T.C.

ANKARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI

TÜRK CEZA HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASI

YÜKSEK LİSANS TEZİ

TUĞBA SAĞLAM
16911845

ANKARA 2020

T.C.

ANKARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI

TÜRK CEZA HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASI

TEZLİ YÜKSEK LİSANS TEZİ

TUĞBA SAĞLAM
16911845

Danışman
PROF. DR. MUHARREM ÖZEN

ANKARA 2020

T.C.

ANKARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI

TÜRK CEZA HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASI

TEZLİ YÜKSEK LİSANS TEZİ

TUĞBA SAĞLAM
16911845

Danışman
PROF. DR. MUHARREM ÖZEN

TEZ JÜRİSİ ÜYELERİ

Adı ve Soyadı	İmzası
1- Prof. Dr. Muharrem ÖZEN	
2- Doç. Dr. Önder TOZMAN	
3- Doç. Dr. Fahri Gökçen TANER	
4-	
5-	

Tez Savunması Tarihi

31.08.2020

T.C. Ankara Üniversitesi Sosyal Bilimler Enstitüsü Müdürlüğü'ne,

Prof. Dr. Muharrem ÖZEN danışmanlığında hazırladığım "Türk Ceza Hukukunda Kişisel Verilerin Korunması (Ankara.2020) " adlı yüksek lisans tezimdeki bütün bilgilerin akademik kurallara ve etik davranış ilkelerine uygun olarak toplanıp sunulduğunu, başka kaynaklardan aldığım bilgileri metinde ve kaynakçada eksiksiz olarak gösterdiğimi, çalışma sürecinde bilimsel araştırma ve etik kurallarına uygun olarak davrandığımı ve aksinin ortaya çıkması durumunda her türlü yasal sonucu kabul edeceğimi beyan ederim.

Tarih: **Adı Soyadı : Tuğba SAĞLAM**

İÇİNDEKİLER

KISALTMALAR VI

GİRİŞ 1

BİRİNCİ BÖLÜM: KAVRAM OLARAK KİŞİSEL VERİ VE KİŞİSEL VERİLERİN KORUNMASI 3

I. KİŞİSEL VERİ ve UNSURLARI 3

A. GENEL OLARAK 3

B. KİŞİSEL VERİNİN UNSURLARI 7

1. Her Türlü Bilgi 8

2. Kimliği Belirli veya Belirlenebilir Bir Gerçek Kişi 10

3. Bilginin kişiye ilişkin olması 12

C. ÖZEL NİTELİKLİ KİŞİSEL VERİ 14

II. KİŞİSEL VERİLERİN KORUNMASININ TARİHÇESİ ve ULUSLARASI DÜZENLEMELER 17

A. TARİHÇE 17

B. ULUSLARARASI DÜZENLEMELER 21

1. OECD Rehber İlkeleri 21

2. Avrupa Konseyi 22

a. Avrupa İnsan Hakları Sözleşmesi 23

b. 108 sayılı Sözleşme 24

3. Birleşmiş Milletler Rehber İlkeleri 26

4. Avrupa Birliği 28

a. Genel Olarak 28

b. 95/46/EC sayılı Direktif 31

b. Genel Veri Koruma Tüzüğü (GDPR) 35

III. KİŞİSEL VERİLERİN KORUNMASI HAKKININ HUKUKİ NİTELİĞİ .. 37

A. GENEL OLARAK 37

B. MÜLKİYET HAKKI GÖRÜŞÜ 38

C. FİKRİ MÜLKİYET HAKKI GÖRÜŞÜ 40

D. KİŞİLİK HAKKI GÖRÜŞÜ 41

IV. KİŞİSEL VERİLERİN İŞLENMESİ 45

A. VERİ SORUMLUSU, VERİ İŞLEYEN VE DİĞER BAZI KAVRAMLAR 45

1. Veri Sorumlusu 45

2. Veri İşleyen 46

3. Diğer Bazı Kavramlar 46

B. KİŞİSEL VERİLERİN İŞLENMESİNDE TEMEL İLKELER 48

1. Genel Olarak 48

2. Kişisel Verilerin Hukuka ve Dürüstlük Kurallarına Uygun Olarak İşlenmesi 48

3. Kişisel Verilerin Toplanma Amaçlarının Belirli, Açık ve Meşru Olması.... 49

4. Kişisel Verilerin İşlendikleri Amaçla Bağlantılı, Sınırlı ve Ölçülü Olması. 50

5. Toplanan Kişisel Verilerin Doğru Olması ve Güncel Olarak Tutulması 52

6. Kişisel Verilerin Saklama Sürelerinin Belirli Olması 53

C. KİŞİSEL VERİLERİN İŞLENME ŞARTLARI 53

1. Genel Olarak 53

2. İlgili kişinin açık rızasının alınması 54

3. Açık rıza alınması haricinde kişisel verilerin işlenmesi 55

D. ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN İŞLENMESİ 57

İKİNCİ BÖLÜM: TÜRK HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASI 59

I. TÜRK CEZA KANUNU DIŞINDA TÜRK HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASI 59

A. ANAYASA 59

B. KİŞİSEL VERİLERİN KORUNMASI KANUNU(KVKK) 62

C. DİĞER KANUNLARDAKİ DÜZENLEMELER 63

1. Türk Medeni Kanunu ve Türk Borçlar Kanunu 63

2. İş Kanunu 64

3. Bilgi Edinme Kanunu 64

4. Fikir ve Sanat Eserleri Kanunu 65

II. TÜRK CEZA KANUNU'NDA KİŞİSEL VERİLERİN KORUNMASI 65

A. GENEL OLARAK 65

B. KİŞİSEL VERİLERİN KAYDEDİLMESİ SUÇU (TCK m. 135) 66

1. Genel Olarak 66

2. Hukuki Konu 73

3. Fail 75

4. Mağdur 76

5. Suçun Unsurları 77

a. Maddi Unsur 77

b. Manevi Unsur 83
c. Hukuka Aykırılık 84
6. Suçun Özel Görünüş Şekilleri 92
a. Teşebbüs 92
b. İştirak 92
c. İçtima 93
7. Suçun Nitelikli Halleri 94
8. Yaptırım 96
9. Soruşturma ve Kovuşturma 97
C. VERİLERİ HUKUKA AYKIRI OLARAK VERME veya ELE GEÇİRME SUÇU(TCK m. 136) 98
1. Genel Olarak 98
2. Hukuki Konu 98
3. Fail 99
4. Mağdur 99
5. Suçun Unsurları 99
a. Maddi Unsur 99
b. Manevi Unsur 110
c. Hukuka Aykırılık 111
6. Suçun Özel Görünüş Şekilleri 114
a. Teşebbüs 114
b. İştirak 114

c. İçtima 115
7. Suçun Nitelikli Halleri 116
8. Yaptırım 117
9. Soruşturma ve Kovuşturma 117
D. VERİLERİ YOK ETMEME SUÇU(TCK m. 138) 118
1. Genel Olarak 118
2. Hukuki Konu 120
3. Fail 122
4. Mağdur 123
5. Suçun Unsurları 124
a. Maddi Unsur 124
d. Manevi Unsur 125
e. Hukuka Aykırılık 125
6. Suçun Özel Görünüş Şekilleri 126
a. Teşebbüs 126
b. İştirak 126
c. İçtima 126
7. Suçun Nitelikli Halleri 127
8. Yaptırım 127
9. Soruşturma ve Kovuşturma 128
SONUÇ 129
KAYNAKÇA 132

KISALTMALAR

AB	: Avrupa Birliği
A.B.D.	: Ana Bilim Dalı
AET	: Avrupa Ekonomik Topluluğu
AİHM	: Avrupa İnsan Hakları Mahkemesi
AİHS	: Avrupa İnsan Hakları Sözleşmesi
AKÇT	: Avrupa Kömür ve Çelik Topluluğu
AÜHFD	: Ankara Üniversitesi Hukuk Fakültesi Dergisi
AYM	: Anayasa Mahkemesi
BDSG	: Bundesdatenschutgesetz – Federal Almanya Veri Koruma Kanunu
Bkz.	: Bakınız
C.	: Cilt
CHD	: Ceza Hukuku Dergisi
CMK	: Ceza Muhakemesi Kanunu
DG	: Genel Müdürlük
E.	: Esas
EC	: Avrupa Konseyi
EU	: Avrupa Birliği
Eurotom	: Avrupa Atom Enerjisi Topluluğu
ENIAC	: Elektronik Sayısal Entegreli Hesaplayıcı
IBM	: Uluslararası İş Makinesi
OECD	: Ekonomik İşbirliği ve Kalkınma Örgütü
GDPR	: Avrupa Veri Koruma Tüzüğü

K.	: Karar
KVKK	: Kişisel Verilerin Koruması Kanunu
M.Ö.	: Milattan Önce
No.	: Numara
PC	: Kişisel Bilgisayar
S.	: Sayı
s.	: Sayfa
TAAD	: Türkiye Adalet Akademisi Dergisi
TC	: Türkiye Cumhuriyeti
Y.	: Yıl

GİRİŞ

Teknolojinin gelişmesinin ve bilgisayarın hayatımıza girmesinin ardından veri kayıtlarının tutulması kolaylaşmış ancak kişisel verileri koruma ihtiyacı doğmuştur. Her ne kadar kişisel veriler kağıt üzerine kaydedilebilir olsa da günümüzde çoğunlukla bilişim sistemleri kullanılmaktadır. Bilişim sistemleri getirdiği kolaylıklar ile birlikte büyük riskler de barındırdığından fayda sağlayan teknolojiden vazgeçilmeden bu faydalı teknolojinin adeta bir yan etkisi niteliğinde olan "kişisel veri kaybının" önlenmesi gerekir. Nitekim kişisel verilerin, kişinin en çok paylaştığı adı, soyadı, TC kimlik numarası, telefon numarası gibi bilgilerinden başlayarak ırk, cinsel hayat, siyasi görüş gibi ayrımcılığa uğramasına neden olabilecek daha mahrem bilgilerine kadar uzanan geniş yelpazesi olduğu düşünüldüğünde bu yan etki kişinin temel haklarına yönelik göz ardı edilemeyecek bir öldürücü bir etkiye sahiptir.

Teknolojinin gösterdiği bu gelişmeyle yarışacak düzeyde sosyal hayatın ve toplumsal ilişkilerin de gelişmesi, günlük hayat içinde kurulan sözleşmelerin çeşitliliğinin ve sayısının artması gibi faktörler ise kişisel verilerin dolaşımını artırmıştır. Neticeten bilişim sistemleri vasıtası ile daha kolay depolanarak ve transfer edilir hale gelen kişisel veriler günlük hayatın gereksinimi içinde kurulan sözleşmelerin çokluğu nedeniyle de sıklıkla hukuka aykırı şekilde aktarılır hale gelmiştir.

Kişisel verilerin kullanımında ve dolaşımında yaşanan bu artış özel hayatın gizlilik alanına dahil olan kişisel verilerin korunmasına dair ihtiyacı da beraberinde getirmiştir. Kişisel verilerin özel hukuk anlamında korunması yanında ceza hukuku anlamında korunması kişilerin güvende hissetmeleri için mühimdir.

Şüphesiz ki kişisel verilerin korunmasından bahsedebilmemiz için hukuka uygun olarak kaydedilmeleri, aktarılmaları ve nihayetinde yok edilmeleri gerekir.

Türk Ceza Kanunu'nun *"Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar"* bölümünde, 135. maddesinde *"Kişisel Verilerin Kaydedilmesi Suçu"*, 136. maddesinde *"Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme Suçu"* ve son olarak 138. maddesinde ise *"Verileri Yok Etmeme"* suçu düzenlenmiştir. 137. maddede ise 135. ve 136. maddelerin ortak nitelikli hallerine yer verilmiştir.

İki bölümden oluşan bu çalışmanın birinci bölümünde "kişisel veri kavramı ve unsurları", "kişisel verilerin korunmasının tarihçesi ve uluslararası düzenlemeler", "kişisel verilerin korunması hakkının hukuki niteliği ile kişisel verilerin işlenmesi" konuları, ikinci bölümünde ise "Türk Hukukunda kişisel verilerin korunması" ve neticeten "Türk Ceza Hukukunda kişisel verilerin korunması" ve bu bağlamda kanunda yer alan suç tipleri incelenmiştir. Çalışmada Türk Hukuku kapsamında suç tiplerinin incelenmesini hedeflenmekte olup çalışma karşılaştırmalı hukuktaki düzenlemeleri kapsamamaktadır. Ancak kavramın anlaşılabilmesi için ve konunun tarihçesi anlatılırken uluslararası düzenlemelerden faydalanılmıştır.

BİRİNCİ BÖLÜM: KAVRAM OLARAK KİŞİSEL VERİ VE KİŞİSEL VERİLERİN KORUNMASI

I. KİŞİSEL VERİ ve UNSURLARI

A. GENEL OLARAK

Kelime olarak *"veri"*; *"bilgi, data"* anlamlarına gelmektedir.[1] Bilgi (information) ve veri (data) kavramları ise literatürde farklı anlamlar taşımaktadır.[2] Veri; *"Bilgi işleme sürecinin temel hammaddesi olarak ve çeşitli sembol, harf rakam ve işaretlerle temsil edilen, ham, işlenmeye hazır işlenmemiş gerçekler yada izlenimler"* anlamına gelmekte olup, bilgi ise; *"verilerin, karar alma sürecine destek sunacak şekilde anlamlı bir biçime getirilmek üzere, analiz edilerek işlenmesiyle ulaşılan sonuçtur."*[3] Ancak kişisel verilerin korunması hukukunda bu ayrıma yer verilmemiş, iki kavram birbiri yerine kullanılmıştır.[4]

---

[1] Türk Dil Kurumu Güncel Türkçe Sözlük, https://www.sozluk.gov.tr/ (Erişim Tarihi: 02.12.2019)

[2] Veri (data), enformasyon (informaiton) ve bilgi (knowledge) şeklindeki üçlü ayrım için bkz.: **KÜZECİ,** Elif; Kişisel Verilerin Korunması, Ankara 2019, s. 9, **HENKOĞLU**, Türkan; Bilgi Güvenliği ve Kişisel Verilerin Korunması, Ankara 2015, s. 27. Bu şekilde yapılan üçlü ayrımda enformasyon ve bilgi arasındaki farklılık insan zihninde var olan bilginin soyuttan somuta dönüşmesi ile enformasyon oluştuğu şeklinde ortaya konulmaktadır. **HENKOĞLU**, s.9.

[3] **BENSGİR,** Türksel Kaya; Bilgi Teknolojileri ve Örgütsel Değişim, Ankara 1996, s. 8.

[4] **AKSOY**, Hüseyin Can; Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması, Ankara 2010, s. 11.

"Ekonomik İşbirliği ve Kalkınma Örgütü (Organization For Economic Co-operation and Development - OECD)" tarafından 1980 yılında yayınlanan "Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Yönlendirici İlkeler" adlı ilkelerinin 1/b maddesinde[5], Avrupa Konseyi tarafından 1981 yılında imzaya açılan "108 sayılı Kişisel Verilerin Otomatik İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşme'nin" 2/a maddesinde[6], 24 Ekim 1995 tarihli ve "95/46/EC sayılı Avrupa Parlamentosu ve Konseyi Direktifi'nin" 2/a maddesinde[7] ve "Avrupa Birliği Genel Veri Koruma Tüzüğü'nde (General Data Protection Regulation – GDPR)" "*kimliği belirli veya belirlenebilir kişiye ilişkin tüm veriler"* kişisel veri olarak tanımlanmıştır.

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun (KVKK) 3/1-d maddesinde ise *"kişisel veri"*, uluslararası metinlere uygun şekilde *"kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi"* olarak tanımlanmıştır.[8] Kanunda ve anılan diğer

[5] Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Yönlendirici İlkeler, s. 13. https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf (Erişim Tarihi: 02.12.2019)

[6] 108 sayılı Kişisel Verilerin Otomatik İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşme, https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37 (Erişim Tarihi: 02.12.2019)

[7] 95/46/EC sayılı Avrupa Parlamentosu ve Konseyi Direktifi, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN (Erişim Tarihi: 02.12.2019) Mayıs 2018'den beri bu direktifin yerini Avrupa Birliği Veri Koruma Tüzüğü almıştır. Bkz. **KÜZECİ**, Kişisel Veriler, s. 160.

[8] 24.07.2012 tarihli Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik'in 3. Maddesinde *"Belirli veya kimliği belirlenebilir gerçek ve tüzel kişilere ilişkin bütün bilgiler"* olarak tanımlanmıştır.

metinlerde kişisel verilerin neler olduğu tahdidi olarak belirtilmemiştir.[9] Bu bilgiler, kişinin *"TC kimlik numarası, fotoğrafı, telefon numarası, doğum tarihi, e-mail adresi,*

Yargıtay ise kişisel veriyi *"Kişisel veri belli veya belirlenebilir olan gerçek veya tüzel bir kişiye ilişkin her türlü bilgiyi ifade eder."* olarak tanımlamaktadır. Yargıtay Hukuk Genel Kurulu, 2014/4-56 E., 2015/1679 K., 17.06.2015 tarihli karar https://www.kazanci.com.tr/ (Erişim Tarihi : 25.03.2020)

[9] Kanun'da 3. Madde gerekçesinde *"Maddeyle, Kanunda kullanılan bazı terimlerin tanımları yapılmıştır. 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 kayıtla 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 kılabilme özellikleri nedeniyle kişisel verilerdir."* açıklamalarına yer verilmiştir. http://www.adalet.gov.tr/Tasarilar/kisisel_verilerin_korunmasi.pdf (Erişim Tarihi: 25.03.2020)

sağlık, eğitim, ikamet bilgileri, etnik kökeni" gibi kişinin doğrudan veya dolaylı olarak belirlenmesine elverişli bilgilerdir.[10]

5237 sayılı Türk Ceza Kanunu'nun *"Kişisel verilerin kaydedilmesi"* başlıklı 135. maddesi gerekçesinde, "gerçek kişiyle ilgili her türlü bilginin" kişisel veri olarak kabul edilmesi gerektiği belirtilmiştir.[11] Ayrıca, Kanun'un 134. ile 139. maddeleri arasında kişisel verilerin korunmasına dair düzenlemeler bulunmaktadır. Kanunda kişisel verinin tanımı yer almamakla beraber kişisel verilere yönelik olarak *"kişilerin özel hayatına ilişkin görüntü veya sesler", "siyasi, felsefi veya dini görüş", "ırki köken", "ahlaki eğilim", "cinsel yaşam", "sağlık durumu"* ve *"sendikal bağlantılar"* gibi kavramlara yer verilmektedir.

Anayasa Mahkemesi 12.11.2015 tarihli kararında kişisel verinin yalnızca kişinin *"kimliğini ortaya koyan bilgileri değil motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, IP adresi, hobileri, grup üyelikleri"* gibi bilgilerini de içerdiğini

[10] **ÖZGENÇ**, İzzet; Türk Ceza Kanunu Gazi Şerhi, Ankara 2005, s. 868; **KILINÇ,** Doğan; Anayasal Bir Hak Olarak Kişisel Verilerin Korunması, AÜHFD, C. 61, S. 3, 2012, s. 1090. **KORKMAZ,** İbrahim; Kişisel Verilerin Ceza Hukuku Kapsamında Korunması, Ankara 2017, s. 24. Belirleme işlemenin yapılabilmesi için bkz: **KUNER,** Cristopher; European Data Privacy Law and Online Business, Oxford University Press, 2003, s.49.

[11] **ÖZGENÇ**, s. 868.

belirtmiştir.[12] Hatta Avrupa İnsan Hakları Mahkemesi bir kararında kişinin ses renginin de kişisel veri olduğuna hükmetmiştir.[13]

B. KİŞİSEL VERİNİN UNSURLARI

Kişisel veri sayılabilecek bilgiler, teknolojik gelişmelere bağlı olarak zamanla değişkenlik gösterebileceğinden kapsamın önceden öngörülmesi ve tüm verilerin tahdidi olarak sayılması mümkün değildir. Ancak ulusal ve uluslararası mevzuat hükümleri ile içtihatlar göz önünde bulundurularak *"kişisel veri; belirli veya kimliği belirlenebilir olmak şartıyla, bir gerçek kişiye ilişkin her türlü bilgi"* olarak tanımlanmaktadır.[14]

---

[12] Anayasa Mahkemesi 2015/32 E., 2015/102 K., 12.11.2015 tarihli kararı. https://www.anayasa.gov.tr/Kararlar/GenelKurul/Basvuru_Karari/2015-102.pdf (Erişim Tarihi: 04.12.2019)

[13] AİHM P.G. ve J.H – Birleşik Krallık Davası, 444787/98 başvuru no.lu, 25.09.2001 tarihli kararı. https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-59665%22]} (Erişim Tarihi: 04.12.2019) **GÜLTEKİN,** Nil Melek; Kişisel Verilerin Ceza Hukuku Yönünden Korunması, Yayımlanmamış Yüksek Lisans Tezi, Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku A.B.D, İstanbul 2012, s. 23; **KORKMAZ**, s. 26.

[14] Bkz.; Yukarıda anılan Anayasa Mahkemesi 2015/32 E., 2015/102 K., 12.11.2015 tarihli kararı.

Tanımdan anlaşılacağı gibi kişisel verinin varlığından bahsedilmesi için bir "bilgi" bulunması, "kimliği belirli veya belirlenebilir bir gerçek kişi" olması ve bu "bilginin kişiye ilişkin olması" unsurlarının birlikte varlığı gerekir.[15]

1. Her Türlü Bilgi

95/46/EC sayılı Direktif ve KVKK uyarınca içeriğinden bağımsız olarak *"bir gerçek kişiye ilişkin tüm bilgiler"* kişisel veridir.[16] Tanımda kullanılan *"her türlü bilgi" (any information)* deyimi kişisel veri kavramının en geniş ve açıklanmaya en muhtaç unsurudur. Bu kapsama kişinin özel yaşamına dair bilgiler gireceği gibi iş ve sosyal hayatına ve ekonomik durumuna ilişkin bilgiler de girer.[17]

---

[15] AB bünyesinde kişisel verilerin korunması için 95/46/EC sayılı Direktifin 29. Maddesi uyarınca kurulan 29. Madde Çalışma Grubu kişisel veri kavramının sınırlarını belirlemede büyük öneme sahip olan 4/2007 sayılı raporunda kişisel veriyi gerçek kişi, gerçek kişinin belirli veya belirlenebilir olması, herhangi bir bilgi, bilginin kişiye ilişkin olması olarak dört unsur üzerinden incelemişse de konu bütünlüğü açısından bu çalışmada gerçek kişi ve gerçek kişinin belirli veya belirlenebilir olması unsurları birlikte ele alınmıştır. 29. Madde Çalışma Grubu 4/2007 sayılı raporu, s.6. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf (Erişim Tarihi: 04.12.2019), **KORKMAZ**, s. 27; **TAŞTAN,** Furkan Güven; Türk Sözleşme Hukukunda Kişisel Verilen Korunması, İstanbul 2017, s. 30.

[16] **KORKMAZ**, s. 27.

[17] 29. Madde Çalışma Grubu 4/2007 sayılı raporu, s. 6; **YILMAZ,** Sabire Sanem; Tıp Alanında Kişisel Verilerin Açıklanması Suçu, Ankara 2017, s. 44.

Kişinin "adı soyadı, doğum tarihi, TC kimlik numarası, medeni durumu gibi kimlik bilgileri, adresi, e-mail adresi, iş adresi, telefon numarası, dahili hattı gibi iletişim bilgileri" kişisel verilere örnektir.

Bir verinin kişisel veri sayılması için bilginin "gizli bilgi" olması dahi gerekmez, kişinin kendisi tarafından alenileştirilmiş bilgiler de kişisel veri niteliğindedir.[18] Örneğin; kişinin oturduğu evin, çalıştığı işin adresi, kullandığı aracın plakası gibi günlük hayatın akışı içinde herkes tarafından bilinebilecek bilgileri de kişisel veri olarak kabul edilmektedir.[19]

Bilginin mahiyeti açısından ise herhangi bir değer yargısı içermeyen objektif bilgiler (örneğin; kişinin kimlik bilgileri) gibi, kişisel değer yargısı içeren sübjektif bilgiler (örneğin; kişinin dürüst, zeki yahut tembel olup olmadığı gibi bilgiler) de kişisel veridir.[20] Ayrıca bilginin gerçek olması da gerekmemektedir.[21] Esasen kişisel verilerin korunmasına yönelik düzenlemelerde de bu nedenle veri sahiplerine bilgiye erişme,

[18] **AKSOY**, s. 14; **KORKMAZ**, s. 27.

[19] **KÖSE AYSUN,** Melike; Kişisel Verilerin Kaydedilmesi Suçu, Ankara 2018, s. 27-28, **KANGAL,** Zeynel T.; Kişisel Verilerin Ceza ve Kabahatler Hukukunda Korunması, İstanbul 2019, s. 22.

[20] 29. Madde Çalışma Grubu 4/2007 sayılı raporu, s. 6; **KÖSE AYSUN**, s. 27,28; AİHM ve AYM kararlarında da objektif bilgilerin kişisel veri sayılacağına hükmedilmiştir. Bkz; yukarıda bahsi geçen Anayasa Mahkemesi 2015/32 E., 2015/102 K. Sayılı, 12.11.2015 tarihli kararı.

[21] **AKDAĞ,** Hale; Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması, Ankara 2013, s. 12.

bilginin düzeltilmesini yahut silinmesini talep etme ve itiraz etme mekanizmaları öngörülmüştür.[22]

Kaydedilme şekli açısından ise numerik, grafiksel, fotografik ya da akustik her tür formattaki veri kişisel veri sayılabilir.[23]

2. Kimliği Belirli veya Belirlenebilir Bir Gerçek Kişi

Kişisel verinin ikinci unsuru ise bilginin, "kimliği belirli veya belirlenebilir bir kişiye ait" olmasıdır. 95/46/EC sayılı Direktif ve 6698 sayılı KVKK'da gerçek kişilerin kişisel verileri güvence altına alınmış olup, tüzel kişilerin verileri kapsam dışında bırakılmıştır.[24] GDPR'da, OECD ilkelerinde ve 108 sayılı Avrupa Konseyi sözleşmesinde de aynı şekilde yalnızca gerçek kişilerin kişisel verileri korunmuştur.

Ulusal ve uluslararası metinlerde kişisel verilerin gerçek kişilere ait veriler olduğunun kabul görmesinin nedeni kişisel verilerin korunması hakkının "özel hayatın gizliliği" kapsamında olması ve "özel hayatın gizliliği" ilkesinin de gerçek kişilere münhasır olmasıdır. Tüzel kişilerin ise yalnızca ticari sırlarının korunmasından

---

[22] **KORKMAZ**, s. 28.

[23] **CATE,** Fred H.; *"The Changing Face of Privacy Protection in the European Union and the United States"*, Indiana Law Review, 1999, C. 33, S. 173, s. 182; **TAŞTAN**, s. 40.

[24] Kar amacı gütmeyen tüzel kişilerin verilerinin kişisel veri sayılması yönündeki görüş için ise bkz. **TAŞTAN**, s. 33. Ancak sırf ticari gizlilik kapsamında verilerinin korunmadığı gerekçesi ile kar amacı gütmeyen tüzel kişilerin verilerini kişisel veri sayması nedeni ile bu görüşe katılmamaktayız.

bahsedilebilir. Fakat tüzel kişiye ait bir veri olsa dahi bu veriden bir gerçek kişiye ulaşılabiliyor ise yine gerçek kişinin kişisel verilerinin korunması söz konusu olacaktır.[25]

Bu konuda doktrinde en çok tartışılan konu ölenin kişisel verilerinin durumu olmuştur. Ölüm ile kişilik sona ereceğinden ölenin kişisel verilerinin KVKK korunmasından bahsedilemez.[26] Bu durumda ancak ölenin kişilik haklarının medeni hukuk kuralları çerçevesinde korunması söz konusu olabilecektir.[27] Ancak ölenin verileri hayattaki diğer bir kişinin de kişisel verisi olma niteliğini haiz ise bu durumda verinin KVKK kapsamında korunması gerekir. Genetik bir hastalığı olan ölenin bu durumunun açıklanmasının çocuğunun kişisel verisini ihlal etme anlamı taşıyacağı örneğinde olduğu gibi.[28]

Kişisel verinin ait olduğu gerçek kişinin kimliğinin *"belirli"* olması, kişinin kim olduğunun diğer kişiler tarafından anlaşılabilmesi anlamına gelirken[29] *"belirlenebilir"* olması ise kimliğinin veri ile ilişkilendirilerek dolaylı yollarla tespit edilebilmesi anlamına gelmektedir.[30] Kişinin kimliğinin belirlenebilmesi için çok basit bir bağlantı

---

[25] **AYDIN,** Sedat Erdem; AİHM İçtihatları Bağlamında Kişisel Verilerin Kaydedilmesi Suçu, İstanbul 2015, s. 9.

[26] **KANGAL**, s. 28.

[27] **AYDIN**, s. 9.

[28] **SERT**, Şeyma; Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması, Ankara 2019, s. 29. Doğmamış bir çocuğun verilerinin aynı zamanda annenin kişisel verisiyse korunması gerektiği yönünde görüş için bkz.; **ROGERS;** Arthur, *"European Data Protection to Give Unborn Children Rights?"* The Lancet, 1997, C. 349, s. 550.

[29] **İTİŞGEN,** Rezzan; *"Türk Ceza Hukukunda Kişisel Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme Suçu"* TAAD, 2015, S. 23, s. 183.

[30] **AYDIN**, s.4-5; **SERT,** s. 21-22.

yeterli ise kişisel verinin ait olduğu gerçek kişinin kimliği belirlidir.[31] Buna karşılık kişiye özgü fiziksel, fizyolojik, zihinsel, ekonomik, sosyal, kültürel veya genetik faktörün değerlendirilmesi ile mümkün olması halinde ise belirlenebilirdir.[32] Buna göre; örneğin bir kişinin telefon numarasının kullanılması halinde o kişinin kimliğinin belirli olduğundan, parmak izinin kullanılması halinde ise kimliğinin belirlenebilir olduğundan bahsedilebilir.

3. Bilginin kişiye ilişkin olması

Üçüncü unsur ise bilginin "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin" olmasıdır. Bir bilginin "kişiye ilişkin" olmaması hali söz konusu bilginin *"sahipsizlik gerekçesiyle"* koruma dışı bırakılmasına neden olur. Zira bu tür veriler esasen anonim verilerdir ve anonim veriler hem ulusal mevzuatımızda hem de Avrupa Birliği mevzuatında kapsam dışıdır.[33]

Bilginin kişiye ilişkin olması, genel olarak bilginin "o kişi hakkında" olması anlamında gelir.[34] Bu durumda bilginin içerik bakımından kişiyle ilgili olmasından bahsedilir. Ancak biraz daha ayrıntılı ifade edecek olursak bilginin içerik, amaç veya

---

[31] **SERT**, s.31.

[32] **KÖSE AYSUN**, s. 34.

[33] **AŞIKOĞLU,** Şehriban İpek; Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri, İstanbul 2018, s. 11.

[34] **AKSOY**, S. 28; 29. Madde Çalışma Grubu 4/2007 sayılı raporu, s. 16-17.

sonuç bakımından "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin olması" gerekmektedir.[35]

Burada amaç bakımından ilişkin olma durumu somut durumun özellikleri bağlamında kişinin durumunu, performansını değerlendirmek ve kişiyi belli davranışlara yönlendirmek amacıyla bilginin toplanmasıdır. Örneğin; bir üretim faaliyetinde makinelerin üretim kapasitesini tespit edebilmek için toplanan veri, makinelerin verimliliğini değil işçilerin performansını ölçmek için kullanılıyorsa, toplanan bilgi amaç bakımından kişiye ilişkindir.[36] Sonuç bakımından ilişkin olmada ise bir bilginin kullanımının kişinin hak ve menfaatlerini etkilemesi söz konusu olur.[37] Örneğin; çalışanlarının kullanımdaki araçları aracın amacına uygun kullanılıp kullanılmadığını tespit etmek amacıyla GPS sistemi ile izleyen bir işyerinde toplanan veriler sürücülerin ikamet bilgilerini de ortaya koyduğundan elde edilen bilgi sonuç açısından kişiye ilişkindir.

Somut olayın özelliğine göre bilgi bazen hem amaç hem de sonuç bakımından kişiye ilişkin olabilir. Bilginin kişiye ilişkin olmasından bahsedebilmek için biri açısından ilişkin olması yeterlidir.

---

[35] **KORFF**, Douwe; *"New Challenges to Date Protection Study-Working Paper No.2: Data Protection Laws in the EU: The Diffuculties in Meeting the Challenges Posed by Global Social and Technical Developments",* European Commission DG Justice, Freedom and Security Report, 2010, s. 42; 29. Madde Çalışma Grubu 4/2007 sayılı raporu, s. 9; **TAŞTAN** s. 42.

[36] **AKSOY** s. 29;

[37] **ERARSLAN TÜRKMEN,** Sevgi; Özel Nitelikli Kişisel Verilerin İşlenmesinde Açık Rızanın Aranmadığı Haller, İstanbul 2019, s. 21.

C. ÖZEL NİTELİKLİ KİŞİSEL VERİ

Gerek ulusal mevzuatta gerekse de uluslararası metinlerde bazı kişisel verilerin daha sıkı korumaya tabi olduğu görülmektedir ve bu özel öneme sahip verilerin varlığı kişisel verileri genel nitelikli ve özel nitelikli kişisel veriler olarak tasnifleme ihtiyacını doğurmaktadır. Kişisel veri türleri açıklanırken genel kabul gören bu ayrıma göre[38] özel nitelikli kişisel veriler hassas[39], kendine özgü özellikleri olan ve kişilerin temel hak ve özgürlükleri ile yakın ilişkili veya kişisel mahremiyet içeren verilerdir.[40] Uluslararası mevzuatta "özel nitelikli kişisel veri" kavramı kabul edilmekle beraber metinlerde bu verilerin sayı ve türleri farklılık arz etmektedir.

