uygulama yapmaya imkân tanımadığı kanaatindeyiz. TCK'ya göre haksızlık yanılığı yalnızca kaçınılmaz olduğu durumda kusuru kaldıracak ve cezasızlık sebebi olarak kabul edilebilecektir.

Tüm bu açıklamaların ışığında kanaatimizce, TCK m.135 ve m.136'da yer alan “*hukuka aykırı olarak*” ifadesi hukuka aykırılık unsuruna dikkat çekmekte ve hâkimi somut olayda bir hukuka uygunluk sebebinin bulunup bulunmadığını araştırmaya yönlendirmektedir. Madde gerekçesinde bu ifadeye açıklık getirilirken hukuka uygunluk sebeplerinin var olabileceğine dikkat çekilmesi de bunu kanıtlar niteliktedir⁴⁴⁰. Bununla birlikte bu ifade sadece suçun genel unsurlarından biri olan hukuka aykırılık konusunda değil, aynı zamanda kusurluluk konusunda da bir fonksiyon görmektedir. Somut olayda failin haksızlık yanılığı içerisinde olup olmadığı araştırılmalıdır. TCK'nın mevcut düzenlemeleri doğrultusunda yalnızca kaçınılmaz haksızlık yanılığının varlığı durumunda

⁴³⁶ **Soyer Güleç, Sesim** (2008) ‘Türk Ceza Kanunu’nda Haksızlık Yanılığı’ Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, C:10, S:1, (s. 59-91), s.84. **Özbek / Doğan / Bacaksız**, Ceza Genel, s.457.

⁴³⁷ **Roxin, Claus** (2006) Yasağa İlişkin Yanılma (Çev.:Osman İsfen), Suç Politikası, Karşılaştırmalı Güncel Ceza Hukuku Serisi 5, Ankara, s.275’ den aktaran **Soyer Güleç**, s.84.

⁴³⁸ Böyle bir ifadenin yer almadığı durumlarda ise olası haksızlık bilinci de tam kusurluluk için yeterli kabul edilebilecektir.

⁴³⁹ **Göktürk** (2016), s.433.

⁴⁴⁰ TCK m.135 Gerekçe: “...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...” **Özbek**, s.946.

fail kusursuz kabul edilebilecek ve cezalandırılmayacaktır. Haksızlık yanılığının kaçınılabilir olduđu durumda ise fail kusurlu kabul edilecek ve cezalandırılacaktır. Fakat hâkim bu yanılıgyı temel cezayı belirlerken göz önünde bulundurabilecek, alt sınıra yakın şekilde cezaya hükmedebilecektir. Yukarıda da ifade ettiğimiz gibi TCK’da haksızlık yanılığının uygulama alanını genişletecek düzenlemelere ihtiyaç duyulmaktadır. Bu düzenlemeler şayet yapılırsa, özellikle failin haksızlık bilincinin derecesinin farklı şekillerde gündeme gelebildiği kişisel verilere ilişkin suç tiplerinde ceza adaletinin sağlanmasında önemli bir fonksiyon görecektir. Doğrudan haksızlık bilincine sahip olmadan kişisel verileri kaydeden kişilerin cezalandırılmamasına veya duruma göre cezasında indirim yapılmasına imkân sağlanmış olacaktır.

2.3. Nitelikli Haller

Kişisel Verilerin Kaydedilmesi suçu için kanunda üç farklı nitelikli hâl düzenlenmiştir. Bunlardan birincisi TCK m.135/2’de yer alan ve suçun konusuna ilişkin olan nitelikli haldir. Diğer iki nitelikli hal ise failin şahsına ve fiilin işlenme şekline ilişkindir. Failin şahsına ve fiilin işlenme şekline ilişkin nitelikli haller, “*Nitelikli Haller*” başlığını taşıyan TCK m.137’de düzenlenmiştir.

2.3.1. Suçun Konusuna (Özel Nitelikli Kişisel Verilere) İlişkin Nitelikli Hâl

TCK m.135/2’de “*Kişisel verinin, kişilerin siyasi, felsefî veya dini görüşlerine, ırkı kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması durumunda birinci fıkra uyarınca verilecek ceza yarı oranında artırılır*” hükmü bulunmaktadır. “*Kişisel Verilerin Kaydedilmesi*” başlığını taşıyan 135inci maddenin birinci fıkrasında suçun temel şekli düzenlenmiş, ikinci fıkrada ise suçun konusunu belirli kategorilerdeki kişisel verilerin oluşturması durumunda birinci fıkra uyarınca verilecek cezanın yarı oranında artırılması öngörülmüştür.

İkinci fıkra hükmü 24/03/2016 tarihinde yapılan değişiklik ile şu anki halini almıştır. Fıkranın ciddi eleştirilere ve tartışmalara sebep olan ilk hali şu şekildedir; *“Kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimse, yukarıdaki fıkra hükmüne göre cezalandırılır.”* Görüldüğü üzere fıkranın ilk halinde özel nitelikli bazı veri kategorileri sayılmış olmasına rağmen herhangi bir ceza artırımına yer verilmemiştir. Özel nitelikli kişisel veriler birinci bölümde de ifade ettiğimiz üzere veri koruma hukukunda daha sıkı şekilde korunması öngörülen veriler olarak kabul edilmektedir. Bu kabulün en büyük sebebi veri sahibinin bu verilerin hukuka aykırı şekilde işlenmesi durumunda diğer verilerin işlenmesine nazaran daha büyük mağduriyetlere uğrama ve ayrımcılığa maruz kalma riskinin bulunmasıdır. İkinci fıkranın ilk haline getirilen en büyük eleştiri ceza artırımını öngörmemesi sebebiyle hiçbir fonksiyonunun bulunmadığı yönünde olmuştur⁴⁴¹. Fıkranın eleştirilmesine sebep olan bir diğer durum ise fıkroda “kişisel veri olarak kaydeden” ibaresine yer verilmiş olmasıdır. Öğretide bu ifadenin yersiz olduğu, zira sayılan bilgilerin zaten kişisel veri niteliğine haiz olduğu, bu ifadeden ise bunların her durumda kişisel veri olarak kabul edilmeyeceği sonucunun çıkabileceği ifade edilmiştir⁴⁴². Bizce de bu eleştiri son derece doğrudur. Bazı yazarlar bu ifadenin verilerin bilgisayar ortamına kaydedilmesi olarak anlaşılması gerektiğini ifade etmiştir. Bu yazarlara göre ikinci fıkroda sayılan kategorilerden birine giren veriler yalnızca bilgisayar ortamına kaydedildiğinde suç oluşacaktır⁴⁴³. Ancak bu yorum kanaatimizce doğru değildir. Zaten ilgili ifade madde metninden çıkarılmıştır.

İkinci fıkroda siyasi, felsefi, dini görüş ve ırkî köken kategorileri için *“hukuka aykırı olarak”* ibaresinin yer almaması, diğer sayılan kategoriler için ise bu ifadeye yer

⁴⁴¹ Dülger haklı olarak bu fıkroda sayılan verilerin zaten birinci fıkra kapsamında korunduğunu, ikinci fıkroda tekrar sayılmalarının bir ceza artırımını yapılmayacaksa lüzumsuz olduğunu savunmuştur. Bkz. **Dülger** (2020), s.699. Özbek de bu fıkroda sayılan özel nitelikli verilerin kaydedilmesine daha ağır ceza öngörülmesi gerektiğini ifade etmiştir. **Özbek**, s.949.

⁴⁴² **Özbek**, s.949.

⁴⁴³ Bahsi geçen yazarlar gerekçedeki *“suç tanımında kişisel verilerin bilgisayar ortamında veya kâğıt üzerinde kayda alınması arasında bir ayırım gözetilmemiştir”* ifadesinin yalnızca birinci fıkra için geçerli olduğu yorumunda bulunmuştur. **Hafızogulları / Özen**, s.269. Akdağ ise *“Kişisel veri olarak kaydetme”* ifadesinin anlamına ilişkin *“2. fıkra ile bu tür verilerin kişisel nitelik taşımayacak şekilde, yani anonim şekilde işlenebileceğinin vurgulanmak istendiği sonucuna ulaşmak mümkündür”* yorumunda bulunmuştur. Fakat anonim şekilde kaydedilen veriler zaten kişisel veri niteliği taşımayacağı için bu suçların konusunu oluşturmayacaktır. Bu durumu ifade etmek için kanunda tekrar belirtmeye gerek yoktur. Bahsi geçen yorum için bkz. **Akdağ**, s.97.

verilmesi farklı yorumlara ve tartışmalara sebep olan bir diğer husustur. Bazı yazarlar siyasi, felsefi, dini görüş ve ırkî köken ile alakalı hukuka aykırı olarak ibaresine yer verilmemesinden bu verilerin kaydedilmesinin her halükârda hukuka aykırı olduğu sonucunun çıkarılması gerektiğini, diğer veriler için ise bir hukuka uygunluk halinin bulunabileceğini ifade etmiştir⁴⁴⁴. Kanaatimizce bu yorum hatalıdır⁴⁴⁵. Zira mutlak dokunulmaz olduğu iddia edilen kategorilere ilişkin verilerin de kanun hükümleri doğrultusunda işlendiği bir gerçektir. Örneğin kişilerin siyasi parti üyelikleri ilgili kurumların kayıtlarında tutulmaktadır. Kanaatimizce kanun koyucu bu ibareye yer vererek bazı veri türlerinin kaydedilmesine ilişkin olaylarda hukuka uygunluk sebepleriyle sıklıkla karşılaşılabileceğine dikkat çekmek istemiş, bu kategoride yer alan verilere ilişkin bir fiilin suç oluşturup oluşturmadığı değerlendirilirken hukuka aykırılık unsurunun daha dikkatli araştırılmasını sağlamaya çalışmıştır⁴⁴⁶.

Hukuka aykırı olarak ibaresine ikinci fıkrada da yer verilmesi birinci fıkradaki hukuka aykırı olarak ibaresi için daha önce yaptığımız yorumu destekler niteliktedir. Keza birinci fıkradaki ibarenin tipikliğe dahil olduğu kabul edilirse ikinci fıkrada neden tekrar bu ibareye yer verildiğini açıklamak mümkün olmayacaktır. Çünkü bir suçun nitelikli hali o suçun temel şekline ait bütün unsurları barındırır. Nitelikli unsur ise bunlara bir ilavedir. Suçun temel halindeki hukuka aykırı olarak ifadesi tipikliğe dahil kabul edilirse ikinci fıkradaki ibare de benzer şekilde yorumlanmalı ve tipikliğe ikinci bir ilave kabul edilmelidir. Bir ifadenin tipikliğe iki defa dahil edilmesi ise anlamsız olacaktır⁴⁴⁷. Dolayısıyla bu maddenin birinci ve ikinci fıkralarındaki hukuka aykırı olarak ifadeleri tipikliğe dahil değildir ve suçun tamamına ilişkin bir değerlendirme anlamı taşımaktadır.

⁴⁴⁴ “TCK m.135/2 fıkrada sayılan veriler arasında bir ayrım yapmış, kişilerin siyasi, felsefi veya dini görüşlerine, ırkî kökenlerine ilişkin verileri mutlak dokunulmaz veriler olarak kabul ederken; ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri nisbi dokunulmaz veriler olarak kabul etmiştir. Diğer bir deyişle ilk grupta yer alan veriler hiçbir şekilde kaydedilemez ve bunu mümkün kılan bir hukuk kuralı yaratılamaz.” **Özbek**, s.949. Özen ve Hafizoğulları da Özbek’e benzer bir yorum yapmış, fakat neden böyle bir ayrıma ihtiyaç duyulduğunun anlaşılamadığını ifade etmişlerdir. **Hafizoğulları / Özen**, s.269

⁴⁴⁵ Bu yorumu eleştiren diğer yazarlar için bkz. **Koca / Üzülmöz** (2020), s.568

⁴⁴⁶ Gerekeçteki ifade de bu kanaatimizi destekler niteliktedir. Gerekeç: “Maddenin ikinci fıkrasında, kişilerin siyasi, felsefi veya dinî görüşlerine, ırkî kökenlerine, ahlâkî eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kayda almak, suç olarak tanımlanmıştır. Ancak, bunlardan kişilerin ahlâkî eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgilerin kayda alınmasına kanunlarda özellikle suçlulukla mücadele bağlamında, suç ve suçluların ortaya çıkarılmasını sağlamak amacıyla belli ölçüde izin verilebilir. Bu durumlarda söz konusu suç oluşmayacaktır.”

⁴⁴⁷ **Maden**, s.74.

Burada dikkat çekmek istediğimiz bir diğer husus KVKK'da sayılan özel nitelikli kişisel veri kategorileri ile TCK'da sayılan özel nitelikli kişisel veri kategorilerinin örtüşmemesidir. KVKK'da kişilerin etnik kökeni, kılık kıyafeti, dernek ve vakıf üyelikleri, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli veriler olarak sayılmışken TCK m.135/2'de bunlara yer verilmemiştir. Buna karşılık KVKK'da ahlaki eğilimlere ilişkin bilgiler özel nitelikli kabul edilmemişken bu veriler TCK m.135/2'de yer almıştır. TCK m.135/2'de sayılan veri kategorilerinin KVKK m.6/1 ile uyumlu hale getirilmesi gerektiği öğretide ifade edilen hususlardan biridir⁴⁴⁸. Şunu belirtmek gerekir ki nitelikli halin meydana gelebilmesi için verilerin m.135/2'de sayılan bu kategorilerden birine ait olması şarttır. Bu kategoriler KVKK m.6/1 hükmüne kıyas edilerek genişletilemez. Böylesi bir yorum kıyas anlamına gelir ve kanunilik ilkesine aykırıdır. İkinci fıkrada sayılan kategorilere girmeyen veriler için birinci fıkra hükmü doğrultusunda işlem yapılacaktır.

2.3.2. Failin Sıfatı ve Fiilin İşlenme Şekliyle İlişkili Nitelikli Haller

“*Nitelikli Haller*” başlığını taşıyan TCK m.137'de failin sıfatı ve fiilin işleniş şekliyle ilişkili nitelikli haller düzenlenmiştir. Bu nitelikli haller hem 135inci madde hem de 136ncı madde için geçerlidir. Buna göre kişisel verilerin kaydedilmesi suçunun; “a) *Kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle*, b) *Belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle*” işlenmesi hallerinde, verilecek ceza yarı oranında artırılır.

A bendinde yer alan nitelikli halin gerçekleşmesi için öncelikle fail kamu görevlisi olmalıdır. Kamu görevlisi kavramı TCK m.6/1-c hükmünde “*kamusal faaliyetin yürütülmesine atama veya seçilme yoluyla ya da herhangi bir surette sürekli, süreli veya geçici olarak katılan kişi*” olarak tanımlanmıştır. Bu tanımdan yola çıkarak kamu görevlisi kavramının geniş yorumlanması gerektiğini söylemek mümkündür. Zira tanımda kişinin kamu görevlisi sayılması için kamusal faaliyette bulunması belirleyici kıstas olarak kabul edilmiştir. Bu faaliyetin sürekli nitelikte olması da gerekmemektedir. Belirli bir statü sınırı da koyulmamıştır. Memurlukların yanı sıra avukatlık, noterlik, bilirkişilik, tercümanlık,

⁴⁴⁸ Kangal, s.68, Dülger (2020), s.700.

tanıklık, askerlik gibi kamusal faaliyetin gerçekleştirildiği her türlü iş ve görevler de kamu görevi sayılabilecek, bu işleri yürüten kişiler TCK bakımından kamu görevlisi kabul edilebilecektir.

A bendindeki nitelikli halin gerçekleşmesi için kişinin kamu görevlisi olması yetmez. Kişinin görevinin verdiği yetkiyi kötüye kullanarak hareket etmesi de şarttır. Dolayısıyla kamu görevlisi kişisel verilerin kaydedilmesi konusunda yetkili olmalıdır. Kamu görevlisi olan fakat kişisel verileri kaydetme yetkisi bulunmayan kişinin bu suçu işlemesi halinde nitelikli hal oluşmayacak, suçun temel şeklinden ceza verilecektir. Bu nitelikli halin gerçekleştiği durumlarda kamu görevlisi bakımından görevi kötüye kullanma (TCK m.257) suçu da oluşacaktır. Fakat burada TCK m.137 özel norm teşkil edeceği için görünüşte içtima hali vardır ve fail yalnızca TCK m.137'den cezalandırılır⁴⁴⁹.

B bendinde “*belirli bir meslek ve sanatın sağladığı kolaylıktan yararlanma*” suretiyle suçun işlenmesi nitelikli hal olarak düzenlenmiştir. Buradaki “*ve*” ifadesinin “*veya*” olarak düzeltilmesi gerektiği kanaatindeyiz. Çünkü *ve* ifadesi failin hem meslek hem de sanat icra ediyor olması gerektiği şeklinde yanlış anlaşılmalara sebebiyet verebilir⁴⁵⁰. Halbuki meslek ve sanat burada birbirlerinin alternatifi olarak düzenlenmiştir. Meslek sözlükte “*bir kimsenin geçimini sağlamak için yaptığı sürekli iş*” olarak tanımlanmaktadır⁴⁵¹. Buradaki meslek tabirinin de bu şekilde anlaşılmasında bir sakınca yoktur. Sanat ise sözlükte “*bir duygu, tasarı, güzellik vb.nin anlatımında kullanılan yöntemlerin tamamı veya bu anlatım sonucunda ortaya çıkan üstün yaratıcılık*” olarak tanımlansa da bu tanım oldukça soyut ve geneldir. Aslında sanat kelimesinin kapsayıcı bir tanımını yapmak oldukça zordur. Öğretide buradaki sanat kelimesinin zanaat manasında kullanıldığı ifade edilmiştir⁴⁵². Zanaat insanların maddi gereksinimlerini karşılamak için yapılan ve el ustalığı gerektiren işlerdir.

B bendindeki nitelikli halin gerçekleşebilmesi meslek veya sanatın kişisel verilere ulaşılması veya bunların kaydedilmesi konusunda bir kolaylık sağlıyor olması gerekir. Somut olayda kaydetme fiili gerçekleştirilirken bu kolaylıktan istifade edildiğinin tespit

⁴⁴⁹ Koca / Üzülmöz (2020), s.570.

⁴⁵⁰ Aynı yöndeki görüş için bkz. Özbek, s.953.

⁴⁵¹ Özbek, s.954.

⁴⁵² Özbek, s.954.

edilmesi de zaruridir⁴⁵³. Örneğin kurye olarak çalışan bir kişi teslimat gerçekleştirdiği müşterilerin adres bilgilerine, sipariş içeriklerine, zaman zaman iletişim bilgilerine, hatta TC kimlik numaralarına vakıf olabilmektedir. Kuryenin teslimat gerçekleştirdiği müşterinin telefon numarasını kendi telefonuna işinin gerekleri ile alakalı olmayan bir şekilde kaydetmesi ve buradan kişiye özel mesajlar göndermesi durumunda bu nitelikli halin uygulanması mümkündür.

Kamu görevlilerine bu nitelikli halin uygulanabilmesi için kişisel veri kaydetmek konusunda yetkili olmalarının gerektiğini ifade etmiştik. Şayet kamu görevlisi yetkisi olmadığı halde bu fiili gerçekleştirmişse B bendinin kapsamına girip girmediği ayrıca değerlendirilmelidir. Yetkisiz bir kamu görevlisinin icra ettiği iş mesleği ise ve bu mesleğin sağladığı bir kolaylıktan faydalanarak kişisel veri kaydetmişse bu kişiye B bendi kapsamında nitelikli hâlin tatbik edilmesine engel bir durumun olmadığı kanaatindeyiz.

2.4. Suçun Özel Görünüş Biçimleri

2.4.1. Teşebbüs

Kişisel verilerin kaydedilmesi suçu sırf hareket suçudur. Sırf hareket suçlarında teşebbüsün gerçekleşmesi neticeli suçlara nazaran daha zordur. İcra hareketlerinin bölünebildiği durumlarda sırf hareket suçlarına teşebbüs mümkün olmaktadır. Kişisel verilerin kaydedilmesi fiilinin icra hareketlerinin bölünebilmesi mümkündür. Verilerin kaydedilmesi yerine göre anlık olarak gerçekleşebileceği gibi yerine göre uzun bir süre de alabilir. Bilişim sistemleri üzerinden yapılan veri kaydetme işlemlerinde verileri içeren dosyanın boyutunun büyüklüğüne göre kaydetme işlemi uzayabilmektedir. Failin kaydetme işlemini başlatmasına rağmen teknik problemler sebebiyle veya failin elinde olmayan diğer sebeplerle fiilin tamamlanamaması durumunda teşebbüs söz konusu olacaktır⁴⁵⁴. Ancak failin kaydetme işleminin yarıda kesilmesine rağmen verilerin bir kısmı kaydedilmişse ve kaydedilen kısım kişisel veri niteliği taşıyorsa artık teşebbüsten değil

⁴⁵³ Koca / Üzülmöz (2020), s.570.

⁴⁵⁴ Sert, s.128. Soyaslan (2020), s.363. Köse Aysun, s.168. Taşçı Aydemir, Ece (2022) Kişisel Verilerin Kaydedilmesi Suçu, 1. Baskı, Ankara, Seçkin, s.124.

tamamlanmış suçtan bahsedilmelidir. Çünkü kaydedilen veriler bakımından icra hareketi tamamlanmıştır. Genellikle bilişim sistemleri üzerinden işlenen fiillerde gündeme gelebilecek olsa da teşebbüsten söz edebilmek için kaydetme fiilinin bilişim sistemleri vasıtasıyla gerçekleştirilmesi şart değildir.

