



KADIR HAS ÜNİVERSİTESİ  
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ  
HUKUK ANABİLİM DALI

**6698 SAYILI KİŞİSEL VERİLERİN KORUNMASI  
KANUNU KAPSAMINDA VERİLERİ HUKUKA AYKIRI  
OLARAK VERME VEYA ELE GEÇİRME SUÇU (TCK m.  
136 ve 137)**

UMUT EMRE YAĞLIDERE  
DANIŞMAN: DR. ÖĞR. ÜYESİ AYSUN ALTUNKAŞ

YÜKSEK LİSANS TEZİ

İSTANBUL, EKİM, 2021

**6698 SAYILI KİŞİSEL VERİLERİN KORUNMASI  
KANUNU KAPSAMINDA VERİLERİ HUKUKA AYKIRI  
OLARAK VERME VEYA ELE GEÇİRME SUÇU (TCK m.  
136 ve 137)**

UMUT EMRE YAĞLIDERE

DANIŞMAN: DR. ÖĞR. ÜYESİ AYSUN ALTUNKAŞ

YÜKSEK LİSANS TEZİ

HUKUK ANABİLİM DALI KAMU HUKUKU PROGRAMI'NDA YÜKSEK  
LİSANS DERECEŚİ İÇİN GEREKLİ KİSMİ ŞARTLARIN YERİNE GETİRİLMESİ  
AMACIYLA KADİR HAS ÜNİVERSİTESİ LİSANSÜSTÜ EĞİTİM  
ENSTİTÜSÜ'NE TESLİM EDİLMİŐTİR.

İSTANBUL, EKİM, 2021

ARAŐTIRMA ETİĐİ VE  
YAYIN YÖNTEMLERİ BİLDİRİMİ

Ben, UMUT EMRE YAĐLIDERE;

- Hazırladığım bu Yüksek Lisans Tezinin tamamen kendi çalışmam olduğunu ve başka çalışmalardan yaptığım alıntıların kaynaklarını kurallara uygun biçimde belirttiğimi;
- Bu Yüksek Lisans Tezinin başka bir eğitim kurumunda bir derece veya diplomaya sunulan veya kabul edilen herhangi bir materyal içermediğini,
- “Yükseköğretim Kurulu Etik Davranış İlkeleri” uyarınca hazırlanan “Kadir Has Üniversitesi Akademik Etik İlkeleri”ni takip ettiğimi onaylıyorum

Buna ek olarak, bu çalışma ile ilgili ortaya çıkabilecek herhangi bir usulsüzlük iddiasının, üniversite mevzuatına uygun olarak disiplin işlemi ile sonuçlanacağını kabul ediyorum.

ÖĐRENCİNİN ADI SOYADI

\_\_\_\_\_

TARİH VE İMZA

(26.10.2021)

## KABUL VE ONAY

**UMUT EMRE YAĞLIDERE** tarafından hazırlanan **6698 SAYILI KİŞİSEL VERİLERİN KORUNMASI KANUNU KAPSAMINDA VERİLERİ HUKUKA AYKIRI OLARAK VERME VEYA ELE GEÇİRME SUÇU (TCK m. 136 ve 137)** başlıklı bu çalışma **26.10.2021** tarihinde yapılan savunma sınavı sonucunda başarılı bulunarak jürimiz tarafından **YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Dr. Öğr. Üyesi Aysun Altunkaş (Danışman) Kadir Has Üniversitesi \_\_\_\_\_

Prof. Dr. Tuğrul Bayazıt Katoğlu Kadir Has Üniversitesi \_\_\_\_\_

Dr. Öğr. Üyesi Elif Küzeci Bahçeşehir Üniversitesi \_\_\_\_\_

Yukarıdaki imzaların adı geçen öğretim üyelerine ait olduğunu onaylıyorum.