"Özel nitelikli kişisel veriler" kanunda tahdidi olarak sayılmış olup KVKK'nın 6. maddesine göre bu veriler "*kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı,*

---

[38] DÜLGER'e göre; kişisel veriler ilk olarak *"insanın varoluşundan kaynaklanan kişiliğine ilişkin bilgiler"* ile *"insanın modern bilişim toplumunda yer alması nedeniyle kendisine verilen ya da çeşitli hizmetlere ulaşmasında kullanılan bilgiler"* şeklindeki ikiye ayrılır. Ancak yazarın da belirttiği üzere bu ayrım kişisel verilerin değeri ve korunmasındaki gözetilen hususlar bakımından bir fark yaratmaz. **DÜLGER,** Murat Volkan; Kişisel Verilerin Korunması Hukuku, İstanbul, 2019, s. 1.

[39] İngiliz Kişisel Verilerin Korunması Kanunu'nda *"sensetive personal data*" olarak geçmektedir.

[40] **DÜLGER**, s. 14-15; 95/46/ EC sayılı Direktif'in de Giriş bölümü 33. Paragrafı. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN (Erişim Tarihi : 20.01.2020)

dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği[41], *sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri*[42]*"* dir.

"Özel nitelikli kişisel veriler" kişisel mahremiyet taşımaları ve elde edilmesi halinde kişilerin ayrımcılığa uğramalarına sebebiyet verebilecek bilgiler olması nedeniyle diğer kişisel verilere nazaran daha sıkı korunmalarını gerektirir.[43] Bu verilerin başkaları tarafından öğrenilmesi halinde bazı önyargılar nedeniyle kişiler ayrımcılıkla karşılaşması riski vardır. Örneğin kişinin ırk ve etnik kökenine dair bilgilerin öğrenilmesi ırkçı muamelelerle karşılaşma riskini taşır.[44]

[41] Kılık ve kıyafet ile dernek üyeliği dışındaki veriler Avrupa Birliği mevzuatında da özel nitelikli kişisel veri olarak sayılmıştır. GDPR m.9 ; **KORFF**, s. 81 vd.

[42] KVKK'da tanımlanmamasına karşın GDPR'ın 4/13 maddesinde *genetik veri, kişinin biyolojik numunesinden çıkarılan, onun fizyolojisine veya sağlığına ilişkin doğuştan gelen veya sonradan ortaya çıkan genetik özellikleri ile ilgili veriler;* GDPR'ın 4/14 maddesinde ise biyometrik veri, *kişinin fiziksel, psikolojik veya davranışsal özelliklerine ilişkin özel bir teknik süreçten çıkarılan kişisel veriler* olarak tanımlanmışlardır. Kişinin parmak izi veya yüzü biyometrik veriye örnektir. **TAŞTAN**, s. 44.

[43] Information Commissioner's Office, *"Guide to Data Protection",* 07 Temmuz 2017, s.7. http://www.inf.ed.ac.uk/teaching/courses/pi/2017_2018/PDFs/guide-to-data-protection-2-9.pdf (Erişim Tarihi : 20.01.2020)

[44] **BAŞALP,** Nilgün; Kişisel Verilerin Korunması ve Saklanması, Ankara 2004, s. 43.

KVKK'nın gerekçesinde de bu verilerin "öğrenilmesi halinde kişinin mağdur olabilmesine veya ayrımcılığa maruz kalabilmesine yol açabileceğinden" bahsedilmiştir.[45]

Hassas nitelikleri nedeniyle daha sıkı korunan özel nitelikli kişisel verilerin doğrudan korunmasının yanında bu tür verileri ortaya çıkaran dolaylı verilerin özel nitelikli kişisel veriler gibi korunmaları gerekir.[46] Örneğin; siyasi partilerin kendi bültenlerine dair abonelikler için tutulan bir liste kişilerin siyasi düşüncelerini ortaya koyabileceğinden bu doğrultuda korunması gerekir.[47]

95/46 EC sayılı Avrupa Birliği Direktifi'nden yola çıkarılarak hazırlanmış olsa dahi KVKK'da özel nitelikli olarak sayılan veri grupları Direktifle birebir aynı değildir. Direktifin 8. maddesinde özel işleme koşulları adı altında sayılan veri gruplarına KVKK'nın 6. madde düzenlemesinde ekleme yapılarak yer verilmiştir. Yapılan eklemelerden en tartışmalısı kılık ve kıyafete dair verilerdir. Kişilerin kılık ve kıyafetlerine dair bilgilerin kişisel veri olarak sayılıp sayılmayacağı değil, özel nitelikli olup olmadığı tartışma konusudur. Zira tanım gereğince "kimliği belirli ya da belirlenebilir gerçek bir kişiye ilişkin her tür bilgi" kişisel veri olabileceğinden kılık ve kıyafete dair bilgiler de tabiatıyla kişisel veridir. Ancak "hassas kişisel veriler" olarak da tabir edilen bu verilerin daha sıkı korumaya tabi tutulmalarının gerekli olup olmadığı değerlendirildiğinde; ülkemizde kılık ve kıyafetin de etnik köken ve ırk bilgisi kadar

[45] https://www.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf, https://www.kvkk.gov.tr/Icerik/5388/Madde-ve-Gerekcesi-ile-Kisisel-Verilerin-Korunmasi-Kanunu-Bilgi-Notu-ve-Kisisel-Verilerin-Korunmasina-Iliskin-Terimler-Sozlugu

[46] **ERARSLAN TÜRKMEN**, s. 25.

[47] **BAŞALP**, s. 43.

ayrımcılığa tabi tutulduğu dönemler olmuştur ve günümüzde halen kılık ve kıyafet bilgisini işlemenin ayrımcılık tehlikesi taşıdığı açıktır.

Ancak burada kişisel verilerin işlenmesinde gözetilmesi gereken mahremiyet ve katma değer arasındaki dengenin korunmasına dikkat edilmesi gerekir. Örneğin e-ticaret yapan bir giyim firmasının işlediği verilerin özel nitelikli kişisel veri olması karşısında katma değer dengede üstün tutulabilmelidir.[48]

II. KİŞİSEL VERİLERİN KORUNMASININ TARİHÇESİ ve ULUSLARASI DÜZENLEMELER

A. TARİHÇE

Bilgi depolama, bilgiyi işleme ve yeni bilgiler türetme, geri getirme ihtiyaçları aslında çok eskilere dayanmaktadır. İnsanlık her dönemde bu amaçlarla çeşitli araçlar geliştirmiş[49] ancak bilgi teknolojilerinde yaşanan hızlı gelişmeler kişisel verilerin işlenmesini kontrolsüz hale getirmiştir. Veri transfer seçeneklerinin artmasıyla kişisel verilerin gerek ulusal bazda gerekse de uluslararası alanda aktarımı ciddi riskleri beraberinde getirmiştir.[50]

---

[48] **TAŞTAN**, s. 45. Yazar, sorunun çözümüne ilişkin olarak Kurul ilke kararı alınabileceği görüşündedir. Bu görüş, hem uygulamadaki sorunları somut durumlar özelinde çözebileceğinden hem de bu veri grubunun taşıdığı ayrımcılık riskini artırmayacağından kanaatimizce de yerindedir.

[49] **AŞIKOĞLU**, s. 29.

[50] **BAŞALP**, s. 23.

Gelişen teknoloji bir yerden sonra kişilerde *"güvensizlik hissi*[51]*"* oluşturmuştur. Ancak teknik olanakların kişilik haklarını daraltması hukuk düzenince kabul edilmesi mümkün olmayan bir durumdur. Oysa ki, teknoloji insanlığa hizmet etmeli, onun mutlak olarak korunması gereken haklarını tehdit etmemelidir.[52] Zira, kişisel verilerin korunması hukukunda korunması hedeflenen veriler değil, verilerin sahibi olan gerçek kişilerdir.[53]

Günümüzde birçok meslek grubuna getirilen sır saklama yükümlülüğünün temeli esasen asırlar öncesine, *Hipokrat*'a dayanmaktadır.[54] Bugün, avukatlar, noterler, bankacılar gibi birçok meslek grubu sır saklamakla mükelleftir.

Henüz bilgisayarın dahi günlük hayatımıza girmediği[55] 1949 yılında George ORWELL tarafından kaleme alınan, çağının çok ilerisini gören ve teknolojik gelişmelerin

---

[51] **AYDIN**, s.9.

[52] **BAŞALP**, s. 23.

[53] **KÜZECİ**, Kişisel Veriler, s. 13; AŞIKOĞLU, s. 25.

[54] Hipokrat yemin metninde yer alan *"Gerek sanatımın icrası sırasında, gerek sanatımın dışında insanlarla münasebette iken, etrafımda olup bitenleri, görüp işittiklerimi bir sır olarak saklayacağım ve kimseye açmayacağım."* şeklindeki ifade hekimlerin sır saklama yükümlülüğünün temelini oluşturmaktadır. **ŞİMŞEK,** Oğuz; Anayasa Hukukunda Kişisel Verilerin Korunması, İstanbul 2008, s. 6.

[55] Bilgisayarın tarihine bakıldığında, ilk bilgisayarın ne zaman icat edildiği konusunda bir birlik yoktur. **ORTA,** Mesut; Bilişim Suçları ve Elektronik Delillerin Toplanması Muhafazası Değerlendirilmesi Sunulması, Ankara 2015, s. 28. Hatta meselenin özü M.Ö. 2000 yılında Çinliler tarafından abaküsün (sayı boncuğu) bulunmasına dayanmaktadır. Bkz. **ÖZTÜRK,** Mustafa; *"Bilişim Cihazlarındaki Sayısal Delillerin Tespiti Ve Değerlendirilmesinde İş Akış Modelleri",* Ankara Üniversitesi Sağlık Bilimleri Enstitüsü Yayımlanmamış Yüksek Lisans Tezi, Ankara 2007, s. 4. Bilgisayarın tarihsel gelişimi 4

devletler tarafından kullanılarak, kişilerin tüm hayatlarının çift taraflı monitörlerle kayda alınması ve davranış ve düşünce dünyalarının şekillendirilmesi[56] anlatılan *"Bin Dokuz Yüz Seksen Dört"* isimli romanda özel hayatın gizliliği ve kişisel verilerin korunmasının önemi çarpıcı bir kurguyla ortaya koymuştur.[57]

1953 yılında IBM (International Business Machine) şirketinin çıkarttığı "IBM 701" ile başlayan veri işletim sistemlerinin icadı[58], 1960'lı yıllarda bilgisayarın günlük

---

döneme ayrılmaktadır. Bu dönemlerin ilki 1940-1959 arası kabul edilmekte olup, günümüz anlamında ilk bilgisayar olarak kabul edilen ENIAC (Electronic Numerical Integrator and Calculator – Elektronik Sayısal Entegreli Hesaplayıcı) 1946 yılında Pennsylvania Üniversitesinde üretilmiştir. **DEMİRCAN,** Tunç; Bilişim Alanında Suçlar, İstanbul 2016, s. 10-11. Ancak bu bilgisayar askeri amaçla topçu atış hesaplamalarını yapabilmek için üretilmiş 30 ton ağırlığında ve 500.000,00 Dolar maliyetinde bir cihazdı. ENIAC hakkında ayrıntılı bilgi için bkz. **GÜRLER,** Fazlı; (Yargıtay Kararları Işığında) Teknik ve Hukuksal Yönleriyle Bilişim Alanında Suçlar, Ankara 2015, s. 65.

[56] Bu durum romanda öyle ciddi boyutlara varmaktadır ki; doğdukları andan itibaren devletin sunduğu çerçevede düşünen, aynı kalıpta yetişen çocuklar kendi ebeveynleri aleyhine devlete casusluk yapmaktadırlar.

[57] **AYDIN**, s. 10; **YEO,** Michael; *"Propaganda and Surveillance in George Orwell's Nineteen Eighty-Four: Two Sides of the Same Coin",* s. 55. https://pdfs.semanticscholar.org/cb63/57378e50118269e7151b4a0431d3ef67e75d.pdf?_ga=2.147388983.1815770433.1579597936-73627067.1579597936 Erişim Tarihi: 21.01.2020.

[58] **BAŞALP**, s. 23,

hayata girmesi ile birlikte[59] toplumda kişisel bilgilerin rahatlıkla kaydedilebileceğine ve "büyük veri tabanı" içerisinde toplanabileceğine ilişkin bir korku oluşmuştur.[60] Nitekim ABD'de ilk bilişim suçunun da 18.10.1966 tarihinde bir bilgisayar uzmanı tarafından işlendiğine dair bir iddia gazetelere yansımıştır.[61]

1970'li yıllarda Federal Almanya'nın Hessen eyaletinde bir veri bankası sistemi oluşturulmuş ve Hessen eyaletinde verilerin korunmasına ilişkin olarak ilk yasal düzenleme yapılmıştır. Bu düzenleme ile federal düzeyde bir koruma ihtiyacı ortaya çıkmış ve 1977 yılında dünyada kişisel verilerin korunmasına ilişkin "Federal Almanya Veri Koruma Kanunu (Bundesdatenschutgesetz – BDSG)" kabul edilmiştir.[62]

Bu tarih aralığında 1973 yılında İsveç'te de İsveç Veri Koruma Kanunu kabul edilmiştir.[63] Ayrıca 1974 yılında Amerika Birleşik Devletleri'nde "Gizlilik Kanunu", 1978 yılında Fransa'da "Bilgisayarlar, Veriler ve Özgürlüklere İlişkin Kanun, Danimarka'da Özel Sicil Kanunu", Norveç'te "Veri Sicil Kanunu" ve Avusturya'da

[59] Bu tarihlerde bilgisayarlar bilgi-işlem merkezlerinde kullanılan cihazlar olmaktan çıkmış, kişisel kullanıma açılmıştır ancak IBM şirketi ilk PC'yi (Personal Computer – Kişisel Bilgisayar) 1981 yılında üretmiştir. **GÜRLER**, s. 66-67. Bilgisayarın icadında yaşanan dönemsel gelişmeler için Bkz. **AKBULUT,** Berrin; Bilişim Alanında Suçlar, Ankara 2017, s. 6 vd. Türkiye'de ise kullanılan ilk bilgisayarın 1960 yılında Karayolları Genel Müdürlüğü tarafından alınan IBM 650 olduğu bilinmektedir. **AKBULUT**, s. 8.

[60] **AYDIN**, s. 11.

[61] **GÜRLER**, s. 66.

[62] **AŞIKOĞLU**, s. 33.

[63] **AŞIKOĞLU**, s. 33.

"Veri Koruma Kanunu", 1979 yılında Lüksemburg'da "Veri Koruma Kanunu" dünyada ilk çıkarılan kanunlardır.[64]

B. ULUSLARARASI DÜZENLEMELER

1. OECD Rehber İlkeleri

1961 yılında kurulan ve ekonomik büyümeyi desteklemek, iş imkanlarını artırmak, başka devletlerin ekonomik büyümelerine ve küresel ekonominin büyümesine katkı sağlamak gibi temel hedefleri olan[65] 1980 yılında "Ekonomik İşbirliği ve Kalkınma Örgütü" tarafından çıkarılan ve 2013 yılında güncellenen "Özel Yaşamın Gizliliğinin ve Sınır Ötesi Veri Akışının Korunmasına İlişkin Rehber İlkeler'in (OECD Rehber İlkeleri)" amacı verilerin serbest piyasada güvenli dolaşımını sağlamak ve uluslararası veri aktarımının önündeki engelleri kaldırmaktır.[66] Örgütün hedefleri ve Rehber İlkeler'i çıkarma amacı göz önünde bulundurulduğunda kişisel verilerin ekonomik önemine de işaret etmektedir.[67]

---

[64] **TAŞTAN**, s. 11.

[65] **KÜZECİ**, Kişisel Veriler, s. 113-114.

[66] **DEVELİOĞLU,** Hüseyin Murat; 6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması, İstanbul 2017, s. 6.

[67] **KÜZECİ**, Kişisel Veriler, s.114.

OECD tarafından alınan kararlar bağlayıcı olmayıp, örgüt genel olarak üyesi olan devletlere kişisel verilerin korunması bağlamında iç hukuklarında yapacakları düzenlemeler konusunda tavsiyelerde bulunmaktadır.[68]

OECD Rehber İlkeleri 7. Ve 15. maddeler arasında açıklanan 8 prensibe dayanır:[69]

- Madde 7: Sınırlı veri toplama,
- Madde 8: Veri kalitesi (verinin belli bir niteliği karşılaması),
- Madde 9: Amacın belirliliği,
- Madde 10: Sınırlı kullanım,
- Madde 11: Veri güvenliği,
- Madde 12: Açıklık,
- Madde 13: Bireyin katılımı,
- Madde 14:.Hesap verilebilirlik.

Bu ilkeler ulusal ve uluslararası birçok düzenlemenin kaynağı olmuştur.[70]

2. Avrupa Konseyi

Kişisel verilerin korunması bağlamında önemli düzenlemeler yapan bir diğer uluslararası kuruluş 1949 yılında II. Dünya Savaşı'nın bitmesiyle savaşın etkilerini ortadan kaldırmak için Londra Antlaşması ile Avrupa Konseyi'dir. Hukukun

---

[68] **AŞIKOĞLU**, s. 36.

[69] OECD Rehber İlkeleri https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm Erişim tarihi: 21.01.2020.

[70] **ÖZDEMİR, Hayrunnisa;** Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması, Ankara 2009, s. 21.

üstünlüğünü, demokrasi ilkelerini ve insan haklarını korumak gibi hedefleri olan konseyin bu doğrultuda attığı en önemli adım Avrupa İnsan Hakları Sözleşmesi'ni (AİHS) imzaya açmak olmuştur.[71] Kişisel verilerin korunması AİHS m. 8 bağlamında "özel hayatın gizliliği hakkı" kapsamında korunmuştur.[72] Ayrıca konsey kişisel verilerin korunmasına hususunda kişisel verilerin işlenmesine dair ilkeleri belirlemek ve bu konuda yapılacak ulusal düzenlemelere ışık tutmak amacıyla[73] 1981 yılında "108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Gerçek Kişilerin Korunmasına Dair Sözleşme" imzaya açmıştır.[74]

a. Avrupa İnsan Hakları Sözleşmesi

Avrupa İnsan Hakları Sözleşmesi'nin *"Özel ve Aile Hayatına Saygı Hakkı"* başlıklı 8. maddesinde *"Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.*

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

[71] **DÜLGER**, Kişisel Veriler, s. 54.

[72] **AKGÜL,** Aydın; Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması, İstanbul 2014, s. 181.

[73] **ÖZDEMİR** s. 21.

[74] 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Gerçek Kişilerin Korunmasına Dair Sözleşme https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108 Erişim Tarihi: 22.01.2020

durumunda söz konusu olabilir." Denilmektedir.[75] Kişisel verilerin korunması hakkı, özel hayata saygı hakkı kapsamındır. Zira AİHM de birçok kararında 8. madde düzenlemesinin kişisel verilerin korunması hakkını da kapsayacağını belirtmiştir.[76]

b. 108 sayılı Sözleşme

1981 yılında imzaya açılan 108 sayılı Sözleşme imza tarihinden dört yıl sonra yürürlüğe girmiştir. Türkiye bakımından ise; "18 Şubat 2016 tarihli ve 29268 sayılı Resmi Gazetede" yayımlanan Sözleşme[77] 01 Eylül 2016 tarihinde yürürlüğe girmiştir.[78]

4. maddesi gereğince kişisel verilerin korunması hakkında kanun çıkarma yükümlülüğünü içeren sözleşme[79] ile Avrupa İnsan Hakları Sözleşmesinde münhasıran düzenlenmeyen bu hak ile ilgili eksikliğin giderilmesi amaçlanmıştır.[80]

---

[75] Sözleşmenin tam metni için bkz.; https://www.echr.coe.int/Documents/Convention_TUR.pdf

[76] Örneğin; Segerstedt-Wiberg ve Diğerleri – İsveç, 06.06.2016 tarihli kararı https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=003-1688388-1769677&filename=003-1688388-1769677.pdf

[77] 2016 yılında onaylanarak Resmi Gazetede yayınlanan hali için bkz.; https://www.resmigazete.gov.tr/eskiler/2016/03/20160317-2.pdf

[78] **ÜÇÜNCÜ,** S. Hilal, Medeni Yargılama Hukukunda Kişisel Verilerin ve Sırların Korunması, İstanbul 2019, s. 110.

[79] **AYÖZGER ÖNGÜN,** Çiğdem; Kişisel Verilerin Korunması Hukuku, İstanbul 2019, s. 73.

[80] **ÜÇÜNCÜ**, s. 110.

Sözleşmede, otomatik sistemler kullanılarak işlenmesi karşısında verilerin korunması için öngörülen asgari kurallar yer almaktadır.[81] Sözleşmenin bazı maddelerinde yer alan ilkeler şöyledir; [82]

- Madde 5: Kişisel verilerin;

  a- Yasal ve adil yollarla toplanarak işlenmesi,

  b- Belli ve meşru amaçlar doğrultusunda kaydedilmesi, belirlenen amaçlar dışında kullanılamaması

  c- Amaçla bağlantılı olarak ve gerektiği kadar saklanması,

  d- Doğru ve gerektiğinde güncel olması,

  e- Amacına uygun süreyi aşmayacak şekilde ilgili kişinin kimliği belirlenebilir olarak saklanması.

- Madde 6: Özel veri kategorilerinin ayrıca korunması.
- Madde 7: Veri Güvenliği.
- Madde 8: İlgili kişilerin bilgi alma, verilere ulaşma ve gerektiğinde düzeltilmesini veya silinmesini talep edebilme hakları ile ilgili hususlar.
- Madde 9: Sözleşmede yer alan hakların sınırlandırılmasının sınırları yer almaktadır.

2001 yılında kabul edilen 181 no'lu Ek Protokol ile Sözleşmenin uygulama alanı genişletilerek sözleşmeye taraf olmayan ülkelere veri aktarımı yapılması hususunda

[81] **UNCULAR,** Selen; İş İlişkisinde İşçinin Kişisel Verilerinin Korunması, Ankara 2018, s. 52.

[82]Orijinal metin için bkz.; https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37

prensipler konularak, taraf ülkelerde de veri koruma mekanizmalarının kurulması yükümlülüğü getirilmiştir.[83]

3. Birleşmiş Milletler Rehber İlkeleri

1945 yılında 51 üye ülke tarafından kurulan Birleşmiş Milletlerin üye sayısı günümüzde 193'ü bulmuştur.[84] 10 Aralık 1948 yılında kabul edilen "Birleşmiş Milletler Evrensel İnsan Hakları Bildirisi'nin"[85] 12. maddesinde *"Hiç kimse, özel yaşamına, ailesine, konutuna yada haberleşmesine yönelik keyfi müdahalelere ya da onur ve şöhretine yönelik saldırılara maruz bırakılmayacaktır. Herkesin, bu tür müdahale ya da saldırılara karşı yasa ile korunma hakkı vardır."* Denilmektedir.

Avrupa Konseyi gibi Birleşmiş Milletler de kişiler verilerin korunmasını özel hayatın korunması hakkı kapsamında değerlendirmiş[86] ve 1990 yılında "45/95 sayılı Bilgisayarla İşlenen Kişisel Veri Dosyalarına İlişkin Rehber İlkeler (Birleşmiş Milletler Rehber İlkeleri)" adıyla bir belge yayınlamıştır.[87] Bu belge ile sadece bilgisayarla işlenen

---

[83] **TAŞTAN**, s. 14.

[84] https://www.un.org/en/about-un/ (Erişim Tarihi: 03.03.2020)

[85] Birleşmiş Milletler Evrensel İnsan Hakları Bildirisi'nin tam metni için bkz.; https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf (Erişim Tarihi: 03.03.2020)

[86] **DEVELİOĞLU, Hüseyin Murat;** 6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku, İstanbul 2017, s. 10.

[87] Tam metni için bkz.; Guidelines Concerning Computerized Personal Data Files https://digitallibrary.un.org/record/43365 (Erişim Tarihi: 03.03.2020)

verilerin korunmasına dair asgari standartlar belirlenmiş,[88] bu ilkelerin nasıl uygulanacağına dair hususlar üye ülkelerin inisiyatifine bırakılmıştır.[89] Bu ilkeler şunlardır;[90]

- "Hukuka uygunluk ve dürüstlük
- Verilerin doğruluğu
- Amacın belirliliği
- İlgili kişinin erişim hakkı
- Ayrımcılıktan kaçınma
- Veri güvenliği
- Denetim ve yaptırım
- Sınır ötesi veri aktarımı"

Avrupa Konseyi Rehber İlkelerinin de tıpkı OECD Rehber İlkeleri gibi bağlayıcılığı yoktur ancak bu ilkeler OECD ilkelerine göre daha az etkili olmuştur. Bu duruma OECD Rehber İlkelerinin bu alandaki ilk uluslararası düzenleme olmasının neden olduğu söylenebilir ise de Birleşmiş Milletlerin etki alanı düşünüldüğünde bu durum oldukça şaşırtıcıdır. Son yıllarda ise Birleşmiş Milletler kişisel verilerin korunması konusuna önem ve bu konuya ilişkin uluslararası toplantılara destek vermekte olup[91] 24

[88] **AKSOY**, s. 6.

[89] **AŞIKOĞLU**, s. 52.

[90] https://digitallibrary.un.org/record/43365 (Erişim Tarihi: 03.03.2020)

[91] **KÜZECİ**, Kişisel Veriler, s. 120.

Mart 2015 yılında "Dijital Çağda Özel Yaşamın Gizliliği Hakkı" başlığıyla yayınlanan [92] kararda özel hayatın gizliliğinin her ortamda korunması gerektiğinden bahsedilmektedir.

4. Avrupa Birliği

a. Genel Olarak

Avrupa'nın bütünleşmesi fikri daha eski zamanlarda ortaya çıkmışsa da bunun bir sürece dönüşmesi 20. yüzyıla rastlamaktadır.[93] 1995 yılında kurulan Avrupa Birliği'nin kuruluş felsefesinde "barış, özgürlük, refah, demokrasi ve hukukun üstünlüğü" ilkeleri yer almaktadır. Kişilerin, malların, sermayenin ve bilginin serbest dolaşımı esasına dayalı olarak iç hukuk düzenlemeleri yapan Avrupa Birliği'nde kişisel verilerin ise serbest dolaşımına izin verilmemiştir.[94]

---

[92] Kararın tam metni için bkz.; https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/28/L.27 (Erişim Tarihi: 03.03.2020)

[93] Üyesi olan devletleri diğer uluslararası antlaşmalardan daha sıkı şekilde bağlayan Avrupa Birliği'nin temellerini 1951 yılında Paris Antlaşması ile kurulan Avrupa Kömür ve Çelik Topluluğu (AKÇT), 1957 yılında Roma Antlaşması ile kurulan Avrupa Ekonomik Topluluğu (AET) ve Avrupa Atom Enerjisi Topluluğu (Eurotom), 1986 Avrupa Tek Senedi ve nihayet bir sonraki aşamada Amsterdam, Nice, Maastricht ve Lizbon Anlaşmaları oluşturmaktadır. **KÜZECİ**, Kişisel Veriler, s. 151.

[94] **KILINÇ,** Doğan**;** *"Anayasal Bır Hak Olarak Kışısel Verılerın Korunması*", AÜHFD, C. 61, S.3, 2012, s. 1117.

II. Dünya Savaşı sonrasında, hukuki düzenlemelerde "özel hayatın korunması hakkı" insanın temel haklarından biri olarak kabul edilmiştir. Bu dönemde azınlık grupları asimile etmek, ırkçılık ve hatta soykırım yapmak için kişisel verilerin kullanılmış olması devletlerin kişisel verilerin toplanması konusunda sıkı kurallar getirmesini zorunlu kılmıştır.[95]

1990 yılı sonrasında Avrupa Birliği, kişisel verilerin korunması çalışmalarına ağırlık vermiş ve 24 Ekim 1995 tarihinde "95/46/EC sayılı Kişisel Verilerin İşlenmesinde Gerçek Kişilerin Korunması ve Serbest Veri Trafiğine İlişkin Direktifi (95/46/EC sayılı Direktif)" kabul etmiştir.[96] Konuya ilişkin genel düzenlemeler içeren 95/46/EC sayılı Direktifini desteklemek üzere bazı sektörlere özellikle de kendine özgü niteliği olan telekomünikasyon alanında tamamlayıcı düzenlemeler yapılmıştır. Bu doğrultuda 15 Aralık 1977 tarihinde "97/66/EC sayılı Telekomünikasyon Alanında Kişisel Verilerin İşlenmesi ve Gizliliği Korunması Direktifi (97/66/EC sayılı Telekomünikasyonun Gizliliği Direktifi)" kabul edilmiştir. Bu direktif "telefon, dijital televizyon, mobil ağlar ve diğer telekomünikasyon sistemlerine" yönelik özel düzenlemeler içermekte olup kullanıcıların iletişiminin gizliliğini sağlamayı hedeflemektedir ve pazarlama amacına yönelik olarak fatura verilerine ulaşma gibi 95/46/EC sayılı Direktifteki veri korumaya ilişkin eksik konularda geniş kapsamlı yükümlülükler getirmiştir.[97]

12 Temmuz 2002 tarihinde ise tamamlayıcı bir nitelik taşıyan "2002/58/EC sayılı Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunmasına İlişkin Direktif (2002/58/EC sayılı Özel Yaşamın ve Elektronik

---

[95] **ŞİMŞEK,** Oğuz**;** Anayasa Hukukunda Kişisel Verilerin Korunması, İstanbul 2008, s. 39-40.

[96] **AYÖZGER ÖNGÜN**, s. 77.

[97] **KÜZECİ**, Kişisel Veriler, s. 184.

Haberleşmenin Korunması Direktifi)" kabul edilerek "97/66/EC sayılı Telekomünikasyonun Gizliliği Direktifi" yürürlükten kaldırılmıştır. "2002/58/EC sayılı Özel Yaşamın ve Elektronik Haberleşmenin Korunması Direktifi" 15 Mart 2006 tarihinde kabul edilen "2006/24/EC sayılı Kamuya Açık Haberleşme Hizmetleri veya Kamu Haberleşme Şebekesi ile Bağlantılı Olarak Üretilen veya İşlenen Verilerin Saklanmasına İlişkin Direktif (2006/24/EC sayılı Veri Saklama Direktifi)" ile "25 Kasım 2009 tarihli 2009/136/EC sayılı Vatandaş Hakları Direktifi" ile "2002/58/EC sayılı Özel Yaşamın ve Elektronik Haberleşmenin Korunması Direktifin" bazı maddelerinde değişiklikler yapılmıştır.[98]

7 Aralık 2000 tarihinde imza altına alınan "Avrupa Birliği Temel Haklar Şartında" ise kişisel verilerin korunması hakkının anayasal hak olarak tanınması önem arz eden bir gelişme olmuştur. Bu gelişme bilginin dolaşımına olanak sağlamakla beraber bireylerin temel haklarını koruması nedeniyle sevindirici bulunmuştur.[99]

Avrupa Birliği Temel Haklar Şartı'nın *"Kişisel verilerin korunması"* başlıklı 8. maddesinde *"(1) Herkes, kendisini ilgilendiren kişisel verilerin korunması hakkına sahiptir.*

(2) Bu veriler, dürüst bir şekilde, belirli amaçlar için ve ilgili kişinin rızasına veya yasa ile öngörülmüş diğer meşru bir temele dayanılarak işlenir. Herkes kendisi hakkında toplanmış verilere erişme ve bunları düzelttirme hakkına sahiptir.

[98] **AYÖZGER ÖNGÜN**, s. 78.

[99] **TOĞUZ,** Özlem; Avrupa Birliği ve Türkiye'de Fikri Mülkiyet ve Veri Korunması, İstanbul 2014, s. 21.

(3) Bu kurallara uyulması bağımsız bir makam tarafından denetlenir." Denilmektedir.[100]

Hüküm temellerini, "95/46/EC sayılı Direktif", "108 sayılı Sözleşme" ve "AİHS'nin 8. maddesinden" almaktadır. Kişisel verilerin korunması hakkının Avrupa Birliği Temel Haklar Şartı'nda özel hayatın gizliliği hakkından bağımsız olarak düzenlenmiş olması kişisel verilerin korunması hakkının artık "bağımsız bir hak" olarak kabul edildiğinin göstergesi olup ayrıca Direktif 'in de temel haklar boyutuna vurgu yapmaktadır.[101]

b. 95/46/EC sayılı Direktif

Avrupa Birliği'nde konuya ilişkin ilk yeknesak düzenleme ilk taslağı 1990 yılında oluşturulan ve 24 Ekim 1995 tarihinde kabul edilen "95/46/EC sayılı Kişisel Verilerin İşlenmesinde Gerçek Kişilerin Korunması ve Serbest Veri Trafiğine İlişkin Direktif'tir."[102] Kabul edilmesinden üç yıl sonra yürürlüğe giren direktif[103] kişisel verilerin korunması konusunda kilometre taşı niteliğinde bir belgedir.[104] Direktif ile önemli ilkeler benimsenmiştir.[105] Kişisel verilerin korunması hukukuna dair kavramlar

---

[100]Avrupa Birliği Temel Haklar Şartı https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN (Erişim Tarihi: 03.03.2020)

[101] **KÜZECİ**, Kişisel Veriler, s. 158 - 159.

[102] **BAŞALP**, s. 26.

[103] **HENKOĞLU**, s 57.

[104] **AŞIKOĞLU**, s. 58.

[105] **AYÖZGER ÖNGÜN**, s. 79.

temelini direktif ve direktifin uygulanmasına yönelik oluşturulan çalışma grubu raporlarından almakta olup direktif yalnızca Avrupa Birliğinde değil, Türkiye dahil birçok ülkede hukuki düzenlemelerin oluşturulmasında *"çerçeve belge*[106]*"* niteliğindedir.