Failin kişisel verileri hukuka aykırı olarak ele geçirmesi fakat kaydetme işlemini elinde olmayan sebeplerle tamamlayamaması durumunda ele geçirme fiilinin TCK m.136'da düzenlenen suçun fiil unsurunu teşkil etmesi sebebiyle failin TCK m.136 uyarınca cezalandırılacağı, m.135'e teşebbüsten ceza verilmeyeceği öğretide genel kabul görmektedir⁴⁵⁵.

2.4.2. İştirak

Kişisel verilerin kaydedilmesi suçu iştirak açısından bir özellik göstermemektedir. Bu suça iştirakin her şekli mümkündür⁴⁵⁶.

İştirak bakımından dikkat edilmesi gereken husus suçun bir görünüşte özgü suç olmasıdır. Yukarıda da belirttiğimiz üzere temel şekli herkes tarafından işlenebilen, nitelikli hali ise yalnızca belirli vasıfları taşıyan kişiler tarafından işlenebilen suçlar görünüşte özgü suç olarak adlandırılmaktadır.

TCK m.40/2 hükmüne göre özgü suçlar için ancak özel faillik niteliği taşıyanlar fail olabilecek, bu suçların işlenişine iştirak eden diğer kişiler ise yalnızca azmettiren veya yardım eden olarak sorumlu tutulabilecektir.

Kamu görevlisi A'nın, görevinin verdiği yetkiyi kötüye kullanmak suretiyle kişisel verileri kaydetme suçunu işlediğini, herhangi bir özel vasfı bulunmayan B'nin ise suça iştirak ettiğini varsayalım. B'nin iştiraki fiil üzerinde A ile ortak hakimiyet kuracak

⁴⁵⁵ **Kangal**, s.84. **Maden**, s.86. **Koca / Üzülmöz** (2020), s.571. Özbek, Doğan ve Bacaksız diğer yazarlardan farklı olarak suçun teşebbüse elverişli olmadığını savunmaktadır. Ele geçirilmiş fakat kaydedilememiş veriler için ise diğer yazarlarla aynı sonuca varmakta, yalnızca TCK m.136'dan hüküm kurulması gerektiğini söylemektedir. Bkz. **Özbek / Doğan / Bacaksız**, Ceza Özel, s.607.

⁴⁵⁶ **Özbek / Doğan / Bacaksız**, Ceza Özel, s.607, **Koca / Üzülmöz** (2020), s.571. "İştirake ilişkin genel hükümler uygulanacaktır." **Soyaslan** (2020), s.363.

seviyedeysse, yani müşterek faillik düzeyinde bir iştirak söz konusuysa B TCK m.137 açısından müşterek fail sayılamayacaktır. Çünkü B TCK m.137’de fail için aranan özel nitelikleri taşımamaktadır ve bu suçun faili olarak sorumlu tutulması mümkün değildir. Yukarıda değindiğimiz TCK m.40/2 hükmü ışığında B’nin TCK m.137’den sorumluluğu yalnızca azmettiren ve yardım eden sıfatıyla olabilir. Şayet bu suç bir gerçek özgü suç olsaydı B’nin yardım eden olarak sorumlu tutulması gerekirdi. Çünkü B’nin hareketleri aynı zamanda yardım etmenin şartlarını da taşımaktadır. Fakat bu suç bir görünüşte özgü suç olduğu için B’nin fiilleri aynı zamanda suçun temel şekli olan TCK m.135’in unsurlarını da oluşturmaktadır. B’nin TCK m.135’ten fail sıfatıyla mı yoksa TCK m.137’den suçun nitelikli haline yardım sıfatıyla mı sorumlu tutulacağı sorusu gündeme gelmektedir. Bu durumda “*failliğin şerikliğe asliliği kuralı*” gereğince B suçun temel şeklinden, yani TCK m.135’ten fail olarak sorumlu tutulacaktır⁴⁵⁷.

2.4.3. İçtima

Kişisel verilerin kaydedilmesi suçu için zincirleme suç, aynı neviden fikri içtima, farklı neviden fikri içtima ve görünüşte içtima durumlarının oluşması mümkündür. Madde metninde içtimaa ilişkin özel bir hüküm bulunmamaktadır. Genel hükümler kapsamında değerlendirme yapılması gerekmektedir⁴⁵⁸.

Zincirleme suç⁴⁵⁹ failin bir suç işleme kararının icrası kapsamında aynı kişiye ilişkin verileri farklı zamanlarda birden fazla kez kaydetmesi ile meydana gelecektir⁴⁶⁰.

Zincirleme suç hükümlerinin uygulamasında fiil unsuruna özellikle dikkat edilmelidir. Veri kaydetme hareketlerinden her birinin farklı fiil oluşturması gerekmektedir. Şayet fail bir mağdura ait birden fazla veriyi tek bir hareketle kaydetmişse tek bir fiil vardır. Yine failin mağdura ait birden fazla veriyi doğal anlamda birden fazla hareket ile kaydettiği durumlarda eğer bu hareketler araya zaman ve mekân ayrımı

⁴⁵⁷ Koca / Üzülmmez (2020), s.571. Maden, s.87.

⁴⁵⁸ Taşçı Aydemir, s.125.

⁴⁵⁹ Zincirleme suçun varlığı halinde faille verilecek ceza TCK m.43/1 hükmü uyarınca dörtte birinden dörtte üçüne kadar artırılır.

⁴⁶⁰ Koca / Üzülmmez (2020), s.572.

girmeden birbirini takip eden seri hareketler şeklinde gerçekleştirilmiş ise tek bir fiilin varlığını kabul etmek gerekir. Örneğin failin bilgisayardaki kişisel verilerden kaydetmek istediklerini teker teker USB belleğine kopyalaması durumunda doğal anlamda birden fazla hareket bulunsada hukuki anlamda tek fiil vardır. Tek bir fiilin varlığının kabul edildiği bu tür durumlarda zincirleme suç hükümleri uygulanmayacaktır.

Hukuki anlamda birden fazla fiilin varlığını tespit etmek zincirleme suçtan söz edebilmek için elbette yeterli değildir. Keza zincirleme suçtan söz edebilmek için gerçekleşmesi gereken bir diğer şart birden fazla fiilin bir suç işleme kararının icrası kapsamında gerçekleştirilmesidir. Bir suç işleme kararının icrasından söz edebilmek için failin fiilleri arasında subjektif bir bağın bulunması, fiillerin birbirinin devamı niteliğinde sayılabilmesi gerekir⁴⁶¹. Şayet fiiller arasındaki subjektif bağ kopar ise zincirleme suçtan söz edilemez ve her fiil için ayrı ayrı cezaya hükmolunur. İki fiil arasına makul sayılamayacak uzun bir sürenin girdiği durumlarda ve failin farklı zamanlarda karşısına çıkan fırsatları değerlendirmek suretiyle suç işlediği durumlarda Yargıtay tek bir suç işleme kararından bahsedilemeyeceğine ve her fiil için ayrı ceza verilmesi gerektiğine hükmetmektedir⁴⁶². Failin her fiil için suç işleme kararını yenileyip yenilemediğini tespit etmek yer yer ispat açısından ciddi bir zorluklar teşkil edebilir. Somut olayda fiillerin işleniş şeklinin, arada geçen zamanın ve failin hareketlerinin kolektif olarak değerlendirilmesi suretiyle bu husus tespit edilmeye çalışılacaktır.

Zincirleme suçtan bahsedebilmek için gerçekleşmesi gereken bir diğer şart aynı suçun işlenmiş olmasıdır. TCK m.135 için düzenlenen bütün nitelikli haller suçun temel şekli ile aynı suç olarak kabul edilmelidir⁴⁶³. Örneğin bir kişinin önce sıradan kişisel verilerini kaydeden (TCK m.135/1) daha sonra özel nitelikli kişisel verilerini kaydeden (TCK m.135/2) failin aynı suçu işlediği kabul edilecek ve diğer şartların da varlığı halinde

⁴⁶¹ Koca / Üzülmöz (2022), 539-540.

⁴⁶² "Aynı suç işleme kararı altında suç işlenmesi her biri ayrı ayrı suç teşkil eden fiilleri birbirine bağlayan ve olaya zincirleme suç özelliğini veren subjektif bir bağdır. Saniğin çıkan fırsatlardan yararlanmak suretiyle suç işlediği ya da suç işleme kararının yenilendiği durumlarda aynı suç işleme kararından söz edilemeyeceğinden, zincirleme suç hükümleri uygulanmayacaktır. Zincirleme suçtan söz edebilmek için failin, başlangıçta genel bir niyet ve suç işleme kararı ile aynı suçu aynı mağdura karşı birden fazla kez işlemesi gerekmektedir. Buna göre "suç işleme konusunda tek kararı" olmayıp, ikinci eylemde suç işleme kararı yenilenmiş ise her bir fiil bağımsız suç olarak kabul edilecek ve zincirleme suç söz konusu olmayacaktır. Saniğin iç dünyasına ilişkin olan bu gereklilik sübjektif bir şart olup, mahkemelerce denetime imkan sağlayacak şekilde tespit edilerek karara yansıtılması gerekecektir." Yargıtay CGK, E. 2013/14-384, K. 2014/2, K.T. 14.01.2014.

⁴⁶³ Bir suçun daha az veya daha ağır cezayı gerektiren nitelikli hallerinin o suçun temel şekli ile aynı suç sayılacağı TCK m.43 hükmünde açıkça ifade edilmiştir.

zincirleme suç hükümleri uygulanacaktır. Yine fail aynı mağdura karşı işlediği kişisel veri kaydetme suçunun birisinde mesleğinin sağladığı kolaylıktan istifade etmiş olabilir, bir diğerinde ise mesleği ile alakası olmayacak bir şekilde bu fiili gerçekleştirmiş olabilir. Yani TCK m.137'deki nitelikli hal ile TCK m.135'teki temel şekli oluşturan suçlar bir zincirleme suçun halkalarını oluşturabilirler. Bu durumda da zincirleme suç hükümlerinin uygulanması için bir engel yoktur. Zincirleme suçu oluşturan suçlardan biri suçun temel şeklini diğeri nitelikli halini oluşturuyorsa zincirleme suç hükümleri doğrultusunda yapılacak olan artırım daha ağır cezayı gerektiren suçun ceza miktarı üzerinden yapılmalıdır⁴⁶⁴.

Aynı neviden fikri içtima hükümleri de şartları gerçekleştiği takdirde uygulanabilecektir. Aynı neviden fikri içtima hâli, suçun birden fazla kişiye karşı tek bir fiil ile işlenmesidir ve bu durumda zincirleme suça ilişkin hükümler uygulanır. Kişisel verilerin kaydedilmesi suçunda aynı neviden fikri içtima durumuyla sıklıkla karşılaşılabilir. Örneğin hukuka aykırı olarak kaydedilen bir excel dosyasında birden fazla farklı kişiye ait kişisel veri yer alması durumunda tek bir fiil, aynı suç ve birden fazla mağdur vardır. Bu durumda mağdur sayısının ceza verilmez. Tek cezaya hükmedilir. Fakat bu ceza dörtte birinden dörtte üçüne kadar artırılır (TCK m.43).

Farklı neviden fikri içtima hükümlerinin de bu suç bakımından uygulanması mümkündür. Farklı neviden fikri içtima TCK m.44'te düzenlenmiştir. Failin, işlediği bir fiil ile birden fazla farklı suçun oluşmasına sebebiyet verdiği durumlarda bunlardan en ağırlı ile cezalandırılmasını sağlar. Ancak farklı neviden fikri içtima hükümlerini uygulayabilmek için suçlar arasında görünüşte içtima ilişkisinin bulunmaması gerekir. Görünüşte içtima söz konusu ise görünüşte içtima kuralları doğrultusunda uygulama

⁴⁶⁴ “Fiillerden bazılarının suçun ağırlaştırılmış şeklinin kapsamına girmeleri halinde, suçun basit şeklinin değil, ağırlaştırılmış şeklinin cezası esas alınır ve artırma da bu ceza üstünden yapılır.” **İçel, Kayıhan** (1972) Suçların İçtimai, İstanbul Üniversitesi Yayınları, Yayın No: 1762, s.153. “Baskın görüşe göre, artırım oranının en ağır ihlale öngörülen ceza miktarı üzerinden belirlenmesi gerekir. Bu halde ceza artırımını teşebbüs aşamasında kalmış suçla tamamlanmış suç arasında teselsül ilişkisi bulunuyorsa tamamlanmış suç üzerinden, basit suçla suçun cezası ağırlaştıran nitelikli hali arasında teselsül bulunuyorsa, nitelikli hal üzerinden yapılmalıdır. Bazen teselsüle dahil olan suçlardan tamamlanmış suça nazaran teşebbüs aşamasında kalan suç için daha ağır bir ceza öngörülmüş olabilir. Bu gibi durumlarda teşebbüs aşamasında kalan suçun cezası esas alınmalıdır. Zincirleme suçu oluşturan unsur suçlardan bir kısmı tamamlanmış basit suç, diğer kısmı teşebbüs aşamasında kalmış cezası ağırlaştıran nitelikli hal ise bu durumda hangi ihlal daha ağır cezalandırılıyorsa temel ceza bu ihlal üzerinden somutlaştırılmalıdır. Hâkim, teselsüle dahil suçların hangi ihlal üzerinden artırılacağına tespiti için öncelikle her bir suç bakımından TCK md. 61'i ayrı ayrı uygulamalıdır. Çünkü zincirleme suçun artırım oranının tespitinde en ağır cezanın belirlenmesi ve belirlenen bu ceza üzerinden artırım oranlarının uygulanması gerekir.” **Öztürk, Mustafa Kağan** (2022) Ceza Hukukunda Zincirleme Suç, 1. Baskı, Ankara, Seçkin, s.108.

yapılacaktır⁴⁶⁵. Hem kişisel verilerin kaydedilmesi suçunun kanuni tanımındaki şartların gerçekleştiği hem de başka suç veya suçların kanuni tanımındaki şartların gerçekleştiği durumlarda genellikle görünüşte içtima haliyle karşılaşılmaktadır.

Görünüşte içtimada suçların çokluğu sadece görünüştedir. Aslında tek bir norm ihlal edilmektedir⁴⁶⁶. Görünüşte içtima halinde hangi normun uygulanacağını tespiti normların yorumlanması suretiyle yapılır. Görünüşte içtimanın bulunduğu haller, hangi normun uygulanacağını tespitini sağlayan ilkelerin yardımıyla sistematize edilmektedir. Bu ilkeler özel normun genel norma önceliği, bir normun diğeri tarafından tüketilmesi ve yardımcı normun sonralığı ilkeleridir⁴⁶⁷.

Normlar arasında özel norm genel norm ilişkisinin varlığı halinde özel norm uygulanacak, genel norm geri çekilecektir. Özel norm somut olay bakımından genel normun taşıdığı tüm özellikleri taşıyan, bunun yanı sıra başka birtakım özellikler de taşıyan normdur. TCK m.135-136 ile “*Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar*” bölümündeki diğer suçlar arasında (TCK m.132-134) genel norm - özel norm ilişkisi olduğu kanaatindeyiz. Kişisel verilerin kaydedilmesi (TCK m.135) ve kişisel verileri hukuka aykırı olarak verme veya ele geçirme (TCK m.136) suçları genel norm iken, TCK m.132 ile 134 arasındaki suçlar (TCK 134/1-c.1 hariç) özel normdur. Zira TCK m.132 ile 134 arasındaki suçların (m.134/1-c.1 hariç) gerçekleştiği her durumda gerçekleştirilen fiiller TCK m.135’in veya yerine göre TCK m.136’nın kanuni tanımına da uymaktadır. Bu suçlardan TCK m.135 ile ilişkili olanlar bu bölümde, TCK m.136 ile ilişkili olanlar TCK m.136 incelenirken ele alınacaktır.

Kişiler arasındaki konuşmaların dinlenilmesi ve kayda alınması başlığını taşıyan **TCK m.133’ün ikinci fıkrası** aşağıdaki şekildedir;

“(2) Katıldığı aleni olmayan bir söyleşiyi, diğer konuşanların rızası olmadan ses alma cihazı ile kayda alan kişi, altı aydan iki yıla kadar hapis veya adli para cezası ile cezalandırılır.”

⁴⁶⁵ Göktürk, Neslihan (2014) ‘Türk Hukuku’nda Suçların İçtimai’ Ceza Hukuku ve Kriminoloji Dergisi, C:2, S:1-2, (s.31-59), s.50.

⁴⁶⁶ Göktürk (2014), s.41.

⁴⁶⁷ Koca / Üzülmüş (2022), s.551

Bu fıkra aleni olmayan bir söyleşide kişilerin seslerinin rızaları olmadan kaydedilmesi suç olarak düzenlenmiştir. Kişilerin ses kayıtlarının **her durumda** kişisel veri teşkil ettiğinde kanaatimizce şüphe yoktur. Dolayısıyla TCK m.133/2’de düzenlenen suçun gerçekleşmesi TCK m.135’in gerçekleşmesiyle birlikte bazı ek şartların da gerçekleşmesine bağlıdır. Bu ek şart kaydedilen kişisel verilerin kişiler arasındaki aleni olmayan konuşmalardan oluşmasıdır. Kaydedilen kişisel verilerin kişiler arasındaki aleni olmayan konuşmalardan müteşekkil olması durumunda özel normun önceliği ilkesi gereği TCK m.133/2 hükmü uygulanacaktır. Şayet genel norm – özel norm ilişkisinin olmadığı kabul edilirse farklı neviden fikri içtima kuralı gereği TCK m.135 uygulanmalıdır⁴⁶⁸. Fakat kanaatimizce bu iki suç tipi arasında genel norm – özel norm ilişkisi bulunmaktadır.

Özel hayatın gizliliğini ihlal başlığı taşıyan **TCK m.134’ün birinci fıkrası** aşağıdaki gibidir;

“(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.

Bu fıkra iki cümleden oluşmaktadır. Birinci cümlede özel hayatın gizliliğinin ihlal edilmesinden bahsedilmiş fakat ihlalin ne şekilde gerçekleştirileceğine ilişkin bir sınır konulmamıştır. Bu suçun özel hayat alanının herhangi bir şekilde ihlal edilmesi ile oluşabileceği anlaşılmaktadır. Örneğin kişinin yatak odasının gözlenmesi, duş alırken izlenmesi şeklinde gerçekleştirilen fiiller bu kapsamda değerlendirilebilir. Özel hayatına ilişkin görüntülerin kayda alınması da bu fıkradaki tanıma uymakla beraber bu durum ikinci cümlede özel olarak düzenlendiği için ikinci cümledeki nitelikli halin kapsamındadır. Kanaatimizce birinci cümlede düzenlenen özel hayatın gizliliğini ihlal suçunun temel şekli ile kişisel verilere ilişkin suçlar arasında genel norm – özel norm ilişkisi bulunmamaktadır. Özel hayatın gizliliğini ihlal hareketi bir kişisel verinin ele geçirilmesi yahut kaydedilmesi şeklinde gerçekleşmek zorunda değildir. Esasen suçun üzerinde gerçekleştiği maddi konu da her durumda kişisel veri olmayabilir. Kişisel verilerin kişinin özel hayat alanına dahil olması da şart değildir. TCK m.135 ve m.136’nın gerçekleştiği her durumda özel hayatın gizliliği de ihlal edilmiş sayılmayacaktır.

⁴⁶⁸ Farklı neviden fikri içtima hükümlerinin uygulanacağı görüşü için bkz. **Maden**, s.182.

Dolayısıyla bir fiilin hem özel hayatın gizliliğini ihlal suçunun temel şeklini hem de kişisel verilere ilişkin suçlardan birini teşkil etmesi durumunda farklı neviden fikri içtima hükümleri uygulanmalıdır.

Birinci fıkranın ikinci cümlesinde özel hayatın gizliliğinin görüntü veya seslerin kayda alınması suretiyle ihlal edilmesi düzenlenmiştir. Bir kişinin özel hayatına ilişkin görüntü ve seslerin o kişinin kişisel verisi olduğunda şüphe yoktur. Özel hayata ilişkin görüntü ve seslerin kayda alınması yerine göre kişisel verileri kaydetme yerine göre de kaydetmek suretiyle ele geçirme fiili ile örtüşecektir. Kaydedilen veya kaydedilmek suretiyle ele geçirilen kişisel verilerin kişinin özel hayatına ilişkin görüntü ve seslerden oluşması hâli TCK m.134/1-c.2’de özel olarak düzenlenmiştir. TCK m.134/1-c.2 ile TCK m.135 ve m.136 arasında genel norm – özel norm ilişkisi bulunmaktadır. Özel norm teşkil eden TCK m.134/1-c.2 hükmü uygulanacak, TCK m.135 ve m.136 hükümleri geri çekilecektir⁴⁶⁹.

Öğretide TCK m.244/4 hükmünde düzenlenen **Bilişim Sistemi Aracılığıyla Haksız Yarar Sağlama** suçunun TCK m.135 açısından tali norm olduğu savunulmaktadır⁴⁷⁰. Biz bu görüşe katılmıyoruz. TCK m.244/4’teki suç “*Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adli para cezasına hükmolunur*” şeklinde tanımlanmıştır. “*Yukarıdaki fıkralarda tanımlanan fiiller*” arasında bir sisteme veri yerleştirme veya var olan verileri başka bir yere gönderme fiilleri de yer almaktadır. Dolayısıyla kişisel verileri bir bilişim sistemine hukuka aykırı şekilde kaydeden ve bundan haksız çıkar sağlayan kişi hem TCK m.135’te düzenlenen suçun hem de TCK m.244/4’te düzenlenen suçun tipik fiilini gerçekleştirmiş olur. Yine kişi bilişim sistemindeki kişisel verileri ele geçirerek veya başkasına vererek haksız çıkar sağlamışsa TCK m.136 ve m.244/4’teki suçların tipik fiilini gerçekleştirmiş olur. TCK m.244/4 hükmünde yer alan “*başka bir suç oluşturmaması*” ibaresinin delaletiyle TCK m.135 ile bu suç arasında asli norm – tali norm ilişkisi olduğu iddia edilmiştir. Fakat kanaatimizce bu görüşe katılmak mümkün değildir. Çünkü TCK m.244/4’ün gerçekleşmesi için “*kişinin haksız bir çıkar sağlamasının başka bir suç oluşturmaması*” aranmaktadır. TCK m.135 veya m.136’daki suçlar kişinin haksız bir çıkar

⁴⁶⁹ Aynı yöndeki görüş için bkz. **Maden**, s.186-187. **Koca / Üzülmaz** (2020), s.572.