İMZA  
Müdür  
Lisansüstü Eğitim Enstitüsü  
ONAY TARİHİ: Gün/Ay/Yıl

# İÇİNDEKİLER

İÇİNDEKİLER .....	iii
ÖZET.....	ix
ABSTRACT .....	xi
TEŞEKKÜRLER .....	xii
KISALTMALAR .....	xiv
GİRİŞ .....	1
I. BÖLÜM: GENEL BİLGİLER.....	2
1. GENEL KAVRAMLAR.....	2
1.1. Kişisel Veri .....	2
1.1.1. Kişisel Verinin Tanımı.....	2
1.1.2. Kişisel Verinin Unsurları .....	5
1.1.2.1. Bilginin Varlığı .....	6
1.1.2.2. Bilginin Gerçek Kişiyeye İlişkin Olması.....	8
1.1.2.3. Kimliği Belirli veya Belirlenebilir Kişinin Varlığı .....	13
1.1.3. Özel Nitelikli Kişisel Veriler .....	15
1.2. Kişisel Verinin İşlenmesi .....	20
1.2.1. Kişisel Verinin İşlenmesinin Tanımı .....	20
1.2.2. Kişisel Verinin İşlenmesinde Benimsenen Genel İlkeler.....	22
1.2.2.1. Hukuka ve Dürüstlük Kurallarına Uygun Olma .....	23
1.2.2.2. Belirli, Açık ve Meşru Amaçlar İçin İşleme .....	25
1.2.2.3. İşleme Amacıyla Bağlantılı, Sınırlı ve Ölçülü Olma .....	28
1.2.2.4. Mevzuatta Öngörülen veya İşlendikleri Amaç İçin Gerekli Olan Süre Kadar Muhafaza Edilme .....	30
1.2.2.5. Doğru ve Gerektiğinde Güncel Olma .....	32
1.3. Kişisel Veri İşleme Sürecindeki Süjeler .....	34
1.3.1. İlgili Kişi .....	34
1.3.2. Veri Sorumlusu .....	34
1.3.3. Veri İşleyen .....	35
2. KİŞİSEL VERİLERİN KORUNMASININ HUKUKSAL GELİŞİMİNİN TARİHİ SÜRECİ .....	36
2.1. Genel Olarak .....	36

2.2. Uluslararası Düzenlemeler .....	37
2.2.1. OECD Düzenlemeleri .....	38
2.2.2. Avrupa Konseyi Düzenlemeleri .....	39
2.2.3. Birleşmiş Milletler Örgütü Düzenlemeleri.....	42
2.2.4. Avrupa Birliği Düzenlemeleri: 95/46/EC Sayılı Direktif ve GDPR .....	43
2.3. Türk Hukukundaki Düzenlemeler .....	45
3. KİŞİSEL VERİLERİN KORUNMASINDA GÜDÜLEN AMAÇ .....	50
II. BÖLÜM: KVKK’NIN CEZA HUKUKU, CEZA MUHAKEMESİ HUKUKU VE DİĞER HUKUK DALLARIYLA İLİŞKİSİ .....	52
1. GENEL OLARAK .....	52
2. KVKK’NIN UYGULANACAĞI HALLER VE KVKK’NIN TCK’NIN 5. MADDESİYLE İLİŞKİSİ.....	55
2.1. KVKK’nın Uygulanacağı Haller.....	55
2.2. KVKK’nın TCK’nın 5. Maddesiyle İlişkisi.....	56
3. KVKK’NIN 17. VE 18. MADDELERİNE İLİŞKİN DEĞERLENDİRMELER... 59	
3.1. Genel Olarak .....	59
3.2. KVKK’nın 17. Maddesine İlişkin Değerlendirmeler.....	60
3.2.1. Cezanın Niteliği ve Derecelendirilmesi Açısından .....	60
3.2.2. Hükümün Uygulanacağı Davranış ve İşlemlerin Kapsamı Açısından.....	61
3.2.3. Cezayı Artıran Sebepler ile Özel Nitelikli Kişisel Veriler Açısından.....	62
3.2.4. Hükümlerin Uygulanabilme Zamanı Açısından .....	63
3.3. KVKK’nın 18. Maddesine İlişkin Değerlendirmeler.....	63
3.3.1. Yaptırıma Konu Aykırılıklar Açısından.....	63
3.3.2. Yaptırımın Derecelendirilmemesi Açısından.....	64
4. KVKK’NIN UYGULANMAYACAĞI HALLER VE BU HALLERDE İZLENİLECEK YÖNTEM.....	65
4.1. Genel Olarak .....	65
4.2. Tam İstisna Halleri (m. 28/1).....	66
4.2.1. Kişinin Kendisiyle veya Aynı Konutta Yaşayan Aile Bireyleriyle İlgili Kişisel Verileri İşlemesi .....	66
4.2.2. İstatistik, Araştırma ve Planlama Amacıyla Kişisel Verilerin İşlenmesi..	68
4.2.3. Sanat, Tarih, Edebiyat veya Bilimsel Amaçlarla ya da İfade Özgürlüğü Kapsamında Kişisel Verilerin İşlenmesi.....	69
4.2.4. Önleyici, Koruyucu ve İstihbari Faaliyetler Kapsamında Kişisel Verilerin İşlenmesi .....	71