Direktifin amacı

1. maddesinde direktifin amacı belirlenirken ilk fıkrada kişisel veriler işlenirken özel hayatın gizliliğinin korunmasının gerekliliğine vurgu yapılırken ikinci fıkrada ise kişisel verilerin serbest dolaşımının sağlanması amaçlanmıştır. Buna göre direktif kişisel verilerin aktarımı ihtiyacı ile temel hakların korunması arasında bir denge kurmayı hedeflemektedir.[107]

Kişisel verilerin korunması ortak pazarın gelişmesine katkı sağlayacağından üye devletlerden beklenen direktifin 5 ile 17. maddeleri arasında düzenlenen temel ilkeler çerçevesinde gerekli hukuki düzenlemeleri yapmalarıdır.[108]

[106] **KÜZECİ**, Kişisel Veriler, s. 160.

[107] **UYGUN,** Murat; Avrupa Birliğinin 95/46 Sayılı Veri Koruma Yönergesi Işığında Kişisel Verilerin Korunması, Gazi Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk A.B.D., Yayınlanmamış Yüksek Lisans Tezi, Ankara 2010, s. 36.

[108] **BAŞALP**, s. 31.

Uygulama alanı ve kapsam

Direktifin uygulama alanı 3. maddesinde belirtildiği üzere "tamamen veya kısmen[109] otomatik yollarla işlenen" veya "otomatik yollarla işlenmese de bir dosyalama sistemine kaydedilen ya da bu kaydedilmek üzere tutulan" verilerle sınırlandırılmıştır. Kişisel verilerin otomasyon sistemleri kullanılarak işlenmesi halinde verilerin otomatik yollarla işlenmesinden bahsedilir. Ayrıca otomatik yollarla işlenme dahi bir "veri kayıt sistemi" dahilinde belli kriterler dahilinde tasniflenerek, dosyalanarak kişisel verilere hızlı erişime elverişli olarak[110] işlenmesi durumunda da direktif uygulama bulacaktır.[111] Maddeden, direktifin hızlı erişebilen ve aktarılabilecek olan verilere yönelik koruma sağlamayı amaçladığı, günümüzde verilerin başta bilgisayar sistemleri olmak üzere büyük oranda otomatik yollarla işlenen veriler olduğu da düşünüldüğünde direktifin neredeyse tüm kişisel verileri korumayı amaçladığı söylenebilir.[112]

Direktifin uygulama alanı aynı zamanda verileri işlenen kişiye ve verilerin işlenme amacına ilişkin olarak da sınırlandırılmıştır. Direktifin 3. maddesi 2. fıkrasında direktifin,

[109] Kısmen otomatik yollarla işlemeye otomatik bir indeksin fiziken tutulan dosyaları kategorize etmekte kullanılması örnek olarak gösterilebilir. **BAŞALP**, s. 32.

[110] Alfabetik, kronolojik ya da numerik bir tasnifleme ile dosya tutulması buna örnek gösterilebilir.

[111] **AŞIKOĞLU**, s. 61.

[112] **ŞİMŞEK**, s. 43; **KÜZECİ**, Kişisel Veriler, s. 163.

- Gerçek kişiler tarafından tamamen kişisel veya ailevi[113] etkinlikler çerçevesinde işlenen verilerin ve
- Avrupa Birliği'nin üçüncü sütununda yer alan ve topluluk hukukun alanına girmeyen ceza hukuku alanındaki devlet faaliyetleri, kamu güvenliği, devlet güvenliği ve savunma alanlarına yönelik kişisel verilerin işlenmesi

Hallerinde uygulanmayacağı hüküm altına alınmıştır.

29. Madde Çalışma Grubu

29. Madde Çalışma Grubu 95/46/EC sayılı Direktif uyarınca Avrupa Birliği üye ülkelerin veri koruma otoritelerinin, "Avrupa Veri Koruma Denetçisi'nin (European Data Protection Supervisor)" ile Avrupa Komisyonu temsilcilerinden oluşan bağımsız bir danışma organıdır. GDPR'ın yürürlüğe girmesi ile yerini "Avrupa Veri Koruma Kurulu'na" bırakmış olsa da GDPR'ın temeli olması ve temel ilkelerini belirlemesi nedeniyle çalışmaları halen geçerliliğini korumaktadır.[114]

[113] 29. Madde çalışma grubu sosyal ağ kullanıcılarının bir kurum ya da şirket adına hareket ettiği, siyasal ya da ekonomik amaçlar taşıdığı haller gibi bazı etkinliklerini bu kapsamda saymamıştır. Bu hallerde kullanıcıların veri sorumlusu olduklarından bahsedilebilir. 29. Madde Çalışma Grubu 5/2009 sayılı raporu, s. 3, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp163_en.pdf (Erişim Tarihi : 14.03.2020)

[114] **UNCULAR**, s. 78.

b. Genel Veri Koruma Tüzüğü (GDPR)

Konuya ilişkin temel kavramları ortaya koyan çerçeve belge olsa da teknolojinin ilerlemesi ile zamanın gerisinde kalan direktifin yerine 14 Nisan 2016 tarihinde "Genel Veri Koruma Tüzüğü (General Data Protection Regulation – GDPR)" kabul edilmiş, GDPR'ın 94. maddesinde yer alan geçiş hükmü ile 2 yıllık bir uyum süresi öngörülerek 25 Mayıs 2018 tarihinden itibaren yürülüğe girmiş olup[115] tüm üye devletlere uygulanma zorunluluğu getirmesi ile 95/46/EC sayılı Direktif'inden ayrılmaktadır.[116]

GDPR'ın 3/3. maddesiyle 95/46/EC sayılı direktifin uygulanma alanı genişletilmiş, 7/3. maddesinde rızanın açıklanmasına ilişkin açıklamalara, 8. maddesinde çocukların rızasına dair özel hükümlere yer verilmiş, 17. maddesinde unutulma hakkı düzenlenmiş, 25/1 maddesiyle tasarımla veri koruma, 25/2 maddesiyle "varsayılan ayarlarla veri koruma" gibi yeni koruma alanları belirlenmiş, 33-34. maddeleriyle veri ihlallerinin bildirim yükümlülüğü getirilmiş, 35. maddesiyle "yüksek riskli kişisel verilerin işlenmesi halinde veri koruma risk değerlendirmesi yapılması" öngörülmüş, 37. maddesinde "veri koruma görevlisi" kavramı getirilmiş, 83. maddesiyle tek veri koruma otoritesi muhatabı belirlenmesi ve veri ihlallerinde yüksek miktarda idari para cezaları düzenlenmesine yönelik düzenlemeler öngörülmüş olup bu gibi yenilikler getirilmiştir.[117]

GDPR'ın en özelliklerinden biri Avrupa Veri Koruma Otoritesi'nin kurulmasını öngörmüş olmasıdır. 95/46/EC sayılı Direktif uyarınca çalışma yürüten "29. Madde

---

[115] **AŞIKOĞLU**, s. 63. https://gdpr-info.eu/ (Erişim Tarihi: 14.03.2020)

[116] **ERARSLAN TÜRKMEN**, s.34.

[117] **RAUL,** Alan Charles; *"Global Overwiev",* The Privacy, Data Protection and Cybersecurity Law Review, Ed. Alan Charles RAUL, Law Business Research, Londra 2017, s. 1-5; **KÜZECİ**, Kişisel Veriler, s. 195; **ERARSLAN TÜRKMEN**, s.34.

Çalışma Grubu" GDPR'da yerini Avrupa Veri Koruma Otoritesi'ne bırakmıştır. Ancak aynı zamanda üye ülkelerin veri koruma otoriteleri de görevlerine devam edecektir. GDPR'a göre veri koruma otoritelerinin veri işleyen şirketin cirosunun %4'üne kadar ceza kesme yetkisi bulunmaktadır. Ayrıca GDPR, Avrupa Birliği dışında faaliyet gösteren "Google", "Facebook" gibi şirketlerin Avrupa Birliği içinde yaşayan veri sahiplerine hizmet sağlamaları halinde kapsamda olacaklarını öngörmüştür.[118]

Türkiye'deki veri sorumluları ve veri işleyenler açısından ise GDPR'ın 3. maddesi 1. fıkrasında belirtildiği üzere uygulama alanı Avrupa Birliği sınırlarında olup olmadığına farketmeksizin Avrupa Birliği'nde yer alan bir veri sorumlusu veya veri işleyene ait bir işletmenin faaliyeti kapsamında veri işlenmesi yeterlidir. Burada "işletme" kavramı geniş yorumlanarak "gerçek ve etkin bir faaliyet"in gerçekleşmesi yeterli görülmektedir.[119]

Aynı zamanda GDPR'ın 3. maddesi fıkrasında Avrupa Birliği dışında faaliyet gösteren veri sorumlusu veya veri işleyenlerin Avrupa Birliği sınırları içinde yaşayan veri sahiplerine mal veya hizmet sunmaları[120] halinde veya Avrupa Birliği'nde bulunan veri sahiplerinin yine Avrupa Birliği içindeki davranışlarının gözlenmesine ilişkin verilerin işlenmesinde de GDPR uygulama alanı bulacaktır.[121]

---

[118] **AYÖZGER ÖNGÜN**, s. 88-89.

[119] Avrupa Adalet Divanı *Weltimmo* kararında Slovakya'da kurulmuş olan şirketin Macaristan sınırları içerisinde yer alan bir işletmesinin Macaristan'da bir temsilcisi, iletişim adresi ve banka hesabı bulunmasını dikkate alarak ülke sınırları içinde "gerçek ve etkin bir faaliyet" gösterdiği sonucuna varmıştır. **DEVELİOĞLU**, s. 16-17.

[120] GDPR'ın giriş kısmına göre bu durum için üye ülkelerden bir veya birkaçında konuşulan bir dilde hizmet vermesi yeterli kabul edilmiştir. Aynı zamanda söz konusu faaliyetlerin kar amacı gütmesi de şart değildir.

[121] **DEVELİOĞLU**, s. 17.

III. KİŞİSEL VERİLERİN KORUNMASI HAKKININ HUKUKİ NİTELİĞİ

A. GENEL OLARAK

Teknolojinin gelişmesiyle bilgi edinme amacından çıkıp satış, pazarlama, reklam, algı odaklı yaklaşımlar vb. birçok stratejinin belirlenmesinde esaslı unsur haline gelen ve hukuki işlemlere konu edilen kişisel verilerin kazandığı bu ticari değer neticesinde kişisel verilerin serbest dolaşımı ihtiyacı ve bundan doğan menfaat ile kişilerin verileri üzerindeki denetim hakkı arasında adil bir denge kurulması zorunlu hale gelmiştir. Bu önem kişisel verilerin korunması başlı başına bir hak olması ve veri koruma hukukunun temelini oluşturması sonucunu doğurmuştur.[122]

Kişisel verilerin korunması hakkının hukuki niteliğine ilişkin görüşler veri kavramına yüklenen anlama göre değişkenlik göstermektedir.[123] Bu itibarla esas olarak kişisel verilerin özünde hangi hak veya menfaatin yattığına göre[124] çeşitli görüşler bulunmaktadır.

[122] **UNCULAR**, s. 37.

[123] **ÜÇÜNCÜ**, s. 37.

[124] **AKSOY**, s. 37.

B. MÜLKİYET HAKKI GÖRÜŞÜ

Mülkiyet hakkı, "kişinin maliki olduğu şey üzerinde hukuk düzeni sınırları içinde kullanma, yararlanma ve tasarrufta bulunma yetkisi" olarak tanımlanmaktadır.[125] Kişisel verilerin korunması hakkını mülkiyet hakkına dayandıran görüşün temeli Amerikan Hukuku'na dayanmaktadır.[126] Kişisel verilerin mülkiyet hakkına konu olarak kabul edilmesi, veri sahiplerine tasarruf yetkisi verir ve bu durumda veri sahipleri kişisel verilerini satabilir veya verilerin hangi şartlarda kullanılabileceğini kontrol edebilirler.[127] Bu durumda kişilerin verileri üzerinde çok geniş yetkilere sahip olması ve yasal korunma olanaklarının artacağı değerlendirilmiştir.[128]

Bilgiyi güç ile eşit tutan ve kişisel verilerin ticari değerinden yola çıkan bu görüş "serbest piyasa ekonomisinde" kişisel verilerin işlenmesini "ticari bir araç" olarak görmektedir.[129] Şirketlerin kişisel verilerin satışını yapmaları, bu veriler doğrultusunda

---

[125] **OĞUZMAN,** M. Kemal; **SELİÇİ,** Özer; **OKTAY ÖZDEMİR**, Saibe; Eşya Hukuku, İstanbul 2018, s. 274.

[126] **BEYTAR,** Erbil; İşçinin Kişiliğinin ve Kişisel Verilerinin Korunması, İstanbul 2018, s. 56.

[127] **ÜÇÜNCÜ**, s. 39.

[128] **AKGÜL**, s. 73.

[129] **AKSOY**, s. 57. Amerika'da Başkan Tramp'ın Federal İletişim Kurulu (Fedaral Communications Commission) tarafından yürürlüğe koyulan *"Genişbant ve Diğer Telekomünikasyon Hizmeti Müşterilerinin Gizliliğini Korumaya Yönelik Rapor ve Talimat (81 Fed. Reg. 87274)"* başlıklı düzenlemeyi yürürlükten kaldıran bir düzenleme ile ABD'de internet servis sağlayıcılarının kişilerin internet kullanımına dair geçmişlerinin açık rızaları olmaksızın satışında yasal engel ortadan kalkmıştır. Bkz.

satış ve pazarlama teknikleri belirlemeleri kişisel verilerin ticari bir araç haline geldiğinin kanıtıdır.

Kişilerin kişisel verilerinin maliki olması düşüncesi doğal gelebilir[130] ve bu alandaki hukuki korumanın temeli de tarihsel anlamda mülkiyet hakkına dayanmaktadır.[131]

Bu görüşü savunanlar kişisel verilerin pazarlığa konu edilebileceğini ve böylece adil bir bedel karşılığında işlenmelerinin sağlanabileceğini savunmaktadırlar. Ancak taraflar arasında çoğunlukla hiyerarşik bir ilişki olacağından bu durum kişilerin verileri üzerindeki haklarından feragat etmesi sonucunu doğurabilir.[132] Nitekim genellikle bu pazarlık masasına oturacak taraflar verileri işlenen gerçek işi ile veri sorumlusu veya veri işleyen özel veya kamu hukuku tüzel kişisi olacak[133] ve pazarlıkta eşit haklara sahip olanaklara sahip olmayacaklardır. Veri sahipleri bir amaca kavuşmak için (örneğin işe

---

"Trump Signs Measure to Let ISPs Sell Your Data Without Consent" https://www.nbcnews.com/news/us-news/trump-signs-measure-let-isps-sell-your-data-without-consent-n742316 (Erişim Tarihi: 18.03.2020) **TAŞTAN**, s. 55.

[130] **WELSS BRANSCOMB,** Ann; *"Who Owns Informatıon? From Prıvacy To Publıc Access"* http://jolt.law.harvard.edu/articles/pdf/v08/08HarvJLTech249.pdf (Erişim Tarihi : 18.03.2020)

[131] **SAMUELSON**, Pamela; *"Privacy As Intellectual Property?"* Stanford Law Review, C.52, Y. 1999 – 200, s. 1377-1394. http://people.ischool.berkeley.edu/~pam/papers/privasip_draft.pdf (Erişim Tarihi: 18.03.2020)

[132] **KÜZECİ**, Kişisel Veriler, s.60-61.

[133] **TAŞTAN**, s. 56.

girmek gibi) hakkından bedelsiz olarak vazgeçmek sorunda kalabilecektir ve bu durum bireyleri savunmasız bırakacaktır.

C. FİKRİ MÜLKİYET HAKKI GÖRÜŞÜ

"Fikri mülkiyet hakkı", fikri hakları ve sınai hakları bünyesinde barındıran üst bir kavram[134] olup özel hukuktan doğan maddi nitelikte olmayan varlık üzerindeki hakları olarak tanımlanmaktadır.[135]

Kişisel verilerin korunması hakkının fikri mülkiyet hakkına dayandığını savunan bu görüşe göre eser sahibinin eseri üzerinde sahip olduğu manevi haklar arasında "amaçsal bir benzerlik" vardır.[136] Tıpkı fikri mülkiyet haklarında olduğu gibi kişisel verilerin korunması hakkında da amaç bilginin hangi şartlar altında dağıtılacağını ve kimler tarafından kullanılacağının kontrolünü sağlamaktır.[137]

Fikri mülkiyete konu olan değerler kişinin iradi olarak gösterdiği güç ve çabanın bir ürünü olarak meydana gelirken kişisel veriler kişinin belirli tercihleri çerçevesinde yaşamının bir parçası olarak ya da kişinin doğal varlığından doğar. Ayrıca, fikri mülkiyet haklarına kıyasen kişisel verilerin korunmaması halinde ortaya çıkabilecek zararların

---

[134] **AYDIN**, Hüseyin; Sınai Mülkiyet Hakları Aleyhine İşlenen Suçlar, Ankara 2003, s. 26.

[135] **KILIÇOĞLU**, Ahmet M.; Sınai Haklarla Karşılaştırmalı Fikri Haklar, Ankara 2017, s. 2.

[136] **ÜÇÜNCÜ**, s. 40.

[137] **TAŞTAN**, s. 58.

ulaşabileceği boyutu öngörmek çok zordur. [138] Nitekim fikri mülkiyet haklarına yönelik bir saldırının varlığı halinde zarar çoğunlukla korunmalarında gözetilen ekonomik temelli nedenlere ilişkin iken, kişisel verilerin korunmasında hakkında bu durum özel hayatın gizliliğine ilişkin olabilir.

D. KİŞİLİK HAKKI GÖRÜŞÜ

Kişilik hakkı, kişinin kendi kişiliğini oluşturan unsurların tümü üzerindeki haklarını ifade eder.[139] Bu hak, kişinin hak sahibi olarak tanınmasını ve menfaati doğrultusunda bu sıfatının korunması için sahip olduğu yetkileri kullanabilmesini sağlar. Kişilik hakkı kişiyi kişi yapan ve menfaatlerine göre kişinin korunmasını gerektiren değerleri içerdiğinden bu değerler zamana bağlı olarak değişebilir.[140] Bu nedenle kişilik haklarını oluşturan değerlerin sınırlı sayıda olması da düşünülemez.

Kişilik haklarının karakteristik iki niteliği mutlak haklardan olmaları ve herkese karşı ileri sürülebilmeleri ile "kişiye sıkı sıkıya bağlı haklardan" olmaları ve bu nedenle

---

[138] **AKSOY**, s. 66-67. Mülkiyet hakkı ve fikri mülkiyet hakkı görüşleri dışında bunlara benzer kapsamlarda ileri sürülen güven teorisi ve ticari sır görüşü için bkz. **KÜZECİ**, Kişisel Veriler, s. 67-68.

[139] **AKİPEK**, Jale - **AKINTÜRK**, Turgut - **ATEŞ**, Derya; Türk Medeni Hukuku Başlangıç Hükümleri Kişiler Hukuku, İstanbul 2018, s. 341.

[140] *"Bir bakıma kişilik hakkı, kişinin hak süjesi olarak herkes tarafından tanınmasını istemek ve bu sıfatla itibar görmek konusundaki menfaat ve yetkileri anlamına gelir."* **AKİPEK – AKINTÜRK – ATEŞ**, s.341-342.

de bu haklardan vazgeçilmesi veya bu hakların devredilmesinin kural olarak mümkün olmamasıdır.[141]

Kıta Avrupası'nda kişisel verilerin korunması hakkının kişilik hakkına dayandığı esası kabul edilmektedir.[142] Bu görüşe göre kişilerin verilerin korunması hakkı temel bir insan hakkıdır ve kişiliğin korunması ve geliştirilmesi hakkına dayanmaktadır. Uluslararası düzenlemelerde[143] de çoğunlukla aynı görüş benimsenmiştir.

Kişisel verilerin kişilik hakkı temelinde ele alınması görüşünün temeli Nazi Almanyası ve Mussolini zamanlarında kişisel verilerin toplanmasının kötüye kullanılmasına dayanmaktadır. Bu kötüye kullanım Avrupa'da kişisel verilerin korunması konusunun katı bir biçimde korunmasına yönelik bir hassasiyete ve bu hakkın kişilik hakkı olarak değerlendirilmesine neden olmuştur.[144] Federal Almanya Anayasa Mahkemesi, Nüfus Sayım Yasası uyarınca 1983 yılında kişilere kapsamlı bilgiler açıklama zorunluluğu getirerek memurların kapı kapı dolaşarak yapılan sayımda başka bilgiler edinilmesi hedeflendiği[145] nüfus sayımına ilişkin verdiği kararda kişinin toplum

---

[141] **AKİPEK – AKINTÜRK – ATEŞ**, s. 342.

[142] **ÜÇÜNCÜ**, s. 41.

[143] Birleşmiş Milletler Evrensel İnsan Hakları Bildirisi 12. Madde, Birleşmiş Milletler Kişisel ve Siyasal Haklar Sözleşmesi 17. Madde, Avrupa İnsan Hakları Sözleşmesi 8. Madde gibi önemli uluslararası metinlerde kişisel verilerin korunması hakkı özel hayatın gizliliği ve mahremiyet hakkı kapsamlarında değerlendirilerek güvence altına alınmıştır. GDPR'ın 1. Maddesinde ve Avrupa Birliği Temel Haklar Şartı'nın 8. Maddesinde ise kişisel verilerin korunması hakkı başlı başına bağımsız bir temel hak olarak kabul edilmiştir.

[144] **BEYTAR**, s. 58.

[145] **KÜZECİ**, Kişisel Veriler, s. 66.

içerisinde kendini geliştirme hakkından yola çıkarak bireyin kişisel verilerinin geleceğini belirleme hakkı (informational self-determination right) kabul edilmiştir.[146] Bu durum hakkın bağımsız bir hak olarak algılanmasına göstergesidir. Öyle ki zaman içinde özel hayatın gizliliği hakkının dahi önüne geçen münhasır bir temel hak olduğu kabul görmüştür.

Bu durum klasik kişilik hakkı görüşüne ilaveten, bireyin kişisel verilerinin geleceğini tayin hakkının kabulü ile ortaya çıkan kişilik hakkına ilişkin yeni bir görüşün doğmasına neden olmuştur.

Kişilik hakkına ilişkin klasik görüşe göre; özellikle özel hayat alanı[147] içinde ve mahremiyet[148] çerçevesinde değerlendirilmesi gereken kişisel verilerin korunması, bilgi mahremiyetinin sağlanması anlamına gelir.[149] Bu görüşe göre kişisel veriler kişinin özel yaşam ve mahremiyet alanına girdiğinden, bu alandaki hak ve yetkiler kişisel verilerinin işlenmesi konusunda kullanılabilir. Alenileştirilmiş kişisel verileri veya gerçeği yansıtmayan kişisel veriler bu sınırlar içinde değerlendirilemeyeceğinden ve yasal düzenlemelerle yalnızca gizli nitelikteki kişisel verilerin değil, aleni ve gerçeğe aykırı

[146] **TAŞTAN**, s. 59.

[147] Özel alan, kişinin ailesi ve arkadaşları gibi yakın çevresi tarafından bilinen olgu ve olayları içeren alanıdır. **DURAL,** Mustafa – **ÖĞÜZ**, Tufan, Türk Özel Hukuku Cilt:2 (Kişiler Hukuku), İstanbul 2019, s. 112.

[148] Mahremiyetin dört farklı şekli vardır. Bunlar; bedensel mahremiyet, iletişim mahremiyeti, mekânsal mahremiyet ve bilgi mahremiyetidir. **DURAL – ÖĞÜZ**, s. 115. **AKSOY**, s. 49.

[149] **TAŞTAN**, s. 65.

kişisel verilerin de korunması da hedeflendiğinden[150] bu görüşe katılmak mümkün değildir.

Klasik kişilik hakkı görüşünden farklı olarak, bireyin kişisel verilerinin geleceğini belirleme hakkına dayanan kişilik hakkına dayanan yeni görüşe göre; kişisel verilerin etkin bir şekilde korunması ancak bu hakkın kişilik hakkının münferit bir görünümü olarak kabul edilmesi ve özel düzenlemelerle korunması halinde mümkündür. Kişinin toplum içerisinde kendini geliştirmesini amaçlayan bireyin kişisel verilerinin geleceğini belirleme hakkının birçok görünümü vardır. Örneğin kişinin kişilerin muhalif düşünceler geliştirme hakkı bu konudaki bilgilerinin toplandığı bir durumda kullanılamaz hale gelir. Kişilik haklarına bağlı olan görünüm şekilleri, kendilerine özgü ihtiyaçları doğrultusunda kişilik haklarından bağımsız olarak ayrıca korunmalarını gerektirir.[151] "Kişisel verilerin korunması hakkının bağımsız bir hak olarak kabul edilmesi gerektiği" görüşü gerek uluslararası gerek ulusal düzenlenmelerde de artık bu şekilde kabul edilen hakkın hukuki nitelendirilmesinde daha isabetlidir. Gelişen dünya ve bilgi aktarımının teknoloji sayesinde kazandığı baş döndürücü hız göz önünde bulundurulduğunda aksi görüşlerin kişilerin verilerin tam anlamıyla korunmasında yaptığı nitelendirmelerin yetersiz kaldığı açıktır.

[150] **TAŞTAN**, s. 65-66.

[151] **TAŞTAN**, s. 67-68.

IV. KİŞİSEL VERİLERİN İŞLENMESİ

A. VERİ SORUMLUSU, VERİ İŞLEYEN VE DİĞER BAZI KAVRAMLAR

1. Veri Sorumlusu

KVKK'nın 3. maddesinde yer alan tanıma göre *"veri sorumlusu", "kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişidir."* Tanımda özellikle bir ayrım yapılmadığından tüzel kişi veri sorumlusu kamu hukuku ya da özel hukuk tüzel kişisi de olabilir. Burada dikkat edilecek husus, veri sorumlusunun tüzel kişi nezdinde veri işleme faaliyetini gerçekleştiren gerçek kişi değil tüzel kişiliğin bizatihi kendisi olmasıdır.

29. madde çalışma grubu veri sorumlusu olarak bir şirket içindeki kişi ya da organ yerine tüzel kişiliğin kendisinin tanınmasını, veri sahibi ilgili kişilere daha sağlam bir güvence tanımak amacına yönelik olduğunu belirtmiştir.[152]

Veri sorumlusu sıfatının kazanılması için kişisel verileri elde bulundurmak yeterli değildir. En başta kişisel verilerin işlenme amaç ve yöntemlerini belirlemek olmak üzere verilerin işlenmesine dair her türlü kararı verebilme yetisine sahip olunması gerekmektedir.[153] Aksi halde veri işleyen sıfatının taşınması da söz konusu olabilir.

Veri sorumlusu sıfatı belirlenirken kişisel verilerin;

- Toplama amaçlarına

---

[152] 29. Madde Çalışma Grubu 1/2010 sayılı Raporu, s. 15. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf (Erişim Tarihi: 01.04.2020)

[153] **UNCULAR**, s. 109.

- Türlerine
- Hangi amaçlarla işleneceğine
- Toplanan verilerin üçüncü kişilerle paylaşılıp paylaşılmayacağına ve paylaşılacaksa kimlerle paylaşılacağına
- Toplanan verilerin hangi sürelerle saklanacağına ve imha edileceğine kimin karar verdiği dikkate alınır.[154]

2. Veri İşleyen

Kanunda yer alan tanıma göre *"veri işleyen"; "veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişidir."* Tanımdan anlaşılacağı üzere veri sorumlusunun verdiği yetki çerçevesinde sınırlı olarak veri işleme faaliyeti gerçekleştirir. Veri işleyen çoğunlukla veri sorumlusuna dışarıdan hizmet veren üçüncü kişilerdir.

Burada dikkat edilecek husus veri işleyenin tüzel kişi veri sorumlusunun organizasyon şeması dışında bir kişi olduğu noktasıdır.[155] Aksi halde veri sorumlusu tüzel kişiliğin bir kısım yükümlülüklerini organizasyon yapısı içinde yer alan birimlere/kişilere yüklemesi anlamına gelecektir ki bu durum kanunun amacına ters düşecektir.

3. Diğer Bazı Kavramlar

Çalışmada yer alan ve kişisel verilerin korunması hukukuna hakim olan birkaç temel ilkeden daha bahsedilmesi, çalışmanın anlaşılır olması açısından yerinde olacaktır.

---

[154] **AŞIKOĞLU**, s. 112-113.

[155] **AŞIKOĞLU**, s. 114.

Kişisel verilerin korunması hukukunda önem arz eden diğer bazı kavramlar ise "kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi" kavramlarıdır.

"Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in" 4. maddesinde "kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi" *"imha"* olarak tanımlanmıştır.

Aynı yönetmeliğin 8. maddesinde *"silme; kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemi",* 9. maddesinde *"yok etme; kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemi"*, 10. maddesinde ise *"anonim hale getirme; kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi"* olarak tanımlanmıştır.

Silme ve yok etmeye dair yönetmelikte yer alan tanımlar büyük oranda benzerlik gösterse de silme işleminde *"kullanıcılar için"* verilere erişimin mümkün olmayacağı şekilde bir imha söz konusu iken yok etme işleminde ise *"hiç kimse tarafından"* hiçbir şekilde geri getirilemeyecek şekilde bir imha söz konusudur.

Anonim hale getirme için ise yönetmeliğin 10. maddesi 2. fıkrasında da söz edildiği üzere "*kişisel verilerin, veri sorumlusu, alıcı veya alıcı grupları tarafından geri döndürme ve verilerin başka verilerle eşleştirilmesi gibi kayıt ortamı ve ilgili faaliyet alanı açısından uygun tekniklerin kullanılması yoluyla dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemez hale getirilmesi"* gerekir.

B. KİŞİSEL VERİLERİN İŞLENMESİNDE TEMEL İLKELER

1. Genel Olarak

Kişisel verilerin korumasının temelinde veri işlemede uyulması gereken bazı temel ilkeler yer almaktadır. 108 Nolu Sözleşme'nin 5. maddesinde, 95/46/EC sayılı Direktif'in 6. maddesinde ve KVVK da ise 4. madde düzenlemesi ile birbirine paralel şekilde "*kişisel verilerin hukuka ve dürüstlük kurallarına uygun olarak işlenmesi, belirli, açık ve meşru amaçlar için toplanması, toplanma amaçlarıyla ilgili, ölçülü ve yeterli olması, doğru ve güncel tutulması ve gerekli olan süre kadar saklanması*" ilkelerine yer verilmiştir. GDPR'da bunlara ek olarak *"veri minimizasyonu"* ilkesi öngörülmüştür. 95/46/EC sayılı Direktif'ten hareketle hazırlanan ve GDPR'ın yayımlanmasından önce yürürlüğe giren KVKK'da yer almamakla birlikte uygulamada Kişisel Verilerin Korunması Kurulu tarafından verilen kararlar ile kabul edildiğinden çalışmada bu ilkeye de yer verilmiştir.

2. Kişisel Verilerin Hukuka ve Dürüstlük Kurallarına Uygun Olarak İşlenmesi

Kişisel verilerin işlenmesinde hukuka ve dürüstlük kurallarına uygun davranılması en temel ilkedir. Nitekim bu ilke, diğer ilkeleri kapsamakta ve onlara kaynaklık etmektedir.[156]

[156] **TAŞTAN**, s. 48.

Kişisel verilerin "*hukuka uygun olarak işlenmesi"*, kişisel verilerin yasal mevzuata, meslek ilkelerine ve varsa diğer özel hukuki metinlere[157] uygun olarak işlenmesini; "*dürüstlük kuralına uygun olarak işlenmesi"* ise verilerin işlenmesinde aydınlatma yükümlülüğüne uygun hareket edilmesi[158] ile kişisel verileri işlenen kişiye karşı açık ve şeffaf olunmasını ifade eder.[159]

Hukukumuzda kişisel verilerin hukuka uygun işlendiğinden bahsedilebilmesi için en başta KVKK'nın 5. Ve 6. maddelerinde ve varsa konuya ilişkin sair hukuki düzenlemelerde öngörülen işlenme şartlarına uygun şekilde işlenmeleri gerekir.

3. Kişisel Verilerin Toplanma Amaçlarının Belirli, Açık ve Meşru Olması

Verilerin toplanmasında hukuka uygunluktan bahsedebilmek için ise *verilerin belirli, açık ve meşru amaçlarla toplanması* gerekmektedir. *Amacın belirli olması,* kişisel verilerin hangi amaçlarla toplandığını; *amacın açık olması*, amaca bağlı kalınmasını ve amacın etrafının dolaşılarak amaca bağlılık ilkesinin zedelenmemesini[160]; *amacın meşru olması* ise amacın hukuka uygun olmasını ifade eder.

Kişisel verilerin işlenmesinde bu ilkeye uygun davranılması veri sahibi ilgili kişilerin verilerinin hangi amaçlarla işlendiğini bilmelerini ve verileri üzerindeki denetim haklarını kullanabilmelerini sağlayacaktır.

---

[157] Taraflar arasında bir sözleşme ilişkisi varsa kişisel verilerin sözleşmede öngörülen şekilde işlenmesi gibi.

[158] **KESER BERBER**, Leyla- **ÜLGÜ**, Mahir- **ER,** Cüneyd; Elektronik Sağlık Kayıtları ve Özel Hayatın Gizliliği, İstanbul Bilgi Üniversitesi 2009, s. 126.

[159] **UYGUN**, s. 53.

[160] **UYGUN**, s. 54.

Bu ilke ile veri sorumlusu ve veri işleyenlerin *"ileride lazım olur"* anlayışıyla gereksiz olarak veri işlemelerinin de önüne geçilmiş olur[161] ve belirlenen amaçlar dışında veri işlenmeleri halinde fiillerinden sorumlu tutulmaları gündeme gelir.[162]

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

İlke ile "işleme amacıyla ilgisi olmayan veya gereksiz, ilgisiz verilerin işlenmemesini" amaçlamaktadır. Amacı dışında başka bir sebeple verinin işlenmesi ancak yasanın açıkça buna cevaz vermesi halinde mümkündür. Bu ilke ile kişisel verilerin bir kez elde edildikten sonra elde edilme amacında işlenmesinin önüne geçilmesi hedeflenmiştir. Aksi halde kişisel verilerin toplandıkları amaç doğrultusunda işlenmelerinin hiçbir garantisi kalmayacaktır[163].