⁴⁷⁰ **Kangal**, s.91.

sağlaması suretiyle meydana gelmemektedir. Zira bu suçların kanuni tanımlarında böyle bir unsur yoktur. Bu sebeple TCK m.135 veya m.136, m.244/4'ün asli normu olarak kabul edilemez. Bu suçların birlikte gerçekleşmesi durumunda farklı neviden fikri içtima kuralı uygulanacak, fail yalnızca m.244/4'te düzenlenen suçtan cezalandırılacaktır⁴⁷¹.

TCK'nın **Ses ve Görüntülerin Kayda Alınması** başlıklı 286ncı maddesinde soruşturma ve kovuşturma işlemleri sırasındaki ses ve görüntülerin yetkisiz olarak kayda alınması veya nakledilmesi 6 aya kadar hapis cezasını icap ettiren bir suç olarak tanımlanmıştır. Bu suç seçimlik hareketli bir suçtur. Ses ve görüntüleri kayda almak veya nakletmek suretiyle işlenebilir. Fiil unsurunun kayda almak şeklinde gerçekleşmesi durumunda kayda alınan ses ve görüntülerin kişisel veri içermesi halinde TCK m.135 ile TCK m.286 arasında içtima ilişkisi gündeme gelecektir. Bu durumda farklı neviden fikri içtima uygulanacak ve daha ağır cezayı gerektiren TCK m.135 hükmü uygulanacaktır.

2.5. Soruşturma, Kovuşturma ve Yaptırım

Suçun soruşturması ve kovuşturması resen yapılır, şikâyete tabi değildir. Suçun kamu görevlisi tarafından görevi sebebiyle işlenmesi halinde soruşturma yapılabilmesi için yetkili merciin izni gerekir. Suç uzlaştırmaya tabi değildir⁴⁷².

Suçun temel şeklinin cezası 1 yıldan 3 yıla kadar hapistir. Suçun konusunu m.135/2'de sayılan özel nitelikli kişisel verilerin oluşturması durumunda veya suçun m.137'de belirtilen kişiler tarafından işlenmesi durumunda verilecek ceza yarı oranında artırılır.

Suçun bir özel hukuk tüzel kişisi yararına tüzel kişinin organ ve temsilcileri tarafından işlenmesi durumunda tüzel kişi hakkında bunlara mahsus güvenlik tedbirlerine hükmolunur.

⁴⁷¹ **Açıkgöz, Emre İkbāl** (2017) Bilişim Sistemi Aracılığıyla Haksız Yarar Sağlama Suçu (Yüksek Lisans), Ankara Yıldırım Beyazıt Üniversitesi Sosyal Bilimler Enstitüsü, s.101.

⁴⁷² **Kangal**, s.92.

3. KİŞİSEL VERİLERİ HUKUKA AYKIRI OLARAK VERME, YAYMA veya ELE GEÇİRME (TCK m.136)

Kişisel verilerin hukuka aykırı olarak verilmesi, yayılması veya ele geçirilmesi fiilleri TCK m.136’da suç olarak düzenlenmiştir. “*Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme*” başlığını taşıyan m.136 hükmü aşağıdaki şekildedir;

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

(2) Suçun konusunun, Ceza Muhakemesi Kanununun 236ncı maddesinin beşinci ve altıncı fıkraları uyarınca kayda alınan beyan ve görüntüler olması durumunda verilecek ceza bir kat artırılır.”

Birinci fıkrada kişisel verilerin verilmesi, yayılması ve ele geçirilmesi fiilleri suçun oluşması için seçimlik hareketler olarak düzenlenmiştir. İkinci fıkrada ise suçun konusuna ilişkin nitelikli hâle yer verilmiştir.

Madde başlığında “*verileri*” şeklinde genel bir ibare kullanılması öğretide eleştirilmektedir⁴⁷³. Bizce de suçun konusunun her türlü veriye değil yalnızca kişisel verilere ilişkin olması sebebiyle madde başlığına “*kişisel*” ibaresinin eklenmesi yerinde olacaktır. Madde başlığına yöneltilen bir diğer eleştiri suç içeriğinde seçimlik hareket olarak yer alan “*yayma*” fiiline başlıkta yer verilmemiş olmasıdır⁴⁷⁴. Bizce de diğer seçimlik hareketlerden farklı bir mana ihtiva eden yayma fiiline başlıkta yer verilmesi gerekirdi.

Kişisel Verileri Hukuka Aykırı Olarak Verme, Yayma veya Ele Geçirme suçunun unsurları m.135’te düzenlenen Kişisel Verilerin Kaydedilmesi suçunun unsurları ile büyük ölçüde benzerlik arz etmektedir. İki suç tipinin örtüşen özelliklerine ilişkin detaylı açıklamalara m.135 bağlamında daha önce yer verildiği için m.136 incelenirken yalnızca bu suçun özellik arz ettiği hususlar üzerinde durulacaktır. Daha önce değindiğimiz hususlara ilişkin ise m.135 bağlamındaki açıklamalarımıza gönderme yapılacaktır.

⁴⁷³ Karagülmez, Ali (2014) Bilişim Suçları ve Soruşturma – Kovuşturma Evreleri, 5. Baskı, Ankara, Seçkin, s.450.

⁴⁷⁴ Maden, s.92.

3.1. Korunan Hukuki Değer

Kişisel verilere ilişkin üç suç tipi bakımından da (TCK m.135, 136 ve 138) korunan hukuki değer kişisel verilerin korunması hakkıdır. Bu konuda TCK m.135 bağlamında yaptığımız açıklamalar aynen geçerlidir. Özellik arz eden bir durum olmadığı için aynı açıklamalara burada tekrar yer verilmemiştir.

3.2. Suçun Unsurları

3.2.1. Maddi Unsurlar

3.2.1.1. Suçun Maddi Konusu

Kişisel Verilerin Kaydedilmesi suçunda olduğu gibi bu suçta da suçun maddi konusunu kişisel veriler oluşturmaktadır. Bu konuya ilişkin detaylı açıklamalar kişisel verilerin kaydedilmesi suçu bağlamında ilgili başlıkta yapılmıştır.

Kişisel verinin elektronik ortamda veya fiziksel ortamda bulunması arasında bu suç bakımından da bir fark bulunmamaktadır. Bilginin kişinin özel hayat alanına ilişkin olması gibi bir şartın bulunmadığı, gerçek kişi hakkında her türlü bilginin kişisel veri olarak kabul edildiği de unutulmamalıdır.

3.2.1.2. Fail

Kişisel verilerin kaydedilmesi suçu bağlamında yapılan açıklamalar burada da aynıyla geçerlidir. Özetle; suçun temel şeklinde suç faili için herhangi bir özellik aranmamıştır. Herhangi bir gerçek kişi suçun faili olabilir. Madde 137’de düzenlenen nitelikli hallerin gerçekleşebilmesi için ise failin belirli şartları taşıması gerekmektedir. Suçun temel şekli herkes tarafından, nitelikli hali ise yalnızca belirli özellikleri taşıyan

kişiler tarafından işlenebildiği için bu suç görünüşte özgü suçtur. Suçun tüzel kişilerin yetkileri tarafından tüzel kişi menfaatine işlenmesi durumunda tüzel kişi hakkında güvenlik tedbirlerine hükmolunur. Suçu bizzat işleyen yetkililer ise suçun faili olarak cezalandırılacaktır.

3.2.1.3. Mağdur

Suçun mağduru kişisel verinin ilişkili olduğu gerçek kişidir. Tüzel kişiler suçun mağduru olamaz, ancak suçtan zarar gören olabilir. Bu suç mağdur bakımından da bir özellik arz etmemektedir. Kişisel Verilerin Kaydedilmesi suçu bağlamında yaptığımız detaylı açıklamalar burada da geçerlidir.

3.2.1.4. Fiil

Bu suç kişisel verileri ele geçirme, verme veya yayma hareketlerinden birinin gerçekleştirilmesiyle işlenebilir. Bu hareketlerden birinin gerçekleştirilmesi yeterlidir. Dolayısıyla bu suç seçimlik hareketli bir suçtur. Seçimlik hareketlerden biri gerçekleştirildikten sonra aynı konu üzerinde başka bir seçimlik hareketin daha gerçekleştirilmesi yeni bir suç oluşturmaz. Üç seçimlik hareket birlikte de gerçekleştirilse tek suç oluşacaktır. Fakat bu husus cezanın belirlenmesinde dikkate alınacaktır⁴⁷⁵.

Herhangi bir neticenin gerçekleşmesi aranmadığından bu suç sırf hareket suçudur. Herhangi bir zararın gerçekleşmesine de gerek bulunmadığı için suç bir tehlike suçudur. Suçun oluşması için herhangi bir somut tehlikenin gerçekleşip gerçekleşmediği de araştırılmayacaktır. Dolayısıyla suç bir soyut tehlike suçudur⁴⁷⁶.

⁴⁷⁵ **Epözdemir, Rezan** (2019) ‘Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme Suçu’ Terazi Hukuk Dergisi, C:14, S:151, (s.528-544), s.531. **Korkmaz**, s.448

⁴⁷⁶ **Epözdemir**, s.532. Suçun neticesiz bir suç olduğu ve soyut tehlike suçu olduğu Yargıtay kararlarında da ifade edilmektedir. Bkz. Ceza Genel Kurulu, E. 2012/1510, K. 2014/331, K.T. 17.06.2014.

Kişisel verileri verme, yayma veya ele geçirme fiillerinin “*tamamen veya kısmen otomatik yollarla veya bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla*”⁴⁷⁷ gerçekleştirilmesi halinde KVKK kapsamında bir veri işlemekten söz edileceği için KVKK hükümleri uygulama alanı bulacaktır. Bu fiillerin otomatik olmayan yollarla ve bir veri kayıt sisteminin de parçası olmadan işlenmesi halinde KVKK kapsamında bir veri işlemekten söz edilemeyeceği için KVKK hükümleri uygulanmayacaktır. Fakat bu fiiller suç oluşturmaya devam edecektir. Suçun fiil unsurunun gerçekleşebilmesi için KVKK kapsamına giren bir fiilin bulunması şart değildir⁴⁷⁸. Fiil unsurunun KVKK kapsamına giren bir fiilden oluşması hukuka uygunluk sebeplerinin belirlenmesinde rol oynamaktadır⁴⁷⁹.

Verme, yayma ve ele geçirme fiillerinin gerçekleştirilebilmesi için kişisel verilerin kaydedilmiş halde bulunmasının şart olup olmadığı tartışma konusu olmuştur. Bir görüşe göre kişi ancak elinde bulundurduğu bir şeyi verebilir veya yayabilir⁴⁸⁰. Verme ve yayma bir araç kullanılarak gerçekleştirilmelidir⁴⁸¹. Dolayısıyla bu verilerin daha önce kaydedilmiş olması gerekir. Ele geçirme de ancak kaydedilmiş bir veri üzerinde gerçekleştirilebilir. Kaydedilmemiş bir veriye salt duyu organları ile vakıf olunması, hafızada tutulup bir başkasına açıklanması bu suçu oluşturmaz. Yargıtay kararlarında da 2019 yılına kadar bu görüşün etkisi gözlemlenmiştir⁴⁸². Ancak Yargıtay 2019 yılındaki bir kararında görüş değişikliğine gitmiş, kişisel verilere salt duyu organları ile vakıf olunmasını da ele geçirme kapsamında değerlendirmiştir⁴⁸³. Kanaatimizce kişisel verilerin

⁴⁷⁷ KVKK m.3/1-e

⁴⁷⁸ Aynı yöndeki açıklamalar için bkz. **Maden**, s.94. Börekçi, KVKK kapsamına girmeyen fiillerin de TCK kapsamına girebileceğini, fakat bu durumun suçun uygulama alanını çok genişlettiğini, TCK’daki fiillerin KVKK kapsamına girmeyen durumları kapsam dışı bırakacak şekilde tekrar düzenlenmesi gerektiğini savunmaktadır. Bkz. **Börekçi**, s.90-91.

⁴⁷⁹ Dülger de KVKK’daki hukuka uygunluk sebeplerinin yalnızca KVKK kapsamına giren fiiller için uygulanacağı kanaatindedir. Bkz. **Dülger** (2020), s.712.

⁴⁸⁰ **Hafizoğulları / Özen**, s.271.

⁴⁸¹ **Özbek / Doğan / Bacaksız**, Ceza Özel, s.608.

⁴⁸² “...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 ise de, kişisel verilerin kaydedilmeden önce öğrenilmesi, hafızada tutulan kişisel verilerin başkalarına açıklanması, kişisel verilere salt duyu organları aracılığıyla vakıf olunması, ancak TCK’nın 134. maddesinin 1. fıkrasının 1. cümlesinde düzenlenen özel hayatın gizliliğini ihlal suçu kapsamında değerlendirilebilir.” 12. CD., E. 2017/12083, K. 2018/2539, K.T. 7.3.2018

⁴⁸³ “Bu noktada belirtmek gerekir ki, 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

verilmesi, yayılması veya ele geçirilmesi için kişisel verinin daha önce kayıtlı olarak bulunması şart değildir. Doktorun hastası hakkında vakıf olduğu bilgileri alakasız üçüncü bir kişiye söz ile açıklaması durumunda kişisel verileri verme söz konusu olduğu için suç oluşacaktır⁴⁸⁴. Bir kişinin telefonunu rızası olmadan alarak arama geçmişine bakan kişi bunları herhangi bir yere kaydetmese de verileri hukuka aykırı olarak ele geçirmiştir⁴⁸⁵. Bir veriyi büyük bir kalabalığa karşı konuşma yaparken söz ile açıklayan kişi kişisel verileri yaymıştır.

Kişisel verileri vermek veya yaymak için önce kaydetmek gerekmediği gibi ele geçirmek de şart değildir. Öğretide verileri ele geçirmeden yaymaya yarayacak yapay zekâ algoritmalarının geliştirilebileceği, bir virüsün kişisel veri toplayıp üçüncü kişilerle otomatik şekilde paylaşacak şekilde programlanabileceği ifade edilmektedir. Bu tür durumlarda virüsü programlayan ve gönderen kişinin veriler üzerinde doğrudan bir hakimiyeti oluşmamaktadır. Kişi bu verilere hiç hâkim olmadan doğrudan üçüncü kişilere ileteceği bir program tasarlayabilir⁴⁸⁶. Esasen verilerin ele geçirilmesi yahut yayılması için mutlaka kaydedilmiş halde bulunması gerektiği düşüncesi kanun metninden ulaşılabilecek bir sonuç da değildir. Kanaatimizce bu yorum gerçekleşebilecek somut olaylar üzerinde düşünen yazarların kaydedilmemiş bir veriyi ele geçirmeyi, ele geçirilmemiş yahut elde bulundurulmayan bir veriyi yaymayı tahayyül edememelerinden, bunu somut olarak imkansız görmelerinden kaynaklanmıştır⁴⁸⁷. Madde gerekçesinin de bu yoruma sebebiyet verebilecek ifadeler içerdiğini kabul etmek gerekir⁴⁸⁸. Fakat kanaatimizce bu suçun oluşması için kişisel verilerin daha önce kaydedilmiş olması şart olmadığı gibi, verme ve yayma için elde bulundurma da şart değildir.

Ele geçirme fiilinin kapsamı ve ifade ettiği anlam tartışma konusudur. Esasen bu fiilin kapsamının zor tespit edilmesinin en büyük sebebi kaydetme fiili ile olan

geçirme” kapsamında değerlendirilebileceği gibi, kişisel verilerin kaydedilmeden önce öğrenilmesi, kişisel verilere salt duyu organları aracılığıyla vakıf olunması da aynı kapsamda değerlendirilmelidir.” 12. CD., E. 2018/8152, K. 2019/4886, K.T. 10.4.2019.

⁴⁸⁴ Koca / Üzülmaz (2020), s.578.

⁴⁸⁵ 12. CD., E. 2018/8152, K. 2019/4886, K.T. 10.4.2019.

⁴⁸⁶ Bu konuda detaylı açıklamalar için bkz. Börekeci, s.81-82.

⁴⁸⁷ Dülger kişisel verileri verme veya yayma suçunun oluşabilmesi için önce verilerin kaydedilmesi gerektiği şeklindeki görüşünden vazgeçtiğini ifade etmektedir. Yukarıda zikrettiğimiz yargıtay kararlarındaki değişimin ve teknolojik gelişmelerin bu görüş değişikliğinde etkili olduğunu belirtmektedir. Bkz. Dülger (2020), s.736.

⁴⁸⁸ Gereke: “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.”

benzerliğidir. Ele geçirme fiili çoğu zaman kaydetme suretiyle gerçekleştirilmektedir. Fakat bu fiiller ayrı maddelerde ayrı cezaları gerektirecek şekilde düzenlendiğine göre kanun koyucu bu iki fiili birbirinden tamamen ayrı görmektedir. Öyleyse bu iki fiili birbirinden ayıracak, somut olayda hangi fiilin gerçekleştiğini tespit etmemizi sağlayacak kriterlere ihtiyaç vardır.

Ele geçirme fiili öğretide farklı şekillerde tanımlanmaktadır. Hafizoğulları ve Özen'e göre kişisel verileri ele geçirmek verileri yakalamak ve onların sahibi olmaktır⁴⁸⁹. Kangal'a göre ele geçirmek bir başkasının elinde bulunan kişisel veriyi elde etmektir⁴⁹⁰. Maden'e göre ele geçirme fail tarafından kişisel verinin hakimiyet altına alınmasıdır⁴⁹¹. Özbek ele geçirme fiili ile ilgili bir tanım yapmamakta, kaydetme dışında kalan durumların ele geçirme anlamına geleceğini ifade etmektedir⁴⁹². Koca ve Üzülmmez'e göre ise ele geçirme *“verinin ilişkili olduğu kişinin rızasına aykırı olarak veya hukuka aykırı şekilde elde edilmesi”* anlamına gelir. Koca ve Üzülmmez'in tanımına yaklaşık olarak katılıyoruz. Kanaatimizce ele geçirme failin **erişim hakkı bulunmayan**⁴⁹³ bir kişisel veriye erişmesi, vakıf olması, bu veriyi elde etmesi, kaydetmesi veya herhangi bir şekilde hakimiyeti altına sokması olarak kabul edilebilir. Bu saydığımız hareketlerden her biri ele geçirme kavramının kapsamına girer. Şayet failin hukuka uygun şekilde erişebildiği veya vakıf olduğu bir veri söz konusu ise, failin bunu hukuka aykırı şekilde kaydetmesi durumunda kişisel verilerin kaydedilmesinden söz edilecektir. Yani erişim hakkı bulunan bir veriyi hukuka aykırı olarak kaydeden kişi TCK m.135 kapsamında kaydetmeden sorumlu tutulacakken, erişim hakkı bulunmayan bir kişisel veriyi kaydeden kişi TCK m.136 kapsamında ele geçirmeden sorumlu tutulacaktır. Koca ve Üzülmmez verileri ele geçirmeyi hırsızlığa benzetmekte ve veri hırsızlığı olarak adlandırmaktadır⁴⁹⁴. Verileri yayma ve vermeyi ise güveni kötüye kullanmaya benzetmektedir⁴⁹⁵. Kanaatimizce bu benzetme kaydetme ve ele geçirme arasındaki ilişkiyi daha iyi açıklamaktadır. Kaydetme fiili güveni kötüye kullanma suçuna benzemekten, ele geçirme fiili hırsızlığa benzemektedir.

⁴⁸⁹ Hafizoğulları / Özen, s.271.

⁴⁹⁰ Kangal, s.112.

⁴⁹¹ Maden, s.108.

⁴⁹² Özbek / Doğan / Bacaksız, Ceza Özel, s.609.

⁴⁹³ Akdağ, s.135.

⁴⁹⁴ Koca / Üzülmmez (2020), s.579.

⁴⁹⁵ Koca / Üzülmmez (2020), s.577.

Ele geirme fiili kişisel verilerin yazılı olduėu belgenin bulunduėu yerden hukuka aykırı şekilde alınması şeklinde gerekleştirebileceėi gibi bilişim sistemine girip oradaki verileri bir belleėe kaydetme şeklinde de gerekleştirebilir⁴⁹⁶. Verinin ieriėinin bakma, okuma veya dinleme suretiyle öğrenilmesi halinde de ele geirme suu oluşabilir⁴⁹⁷. Yargıtay da yukarıda zikrettiėimiz bir kararında kişisel verilere salt duyu organlarıyla vakıf olmayı ele geirme olarak kabul etmiştir⁴⁹⁸. Elbette diėer yollarla ele geirmede olduėu gibi duyu organları ile vakıf olarak ele geirmede de suun diėer unsurlarının da varlıėı şarttır.

Kişisel veriler genellikle kaydedilerek ele geirilmektedir. Örneėin bir bilişim sistemine izinsiz girerek verileri kendi USB belleėine aktaran kişi verileri kaydetmek suretiyle ele geirmektedir. Verilerin kaydetme suretiyle ele geirildiėi durumlarda fail yalnızca kişisel verileri ele geirme suundan cezalandırılacak, ayrıca kaydetme suundan cezalandırılmayacaktır⁴⁹⁹.