4.2.5. Soruşturma, Kovuşturma, Yargılama veya İnfaz İşlemlerinde Kişisel Verilerin İşlenmesi .....	72
4.3. Kısmî İstisna Halleri (m 28/2).....	73
4.3.1. Kişisel Veri İşlemenin Suç İşlenmesinin Önlenmesi veya Suç Soruşturması İçin Gerekli Olması .....	74
4.3.2. Kişinin Kendisi Tarafından Alenileştirilmiş Kişisel Verilerin İşlenmesi .	74
4.3.3. Kişisel Veri İşlemenin Denetleme veya Düzenleme Görevlerinin Yürütülmesi ile Disiplin Soruşturma veya Kovuşturması İçin Gerekli Olması..	75
4.3.4. Kişisel Verilerin Bütçe, Vergi ve Mali Konulara İlişkin Olarak Devletin Ekonomik ve Mali Çıkarlarının Korunması Kapsamında İşlenmesi .....	76
4.4. KVKK'nın Kişisel Verinin Tutulduğu Yer Bakımından Uygulanmaması .....	76
4.5. KVKK'nın Uygulanmadığı Hallerde Hukuka Uygunluk Tespitinde İzlenilecek Yöntem.....	77
<b>5. VERİ İŞLEME ŞARTLARININ GENEL HUKUKA UYGUNLUK NEDENLERİYLE KARŞILAŞTIRILMASI.....</b>	<b>78</b>
5.1. Genel Olarak .....	78
5.2. Açık Rıza.....	80
5.2.1. Açık Rıza Kavramı.....	80
5.2.3. Açık Rızanın Geçerlilik Unsurları .....	82
5.2.4. Açık Rızanın Hukukî Niteliği .....	88
5.2.5. Açık Rıza Gösterme Ehliyeti .....	89
5.2.6. Çocukların Rızası .....	91
5.2.7. Açık Rıza ile İlgili Diğer Hususlar.....	93
5.2.8. TCK'daki İlgilin Rızasıyla Arasındaki İlişki .....	95
5.3. Kanunlarda Açıkça Öngörülme (m. 5/2-a) ile Hukukî Yükümlülüğün Yerine Getirilmesi (m. 5/2-ç).....	97
5.3.1. Kanunlarda Açıkça Öngörülme (m. 5/2-a).....	97
5.3.2. Hukukî Yükümlülüğün Yerine Getirilmesi (m. 5/2-ç).....	98
5.3.3. TCK'daki Kanunun Hükmünü İcra ve Yetkili Merciiin Emrini Yerine Getirme Arasındaki İlişkisi .....	99
5.4. Fiili İmkânsızlık ve Zorunluluk Hali (m. 5/2-b) .....	101
5.4.1. KVKK'daki Düzenleme.....	101
5.4.2. TCK'daki Zorunluluk Hali ile İlişkisi.....	103
5.5. Bir Sözleşmenin Kurulması veya İfası (m. 5/2-c).....	105
5.6. İlgili Kişi Tarafından Alenileştirilmiş Olma (m. 5/2-d).....	109
5.7. Bir Hakkın Tesisi, Kullanılması veya Korunması (m. 5/2-e) .....	110

5.7.1. KVKK'daki Düzenleme.....	110
5.7.2. TCK'daki Hakkın Kullanılması ile İlişkisi .....	112
5.8. Meşru Menfaat (m. 5/2-f).....	113
5.9. Özel Nitelikli Kişisel Verilerin İşlenme Şartları .....	116
5.9.1. Sağlık ve Cinsel Hayat Dışındaki Kişisel Verilerin İşlenmesi.....	118
5.9.2. Sağlık ve Cinsel Hayata İlişkin Kişisel Verilerin İşlenmesi .....	119
5.9.2.1. Amaç Yönünden İşleme .....	120
5.9.2.2. Kişi Yönünden İşleme.....	125
5.9.3. Özel Nitelikli Kişisel Verilerin İşlenmesinde Ek Güvenlik Tedbirleri ...	132
6. KVKK'NIN ÖNLEYİCİ KOLLUK FAALİYETLERİ, CEZA MUHAKAMESİ İŞLEMLERİ VE CEZALARIN İNFAZ İŞLEMLERİYLE İLİŞKİSİ .....	134
6.1. KVKK'nın Önleyici Kolluk Faaliyetleriyle İlişkisi .....	134
6.2. KVKK'nın Ceza Muhakemesi İşlemleriyle İlişkisi .....	138
6.3. KVKK'nın Cezaların İnfaz İşlemleriyle İlişkisi .....	141
7. KVKK AÇISINDAN SUÇLULARIN İADESİNE İLİŞKİN DÜZENLEMELER .....	145
8. KİŞİSEL VERİLERİN KORUNMASIYLA İLGİLİ TCK'DA YER ALAN SUÇLAR .....	148
8.1. Kişisel Verilerin Kaydedilmesi Suçu (m. 135) .....	149
8.2. Verileri Yok Etmeme Suçu (m. 138) .....	150
III. BÖLÜM: VERİLERİ HUKUKA AYKIRI OLARAK VERME VEYA ELE GEÇİRME SUÇU (TCK m. 136) VE NİTELİKLİ HALİ (TCK m. 137) .....	152
1. GENEL OLARAK .....	152
1.1. Suç Hakkında Genel Değerlendirmeler .....	152
1.2. 765 Sayılı TCK ile Karşılaştırma .....	156
2. SUÇUN HUKUKÎ KONUSU .....	157
2.1. Genel Olarak .....	157
2.2. Kişisel Verilerin Korunması Hakkına Yönelik Görüş ve Yaklaşımlar .....	158
2.2.1. Ekonomik Hak Yaklaşımı .....	159
2.2.1.1. Mülkiyet Hakkı Görüşü.....	159
2.2.1.2. Fikrî Hak Görüşü .....	161
2.2.2. İnsan Haklarına Dayalı Yaklaşımlar .....	161
2.2.2.1. Özel Hayatın Korunması Hakkı Kapsamında Değerlendirme .....	162
2.2.2.2. İnsan Onuru Kapsamında Değerlendirme .....	164
2.2.2.3. Kişilik Hakkı Kapsamında Değerlendirme .....	165