Bu ilkenin unutulma hakkıyla da ilişkilendirilmesi mümkündür; unutulma hakkı, kişisel verilerin durumun gerektiği ölçüde ve en kısa sürelerle depolanmasını içeren kişisel verilerin korunması hakkının da çatısıdır.[164]

---

[161] **BEYTAR**, s. 62-63.

[162] **TAŞTAN**, s. 50-51.

[163] **BEYTAR**, s. 63.

[164] **TAŞTAN**, s. 51-52. *"Unutulma hakkına gelince;* ***unutulma hakkı ve bununla ilişkili olan gerektiği ölçüde ve en kısa süreliğine kişisel verilerin depolanması veya tutulması konuları, aslında kişisel verilerin korunması hakkının çatısını oluşturmaktadır.*** *Her iki hakkın temelinde bireyin kişisel verileri üzerinde serbestçe tasarruf edebilmesini, geçmişin engeline takılmaksızın geleceğe yönelik plan yapabilmesini, kişisel verilerin kişi aleyhine kullanılmasının engellenmesini sağlamak yatmaktadır. Unutulma hakkı ile geçmişinde kendi iradesi ile veya üçüncü kişinin neden olduğu bir olay nedeni ile kişinin*

geleceğinin olumsuz bir şekilde etkilenmesinin engellenmesi sağlanmaktadır. Bireyin geçmişinde yaşadığı olumsuz etkilerden kurtularak geleceğini şekillendirebilmesi bireyin yararına olduğu gibi toplumun kalitesinin gelişmişlik seviyesinin yükselmesine etkisi de tartışılmazdır.

Unutulma hakkı; üstün bir kamu yararı olmadığı sürece, dijital hafızada yer alan geçmişte yaşanılan olumsuz olayların bir süre sonra unutulmasını, başkalarının bilmesini istemediği kişisel verilerin silinmesini ve yayılmasının önlemesini isteme hakkı olarak ifade edilebilir.

Bu hak bir yandan kişiye "geçmişini kontrol etme", "belirli hususların geçmişinden silinmesini ve hatırlanmamayı isteme hakkı" sağladığı gibi, diğer yandan muhataplarına kişi hakkındaki bir kısım bilgilerin üçüncü kişilerin kullanmamasını veya üçüncü kişilerin hatırlamamasına yönelik önlenmeleri alma yükümlülüğü yükler. Bu hakkın; bireylerin fotoğraf, internet günlüğü gibi kendileri hakkındaki içerikleri silmek için üçüncü şahısları zorlamayı içermesinin yanında geçmişteki cezalarına ilişkin bilgilerin veya haklarında olumsuz yorumlara neden olabilecek bilgi ve fotoğraflarının kaldırılmasını isteme hakkını tanıdığı kabul edilmektedir. Diğer taraftan bu hak, bireyin geçmişindeki belirli yönlerinin mümkün olmayacak biçimde hatırlanmaması için önlemler alınmasını gerektirmektedir.

Avrupa İnsan Hakları Sözleşmesi (AİHS)'nin 8. maddesinde yer alan özel yaşama saygı hakkı altında korunan "mahremiyet hakkı"nın, bireyin kendisi hakkındaki bilgileri kontrol edebilmesi şeklindeki hukuki çıkarlarını da içerdiği ifade edilmektedir. Zira bireyin kendisine ait herhangi bir bilginin, kendi rızası olmaksızın açıklanmaması, yayılmaması ve bu bilgilere başkalarının ulaşamaması kısacası kişisel verilerinin mahrem kalması konusunda hukuki menfaati bulunmaktadır. (Gülay Arslan Öncü,

KVKK'da açıkça anılmayan ancak GDPR'ın önemli ilkelerinden olan ve basit bir tabirle *"ne kadar gerekli ise o kadar veri işle"* anlamına gelen *"Veri Minimizasyonu"* ilkesinin de bu ilkede saklı olduğuna dair görüşler mevcuttur.[165]

5. Toplanan Kişisel Verilerin Doğru Olması ve Güncel Olarak Tutulması

Bu ilke ise "*toplanan kişisel verilerin doğru toplanmasına* ve *güncel olarak tutulmasına"* ilişkindir. Güncellikten anlaşılması gereken zamanında doğru, son yeni bilginin işlenmesidir. Kişisel verilerin "doğru ve gerektiğinde güncel olması" ilkesi KVKK'nın 11. maddesi uyarınca veri sahibi ilgili kişinin *"kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme"* hakkına ilişkindir.

Ancak bu ilke aynı zamanda veri sorumlusu veya veri işleyeni de korumaktadır. Zira, hatalı yahut güncel olmayan verilerin işlenmesi halinde veri sorumlusu veya veri işleyenin işleme amacına ulaşması mümkün olmayabilir.[166]

Avrupa İnsan Hakları Sözleşmesinde Özel Yaşamın Korunması, Beta Yayınları, İstanbul 2011, s.182)

Kişiye unutulma hakkının sağlanması ile birlikte özel hayatının gizliliği korunmuş olacaktır." Yargıtay Hukuk Genel Kurulu 2014/4-56 E., 2015/1679 K., 17.06.2015 tarihli kararı. https://www.kazanci.com.tr/ (Erişim Tarihi: 25.05.2020)

[165] Bkz. **DEVELİOĞLU**, s. 47.

[166] **DEVELİOĞLU**, s. 48.

6. Kişisel Verilerin Saklama Sürelerinin Belirli Olması

Son olarak; kişisel verilerin saklama sürelerinin belirli olmalı ve bu sürelerin sonunda veriler imha edilmelidir.[167] KVKK'nın 4. maddesine göre saklama sürelerinin sınırı "kişisel verilerin ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar" saklanmasıdır.

Verilerin saklanması gerekliliğinin amaç devam ettiği sürece var olduğunu, amaç ortadan kalktığında saklama ihtiyacının da sona ereceğinin göz ardı edilmemesi gerekir.[168]

C. KİŞİSEL VERİLERİN İŞLENME ŞARTLARI

1. Genel Olarak

Kişisel verilerin işlenmesi kural olarak yasaktır. Ancak belli hallerin varlığı halinde kişisel verilerin işlenmesi mümkündür.[169] Bu haller "kişisel verilerin işlenmesinde hukuka uygunluk halleri" veya "kişisel verilerin işlenme şartları" olarak sayılmaktadır.

[167] **UYGUN**, s. 55.

[168] **KESER BERBER / ÜLGÜ / ER,** s.127.

[169] **BAŞALP**, s. 39.

2. İlgili kişinin açık rızasının alınması

Kişisel veriler işlenmeden kural olarak öncelikle "ilgili kişinin açık rızasının alınması" gerekir.

95/46/EC sayılı Direktif'in 2. maddesinde "rıza; ilgili kişinin kendisiyle ilgili kişisel verilerin işlenmesine yönelik olarak belirli bir konuda ve aydınlatılmış özgür irade açıklaması" olarak tanımlanmaktadır.[170] GDPR'ın 4. maddesinde bu tanım, "ilgili kişinin kişisel verilerinin işlenmesine özgürce verilmiş, konuya özel, bilgilendirilmiş ve kişinin isteklerine ilişkin bir belirsizlik barındırmayan bir beyan veya olumlu bir eylem şeklindeki onayı" olarak yer almıştır. KVKK'nın 3. maddesinde ise *"açık rıza"; "belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza"* olarak tanımlanmıştır.

Buradaki irade açıklaması, muhatabına ulaşmış, onay anlamı taşıyan dışarıya yönelik bir davranıştır. Veri sahibinin susması rızanın varlığı anlamına gelmez.[171] Ayrıca direktifin 7. maddesine göre rızanın asli unsuru tereddüde yer vermeyecek şekilde verilmiş olmasıdır. Rızanın şekli konusunda ise direktifte bir düzenleme yer almamaktadır.[172] KVKK'da da rızanın şekli konusunda bir düzenleme yer almadığından, şeklin ispat konusunda önemli olduğu söylenebilir.

Rızanın geçerli olabilmesi için rızası alınanın kişisel verilerin işlenmesinin amacı, içeriği, verilerin ne kadar süreyle nerelerde kullanılacağı gibi konularda aydınlatılmış olması gerekir. Ayrıca rızanın serbest iradeyle, konuya özel ve kesin olması gerekir.[173]

---

[170] **UYGUN**, s. 56.

[171] **ŞİMŞEK**, s. 45.

[172] **BAŞALP**, s. 39-40.

[173] **AYÖZGER ÖNGÜN**, s. 135.

İleride işlenmesi hedeflenen verilere ilişkin önceden alınacak toptan bir rıza beyanının da kişisel verileri koruma hukuku açısından geçerliliğinden söz edilemez.[174]

Ayrıca veri sahibi rızasını her zaman geri alabilir.[175]

KVKK'nın 5. maddesine göre açık rıza alınması dışında; "*kanunlarda açıkça öngörülmesi, 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, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması, ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması"* hallerinde kişisel verilerin işlenmesi hukuka uygundur.

3. Açık rıza alınması haricinde kişisel verilerin işlenmesi

Kişisel verilerin veri sorumlularınca yasal bir zorunluluğu yerine getirmek adına işlenmesi de hukuka uygunluk sebebidir. Bu nedenle "kanunlarda açıkça öngörülmesi halinde" kişisel veriler rıza alınmaksızın işlenebilir.

Bu şarta dayalı olarak yapılan işlemeler genellikle kamu düzeni için yapılan işlemelerdir.[176] Örneğin suçların soruşturulması adına resen yapılan işlemler veya bir suç

---

[174] **ÖZDEMİR**,

[175] **DEVELİOĞLU**, s. 53.

[176] **BEYTAR**, s. 65.

işlendiğini öğrenen veri sorumlusunun yetkili merci ile kişisel verileri paylaşması hallerinde hukuka uygunluk olacaktır.[177]

"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" şeklinde anılan hukuka uygunluk sebebi ise hukukumuzdaki "üstün özel yarar" kavramının karşılığıdır. Ancak hayati çıkardan kastın ne olduğu tam olarak anlaşılamadığından tartışmalı bir kavramdır[178].

Kişisel verilerin sözleşme ilişkisinden doğan işlemleri gerçekleştirme amacıyla işlenmesi veya kurulması amaçlanan bir sözleşmenin kurulması için sözleşme öncesi alınması gereken verilerin işlenmesi hukuka uygunluk sebebidir.

Bu hükmün amacı, veri sorumlusunu sözleşme ilişkisi içinde olduğu veya sözleşme ilişkisi kurulmasının potansiyel olduğu hallerde aldığı kişisel verilerden doğacak risklere karşı korumaktır. Ancak sözleşmenin kurulmaması halinde alınan verilerin imha edilmesi gerekir.[179]

"Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması" hali de bir hukuka uygunluk sebebi olup buna örnek olarak sosyal güvenlik mevzuatı uyarınca işlenmesi gerekli veriler gösterilebilir.[180]

Kişisel verilerin "ilgili kişinin kendisi tarafından alenileştirilmiş olması" hali de hukuka uygunluk sebebidir.

Başka bir uygunluk sebebi ise "bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olmasıdır". Kişisel veriler yasal bir düzenleme ile

---

[177] **DEVELİOĞLU**, s. 65.

[178] **BAŞALP**, s. 41.

[179] **DEVELİOĞLU**, s. 60-61.

[180] **DEVELİOĞLU**, s. 62.

yetkilendirilmiş kamu kurumları tarafından işlenebilirler. Yasal düzenlemelerin kişinin verilere ilişkin haklarının korunması için gerekli güvenceleri ve istisnaları içermesi gerekir.[181] Ancak eklemek gerekir ki bu durum sadece kamu kurumlarına ilişkin olmayıp örneğin baroların resmi yetkileri kapsamında disiplin soruşturması yapmak için üyelerinin kişisel verilerini işlemesi de bu kapsamdadır.[182]

Nihayet, veri sahibinin temel hak ve özgürlüklerine zarar vermediği sürece meşru bir menfaatin varlığı verilerin işlenmesinde hukuka uygunluk sebebidir. Örneğin güvenlik kamera kayıtları bu kapsamdadır.[183]

D. ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN İŞLENMESİ

Diğer kişisel verilerin işlenmesinde olduğu gibi özel nitelikli kişisel verilerin işlenmesinde de "hukuka ve dürüstlük kurallarına uygun olma", "doğru ve gerektiğinde güncel olma", "belirli, açık ve meşru amaçlar için işlenme", "işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma" ve "ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme" şeklinde öngörülen genel ilkelere uyulması ve "verilerin kanunlarda öngörülen usul ve esaslara uygun olarak işlenmesi" şarttır.

Özel nitelikli kişisel veriler kişisel mahremiyet taşımaları ve elde edilmesi halinde kişilerin ayrımcılığa uğramalarına sebebiyet verebilecek bilgiler olduğundan bu verilerin işlenmesinde açık rıza alınması KVKK'nın 6. maddesinde yasal zorunluluk olarak öngörülmüştür.

---

[181] **ŞİMŞEK**, s. 106-107.

[182] **DEVELİOĞLU**, s. 64.

[183] **UYGUN**, s. 58-59.

Ancak aynı maddenin üçüncü fıkrasına göre özel nitelikli kişisel verilerden *"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."*

Madde metninden anlaşılacağı üzere, sağlık ve cinsel hayata ilişkin olmayan özel nitelikli kişisel verilerin işlenmesi yasağına getirilen hukuka uygunluk sebebi genel nitelikteki kişisel verilere ilişkin işleme şartlarından yalnızca *"kanunlarda öngörülen hâller"*dir. Sağlık ve cinsel hayata ilişkin özel nitelikli kişisel verilerin işlenmesi 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" açık rıza olmaksızın işlenebilir.

Sağlık verisi işleyen özel hukuk gerçek ve tüzel kişileri ile kamu hukuku tüzel kişileri tarafından yürütülen süreç ve uygulamalarda uyulacak usul ve esaslar Kişisel Sağlık Verileri Hakkında Yönetmelik ile düzenlenmiştir.

İKİNCİ BÖLÜM: TÜRK HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASI

I. TÜRK CEZA KANUNU DIŞINDA TÜRK HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASI

A. ANAYASA

Anayasamızda konuya ilişkin olarak doğrudan ve dolaylı koruma sağlar nitelikte hükümler bulunmaktadır.

Anayasanın 2. maddesinde yer alan "hukuk devleti ilkesi", 17. maddesindeki "kişilerin maddi ve manevi varlığını koruma ve geliştirme hakkı", 22. maddesindeki "haberleşme hürriyeti", 24. maddesindeki "dini inanç ve kanaatlerini açıklamaya zorlanamama hakkı", 25. maddesindeki "düşünce ve kanaatlerini açıklamaya zorlanamama hakkı" kişisel verileri dolaylı olarak koruyan anayasal düzenlemelerdir.[184]

Anayasanın 20. maddesinde düzenlenen "özel hayatın gizliliği hakkı" ise kişisel verilerin korunmasının anayasal temelini teşkil etmektedir. 2010 yılında yapılan değişiklik ile maddeye eklenen son fıkrada *"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."* Denilmekte olup kişisel veriler doğrudan anayasal koruma altına alınmıştır. Madde ile kişisel verilerin korunması hakkı kapsamında "bilgi edinme hakkı", "verilere erişme hakkı", "verilerin

[184] **ŞİMŞEK**, s. 94.

düzeltilmesini ve silinmesi talep etme hakkı", "amaca bağlılık ilkesi" ve "orantılılık ilkesi" korunmuş ve kişisel verilerin "veri sahibi ilgili kişinin açık rızası" ile ve "kanunda öngörülen hallerde" işlenebileceği öngörülmüştür.[185]

Anayasa Mahkemesi Elektronik Haberleşme Kanunu'nun *"Bilgi Teknolojileri ve İletişim Kurumu, elektronik haberleşme sektörüyle ilgili kişisel verilerin işlenmesi ve gizliliğinin korunmasına yönelik usul ve esasları belirlemeye yetkilidir"* şeklindeki 51. madde düzenlemesini, "anayasada kişisel verilerin korunmasına ilişkin usul ve esasların ancak kanunla düzenlenebileceğine ilişkin güvenceye aykırı olduğu" gerekçesi ile iptal etmiştir.[186]

---

[185] **AYÖZGER ÖNGÜN**, s. 95.

[186] Kararın gerekçesinde *"Kişisel veri kavramı, belirli veya kimliği belirlenebilir olmak şartıyla, bir kişiye ilişkin bütün bilgileri ifade etmektedir. Bu bağlamda adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil; telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler, IP adresi, e-posta adresi, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler kişisel veri kapsamındadır.*

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. Bilişim teknolojilerindeki gelişmeler sonucunda, geleneksel yöntemlerle mümkün olmayan çok sayıda verinin toplanabilmesi; daha önce birbirinden ilişkisiz şekilde tutulan pek çok verinin merkezi olarak bir araya getirilebilmesi; verilerin, veri eşleştirme ve veri madenciliği gibi ileri teknolojik imkânlarla analize tabi tutulmak suretiyle, veriden yeni

Ayrıca Anayasanın 90. maddesi gereğince de "usulüne göre yürürlüğe konulmuş uluslararası sözleşmeler kanun hükmünde" olduğundan AİHS'nin AİHM'in de birçok kararında kişisel verilerin korunması hakkını da kapsayacağını belirttiği 8. madde düzenlemesi ve AİHS ile yargı yetkisi tanınan AİHM içtihatları da Türk Hukuku açısından bağlayıcıdır.[187]

---

veriler üretme kapasitesinin artması; verilere erişim ve veri transferinin kolaylaşması; kişisel verilerin ticari işletmeler için kıymetli bir varlık niteliği kazanması neticesinde, özel sektör unsurlarınca yaratılan risklerin daha yaygın ve önemli boyutlara ulaşması ve terör ve suç örgütlerinin kişisel verileri ele geçirme yönündeki faaliyetlerinin artması gibi etkenler, günümüzde kişisel verilerin en üst seviyede korunmasını zorunlu kılmaktadır. Bu bağlamda Anayasa'nın 20. maddesinin üçüncü fıkrasının son cümlesinde, "Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." hükmüne yer verilerek kişisel verilerin korunması hakkı anayasal güvenceye bağlanmış ve bu şekilde kamu makamlarının keyfi müdahalelerine karşı koruma altına alınmıştır.

Yasama yetkisinin devredilemezliği ilkesi gereğince, Anayasa'nın açıkça kanunla düzenlenmesini öngördüğü konularda yürütme organına doğrudan ve ilk elden düzenleyici işlem yapma yetkisi verilemez. Elektronik haberleşme sektörüyle ilgili kişisel verilerin işlenmesi ve gizliliğinin korunmasına yönelik usul ve esasları belirleme yetkisini Bilgi Teknolojileri ve İletişim Kurumuna veren itiraz konusu kural, Anayasa'nın 20. maddesinde öngörülen kişisel verilerin korunmasına ilişkin usul ve esasların ancak kanunla düzenlenebileceğine ilişkin güvenceye aykırıdır." Denilmektedir. http://kararlaryeni.anayasa.gov.tr/Karar/Content/94117278-50ca-4203-88f3-72a5537258a5?excludeGerekce=False&wordsOnly=False (Erişim Tarihi: 01.04.2020)

[187] **KÜZECİ**, Elif; *"Anayasal Bir Hak: Kişisel Verilerin Korunması"*, Bilişim Dergisi, S: 128, 2011, s. 142 vd; **AYÖZGER ÖNGÜN**, s. 96.

B. KİŞİSEL VERİLERİN KORUNMASI KANUNU(KVKK)

Ülkemizde KVKK için yapılan çalışmalara 1989 yılında başlandığı bilinmekte ise de[188] kanun ancak 24 Mart 2016 tarihinde kabul edilerek 07.04.2016 tarihinde Resmi Gazete yayımlanmıştır. Kanunun *"Kişisel verilerin aktarılması"* başlıklı 8'inci, *"Kişisel verilerin yurt dışına aktarılması"* başlıklı 9'uncu, *"İlgili kişinin hakları"* başlıklı 11'inci, "Veri sorumlusuna başvuru" başlıklı 13'üncü, *"Kurula şikâyet"* başlıklı 14'üncü, *"Şikâyet üzerine veya resen incelemenin usul ve esasları"* başlıklı 15'inci, *"Veri Sorumluları Sicili"* başlıklı 16'ncı, "Suçlar" başlıklı 17'nci ve *"Kabahatler"* başlıklı 18'inci maddeleri yayımı tarihinden altı ay sonra, diğer maddeleri ise yayımı tarihinde yürürlüğe girmiştir.

Anayasanın 20. maddesi 3. fıkra son cümlesinde yer alan *"Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."* şeklindeki ibarenin 2010 değişikliği ile eklendiği düşünüldüğünde KVKK'nın 2016'da ancak yürürlüğe girmesi şaşırtıcıdır.

Birinci maddesinde belirtildiği üzere 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."* Bu amaç kanunun esas alınarak hazırlandığı 95/46/EC sayılı Direktif amacı ile aynıdır.

Kanun hazırlanırken GDPR yerine 95/46/EC sayılı Direktifin esas alınması doktrinde eleştiri konusu olmuştur ancak 95/46/EC sayılı Direktif'in temel ve daha detaylı düzenlemeler içermesi, Avrupa'nın bu detaylı düzenlemeyi 20 küsür yıllık

[188] **KÜZECİ**, Kişisel Veriler, s. 311.

uygulama tecrübesinden sonra daha sade bir düzenleme olan GDPR'a geçmesi nedenleri ile ülkemizde bu konunun ilk defa bir kanunla düzenlediği de dikkate alındığında direktifin esas alınması isabetli olmuştur.

C. DİĞER KANUNLARDAKİ DÜZENLEMELER

1. Türk Medeni Kanunu ve Türk Borçlar Kanunu

Türk Medeni Kanunu'nda *"Kişiliğin korunması"* başlıklı bölümde yer alan 23., 24. Ve 25. maddeler dolaylı olarak kişisel verileri de korumaktadır. Kanunun 24. maddesi kişisel verileri içine alan ve kişiliği koruyan bir düzenlemedir. Madde metninde "kişilik hakkı zedelenen kişinin rızası", "daha üstün nitelikte özel veya kamusal yarar" ya da "kanunun verdiği yetkinin kullanılması" sebeplerinden biri olmadıkça kişilik haklarına yapılan saldırıların hukuka aykırı olduğunu hükme bağlanmış ve kişilik hakkı saldırıya uğrayan kişinin hakimden koruma isteyebileceği düzenlenmiştir. 25. maddede[189] ise bu

[189] ***Madde 25-*** *Davacı, hâkimden saldırı tehlikesinin önlenmesini, sürmekte olan saldırıya son verilmesini, sona ermiş olsa bile etkileri devam eden saldırının hukuka aykırılığının tespitini isteyebilir.*

Davacı bunlarla birlikte, düzeltmenin veya kararın üçüncü kişilere bildirilmesi ya da yayımlanması isteminde de bulunabilir.

Davacının, maddî ve manevî tazminat istemleri ile hukuka aykırı saldırı dolayısıyla elde edilmiş olan kazancın vekâletsiz iş görme hükümlerine göre kendisine verilmesine ilişkin istemde bulunma hakkı saklıdır.

Manevî tazminat istemi, karşı tarafça kabul edilmiş olmadıkça devredilemez; miras bırakan tarafından ileri sürülmüş olmadıkça mirasçılara geçmez.

saldırılara karşı açılabilecek davalar sayılmıştır. Kanunun 26. maddesinde ise doğrudan adı korunması hedeflenerek adı haksız olarak kullanılan kişiye saldırıya son verilmesini talep etme ve kusur ile zararın varlığı halinde maddi-manevi tazminat talep edebilme hakkı tanınmıştır.

Türk Borçlar Kanunu'nun 49 ve devamı maddelerinde ise "haksız fiil sorumluluğu" düzenlenmiş olup, *"Kişilik Hakkının Zedelenmesi"* başlıklı 58. maddede kişilik hakkı zedelenen kişinin manevi tazminat talep edebileceği düzenlenmiştir.

2. İş Kanunu

4857 sayılı İş Kanunu'nda 75. maddesinin ilk fıkrasında işverenin işçi için tutacağı özlük dosyasında bulunması gerekli belgelerden bahsedilirken ikinci fıkrasında "İşverenin, işçi hakkında edindiği bilgileri dürüstlük kuralları ve hukuka uygun olarak kullanmak zorunda olduğu" ve "gizli kalmasında işçinin haklı çıkarı bulunan bilgileri açıklamama yükümlülüğü bulunduğu" belirtilmiştir.

3. Bilgi Edinme Kanunu

Bilgi Edinme Kanunu'nun "Özel Hayatın Gizliliği" başlıklı 21. maddesinde *"Kişinin izin verdiği hâller saklı kalmak üzere, özel hayatın gizliliği kapsamında, açıklanması hâlinde kişinin sağlık bilgileri ile özel ve aile hayatına, şeref ve haysiyetine, meslekî ve ekonomik değerlerine haksız müdahale oluşturacak bilgi veya belgeler, bilgi edinme hakkı kapsamı dışındadır.*

Davacı, kişilik haklarının korunması için kendi yerleşim yeri veya davalının yerleşim yeri mahkemesinde dava açabilir.

Kamu yararının gerektirdiği hâllerde, kişisel bilgi veya belgeler, kurum ve kuruluşlar tarafından, ilgili kişiye en az yedi gün önceden haber verilerek yazılı rızası alınmak koşuluyla açıklanabilir." denilmektedir. Madde ile getirilen bu sınırlama ile kişisel verileri koruyan bir düzenleme öngörülmüştür.

4. Fikir ve Sanat Eserleri Kanunu

Fikir ve Sanat Eserleri Kanunu'nun 4. maddesinden hareketle kişilerin kendilerine ait fotoğrafları eser niteliğinde olup ancak eser sahibinin izni ile kullanılabilirler.[190] Kanunun 70. maddesi 3. fıkrası uyarınca fikri hakkı ihlal edilen kimse tazminattan başka "temin edilen karın kendisine verilmesini" de isteyebilir.[191]

II. TÜRK CEZA KANUNU'NDA KİŞİSEL VERİLERİN KORUNMASI

A. GENEL OLARAK

Kişisel verilerin korunmasına yönelik suç tipleri Türk Ceza Kanunu'nun *"Kişilere Karşı Suçlar"* kısmında "*Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar*" başlıklı bölümde düzenlenmiştir. TCK'da *"Madde 135: Kişisel verilerin kaydedilmesi", "Madde 136: Verileri hukuka aykırı olarak verme veya ele geçirme"* ve *"Madde 138: Verileri yok etmeme"* suçlarına yer verilmiş, 137. maddesinde ise "kişisel verilerin kaydedilmesi" ve "verileri hukuka aykırı olarak verme veya ele geçirme" suçlarının nitelikli halleri

[190] **AYÖZGER ÖNGÜN**, s. 97.

[191] **ÖZDEMİR**, s. 96-97.

düzenlenmiş, 140. maddede ise bu iki suçla ilgili olarak "tüzel kişiler hakkında uygulanacak güvenlik tedbirlerine" yer verilmiştir.

KVKK'nın *"Suçlar"* başlıklı 17. maddesinde ise *"Kişisel verilere ilişkin suçlar bakımından 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanunu'nun 135 ila 140'ıncı madde hükümleri uygulanır.*

Bu Kanunun 7'nci maddesi hükmüne aykırı olarak; kişisel verileri silmeyen veya anonim hâle getirmeyenler 5237 sayılı Kanunun 138 inci maddesine göre cezalandırılır." Denilmektedir.

Öncelikle belirtmek gerekir ki KVKK kapsamına giren her ihlal durumunda cezai himayeden yararlanılamayacaktır. Ayrıca 5326 sayılı Kabahatler Kanunu'nun "İçtima" başlıklı 15. maddesi son fıkrasında belirtildiği üzere *"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."*

Anılan maddelerden KVKK'nın alanına giren her konunun ceza hukuku kapsamında değerlendirilemeyeceği, KVKK'ya aykırı olan bir durumun ceza hukuku anlamında suç teşkil edip etmediğinin ayrıca değerlendirilmesi gerektiği anlaşılmaktadır.

B. KİŞİSEL VERİLERİN KAYDEDİLMESİ SUÇU (TCK m. 135)

1. Genel Olarak

TCK'nın 135. maddesinin birinci fıkrasında "hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası" verileceği, ikinci fıkrasında ise "kişisel verilerin, kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin" olması halinde cezada artırım yapılacağı düzenlenmiştir.

Kişisel veri kavramı Türk Ceza Kanunu'nda tanımlanmamıştır. 135. madde gerekçesinde ise *"gerçek kişiyle ilgili her türlü bilginin kişisel veri olarak kabul edilmesi"* gerektiği belirtilmiştir.[192] Gerekçede yer alan tanımdan tüzel kişilerin verilerinin cezai himaye kapsamında olmadığı anlaşılmaktadır.[193]

TCK'da kişisel veri tanımının yapılmamış olması KVKK yürürlüğe girene kadar eleştiri konusu olmuştur. Tanım yapılmayarak kapsamın geniş tutulmasının belirlilik ilkesine[194] ve kanunilik ilkesine[195] aykırı olduğu yönünde görüşler sunulmuş olup KVKK'nın 3. maddesinde yapılan tanım ile bu tartışmalar son bulmuştur.[196]

KVKK'nın yürürlüğe girmesinden önceki tarihli bir kararında Yargıtay Ceza Genel Kurulu kişisel veri kavramını şu şekilde değerlendirmiş ve kişisel veriyi tanımlamıştır: *"Bugüne kadar kişisel verilerin neler olduğuna dair kanunun çıkarılmaması nedeniyle TCK'daki 135 ve 136. maddelerindeki hukuka aykırılığın hangi hallerde oluştuğuna ilişkin başvurulabilecek kapsayıcı bir kaynak ya da norm olmaması nedeniyle bu iki madde eksik norm sayılırlar. Belki zamanın ihtiyaçlarına cevap verecek 'Kişisel Verilerin Korunması Kanunu' Meclisten geçtiğinde bu çerçeve düzenleme tamamlanmış olacaktır. Bununla beraber adı geçen ceza maddeleri yürürlükte*

---

[192] **ÖZGENÇ**, s.868.

[193] **HAFIZOĞULLARI**, Zeki - **ÖZEN**, Muharrem; Türk Ceza Hukuku Özel Hükümler Kişilere Karşı Suçlar, Ankara 2016, s.287.

[194] Ayrıntılı bilgi için bkz. **DÜLGER**, Murat VOLKAN; Bilişim Suçları ve İnternet Bilişim Hukuku, Ankara 2012.

[195] Bkz. **YAŞAR**, Osman – **GÖKCAN**, Hasan Tahsin – **ARTUÇ**, Mustafa; Yorumlu – Uygulamalı Türk Ceza Kanunu, Cilt 3, Ankara 2014, s. 4432.

[196] **KORKMAZ**, s. 325-326.

olduğundan uygulanması sırasında çok dikkatli olunması gerekir. Doktrinde birçok tanım ve kapsam belirlemesi yapılmaktadır. Bu bilimsel görüşlerden hareketle kişisel verilerin hangileri olabileceğini belirlemek gerekir. Şu da bir gerçek ki bu verilerin tamamının da ceza normları ile korunması gerektiği düşünülmemelidir. Bu tasnifin esasını genel yaşam mahremiyetinden hareketle özel hayatın gizli alanını korumayı amaçlayan ve sağlayan bilgiler olarak anlamak gerekir.

Bilimsel görüşlerden hareketle kişisel verilerin neler olabileceğini şu başlıkları altında sınıflandırabiliriz.

a- Yaşam şekline ilişkin kişisel veriler: Kişilerin üçüncü kişiler tarafından ayırımcılığa uğramaması ve haysiyetinin korunmasıyla ilişkili olarak dini inançları, cinsel tercihleri, etnik kökeni, suç geçmişi, politik eğilimleri ve kişisel özel aktivitelere ilişkin bilgiler.

b- Ekonomik ve finansal kişisel veriler: Suçlular tarafından suistimale ve kimlik hırsızlığına hedef olmamak için kişinin mali varlığı, sahip olduğu hisse ve hesaplar, borçları, yaptığı alış verişler, kredi kartlarına ilişkin veriler. Ayrıca sayılan bu bilgiler ile kişinin nerede ve kimlerle bulunduğuna, sağlık bilgilerine ilişkin bilgiler de ortaya çıkarabileceğinden ve varlık bilgisinin toplumsal açıdan da özel sayılmasından dolayı önemi artmaktadır.

c- Bilişim alanına ilişkin kişisel veriler: e-postaların bizzat adresleri veya şifreleri, internet ortamında paylaşılan kişisel veriler mahrem olarak değerlendirilebilir. Bunun önemi şu bakımdan artmaktadır, internette gezinti yapan kişi birçok kişisel bilgileri paylaşmakta, bu bilgiler kayıt altına alınmakta, yine internet erişimine ilişkin iz kayıtlarının hizmet sağlayıcı ve sunucu sahipleri tarafından tutulabiliyor olması nedenleriyle artmaktadır.

d- Sağlıkla ilgili kişisel veriler: Sağlık verileri kişilerin iş güvenliğini, toplum içindeki statüsünü ve sigorta kapsamını etkileyen hassas bilgilerdir. Ayrıca sağlık verileri kişilerin sosyal yaşantısı ve psikolojik durumları hakkında bilgi edinilmesine neden olabilir. Biyometrik veriler de (kişinin kendine özgü fiziksel veya biyolojik niteliklerine dayalı olarak insanların kimliğini tespit için dijital teknolojiden faydalanma bilimi) kişisel veriler arasındadır.

e- Politik kişisel veriler: Toplum içinde yaşayan kişilerin siyasi tercihleri toplum katmanları arasında bilinme halinde ayırımcılığa maruz kalma ihtimali bulunduğundan bu bilgilerde kişisel veridir.