Ele geirme fiilinin hem gerekleşme biimi olarak hem de haksızlık ieriėi olarak diėer seçimlik hareketlere yakın olmadığı, bu fiilin kaydetme fiiline daha yakın olduėu, bu sebeple m.136’dan çıkarılarak m.135’e seçimlik hareket olarak eklenmesi gerektiėi savunulmaktadır⁵⁰⁰. Kanaatimizce ele geirmenin m.136’da düzenlenmesi kanun koyucunun kişisel veriyi hukuka aykırı olarak veren ve hukuka aykırı olarak alan kişiyi denk görmesinden, bunlar arasında bir ayırım yapmak istememesinden kaynaklanmıştır.

Su tipinde yer alan diėer bir seçimlik hareket **verme** fiilidir. Verme fiili sözlükte “*üzerinde, elinde veya yakınında olan bir şeyi birisine eriştirmek, iletmek; düşünce veya bilgi anlatan şeyleri başkalarına iletmek, bildirmek*” şeklinde tanımlanmaktadır⁵⁰¹. Bu su tipi açısından vermek fiili üçüncü bir kişiye kişisel veriyi iletmeyi, aktarmayı, verileri o kişinin bilgisine sunmayı veya verilerin kayıtlı bulunduėu dosyayı-belleėi üçüncü kişiye teslim etmeyi ifade eder. Verme fiilinin gerekleşmesi için verilerin üçüncü kişi tarafından

⁴⁹⁶ Dölger (2020), s.739.

⁴⁹⁷ Maden, s.108.

⁴⁹⁸ 12. C.D., E. 2018/8152, K. 2019/4886, K.T. 10.4.2019.

⁴⁹⁹ Koca / Üzülmöz (2020), s.580.

⁵⁰⁰ Koca / Üzülmöz (2020), s.577.

⁵⁰¹ TDK Güncel Türke Sözlük, (<https://sozluk.gov.tr/>) s.e.t. 17.01.2023

öğrenilebilir hale gelmesi yeterlidir. Üçüncü kişinin verilerin içeriğine vakıf olup olmadığı, verileri inceleyip incelemeyeceği, öğrenip öğrenmediği ayrıca araştırılmayacaktır⁵⁰².

Verme fiili karşı tarafında bir de alanın olduğu iki taraflı bir fiildir. Kişisel verileri alan kişi eğer kasten hareket ediyorsa ve alan kişi bakımından bir hukuka uygunluk sebebi yoksa verileri ele geçirme suçunu işlemiş olur. Kusurluluğu ortadan kaldıran bir durum da yoksa cezalandırılır. Yargıtay önüne gelen bir olayda hem ayrıldığı kız arkadaşının numarasını arkadaşına veren kişinin ve hem de numarayı alan kişinin kişisel verileri verme, yayma veya ele geçirme suçundan mahkûm edilmesi gerektiğine karar vermiştir⁵⁰³. Bu tür olaylarda veriyi veren kişinin veya alan kişinin kastı veya kusurluluğu ortadan kaldıran bir hata hali içerisinde olup olmadığı titizlikle incelenmelidir.

Verinin verildiği kişi bir gerçek kişi olabileceği gibi bir tüzel kişi de olabilir. İki durumda da verme fiili gerçekleşmiştir. Bir görüşe göre verileri alan kişinin gerçek kişi olması zorunludur⁵⁰⁴. Ancak bizim de katıldığımız görüşe göre kişisel verilerin tüzel kişiye verilmesi durumunda da veren bakımından suç oluşacaktır. Yargıtayın uygulaması da bu yöndedir⁵⁰⁵.

Verme fiiline konu olan verilerin hukuka aykırı veya hukuka uygun yollarla ele geçirilmiş olmasının bir önemi yoktur. Önemli olan verme fiilinin hukuka aykırı olmasıdır⁵⁰⁶.

Suç tipinde yer alan bir diğer seçimlik hareket ise **yayma** fiilidir. Yayma fiili sözlükte “*birçok kimseye duyurmak*” olarak tanımlanmaktadır⁵⁰⁷. Esasen hem yayma fiili hem de verme fiili verileri üçüncü kişi veya kişilere ulaştırmak şeklinde gerçekleşmektedir. Yayma fiilini verme fiilinden ayıran husus; verme fiilinin belirli bir kişi veya kişilere yönelik olmasına karşın yayma fiilinin hedef gözetmeden çok sayıda kişiye veri

⁵⁰² Sağlam, s.101.

⁵⁰³ 12. CD., E. 2014/607, K. 2014/16665, K.T. 7.7.2014.

⁵⁰⁴ Koca / Üzülmaz (2020), s.578.

⁵⁰⁵ “Kişisel verileri bir başkasına verme” seçimlik hareketinde, maddede geçen “başkası” gerçek bir kişi olabileceği gibi tüzel kişi de olabilecek, veriler bu kişilere elden, posta ya da internet üzerinden elektronik posta ile vb. şekillerde verilebilecektir.” Ceza Genel Kurulu, E. 2017/829, K. 2017/363, K.T. 4.7.2017

⁵⁰⁶ Soyaslan (2020), s.364. Aynı yönde Ceza Genel Kurulu Kararı, E. 2017/829, K. 2017/363, K.T. 4.7.2017

⁵⁰⁷ TDK Güncel Türkçe Sözlük, (<https://sozluk.gov.tr/>) s.e.t. 17.01.2023.

ulaştırmayı amaçlamasıdır⁵⁰⁸. Yayma fiili için verilerin içeriğinin çok sayıda kişinin erişimine sunulması gerekmektedir⁵⁰⁹. Bu fiilin yazılı, sözlü, görsel veya sanal yollarla işlenebilmesi mümkündür⁵¹⁰. Örneğin kişisel verileri bir çok kişiye toplu e posta olarak göndermek, bir internet sitesinde yayınlamak, afiş veya broşür şeklinde dağıtmak, herkes tarafından görülebilir bir panoya asmak gibi eylemler yayma olarak kabul edilebilir. Verilerin kaç kişiye verilmesinin verme, kaç kişiye verilmesinin yayma olarak kabul edileceği tartışmasına girmeye lüzum yoktur. Zira verme veya yayma fiillerinden hangisinin gerçekleştiğini tespit etmenin herhangi bir önemi yoktur. İki hareketten birinin varlığı fiil unsurunun yerine gelmesi için yeterlidir ve iki fiil için de aynı ceza öngörülmüştür.

Verme fiilinde olduğu gibi yayma fiilinde de kişisel verilerin muhatapları tarafından öğrenilmesi şart değildir. Kişisel verinin içeriğinin birden fazla kişi tarafından öğrenilebilir kılınması yeterlidir⁵¹¹.

Bu fiillerin ihmali hareketle işlenebilmesi de mümkündür. Örneğin hukuka uygunluk sebeplerinden birine dayanarak otomatik yollarla veri aktarımı yapan bir kişi hukuka uygunluk sebepleri ortadan kalktığında veri aktarımını durdurmak zorundadır. Hukuka uygunluk sebebinin kalktığını ve artık veri aktarımının haksızlık teşkil edeceğini bilmesine rağmen otomatik işlemlere müdahale etmeyen, bu suretle verilerin verilmesini veya yayılmasını sağlayan kişi ihmali hareketle suç işlemiş olur.

Bir görüşe göre toplumda geniş müsamaha ile karşılanan veya günlük hayatın bir parçasını oluşturan bir fiil söz konusu olduğunda, bu fiili gerçekleştiren kişilerin haksızlık bilinci taşıyarak hareket ettiklerinin özel olarak tespit edilmesi gerekir⁵¹². Kanaatimizce kişilerin haksızlık yanılgılarının (haksızlık bilinci taşımamalarının) kusurluluğu ortadan kaldırabilmesi için bu yanılgının kaçınılmaz olması gerekmektedir. TCK ancak kaçınılmaz haksızlık yanılgısı halinde kişiye ceza verilmeyeceğini kabul etmekte, yanılgının kaçınılabilir olması durumunda failin cezalandırılmasını öngörmektedir (TCK m.30/4). Suçun kanuni tanımında hukuka aykırılık bilincine özellikle işaret edilen bu gibi suç tipleri

⁵⁰⁸ Kangal'a göre verilerin birden fazla kişiye verilmesi yayma anlamına gelir. Kişilerin belirli ya da belirsiz sayıda olmasının bir önemi yoktur. **Kangal**, s.110.

⁵⁰⁹ **Akdağ**, s.131.

⁵¹⁰ **Kangal**, s.110.

⁵¹¹ **Akdağ**, s.131, **Sağlam**, s.107, **Kangal**, s.112.

⁵¹² **Koca / Üzülmaz** (2020), s.579.

bakımından özel bir uygulama yapmaya yürürlükteki hükümler imkân vermemektedir. Bu tür suçlarda failin, ancak doğrudan haksızlık bilinci ile hareket etmesi halinde cezalandırılabilmesini sağlayacak bir hukuki düzenlemeye ihtiyaç olduğu kanaatindeyiz.

3.2.2. Manevi Unsur

Bu suç manevi unsur bakımından da bir özellik arz etmemektedir. Suç doğrudan kastla işlenebilir. Kanuni tanımda “*hukuka aykırı olarak*” ibaresinin bulunması sebebiyle suçun olası kastla işlenip işlenemeyeceği öğretide tartışma konusudur. Fakat kanaatimizce TCK’nın sistematığı suçun olası kast ile işlenmesini mümkün kılmaktadır. Bu konuda detaylı açıklamalar kişisel verilerin kaydedilmesi suçu bağlamında yapılmıştır.

Suçun taksirle işlenmesi mümkün değildir. Failin özel bir saikle hareket etmesi aranmamaktadır.

3.2.3. Hukuka Aykırılık Unsuru

Suçun oluşması için bütün maddi unsurlar gerçekleştikten sonra hukuka aykırılık unsurunun da gerçekleşmesi gerekir. Şayet somut olayda bir hukuka uygunluk sebebi bulunmuyorsa hukuka aykırılık unsuru da gerçekleşmiş olur ve suç oluşur.

Kişisel verilerin kaydedilmesi suçunda gündeme gelebilecek olan hukuka uygunluk sebepleri bu suç için de gündeme gelebilecektir. Dolayısıyla önceki suç tipi için yaptığımız açıklamalar burada da geçerlidir.

Burada ayrıca belirtilmesi gereken husus mahkeme tarafından kişisel verilerin istenmesi halinde kanunun hükmünü icra veya amirin emrini ifa hukuka uygunluk sebebinin sır saklama yükümlülüğüne sahip bazı meslek gruplarına uygulanmasının mümkün olmayacağıdır. CMK’nın 46ncı maddesinin avukatların, avukatların yanında çalışan kişilerin, sağlık mesleği mensuplarının, mali müşavirlerin ve noterlerin görevleri

dolayısıyla öğrendikleri bilgilerle ilgili olmak üzere tanıklıktan çekinme haklarının oldukları ifade edilmiştir. Mahkemenin bu kişilerden bilgi talep etmesi durumunda şayet sanığın tanıklığa rızası yoksa bu kişilerin bilgi vermeleri kanunun hükmünü veya amirin emrini ifa hukuka uygunluk sebebi kapsamına girmeyecektir. Diğer bir ifadeyle CMK m.46 kapsamında tanıklıktan çekinme hakkı bulunanların sanığın rızası olmadan tanıklık yapmaları durumunda TCK m.136'da düzenlenen kişisel verileri hukuka aykırı olarak verme, yayma veya ele geçirme suçundan sorumlu tutulacakları kabul edilmektedir⁵¹³.

Üçüncü bölümün başında ve önceki suç tipinde değindiğimiz üzere; bu suçlarda hangi hukuka uygunluk sebeplerinin uygulanabileceğini tespit edebilmek için öncelikle fiilin KVKK kapsamına girip girmediğini tespit etmek gerekir. KVKK kapsamına giren bir fiil söz konusuysa öncelikle KVKK kapsamında yer alan veri işleme şartlarından birinin somut olayda gerçekleşip gerçekleşmediğine bakılmalıdır. Bu şartlardan hiçbiri gerçekleşmemişse genel hukuka uygunluk sebeplerinden birinin veri işlemeyi hukuka uygun hale getirip getirmediği araştırılmalıdır⁵¹⁴. Genel hukuka uygunluk sebepleri bakımından da fiili hukuka uygun hale getirecek bir durum yoksa hukuka aykırılık unsuru gerçekleşir ve suç oluşur.

Somut olayda KVKK kapsamına girmeyen bir fiil söz konusuysa KVKK hükümlerine başvurulmayacak, genel hukuka uygunluk sebepleri çerçevesinde değerlendirme yapılacaktır.

KVKK kapsamındaki hukuka uygunluk sebepleri ve genel hukuka uygunluk sebepleri bir önceki suç tipinde detaylıca incelendiği için burada tekrara düşmemek adına bunlara değinilmemiştir.

⁵¹³ Hakeri, s.254.

⁵¹⁴ Ancak genel hukuka uygunluk sebeplerinden rızanın, KVKK kapsamındaki fiilleri hukuka uygun hale getirmeyeceğini unutmamak gerekir. KVKK kapsamına giren durumlarda özel düzenleme bulunduğu için sadece açık rıza kabul edilebilir.

3.3. Nitelikli Haller

Bu suça ilişkin nitelikli haller TCK m.136/2’de ve TCK m.137’de düzenlenmiştir. TCK m.136/2’de düzenlenen nitelikli hâl suçun konusuna ilişkin iken, m.137’de düzenlenen nitelikli haller failin şahsına ve fiilin işleniş şekline ilişkindir.

Suçun konusuna ilişkin nitelikli halin düzenlendiği m.136/2 hükmü şu şekildedir; *“Suçun konusunun, Ceza Muhakemesi Kanununun 236ncı maddesinin beşinci ve altıncı fıkraları uyarınca kayda alınan beyan ve görüntüler olması durumunda verilecek ceza bir kat artırılır.”*

Ceza Muhakemesi Kanunu’nun 236ncı maddesinin beşinci ve altıncı fıkralarında vücuda organ veya sair bir cisim sokulması suretiyle gerçekleştirilen cinsel saldırı (TCK m.102/2) ve cinsel istismar (TCK m.103/2) mağduru kişi ve çocukların ifadelerine ilişkin beyan ve görüntülerinin kayda alınması düzenlenmektedir. Bu kayıtların kişisel veri olduğunda şüphe yoktur. Suçun konusunun bu fıkralar uyarınca kayda alınan kişisel verilerden müteşekkil olması durumunda faile verilecek ceza bir kat artırılabacaktır. Bu nitelikli halin meydana gelmesi için failin kamu görevlisi olması gerekmez.

Failin şahsına ve fiilin işleniş şekline ilişkin nitelikli hallerin düzenlendiği m.137 hükmüne göre suçun *“kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle”* veya *“belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle”* işlenmesi durumlarında verilecek ceza yarı oranında artırılabacaktır. Bu nitelikli hale ilişkin detaylı açıklamalar kişisel verilerin kaydedilmesi suçu bağlamında yapılmıştır.

Son olarak; TCK m.135/2’de sadece kişisel verilerin kaydedilmesi suçunda uygulanacak şekilde düzenlenen nitelikli halin (özel nitelikli kişisel verilere ilişkin nitelikli hâl) m.136’yı ve m.138’i de kapsar hale getirilmesi gerektiğini düşünüyoruz. Zira suçun konusunu özel nitelikli kişisel verilerin oluşturması halinde ceza artırımı yapılması, özel nitelikli kişisel verilerin kaydedilmesinin soyut olarak diğer kişisel verilerin kaydedilmesinden daha ciddi bir tehlike ve haksızlık oluşturduğu düşüncesine dayanmaktadır. Şayet kişisel verilerin kaydedilmesi halinde suçun konusunun bu kategorilere ilişkin olması özellik arz ediyorsa, kişisel verilerin verilmesi, yayılması, ele

geçirilmesi ve yok edilmemesi durumlarında da suçun konusunun hassas verilerden oluşması özellik arz etmelidir.

3.4. Suçun Özel Görünüş Biçimleri

3.4.1. Teşebbüs

Kişisel verilerin kaydedilmesi suçu gibi kişisel verileri verme, yayma veya ele geçirme suçu da bir sırf hareket suçu olduğu için teşebbüs ancak icra hareketlerinin bölünebilir olduğu durumlarda mümkündür. Bu sebeple bu suçlarda teşebbüs ile karşılaşılması zordur. Fakat yine de teşebbüsün mümkün olduğu kabul edilmelidir. Örneğin posta ile gönderilen bir verinin herhangi bir kişi tarafından erişilebilir hale gelmeden yolda aracın yanması sonucu yok olması halinde teşebbüs söz konusu olabilir.

3.4.2. İştirak

Bu suç iştirak açısından bir özellik arz etmemektedir. İştirake ilişkin genel hükümler uygulanacaktır⁵¹⁵. Ancak bu suçun bir görünüşte özgü suç olduğuna dikkat etmek gerekmektedir. Kamu görevlisi A ile özel bir sıfatı bulunmayan B fiil üzerinde ortak hakimiyet kurarak bu suçu işlediklerinde A m.137'deki nitelikli halden sorumlu tutulacaktır. B'nin m.137'de fail için aranan özel nitelikleri taşıması sebebiyle m.137 bakımından fail olabilmesi mümkün değildir. B m.137'den ancak azmettiren veya yardım eden olarak sorumlu tutulabilir. Fakat B aynı zamanda suçun temel şeklinin (m.136) failidir. Bu durumda B'nin sorumluluğu *failliğin şerikliğe asliliği*⁵¹⁶ kuralı gereğince yalnızca m.136'dan olacaktır⁵¹⁷.

⁵¹⁵ Dülger (2020), s.748.

⁵¹⁶ Özgenç, s.736.

⁵¹⁷ Detaylı anlatım için kişisel verilerin kaydedilmesi suçu bağlamında yapılan açıklamalara bakınız.

3.4.3. İçtima

Bu suç için de madde metninde içtimaa ilişkin özel bir hüküm yer almamaktadır. Genel hükümlere göre değerlendirme yapılacaktır. Şartlarının gerçekleşmesi durumunda zincirleme suç, aynı neviden fikri içtima ve farklı neviden fikri içtima hükümleri uygulanabilecektir. Yine bazı durumlarda bu suç ile diğer suçlar arasında görünüşte içtima ilişkisi bulunabilir. Görünüşte içtima ilişkisinin bulunduğu hallerde tek suçun varlığından söz edilebileceği için içtima hükümlerine başvurulmayacak, görünüşte içtima ilkelerine göre belirleme yapılacaktır.

Bir suç işleme kararının icrası kapsamında aynı kişinin verilerini farklı zamanlarda veren, yayan veya ele geçiren kişi hakkında zincirleme suç hükümleri uygulanabilir.

Tek bir fiil ile birden fazla kişinin verisini ele geçiren, veren veya yayan kişi hakkında aynı neviden farklı içtima hükümleri uygulanacaktır. Bu durumla uygulamada sıklıkla karşılaşılabilir. Örneğin fail içerisinde pek çok kişinin verilerinin bulunduğunu bir dosyayı ele geçirdiğinde aynı neviden fikri içtima söz konusu olacaktır.

Bu suç için farklı neviden fikri içtimanın gerçekleşmesi de mümkündür. Failin fiili TCK m.136'nın yanında başka maddelerde düzenlenmiş bir suçu veya suçları da oluşturuyorsa farklı neviden fikri içtima gündeme gelecektir. Ancak farklı neviden fikri içtima değerlendirmesi yaparken görünüşte içtima halinin bulunup bulunmadığına dikkat edilmelidir. Zira görünüşte içtimanın varlığı durumunda tek suç vardır ve içtima hükümleri uygulanamayacaktır. Hangi suçun olduğu görünüşte içtima kurallarına göre tespit edilecektir. Aşağıda TCK m.136 ile aralarında fikri içtima ilişkisi bulunan suçlar ve görünüşte içtima ilişkisi bulunan suçlar incelenecektir.

Haberleşmenin gizliliğini ihlal başlığını taşıyan TCK m.132 aşağıdaki şekildedir;

“(1) Kişiler arasındaki haberleşmenin gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Bu gizlilik ihlali haberleşme içeriklerinin kaydı suretiyle gerçekleşirse, verilecek ceza bir kat artırılır.

(2) Kişiler arasındaki haberleşme içeriklerini hukuka aykırı olarak ifşa eden kimse, iki yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(3) Kendisiyle yapılan haberleşmelerin içeriğini diğer tarafın rızası olmaksızın hukuka aykırı olarak alenen ifşa eden kişi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Ifşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur.”

Birinci fıkranın birinci cümlesinde haberleşmenin gizliliğinin ihlal edilmesinden bahsedilmektedir. Bu suç haberleşmede kullanılan aracın özelliğine göre haberleşme içeriğinin okunması ya da dinlenilmesi suretiyle gerçekleştirilebilir⁵¹⁸. Haberleşmenin gizliliğini ihlalin, içeriğin kaydedilmesi suretiyle gerçekleştirilmesi ise ikinci cümlede cezayı artıran nitelikli hal olarak düzenlenmiştir. Kişilerin haberleşme içerikleri ancak bir kişiden sadır olmuş ses, yazı veya sembol olabilir. Kişilerin seslerinin de kişisel veri olarak kabul edilmesi konusunda tereddüt yoktur. Kişilerin bir başkasına iletişim araçları vasıtasıyla gönderdikleri yazılar ve semboller de kanaatimizce kişisel veri olarak kabul edilmelidir. Buradan yola çıkarak; birinci fıkranın birinci cümlesindeki tanıma uygun olarak haberleşmenin gizliliğinin ihlal edildiği **her durumda** (mektubun izinsiz okunması, e posta içeriklerinin okunması vs.) aynı zamanda kişisel verilerin de ele geçirildiği söylenebilir. Kişisel verilerin ele geçirilmesi ise TCK m.136’da düzenlenmiştir. Ancak kişisel verilerin ele geçirildiği her durumda haberleşmenin gizliliğinin ihlal edildiğinden bahsedilemeyecektir. Kanaatimizce haberleşmenin gizliliğini ihlal suçu, kişisel verilerin ele geçirilmesi suçunun bütün unsurlarının gerçekleşmesi ve buna ilave olarak bazı ek hususiyetlerin de bulunması halinde meydana gelebilmektedir. Bu ek hususiyet kişisel verilerin kişiler arasındaki gizli haberleşmenin içeriğine dair olmasıdır. Sonuç olarak; ele geçirilen kişisel verilerin kişiler arasındaki haberleşme içeriklerine ilişkin olması durumunda özel normun önceliği ilkesi gereği TCK m.132/1 c.1 hükmü uygulanacaktır.