2- Anayasanın 38/3 ve Türk Ceza Kanunun 2. maddesi suçta ve cezada kanunilik ilkesini düzenlemektedir. TCK'nın 2. maddesi 'Kanunun açıkça suç saymadığı bir fiil için kimseye ceza verilemez' hükmünü içermektedir. Madde metninden de açıkça anlaşıldığı gibi fiilin kanunda suç olarak gösterilmesi yetmez, bunun açık bir biçimde belirlenebilir olması gerekir. Suçların ve cezaların kanunda önceden açık ve anlaşılır bir şekilde düzenlenmesi gerekir ki insanlar neyin suç olduğunu önceden kolayca bilebilsin ve davranışlarını buna göre ayarlayabilsinler.

Bu haliyle de TCK'nın 135 ve 136. maddeleri Anayasanın 38/3. maddesine de aykırıdır. Öncelikle bu husus da düşünülüp maddelerin iptali için Anayasa Mahkemesine başvurulmalı ve bekletici mesele yapılması gerekir. Şu aşamada ne kadar uygulayıcı ve bilim adamı varsa herkes kendine göre farklı bir kişisel veri tanımı yapmakta olduğundan

sanığın eylemini suç kapsamında değerlendirip cezalandırmamak gerekir."[197] şeklinde açıklamakta idi.

KVKK'nın yürürlüğe girmesinden sonra ise Yargıtay Ceza Genel Kurulu KVKK m.3'te yer alan kişisel veri tanımını kararlarına taşımıştır.[198]

---

[197] Yargıtay Ceza Genel Kurulu 2012/12-1514 E., 2014/312 K. sayılı, 10.06.2014 tarihli kararı.

[198] Yargıtay Ceza Genel Kurulu 2015/12-708 E., 2019/414 K. sayılı ve 09.05.2019 tarihli kararı. Ayrıca belirtmek gerekir ki Yargıtay 12. Ceza Dairesi KVKK öncesi ve sonrası kararlarına göre kişisel veri kavramından *"kişinin, yetkisiz üçüncü kişilerin bilgisine sunmadığı, istediğinde başka kişilere açıklayarak ancak sınırlı bir çevre ile paylaştığı nüfus bilgileri (T.C. kimlik numarası, adı, soyadı, doğum yeri ve tarihi, anne ve baba adı gibi), adli sicil kaydı, yerleşim yeri, eğitim durumu, mesleği, banka hesap bilgileri, telefon numarası, elektronik posta adresi, kan grubu, medeni hali, parmak izi, DNA'sı, saç, tükürük, tırnak gibi biyolojik örnekleri, cinsel ve ahlaki eğilimi, sağlık bilgileri, etnik kökeni, siyasi, felsefi ve dini görüşü, sendikal bağlantıları gibi kişinin kimliğini belirleyen veya belirlenebilir kılan, kişiyi toplumda yer alan diğer bireylerden ayıran ve onun niteliklerini ortaya koymaya elverişli, gerçek kişiye ait her türlü bilginin anlaşılması gerekir."* Denilmektedir. (Bkz.; Yargıtay Ceza Genel Kurulu 2012/12-1510 E., 2014/331 K. sayılı 17.06.2014 tarihli, 2017/12-829 E., 2017/363 K. sayılı 04.07.2017 tarihli, 2015/12-708 E., 2019/414 K. sayılı ve 09.05.2019 tarihli kararları. (Erişim Tarihi: 23.05.2020) Bu tanımdan kişinin kendisi tarafından alenileştirilen kişisel verilerin kapsam dışında tutulduğu anlaşılmaktadır. Ancak Yargıtay Ceza Genel Kurulu tarafından verilen kararlarda da isabetle belirtildiği üzere *"TCK'nun 136. maddesinde korunan hukuki değer genel olarak kişilerin özel hayatı ve hayatın gizli alanı, özelde ise kişisel*

Tekrar hatırlatmak gerekirse KVKK'nın 3. maddesine göre *"Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade eder."*

Ancak bu tanım, geniş çerçevesi nedeniyle ceza hukuku bakımından uygulama sorunlarını da beraberinde getirmiş ve Yargıtay kararlarına *"Verileri hukuka aykırı olarak verme veya ele geçirme suçunun maddi konusunu oluşturan "kişisel veri" kavramından, kişinin, yetkisiz üçüncü kişilerin bilgisine sunmadığı, istediğinde başka kişilere açıklayarak ancak sınırlı bir çevre ile paylaştığı nüfus bilgileri (T.C. kimlik numarası, adı, soyadı, doğum yeri ve tarihi, anne ve baba adı gibi), adli sicil kaydı, yerleşim yeri, eğitim durumu, mesleği, banka hesap bilgileri, telefon numarası, elektronik posta adresi, kan grubu, medeni hali, parmak izi, DNA'sı, saç, tükürük, tırnak gibi biyolojik örnekleri, cinsel ve ahlaki eğilimi, sağlık bilgileri, etnik kökeni, siyasi, felsefi ve dini görüşü, sendikal bağlantıları gibi kişinin kimliğini belirleyen veya belirlenebilir kılan, kişiyi toplumda yer alan diğer bireylerden ayıran ve onun niteliklerini ortaya koymaya elverişli, gerçek kişiye ait her türlü bilginin anlaşılması gerekir. Herkes tarafından bilinen ve/veya kolaylıkla ulaşılması ve bilinmesi mümkün olan kişisel bilgiler de, yasal anlamda "kişisel*

---

verilerdir. Bu düzenlemeler ile tüm kişisel veriler koruma altına alındığından kişisel verilerin mutlaka gizli olması zorunlu değildir. Gizli olmayan ve herkes tarafından bilinen kişisel veriler de hukuka aykırı eylemlere karşı korunmalıdır. Zira kişisel verilerin korunmasına ilişkin suçlarda korunan hukuki değer "sır" olmayıp, verinin ilgilisi olan kişinin kişilik haklarıdır." alenileştirilmiş veriler de kişisel veri niteliğindedir. (Bkz.; Yargıtay Ceza Genel Kurulu 2012/12-1510 E., 2014/331 K. sayılı 17.06.2014 tarihli, 2017/12-829 E., 2017/363 K. sayılı 04.07.2017 tarihli, 2015/12-708 E., 2019/414 K. sayılı ve 09.05.2019 tarihli kararları. https://www.kazanci.com.tr/ (Erişim Tarihi: 23.05.2020)

veri" olarak kabul edilmekte ise de, ***anılan maddenin uygulama alanının amaçlanandan fazla genişletilerek, uygulamada belirsizlik ve hemen her eylemin suç oluşturması gibi olumsuz sonuçların doğmaması için, maddenin uygulamasında, somut olayın özellikleri dikkate alınarak titizlikle değerlendirme yapılması, olayda herhangi bir hukuk dalı tarafından kabul edilebilecek bir hukuka uygunluk nedeni veya bu kapsamda nazara alınabilecek bir hususun bulunup bulunmadığının saptanması ve sanığın eylemiyle hukuka aykırı hareket ettiğini bildiği ya da bilebilecek durumda olduğunun da ayrıca tespit edilmesi*** *gerekir."*[199] şeklinde yansımıştır.

Kanaatimce; uluslararası düzenlemeler de dikkate alındığında KVKK m. 3'teki tanım yerinde olmakla birlikte cezai himaye bakımından tanımın geniş ve belirsiz olmasının sakıncaları suç tipinde hukuka özel aykırılık aranması ile giderilmektedir. Ancak TCK m. 135'te düzenlenen suçun maddi konusu olan "kaydetme" fiilinin ve özellikle TCK m. 136'da düzenlenen seçimlik hareketlerden "verme" fiilinin şekli açısından yaşanan sorunlar ayrıca değerlendirilmelidir. Hukuka özel aykırılık konusuna ve anılan fiillere aşağıda ilgili başlıklarda yer verilmiştir.

[199] Yargıtay 12. Ceza Dairesi 2017/12083 E., 2018/2539 K. sayılı ve 07.03.2018 tarihli kararı, Yargıtay 15. Ceza Dairesi 2015/1659 E., 2018/2748 K. sayılı ve 18.04.2018 tarihli kararı. https://www.kazanci.com.tr/ (Erişim Tarihi: 23.05.2020)

2. Hukuki Konu

Suçun hukuki konusu, ceza düzeni tarafından korunan ve suç tarafından ihlal edilen hukuki varlık veya menfaattir.[200] Başka bir deyişle ise kanun koyucuyu suç tipini düzenlemeye sevk eden ve bu suçun cezalandırılması ile "korunan hukuki değer"dir.[201]

Kişisel verilerin korunması, Türk hukukunda Anayasa Mahkemesinin 1996/68 E., 1999/1 K., sayı ve 06.01.1999 tarihli kararı[202] ile tartışılmaya başlanılmış ve Anayasanın

---

[200] **TOROSLU**, Nevzat; Cürümlerin Tasnifi Bakımından Suçun Hukuki Konusu, Sevinç Matbaası, Ankara 1970, s.288.

[201] **ÖZGENÇ**, İzzet; Türk Ceza Hukuku Genel Hükümler, Ankara 2016, s. 199.

[202] 1774 sayılı Kimlik Bildirme Kanununa eklenen maddeyi de içeren bazı kanun maddelerine ilişkin iptal davasında verilen kararda şu tespitler yer almaktadır: *"İptali istenen düzenlemeyle bu Anayasal hak sınırlandırılmıştır. Maddede bilginin niteliği ve toplanma amacı belirtilmediği için, düzenlemenin adli soruşturma ve kovuşturma istisnası içinde değerlendirilmesi de mümkün değildir. Çünkü, genel kolluk kuvvetleri yakaladıkları şüphelilerin kimliklerine ilişkin bilgileri depolayabilecekleri gibi, herhangi bir suç kovuşturmasıyla ilgili salt gözlemlerine ve değerlendirmelerine ilişkin bilgileri de depolayabilirler.*

Ayrıca, maddede, özel ve resmi konaklama tesislerinden gelecek bilgilerinin niteliğine ilişkin belirginlik de yoktur. Örneğin bir pansiyon sahibinin müşterisinin aile yaşamı ve siyasi görüşleri konusundaki kişisel değerlendirmesi de, kayıtlara geçebilecektir.

...

Özetle, iptali istenen hüküm, genel kolluk kuvvetlerinin bilgisayarlarında kişisel bilgilerin toplanması yetkisini tanımış, fakat bu yetkinin Anayasal haklara getireceği

"Özel Hayatın Gizliliği" başlıklı 20. maddesine 07.05.2010 tarihinde *"Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."* şeklindeki fıkra eklenmiş ve kişisel verilerin korunması hakkı özel hayatın gizliliği hakkı kapsamında korunan anayasal bir hak haline gelmiştir.

---

sınırlamayı sınırlamamıştır. Söz konusu yetkinin hangi koşullarla verilebileceği ve yetki kullanılırken hangi ilkelere uyulması gerektiği Avrupa hukuku çerçevesinde ayrıntılı bir şekilde belirlenmiştir. Avrupa ile bütünleşmeyi amaçladığını her fırsatta dile getiren bir ülkede, bu esaslara uyulmadan yapılan düzenleme, demokratik toplum düzeninin gerekleriyle bağdaşamaz.

Sonuç olarak, 4178 sayılı Yasa'nın 10. maddesi, özel hayatın gizliliğini düzenleyen Anayasa'nın 20. maddesine; temel hak ve hürriyetlerin demokratik toplum düzenin gereklerine aykırı olarak sınırlanamayacağını düzenleyen 13. maddesine ve Türkiye Cumhuriyeti'nin demokratik hukuk devleti olduğunu düzenleyen 2. maddesine aykırıdır." Kararın tam metni için bkz. http://kararlaryeni.anayasa.gov.tr/Karar/Content/9f7b3df0-e060-4c61-9dc8-f9e43a52adf4?excludeGerekce=False&wordsOnly=False (Erişim Tarihi: 23.05.2020)

O halde kişisel verilerin kaydedilmesi suçunun cezalandırılması ile korunan hukuki değer; özel hayatın gizliliği hakkı kapsamındaki haklardan olan kişisel verilerin korunması hakkıdır.[203]

3. Fail

Madde metninde *"kişisel verileri kaydeden kimse"* denilmekte olup suçun faili için bir özellik aranmadığından fail herkes olabilir.[204] TCK m. 20[205] uyarınca tüzel

---

[203] **HAFIZOĞULLARI - ÖZEN**, Kişilere Karşı Suçlar, s.287; **SOYASLAN,** Doğan Ceza Hukuku Özel Hükümler, Ankara 2014, s. 356. Doktrinde korunan hukuki değerin farklı olduğunu savunan görüşler de mevcuttur, dikkat çekici bir görüşe göre; bu suç tipiyle korunan hukuki değer korunan verinin niteliğine göre değişkenlik gösterebilir. Bu görüşe göre örneğin; sağlık durumuna ilişkin bir verinin kaydı söz konusu ile korunan hukuki değer sağlık hakkıdır. Bkz; **HAKERİ**, Hakan; *"Verileri Hukuka Aykırı Olarak Verme (Sır saklama yükümlülüğünün ihlali) suçu",* Tıbbi Müdahaleden Kaynaklanan Hukuki Sorumluluk Sempozyumu, 16-17 Ocak 2009, Mersin Barosu Yayını, Mersin 2009, s. 127.

[204] HAFIZOĞULLARI – ÖZEN, Kişilere Karşı Suçlar, s. 287; **ÖZBEK**, Veli Özer – **DOĞAN**, Koray – **BACAKSIZ**, Pınar – **TEPE**, İlker; Türk Ceza Hukuku Özel Hükümler, Ankara 2016, s. 568; **YAŞAR – GÖKCAN – ARTUÇ**, s. 4433; **ARTUÇ**, Mustafa; Kişilere Karşı Suçlar, Ankara 2018, s. 1626.

[205] ***Madde 20-*** *(1) Ceza sorumluluğu şahsidir. Kimse başkasının fiilinden dolayı sorumlu tutulamaz.*

(2) Tüzel kişiler hakkında ceza yaptırımı uygulanamaz. Ancak, suç dolayısıyla kanunda öngörülen güvenlik tedbiri niteliğindeki yaptırımlar saklıdır.

kişilerin fail olması mümkün değildir. Suçun bir tüzel kişinin faaliyeti içinde işlenmesi halinde fail, fiili gerçekleştiren gerçek kişi olmakla beraber suçun yararına işlendiği tüzel kişi hakkında ise güvenlik tedbirleri uygulanabilecektir.[206]

TCK'nın 137. maddesinde suçun *"kamu görevlisi tarafından"* veya *"belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle"* işlenmesi hali cezayı artıran neden olarak öngörülmüştür.[207]

4. Mağdur

Suçun mağduru ile ilgili özel bir düzenleme öngörülmediğinden herkes mağdur olabilir.[208]

Tüzel kişiler açısından ise suçun mağdur olmaları mümkün olmadığından suç nedeniyle zarara uğramaları halinde "suçtan zarar gören" olabilirler.[209]

---

[206] **KANGAL**, s. 61.

[207] **HAFIZOĞULLARI – ÖZEN**, Kişilere Karşı Suçlar, s. 287; **ÖZBEK – DOĞAN – BACAKSIZ – TEPE**, s. 568; **YAŞAR – GÖKCAN – ARTUÇ**, s. 4433; **ARTUÇ**, s. 1626.

[208] **HAFIZOĞULLARI – ÖZEN**, Kişilere Karşı Suçlar, s. 287; **ÖZBEK – DOĞAN – BACAKSIZ – TEPE**, s. 568; **YAŞAR – GÖKCAN – ARTUÇ**, s. 4433; **ARTUÇ**, s. 1626.

[209] **KOCA**, Mahmut- **ÜZÜLMEZ**, İlhan, Türk Ceza Hukuku Genel Hükümler, Ankara 2017, s. 114; **ÖZGENÇ**, s. 202; Tüzel kişilerin suçun mağduru olabileceğine ilişkin açıklamalar için bkz. **KATOĞLU**, Tuğrul; *"Ceza Hukukunda Suçun Mağduru Kavramının Sınırları",* AÜHFD, Y. 2012, C. 61 , S. 2, s. 672.

5. Suçun Unsurları

a. Maddi Unsur

Suçun maddi unsuru olan fiil, kanunda *"kişisel verilerin hukuka aykırı olarak kaydedilmesi"* olarak belirtilmiş olup kaydetmenin şekli ise tanımlanmamıştır. Kelime olarak *"kaydetmek*; *yazmak, not etmek, sesi veya resmi manyetik bant üzerine geçirmek, elektronik veya sayısal araçlarda bilgiyi korumaya almak"* gibi anlamlara gelmektedir.[210] Kayıttan anlaşılması gereken verileri gerektiğinde tekrar kullanılabilecek şekilde hazır bulundurmaktır.[211] Madde gerekçesinde kişisel verilerin bilgisayar sistemine yada kağıda kaydedilmesi arasında bir ayırım gözetilmediği ifade edilmiş olup[212] kişisel verilerin ne şekilde kaydedildiği suçun oluşması bakımından önem arz etmez.

Doktrinde bir görüş, kişisel verilerin kağıt üzerine kaydedilmesini bu suç açısından kaydetmek olarak kabul edilemeyeceğini savunmaktadır.[213] Kaydetmekteki amacın tekrar kullanılabilirliği ve saklanılabilirliği sağlamak olduğuna değinen ve bunun ancak elektronik yada manyetik araçlarla mümkün olduğunu savunan bu görüşe katılmak mümkün değildir. Zira, kağıt üzerine kaydetmek de tekrar kullanmaya elverişli olup, suç tipinde böyle bir kriter tanımlanmadığı gibi gerekçede de bunun bilinçli bir tercih olduğu

---

[210] Türk Dil Kurumu Güncel Türkçe Sözlük https://www.sozluk.gov.tr/ (Erişim Tarihi: 11.05.2019)

[211] **YAŞAR – GÖKCAN – ARTUÇ**, s. 4437.

[212] **ARTUK**, Mehmet Emin- **GÖKCEN**, Ahmet- **YENİDÜNYA**, A. Caner; Türk Ceza Kanunu Şerhi, Madde 88-153, Üçüncü Cilt, Ankara 2014, s.4639.

[213] **ÖZBEK – DOĞAN – BACAKSIZ – TEPE**, s. 574.

belirtilmiştir.[214] Suç yaygın olarak bilişim sistemleri üzerinden işleniyor olsa da suçun sadece bu şekilde işlenebileceği kabul edilemez.[215] Dolayısıyla kağıt üzerine kişisel verilerin yazılması halinde de kanuni tipe uygun bir fiilden bahsedilebileceğinden suç oluşacaktır.[216]

Kağıt üzerine yazılmak suretiyle kaydedilen verilerin de suç kapsamında olacağına ilişkin yaklaşımın kişinin kendisi için not tutmasının dahi suç olarak değerlendirilmesine neden olabilir. Ancak suçun oluşması için tutulan kayıtların dış dünyaya yansıması ve veri sahibi aleyhine bir tehlike oluşturması gerektiğinden kişilerin özel yaşamlarına müdahale edildiğinden bahsedilemeyecektir. [217]

Bir diğer görüşe göre ise suçun oluşması kişisel verilerin hukuka aykırı olarak *"tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin bir parçası olmak kaydıyla otomatik olan ya da otomatik olmayan yollarla"* kaydedilmesi halinde mümkündür. Bu görüş dayanağını Kişisel Verilerin Korunması Kanunu'ndan almakta olup; bahsi geçen kaydetme şekli KVKK'nın 3. maddesinde *"Veri İşleme"* tanımı kapsamındadır. Bu görüşe göre verilerin kağıda yazılması eyleminin suç teşkil etmesi için

[214] **SERT**, s.102.

[215] **KARAGÜLMEZ**, Ali; Bilişim Suçları ve Soruşturma – Kovuşturma Evreleri, Ankara 2005, s. 231.

[216] **HAFIZOĞULLARI – ÖZEN**, Kişilere Karşı Suçlar, s. 288.

[217] **AKDAĞ**, s. 100.

bir "veri kayıt sisteminin"[218] parçası olması gerekmektedir. Aksi halde "otomatik olmayan yolla"[219] yapılan bu kaydetme eylemi suç teşkil etmez.[220]

Bir "veri kayıt sisteminin parçası" olmaksızın kağıt üzerine hukuka aykırı olarak kaydedilen kişisel verilerin TCK m. 135 kapsamı dışında kaldığını kabulü, TCK m. 135'in kapsamını kanun koyucunun amacına ve tipikliğe aykırı olarak daraltmak, kanundaki suç tipine uygun olmasına rağmen bu fiilleri kapsam dışı bırakmak anlamına gelecektir. Ancak verilerin okunması, dinlenmesi veya ezberlenmesi kaydetme kapsamına girmez.[221]

---

[218] KVKK madde 3'te veri kayıt sistemi *"Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi"* olarak tanımlanmıştır.

[219] KVKK'nın genel gerekçesinde kişisel verilerin otomatik yollarla işlenmesinden, bilişim sistemleri üzerinden gerçekleştirilen faaliyetler kastedildiği anlaşılmaktadır.

[220] **KORKMAZ**, s.332.

[221] **MALKOÇ**, İsmail; Açıklamalı – İçtihatlı 5237 sayılı Yeni Türk Ceza Kanunu (Madde 82-149), İkinci Cilt, Ankara 2007, s. 2198; **AYDIN**, s. 132; **KÖSE AYSUN**, s.122; *"Kişisel verilerin kaydedilmeden önce öğrenilmesi, hafızada tutulan kişisel verilerin başkalarına açıklanması, kişisel verilere salt duyu organları aracılığıyla vakıf olunması, ancak TCK'nın 134/1. maddesinin 1. cümlesinde düzenlenen özel hayatın gizliliğini ihlal suçu kapsamında değerlendirilebilir.*

Bu açıklamalar ışığında incelenen dosyada, elektronik mühendisi olan sanığın, teknik servis elemanı olarak çalıştığı sırada, T.. Ö.. Tıp Merkezi psikiyatri anabilim dalında tedavi gören mağdure hemşirenin, C.. adlı bilgi sisteminde bulunan muayene bilgilerini

Kaydetmenin suç teşkil etmesi için suça konu kişisel verilerin hukuka aykırı olarak ilk defa kaydediliyor olması gerekmez. Daha önce hukuka uygun olarak kaydedilen bir kişisel verinin daha sonra hukuka aykırı olarak yeniden kaydedilmesi halinde de suç oluşur.[222] Ayrıca hukuka uygun olarak kaydedilmiş bir kişisel verinin hukuka aykırı olarak amacı dışında kullanılması halinde ise bu suç oluşmaz.[223]

---

okuyup, hastane çalışanlarına, mağdurenin intihar girişiminde bulunduğunu anlattığı olayda,

Dairemizin değişen görüşüne göre;

Mağdurenin kişisel verilerini, kaydedilmiş haliyle ele geçirip, bu haliyle başkalarına verdiğine veya yaydığına dair hakkında bir delil bulunmayan sanığın, mağdurenin özel yaşam alanındaki sağlık bilgilerini okuyup, içeriğini öğrendiği mağdureye ait kişisel verileri başkalarına açıklaması eyleminin, TCK'nın 134/1-1. maddesinde tanımlanan özel hayatın gizliliğini ihlal suçunu oluşturacağı gözetilmeden, suç vasfında yanılgıya düşülerek, sanık hakkında, verileri hukuka aykırı olarak verme veya ele geçirme suçundan mahkumiyet kararı verilmesi…" Yargıtay 12. Ceza Dairesi 2014/3107 E., 2014/20959 K., 27.10.2014 tarihli kararı. https://www.kazanci.com.tr/ (Erişim Tarihi: 23.05.2020)

[222] **GÜLTEKİN**, s. 127; **DÜLGER**, Bilişim Suçları, s. 679; Bir görüşe göre bu, maddenin geniş yorumlanması anlamına gelmekte olup kanunilik ilkesine ters düşmektedir. Bu görüşe göre kişisel verilerin ancak ilk kez kaydedilmesinde suç oluşur, kaydedilmiş kişisel verilerin sonraki kullanımlarında ancak TCK m. 136'da düzenlenen kişisel verileri hukuka aykırı olarak ele geçirme suçu söz konusu olabilir. Ayrıntılı bilgi için bkz.; **AKDAĞ**, s. 104.

[223] **KÖSE AYSUN**, s. 122.

Maddi unsura göre suçların tasnifi bakımından bu suç; hareketin şekline göre icrai suçtur. Suç ancak failin aktif bir hareketi olan hukuka aykırı kaydetme eylemi ile gerçekleşebilir. Dolayısıyla suçun ihmali hareketle işlenmesi mümkün değildir.[224] Suçun işlenmesi için kanunda hareketin, kaydetmenin, şekli belirtilmediğinden suç serbest hareketli suçtur.[225]

Bu suç aynı zamanda sırf hareket suçudur. Suçun maddi unsuru kişisel verilerin hukuka aykırı olarak kaydedilmesinden ibarettir, ayrıca bir neticenin gerçekleşmesi gerekmez.[226] Bu suçtan bir zarar doğması yahut yarar sağlanması şart olmadığı gibi verilerin kullanılması da şart değildir.[227]

Suçun tamamlanması için bir zararın meydanı gelmesi aranmadığından suç tehlike suçudur.[228] Fiilin cezalandırılması için bir menfaatin somut olarak tehlikeye düşmesi gerekmediğinden soyut tehlike suçudur.[229]

---

[224] **HAFIZOĞULLARI-ÖZEN**, Kişilere Karşı Suçlar, s. 288.

[225] **AKDAĞ**, s. 97; Hareketin şeklinin kanunda belirtilmesi nedeniyle suçun bağlı hareketli suç olduğu yönündeki görüş için bkz. **ÖZBEK – DOĞAN – BACAKSIZ – TEPE**, s. 569.

[226] **AKDAĞ**, s.97; Suçun neticeli bir suç olduğu, kaydetmenin netice olduğu yönündeki görüş için bkz. **DÜLGER**, Kişisel Veriler, s. 318.

[227] **YAŞAR– GÖKCAN– ARTUÇ**, s. 4438.

[228] **DÜLGER**, Bilişim Suçları, s. 272.

[229] **AKDAĞ**, s. 98.

Maddenin ikinci fıkrasında suçun konusu olarak bazı veriler ayrıca belirtilmiş ve *"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."* şeklinde düzenleme yapılmıştır. Madde metninde sayılan kişisel verilerin bir kısmı için verilerin hukuka aykırı olarak kaydedilmesi özellikle vurgulanmıştır. Bu durum doktrinde, fıkrada sayılan *"kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine ilişkin"* kişisel verilerin "*mutlak dokunulmaz veriler"* olarak; *"ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin"* verilerin "*nisbi dokunulmaz veriler"* olarak kabul edilmesine neden olmuştur.[230] Bu görüşe göre ilk grupta sayılan verilen ve mutlak dokunulmaz veriler olarak adlandırılan kişisel veriler hiçbir şekilde kaydedilemez. Ancak ikinci fıkranın cezayı ağırlaştıran hal olduğu göz önünde bulundurulduğunda ve suçun temel şeklinde cezalandırılan fiilin "kişisel verilerin hukuka aykırı olarak kaydedilmesi" olduğu değerlendirildiğinde maddenin ikinci fıkrasının bu şekilde düzenlenmesinin kanun yapma tekniği açısından uygun olmadığı, birinci fıkra ve ikinci fıkra arasında bir çelişki oluşturulduğu açıktır. Nitekim karşıt bir görüşe göre de suçun temel şeklinde hukuka aykırı olarak veri kaydetmenin cezalandırılıyor olması nedeniyle hukuka aykırılığın

[230] Bu görüşe göre; ikinci fıkrada yer alan "hukuka aykırı olarak" ibaresinden bu sonuç ortaya çıkmaktadır. Madde gerekçesinde *"..Ancak, bunlardan kişilerin ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına ve 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."* denilmekte olması görüşe dayanak gösterilmektedir. **ÖZBEK – DOĞAN – BACAKSIZ – TEPE**, s. 567.

maddenin her iki fıkrasında sayılan kişisel veriler için geçerli olacağı belirtilmiştir.[231] Ancak bu durum da düzenlemeyi kanunun lafzından farklı yorumlamak anlamına geleceğinden tipikliğe aykırıdır.

b. Manevi Unsur

TCK m. 135'te suçun işlenmesi için özel bir kast aranmadığından suç genel kastla işlenebilir.[232] Failin kasten hareket etmesi; hukuka aykırı olarak bir kimseye ait kişisel verileri bilerek ve isteyerek kaydetmesi gerekir.[233] Bu suç taksirle işlenemez.[234] Failin kişisel veriyi kaydederken daha sonra bu verileri kullanma amacı olması gerekmez, veriyi hukuka aykırı olarak kaydetmesi yeterlidir.[235]

Suç tanımında kanunda özellikle hukuka aykırı olarak denildiğinden başka bir deyimle kanun koyucu bu suç açısından hukuka özel aykırılık aradığından suç ancak doğrudan kastla işlenebilir.[236]

---

[231] **YAŞAR – GÖKCAN – ARTUÇ**, s. 4438.

[232] **TAŞKIN**, Şaban Cankat; Bilişim Suçları, İstanbul 2008, s. 103; **KORKMAZ**, s. 344; Kanunun failde özellikle kişisel verileri hukuka aykırı olarak kaydetme kastı aradığı bu nedenle de suçun özel kastla işlenebileceği yönündeki görüş için bkz. **KARAGÜLMEZ**, s. 232.

[233] **HAFIZOĞULLARI - ÖZEN**, Kişilere Karşı Suçlar, s. 289.

[234] **YAŞAR – GÖKCAN – ARTUÇ**, s. 4438.

[235] **AKDAĞ**, s. 105.

[236] **ÖZGENÇ**, s. 289.

c. Hukuka Aykırılık

Bir fiilin suç sayılabilmesi için sadece kanundaki tanıma uyması yeterli değildir. Aynı zamanda fiilin hukuka aykırı bir fiil olması gerekir. Aksi halde ortada bir suç olduğundan bahsedilemez.[237]

TCK m. 135'te özel olarak "kişisel verilerin kaydedilmesi" fiilinin değil, "hukuka aykırı olarak kaydedilmesi" fiilinin cezalandırılacağı belirtilmiştir. Aynı şekilde TCK m. 136'da da suç tanımında fiilin "hukuka aykırı olarak" gerçekleştirilmesi gerektiği özellikle ifade edilmiştir. Suçun tanımında hukuka aykırılığın ayrıca zikredildiği bu gibi durumlar *"hukuka özel aykırılık"* olarak halleridir.[238] Bu hallerde suç ancak doğrudan kastla işlenebilir ve failin cezalandırılabilmesi için gerçekleştirdiği fiilin hukuka aykırı olduğunu da ayrıca bilmesi gerekir.[239]

Hukuka aykırılık fiil ile hukuk düzeni arasındaki çatışmadır. Hukuka aykırılık unsurunun yokluğu halinde suç da yoktur. Ancak kanunda fiilin özellikle "hukuka aykırı olarak" gerçekleştirilmesi gerektiğini belirttiği bu gibi *"hukuka özel aykırılık"* hallerinde failin kastının hukuka aykırılığı kapsaması yani fiilin hukuka aykırı olduğunu bilmesi ve

---

[237] **HAFIZOĞULLARI**, Zeki- **ÖZEN**, Muharrem; Türk Ceza Hukuku Genel Hükümler, Ankara 2017, s. 195. Suç olarak düzenlenen fiiller kural olarak zaten hukuka aykırıdırlar ancak madde metninde özellikle "hukuka aykırı olarak" ifadesinin yer almasına doktrinde farklı anlamlar izafe edilmiştir. Ayrıntılı bilgi için bkz. **KATOĞLU**, Tuğrul; Ceza Hukukunda Hukuka Aykırılık, Ankara 2003, s.125.

[238] **ÖZBEK – DOĞAN – BACAKSIZ – TEPE**, s. 573.

[239] **ARTUK**, Mehmet Emin- **GÖKCEN**, Ahmet- **YENİDÜNYA**, A. Caner; Ceza Hukuku Genel Hükümler, Ankara 2007, s. 527.

istemesi gerekmektedir.[240] Dolayısıyla, hukuka özel aykırılık hallerinin varlığı halinde hakim failin hukuka aykırılığı bilip bilmediğini ve kusurluluğunun hukuka aykırılığı kapsayıp kapsamadığını ayrıca araştırmalıdır.[241]

Yargıtay da aynı görüşte olup kararlarında hukuka aykırılığın varlığının ayrıca araştırılması gerektiğine işaret etmiştir: "*anılan maddenin uygulama alanının amaçlanandan fazla genişletilerek, uygulamada belirsizlik ve hemen her eylemin suç oluşturması gibi olumsuz sonuçların doğmaması için, maddenin uygulamasında, somut olayın özellikleri dikkate alınarak titizlikle değerlendirme yapılması**, olayda herhangi bir hukuk dalı tarafından kabul edilebilecek bir hukuka uygunluk nedeni veya bu kapsamda nazara alınabilecek bir hususun bulunup bulunmadığının saptanması ve sanığın eylemiyle hukuka aykırı hareket ettiğini bildiği ya da bilebilecek durumda olduğunun da ayrıca tespit edilmesi gerekir**.*"[242]

Kişisel verileri kaydetme suçu için kanunda öngörülmüş özel bir hukuka uygunluk nedeni bulunmadığından genel hükümler doğrultusunda hukuka uygunluk nedenlerinin varlığı araştırılmalıdır.

---

[240] **İÇEL**, Kayıhan – **SOKULLU AKINCI**, Füsun – **ÖZGENÇ**, İzzet – **SÖZÜER**, Adem – **MAHMUTOĞLU**, Fatih S. – **ÜNVER**, Yener; Suç Teorisi, İstanbul 2004, s. 110.

[241] **DÖNMEZER**, Sulhi – **ERMAN**, Sahir; Nazari ve Tatbiki Ceza Hukuku, Cilt II, İstanbul 1985, s. 21.

[242] Yargıtay 12. Ceza Dairesi 2017/12083 E., 2018/2539 K. sayılı ve 07.03.2018 tarihli kararı, Yargıtay 15. Ceza Dairesi 2015/1659 E., 2018/2748 K. sayılı ve 18.04.2018 tarihli kararı, Yargıtay 12. Ceza Dairesi 2016/9759 E., 2017/10938 K. sayılı ve 26.12.2017 tarihli kararı, Yargıtay 12. Ceza Dairesi 2016/9332 E., 2016/13355 K. sayılı ve 14.12.2016 tarihli kararı. https://www.kazanci.com.tr/ (Erişim Tarihi: 23.05.2020)

TCK m. 26/1'e göre *"hakkını kullanan kişiye ceza verilmez."* Hukuk düzenince bir kişiye bir hak tanınmış olması halinde bu hakkın kullanılması halinde başkalarının menfaati zarar görse dahi hakkını kullanana üstünlük tanınır ve ceza verilmez. Hakkın kullanılmasının hukuken kabulü için ise dört şartın varlığı aranır; [243]

- Hukuk düzeninde kabul edilen bir hakkın varlığı,
- Hukuk düzeninin öngördüğü sınırlar içinde hakkın kullanılması,
- Hakkın doğrudan doğuya kullanılabilir bir hak olması[244]
- Suç ile hakkın kullanılması arasında nedensellik bağı olması.

Kişisel verilerin kaydedilmesinde hakkın kullanılmasına örnek olarak işverenin yönetim hakkı kapsamında güvenlik kamera kayıtları gösterilebilir.[245]

Yine kişilerin yetkili makamlara verdikleri dilekçelerinde iddialarının dayanağını oluşturan somut olaya ilişkin belgelerde yer alan kişisel veriler de dilekçe hakkının kullanılması kapsamında değerlendirilerek hukuka uygun kabul edilmelidir.[246]

---

[243] **ARTUK – GÖKCEN – YENİDÜNYA**, Genel Hükümler, s. 396.

[244] Bu unsur gerekçede *"Eğer hak, bir mercie başvurularak kullanılabilecekse, artık buradaki hak kapsamında kabul olunmayacaktır."* şeklinde açıklanmıştır.

[245] **KÖSE AYSUN**, s. 150.

[246] **KANGAL**, s. 77; *"Sanık ... ile hakkındaki hükmün açıklanması geri bırakılan sanık ...'e ait ortak işyerinde, üçüncü kişilere ait çok sayıda nüfus cüzdanı fotokopisinin hukuka aykırı olarak saklandığı iddiasıyla ilgili olarak mahkemece kişisel verilerin hukuka aykırı olarak kaydedilmesi suçundan sanık ... hakkında mahkumiyet hükmü kurulmuş ise de; TCK'nın 135. maddesinde düzenlenen "Kişisel Verilerin Kaydedilmesi" suçunun konusunu oluşturan kişisel veri kavramından, kişinin, yetkisiz üçüncü kişilerin bilgisine sunmadığı, istediğinde başka kişilere açıklayarak ancak sınırlı bir çevre ile paylaştığı, herkes tarafından bilinmeyen ve/veya kolaylıkla ulaşılması ve bilinmesi mümkün*

TCK m.26/2'de rıza çerçevesinde işlenen fiilin cezalandırılmayacağı düzenlenmiştir. Kişinin hangi hakları üzerinde mutlak tasarrufta bulunabileceği tartışmalı[247] olsa da genellikle özel sırların ihlal edilmezliğine ilişkin haklar üzerinde tasarruf yetkisinin tam olduğu kabul edilir.[248]

Veri sahibinin kişisel verilerinin kaydedilmesine rıza göstermesi fiili hukuka uygun hale getirecektir. Örneğin gerçekleştirdiğimiz banka işlemlerinde, dernek

---

olmayan, kişinin kimliğini belirleyen veya belirlenebilir kılan, kişiyi toplumda yer alan diğer bireylerden ayıran ve onun niteliklerini ortaya koymaya elverişli, gerçek kişiye ait her türlü bilginin anlaşılması gerektiği, belirli veya belirlenebilir bir kişiye ait her türlü bilginin, hukuka aykırı olarak kaydedilmesi gerektiği gözetildiğinde; üçüncü kişilere ait nüfus cüzdanı fotokopilerinin, bu kişilerin rızaları dışında hukuka aykırı olarak ele geçirilip sanığın işyerinde bulundurulduğuna dair bir iddia bulunmadığı gibi, nüfus cüzdanı sahiplerinin ifadelerinde kendi rızaları ile birtakım hukuki işlemler nedeniyle nüfus cüzdanlarını verdiklerini beyan etmeleri karışısında sanık ...'in, unsurları oluşmayan hukuka aykırı olarak kişisel verileri kaydetmek suçundan beraati yerine mahkumiyetine karar verilmesi" Yargıtay 5. Ceza Dairesi 2014/10479 E., 2018/4622 K. Sayılı, 21.06.2018 tarihli kararı https://www.kazanci.com.tr/ (Erişim Tarihi: 24.05. 2020)

[247] Kişinin özgürlükleri üzerinde mutlak bir tasarruf yetkisinin olmadığını savunun bir görüşe göre bu özgürlükleri koruyan cezai düzenlemelere ilişkin rıza ancak suç tipinde rızanın olmaması hali özellikle aranıyorsa geçerlidir. Ayrıntılı bilgi için bkz. **CENTEL**, Nur – **ZAFER**, Hamide – **ÇAKMUT**, Özlem; Türk Ceza Hukukuna Giriş, İstanbul 2008, s. 321- 322.

[248] **TOROSLU**, Nevzat - **TOROSLU**, Haluk; Ceza Hukuku Genel Kısım, Ankara 2016, s. 185.

üyeliklerinde, internet alışverişlerinde ve günlük hayatta gerçekleştirdiğimiz birçok işlemde kişisel verilerimizin kaydedilmesine rıza göstermekteyiz.[249]

Hukuken geçerli bir rızadan söz edebilmek için; en başta rıza gösterenin suçun mağduru olması ve mağdurun da ehil olması gerekir. Aynı zamanda rızanın suç işlenmeden veya en geç suç işlendiği anda gösterilmesi gerekir. [250]

Genel hükümlere göre rıza açık veya örtülü olabilir[251] ancak kişisel verilerin kaydedilmesi açısından KVKK'nın 5. maddesi ilk fıkrası uyarınca kişisel veriler kural olarak veri sahibinin açık rızası[252] olmadan işlenemez.[253] Maddenin ikinci fıkrasında ise hangi hallerde ilgilinin açık rızası olmasa dahi kişisel verilerin işlenebileceği

---

[249] **ÖZEN**, Mustafa; *Kişisel Verilerin Kaydedilmesi, Verilmesi veya Ele Geçirilmesi ve Yok Edilmemesi Suçları (TCK m.136, 137, 138)*, Kamu Hukuku Arşivi, Mart 2009, s. 17.

[250] **HAFIZOĞULLARI - ÖZEN**, Genel Hükümler, s. 227- 228.

[251] **HAFIZOĞULLARI - ÖZEN**, Genel Hükümler, s. 228.

[252] KVKK m.3/1-b uyarınca *"açık rıza"* belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızadır.

[253] KVKK m. 3/1-e fıkrasına göre *"kişisel verilerin işlenmesi"; "kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi"* ifade eder. Dolayısıyla kişisel verilerin kaydedilmesi, KVKK anlamında kişisel verilerin işlenmesi içinde yer almaktadır.

belirtilmiştir.[254] Rızanın geçerli olabilmesi için kişiye kişisel verilerinin işleneceğinin, bu işlemenin amaçları ve sınırları hakkında bilgilendirme yapılması gerekmektedir.[255] Rızanın örtülü olması veya varsayılması mümkün değildir.[256] Rıza verinin kim tarafından hangi amaçlarla işleneceğini, nasıl kullanılacağını da kapsar şekilde alınmalıdır.[257] Aksi

---

[254] ***Kişisel verilerin işlenme şartları***

MADDE 5- *(1) Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez.*

(2) Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür:

a) Kanunlarda açıkça öngörülmesi.

b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.

c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.

ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.

d) İlgili kişinin kendisi tarafından alenileştirilmiş olması.

e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.

f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.

[255] **MORGAN**, Richard – **BOARDMAN**, Ruth; Data Protection Strategy – Implementing Data Protection Compliance, Thompson Sweet & Maxwell, London 2003, s.85.

[256] **CAREY**, Peter; Data Protection – A Pratical Guide to UK and EU Law, Third Edition, Oxford University Press, Oxford 2009,s. 66.

[257] **AKDAĞ**, s. 114-115.

halde kişisel verilerin kaydedilmesi fiilinin hukuka uygunluğundan bahsedilmesi mümkün değildir.

Ancak kişisel verilerin alınan rıza doğrultusunda kaydedilmesinden sonra bildirilen amaca aykırı olarak rızanın kapsamını aşacak şekilde kullanılması halinde bu suçun değil TCK m. 136'da düzenlenen "kişisel verileri hukuka aykırı olarak başkalarına verme, yayma veya ele geçirme" suçunun oluşması söz konusu olabilecektir.[258]

Fiili hukuka uygun hale getiren rızanın, fiil tamamlanıncaya kadar geri alınması her zaman mümkündür.[259] Rıza, fiil tamamlanmadan önce geri alınırsa fiil, mağdurun "rızasını geri aldığı andan itibaren" suç teşkil eder.[260] Başka bir deyişle rızanın fiil tamamlanmadan önce verilmiş olması ve fiil tamamlanana kadar devam etmesi gerekir ki aksi halde fiil tamamlandıktan sonra verilen rıza icazet olarak adlandırılır ve fiili suç olmaktan çıkarmaz.[261] Rıza, veri sahibi tarafından istenildiği zaman geri alınabilir. Örneğin; görüntülerinin kaydedilmesine izin veren bir kişi sonradan çeşitli nedenlerle rızasını geri alabilir. Bu durumda rıza geri alındıktan sonra kaydedilecek görüntüler açısından suç oluşur. [262]

[258] **AYDIN**, s. 149.

[259] **DEMİRBAŞ**, Timur; Ceza Hukuku Genel Hükümler, Ankara 2017, s. 331.

[260] **AKYÜREK**, Güçlü; Özel Hayatın Gizliliğini İhlal Suçu, Ankara 2011, s.285; **AKDAĞ**, s.115.

[261] **HAFIZOĞULLARI - ÖZEN**, Genel Hükümler, s. 227.

[262] **AYDIN**, s. 149.

Kişinin kendisi tarafından alenileştirilmiş kişisel verilerinin kaydedilmesi halinde ise rıza aranmaz.[263] Örneğin internette kişinin kişisel verilerini paylaşması ve bu verilerin bir başkası tarafından kaydedilmesi halinde suç oluşmaz.[264]

TCK'nın 24. maddesine göre "kanun hükmünü yerine getiren kimseye ceza verilmez." Kişisel veriler kaydedilmeden günlük hayatın devam etmesinin mümkün olmadığı[265] bir çağda yaşıyoruz. Ancak kişisel verilerin kaydedilmesi bir ihtiyaç olduğu gibi bu kaydetmenin istisnai hallerde ve belli şartlar dahilinde yapılması da zaruridir. Bu da ancak kanun marifetiyle yapılabilir.

KVKK'nın 5/2-a maddesine göre ise; "kanunlarda açıkça öngörülmesi halinde" kişisel veriler ilgilinin rızası aranmaksızın kaydedilebilir. Yine KVVK'nın 6. maddesine göre ise; "sağlık ve cinsel hayat dışındaki" özel nitelikli kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir.

Örnek olarak; "5352 sayılı Adli Sicil Kanunu" 2. maddesinde kişilerin mahkumiyetine ilişkin veriler adli sicilde tutulur. Yine, "2559 sayılı Polis Vazife ve Salahiyet Kanunu'nun" 5. maddesine göre polis tarafından alınan parmak izi ve fotoğrafların, CMK m. 75 ve m. 76'ya göre şüpheli, sanık veya mağdurun vücudundan alınan örneklerin, CMK m. 78 gereğince moleküler genetik incelemelerden elde edilen örneklerin, CMK m. 81'e göre alınan ölçü, fotoğraf, parmak izi ve avuç içi izi, ses ve görüntülerin, CMK m. 134/3'e göre yapılacak veri yedeklemelerinin, CMK m. 135/6'ya

[263] **AYDIN**, s. 147.

[264] **KARAGÜLMEZ**, s. 354.

[265] **AKDAĞ**, s. 120.

göre şüpheli veya sanığa ait telefonların görüşme kayıt ve sinyal bilgilerinin kişisel veri olarak kaydedilmesi kanunun hükmünün yerine getirilmesidir.[266]

6. Suçun Özel Görünüş Şekilleri

a. Teşebbüs

Kural olarak sırf hareket suçlarına teşebbüsten bahsedilemez. Ancak hareketin parçalara bölünebildiği durumlarda teşebbüsten bahsedilebilecektir.[267] Failin kişisel verileri toplamaya başladığı anda yakalanması durumunda teşebbüs söz konusu olacaktır.[268] Ancak kişisel verilerin hukuka aykırı olarak elde edilmiş ancak kaydedilmemiş olması durumunda suçun teşebbüs aşamasında kaldığından ziyade TCK m. 136'nın oluşma ihtimalidir.

b. İştirak

Suçun, iştirak hükümleri açısından herhangi bir özelliği yoktur. TCK'nın iştirake ilişkin tüm hükümleri bu suç için de uygulanabilir. TCK m. 137 gereğince iştirak edenin

---

[266] **KORKMAZ**, s.354 vd., **SERT**, s. 116 vd.

[267] **HAFIZOĞULLARI - ÖZEN**, Özel Hükümler, s. 323.

[268] **YAŞAR – GÖKCAN - ARTUÇ**, s. 4440; **AKDAĞ**, s. 123; Aksi yöndeki görüş için bkz.; **ÖZBEK – DOĞAN – BACAKSIZ – TEPE**, s. 576. Yazarlara göre; TCK m. 136'da kişisel verileri ele geçirme ayrıca suç olarak tanımlandığından kişisel verilerin ele geçirilmiş ancak henüz kaydedilmemiş olması halinde teşebbüsten bahsedilemez.

"kamu görevlisi olması" veya "belli bir meslek ve sanatın sağladığı kolaylıktan yararlanması" durumunda cezaları yarı oranında artırılır.[269]

c. İçtima

Suçun zincirleme suç şeklinde işlenmesi mümkündür. Suçun, "aynı suç işleme kararının icrası kapsamında aynı kişiye karşı birden fazla kez" veya "tek hareketle birden fazla kişiye karşı" işlenmesi halinde zincirleme suç oluşur.[270]

Öte yandan, örneğin kişisel verilerin hukuka aykırı olarak bir internet sitesine kaydedilmesi halinde TCK m. 135 ve TCK m. 136'da düzenlenen iki suç da işlenmiş olur ve fikri içtima uygulanır.[271]

Kaydedilen veri kişisel veri niteliğinde olmayıp kişinin özel hayatına ilişkin ise özel hayatın gizliliğini ihlal suçu oluşur.[272]

---

[269] **DÜLGER**, Bilişim Suçları, s. 703; Bir görüşe göre suçun TCK m. 137'de düzenlenen nitelikli halleri özgü suç olduğundan bu suçlara madde metninde belirtilen nitelikleri taşımayan kişiler tarafından dolaylı fail veya müşterek fail olarak iştirak edilmesi mümkün değildir. Bkz.; **AYDIN**, s. 162.

[270] **YAŞAR – GÖKCAN - ARTUÇ**, s. 4440.

[271] **ÖZBEK – DOĞAN – BACAKSIZ – TEPE**, s. 576.

[272] Yargıtay 12. Ceza Dairesi 2012/17703 E., 2012/18222 K. Sayılı, 11.09.2012 tarihli kararında *"5237 sayılı TCK'nın 135. maddesinde düzenlenen "Kişisel verilerin kaydedilmesi" suçunun oluşabilmesi için belirli veya belirlenebilir bir kişiye ait her türlü bilginin, hukuka aykırı olarak kaydedilmesi gerekmekte olup; suçun maddi konusunu*

7. Suçun Nitelikli Halleri

TCK m. 135'in ikinci fıkrasında "kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine, ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin verilerin kaydedilmesi", suçun nitelikli hali olarak düzenlenmiştir.

KVKK m. 6'da ise "özel nitelikli veriler" *"kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf*

---

oluşturan "kişisel veri" kavramından, kişinin, yetkisiz üçüncü kişilerin bilgisine sunmadığı, istediğinde başka kişilere açıklayarak ancak sınırlı bir çevre ile paylaştığı, herkes tarafından bilinmeyen ve/veya kolaylıkla ulaşılması ve bilinmesi mümkün olmayan, kişinin kimliğini belirleyen veya belirlenebilir kılan, kişiyi toplumda yer alan diğer bireylerden ayıran ve onun niteliklerini ortaya koymaya elverişli, gerçek kişiye ait her türlü bilginin anlaşılması gerektiği; bir özel hayat görüntüsü ya da sesinin, "kişisel veri" olduğunda kuşku bulunmamakta ise de, kişinin özel hayatına ilişkin görüntüsü ya da sesinin, bilgisi dışında, resim çekme veya kaydetme özelliğine sahip aletle belli bir elektronik, dijital, manyetik yere sabitlenmesi eyleminin, 5237 sayılı TCK'nın 134/1. maddesinin 2. cümlesinde tanımlanan özel hayatın gizliliğini ihlal suçu kapsamında değerlendirilmesi gerektiği, kişinin özel hayatına ilişkin görüntü, fotoğraf ya da sesin, 5237 sayılı TCK'nın 135. maddesi kapsamında kişisel veri olarak kabul edilemeyeceği, iddiaya konu olayda, mağdurenin çıplak vaziyetteki görüntü ve fotoğraflarının kaydedilmesinden ibaret eylemin, "Kişisel verilerin kaydedilmesi" suçunu oluşturmayacağı, çekimin, mağdurenin bilgisi ve rızası kapsamında gerçekleşmesi nedeniyle, özel hayatın gizliliğini ihlal suçunun da oluşmadığı anlaşıldığından,"; **YAŞAR – GÖKCAN - ARTUÇ**, s. 4440.

ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri" olarak sayılmıştır.

Esasen bu iki düzenleme birbiri ile örtüşmemektedir. KVKK'da sayılmış fakat TCK'da sayılmayan özel nitelikli verilerin kaydedilmesi halinde, kanunilik ilkesi gereğince; özel nitelikli veriler için ikinci fıkrada öngörülen şekilde cezada artırım yapılamayacak ancak fail birinci fıkradaki temel ceza ile cezalandırılabilecektir.

TCK m. 137'de ise; 135. madde ve 136. madde için ortak nitelikli haller düzenlenmiştir.

Bu maddede düzenlenen nitelikli hallerden ilki "suçun kamu görevlisi tarafından görevinin verdiği yetki kötüye kullanılmak" suretiyle işlenmesidir. Fail hakkında nitelikli halin uygulanıp uygulanmayacağının tespitinde öncelikle failin kamu görevlisi olup olmadığının tespiti gerekir.

"Kamu görevlisi", TCK m. 6/1-c bendinde *"kamusal faaliyetin yürütülmesine atama veya seçilme yoluyla ya da herhangi bir surette sürekli, süreli veya geçici olarak katılan kişi"* olarak tanımlanmıştır. Tanımdan kamu görevlisi sayılmanın iki ölçütü olduğu anlaşılmakta olup bunlar kamusal faaliyetin varlığı ile kişinin yürütülen bu kamusal faaliyete katılmasıdır.[273]

İkinci olarak failin kamu görevlisi olması yanında kişisel verilerin hukuka aykırı olarak kaydedilmesi fiilini "görevinin verdiği yetkiyi kötüye kullanarak" gerçekleştirmesi aranmaktadır. Örneğin, vergi dairesi görevlilerinin görevleri gereği erişim yetkileri bulunan kişisel verileri görevleri gerektirmediği halde hukuka aykırı olarak kaydetmeleri

[273] **AYDIN**, Hüseyin; *Ceza Hukukunda Kamu Görevlisi Kavramı*, Ankara Barosu Dergisi, S.: 2010/1, 118, 119.

halinde bu fıkra uyarınca işledikleri suça ilişkin verilecek cezada artırım yapılması gerekecektir.[274]

TCK m.137'de düzenlenen diğer nitelikli hal suçun "belli bir meslek ve sanatın sağladığı kolaylıktan yararlanılarak" işlenmesi halidir. Bu hal için önemli olan husus ise failin yaptığı meslek ve sanatın faile suçu işlemede bir kolaylık sağlamasıdır. Örneğin; serbest çalışan bir doktorun hastalarının tahlil sonuçlarını kendisine ait bilgisayarda depolaması halinde bu suç oluşacaktır.[275]

8. Yaptırım

Suçun temel şeklinin cezası "1 yıldan 3 yıla kadar hapis cezası" olarak düzenlenmiştir. Suçun maddenin ikinci fıkrasında belirtilen kişisel verilere hakkında işlenmesi halinde ise "birinci fıkra uyarınca verilecek ceza yarı oranında artırılır." Yine, TCK m. 137'de düzenlenen nitelikli hallerin işlenmesi durumunda da verilecek ceza yarı oranında artırılır.

Madde yaptırım bakımından 2 kez değişikliğe uğramıştır. İlk olarak maddenin ilk fıkrasında öngörülen cezanın altı sınırı 6 aydan bir yıla çıkarılmış[276] daha sonra ise kişisel

[274] **KÖSE AYSUN**, s. 144.

[275] **YAŞAR -GÖKCAN- ARTUÇ**, s. 4439.

[276] 21.02.2014 tarihli ve 6526 sayılı Kanunun 3. maddesi ile cezanın alt sınırı artırılmıştır.

verilerin maddenin ikinci fıkrasında sayılan özel nitelikli kişisel verilerden olması hali cezada artırım sebebi olarak öngörülmüştür.[277]

Ayrıca TCK m.140 uyarınca tüzel kişiler hakkında güvenlik tedbirlerine hükmolunabilecektir.

9. Soruşturma ve Kovuşturma

TCK m. 139 gereğince suç, re'sen soruşturulan ve kovuşturulan bir suçtur. Öngörülen cezanın üst sınırına göre görevli mahkeme asliye ceza mahkemesidir.

Suçun kamu görevlisi tarafından görevi sebebiyle işlenmesi halinde soruşturma yapılması izne tabi olacağından 4483 sayılı Memurlar ve Diğer Kamu Görevlilerinin Yargılanması Hakkında Kanun uyarınca yetkili merciden izin alındıktan sonra soruşturma yapılması gerekir.[278]

[277] Bu fıkrada yer alan *"Kişilerin"* ibaresi *"Kişisel verinin, kişilerin"* şeklinde; *"bilgileri kişisel veri olarak kaydeden kimse, yukarıdaki fıkra hükmüne göre cezalandırılır"* ibaresi *"olması durumunda birinci fıkra uyarınca verilecek ceza yarı oranında artırılır"* şeklinde değiştirilmiştir.

[278] **ARTUÇ**, s. 1635.

C. VERİLERİ HUKUKA AYKIRI OLARAK VERME veya ELE GEÇİRME SUÇU(TCK m. 136)

1. Genel Olarak

TCK m. 136'da *"Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır."* denilmektedir. 17/10/2019 tarihinde ise madde metnine *"Suçun konusunun, Ceza Muhakemesi Kanununun 236'ncı maddesinin beşinci ve altıncı fıkraları uyarınca kayda alınan beyan ve görüntüler olması durumunda verilecek ceza bir kat artırılır."* şeklindeki ikinci fıkra eklenmiştir.

Madde başlığında *"Verileri hukuka aykırı olarak verme veya ele geçirme"* denilmekte ise de içeriğinden anlaşılacağı üzere suç, *"vermek", "yaymak"* veya *"ele geçirmek"* suretleriyle işlenebilir. Yine madde başlığında *"kişisel veri"* denilmek yerine üst kavram olan *"veri"* kelimesi kullanılmıştır.

Çalışmanın bu bölümünde kişisel verileri hukuka aykırı olarak kaydetmek suçuyla aynı özelliği taşıyan durumlara kısaca değinilmekle yetinilmiştir.

2. Hukuki Konu

Yasal düzenleme ile tıpkı kişisel verileri hukuka aykırı olarak kaydetme suçundaki gibi 2010 yılındaki Anayasa değişikliğiyle anayasal temele kavuşan kişisel verilerin korunması hakkı korunmaktadır.[279]

[279] **HAFIZOĞULLARI – ÖZEN**, s. 290; **SOYASLAN**, s. 360; **KORKMAZ**, s. 384, 385.

3. Fail

Madde metninde *"kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi"* denilmekte olup fail açısından bir özellik aranmadığından suçun faili herkes olabilir.[280] Bu suçta da suçun "kamu görevlisi tarafından veya belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle" işlenmesi TCK m. 137'de cezayı artıran neden olarak düzenlenmiştir.

4. Mağdur

Herkes suçun mağduru olabilir. Suça konu kişisel verilerin sahibi kimse suçun mağdurudur.[281]

5. Suçun Unsurları

a. Maddi Unsur

Madde metninde kişisel verileri ele geçirme, bir başkasına verme ve yayma suç olarak sayılmış olup suç üç seçimlik hareketten biri gerçekleştirilerek işlenebilir. Başka

[280] **ÖZBEK – DOĞAN – BACAKSIZ – TEPE**, s. 577; **HAFIZOĞULLARI – ÖZEN**, s. 289; **SOYASLAN**, s. 360.

[281] **HAFIZOĞULLARI – ÖZEN**, s. 290; **ÖZBEK – DOĞAN – BACAKSIZ – TEPE**, s. 577; **SOYASLAN**'a göre tüzel kişiler de suçun mağduru olabilir. Bkz.; **SOYASLAN**, s. 360.

bir deyişle suç "seçimlik hareketli" bir suçtur[282] ve suçun gerçekleşmesi için seçimlik hareketlerden birinin yapılması yeterlidir.[283] Seçimlik hareketlerden birkaçının birlikte yapılması halinde ise birden çok suç oluşmaz yine tek suç oluşur.[284]

Madde gerekçesinde de belirtildiği üzere ele geçirilen, verilen ya da yayılan kişisel verilerin hukuka uygun ya da hukuka aykırı kaydedilmiş olmasının bir önemi bulunmamaktadır zira TCK m. 135 ve TCK m. 136'da düzenlenen iki suç tipi birbirinden bağımsızdır.[285] Ancak suça konu fiillerin gerçekleştirilmesi için hukuka uygun yada

---

[282] **ÖZBEK – DOĞAN – BACAKSIZ – TEPE**, s. 578; **KORKMAZ**, s. 387, 388.

[283] **KANGAL**, s. 96.

[284] **HAFIZOĞULLARI – ÖZEN**, s. 290

[285] **DÜLGER**, Kişisel Veriler, s. 347, 348; *"TCK'nın 135 ve 136. maddelerinde düzenlenen "Kişisel Verilerin Kaydedilmesi" ve "Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme" suçlarının konusunu oluşturan kişisel veri kavramından, kişinin, yetkisiz üçüncü kişilerin bilgisine sunmadığı, istediğinde başka kişilere açıklayarak ancak sınırlı bir çevre ile paylaştığı, herkes tarafından bilinmeyen ve/veya kolaylıkla ulaşılması ve bilinmesi mümkün olmayan, kişinin kimliğini belirleyen veya belirlenebilir kılan, kişiyi toplumda yer alan diğer bireylerden ayıran ve onun niteliklerini ortaya koymaya elverişli, gerçek kişiye ait her türlü bilginin anlaşılması gerektiği, belirli veya belirlenebilir bir kişiye ait her türlü bilginin, hukuka aykırı olarak kaydedilmesi, TCK'nın 135. maddesinde "Kişisel verilerin kaydedilmesi" başlığı altında, belirli veya belirlenebilir bir kişiye ait her türlü bilginin, başkasına verilmesi, yayılması ya da ele geçirilmesi, aynı Kanunun 136/1. maddesinde "Verileri hukuka aykırı olarak verme veya ele geçirme" başlığı altında birbirinden bağımsız iki ayrı suç olarak tanımlanmıştır."* Yargıtay 12. Ceza Dairesi 2015/4349 E., 2016/5349 K. Sayılı ve 30.03.2016 tarihli kararı https://www.kazanci.com.tr/ (Erişim tarihi : 24.05.2020)

aykırı olduğu farketmeksizin kişisel verilerin kaydedilmesi zorunlu olup kaydedilmemiş kişisel verilerin ele geçirilmesi, verilmesi ya da yayılması mümkün değildir.[286]

Sözlük anlamıyla *"vermek"*; *"üzerinde, elinde veya yakınında olan bir şeyi birisine eriştirmek, iletmektir."*[287] Kişisel veriyi birine vermek veriyi birisine ulaştırmak demektir.[288] Vermenin, yayma düzeyine varmayan bir fiil olduğu söylenilebilir.[289] Suç, kişisel verilerin verildiği kişi tarafından "öğrenilebilir hale geldiğinde" suç tamamlanmış olur, verilerin içeriğine vakıf olunup olunmaması suçun sübutu açısından önem taşımaz.[290]

---

[286] *"TCK'nın 136/1. maddesinin, "Bu madde hükmü ile hukuka uygun olarak kaydedilmiş olsun veya olmasın, kişisel verileri hukuka aykırı olarak başkalarına vermek, yaymak veya ele geçirmek, bağımsız bir suç olarak tanımlanmıştır." şeklindeki gerekçesinden de anlaşılacağı üzere, kişisel verilerin, "verildiği", "yayıldığı" veya "ele geçirildiği"nin kabul edilebilmesi için, kişisel verilerin kaydedilmiş halde bulunması, kaydedilmiş haliyle başkalarına verilmesi, yayılması ya da ele geçirilmesi gerekir."* Yargıtay 12. Ceza Dairesi 2015/10737 E., 2016/13557 K. Sayılı ve 21.12.2016 tarihli kararı https://www.kazanci.com.tr/ (Erişim tarihi : 24.05.2020)

[287] Türk Dil Kurumu Güncel Türkçe Sözlük, https://www.sozluk.gov.tr/ (Erişim Tarihi: 24.05.2020); Ayrıca bkz. Yargıtay Ceza Genel Kurulu 2017/12-829 E., 2017/363 K. sayılı ve 04.07.2017 tarihli kararı. https://www.kazanci.com.tr/ (Erişim tarihi : 24.05.2020)

[288] **YAŞAR -GÖKCAN- ARTUÇ**, s. 4439.

[289] **TAŞKIN**, s. 107; **KORKMAZ**, s. 387.