Aynı gerekçelerle; TCK m.132/1’in ikinci cümlesi ile de verileri hukuka aykırı olarak verme veya ele geçirme suçu (TCK m.136) arasında genel norm - özel norm ilişkisi bulunmaktadır⁵¹⁹. Hukuka aykırı olarak ele geçirilmek suretiyle kaydedilen kişisel verilerin

⁵¹⁸ Mesajla yapılan bir haberleşmede okuma söz konusu olacakken ses ile yapılan bir haberleşmede dinleme söz konusu olacaktır.

⁵¹⁹ Kaydedilen verilere yetkisiz bir erişim söz konusu olduğu için TCK m.135 anlamında kaydetmeden değil TCK m.136 kapsamında ele geçirmeden söz edilir. Ancak her halükârda TCK m.132/1-c.2 özel norm olduğu için ne TCK m.135’in ne de TCK m.136’nın bu durumda uygulanma imkânı bulunmamaktadır.

kişilerin haberleşme içeriklerine ilişkin olması durumunda özel normun önceliği ilkesi gereği TCK m.132/1-c.2 hükmü uygulanacaktır.

Hukuka aykırı olarak ifşa edilen kişisel verilerin kişiler arasındaki haberleşme içeriklerine ilişkin olması durumunda özel normun önceliği ilkesi gereği TCK m.136 değil m.132/2 uygulanmalıdır.

Kendisiyle yapılan haberleşme içeriğini karşı tarafın rızası olmadan ifşa eden kişi hakkında da yine özel normun önceliği ilkesi gereği TCK m.136 değil m.132/3 hükmü uygulanacaktır.

Şayet 132nci maddede düzenlenen haberleşmenin gizliliğini ihlal suçu ile TCK m.136 hükümleri arasında özel norm - genel norm ilişkisinin kurulamayacağı kabul edilirse bir fiil ile iki suçun oluştuğu kabul edilecek ve farklı neviden fikri içtima kuralları uygulanacaktır. Farklı neviden fikri içtimanın varlığı kabul edildiğinde somut olaydaki suçlardan en ağır cezayı gerektiren hangisi ise yalnızca o suçtan ceza verilecektir. Bu durumda TCK m.132/1-c.1 ile TCK m.136'dan daha ağır cezayı gerektiren TCK m.136 uygulanacak, TCK m.132/3 ile TCK m.136'dan ise daha ağır cezayı gerektiren TCK m.136 uygulanacaktır. Diğer durumlar için de görünüşte içtima kuralları yerine fikri içtima kuralları uygulanacak olsa da ulaşılan sonuç değişmeyecektir. Ancak biz TCK m.132 ile TCK m.136 arasında özel norm - genel norm ilişkisi bulunduğunu düşündüğümüz için fikri içtima hükümlerinin uygulanmayacağı kanaatindeyiz⁵²⁰.

Kişiler arasındaki konuşmaların dinlenilmesi ve kayda alınması başlığını taşıyan TCK m.133'ün birinci ve üçüncü fıkraları aşağıdaki şekildedir⁵²¹;

⁵²⁰ TCK m.132 ile TCK m.136 arasında tüketen norm – tüketilen norm ilişkisi bulunduğu şeklindeki görüş için bkz. **Birtek, Fatih** (2012) Haberleşmenin Gizliliğini İhlal Suçları, 1. Baskı, Ankara, Seçkin, s.263. Korkmaz ise haberleşmenin gizliliğini ihlal suçlarının işlenmesi halinde aynı zamanda kişisel verilere karşı suçların da işlenmiş olacağını, haberleşmenin gizliliğini ihlalin TCK m.132'de özel olarak düzenlenmesi sebebiyle bu hükmün uygulanacağını ifade etmesine rağmen (bkz **Korkmaz**, s.379) kitabın ilerleyen bölümlerinde bu suçlar arasında farklı neviden fikri içtima uygulamasının yapılabileceğini ifade etmektedir (bkz. **Korkmaz**, s.428). Kanaatimizce bu ifadeler çelişkilidir.

⁵²¹ İkinci fıkra kanaatimizce TCK m.135 ile ilişkilidir ve kişisel verilerin kaydedilmesi suçu incelenirken içtima başlığında ele alınmıştır.

“(1) Kişiler arasındaki aleni olmayan konuşmaları, taraflardan herhangi birinin rızası olmaksızın bir aletle dinleyen veya bunları bir ses alma cihazı ile kaydeden kişi, iki yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(3) Kişiler arasındaki aleni olmayan konuşmaların kaydedilmesi suretiyle elde edilen verileri hukuka aykırı olarak ifşa eden kişi, iki yıldan beş yıla kadar hapis ve dörtbin güne kadar adli para cezası ile cezalandırılır. Ifşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur.”

Birinci fıkrada kişiler arasındaki aleni olmayan konuşmaların dinlenilmesi ve kayda alınması seçimlik hareketler olarak düzenlenmiştir. Konuşmalar kanaatimizce kişisel veri niteliği taşıdığı için bu seçimlik hareketlerden her ikisi de TCK m.136 ile ilişkilidir⁵²². Ancak özel normun önceliği ilkesi gereği her iki seçimlik hareket için de yalnızca TCK m.133/1 hükmü uygulanacaktır. Şayet kişiler arasındaki konuşmaların her zaman kişisel veri anlamına gelmeyebileceği kabul edilirse, genel suç – özel suç ilişkisinden bahsedilemeyecek ve her iki suçu da teşkil eden tek fiilin bulunduğu hallerde farklı neviden fikri içtima kuralı uygulanacaktır. TCK m.133/1 hükmü TCK m.136’dan daha ağır ceza öngördüğü için farklı neviden fikri içtima kuralı da uygulansa sonuç bakımından bir değişiklik oluşmayacaktır.

TCK m.133/3 hükmünde de kişilerin ses kayıtlarının ifşa edilmesi durumu söz konusudur. Bu fiil de şüphesiz TCK m.136 ile ilişkilidir. Ancak TCK m.133/3 özel norm niteliğindedir ve özel normun önceliği ilkesi gereği bu hüküm uygulanmalıdır.

Özel hayatın gizliliğini ihlal başlığı taşıyan TCK m.134’ün ikinci fıkrası aşağıdaki gibidir⁵²³;

“(2) 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.”

⁵²² Kaydetme fiilini TCK m.135 ile değil TCK m.136 ile ilişkilendirmemizin sebebi kaydetmenin verilere erişim yetkisi bulunmayan bir kişinin ele geçirmesi suretiyle gerçekleştirilmesidir.

⁵²³ Birinci fıkra TCK m.135’in içtima ilişkileri incelenirken ele alınmıştır.

Bu fıkra kişilerin özel hayatına ilişkin görüntü veya seslerinin ifşa edilmesini suç olarak düzenlemektedir. Ifşa etme fiili ile yayma fiilleri aynı niteliktedir. Bu suç ile TCK m.136 arasında genel norm – özel norm ilişkisi vardır. Ifşa edilen kişisel verilerin kişinin özel hayatına ilişkin görüntü veya seslerden oluşması halinde TCK m.134/2 hükmü uygulanacaktır⁵²⁴.

TCK m.243'te düzenlenen Bilişim Sistemine Girme suçları ve **m.244'te düzenlenen Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme** suçları ile m.136 arasında içtima ilişkisi oluşması mümkündür. Bu suçlar ile TCK m.136 arasında şartlarının oluşması durumunda farklı neviden fikri içtima kuralına göre uygulama yapılmalıdır. Örneğin kişisel verilerin bilişim sistemine girmek suretiyle ele geçirilmesi durumunda hem bilişim sistemine girme (TCK m.243/1) hem de verileri ele geçirme suçu (TCK m.136) oluşacaktır. Bu iki suçu oluşturan fiilin tek fiil olması durumunda farklı neviden fikri içtima hükümleri uygulanacaktır⁵²⁵. İki ayrı fiilin varlığı durumunda ise iki ayrı suçtan ayrı ayrı ceza verilecektir. Şayet kişi kişisel verileri ele geçirmek maksadıyla bilişim sistemine giriyorsa, bilişim sistemine girme hareketi ile verileri ele geçirme hareketi bütünlük arz edecek şekilde birbirine bağlı ise tek fiilin varlığı kabul edilmelidir. Ancak kişinin girdiği bilişim sisteminde rastladığı kişisel verileri ele geçirme iradesi göstererek, planlanmayan ikinci bir harekete girişmesi durumunda iki fiilin varlığı kabul edilmelidir.

TCK m.136'nın hakaret suçu ile içtima ilişkisinin söz konusu olması da mümkündür. Yargıtay kararına konu olan bir örnek üzerinden konuyu ele alabiliriz⁵²⁶. Bir gazetecinin köşe yazılarının yayınlandığı köşesindeki fotoğrafı alıp bir arkadaşlık sitesinde oluşturduğu sahte profile “*bekar ve erkek arkadaş arıyor*” şeklinde ifadelerle koyan fail hakkında yargılama yapılmış, ilk derece mahkemesi özel hayatın gizliliğini ihlal suçundan faili mahkûm etmiştir. Yargıtay özel dairesi fiilin kişisel verileri yayma suçunu oluşturduğunu kabul ederek kararı bozmuştur. Yargıtay Cumhuriyet Başsavcılığı ise fiilin “*kişiyi tahkir edici, incitici ve şeref ve itibarını zedeleyici nitelikte olup basın yoluyla hakaret suçunu oluşturduğunu*” ifade etmiştir. Ceza Genel Kurulu failin eylemlerinin kişiyi tahkir edici nitelikte olup basın yoluyla hakaret suçunu (TCK m.125/1-4)

⁵²⁴ Aynı yöndeki görüş için bkz. **Maden**, s.187.

⁵²⁵ **Maden**, s.191,

⁵²⁶ Ceza Genel Kurulu, E. 2012/1510, K. 2014/331, K.T. 17.06.2014.

oluşturmakla birlikte kişisel verileri yayma (TCK m.136) suçunu da oluşturduğunu, tek fiil ile birden fazla suç işleyen sanığın farklı neviden fikri içtima kuralları doğrultusunda bunlardan en ağır cezayı gerektiren TCK m.136'dan cezalandırılması gerektiğine hükmetmiştir. Kanaatimizce bu karar isabetlidir⁵²⁷.

TCK m.209/2'da ele geçirilen yahut elde bulundurulan imzanın hukuki sonuç doğuracak şekilde kullanılması suç olarak düzenlenmiştir. Bu suçun imzanın ele geçirilerek işlenmesi durumunda TCK m.136'da tanımlanan kişisel verinin ele geçirilmesi durumu söz konusudur. Şayet ele geçirme ve hukuki sonuç doğuracak şekilde kullanma hareketleri tek bir fiil teşkil edecek şekilde gerçekleştirilmişse görünüşte içtima kuralları gereği yalnızca TCK m.209/2'den sorumluluk doğacaktır. Ancak fail önce hukuki sonuç doğuracak şekilde kullanma amacı olmadan ele geçirmiş, daha sonra yeni bir karar ile bu imzayı kullanmış ise iki ayrı fiilden söz edileceği için kanaatimizce içtima kuralları uygulanamayacak, fail her iki suçtan da sorumlu tutulacaktır.

TCK m.245'te Banka veya Kredi Kartlarının Kötüye Kullanılması suçu düzenlenmiştir. Bu suçu kredi kartını ele geçirip sahibinin rızası hilafına kullanarak yarar sağlayan kişinin eylemlerinin kredi kartı bilgilerini ele geçirmekten ibaret olan kısmı TCK m.136'da düzenlenen suçun fiil unsurunu oluşturmaya elverişlidir. Kredi kartı bilgilerinin sahibinin rızası hilafına kullanarak yarar sağlamak maksadıyla ele geçirildiği durumlarda failin hareketlerinin bir bütün halde tek fiil olduğu kabul edilmeli, fikri içtima kuralı gereği sorumluluk sadece m.245'ten doğmalıdır. Ancak failin ele geçirdiği kredi kartı bilgilerini ikinci bir karar ile kullanması ve m.245'teki suçu işlemesi halinde hukuki anlamda iki ayrı fiil ve dolayısıyla iki ayrı suç söz konusu olacaktır.

⁵²⁷ Ceza Genel Kurulu Başkanı ve 4 üye karara muhalefet etmiştir. Muhalefet şerhinde katılanın fotoğrafının kendisi tarafından gazete köşesinde kullanılmakla zaten yayılmış olduğu, bu sebeple kişisel verileri yayma suçunun oluşmayacağı ifade edilmiştir. Koca / Üzülmüş de bu görüşe katılmıştır. (Bkz. **Koca / Üzülmüş** (2020), s.574) Ancak kanaatimizce Ceza Genel Kurulu'nun görüşü isabetlidir. Zira kişisel verilerin korunması hakkı kişinin bizzat kendisi tarafından alenileştirilmiş verileri üzerinde de devam eder. Bu veriler korunmadan büsbütün hariç tutulmamaktadır. Verinin sahibi tarafından alenileştirilmiş olması açık rıza aranmadan işlenebilmesine imkân verse de, bu işleme faaliyeti verinin alenileştirilme amacına ve dürüstlük kuralına uygun olarak gerçekleştirilmelidir. Alenileştirilmiş verilerin alenileştirilme amacına ve dürüstlük kuralına aykırı şekilde kullanılması hukuka aykırı olmaya devam eder. Kişisel verilerin korunma amacı bu veriler kullanılarak sanığın temel hak ve hürriyetlerinin ihlal edilebileceği anlamına gelmez. Bu tür durumlarda yalnızca ihlal edilen hakka ilişkin özel suçun değil (somut olayda hakaret suçu) aynı zamanda kişisel verilerin hukuka aykırı olarak kaydedilmesi, verilmesi veya yayılması suçlarının da oluşabileceği kabul edilmelidir.

TCK m.258’de Göreve İlişkin Sırrın Açıklanması suçu düzenlenmiştir⁵²⁸. Bu suçun konusun kişisel verilerden oluşması durumunda TCK m.136’da düzenlenen suçun oluşması da mümkündür. TCK m.258’de düzenlenen suç kamu görevlisi tarafından ve görevin verdiği yetki kötüye kullanılmak suretiyle işlenebilmektedir. Dolayısıyla TCK m.136’da düzenlenen suç ile içtima ilişkisi suçun temel şekli üzerinden değil m.137/1-a’da düzenlenen nitelikli hal üzerinden gerçekleşecektir. Farklı neviden fikri içtima kuralı gereği sorumluluk yalnızca Kişisel Verileri Hukuka Aykırı Olarak Verme, Yayma veya Ele Geçirme suçunun nitelikli halinden olacaktır.

3.5. Soruşturma, Kovuşturma ve Yaptırım

Suçun soruşturması ve kovuşturması resen yapılır, şikâyeteye tabi değildir. Suçun kamu görevlisi tarafından görevi sebebiyle işlenmesi halinde soruşturma yapılabilmesi için yetkili merciin izni gerekir. Suç uzlaştırmaya tabi değildir⁵²⁹.

Suçun temel şeklinin cezası 2 yıldan 4 yıla kadar hapidir. Nitelikli hallerin varlığı halinde ceza artırılabilecektir. Suçun konusunu Ceza Muhakemesi Kanunu’nun yukarıda bahsettiğimiz hükümleri doğrultusunda kaydedilen beyan ve görüntülerden oluşması halinde failin cezası bir kat artırılır. 137nci maddede düzenlenen nitelikli hallerin gerçekleşmesi durumunda ise ceza yarı oranında artırılacaktır.

Suçun bir özel hukuk tüzel kişisi yararına tüzel kişinin organ ve temsilcileri tarafından işlenmesi durumunda tüzel kişi hakkında bunlara mahsus güvenlik tedbirlerine hükmolunur.

⁵²⁸ Bu suça ilişkin detaylı bilgi üçüncü bölümde Göreve İlişkin Sırrın Açıklanması başlığında verilmiştir.

⁵²⁹ Kangal, s.152.

4. KİŞİSEL VERİLERİ YOK ETMEME (TCK m.138)

Kişisel verileri yok etmeme suçu, kişisel verilerin korunması hakkını ihlallere karşı koruma maksadıyla ihdas edilmiş bir diğer suç tipidir. Suç ile korunan hukuki değer kişisel verilerin korunması hakkıdır. Anayasa'nın 20nci maddesine göre 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. Görüldüğü üzere kişisel verilerin korunması hakkının bir boyutu olan verilerin silinmesini isteme hakkı Anayasa’da açıkça ifade edilmiştir. Anayasa’da hakkın bu boyutuna özellikle vurgu yapılması, kişisel verilerin silinmesinin, hakkın korunabilmesi için ne denli önemli olduğunu göstermektedir.

Her gerçek kişi esasen kişisel verilerinin kaydedilmemesini isteme hakkına sahiptir. Kural, kişisel verilerin hiç kaydedilmemesidir. Ancak kişisel veriler ilgili kişinin açık rızasının bulunması veya kanunlarda öngörülmesi durumunda kaydedilebilmektedir. Günümüzde de kamu hizmetlerinin görülmesi, sözleşmeden doğan yükümlülüklerin yerine getirilebilmesi, sosyal ve ticari hayatın sürdürülebilmesi, güvenliğin ve kamu düzeninin sağlanması gibi pek çok sebeple kişisel veriler kaydedilmektedir. Kişisel verilerin korunması kural, kaydedilmesi istisna olması gerekirken; bilgi toplumunun ve gözetim toplumunun yükselişi ile kişisel veriler her an kaydedilir ve depolanır hale gelmiştir. Modern toplumda kişiler doğumlarından ölümüne kadar dijital bir gözetim altındadır. Teknolojinin gelişmesi ve dijitalleşmenin artmasıyla kişisel verilerin kaydedilme miktarı da devasa boyutlara ulaşmıştır.

Kişisel verilerin hukuka aykırı olarak kaydedilmesinin önlenmesi kadar, hukuka uygun olarak kaydedilmiş kişisel verilerin kaydetmeyi hukuka uygun hale getiren sebebin ortadan kalktığı anda silinmesinin sağlanması da oldukça önemlidir. Meşru bir sebebe dayalı olarak kaydedilmiş kişisel veriler, kaydetmeyi gerektiren sebep ortadan kalktığında yok edilmelidir. Kişisel veri işleme sürecine hâkim olan temel ilkelerden biri verilerin toplandıkları amaç için gerekli olan süre kadar muhafaza edilmesidir. Bu ilke KVKK m.4’te de açıkça ifade edilmiştir.

İşlenme amacı için gereken sürenin sona ermesinden sonra da verilerin muhafazasına devam edilmesi verileri toplanan kişiler için ciddi riskler oluşturacaktır. Kişisel verilerin hukuka aykırı olarak kullanılması sonucu kişilerin pek çok temel hak ve hürriyetinin ihlal edilmesi mümkündür. Verilerin sürekli toplandığı ancak hiç silinmediği bir dünyada insanların kendilerini tehdit altına hissetmeden kişiliğini özgürce geliştirme hakkını kullanabilmeleri mümkün değildir. Bu sebeple başta kişisel verilerin korunması hakkı olmak üzere bireylerin temel hak ve hürriyetlerinin korunabilmesi için kişisel verilerin yok edilmesi son derece önemlidir. Verileri yok etmeme suçunun ihdas edilme amacı verileri yok etmekle görevli kişileri görevlerini yerine getirmeye zorlamaktır. Bu sayede devlet kişisel verileri korumak konusundaki pozitif yükümlülüğünü yerine getirmektedir.

Kişisel verileri yok etmeme suçu 2005 yılında TCK'nın uygulanmaya başlaması ile yürürlüğe girmiştir. Suçun düzenlendiği TCK m.138 hükmüne 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”*. Bu suç genellikle kamu kurumları tarafından kanun hükümlerine istinaden toplanan kişisel verilerin kanunların öngördüğü süre kadar muhafaza edildikten sonra silinmelerini sağlama fonksiyonu görmüştür. KVKK'nın kabulü ile birlikte ise hükmün uygulama alanı bir hayli genişlemiştir. KVKK hem devlet hem de özel sektör tarafından yürütülen veri işleme faaliyetlerini disiplinize etmiş, veri işleyen tüm gerçek ve tüzel kişilere ciddi sorumluluklar yüklemiştir.

KVKK'nın getirdiği en önemli yükümlülüklerden birisi işlenmesini gerektiren sebeplerin ortadan kalkması halinde kişisel verilerin yok edilmesidir. Bu yükümlülük kanunun 7nci maddesinde düzenlenmiştir. Buna göre *“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”*.

7nci madde hükmünden de anlaşılacağı üzere kanun koyucu verileri yok etme görevini veri sorumlusuna yüklemiştir. Bu sebeple veri sorumlusu kavramı suç için önem arz etmektedir. Veri sorumlusu *“kişisel verilerin işleme amaçlarını ve vasıtalarını*

belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi” ifade etmektedir.