[290] **AKDAĞ**, s. 130; **KANGAL**, s. 106; *"Sanığın, 19 Eylül 2012 tarihinde uğradığı suikast sonucu öldürülen.... Cumhuriyet savcısı.... ve onun eşi olan katılana ait ... adliye lojmanlarındaki ev eşyalarını ...'a taşımak için çalışmakta olduğu nakliye firması*

tarafından görevlendirildikten ve eşyaların 20.10.2012 tarihinde kamyona yüklenmesinden sonra, adı geçen Cumhuriyet savcısının şahsi bilgisayarını katılana teslim etmeyip, bilgisayarda gördüğü kişisel ve ailevi bilgi, belge ve görüntüleri 21.10.2012 tarihinde sildiği, durumun fark edilerek, sanıktan bilgisayarı geri getirmesinin istenmesi üzerine, sanığın, önce inkar ederek bilgisayarın kendisinde olmadığını ifade ettiği, daha sonra, bilgisayarın kazaen düştüğünü ve içindeki verileri yanlışlıkla sildiğini beyanla bilgisayarı tamir ettirip getireceğini söylediği, 22.10.2012 tarihinde de, bilgisayarı ...'taki bir tamirciye götürüp, ondan silinen verileri kurtarmasını istediği, 23.10.2012 tarihinde bilgisayara kurulan bir program sayesinde, tamirci tarafından bir kısmının içeriğine vakıf olunan silinen verilerin tespit edilip geri getirildiği, aynı gün tamirciden aldığı bilgisayarı teslim etmek üzere ...a gelen sanığın, bilgisayarla birlikte yakalandığı olayda,

Cumhuriyet savcısına ait şahsi bilgisayarla iki adet kol saatinin katılana teslim edilmediği iddiasına dayalı olarak sanık hakkında güveni kötüye kullanma suçundan yürütülen soruşturma evrakı tefrik edilip, sanığın özel hayatın gizliliğini ihlal ve verileri hukuka aykırı olarak verme veya ele geçirme suçlarından cezalandırılması istemiyle dava açıldığı, iddianamede, "Bilgisayar içerisinde bulunan özel bilgilere ulaşmak" şeklinde tarif edilen eylemle ilgili olarak özel hayatın gizliliğini ihlal suçundan açılan dava hakkında hüküm kurulmasına yer olmadığına karar verildiği, iddianamedeki anlatım ve uygulanması istenen sevk maddelerine göre, bilişim sistemindeki verilerin silinmesinden dolayı TCK'nın 244/2. maddesindeki sistemi engelleme, bozma, verileri yok etme veya değiştirme suçundan açılmış bir dava bulunmadığı ve sanığın temyiz isteminin verileri hukuka aykırı olarak verme veya ele geçirme suçundan kurulan mahkumiyet hükmüne yönelik olduğu anlaşıldığından, verileri hukuka aykırı olarak verme veya ele geçirme suçundan kurulan mahkumiyet hükmüne hasren yapılan temyiz incelemesinde:

Kişisel verilerin hangi ortamda ve surette verildiği bir önem taşımamaktadır. Suç, verilerin (elden) fiziken teslim edilmesi ile gerçekleşebileceği gibi (flash bellek gibi)

İddianamedeki anlatıma, temyizin kapsamına, dosyada mevcut delillere nazaran, kişisel veri niteliğindeki kayıtların bulunduğu bilgisayarı zamanında katılana teslim etmeyip, bilgisayarda kayıtlı kişisel ve ailevi bilgi, belge ve görüntülere bakan, bilgisayarı tamirciye bırakıp, kişisel verilerin tamirci tarafından öğrenilmesine neden olan sanığın üzerine atılı verileri hukuka aykırı olarak verme veya ele geçirme suçunun sübut bulduğuna ve eylemin hukuki nitelendirmesine yönelik yerel mahkemenin kabulünde bir isabetsizlik görülmemiş…" Yargıtay 12. Ceza Dairesi 2014/19849 E., 2015/4801 K. Sayılı 23.03.2015 tarihli kararı https://www.kazanci.com.tr/ (Erişim tarihi : 24.05.2020)

dijital ortamda veya (faks, e-mail[291], SMS[292], WhatsApp gibi) haberleşme araçlarıyla gönderilmek suretiyle de verilebilir.[293]

---

[291] *"Katılan ...'nun internette gördüğü iş ilanı üzerine sanık ...'e ait.... Danışma Merkezi'ne geçici mezuniyet belgesi, adli sicil kaydı, doktor raporu, nüfus cüzdan örneği gibi belgeler ile bizzat müracaat ettiği, aradan epey bir süre geçmesine rağmen herhangi bir netice çıkmaması ve katılanın durumdan şüphelenmesi üzerine vermiş olduğu belgeleri geri istediği ancak sanığın belgeleri geri iade etmediği gibi bu belgeleri Gaziantep'te bulunan diğer sanık ...'ya posta yoluyla gönderdiği, sanık ...'nun da bu belgeleri Gaziantep'te açacağı ....ezi'nin kuruluş aşamasında Milli Eğitim Müdürlüğü, SGK, Vergi Dairesi gibi kurumlara müracaatında kullandığı dosya kapsamından anlaşılmakla; sanık ...'ün kendisine iş başvurusu sırasında katılan tarafından verilen belgeler üzerinde sahtecilik yaptığı veya bu belgeleri diğer sanık ... ile birlikte Gaziantep'te açılacak olan.... ve Rehabilitasyon Merkezi'nin kuruluş aşamasında kurumlara karşı kullandığı sabit değil ise de, gerek katılan ...'in beyanları, gerekse sanık ...'nun savunmalarına göre bu belgeleri ...'ya sanık ...'ün gönderdiği anlaşıldığından, sanığın eyleminin bu haliyle TCK'nın 136/1. maddesindeki "verileri hukuka aykırı olarak verme veya ele geçirme" suçunu oluşturup oluşturmayacağı değerlendirilmeden eksik inceleme ile yazılı şekilde beraate hükmedilmesi"* Yargıtay 11. Ceza Dairesi 2015/8796 E., 2017/5266 K. Sayılı, 10.07.2017 tarihli kararı https://www.kazanci.com.tr/ (Erişim tarihi : 24.05.2020)

[292] *"Bu açıklamalar ışığında incelenen dosya kapsamına göre; kız öğrencilerle iletişime geçme amacını taşıyan sanık ...'nin, katılan mağdur ... ve arkadaşlarının öğrenim gördüğü lisenin telefon numarasını arayarak, santraldeki görevli tarafından, talebi üzerine yönlendirildiği okul kantinindeki çalışan ile konuşup, kız öğrencilerden birisinin telefona bakmasını istemesinin ardından görüştüğü mağdurun sınıf arkadaşı 16 yaşındaki*

Kişisel verilerin verildiği kişi gerçek ya da tüzel kişi olabilir.[294]

Tayyibe'ye, kendisini "Ali Hoca" olarak tanıtarak, okul müdür yardımcısının adının da Ali olması sebebiyle mağdurun arkadaşını kandırıp, onun güvenini kazandıktan sonra, ekonomik durumu zayıf ve başarılı olan öğrencilerin kendisine kontenjan ayrılan dershanelere burslu gönderileceğini bahane ederek mağdurun arkadaşından bu niteliklere sahip kız öğrencilerin isim ve cep telefonu numaralarını göndermesini istediği ve mağdurun arkadaşı tarafından kullanımındaki cep telefonuna gönderilen mesaj sayesinde mağdurun kişisel veri niteliğindeki adı, soyadı ve cep telefonu numarasını, hukuka uygunluk nedenlerinin bulunmaması sebebiyle hukuka aykırı olduğunda tereddüt bulunmayan bir yöntemle ele geçirdiği anlaşılmakla," Yargıtay 12. Ceza Dairesi 2015/9893 E., 2016/12504 K. Sayılı, 09.11.2016 tarihli kararı https://www.kazanci.com.tr/ (Erişim tarihi : 24.05.2020)

[293] **DÜLGER**, Kişisel Veriler, s. 350; **KANGAL**, s. 106, 107.

[294] **SERT**, s. 138; **DÜLGER**, Kişisel Veriler, s. 351; *""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. Türk Dil Kurumu Büyük Türkçe Sözlüğünde "vermek"; "üzerinde, elinde veya yakınında olan bir şeyi birisine eriştirmek, iletmek, düşünce veya bilgi anlatan şeyleri başkalarına iletmek, bildirmek" şeklinde açıklanmıştır. Bu seçimlik harekette verilerin hukuka uygun ya da aykırı yöntemle elde edilmiş olmasının önemi bulunmamakta olup, önemli olan husus verme eyleminin hukuka aykırı olmasıdır."* Yargıtay Ceza Genel Kurulu 2017/12- 829 E., 2017/363 K. Sayılı, 04.07.2017 tarihli kararı https://www.kazanci.com.tr/ (Erişim Tarihi: 24.05.2020)

"Yaymak" ise; *"Birçok kimseye duyurmak"* anlamına gelmektedir.[295] Kişisel verileri yaymak, iki ve daha fazla kişinin öğrenebileceği şekilde duyurmaktır.[296] Yaymak fiili de tıpkı vermek fiilinde olduğu gibi birçok şekilde gerçekleştirilebilir. Yaymanın fiziken, dijital ortamda ya da internet üzerinden gerçekleştirilmesi mümkündür. Benzer şekilde, kişisel veriler yazılı, görsel veya işitsel olarak da yayılabilir. [297] Suçun bu

---

[295] Türk Dil Kurumu Güncel Türkçe Sözlük, https://www.sozluk.gov.tr/ (Erişim Tarihi: 24.05.2020)

[296] **HAFIZOĞULLARI – ÖZEN**, s. 290.

[297] **KORKMAZ**, s. 388. *"Sanığın, kız arkadaşının husumetli olduğu mağdurlar adına, internette bir arkadaşlık sitesinde "Atesli_Dizdar" ve "Afet-i Derya" kullanıcı isimleri ile üyelik işlemleri yapıp, oluşturduğu profil sayfalarında, mağdurların şeref, onur ve saygınlığını rendice edecek nitelikte ibareler ile birlikte kişisel veri niteliğindeki fotoğraflarını ve telefon numaralarını ilgili siteye kaydedip, yayımlaması biçimindeki eyleminin, TCK'nın 135/1, 136/1 ve 125/2-1-4 maddelerine uyan, kişisel verilerin kaydedilmesi, verileri hukuka aykırı olarak verme veya ele geçirme ve hakaret suçlarını oluşturduğu, sanığın tek eyleminin kanundaki birden fazla suçları oluşturması nedeniyle TCK'nın 44. maddesinde düzenlenen fikri içtima kuralı uyarınca en ağır cezayı gerektiren TCK'nın 136/1. madde ve fıkrasında tanımlanan verileri hukuka aykırı olarak verme veya ele geçirme suçundan cezalandırılması gerektiği ve fikri içtima kuralı nazara alınmadan, daha hafif cezayı gerektiren TCK'nın 135/1. maddesi uyarınca hüküm kurulması,*

... Kanuna aykırı olup, sanık müdafiinin temyiz itirazları bu itibarla yerinde görüldüğünden, hükmün bu sebeplerden dolayı 5320 sayılı Kanun'un 8. maddesi uyarınca halen uygulanmakta olan 1412 sayılı CMUK'un 321. maddesi gereğince isteme aykırı olarak bozulmasına," Yargıtay 12. Ceza Dairesi 2014/1463 E., 2014/17262 K. Sayılı, 08.09.2014 tarihli kararı. https://www.kazanci.com.tr/ (Erişim tarihi : 24.05.2020)

seçimlik hareketle işlenmesi halinde de yayılan kişisel verilerin başkaları tarafından öğrenilip öğrenilmemesi suçun sübutu açısından önem taşımaz, birden fazla kişinin öğrenmesine imkan verir şekilde yayılmış olması yeterlidir.[298]

Bir kişisel verilerin erişilebilir bir yerde yayınlanmış olması o veriyi kişisel veri olmaktan çıkarmaz.[299] Hatta kişisel veri rıza ile yayınlanmış olsa bile veri sahibi ilgili kişi aynı verinin başka mecralarda yayılmasına karşı çıkabilir.[300] Örneğin, cep telefonu numarasının bağlı bulunduğu baronun internet sitesinde yayınlanmasına rıza gösteren bir avukat başka sitelerde numarasının yayılmasına rıza göstermeyebilir. Kişinin kendisi tarafından alenileştirilmiş olsa dahi bu kişisel verinin hukuka aykırı olarak yayılması halinde suç oluşacaktır. Ancak buradan elde edilen kişisel verilerin yayılmaması yalnızca ele geçirilmesi halinde suçun oluşması söz konusu değildir.

"Ele geçirmek" ise sözlükte *"Yakalamak, sahibi olmak, gizlenmek istenen bir şeyi elde etmek"* gibi anlamlara gelmektedir.[301] Kişisel verileri ele geçirmek, başkasının hakimiyet alanında bulunan kişisel verilerin o kişinin iradesi dışında elde edilmesidir.[302]

---

[298] **AKDAĞ**, s. 131.

[299] **PARENT**, W.A.; *"A New Definition of Privacy for the Law",* Law and Philosophy, V. 2, 1983, s. 308. http://people.brandeis.edu/~teuber/Parent_on_Privacy.pdf (Erişim tarihi : 24.05.2020)

[300] **AKDAĞ**, s. 132.

[301] Türk Dil Kurumu Güncel Türkçe Sözlük, https://www.sozluk.gov.tr/ (Erişim Tarihi: 24.05.2020)

[302] **AKDAĞ**, s. 135.

Kişisel verileri başkasına verme veya yayma hareketi o kişisel verileri elinde bulunduran kişi açısından gerçekleştirilebilirken, ele geçirme ise elinde kişisel veri bulunmayıp elde etmek isteyen kişi tarafından gerçekleştirilmektedir.[303]

Ele geçirme fiziki bir belgenin fiziken bir yerden alınması veya kayıtlı olduğu sisteme girilerek oradan herhangi bir suretle alınması şeklinde olabilir.[304]

Kişinin kendisine ait kişisel verileri umuma açık olarak paylaştığı yerden elde edilmesi halinde suçtan bahsedilemez[305] çünkü veriyi hakimiyeti altına alan kişinin bunu gerçekleştirmek için bir müdahalesi söz konusu değildir, veri sahibinin iradesi ile ulaşılabilir hale getirilmiştir.[306] Ancak kişinin erişim yetkisi olmadığı halde kendi uhdesine almasa dahi kişisel verilere yalnızca görerek vakıf olması halinde de suç gerçekleşmiş olur.[307] Zira, kişisel verilerin korunması ile ilgili hükümlerin amacı verinin

---

[303] **YAŞAR – GÖKCAN- ARTUÇ**, s. 4446.

[304] **DÜLGER**, Kişisel Veriler, s. 352.

[305] **KARAGÜLMEZ**, s. 232.

[306] **AKDAĞ**, s. 135.

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

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

değil veri sahibi kişinin korunmasıdır. Dolayısıyla kişisel verinin öğrenildiği durumlarda da suçun işlendiğinin kabulü gerekir.[308] Bilişim alanındaki suçlarda korunan verinin veya

istenildiğinde tekrar kullanılabilmesi olanağını sağlayan her türlü faaliyet, kişisel verileri "ele geçirme" kapsamında değerlendirilebileceği gibi, kişisel verilerin kaydedilmeden önce öğrenilmesi, kişisel verilere salt duyu organları aracılığıyla vakıf olunması da aynı kapsamda değerlendirilmelidir.

Bu açıklamalar ışığında incelenen dosya kapsamına ve ikrar içeren savunmaya göre; katılan ile bir dönem duygusal birliktelik yaşayan sanığın, katılanın hazırlandığı sırada katılanın rızası dışında cep telefonunu alarak arama kayıtlarına baktığı iddiasına konu olayda; TCK'nın 132/1. madde ve fıkrasındaki suçun konusunun, haberleşme içeriği olup söz konusu suçun, belirli kişiler arasındaki haberleşme içeriğinin hukuka aykırı biçimde öğrenilmesiyle oluşacağı, haberleşmenin gizliliğinden söz edebilmek için, kişiler arasında haberleşme olarak isimlendirilebilecek bir iletişimin olması, en az iki kişi arasında bir haberleşme vasıtası olması (telefon, mektup, e-posta vb.) ve tarafların bu haberleşmeyi gizlilik önlemlerini alarak yapması gerektiği, katılanın, kim ile, ne zaman, hangi sıklıkla, hangi süreyle görüştüğüne ilişkin bilgiler kişisel veri kapsamında olup haberleşme olarak nitelendirilemeyeceği anlaşıldığından, katılana ait kişisel veri kapsamındaki arama kayıtlarına katılanın rızası dışında bakarak içeriğine vakıf olan sanık hakkında TCK'nın 136/1. madde ve fıkrasındaki verileri hukuka aykırı olarak verme veya ele geçirme suçundan mahkumiyet kararı verilmesi gerektiği gözetilmeden, delillerin takdirinde ve hukuki nitelendirmede yanılgıya düşülerek yazılı şekilde haberleşmenin gizliliğini ihlal suçundan beraat hükmü kurulması," Yargıtay 12. Ceza Dairesi 2018/8152 E., 2019/4886 K. Sayılı, 10.04.2019 tarihli kararı. https://www.kazanci.com.tr/ (Erişim tarihi : 24.05.2020)

[308] **AKDAĞ**, s. 136. Aksi yönde görüş için bkz. **DÜLGER**, Kişisel Veriler, s. 353.

bilişim sisteminin güvenliği iken kişisel verilere yönelik suçlarda kişisel verilerin korunması hakkıdır.

"Kişisel verileri hukuka aykırı olarak ele geçirme, bir başkasına verme ve yayma suçu" sırf hareket suçudur. Seçimlik hareketlerden birinin gerçekleşmesiyle suç tamamlanmış olur.[309]

Öngörülen seçimlik hareketler icrai hareketlerdir,[310] suç ihmali hareketle işlenemez.[311]

Suç aynı zamanda bir soyut tehlike suçudur. Suçun gerçekleşmesi için bir zararın meydana gelmesi yahut somut bir tehlikenin varlığı aranmaz.[312]

b. Manevi Unsur

Suç, kasten işlenebilir. Failin mağdurun kişisel verilerini hukuka aykırı olarak ele geçirdiğini, bir başkasına verdiğini veya yaydığını bilmesi ve istemesi gerekir.[313] Suçun oluşması bakından failin belli bir amaçla hareket etmesi aranmamıştır.[314]

---

[309] **ÖZBEK – DOĞAN – BACAKSIZ – TEPE**, s. 578.

[310] **KANGAL**, s. 97.

[311] **HAFIZOĞULLARI – ÖZEN**, Kişilere Karşı Suçlar, s. 291.

[312] **ÖZBEK – DOĞAN – BACAKSIZ – TEPE**, s. 579. **YAŞAR – GÖKCAN – ARTUÇ**, s. 4433; **ARTUÇ**, s. 1626.

[313] **HAFIZOĞULLARI – ÖZEN**, Kişilere Karşı Suçlar, s. 291.

[314] **KANGAL**, s. 120; *"Oluşa ve dosya kapsamına göre; sanık ... ile katılan mağdur ...'ın bir müddet aynı kargo firmasına ait iş yerinde birlikte çalışmalarından dolayı birbirlerini tanıdıkları, sanığın iş yerinden ayrıldığı dönemde, profil resmi olarak sanığın resminin kullanıldığı ... adlı facebook hesabından, mağdurun facebook hesabına, "Selam Sultan*

c. Hukuka Aykırılık

Bu suç tipinde de TCK m. 135'teki gibi "hukuka aykırılık" ibaresine ayrıca yer verilmiştir. Hukuka özel aykırılık halinde suçun ancak doğrudan kastla işlenebileceğine

---

Hanım, nasılsınız?" ve "İnsan bu kadar güzel olunca cevap vermiyor, haklısın da." şeklinde 16.09.2013 tarihli iki mesaj gönderilmesini müteakip, mağdurun, iş yeri sahibi olan tanık Beşir'den sanığı telefonla arayıp, olayla ilgisinin bulunup bulunmadığını öğrenmesini istediği, mağdurun talebi doğrultusunda, 17.09.2013 günü saat 10.00 sularında, sanığı telefonla arayan tanık Beşir'in konuyu sanığa ilettiği ve sanığın ... adlı facebook hesabı ile bir ilgisinin bulunmadığını ifade ettiği; ancak, bu telefon görüşmesinden yaklaşık 2 saat sonra, ... adlı facebook hesabındaki sanığa ait profil resminin kaldırılıp, profile manzara resmi konulduğu ve aynı gün saat 13.00 sularında, mağdurun iş yerine giderek, onunla tartışan sanığın, ... adlı facebook hesabının sahibi olmadığını ve facebook adlı sosyal paylaşım sitesinde başkalarına ait resimlerle rahatlıkla sahte hesaplar açılabileceğini mağdura ispatlama saikiyle ve onun rızası olmaksızın mağdurun facebook profilindeki resmini kullanarak "Nesrin Hülya E." adıyla yeni bir facebook hesabı açtığı olayda,

Mağdurun kişisel veri niteliğindeki resmini, hukuka uygunluk nedenlerinin bulunmaması sebebiyle hukuka aykırı olduğunda tereddüt bulunmayan bir yöntemle "Nesrin Hülya E." adlı facebook hesabı üzerinden başkalarının görgüsüne sunan sanık hakkında, ***genel kastla işlenen verileri hukuka aykırı olarak verme veya ele geçirme suçundan dolayı mahkumiyet kararı verilmesine dair yerel mahkemenin kabulünde bir isabetsizlik görülmemiştir.****"* Yargıtay 12. Ceza Dairesi 2015/13248 E., 2017/3108 K. Sayılı, 12.04.2017 tarihli kararı https://www.kazanci.com.tr/ (Erişim tarihi : 24.05.2020)

ve failin cezalandırılabilmesi için gerçekleştirdiği fiilin hukuka aykırı olduğunu da ayrıca bilmesi gerektiğine ilişkin açıklamalar bu suç için de geçerlidir.

İlgilinin rızasının bulunması[315], kanun hükmünün yerine getirilmesi, hakkın kullanılması hallerinde fiil hukuka uygundur ve dolayısıyla suç oluşmaz.[316]

Ayrıca belirtmek gerekir ki suçun uygulama alanının amaçlananın ötesinde genişlememesi için uygulamada belirsizliğe neden olmaması ve hemen her olayın suç teşkil etmemesi için somut olay özelinde değerlendirme yapılarak hukuka uygunluk nedeni olup olmadığı belirlenmelidir.

Yargıtay da bir kararında bu hususu vurgulayarak *"Soruşturma evresinde katılana ait cep telefonu numarasını kimseye vermediğini ifade eden sanık ...'in, kovuşturma evresinde, arkadaşı N.'ın köyde borcu olanların telefon numaralarını istemesi nedeniyle katılana ait cep telefonu numarasını arkadaşına verdiğine dair ilk ifadesiyle çelişen tutarsız savunmalarına itibar edilemeyeceği ve* ***arkadaşı olan N.'ın da evini ve adresini bildiği katılanla doğrudan iletişim kurmak yerine*** *2012 yılından beri tahsil etmediği 90,00 TL'lik borcun ödenmesi için* ***katılanı iki yıl sonra aynı gün birden fazla defa telefonla aramasının hayatın olağan akışına uygun düşmediği*** *gözetildiğinde, sanık ...'in,* ***katılana ait GSM numarasını arkadaşına vermesini gerektiren makul, meşru ve mantıklı bir sebep bulunmaması nedeniyle katılanın rızası dışında hareket ettiğinin açıkça anlaşılması*** *karşısında,*

Sanık ...'in, kişisel veri niteliğindeki katılana ait cep telefonu numarasını kaydedilmiş haliyle ve hukuka uygunluk nedenlerinin bulunmaması nedeniyle hukuka

---

[315] Suç şikayete tabi olmadığından ilgilinin rızasının bu suç açısından hukuka uygunluk nedeni olmayacağına dair görüş için bkz.; **ÖZBEK – DOĞAN – BACAKSIZ – TEPE**, s. 580.

[316] **KANGAL**, s. 123-131;

aykırı olduğunda tereddüt bulunmayan bir yöntemle arkadaşına vermesi şeklinde sübut bulan eyleminden dolayı TCK'nın 136/1. madde ve fıkrasında tanımlanan verileri hukuka aykırı olarak verme veya ele geçirme suçundan mahkumiyetine karar verilmesi gerekirken, "... sanığın katılana ait cep telefonunu ... verme şeklinde gerçekleşen ve sabit olan eylemin, cep telefonu numarasının kolaylıkla ulaşılabilmesi ve bilinmesi mümkün olan kişisel veri niteliğinde olduğu değerlendirilerek maddede belirtilen suçun yasal unsurlarının oluşmadığı..." biçimindeki yasal ve yeterli olmayan gerekçelerle sanık hakkında CMK'nın 223/2-e madde, fıkra ve bendi gereğince beraat hükmü kurulmasını" bozma sebebi yapmıştır.[317]

Özellikle "verme" seçimlik hareketinin cezalandırılması açısından hukuka özel aykırılık araştırmasının sağlıklı yapılması özellikle önem arz etmektedir. Nitekim suçun soyut tehlike suçu olarak düzenlenmiş olmasının doğurduğu, öngörülebilir olamayan ve hiçbir meşru menfaati zarara uğratmayan ya da tehlikeye sokmayan davranışların cezalandırılması tehdidini oluşturmakta ve uygulamada bu durumun önüne bu tarz kararlar ile geçilmeye çalışılmaktadır.[318]

---

[317] Yargıtay 12. Ceza Dairesi 2018/8466 E., 2019/9054 K. Sayılı ve 18.09.2019 tarihli kararı. https://www.kazanci.com.tr/ (Erişim tarihi : 24.05.2020)

[318] **TANER**, Fahri Gökçen; TBB Eğitim Merkezi Kişisel Verilerin Ceza Hukuku ve KVKK Kapsamında Korunması Online Eğitimi, sunum slaytı; https://www.academia.edu/43057536/TCK_da_Ki%C5%9Fisel_Verilerin_Korunmas%C4%B1_TBB_TV_SLAYT_15_05_2020_ video kaydı; http://www.tbbegitim.com/Video/VideoGaleri?egitimId=3401 (Erişim Tarihi: 30.07.2020)

6. Suçun Özel Görünüş Şekilleri

a. Teşebbüs

Suç, "sırf hareket suçu" olduğundan kural olarak teşebbüse elverişli değildir. Hareketin parçalara ayrılabildiği hallerde[319] teşebbüs söz konusu olabilir ancak suçun oluşması için netice aranmadığından teşebbüs aşamasında kaldığına pek rastlanmaz.[320]

b. İştirak

Suç, iştirak açısından bir özellik taşımamaktadır.[321] Ancak iştirak edenlerin "kamu görevlisi olması" veya "belli bir meslek ve sanatın sağladığı kolaylıktan yararlanması" durumunda cezaları TCK m. 137 gereğince artırılarak verilir.[322]

---

[319] Örneğin; failin kişisel verilerin tutulduğu kilitli dolabı açması yahut kişisel verilerin tutulduğu sisteme girmesi ancak henüz verilere ulaşamamış olması. **AKDAĞ**, s. 139. Yazarın isabetle belirttiği üzere böyle bir durumda fail sisteme girdikten sonra, kişisel verileri ele geçirmekten kendi iradesiyle vazgeçerse gönüllü vazgeçme söz konusu olur ve bu durumda fail bilişim sistemine girme suçunu işlemiş olur.

[320] **DÜLGER**, Kişisel Veriler, s. 356.

[321] **ÖZBEK – DOĞAN – BACAKSIZ – TEPE**, s. 580.

[322] **DÜLGER**, Kişisel Veriler, s. 356.

c. İçtima

Suç, zincirleme suç olarak işlenebilir. Suçun, "aynı suç işleme kararının icrası kapsamında aynı kişiye karşı birden fazla kez" veya "tek hareketle birden fazla kişiye karşı" işlenmesi halinde zincirleme suç oluşur. Ancak aynı kişiye ait kişisel verilerin aynı anda bir başkasına verilmesi ve yayılması gibi kanunda öngörülen seçimlik hareketlerin tek fiille gerçekleştirilmesi halinde tek suç oluşur.[323]

Ayrıca kişisel verilerin hukuka aykırı olarak kaydedilmesi suçunda bahsedildiği gibi kişisel veriyi hukuka aykırı olarak kaydetmek ile başkasına vermek veya yaymak fiilleri aynı anda gerçekleştirilebilir. Bu durumda TCK m. 135 ve TCK m. 136'da düzenlenen bu iki suç da işlenmiş olur ve fikri içtima uygulanır.[324]

Kişisel veri niteliğinde olmayan kişinin özel hayatına ilişkin verilerin suça konu olması halinde özel hayatın gizliliğini ihlal suçu oluşur.[325]

---

[323] **YAŞAR – GÖKCAN – ARTUÇ**, s. 4449.

[324] **ÖZBEK – DOĞAN – BACAKSIZ – TEPE**, s. 580.

[325] Yargıtay 4. Ceza Dairesinin 2011/10616 E., 2013/7641 K. Sayılı, 18.03.2013 tarihli kararında *"Sanığın, cinsel ilişkilerine ilişkin video görüntülerini mağdurenin rızası olmadan tanıklara izlettirme biçimindeki eyleminin TCK'nın 134/2 maddesine uyan, özel hayatın gizliliğini ihlal suçunu oluşturduğu gözetilmeden, olayda uygulama yeri bulunmayan aynı Kanunun 136. maddesi uyarınca hüküm kurulması"*; **YAŞAR – GÖKCAN – ARTUÇ**, s. 4442.

7. Suçun Nitelikli Halleri

TCK m. 136'nın ikinci fıkrasında *"Suçun konusunun, Ceza Muhakemesi Kanununun 236 ncı maddesinin beşinci ve altıncı fıkraları uyarınca kayda alınan beyan ve görüntüler olması durumunda verilecek ceza bir kat artırılır."* denilmektedir.[326] Bu fıkra ile "cinsel istismar suçu mağduru çocuğun veya vücuda organ veya sair bir cisim sokulması suretiyle cinsel saldırı suçunun mağduru olanların ifadesine ilişkin beyan ve görüntülerin suça konu olması" hali cezayı ağırlaştıran neden olarak öngörülmüştür.

TCK m. 137'de düzenlenen "kamu görevlisi olması veya belli bir meslek ve sanatın sağladığı kolaylıktan yararlanılarak işlenmesi" haline ilişkin artırım hem 135. maddede düzenlenen "kişisel verilerin kaydedilmesi" hem de 136. maddede düzenlenen

---

[326] *Mağdur ile şikâyetçinin dinlenmesi – Madde 236*

... (5) Türk Ceza Kanununun 103 üncü maddesinin ikinci fıkrasında düzenlenen suçlardan mağdur olan çocukların soruşturma evresindeki beyanları, bunlara yönelik hizmet veren merkezlerde Cumhuriyet savcısının nezaretinde uzmanlar aracılığıyla alınır. Mağdur çocuğun beyan ve görüntüleri kayda alınır. Kovuşturma evresinde ise ancak, maddi gerçeğin ortaya çıkarılması açısından mağdur çocuğun beyanının alınması veya başkaca bir işlem yapılmasında zorunluluk bulunması hâlinde bu işlem, mahkeme veya görevlendireceği naip hâkim tarafından bu merkezlerde uzmanlar aracılığıyla yerine getirilir. Mağdur çocuk yargı çevresi ve mülkî sınırlara bakılmaksızın en yakın merkeze götürülmek suretiyle bu fıkrada belirtilen işlemler yerine getirilir.

(6) Türk Ceza Kanununun 102 nci maddesinin ikinci fıkrasında düzenlenen suçlardan mağdur olanların soruşturma evresindeki beyanları bakımından da beşinci fıkra hükmü uygulanır. Ancak, beyan ve görüntülerin kayda alınmasında mağdurun rızası aranır.

"verileri hukuka aykırı olarak verme veya ele geçirme" suçları için ortak nitelikli hal olup TCK m. 135 incelenirken yaptığımız açıklamalar bu suç için de geçerlidir.

8. Yaptırım

Suçun temel halinde ceza "2 yıldan 4 yıla kadar hapis cezası" olarak belirtilmiştir. Madde yaptırım bakımından 2 kez değişikliğe uğramıştır. İlk olarak maddenin ilk fıkrasında öngörülen cezanın altı sınırı 1 yıldan 2 yıla çıkarılmış[327] daha sonra ise 17/10/2019 tarihinde eklenen ikinci fıkrası ile suçun konusunun, "Ceza Muhakemesi Kanununun 236'ncı maddesinin beşinci ve altıncı fıkraları uyarınca kayda alınan beyan ve görüntüler" olması cezada artırım sebebi olarak öngörülmüştür.

Bu suçta da TCK m. 137'de düzenlenen nitelikli hallerin işlenmesi durumunda verilecek ceza yarı oranında artırılır. Ayrıca TCK m.140 uyarınca tüzel kişiler hakkında güvenlik tedbirlerine hükmolunabilecektir.

9. Soruşturma ve Kovuşturma

TCK m. 139 gereğince suç, re'sen soruşturulur ve kovuşturulur. Öngörülen cezanın üst sınırına göre görevli mahkeme asliye ceza mahkemesidir. [328]

[327] 21/2/2014 tarihli ve 6526 sayılı kanunun 4 üncü maddesiyle bu fıkrada yer alan "bir yıldan" ibaresi "iki yıldan" şeklinde değiştirilmiştir.

[328] **ÖZBEK – DOĞAN – BACAKSIZ – TEPE**, s. 581.

Suçun kamu görevlisi tarafından görevi sebebiyle işlenmesi halinde soruşturma yapılması izne tabi olacağından yetkili merciden izin alındıktan sonra soruşturma yapılması gerekir.[329]

D. VERİLERİ YOK ETMEME SUÇU(TCK m. 138)

1. Genel Olarak

Kişisel verilerin veri sahibi ilgili kişiler tarafından bir kısım kişi, kurum veya kuruluşlara verilmesi zorunluluk arz edebilir. Bu verilerin sahiplerinin rızası ile verilmesi ve hukuka uygun olarak toplanması, onların süresiz olarak tutulabileceği anlamını taşımaz.[330] Kişisel verilerin hukuka uygun olarak elde edilmesi kadar kişisel verilere olan ihtiyaç sona erdiğinde ve nihayet en geç kanunlarda öngörülen sürelerin sonunda yok edilmeleri de elzemdir.

Kişisel verilerin süresiz olarak tutulmaması amaçla bağlılık ilkesi ile ilişkilidir.[331] Bu kapsamda kişisel verilerin saklanma süreleri kullanılma amaçları ile bağlantılı olarak kısıtlanmıştır.[332]

TCK m. 138'de "kanunlarda belirlenen sürelerin geçmiş olmasına rağmen verilerin sistem içinde yok edilmemesi" halinde görevini yerine getirmeyen failin "bir

---

[329] **ARTUÇ**, s. 1635.

[330] **DÜLGER**, Bilişim Suçları, s. 281; **KORKMAZ**, s. 422.

[331] **KUŞKONMAZ**, Elif Mendos; Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku A.B.D. Yayımlanmamış Yüksek Lisans Tezi, İstanbul 2013, s. 161.

[332] **HAFIZOĞULLARI – ÖZEN**, Kişilere Karşı Suçlar, s. 291.

yıldan iki yıla kadar hapis cezası" ile cezalandırılacağı hüküm altına alınmıştır. İkinci fıkrada *"Suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması hâlinde verilecek ceza bir kat artırılır."* denilmektedir.

Madde başlığında 136. Maddede de olduğu gibi *"kişisel verileri yok etmeme"* denilmek yerine *"verileri yok etmeme"* denilmiştir. Ancak bu suç tipinde madde metninde de kişisel veri denilmek yerine *"Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde"* denilmiştir. TCK m. 136 incelenirken ifade edildiği üzere farklı kavramlar olmaları nedeni maksadın kişisel verilerin korunması olduğu anlaşılmasına rağmen madde başlığının ve içeriğinin *"verileri yok etmeme"* denilmesi uygun olmamıştır.

KVKK'nın "Suçlar" başlıklı 17. Maddesi ikinci fıkrasında *"Bu Kanunun 7 nci maddesi hükmüne aykırı olarak; kişisel verileri silmeyen veya anonim hâle getirmeyenler 5237 sayılı Kanunun 138 inci maddesine göre cezalandırılır."* Denilmektedir.

Aynı Kanunun 7. Maddesi ilk fıkrasına göre ise *"Bu Kanun veya 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."*

Çalışmanın birinci bölümünde "Kişisel Verilerin İşlenmesi" başlığı altında incelenen kavramlardan olan "silme", "yok etme" ve "anonim hale getirmenin" faklı kavramlar olduğu ifade edilmiştir. Kısaca hatırlatmak gerekirse; Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in 4. Maddesinde "kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi" süreçlerinin tümü *"imha"* olarak tanımlanmıştır.