Hem KVKK’nın 7nci maddesindeki verileri silme, yok etme veya anonim hale getirme yükümlülüğün yerine getirilmemesi durumunda, hem de diğer kanunlar tarafından verilmiş yok etme görevinin yerine getirilmemesi durumunda TCK m.138’de düzenlenen suç oluşacaktır. KVKK m.17/2’de yer alan *“bu Kanunun 7 nci maddesi hükmüne aykırı olarak; kişisel verileri silmeyen veya anonim hâle getirmeyenler 5237 sayılı Kanunun 138 inci maddesine göre cezalandırılır”* hükmü de bunu ifade etmektedir. Bazı yazarlar bu hüküm ile *“kişisel verileri silmeme veya anonim hale getirmeme”* adı altında yeni bir suç tipi ihdas edildiği görüşündedir.⁵³⁰ Fakat bizim de katıldığımız görüşe göre⁵³¹ kanun koyucu burada yeni bir suç ihdas etmemiş, KVKK m.7’ye aykırı hareketlerin de TCK m.138 kapsamında değerlendirilmesi gerektiğini vurgulamak istemiştir⁵³².

TCK m.138’in başlığında ve metninde *“kişisel verileri”* yerine *“verileri”* ifadesi kullanılmıştır. Ancak bundan kişisel verilerin anlaşılması gerekir. Zira madde gerekçesinde de kişisel veri ibaresi kullanılmıştır. Kanun koyucunun kelimeleri özensiz şekilde kullanması söz konusudur ve durum tartışmalara sebebiyet verebilecek niteliktedir. Kanaatimizce madde başlığındaki ve madde metnindeki *“verileri”* ibareleri *“kişisel verileri”* olarak değiştirilmelidir.

Suçun oluşması için özetle; hukuka uygun olarak sisteme kaydedilmiş bir kişisel veri bulunmalıdır, verilerin sistem içerisinde ne kadar süre tutulacağı kanunla belirlenmiş olmalıdır ve bu sürelerin geçmesine rağmen verileri yok etmekle yükümlü kişiler yükümlülüklerini yerine getirmemelidir⁵³³.

⁵³⁰ Koca / Üzülmöz (2020), s.587. Maden, s.131-142. Dülger (2020), s.764.

⁵³¹ Kangal, s.153-154. Sağlam, s.120. Yıldız, s.86.

⁵³² Bu konu hakkında detaylı açıklamalar ikinci bölümde 6.2.1. numaralı başlıkta yapılmıştır.

⁵³³ Koca / Üzülmöz (2020), s.586.

4.1. Korunan Hukuki Değer

Bu suç ile korunan hukuki değer diğer suç tiplerinde de olduğu gibi kişisel verilerin korunması hakkıdır. Bir görüşe göre bu suçla kişisel verilerin korunması hakkının yanı sıra kamu idaresinin güvenilirliği de korunmaktadır⁵³⁴. KVKK'nın kabulünden önce söz konusu yükümlülüğün genellikle kamu görevlileri bakımından ortaya çıkması bu düşüncenin gelişmesine sebep olmuştur. Ancak günümüzde özel sektörün veri işleme kapasitesi kamu kurumlarının veri işleme kapasitesinin üzerine çıkmıştır ve bu yükümlülük kamu kurumları kadar özel kişiler açısından da doğmaktadır. Suçun kamu idaresinin güvenilirliğini koruma fonksiyonunun ikinci planda kaldığı söylenebilir.

4.2. Suçun Unsurları

4.2.1. Maddi Unsurlar

4.2.1.1. Fail

Herkes bu suçun faili olamaz. Suçun faili ancak verileri sistem içerisinde yok etmekle, silmekle veya anonim hale getirmekle görevli olan bir kişi olabilir. Suçun faili kamu görevlisi olabileceği gibi özel bir şahıs da olabilir⁵³⁵. Suçun faili için özel bir vasıf arandığı için bu suç özgü suçtur.

Madem ki suçun faili olabilmek için görevli olmak gerekmektedir, öyleyse failin belirlenmesi için de görevin tanımlandığı kanun hükmünün dikkate alınması gerekir. Somut olayda kanun verileri imha etme görevini kime yüklemişse fail odur. Ancak şunu belirtmek gerekir ki yükümlülüğün her zaman kanunla yüklenmiş olması gerekmez⁵³⁶. Yönetmelik, tüzük veya karar gibi idari işlemlerle de bu görev yüklenebilir.

⁵³⁴ Soyaslan (2020), s.369. Dülger (2020), s.753.

⁵³⁵ Soyaslan (2020), s.369.

⁵³⁶ Koca / Üzülmöz (2020), s.592.

Bu konudaki esas ve en kapsamlı görevlendirme KVKK'nın 7nci maddesi ile yapılmıştır. Bu maddeye göre veri sorumluları verileri yok etmekle görevlidir. Dolayısıyla veri sorumluları suçun faili olacaktır. KVKK'ya göre veri sorumlusu *“kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi”* ifade eder. Veri sorumlusunun tüzel kişi olması durumunda tüzel kişi suçun faili olamayacağı için tüzel kişinin veri kayıt sisteminden sorumlu olan kişi suçun faili olarak kabul edilmelidir⁵³⁷.

KVKK dışındaki kanunlarla da belirli kişilere bu konuda sorumluluk yüklenmiştir. 5271 sayılı CMK'nın pek çok maddesinde muhakeme işlemleri sırasında elde edilen verilerin yok edilmesi düzenlenmiştir. CMK m.75, m.76 ve m.78'de şüpheli, sanık ve mağdurdan kan, saç ve tükürük gibi örneklerin alınabileceği, bunların moleküler genetik incelemeye tabi tutulabileceği düzenlenmiştir. CMK m.80'de ise bu yollarla elde edilen verilerin kişisel veri niteliğinde olduğu belirtildikten sonra *“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”* hükmüne yer verilmiştir. Ayrıca Adalet Bakanlığı tarafından bu işlemlerin düzenlenmesi maksadıyla çıkarılan yönetmeliğin⁵³⁸ 22nci maddesinde *“Cumhuriyet başsavcılıklarınca yapılan iş bölümlerinde, bu Yönetmelik kapsamında elde edilen verilerin imha edilmesi ve diğer işlemlerin yürütülmesi amacıyla yeterli sayıda Cumhuriyet savcısı görevlendirilir”* hükmü yer almaktadır. Dolayısıyla CMK m.80 ve ilgili yönetmelik doğrultusunda Başsavcılık tarafından görevlendirilecek cumhuriyet savcısı TCK m.138'de düzenlenen suçun faili olabilecektir. Bunun dışında cumhuriyet savcısı CMK m.81 uyarınca fiziki kimliği tespit eden verileri, m.137 uyarınca iletişimin tespiti suretiyle elde edilmiş verileri, m.140 uyarınca teknik araçlarla izleme suretiyle elde edilmiş verileri yok etmekle görevlidir. Bu verilerin yok edilmemesi durumunda cumhuriyet savcısı suçun faili olarak sorumlu tutulacaktır.

⁵³⁷ Kangal, s.158.

⁵³⁸ Ceza Muhakemesinde Beden Muayenesi, Genetik İncelemeler ve Fizik Kimliğin Tespiti Hakkında Yönetmelik, Tam metin için bkz. (<https://www.resmigazete.gov.tr/eskiler/2005/06/20050601-13.htm>) s.e.t. 17.01.2023

4.2.1.2. Mağdur

Suçun mağduru sistemde kayıtlı olan kişisel verisi yok edilmeyen gerçek kişidir. Kişisel veriler yalnızca gerçek kişilere ilişkin olabileceği için tüzel kişiler bu suçun mağduru olamaz.

Suç ile korunan hukuki değerin kamu idaresine karşı duyulan güven olduğu, bu sebeple suçun mağdurunun kamu olduğu, kişisel verisi imha edilmeyen gerçek kişinin ise ancak suçtan zarar gören olabileceği yönündeki görüşe⁵³⁹ katılmıyoruz.

4.2.1.3. Suçun Konusu

Suçun konusunu kişisel veriler oluşturur. Kişisel verinin ne olduğuna ilişkin gerek birinci bölümde gerek kişisel verilerin kaydedilmesi suçu başlığında detaylı açıklamaları yaptığımız için bu konuyu tekrar burada ele almayacağız.

Bu suçun konusunu oluşturacak kişisel verinin sisteme daha önce hukuka uygun bir şekilde kaydedilmiş olması gerekir. Sistemde kayıtlı olmayan veriler suçun konusunu oluşturamaz. Verilerin sisteme hukuka aykırı olarak kaydedilmiş olması durumunda kişisel verilerin kaydedilmesi suçu oluşur. Hukuka aykırı olarak kaydedilmiş verilerin silinmemesi ise verileri yok etmeme suçunu oluşturmayacaktır⁵⁴⁰.

Sistem kelimesi her ne kadar elektronik bir sistemi çağırırsa da bu sistem elektronik veya manyetik bir sistem olabileceği gibi fiziki bir dosya da olabilir. KVKK m.7’de yer alan imha yükümlülüğüne konu verilerin kayıtlı oldukları yer yine KVKK m.3/1-h bendinde tanımlanan veri kayıt sistemi olacaktır. KVKK’ya göre veri kayıt sistemi “*kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini*” ifade eder. Bu sistem fiziki olabileceği gibi elektronik de olabilir. CMK hükümleri doğrultusunda kaydedilen kişisel veriler zaman zaman dosyalarda, zaman zaman CD –

⁵³⁹ Dülger (2020), s.755.

⁵⁴⁰ Koca / Üzülmaz (2020), s.591.

DVD gibi aygıtlarda tutulmaktadır. Bu dosya ve CD'ler de sistem olarak kabul edilebilecektir.

4.2.1.4. Fiil

Suçun fiil unsuru kanunların belirlediği süreler geçmiş olmasına rağmen kişisel verilerin yok edilmemesidir. Kanuni tariftten yola çıkarak fiil unsurunun gerçekleşmesi için iki hususun yerine gelmesi gerektiğini söyleyebilir. Bunlardan birincisi kanunların belirlediği sürelerin geçmiş olmasıdır. İkinci ise verilerin yok edilmemesidir. Verileri yok etmeme ihmali davranışını gerçekleştirmesi gereken failin hukuken verileri yok etmekle görevli olması gerektiğinde şüphe yoktur. Bu husus yukarıda fail başlığında açıklanmıştır. Suç teşkil eden ihmali davranış kanunda açıkça belirtildiği için bu suç gerçek ihmali suçtur⁵⁴¹.

Kanunların belirlediği süre ifadesindeki kanundan ne anlaşılması gerektiği konusunda öğretide farklı görüşler bulunmaktadır. Bir görüşe göre bu ifadeden TBMM tarafından çıkarılan kanun anlaşılmalıdır. Bu sürenin tüzük, yönetmelik veya yönerge gibi düzenleyici idari işlemlerle belirlenmesi kanunilik ilkesinin ihlali anlamına gelecektir⁵⁴². Bir diğer görüşe göre kanun ifadesi hukuk kuralı olarak anlaşılmalıdır. Sürelerin idarenin herhangi bir düzenleyici işlemiyle belirlenmesi mümkündür⁵⁴³.

Kanaatimizce verileri yok etme yükümlülüğünün ne zaman doğacağı genel hatlarıyla kanun ile belirlenmelidir. Ancak kanunda net bir sürenin ifade edilmesi şart değildir. Verilerin yok edilme zamanı belirli bir olayın gerçekleşme zamanı olarak da öngörülebilir. Örneğin CMK m.80/2'de verilerin *“kovuşturmaya yer olmadığı kararına itiraz süresinin dolması, itirazın reddi, beraat veya ceza verilmesine yer olmadığı kararı verilip kesinleşmesi hâllerinde Cumhuriyet savcısının huzurunda derhâl yok edilmesi”* gerektiği hükme bağlanmıştır. Görüldüğü üzere burada süre net değildir ve beraat kararı verilmesi gibi belirli olayların gerçekleşmesi ile verilerin yok edilmesi öngörülmüştür. Belirli bir olayın gerçekleşmesiyle verilerin yok edileceğinin kanunda öngörüldüğü

⁵⁴¹ Koca / Üzülmmez (2020), s.592.

⁵⁴² Koca / Üzülmmez (2020), s.592.

⁵⁴³ Özbek / Doğan / Bacaksız, Ceza Özel, s.616.

durumlarda, olay gerekleřtikten sonra verilerin ne kadar sre ierisinde yok edileceėi sorusu akla gelebilir. Zira kanunda derhal ifadesi yer alsa da olayın gerekleřme anında eř zamanlı olarak verilerin yok edilmesinin mmkn olmadığı aıktır. Bu tr durumlarda ynetmelik gibi dzenleyici iřlemlerle verilerin yok edilmesi iin makul bir sre (rneėin 10 gn veya 20 gn gibi) ngrlebilir. Bu durumda bu sre esas alınacaktır. Eėer byle bir sre ngrlmemiřse verilerin makul bir sre ierisinde yok edilmesi gerekecektir. Dava konusu somut olaylarda makul srenin ařılıp ařılmadığını yargı makamları tespit ve takdir edecektir. Kanunda srenin net olarak ifade edildiėi durumlarda ise bu srenin esas alınacağında řphe yoktur.

KVKK'nın sistematik veri iřleme faaliyetlerini disiplinize eden ana kanun olması sebebiyle veri iřleme faaliyetlerinin byk oėunluėu bu kanuna tabi olarak gerekleřtirilmektedir. Bu kanun hkmlerine tabi olarak veri iřleyen kiřilere kanunun 7nci maddesiyle verileri silme, yok etme veya anonim hale getirme ykmllė yklenmiřtir. Veri iřleyen ok sayıda kiřiye sorumluluk ykleme sebebiyle uygulamada en sık karřılařılacak hkm budur. Bu hkme aykırı hareketler TCK m.138'de dzenlenen tipik fiili teřkil edecektir. Bu sebeple KVKK m.7 hkmnn incelenmesi gerekmektedir. “Kiřisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi” bařlıklı 7nci madde hkm ařaėıdaki gibidir;

“(1) Bu Kanun ve ilgili diėer kanun hkmlerine uygun olarak iřlenmiř olmasına raėmen, iřlenmesini gerektiren sebeplerin ortadan kalkması hlinde kiřisel veriler resen veya ilgili kiřinin talebi zerine veri sorumlusu tarafından silinir, yok edilir veya anonim hle getirilir.

(2) Kiřisel verilerin silinmesi, yok edilmesi veya anonim hle getirilmesine iliřkin diėer kanunlarda yer alan hkmler saklıdır.

(3) Kiřisel verilerin silinmesine, yok edilmesine veya anonim hle getirilmesine iliřkin usul ve esaslar ynetmelikle dzenlenir.”

Birinci fıkradan anlařılacağı zere hem KVKK hkmleri doėrultusunda veri iřleyenler hem de diėer kanunlarda yer alan hkmler doėrultusunda veri iřleyen kiřiler bu hkmn kapsamındadır. İkinci fıkrada ise diėer kanunlarda yer alan hkmlerin saklı olduėu ifade edilmiřtir. Birinci fıkra ile ikinci fıkra birlikte yorumlandığında ıkarılması gereken sonu; diėer kanun hkmlerine gre veri iřleyen kiřiler bu kanunlarda verilerin

silinmesi, yok edilmesi veya anonim hale getirilmesine dair bir hüküm varsa bu hükme tabi olacaktır⁵⁴⁴. Bu kanunlarda hüküm bulunmayan durumlar için ise KVKK m.7 hükmü uygulanacaktır.

Birinci fıkradan anlaşılacağı üzere kişisel verilerin silinmesi yükümlülüğü verilerin işlenmesini gerektiren sebeplerin **tamamının**⁵⁴⁵ ortadan kalkması ile doğacaktır. Verilerin işlenmesini gerektiren sebepler ortadan kalkmasına rağmen verileri silmeyen, yok etmeyen veya anonim hale getirmeyen kişi TCK m.138’de düzenlenen verileri yok etmeme suçunun faili haline gelecektir. Elbette işlenmesini gerektiren sebeplerin ortadan kalkmasıyla suç derhal meydana gelmiş olmayacaktır. Verilerin ne kadar süre içerisinde imha edileceği konusundaki detaylar üçüncü fıkra hükmü doğrultusunda çıkarılan yönetmelikle⁵⁴⁶ belirlenmiştir.

Yönetmelik ilgili kişinin talebi üzerine imha etme⁵⁴⁷ ve resen imha etme hâllerini ayrı ayrı düzenlemiştir. Şayet imha etme işlemi ilgilinin talebi üzerine yapılıyorsa talep tarihinden itibaren en geç 30 gün içerisinde veri sorumlusu işlemi gerçekleştirmelidir⁵⁴⁸.

İmha etme işleminin resen yapılması durumunda yönetmelik imha politikası hazırlayan ve hazırlamayan veri sorumluları arasında ayrıma gitmiştir. Veri saklama ve imha politikası⁵⁴⁹ hazırlamış olan veri sorumlusu yükümlülüğün ortaya çıktığı tarihi takip eden ilk periyodik imha⁵⁵⁰ işleminde kişisel verileri imha etmelidir. Periyodik imha aralığı veri sorumlusu tarafından belirlenir. Bu süre her halde 6 ayı geçemez. Veri saklama ve

⁵⁴⁴ Gerekçede de bu husus şu şekilde ifade edilmiştir; “Maddenin ikinci fıkrasıyla, kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin diğer kanunlarda yer alan hükümlerin saklı tutulması öngörülmektedir. Bu kapsamda, örneğin Adli Sicil Kanununda verilerin silinmesini veya yok edilmesini düzenleyen hükümler Kanuna göre öncelikli olarak uygulanacaktır.”

⁵⁴⁵ Kişisel verilerin işleme şartları KVKK m.5 ve m.6’da düzenlenmiştir. Bu şartların tamamının ortadan kalkmış olması gerekmektedir.

⁵⁴⁶ Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik, Tam metin için bkz. (<https://www.resmigazete.gov.tr/eskiler/2017/10/20171028-10.htm>) s.e.t. 17.01.2023.

⁵⁴⁷ Yönetmeliğe göre imha etme kavramı “Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesini” ifade eder. Bkz. Yönetmelik m.4/1-c.

⁵⁴⁸ Şayet veri işleme şartları ortadan kalkmamışsa veri sorumlusu ilgili kişinin bu talebini reddedebilir. Bkz. Yönetmelik m.12.

⁵⁴⁹ Veri sorumluları siciline kaydolma yükümlülüğü olan veri sorumluları veri saklama ve imha politikası hazırlamakla yükümlüdür. Veri sorumluları siciline kaydolma yükümlülüğü bulunan veri sorumluları KVKK’nın 16ncı maddesi doğrultusunda Kişisel Verileri Koruma Kurulu tarafından belirlenecektir. Yönetmelik m.5/1

⁵⁵⁰ Periyodik imha; “kanunda yer alan kişisel verilerin işleme şartlarının tamamının ortadan kalkması durumunda kişisel verileri saklama ve imha politikasında belirtilen ve tekrar eden aralıklarla resen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemini” ifade eder. Bkz. Yönetmelik m.4/1-ğ

imha politikası hazırlama yükümlülüğü bulunmayan veri sorumlusu ise yükümlülüğün ortaya çıktığı tarihten itibaren 3 ay içinde verileri imha etmelidir⁵⁵¹.

KVKK m.7 kapsamında kişisel verileri imha etme yükümlülüğü bulunan veri sorumluları bakımından TCK m.138’de tanımlanan suçun oluşup oluşmadığını tespit için yönetmelik tarafından belirlenen süreler dikkate alınacaktır. Süresi içerisinde imha işlemi gerçekleştirilirse suç oluşmayacaktır. Dolayısıyla tespit edilmesi gereken bir diğer husus imha işleminin gerçekleştirilip gerçekleştirilmediğidir. İmha kavramı yönetmelikte verilerin silinmesi, yok edilmesi ve anonim hale getirilmesini kapsayacak şekilde tanımlanmıştır. Kanaatimizce TCK m.138’de yer alan yok etme kavramı imha ile eş anlamlıdır. Yani TCK m.138’deki yok etmenin silme ve anonim hale getirmeyi de kapsadığını kabul etmek gerekir.

Yok etme, silme ve anonim hale getirme kavramları yönetmelikte tanımlanmıştır. Buna göre yok etme *“kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi”* anlamına gelir. Silme *“kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi”* anlamına gelir. Anonim hale getirme ise *“kişisel verilerin anonim hale getirilmesi, kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi”* anlamına gelmektedir.

Silme, yok etme ve anonim hale getirme hareketlerinin her biri kişisel verileri imha yöntemidir. Veri sorumlusu, kurul tarafından aksi yönde bir karar alınmadıkça hangi imha yöntemini uygulayacağına kendisi karar verir⁵⁵². Bu yöntemlerden birisini uygulamakla sorumluluğunu yerine getirmiş olacaktır. Tanımlardan ve hangi yöntemin kullanılacağını veri sorumlusuna bırakılmasından hareketle bu yöntemlerin birbiri ile aynı işlevi gören yöntemler olduğu sonucuna varmak mümkündür. Kanaatimizce TCK m.138’deki yükümlülüğün yerine getirilebilmesi için de bu yöntemlerden herhangi birinin kullanılması yeterli sayılmalıdır. Zaten silme ve yok etme neredeyse eş anlamlı kelimelerdir. Öğretide de özellikle KVKK’nın kabulünden önce yok etme kavramını açıklarken silme ifadesinin kullanıldığı göze çarpmaktadır⁵⁵³. Silme kavramı daha çok verilerin elektronik ve manyetik

⁵⁵¹ Yönetmelik m.11.

⁵⁵² Yönetmelik m.7/5

⁵⁵³ Bkz. **Hafızoğulları / Özen**, s.273.

ortamda yok edilmesi anlamında kullanılırken, yok etme kavramı daha çok fiziksel olarak erişilemez ve kullanılamaz hale getirme anlamında kullanılmaktadır. Anonim hale getirmede ise kişi ile veri arasındaki bağlantı geri döndürülemeyecek şekilde koparılmaktadır. Veri, belirli veya belirlenebilir bir kişiye ilişkin olma niteliğini kaybetmekte, dolayısıyla kişisel veri olmaktan çıkmaktadır. Dolayısıyla anonim hale getirmede de ortada bir kişisel veri kalmamakta, kişisel veri yok edilmiş olmaktadır.