Aynı yönetmeliğin 8. Maddesinde *"silme"; "kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemi"*, 9. Maddesinde *"yok etme"; "kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemi",* 10. Maddesinde ise *"anonim hale getirme"; "kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi"* olarak tanımlanmıştır.

TCK m. 138'de yer alan *"yok etme"* kavramı yorumlanırken KVKK mevzuatında bahsedilen ve üst kavram olarak *"imha"* şeklinde adlandırılan silme, yok etme ve anonim hale getirme işlemlerinin tümü algılanmalıdır.

Ancak KVVK m. 17'de "kişisel verileri silmeyen veya anonim hâle getirmeyenlerin" TCK m. 138 uyarınca cezalandırılacağı düzenlenmiş olup doktrinde bu maddede verileri yok etmenin yazılmamış olması eksiklik olarak değerlendirilmiştir.[333] TCK m. 138'de yalnızca yok etmeden bahsedildiğinden KVKK m. 17 ile silme veya anonim hale getirmeye ilişkin eksikliğin giderilmeye çalışıldığı anlaşılmaktadır.

2. Hukuki Konu

Bu suçla korunan hukuki değer bir görüşe göre özel hayatın gizliliği yanında kamu idaresine karşı duyulan güvendir.[334] Bu görüşe göre suçla, kamu görevinin yerine getirilmesinden beklenen kamusal yararın elde edilmesi hedeflenmektedir.[335] Ancak

[333] **KORKMAZ**, s. 424.

[334] **DÜLGER**, Kişisel Veriler, s. 360; **SOYASLAN**, s. 364; **KARAGÜLMEZ**, s. 468.

[335] **DÜLGER**, Kişisel Veriler, s. 360.

kişisel verileri yok etme yükümlülüğü sadece kamu görevlileri için öngörülmediğinden bu görüşe katılmak mümkün değildir. Katıldığımız diğer görüşe göre ise suçla korunan hukuki değer özel hayatın gizliliği hakkı[336] kapsamında kişisel verilerin korunması hakkıdır.

Kişisel verilerin silinmesini isteme unutulma hakkının görünüm biçimlerinden biridir ve Anayasa'nın 20. Maddesinde koruma altına alınmıştır.[337] Kişisel verilerin silinmesini talep etme hakkı kişisel verilerin tutulmasında veri minimizasyonu ilkesine ve verilerin gereğinden fazla tutulmaması ilkesine dayanmaktadır. Veri minimizasyonu (diğer adıyla verilerin asgarileştirilmesi) ilkesi kişisel verilerin işleme amacının gerektirdiği ölçüde toplanmasını ifade eder ve bu nedenle de işleme amacı sona erdiğinde verilerin imha edilmesi yükümlülüğü doğar.[338]

[336] **HAFIZOĞULLARI – ÖZEN**, Kişilere Karşı Suçlar, s. 292; **ÖZBEK – DOĞAN – BACAKSIZ – TEPE**, s. 582; **YAŞAR – GÖKCAN – ARTUÇ**, s. 4461.

[337] **KANGAL**, s. 155.

[338] **SÖZÜER**, Eren; Unutulma Hakkı, İnsan Hakları Hukuku Perspektifinden Bir İnceleme, İstanbul 2017, s. 37; **ÇIRAK**, Ezgi; *"Dijital Çağda Sonsuza Kadar Hatırlanmaya Karşı: Unutulma Hakkı",* CHD, Y. 2014, S. 36, s. 163, 164; **KANGAL**, s. 155.

3. Fail

Madde metninde *"verileri sistem içinde yok etmekle yükümlü olanlar"* denildiğinden suçun faili herkes olamaz ve sadece kişisel verileri korundukları sistemde yok etmekle yükümlü olan kimse fail olabileceğinden suç, özgü suçtur. [339]

Mahiyeti gereğince suç daha çok kamu görevlileri tarafından işlenmekte ise de kamu görevlisi olmak bu suçun oluşumuna ya da cezanın ağırlaştırılmasına etkili değildir.[340]

Burada dikkat edilecek husus, kendi tabi olduğu sair mevzuat veya KVKK hükümleri uyarınca kişisel verilerin yok edilmesinin failin görev alanına girip girmediğidir.[341] KVKK m. 7[342] uyarınca "kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi" işlemi veri sorumlusu tarafından yerine getirilir. Yine "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında

---

[339] **HAFIZOĞULLARI – ÖZEN**, Kişilere Karşı Suçlar, s. 292; **ÖZBEK – DOĞAN – BACAKSIZ – TEPE**, s. 582; **YAŞAR – GÖKCAN – ARTUÇ**, s. 4461.

[340] **HAFIZOĞULLARI – ÖZEN**, Kişilere Karşı Suçlar, s. 292.

[341] **KANGAL**, s. 158.

[342] KVKK m. 7/1: *"Bu Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir.*

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

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

Yönetmeliğin" 7. Maddesine göre de bu görev veri sorumlusuna aittir. Yönetmeliğin anılan maddesinin dördüncü fıkrası uyarınca ise *"veri sorumlusu, kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi işlemiyle ilgili uyguladığı yöntemleri ilgili politika ve prosedürlerinde açıklamakla yükümlüdür."*

Hatırlatmak gerekirse KVKK m. 3/1-ı uyarınca veri sorumlusu *"Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişidir."* Ancak tüzel kişiler fail olamayacağından "tüzel kişinin veri kayıt sisteminden sorumlu olan gerçek kişiyi" sorumlu tutmak gerekecektir.[343] Ancak uygulamada iş kazaları nedeniyle yapılan ceza yargılamalarında da görüldüğü gibi gerekli ve yeterli araştırma yapılmadan tüzel kişiliğin tüm yönetim kurulu üyeleri ve/veya üst düzey yöneticileri hakkında dava açılmaktadır.[344] İş hukukunda bu durumun önleyicisi olarak iş güvenliği uzmanı atanması söz konusu olup KVKK anlamında da tüzel kişi veri sorumlularının organizasyon şemalarında bir veri sorumlusu gerçek kişi ataması, sorumlu kişinin belirlenmiş olması nedeniyle cezai müeyyideden sorumlu olacakları netleştirmiş olacaktır.

4. Mağdur

Suçun mağduru herkes olabilir; öngörülen sürelerin geçmesine rağmen kişisel verileri ceza hukukunda deyimi ile yok edilmeyen herkes suçun mağduru sayılır.[345]

---

[343] **KANGAL**, s. 158.

[344] **DÜLGER**, Kişisel Veriler, s. 362.

[345] **ÖZBEK– DOĞAN – BACAKSIZ – TEPE**, s. 582; **HAFIZOĞULLARI – ÖZEN**, Kişilere Karşı Suçlar, s. 292; **YAŞAR – GÖKCAN – ARTUÇ**, s. 4461.

5. Suçun Unsurları

a. Maddi Unsur

Suç ihmali hareketle işlenebilir. Kişisel verilerin sistemde yok edilmesi gerekirken kanunun öngördüğü süre içinde yok edilmemesi halinde suç oluşur.[346] Yok etme süresi genellikle kanunlarda gün, hafta, ay, yıl olarak net şekilde belirtilir ancak mevzuatta süre belirtilmeyip "derhal" gibi ibarelerin geçmesi halinde somut olaya göre makul sürede yok etme fiilinin gerçekleştirilmesi beklenir. Ancak böyle bir durumda makul süre ay, yıl olarak yorumlanamaz.[347]

Yukarıda bahsedildiği üzere Türk Ceza Kanunu'nda yer alan "yok etme" deyiminden teknik anlamda KVKK'da tanımlanan "yok etme", "silme" ve "anonim hale getirme" işlemlerinin tümü anlaşılmalıdır.

Madde metninde geçen kanunlarda öngörülen süre deyiminden şekli anlamda kanun anlaşılmaması gerekir, idarenin düzenleyici işlemleriyle süre öngörülmüş olması halinde de yok etme yükümlülüğü vardır.[348] Nitekim imhaya ilişkin süreler şekli anlamda kanunlarda düzenlenmemiş olabilir hatta çoğunlukla yönetmeliklerle veya idarenin diğer düzenleyici işlemleriyle öngörülür.

---

[346] **HAFIZOĞULLARI – ÖZEN**, Kişilere Karşı Suçlar, s. 292; **ÖZBEK– DOĞAN – BACAKSIZ – TEPE**, s. 582.

[347] **YAŞAR – GÖKCAN – ARTUÇ**, s. 4464.

[348] **AKDAĞ**, s. 146.

d. Manevi Unsur

Suç kasten işlenebilen bir suçtur. Failin kastı; kanunun kendisine yüklediği yok etme yükümlülüğünü bilerek ve isteyerek ihmal etmesidir. Failin yok etmeye dair sürelerin hesabında hataya düşmesi halinde (fiili hata) kastı ortadan kalkar. [349]

e. Hukuka Aykırılık

Her suçta olduğu gibi bu suçta da fiil hukuka aykırı olmalıdır.[350] Mağdurun rızası fiili hukuka uygun hale getirmez.[351] Ancak uygulanması gereken başka bir kanun hükmü bulunması halinde (örneğin verileri yok etmekle görevli olan fail başka bir kanun hükme nedeniyle yok etme işlemini gerçekleştirmezse) fiilin hukuka uygun olacağından suç oluşmaz.[352]

[349] **HAFIZOĞULLARI – ÖZEN**, Kişilere Karşı Suçlar, s. 293;

[350] **KORKMAZ**, s. 434.

[351] **HAFIZOĞULLARI – ÖZEN**, Kişilere Karşı Suçlar, s. 292.

[352] **ÇOKMUTLU**, s. 249; **KORKMAZ**, s. 435.

6. Suçun Özel Görünüş Şekilleri

a. Teşebbüs

Kanunda öngörülen sürelerin geçmesine rağmen yok edilmesi gereken kişisel verilerin yok edilmemesi ile suç tamamlanmış olur, bu nedenle suçun teşebbüse elverişli değildir.[353]

b. İştirak

Suç, "özgü suç" olduğundan kişisel verileri yok etme yükümlülüğü olmayan kimselerin suça iştirak etmesi mümkün değildir.[354]

c. İçtima

Bu suç da zincirleme olarak işlenebilir.[355] Ancak aynı kişisel verilerin uzun zaman silinmemesi halinde durumunda tek suç oluşacaktır.[356]

---

[353] **YAŞAR – GÖKCAN – ARTUÇ**, s. 4461.

[354] **YAŞAR – GÖKCAN – ARTUÇ**, s. 4464.

[355] **ÖZBEK– DOĞAN – BACAKSIZ – TEPE**, s. 585.

[356] **YAŞAR – GÖKCAN – ARTUÇ**, s. 4466.

7. Suçun Nitelikli Halleri

Maddenin 21.02.2014 tarihinde eklenen ikinci fıkrasına göre; *"Suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması hâlinde verilecek ceza bir kat artırılır."*

Örneğin; "iletişimin tespiti, dinlenmesi ve kayda alınması" ile ilgili olarak CMK m. 137/3 uyarınca *"135 inci maddeye göre verilen kararın uygulanması sırasında şüpheli hakkında kovuşturmaya yer olmadığına dair karar verilmesi ya da aynı maddenin birinci fıkrasına göre hâkim onayının alınamaması halinde, bunun uygulanmasına Cumhuriyet savcısı tarafından derhâl son verilir. Bu durumda, yapılan tespit veya dinlemeye ilişkin kayıtlar Cumhuriyet savcısının denetimi altında en geç on gün içinde yok edilerek, durum bir tutanakla tespit edilir."* Denilmekte olup öngörülen sürede kayıtların yok edilmemesi halinde nitelikli hal gerçekleşmiş olur.[357]

8. Yaptırım

Suçun cezası "bir yıldan iki yıla kadar hapis cezası" olarak öngörülmüştür. Esasen maddenin ilk halinde *"altı aydan bir yıla kadar"* olan düzenleme 21.02.2014 tarihli ve 6526 sayılı Kanunun 5. Maddesi ile değiştirilerek suçun cezası artırılmıştır.[358]

[357] **DÜLGER**, Kişisel Veriler, s. 366, 367.

[358] **YAŞAR – GÖKCAN – ARTUÇ**, s. 4466.

9. Soruşturma ve Kovuşturma

TCK m. 139 uyarınca suç, re'sen soruşturulur ve kovuşturulur. Öngörülen cezanın üst sınırına göre görevli mahkeme asliye ceza mahkemesidir. [359]

[359] **ÖZBEK – DOĞAN – BACAKSIZ – TEPE**, s. 585.

SONUÇ

"Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi" şeklindeki geniş çerçeveli tanımından da anlaşılabileceği üzere kişisel veriler; hayatımızın her alanında görsel ve işitsel her türlü algımız dahiline giren geniş bir yelpazede ad, soyad, görüntü, ses gibi en temel bilgilerden fiziksel, kültürel, sosyal veya psikolojik kimliği ortaya koyan her türlü bilgiye kadar uzanan bir alana sahiptir.

Günümüzde sosyal ilişki ve gereksinimlerin artması, teknolojinin ilerlemesi gibi sebeplerle hem kişisel verilerle temas çoğalmış hem de verilerin dolaşımı kontrol edilemez boyutlara varmıştır. Bu durum kişisel verilerin korunmasına dair artan ihtiyacı da gözler önüne sermiştir. KVKK ile kişisel verilerin korunması anlamında büyük adımlar atılırken, ceza hukuku anlamında da kişisel verilerin korunmasına dair cezai düzenlemelerin yorumunu etkileyecek gelişmeler olmuştur.

TCK'da kişisel verilerin korunmasına dair hükümlerin özel hayatın gizliliğinden ayrı ve ayrıntılı olarak düzenlenmesi son derece isabetli olmuşsa da kavram karışıklıkları uygulamada çoğu zaman güçlüğe neden olmuştur. KVKK'nın yürürlüğe girmesinden sonra kişisel verilerin teorik ve pratik anlamda daha geniş ve ayrıntılı çalışmalara konu olması, ceza hukuku anlamında da kişisel verileri koruyan kanun maddelerin yorumlanmasında faydalı olmuştur. Ancak yine de TCK'da yer alan düzenlemeler kişisel verileri korumada yetersiz kalmış, KVKK ile TCK arasında kavram birliği bulunmaması uygulamada güçlüklere neden olmuştur. KVKK ile kavram kargaşasının bir nebze önüne geçilmişse de TCK'da yer alan hükümlerin de gelişen ve değişen ihtiyaçlar gözetilerek daha kapsayıcı şekilde revizesi gerekmektedir.

Bu doğrultuda gerek TCK'nın ve hatta Anayasanın ilgili maddesinin yeniden gözden geçirilmesi ve kanunilik ilkesi de dikkate alınarak kavram tartışmalarına yer bırakmayacak şekilde birbiriyle uyumlu hale getirilmesi gerekmektedir.[360]

TCK m. 135 ile kişisel verilerin hukuka aykırı olarak kaydedilmesi yaptırıma bağlanmıştır. Esas olan kişisel verilerin kayıt altına alınmaması ve mahremiyeti olup kanun koyucu kişisel verilerin kaydedilmesinin cezalandırılması için verilerin hukuka aykırı kaydedilmesini şart koşmuştur. TCK'nın 135. Maddesi, kişisel verilerle temasın çoğunlukla kayıt ile başlaması nedeni ile büyük önem arz etmektedir. Yasal düzenleme ile kişisel verilerin kaydedilmesi cezalandırılırken, ikinci fıkra ile bazı hassas nitelikli verilerin kaydedilmesi halinde cezada artırım yapılacağı hüküm altına alınmıştır. Ancak; bu fıkrada sayılan "özel nitelikli (hassas) veriler" ile KVKK anlamında hassas veriler birbiri ile örtüşmemektedir. Bu anlamda TCK'da sayılan özel nitelikli verilerin, KVKK'da sayılan şekle uygun hale getirilmesi daha isabetli olacaktır.

136. maddede ise kişisel verilerin hukuka aykırı olarak bir başkasına verilmesi, yayılması veya ele geçirilmesi yaptırıma bağlanmıştır. Bu maddede yer alan seçimlik hareketlerden *"ele geçirme"* çoğunlukla 135. maddede düzenlenen *"kaydetme"* den önce gerçekleşmekte olup bazense tam tersi şekilde ortaya çıkmaktadır. Hukuka uygun olarak kaydedilmiş bulunan kişisel verilerin hukuka aykırı olarak ele geçirilmesi (veya başkasına verilmesi yahut yayılması) halinde 136. maddede düzenlenen (veya hukuka uygun olarak kaydedilmiş olan bu veriler ele geçirildikten sonra yeniden ve bu defa hukuka aykırı olarak kaydediliyorsa ayrıca 135. maddede öngörülen) suç tipi oluşuyorken hukuka aykırı olarak kaydedilen kişisel verilerin yine hukuka aykırı olarak başkasına verilmesi veya

[360] **ERDOĞAN**, Yavuz; *"Kişisel Verilerin Korunması Bakımından Türk Ceza Kanunu Hükümlerinin Değerlendirilmesi"* ERÜHFD Y. 2013, S. 2, s. 627, 628.

yayılması halinde ise her iki suç da oluşur. Bu gibi durumlar hem içtima ve teşebbüs hükümlerinin uygulanmasına karışıklığa ve tartışmalara neden olmakta hem de "ele geçirme" ile "kaydetme" kavramlarının karışmasına yol açmaktadır. Kaydetmenin şekli açısından kağıda kaydetme halinde suçun oluşup oluşmadığı, ele geçirmede ise yalnızca hafızada tutmanın ele geçirmenin suça vücut verip vermeyeceği çokça tartışılmıştır. Yine kaydetme suçunda failin kaydetmeyi tamamlayamadan yakalanması gibi bir durumda teşebbüs aşamasında kalan kaydetme suçunun değil aslında ele geçirme suçunun oluştuğu ve bu durumda faile 135. maddeye teşebbüsten değil 136. maddede yer alan ele geçirme fiilin tamamlanmış halinden -ki 136. maddenin cezası 135. Maddeden daha ağırdır- ceza verilmesi gerektiği gibi çelişkili bir hal ortaya çıkmasına neden olmuştur.

Bu doğrultuda TCK m. 135 ve 136'nın tek bir maddede birleştirilerek eylemin derecesine göre yaptırım öngörülmesi kaydetmenin ve ele geçirmeden daha ağır ve yaptırıma bağlanması isabetli olacaktır.[361]

[361] **ERDOĞAN**, s. 628.

KAYNAKÇA

AKBULUT, Berrin; Bilişim Alanında Suçlar, Ankara 2017.

AKDAĞ, Hale; Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması, Ankara 2013.

AKGÜL, Aydın; Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması, İstanbul 2014.

AKİPEK, Jale - **AKINTÜRK**, Turgut - **ATEŞ**, Derya; Türk Medeni Hukuku Başlangıç Hükümleri Kişiler Hukuku, İstanbul 2018.

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

AKYÜREK, Güçlü; Özel Hayatın Gizliliğini İhlal Suçu, Ankara 2011.

ARTUK, Mehmet Emin- **GÖKCEN**, Ahmet- **YENİDÜNYA**, A. Caner; Ceza Hukuku Genel Hükümler, Ankara 2007.

ARTUK, Mehmet Emin- **GÖKCEN**, Ahmet- **YENİDÜNYA**, A. Caner; Türk Ceza Kanunu Şerhi, Madde 88-153, Üçüncü Cilt, Ankara 2014.

AŞIKOĞLU, Şehriban İpek; Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri, İstanbul 2018.

AYDIN, Hüseyin; *Ceza Hukukunda Kamu Görevlisi Kavramı*, Ankara Barosu Dergisi, S.: 2010/1, 109-128.

AYDIN, Hüseyin**;** Sınai Mülkiyet Hakları Aleyhine İşlenen Suçlar, Ankara 2003.

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

AYÖZGER ÖNGÜN, Çiğdem; Kişisel Verilerin Korunması Hukuku, İstanbul 2019.

BAŞALP, Nilgün; Kişisel Verilerin Korunması ve Saklanması, Ankara 2004.

BENSGİR, Türksel Kaya; Bilgi Teknolojileri ve Örgütsel Değişim, Ankara 1996.

BEYTAR, Erbil; İşçinin Kişiliğinin ve Kişisel Verilerinin Korunması, İstanbul 2018.

CENTEL, Nur – **ZAFER**, Hamide – **ÇAKMUT**, Özlem; Türk Ceza Hukukuna Giriş, İstanbul 2008.

CATE; Fred H., *"The Changing Face of Privacy Protection in the European Union and the United States",* Indiana Law Review, 1999, C. 33, S. 173, s. 173-232. https://mckinneylaw.iu.edu/ilr/pdf/vol33p173.pdf

ÇIRAK, Ezgi; *"Dijital Çağda Sonsuza Kadar Hatırlanmaya Karşı: Unutulma Hakkı",* CHD, Y. 2014, S. 36, s.161-189.

DEMİRBAŞ, Timur; Ceza Hukuku Genel Hükümler, Ankara 2017.

DEMİRCAN, Tunç; Bilişim Alanında Suçlar, İstanbul 2016.

DEVELİOĞLU, Hüseyin Murat; 6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması, İstanbul 2017.

DÖNMEZER, Sulhi – **ERMAN**, Sahir; Nazari ve Tatbiki Ceza Hukuku, Cilt II, İstanbul 1985.

DURAL, Mustafa – **ÖĞÜZ**, Tufan, Türk Özel Hukuku Cilt:2 (Kişiler Hukuku), İstanbul 2019.

DÜLGER, Murat Volkan; Kişisel Verilerin Korunması Hukuku, İstanbul, 2019.

DÜLGER, Murat Volkan; Bilişim Suçları ve İnternet Bilişim Hukuku, Ankara 2012.

ERARSLAN TÜRKMEN, Sevgi; Özel Nitelikli Kişisel Verilerin İşlenmesinde Açık Rızanın Aranmadığı Haller, İstanbul 2019.

GÜLTEKİN, Nil Melek; Kişisel Verilerin Ceza Hukuku Yönünden Korunması, Yayımlanmamış Yüksek Lisans Tezi, Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku A.B.D, İstanbul 2012.

GÜRLER, Fazlı; (Yargıtay Kararları Işığında) Teknik ve Hukuksal Yönleriyle Bilişim Alanında Suçlar, Ankara 2015.

HAFIZOĞULLARI, Zeki – **ÖZEN**, Muharrem; Türk Ceza Hukuku Genel Hükümler, Ankara 2017.

HAFIZOĞULLARI, Zeki - **ÖZEN**, Muharrem; Türk Ceza Hukuku Özel Hükümler Kişilere Karşı Suçlar, Ankara 2016.

HENKOĞLU, Türkan; Bilgi Güvenliği ve Kişisel Verilerin Korunması, Ankara 2015.

İÇEL, Kayıhan – **SOKULLU AKINCI**, Füsun – **ÖZGENÇ**, İzzet – **SÖZÜER**, Adem – **MAHMUTOĞLU**, Fatih S. – **ÜNVER**, Yener; Suç Teorisi, İstanbul 2004.

İTİŞGEN, Rezzan; *"Türk Ceza Hukukunda Kişisel Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme Suçu"* TAAD, 2015, S. 23, s. …-…

KANGAL, Zeynel T.; Kişisel Verilerin Ceza ve Kabahatler Hukukunda Korunması, İstanbul 2019.

KARAGÜLMEZ, Ali; Bilişim Suçları ve Soruşturma – Kovuşturma Evreleri, Ankara 2005.

KATOĞLU, Tuğrul; Ceza Hukukunda Hukuka Aykırılık, Ankara 2003.

KESER BERBER, Leyla, **ÜLGÜ,** Mahir, **ER**, Cüneyd; Elektronik Sağlık Kayıtları ve Özel Hayatın Gizliliği, İstanbul …..,

KILIÇOĞLU, Ahmet M.; Sınai Haklarla Karşılaştırmalı Fikri Haklar, Ankara 2017.

KILINÇ; Doğan, *"Anayasal Bır Hak Olarak Kışısel Verılerın Korunması",* AÜHFD, C. 61, S.3, 2012, s. 1089-1170.

KOCA, Mahmut- **ÜZÜLMEZ**, İlhan, Türk Ceza Hukuku Genel Hükümler, Ankara 2017.

KORKMAZ, İbrahim; Kişisel Verilerin Ceza Hukuku Kapsamında Korunması, Ankara 2017.

KORFF, Douwe; "*New Challenges to Date Protection Study-Working Paper No.2: Data Protection Laws in the EU: The Diffuculties in Meeting the Challenges Posed by Global Social and Technical Developments",* European Commission DG Justice, Freedom and Security Report, 2010.

KÖSE AYSUN, Melike; Kişisel Verilerin Kaydedilmesi Suçu, Ankara 2018.

KUNER, Cristopher; European Data Privacy Law and Online Business, Oxford University Press, 2003.

KUŞKONMAZ, Elif Mendos; Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması, İstanbul ÜniversiTesi Sosyal Bilimler Enstitüsü Kamu Hukuku A.B.D. Yayımlanmamış Yüksek Lisans Tezi, İstanbul 2013.

KÜZECİ, Elif; Kişisel Verilerin Korunması, Ankara 2019.

KÜZECİ, Elif; *"Anayasal Bir Hak: Kişisel Verilerin Korunması",* Bilişim Dergisi, S: 128, 2011, s. 142-149.

MALKOÇ, İsmail; Açıklamalı – İçtihatlı 5237 sayılı Yeni Türk Ceza Kanunu (Madde 82-149), İkinci Cilt, Ankara 2007.

MORGAN, Richard – **BOARDMAN**, Ruth; Data Protection Strategy – Implementing Data Protection Compliance, Thompson Sweet & Maxwell, London 2003.

OĞUZMAN, M. Kemal- **SELİÇİ**, Özer- **OKTAY ÖZDEMİR**, Saibe; Eşya Hukuku, İstanbul 2018.

ORTA, Mesut; Bilişim Suçları ve Elektronik Delillerin Toplanması Muhafazası Değerlendirilmesi Sunulması, Ankara 2015

ÖZDEMİR, Hayrunnisa; Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması, Ankara 2009

ÖZEN, Mustafa; *Kişisel Verilerin Kaydedilmesi, Verilmesi veya Ele Geçirilmesi ve Yok Edilmemesi Suçları (TCK m.136, 137, 138)*, Kamu Hukuku Arşivi, Mart 2009, s. 13-28.

ÖZGENÇ, İzzet; Türk Ceza Hukuku Genel Hükümler, Ankara 2016

ÖZTÜRK, Mustafa; *"Bilişim Cihazlarındaki Sayısal Delillerin Tespiti Ve Değerlendirilmesinde İş Akış Modelleri",* Ankara Üniversitesi Sağlık Bilimleri Enstitüsü Yayımlanmamış Yüksek Lisans Tezi, Ankara 2007.

RAUL, Alan Charles; *"Global Overwiev",* The Privacy, Data Protection and Cybersecurity Law Review, Ed. Alan Charles RAUL, Law Business Research, Londra 2017, s. 1-5.

SAMUELSON, Pamela; "Privacy As Intellectual Property?" Stanford Law Review, C.52, Y. 1999 – 200, s. 1377-1394. http://people.ischool.berkeley.edu/~pam/papers/privasip_draft.pdf (Erişim Tarihi: 18.03.2020)

SERT, Şeyma; Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması, Ankara 2019.

SOYASLAN, Doğan Ceza Hukuku Özel Hükümler, Ankara 2014.

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

ŞİMŞEK, Oğuz; Anayasa Hukukunda Kişisel Verilerin Korunması, İstanbul 2008.

TANER, Fahri Gökçen; TBB Eğitim Merkezi Kişisel Verilerin Ceza Hukuku ve KVKK Kapsamında Korunması Online Eğitimi, sunum slaytı; https://www.academia.edu/43057536/TCK_da_Ki%C5%9Fisel_Verilerin_Korunmas%

C4%B1_TBB_TV_SLAYT_15_05_2020_ video kaydı; http://www.tbbegitim.com/Video/VideoGaleri?egitimId=3401 (Erişim Tarihi: 30.07.2020)

TAŞKIN, Şaban Cankat; Bilişim Suçları, İstanbul 2008.

TAŞTAN, Furkan Güven; Türk Sözleşme Hukukunda Kişisel Verilen Korunması, İstanbul 2017.

TEKİNALP, Ünal; Fikri Mülkiyet Hukuku

TOROSLU, Nevzat; Cürümlerin Tasnifi Bakımından Suçun Hukuki Konusu, Sevinç Matbaası, Ankara 1970.

TOROSLU, Nevzat - **TOROSLU**, Haluk; Ceza Hukuku Genel Kısım, Ankara 2016.

TOĞUZ, Özlem; Avrupa Birliği ve Türkiye'de Fikri Mülkiyet ve Veri Korunması, İstanbul 2014, s. 21.

UNCULAR, Selen; İş İlişkisinde İşçinin Kişisel Verilerinin Korunması, Ankara 2018.

UYGUN, Murat; "Avrupa Birliğinin 95/46 Sayılı Veri Koruma Yönergesi Işığında Kişisel Verilerin Korunması" Gazi Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk Anabilim Dalı Avrupa Birliği Hukuku Yayınlanmamış Yüksek Lisans Tezi, Ankara 2010.

ÜÇÜNCÜ, S. Hilal, Medeni Yargılama Hukukunda Kişisel Verilerin ve Sırların Korunması, İstanbul 2019.

WELSS BRANSCOMB, Ann; "Who Owns Informatıon? From Prıvacy To Publıc Access" http://jolt.law.harvard.edu/articles/pdf/v08/08HarvJLTech249.pdf (Erişim Tarihi : 18.03.2020)

YEO, Michael; *"Propaganda and Surveillance in George Orwell's Nineteen Eighty-Four: Two Sides of the Same Coin",* s. 55.

https://pdfs.semanticscholar.org/cb63/57378e50118269e7151b4a0431d3ef67e75d.pdf?_ga=2.147388983.1815770433.1579597936-73627067.1579597936

YILMAZ, Sabire Sanem; Tıp Alanında Kişisel Verilerin Açıklanması Suçu, Ankara 2017.

PARENT, W.A.; "A New Definition of Privacy for the Law", Law and Philosophy, V. 2, 1983, s.305-338. http://people.brandeis.edu/~teuber/Parent_on_Privacy.pdf (Erişim tarihi : 24.05.2020)

Diğer Çevrimiçi kaynaklar

Türk Dil Kurumu Güncel Türkçe Sözlük, https://www.sozluk.gov.tr/

Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Yönlendirici İlkeler, https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf

108 sayılı Kişisel Verilerin Otomatik İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşme, https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37

95/46/EC sayılı Avrupa Parlamentosu ve Konseyi Direktifi, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN

Kazancı İçtihat Bankası

KVVK Kanun Gerekçesi, http://www.adalet.gov.tr/Tasarilar/kisisel_verilerin_korunmasi.pdf

Anayasa Mahkemesi Kararları, https://www.anayasa.gov.tr/Kararlar/GenelKurul/Basvuru_Karari/2015-102.pdf

AİHM Kararları, https://hudoc.echr.coe.int/eng

29. Madde Çalışma Grubu 4/2007 sayılı raporu, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf

https://www.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf, https://www.kvkk.gov.tr/Icerik/5388/Madde-ve-Gerekcesi-ile-Kisisel-Verilerin-Korunmasi-Kanunu-Bilgi-Notu-ve-Kisisel-Verilerin-Korunmasina-Iliskin-Terimler-Sozlugu

OECD Rehber İlkeleri, https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Gerçek Kişilerin Korunmasına Dair Sözleşme, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108

Resmi Gazete, https://www.resmigazete.gov.tr

Birleşmiş Milletler Evrensel İnsan Hakları Bildirisi, https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf

Avrupa Birliği Temel Haklar Şartı, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN

29. Madde Çalışma Grubu 5/2009 sayılı raporu, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp163_en.pdf

29. Madde Çalışma Grubu 1/2010 sayılı Raporu, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf

ÖZET

Bu çalışma iki bölümden oluşmaktadır.

Birinci bölümde kişisel veri kavramı ve unsurları, kişisel verilerin korunmasının tarihçesi ve uluslararası düzenlemeler, kişisel verilerin korunması hakkının hukuki niteliği ile kişisel verilerin işlenmesi konuları ele alınmıştır.

İkinci bölümünde ise genel olarak Türk Hukukunda kişisel verilerin korunması ve özellikle Türk Ceza Hukukunda kişisel verilerin korunması ile bu bağlamda kanunda yer alan suç tipleri incelenmiştir. Bu suç tipleri Türk Ceza Kanunu'nun "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" bölümünde düzenlenen 135. Maddesi "Kişisel Verilerin Kaydedilmesi Suçu", 136. maddesi "Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme Suçu" ve son olarak 138. maddesi "Verileri Yok Etmeme" suçlarıdır. Suç tipleri Türk Ceza Hukuku açısından değerlendirilmiş ve bu suçların unsurları ile özel görünüş şekilleri ve usul hükümleri incelenmiştir.

Anahtar Sözcükler: kişisel veri, kişisel verilerin korunması hakkı, suç, kişisel verilerin kaydedilmesi, kişisel verilerin hukuka aykırı olarak ele geçirilmesi, kişisel verilerin yok edilmemesi.

ABSTRACT

This study consists of two parts.

In the first part, the concept and elements of personal data, the history of personal data protection and international regulations, the legal nature of the right of protection of personal data and the processing of personal data are discussed.

In the second part, personal data protection in Turkish Law, especially the protection of personal data in Turkish Criminal Law and the types of crimes prescribed by law are examined generally. The types of crimes that are examined in this study are; Article 135 "Recording of Personal Data", Article 136 "Illegally Obtaining or Giving Data" and finally Article 138 "Destruction of Data" legislated in Penal Code of Turkey under the title of "Offences Against Privacy and Confidentiality Violation of Confidentiality of Communication". The types of crime have been evaluated in terms of Turkish Criminal Law, and the elements of these crimes, their specific appearance and procedural provisions have been examined.

Key words: personal data, the right of protection of personal data, crime, recording of personal data, illegally obtaining or giving personal data, destruction of personal data.