Yukarıdaki açıklamalar ışığında özetle; TCK m.138’de tanımlanan suçun fiil unsurunun gerçekleştiğini kabul etmek için öncelikle kanunlarda belirlenmiş sürelerin geçip geçmediği araştırılacaktır. KVKK kapsamına giren hallerde bu sürelerin tespiti için yönetmelik hükümlerine başvurulacaktır. KVKK kapsamına girmeyen hallerde⁵⁵⁴ veya KVKK kapsamına girmekle birlikte hakkında başka kanunlarda hüküm bulunan hallerde ilgili kanun hükmü uygulanacaktır. Bahse konu durum KVKK kapsamına da girmiyor başka bir kanunun kapsamına da girmiyorsa zaten ortada kanunlar tarafından yüklenmiş bir yükümlülük bulunmadığı için bu suç gündeme gelmeyecektir. Örneğin A erkek arkadaşı B’ye fotoğraflarını göndermiş olsun. Daha sonra ayrılınsınlar ve A B’den bu fotoğrafları silmesini istesin. B A’nın rızasının ortadan kalktığını bilmesine rağmen kasten bu fotoğrafları elinde tutmaya devam ederse kişisel verileri yok etmeme suçundan sorumlu tutulamayacaktır. Ancak B kişisel verileri kaydetme (TCK m.135) suçundan sorumlu tutulabilecektir.

4.2.2. Manevi Unsur

Bu suç ancak kasten işlenebilir. Suçun taksirli şekli kanunda düzenlenmemiştir. Kastın varlığı için failin kendisine verileri yok etme görevi verildiğini, verileri yok etmesi gereken sürenin dolduğunu ve buna rağmen verileri yok etmediğini bilmesi gerekir⁵⁵⁵. Failin özel bir amaç doğrultusunda hareket etmesi de aranmamıştır. Genel kastla işlenebilen suçların kanunda bunu engelleyen bir ifade olmaması durumunda olası kastla da işlenebilmesi mümkün olduğu için bu suçun olası kastla işlenebilmesi mümkündür⁵⁵⁶.

⁵⁵⁴ KVKK m.28’de kanun kapsamına girmeyen istisna halleri düzenlenmiştir.

⁵⁵⁵ Koca / Üzülmöz (2020), s.595.

⁵⁵⁶ Özbek / Doğan / Bacaksız, Ceza Özel, s.618.

Kişinin dikkat ve özen yükümlülüğüne aykırı hareketi sebebiyle verileri yok etmediği durumlarda kast değil taksir söz konusu olacağı için suçun manevi unsuru gerçekleşmeyecektir. Örneğin verileri yok etmek üzere götürürken dosyadaki bir kâğıdın dikkatsizlik sonucu fark etmeden düşürülmesi durumunda kasttan söz edilemez. Suçun taksirli hali de düzenlenmediği için bu durumda suç oluşmayacaktır.

4.2.3. Hukuka Aykırılık Unsuru

Diğer suç tiplerinde olduğu gibi bu suç tipinde de fiilin işlenmesini hukuka uygun hale getiren bir hukuka uygunluk sebebinin bulunması durumunda fiil hukuka uygun hale gelecek ve suç oluşmayacaktır. Ancak bu suçun karakteri gereği bir hukuka uygunluk sebebinin gerçekleşmesi oldukça zordur. Zaten kişisel verileri sistemde kayıtlı tutmak için bir hukuka uygunluk sebebine ihtiyaç vardır. Ancak bu hukuka uygunluk sebebinin ortadan kalktığı durumlarda verileri yok etme yükümlülüğünden bahsedilmektedir. Dolayısıyla bu suçun fiil unsurunun gerçekleştiği durumlarda genellikle bir hukuka uygunluk sebebi bulunamayacaktır. Buna rağmen bazı istisnai durumlarda hukuka uygunluk sebebinin meydana gelebilmesi de mümkündür. Örneğin bir hukuka uygunluk sebebine dayalı olarak işlenen kişisel verilerin işlenme sebebi ortadan kalkmış olsun. Verilerin imhası için belirlenen süre geçmeden ilgili kişi verilerinin silinmemesine ve sistemde tutulmaya devam edilmesine rıza göstermiş olsun. Rıza alındıktan sonra kanuni süre dolduğunda tipik fiilin gerçekleştiği kabul edilebilirse de ilgilinin rızası sebebiyle fiil hukuka uygun hale gelecektir.

Başka bir örnek vermek gerekirse; rızaya dayalı olarak verisi sistemde kayıtlı tutulan bir kişi rıza göstermediği verilerin de sistemde kayıtlı tutulduğu gerekçesiyle veri sorumlusu hakkında suç duyurusunda bulunmuş, aynı zamanda veri sorumlusundan kayıtlı bütün verilerinin silinmesini talep etmiş olsun. Normalde veri sorumlusu rızaya dayalı olarak verileri tuttuğu için ve ilgilinin rızası da ortadan kalktığı için verileri silmekle yükümlü olacaktır. Ancak veri sorumlusu suç duyurusu sebebiyle hakkında yürütülen kovuşturmada kendisini savunabilmek ve yalnızca ilgilinin rıza gösterdiği verileri sistemde tuttuğunu ispatlayabilmek için verileri sistemde tutmaya devam ederse burada “*savunma hakkının kullanılması*” sebebiyle fiil hukuka uygun hale gelebilecektir.

4.3. Nitelikli Haller

Kişisel Verileri Yok Etmeme suçunu düzenleyen 138inci maddenin ikinci fıkrasında bu suçun konusunun CMK hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken verilerden oluşması suçun nitelikli hali olarak düzenlenmiştir. CMK'nın kişisel verilerin yok edilmesine dair hükümleri 80, 81, 135, 137 ve 140ıncı maddelerinde yer almaktadır.

CMK'nın m.75, m.76 ve m.78 hükümleri doğrultusunda şüpheli, sanık veya mağdurdan gerektiği durumlarda kan, saç, tükürük, tırnak veya benzeri biyolojik örnekler alınabilmektedir. CMK m.80'de alınan bu örneklerin kişisel veri niteliğinde olduğu, amacı dışında kullanılamayacağı, kovuşturmaya yer olmadığı kararına itiraz süresinin dolması, itirazın reddi, beraat veya ceza verilmesine yer olmadığı kararı verilip kesinleşmesi hâllerinde Cumhuriyet savcısının huzurunda derhâl yok edileceği ifade edilmiştir.

CMK m.81'in birinci fıkrasında *“şüpheli veya sanığın, kimliğinin tespiti için gerekli olması halinde, Cumhuriyet savcısının emriyle fotoğrafı, beden ölçüleri, parmak ve avuç içi izi, bedeninde yer almış olup tespitini kolaylaştıracak diğer özellikleri ile sesi ve görüntülerinin”* kayda alınabileceği düzenlenmiştir. İkinci fıkrada bu kayıtların belirli olayların gerçekleşmesi ile bu kayıtların yok edileceği hükme bağlanmıştır.

CMK m.135 ila 137nci maddelerde şüpheli ve sanığın iletişiminin dinlenebileceği ve kayda alınabileceği, m.140'ta kamuya açık yerlerdeki faaliyetlerinin izlenip ses ve görüntü kaydı alınabileceği düzenlenmiş, yine aynı maddelerde belirli olayların gerçekleşmesi ile bu kayıtların imha edileceği hükme bağlanmıştır.

Kişisel Verileri Yok Etmeme suçunun maddi konusunun CMK'nın yukarıdaki hükümleri doğrultusunda yok edilmesi gereken verilerden oluşması durumunda 138nci maddenin ikinci fıkrasına göre nitelikli hal uygulanacak ve ceza bir kat artırılacaktır.

4.4. Suçun Özel Görünüş Biçimleri

4.4.1. Teşebbüs

Kişisel verileri yok etmeme suçu gerçek ihmalî suçtur. Gerçek ihmalî suçlara teşebbüsün mümkün olmadığı kabul edilmektedir. Çünkü kanunlar tarafından belirlenen süre henüz dolmamışsa kanuni tipe uygun bir hareketin gerçekleştirildiğini veya başladığını söylemek mümkün değildir⁵⁵⁷. Süre dolduğunda ise suç tamamlanmış olacağından tamamlanmış suça teşebbüs söz konusu olamayacaktır. İnceleme konusu suç bakımından verileri yok etmek için kanunlar tarafından belirlenen sürenin dolması ile suç meydana gelecektir. Sürenin dolmasından önce ise failin halen yükümlülüğü yerine getirme imkânı olduğu için başlamış bir tipik hareket söz konusu değildir. Dolayısıyla bu suça teşebbüs mümkün değildir⁵⁵⁸.

4.4.2. İştirak

Kişisel verileri yok etmeme suçu bir özgü suçtur. Dolayısıyla bu suçun faili ancak faillik vasfını taşıyan kişiler olabilir. Fail için aranan özel vasfı taşımayan kişiler bu suç bakımından yalnızca azmettiren veya yardım eden sıfatıyla suça iştirak edebilirler⁵⁵⁹. Suç işleme fikri olmayan kişiye suç işleme kararını aldırarak kişi azmettiren olarak, suç işleme kararı olan birinin bu kararını kuvvetlendiren kişi yardım eden olarak sorumlu tutulabilir.

4.4.3. İctima

Madde metninde içtimaa ilişkin özel bir hüküm bulunmamaktadır. Genel hükümler kapsamında değerlendirme yapılacaktır.

⁵⁵⁷ **Tozman, Önder** (2009) ‘İhmal Suçlarında Teşebbüs ve Gönüllü Vazgeçme’ Türkiye Barolar Birliği Dergisi, S:84, s.175.

⁵⁵⁸ **Maden**, s.426. **Kangal**, s.173. **Soyaslan** (2020), s.370. **Özbek / Doğan / Bacaksız**, s.618. **Koca / Üzülmmez** (2020), s.597. **Dülger** (2020), s.273. **Hafızogulları / Özen**, s.273. **Akdağ**, s.155.

⁵⁵⁹ **Sert**, s.167. **Korkmaz**, s.502.

Faile verilmiş bir görevin gerçekleştirilmemesi bir fiil olarak kabul edilmelidir. Yok edilmeyen kişisel veri sayısı dikkate alınmamalıdır. Bazen kişi hakkındaki çok sayıda kişisel verinin imha edilmesi fail için tek bir yükümlülük halinde doğabilir. Bu verileri imha etmemek tek suç anlamına gelir. Bazı durumlarda ise bir kişiye ait kişisel veriler farklı sebepler doğrultusunda işlenebilir. Kişiye ait birtakım verilerin silinmesi yükümlülüğü doğmuşken birtakım verilerin silinme yükümlülüğü henüz doğmamış olabilir. Örneğin A'nın TC kimlik numarasının silinme yükümlülüğü bugün doğmuş olsun. Telefon numarasının silinme yükümlülüğü ise 3 ay sonra doğsun. Şayet fail A'nın hiçbir verisini silmemek üzere baştan bir karar almışsa, süreleri dolmasına rağmen bu iki veriyi de silmediğinde zincirleme suç gündeme gelebilecektir.

Bazen birden çok kişinin verilerinin silinmesi fail için tek yükümlülük halinde doğmuş olabilir. Bu tür durumlarda tek bir fiil ile aynı suçun birden fazla kişiye karşı işlenmesi söz konusu olacağı için aynı neviden fikri içtima hükmü uygulanabilecektir⁵⁶⁰.

Kişisel verileri yok etme görevinin kamu görevlisine verilmiş olması halinde bu görevi yerine getirmeyerek kişilerin veya kamunun mağduriyetine sebep olan kamu görevlisi için görevi kötüye kullanma suçunun ihmalî davranışla gerçekleştirilmesini düzenleyen TCK m.257/2 hükmü de gündeme gelebilecektir. Fakat bu durumda özel norm olan TCK m.138 hükmü uygulanacaktır⁵⁶¹.

4.5. Soruşturma, Kovuşturma ve Yaptırım

Suçun soruşturması ve kovuşturması resen yapılır, şikâyete tabi değildir. Suçun kamu görevlisi tarafından görevi sebebiyle işlenmesi halinde soruşturma yapılabilmesi için yetkili merciin izni gerekir. Suç uzlaştırmaya tabi değildir.⁵⁶²

Suçun temel şeklinin cezası bir yıldan iki yıla kadar haptir. Nitelikli halin gerçekleşmesi durumunda ceza bir kat artırılır.

⁵⁶⁰ Koca / Üzülmaz (2020), s.597.

⁵⁶¹ Koca / Üzülmaz (2020), s.598.

⁵⁶² Kangal, s.176.

Suçun bir özel hukuk tüzel kişisi yararına tüzel kişinin organ ve temsilcileri tarafından işlenmesi durumunda tüzel kişi hakkında bunlara mahsus güvenlik tedbirlerine hükmolunur.



SONUÇ

Kişisel verilere ilişkin suçları tanımlayan ve Türk Ceza Kanunu'nun 135, 136 ve 138inci maddelerinde yer alan hükümler 2005 yılında yürürlüğe girmiştir. Bu hükümler Türk Hukuku'nda kişisel verilerin korunmasına özgülenmiş ilk hükümler olma özelliğini taşımaktadır. Kişisel verilerin korunması hukuku kendine özgü kavramları ve ilkeleri barındıran özel bir alandır. TCK'nın yürürlüğe girdiği 2005 yılından KVKK'nın yürürlüğe girdiği 2016 yılına kadar kişisel verilerin korunmasına dair usul ve esasların belirlendiği, kavramların tanımlandığı, ilkelerin açıklandığı bir kanun ülkemizde bulunmamaktadır. Bu sebeple TCK'nın bahsi geçen hükümlerinin uygulanmasında bazı sorunlarla karşılaşmıştır. Kişisel veri kavramının kanunlarla tanımlanmamış olması sebebiyle suçun maddi konusunun sınırlarının doğru tespit edilememesi bu sorunların başında gelmiştir. Madde gerekçesinde açıkça yer almasına rağmen, gerçek kişi hakkındaki her türlü bilginin kişisel veri olarak kabul edilmesinin ceza sorumluluğunu çok fazla genişleteceği düşünülmüş, kişinin kendisi tarafından alenileştirilmiş veriler ve kişinin özel alanına dahil olmayan veriler kapsam dışı bırakılmaya çalışılmıştır. Yargıtay kararlarında da uzun bir süre bu anlayışın tesiri görülmüştür.

2016 yılında KVKK'nın yürürlüğe girmesi ile birlikte başta kişisel veri kavramı olmak üzere konuyla ilgili kavramlar kanuni tanıma kavuşmuş, veri işleme süreçlerine hâkim ilkeler açıklanmış, hangi şartların varlığı halinde ilgilinin açık rızası olmadan kişisel verilerin işlenebileceği kanunla belirlenmiştir. Kişisel veriler bahsi geçen suç tiplerinin maddi konusunu oluşturduğu için kişisel veri kavramının kanuni tanıma kavuşması suçun maddi konusu etrafındaki tartışmaların bir hayli azalmasını sağlamıştır. Kişinin yalnızca özel alanına ilişkin verileri değil her türlü verisi suçun konusu olarak kabul edilmeye başlanmıştır. Bizce de doğru olan budur. Bir verinin kişisel veri olarak kabul edilmesi için kişinin özel hayat alanına ait olması şart değildir. Zira kişinin, özel alanına ilişkin olmayan ve herkes tarafından bilinebilir nitelikte olan verilerinin hukuka aykırı şekilde işlenmesiyle de çeşitli mağduriyetlere uğraması mümkündür. Kişinin kendisi tarafından alenileştirilmiş veriler ancak alenileştirme amacına uygun olarak işlendiğinde hukuka uygun bir veri

işlemeden söz edilebilir. Bu verilerin alenileştirilme amacının dışında kullanılması ise hukuka aykırı olmaya devam edecektir. Verinin alenileşmiş olması kişisel veri niteliğini kaybetmesine sebep olmaz. Örneğin kişinin herkese açık sosyal medya profilinde yayınladığı fotoğrafının alınıp bir arkadaşlık sitesinde sahte profil oluşturmak için kullanılması durumunda kişisel veriler hukuka aykırı olarak yayılmıştır. Öğretide aksi görüşler olsa da Yargıtayın güncel uygulaması da bu şekildedir.

Suçun maddi konusuna ilişkin bir diğer tartışma tüzel kişilere ait verilerin suçun konusunu oluşturup oluşturmayacağı hakkındadır. KVKK henüz tasarı aşamasındayken tüzel kişilere ait veriler de tasarı kapsamında yer almıştır. Ancak kanunlaştırma esnasında tüzel kişiler kapsam dışı bırakılmıştır. KVKK yürürlüğe girmeden önce bazı yazarlar gerek tasarıdan gerek bazı AYM kararlarından etkilenecek tüzel kişilere ait verilerin de suçun maddi konusunu oluşturabileceğini savunmuştur. Bugün de bu görüşü savunanlar mevcuttur. Ancak KVKK'nın yürürlükteki hali, TCK m.135'in gerekçesi, Yargıtay'ın yerleşik uygulaması ve öğretideki yaygın kabul dikkate alındığında tüzel kişilere ait verilerin suçun maddi konusunu oluşturmayacağını kabul etmek gerekmektedir.

KVKK'nın yürürlüğe girmesi ile bazı tartışmalar son bulmuş fakat bazı yeni tartışmalar gündeme gelmiştir. Bu tartışmalardan en önemlisi KVKK m.17/2 hükmü hakkındadır. Öğretide bazı yazarlar KVKK m.17/2 hüküm ile yeni bir suç tipi ihdas edildiği görüşündedir. Bizim de katıldığımız diğer bir görüşe göre ise kanun koyucu bu hükümle TCK m.138 hükmünün KVKK m.7'ye aykırı davranışlar için de uygulanacağını teyit etmek istemiştir. Kanaatimizce bu tartışmaya kanun koyucunun özensizliği sebep olmuştur. Şayet kişisel verilerin silinmemesi ve anonim hale getirilmemesi fiillerinin de TCK m.138 kapsamına gireceği teyit edilmek isteniyorsa yok etme fiilinin bu fiilleri kapsayacak şekilde tanımlanması ile bu sağlanabilirdi. Yahut silme ve anonim hale getirme fiilleri TCK m.138'e seçimlik hareketler olarak eklenebilirdi. Kanaatimizce bu iki yöntemden birisi benimsenerek ilgili hükümlerin yeniden düzenlenmesi tartışmaların giderilmesi için gereklidir.

KVKK'nın kabulüyle birlikte tartışma konusu haline gelen bir diğer husus TCK'daki suç tiplerinin fiil unsurudur. KVKK'da veri işleme kişisel veriler *üzerindeki* “tamamen veya kısmen otomatik yollarla veya bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla” gerçekleştirilen her türlü işlem olarak tanımlanmıştır.

Öğretide bazı yazarlar TCK m.135'te yer alan verileri kaydetme suçunun fiil unsurunun oluşması için *“tamamen veya kısmen otomatik yollarla veya bir veri kayıt sisteminin parçası olmak üzere otomatik olmayan yollarla”* verilerin kaydedilmesi gerektiğini ifade etmiştir. TCK m.135'in kanuni tanımında ise fiil unsuru için böyle bir şart aranmamaktadır. Suçun fiil unsuru veri işleme değil verileri kaydetme olarak tanımlanmıştır. Ne TCK m.135 için ne de m.136 ve 138 için böyle bir kriter getirilmesi doğru değildir. Zira KVKK kapsamına girmeyen fiiller için de TCK hükümlerinin uygulanmasına devam edileceği KVKK gerekçesinde de açıkça ifade edilmiştir. Esasen kanunların lafzı da böyle bir yoruma imkân verebilecek nitelikte değildir. Bu yorum TCK hükümlerinin uygulama alanını gereksiz şekilde daraltacak ve uygulamada ciddi problemlere yol açabilecek niteliktedir.

KVKK'nın yürürlüğe girmesi ile TCK'da yer alan suçların fiil unsurları bakımından ikili bir durumun oluştuğunu söylemek gerekir. Şayet fiil unsurunu oluşturan kişisel verileri kaydetme, ele geçirme, verme veya yayma fiilleri KVKK kapsamına girecek bir şekilde gerçekleşmiş ise KVKK hükümleri uygulama alanı bulacaktır. Bu fiiller KVKK kapsamına girmeyecek bir şekilde gerçekleşmiş ise KVKK hükümleri doğal olarak uygulanmayacaktır. KVKK hükümlerinin uygulanıp uygulanmayacağını tespit etmek özellikle suçun hukuka aykırılık unsurunun değerlendirilmesi noktasında hayati önem taşımaktadır. Çünkü KVKK'da yalnızca bu kanun kapsamına giren fiiller için uygulanabilecek bazı hukuka uygunluk sebepleri (veri işleme şartları) öngörülmüştür. KVKK kapsamına giren fiiller için hem bu hukuka uygunluk sebepleri hem de genel hukuka uygunluk sebepleri gündeme gelebilecektir. KVKK kapsamına girmeyen fiiller için ise yalnızca genel hukuka uygunluk sebepleri uygulanacaktır. Ayrıca KVKK kapsamına giren fiillerin hukuka uygunluğu değerlendirilirken veri işleme sürecine hâkim ilkeler de göz önünde bulundurulacaktır. KVKK m.28/1'de düzenlenen tam istisna hallerinde KVKK hükümlerinin uygulanmayacağına özellikle dikkat edilmelidir. Bazı yazarlar m.28/1'de yer alan istisna hallerini hukuka uygunluk sebepleri olarak nitelendirse de kanaatimizce bu yorum yanlıştır. İstisna halleri 6698 sayılı kanunun uygulanmayacağı halleri düzenlemiştir. Bu durumlarda diğer kanunların hükümleri ve dolayısıyla TCK hükümleri uygulanmaya devam edecektir.

KVKK kapsamına giren bir fiil hakkında değerlendirme yapılırken öncelikli olarak başvurulması gereken kanun KVKK'dır. Örneğin rıza hem TCK'da hem KVKK'da

düzenlenmiş bir hukuka uygunluk sebebidir. KVKK’da rızaya ilişkin şartlar TCK’ya göre daha katıdır. KVKK’da özel düzenleme olması sebebiyle KVKK kapsamına giren fiiller TCK’da yer alan genel rıza ile hukuka uygun hale gelemeyecektir, açık rıza aranacaktır. KVKK hükümleri ile çelişmeyen diğer kanun hükümleri ise uygulanmaya devam edecektir.

Bu suç tipleri bakımından tartışma oluşturan bir diğer husus madde metinlerinde yer alan “*hukuka aykırı olarak*” ifadeleridir. Esasen bu ifadeye TCK’nın başka maddelerinde de yer verilmiştir. Bu ifadeye ilişkin tartışma bu suçlara özgü değildir. Biz bu suçların tanımlarındaki (TCK m.135 ve 136) “*hukuka aykırı olarak*” ifadelerinin tipikliğe dahil olmadığını, tipik haksızlığın tamamının değerlendirilmesine ilişkin olduğunu düşünüyoruz. Bizim de katıldığımız görüşe göre tipik haksızlığın tamamını niteleyen bu tür ifadeler hukuka aykırılık unsuru bakımından yeni bir durum doğurmaz. Kanun koyucu bu suçlar için bir hukuka uygunluk sebebinin bulunabileceği konusunda hâkimi uyarmaktadır. Bununla birlikte bu ifadenin tek fonksiyonu hukuka aykırılık alanına ilişkin değildir. Bu ifade kusurluluk alanındaki haksızlık bilinci için de bir bağlantı noktası oluşturmaktadır. Kanun koyucu bu suçların doğrudan haksızlık bilinci ile işlenmesini failin kusurlu kabul edilebilmesi için gerekli görmektedir. Ancak TCK’nın haksızlık yanılığını düzenleyen m.30/4 hükmü failin kusursuz kabul edilebilmesi için haksızlık yanılığının kaçınılmaz olmasını şart koşturmaktadır. Kanaatimizce TCK’nın m.30/4 hükmüne kaçınılabilir haksızlık yanılığı hallerinin de bazı durumlarda cezalandırılmamasını sağlayacak bir hüküm eklenmelidir. Böylece bu suçların (TCK m.135 ve m.136) doğrudan haksızlık bilinci ile işlenmesinin failin cezalandırılabilirliği için gerekli olduğu, haksızlık yanılığı hallerinde ceza verilmemesi gerektiği kabul edilebilir hale gelecektir. TCK’nın mevcut hali kanaatimizce böyle bir uygulama yapmaya müsait değildir.

TCK m.135’te yer alan kaydetme fiili ile m.136’da yer alan ele geçirme fiillerinin birbirinden farklı anlamlar taşıdığını kabul etmek gerekir. Kanaatimizce bu iki fiili birbirinden ayıran nokta failin erişim yetkisi bulunmayan bir verinin söz konusu olmasıdır. Şayet kişi erişim yetkisi olan bir veriyi hukuka aykırı olarak kaydediyorsa kişisel verileri kaydetme suçundan, erişim yetkisi olmayan bir veriyi hukuka aykırı şekilde erişerek kaydediyorsa kişisel verileri ele geçirme suçundan bahsedilmelidir.

TCK m.135 ve 136 hükümleri uygulanırken içtima veya görünüşte içtima hallerinden birinin bulunup bulunmadığı da titizlikle araştırılmalıdır.

TCK ve KVKK'nın sözünü ettiğimiz hükümleri gözden geçirilmeli, karışıklıklara sebebiyet veren yerler baştan düzenlenmelidir. Yargıtay kişisel veri kavramının kapsamı, hukuka aykırılık unsuru ve kusurluluk konularını birbirine karıştırmadan, bu konuların her birini somut olayda titizlikle incelemelidir. Somut olay adaletini sağlamak için kavramların esnetilmesi yerine, uygulamada birlik oluşturacak istikrarlı görüşler benimsenmesi gerekmektedir. Hukuka aykırılık unsuru ve kusurluluk bağlamındaki değerlendirmeler sağlıklı şekilde yapılarak da somut olay adaletinin sağlanması pekâlâ mümkündür. Mevzuattaki eksiklikler yargı kararlarına yansıtılmalı, kanun koyucu eksiklikleri gidermeye yönlendirilmelidir.

KAYNAKÇA

Açıkgöz, Emre İkbāl (2017) Bilişim Sistemi Aracılığıyla Haksız Yarar Sağlama Suçu (Yüksek Lisans), Ankara Yıldırım Beyazıt Üniversitesi Sosyal Bilimler Enstitüsü.

Akdağ, Hale (2013) Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması, 1. Baskı, Ankara, Adalet Yayınevi.

Akgül, Aydın (2013) Kişisel Verilerin Korunması Açısından İdarenin Hukuki Sorumluluğu ve Yargısal Denetim (Doktora), Kocaeli Üniversitesi Sosyal Bilimler Enstitüsü.

Akıncı, Ayşe Nur (2017) Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi, Kalkınma Bakanlığı Yayın No:2968.

Akkurt, Sinan Sami (2020) 'Kişisel Veri Kavramının Hukuki Niteliğine İlişkin Yaklaşımlara Mukayeseli Bir Bakış' Kişisel Verileri Koruma Dergisi, C:2, S:1, (s.20-32).

Akkurt, Sinan Sami (2020) Sosyal Medyada Gerçekleşen İhlaller Karşısında Kişilik Hakkının Korunması, 2. Baskı, Ankara, Seçkin.

Aksoy, Hüseyin Can, (2008) Kişisel Verilerin Korunması (Yüksek Lisans), Ankara Üniversitesi Sosyal Bilimler Enstitüsü.

Akyürek, Güçlü (2021) Özel Hayatın Gizliliğini İhlal Suçu, 3. Baskı, Ankara, Seçkin.

Alşahin, Mehmet Emin (2014) 'Göreve İlişkin Sırrın Açıklanması Suçu' Marmara Üniversitesi Hukuk Fakültesi Dergisi, C:20, S:2, (s.219-250).

Altuner, İlyas (2015) 'Hipokrat Yemini' Iğdır Üniversitesi Sosyal Bilimler Dergisi, S:7, (s.1-7).

Antalya, Gökhan / Topuz, Murat (2021) Medeni Hukuk Cilt: I, 4. Baskı, Ankara, Seçkin.

Artuk, Mehmet Emin / Gökçen, Ahmet / Alaşahin, Mehmet Emin / Çakır, Kerim (2019) Ceza Hukuku Genel Hükümler, 13. Baskı, Ankara, Adalet Yayınları.

Aydın, Sedat Erdem (2015) AİHM İçtihatları Bağlamında Kişisel Verilerin Kaydedilmesi Suçu, 1. Baskı, İstanbul, On İki Levha Yayınları.

Baskın, Onur (2021) Türk Hukuku Bakımından Kişilik Hakkı Kapsamında Kişisel Verilerin Korunması, 1. Baskı, Ankara, Seçkin.

Başalp, Nilgün (2003) Kişilik Hakkının Korunması Sorunu Çerçevesinde Kişisel Verilerin Korunması ve Saklanması (Yüksek Lisans), İstanbul Üniversitesi Sosyal Bilimler Enstitüsü.

Bayraktar, Köksal / Evik, Vesile Sonay / Kangal, Zeynel T. / Yıldız, Ali Kemal / Zafer, Hamide ve diğerleri (2021) Özel Ceza Hukuku Cilt IX – Kamu İdaresinin Güvenilirliğine ve İşleyişine Karşı Suçlar, 1. Baskı, İstanbul, On İki Levha Yayınları

Bilir, Faruk (2021) ‘Kişisel Verilerin Korunması Kişinin Kendisinin Korunmasıdır’ TRT Akademi Dergisi, C:6, S:11, (s.172-181).

Birtek, Fatih (2012) Haberleşmenin Gizliliğini İhlal Suçları, 1. Baskı, Ankara, Seçkin.

Börekçi, Eşref Barış (2020) Kişisel Verileri Verme, Yayma veya Ele Geçirme Suçu, 1. Baskı, İstanbul, On İki Levha Yayınları.

Bük, Alaattin (2018) Bilişim Alanında Kişisel Verilerin Korunması, 1. Baskı, Ankara, Seçkin.

Bygrave, Lee A. (2002) Data Protection Law: Approaching Its Rationale, Logic and Limits, Hollanda, Kluwer Law International.

Çelik, Işıl (2022) 6698 Sayılı Kişisel Verilerin Korunması Kanunu ve 2016/679 Sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü Kapsamında Kişisel Verilerin Yurt Dışına Aktarılması (Yüksek Lisans), İstanbul Üniversitesi Sosyal Bilimler Enstitüsü.

Çırak, Ezgi (2022) ‘Ticari Sırrın İfşasından Doğan Ceza Sorumluluğuna İlişkin Türk ve Alman Hukuk Sistemlerindeki Güncel Durumun Değerlendirilmesi’ Ticaret ve Fikri Mülkiyet Hukuku Dergisi, C:8, S:1, (s.179-206).

Çokmutlu, Metin (2014) Türk Ceza Hukukunda Kişisel Verilerin Korunması (Doktora), Kocaeli Üniversitesi Sosyal Bilimler Enstitüsü.

Demirbaş, Timur (2022) Ceza Hukuku Genel Hükümler, 17. Baskı, Ankara, Seçkin Yayınları.

Dolgun, Uğur (2004) ‘Gözetim Toplumunun Yükselişi: Enformasyon Toplumundan Gözetim Topluma’ Yönetim Bilimleri Dergisi, C:2, S:1, (s.55-74).

Duman, Berat (2020) Anayasa Hukukunda Kişisel Verilerin Korunması (Doktora), Selçuk Üniversitesi Sosyal Bilimler Enstitüsü.

Dülger, Murat Volkan (2021) Bilişim, Kişisel Verilerin Korunması ve İnternet iletişimi Mevzuatı, 7. Baskı, Ankara, Seçkin.

Epözdemir, Rezan (2019) ‘Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme Suçu’ Terazi Hukuk Dergisi, C:14, S:151, (s.528-544).

Erdoğan, İhsan / Keskin, Dilşad (2020) Türk Medeni Hukuku, 3. Baskı, Ankara, Gazi Kitabevi.

Erdoğan, Yavuz (2013) ‘Kişisel Verilerin Korunması Bakımından Türk Ceza Kanunu Hükümlerinin Değerlendirilmesi’ ERÜHFD, C:8, S:2, Doğan Soyaslan Armağanı, (s.569-632).

Ersoy, Uğur (2009) Bir İnsan Hakları Kavramı Olarak Kişisel Verilerin Korunması (Yüksek Lisans), Gazi Üniversitesi Sosyal Bilimler Enstitüsü, s.79.

Göktürk, Neslihan (2014) ‘Türk Hukuku’nda Suçların İçtimai’ Ceza Hukuku ve Kriminoloji Dergisi, C:2, S:1-2, (s.31-59).

Göktürk, Neslihan (2016) ‘Suçun Yasal Tanımında Yer Alan Hukuka Aykırılık İfadesinin İcra Ettiği Fonksiyon’ İnönü Üniversitesi Hukuk Fakültesi Dergisi, C:7, S:1, (s.407-450).

Gültekin, Nil Melek (2012) Kişisel Verilerin Ceza Hukuku Yönünden Korunması (Yüksek Lisans) Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü.

Hafizoğulları, Zeki / Özen, Muharrem (2010) Türk Ceza Hukuku Özel Hükümler: Kişilere Karşı Suçlar, Ankara, U S-A Yayınları.

Hakeri, Hakan (2022) Tıp Ceza Hukuku, 2. Baskı, Ankara, Seçkin.

İçel, Kayıhan (1972) Suçların İçtimai, İstanbul Üniversitesi Yayınları, Yayın No: 1762.

İçel, Kayıhan (2020) ‘Ceza Hukuku Açısından Kişisel Verilerin Korunmasında “Kişisel Veri” ve “Hukuka Aykırılık” Kavramları’ İstanbul Barosu Dergisi, C:94, S:2, (s.15-23).

Kangal, Zeynel Temel (2019) Kişisel Verilerin Ceza ve Kabahatler Hukukunda Korunması, 1. Baskı, İstanbul, On İki Levha Yayınları.

Karagülmez, Ali (2014) Bilişim Suçları ve Soruşturma – Kovuşturma Evreleri, 5. Baskı, Ankara, Seçkin.

Karınçu, Sümeyra (2019) Kişisel Verilerin Korunması Kanunu Kapsamında Aydınlatma Yükümlülüğünün Yerine Getirilmemesi Kabahati (Yüksek Lisans), İstanbul Üniversitesi Sosyal Bilimler Enstitüsü.

Ketizmen, Muammer (2006) Türk Ceza Hukukunda Bilişim Suçları (Doktora), Ankara Üniversitesi Sosyal Bilimler Enstitüsü.

Koca, Mahmut / Üzülmez, İlhan (2022) Ceza Hukuku Genel Hükümler, 15. Baskı, Ankara, Seçkin.

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

Korkmaz, İbrahim (2019) Kişisel Verilerin Ceza Hukuku Kapsamında Korunması, 2. Baskı, Ankara, Seçkin.

Köse Aysun, Melike (2021), Kişisel Verilerin Kaydedilmesi Suçu, 2. Baskı, Ankara, Seçkin Yayınları.

Küzeci, Elif (2021) Kişisel Verilerin Korunması, 4. Baskı, İstanbul, On İki Levha Yayıncılık.

Lyon, David (1994) The Electronic Eye, Cambridge, Polity Press.

Maden, Mehmet (2021) Ceza Hukukunda Kişisel Verilerin Korunması, 1. Baskı, Ankara, Adalet Yayınları.

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

Nur, Pınar (2022) Vergi Hukuku Açısından Kişisel Verilerin Korunması (Doktora), Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü.

Orhan, Uğur (2021) ‘Kişisel Verilerin Korunmasına İlişkin Türk Ceza Hukuku Düzenlemeleri Üzerine Değerlendirme’ Ankara Üniversitesi Hukuk Fakültesi Dergisi, C:70, S:4, (s.1359-1384).

Özbek, Veli Özer (2008) Yeni Türk Ceza Kanunu’nun Anlamı (TCK İzmir Şerhi), 1.Baskı, Ankara, Seçkin Yayıncılık, Cilt: 2.

Özbek, Veli Özer / Doğan, Koray / Bacaksız, Pınar (2022) Türk Ceza Hukuku Genel Hükümler, 13. Baskı, Ankara, Seçkin.

Özbek, Veli Özer / Doğan, Koray / Bacaksız, Pınar (2022) Türk Ceza Hukuku Özel Hükümler, 17. Baskı, Ankara, Seçkin.

Özen, Muharrem / Köksal, Atacan (2020) ‘Göreve İlişkin Sırrın Açıklanması Suçu’ Ankara Üniversitesi Hukuk Fakültesi Dergisi, C:69, S:1, (s.189-232)

Özgenç, İzzet (2022) Türk Ceza Hukuku Genel Hükümler, 15. Baskı, Ankara, Seçkin.

Özkan, Oğulcan (2020) Kişisel Verilerin Korunması (Yüksek Lisans), Ankara Üniversitesi Sosyal Bilimler Enstitüsü.

Öztürk, Bahri / Seyhan, Serkan / Altınok Çalışkan, Elif (2022) Kişisel Verilerin Korunması Hukuku, 2. Baskı, Ankara, Seçkin.

Öztürk, Mustafa Kağan (2022) Ceza Hukukunda Zincirleme Suç, 1. Baskı, Ankara, Seçkin.

Petek, Hasan (2015) Kişilik Değerlerinin Ölümden Sonra Korunması, 1. Baskı, Ankara, Yetkin.

Roxin, Claus (2006) Yasağa İlişkin Yanılma (Çev.:Osman İsfen), Suç Politikası, Karşılaştırmalı Güncel Ceza Hukuku Serisi 5, Ankara.

Sağlam, Tuğba (2020) Türk Ceza Hukukunda Kişisel Verilerin Korunması (Yüksek Lisans), Ankara Üniversitesi Sosyal Bilimler Enstitüsü.

Sariusta, Kader (2018) Kişisel Verilerin Ceza Hukuku Yoluyla Korunması (Yüksek Lisans), Gaziantep Üniversitesi Sosyal Bilimler Enstitüsü.

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

Soyaslan, Doğan (2022) Ceza Hukuku Genel Hükümler, 10. Baskı, Ankara, Yetkin Yayınları.

Soyaslan, Doğan (2020) Ceza Hukuku Özel Hükümler, 13. Baskı, Ankara, Yetkin Yayınları.

Soyer Güleç, Sesim (2008) ‘Türk Ceza Kanunu’nda Haksızlık Yanılgısı’ Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, C:10, S:1, (s. 59-91).

Soysal, Tamer (2019) ‘Unutulma Hakkının Avrupa Birliği’nin Genel Veri Koruma Tüzüğü Çerçevesinde İncelenmesi’ Uyuşmazlık Mahkemesi Dergisi, S:13, (s. 339-422).

Suluk, Cahit / Karasu, Rauf / Nal, Temel (2021) Fikri Mülkiyet Hukuku, 5. Baskı, Ankara, Seçkin.

Sümer, Haluk Hadi (2020) Hukuka Giriş, 4. Baskı, Ankara, Seçkin.

Şen, Ersan (2006) Yeni Türk Ceza Kanunu Yorumu, İstanbul, Vedat Kitapçılık, Cilt:1.

Şimşek, Sıla Türkan (2020) Kişisel Verilerin Kaydedilmesi Suçu (Yüksek Lisans), Bahçeşehir Üniversitesi Sosyal Bilimler Enstitüsü.

Taşçı Aydemir, Ece (2022) Kişisel Verilerin Kaydedilmesi Suçu, 1. Baskı, Ankara, Seçkin Yayınları.

Taştan, Furkan Güven (2017) Türk Sözleşme Hukukunda Kişisel Verilerin Korunması, 1. Baskı, İstanbul, On İki Levha Yayınları.

Tekgül, Ahmet Tamer (1997) Bilgi Toplumu ve İnternet (Yüksek Lisans), İstanbul Üniversitesi Sosyal Bilimler Enstitüsü.

Titrek, Gizem Büşra (2020) Türk Ceza Hukukunda Kişisel Verilerin Korunmasına Yönelik Suçlar (Yüksek Lisans), Uludağ Üniversitesi Sosyal Bilimler Enstitüsü.

Tozman, Önder (2009) ‘İhmal Suçlarında Teşebbüs ve Gönüllü Vazgeçme’ Türkiye Barolar Birliği Dergisi, S:84.

Turan Başara, Gamze (2020) ‘Kişiliğin Korunması Kapsamında Ölümden Sonra Hatıranın Korunması Teorisi’ Çankaya Üniversitesi Hukuk Fakültesi Dergisi, C:5, S:1, (s.341-390).

Uçak, Murat (2021) ‘Kişisel Verilerin Ölümden Sonra Korunması’ İMHFD, C:VI, S:10, (s. 97-123).

Uyar, Lema (2006) Birleşmiş Milletler’de İnsan Hakları Yorumları, 1. Baskı, İstanbul, Bilgi Üniversitesi Yayınları.

Uyarer, Sinem Göçmen (2020) Kişisel Verilerin Korunması, 2. Baskı, Ankara, Seçkin.

Üstün, Ezgi (2020) Gözetim Toplumu Olgusunun Sosyal Medya Bağlamında Değerlendirilmesi (Yüksek Lisans), Pamukkale Üniversitesi Sosyal Bilimler Enstitüsü.

Yaşar, Osman / Gökcan, Hasan Tahsin / Artuç, Mustafa (2010) Yorumlu Uygulamalı Türk Ceza Kanunu, 1. Baskı, Ankara, Adalet Yayınevi, C: 3.

Yıldız, Gamze (2022) Kişisel Verilerin Korunması Bağlamında Verileri Yok Etmeme Suçu (Yüksek Lisans), Ankara Üniversitesi Sosyal Bilimler Enstitüsü.

Yılmaz, Berrak (2019) Türk Anayasa Mahkemesi ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması (Doktora), Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü.

Yılmaz, Sacit (2016) Türk Ceza Hukuku Sisteminde Siber Suçlar, 1. Baskı, Ankara, Adalet Yayınları.

Yokuş Sevik, Handan (2009) ‘Haberleşmenin Gizliliğini İhlal Suçu’ Dicle Üniversitesi Hukuk Fakültesi Dergisi, C:12-13, S:16-17-18-19, (s.159-195).

Yüzbaşı Tobaz, Firdevs (2021) Uluslararası İnsan Hakları Hukukunda ve Türk Hukukunda Kişisel Verilerin Korunması (Doktora), Trabzon Üniversitesi Lisansüstü Eğitim Enstitüsü.

<https://sozluk.gov.tr>

<https://www.oecd.org/>

<http://www2.tbmm.gov.tr/>

<https://gdpr.eu/tag/gdpr/>

<https://normkararlarbilgibankasi.anayasa.gov.tr/>

<https://www.mevzuat.gov.tr/>

<https://www.resmigazete.gov.tr/>

<https://www.kvkk.gov.tr/>

<https://ec.europa.eu/>

<https://hudoc.echr.coe.int/eng?i=001-59665>

<https://inhak.adalet.gov.tr/>

<https://www.coe.int/>

<https://www.ab.gov.tr/>

<https://eur-lex.europa.eu/>

<http://www.bilgitoplumu.gov.tr/>

<https://www.cnil.fr/>