2.2.2.4. Bilgi Edinme Hakkı Kapsamında Değerlendirme.....	166
2.3. Değerlendirme.....	168
3. SUÇUN MADDİ KONUSU .....	169
4. SUÇUN FAİLİ .....	169
5. SUÇUN MAĞDURU .....	171
6. SUÇUN MADDİ UNSURU .....	174
6.1. Davranış .....	174
6.1.1. Genel Olarak .....	174
6.1.2. Verme.....	178
6.1.3. Yayma .....	179
6.1.4. Ele Geçirme.....	181
6.2. Netice .....	183
7. SUÇUN MANEVİ UNSURU.....	185
8. HUKUKA UYGUNLUK NEDENLERİ .....	187
8.1. “Hukuka Aykırı Olarak” İfadesinin Anlamı .....	187
8.2. KVKK’daki ve TCK’daki Hukuka Uygunluk Nedenleri.....	188
9. KUSURLULUĞU ETKİLEYEN HALLER.....	190
10. SUÇUN ÖZEL GÖRÜNÜŞ ŞEKİLLERİ .....	191
10.1. Teşebbüs.....	191
10.2. İştirak .....	193
10.3. İçtima.....	195
10.3.1. TCK’nın 43. Maddesi Açısından İnceleme.....	195
10.3.2. TCK’da Düzenlenen Diğer Suç Tipleri ile Olan İçtima İlişkisi.....	196
10.3.2.1. Haberleşmenin Gizliliğini İhlal ve Kişiler Arasındaki Konuşmaların Dinlenmesi ve Kayda Alınması Suçları .....	197
10.3.2.2. Özel Hayatın Gizliliğini İhlal Suçu.....	198
10.3.2.3. Kişisel Verileri Kaydetme Suçu.....	200
10.3.2.4. Hakaret Suçu .....	201
10.3.2.5. Bilişim Sistemine Girme Suçu .....	202
11. SUÇUN NİTELİKLİ HALLERİ .....	202
11.1. Genel Olarak .....	202
11.2. Mağdurun Dinlenmesi.....	202
11.3. Kamu Görevlisi Olma veya Kolaylıktan Yararlanma.....	204
11.3.1. Kamu Görevlisi Olma .....	204

11.3.2. Meslek veya Sanatın Sağladığı Kolaylıktan Yararlanma.....	205
12. YAPTIRIM .....	207
13. SORUŞTURMA VE KOVUŞTURMA.....	209
14. GÖREVLİ VE YETKİLİ MAHKEME .....	210
15. ZAMANAŞIMI.....	212
SONUÇ.....	213
KAYNAKÇA.....	220
KİTAP, MAKALE VE TEZLER.....	220
ULUSLARARASI BELGE, GÖRÜŞ, SÖZLEŞME, REHBER VE RAPORLAR..	231
AİHM KARARLARI.....	234
AYM KARARLARI.....	234
YARGITAY KARARLARI.....	236
KİŞİSEL VERİLERİ KORUMA KURULU KARARLARI.....	238
KİŞİSEL VERİLERİ KORUMA KURUMU YAYINLARI.....	241
ULUSAL KANUNLAR .....	243
ULUSAL YÖNETMELİKLER .....	245
DİĞER .....	246
YARARLANILAN BAŞLICA İNTERNET SİTELERİ.....	248
ÖZGEÇMİŞ .....	250

## ÖZET

YAĞLIDERE, UMUT EMRE. 6698 SAYILI KİŞİSEL VERİLERİN KORUNMASI KANUNU KAPSAMINDA VERİLERİ HUKUKA AYKIRI OLARAK VERME VEYA ELE GEÇİRME SUÇU (TCK m. 136 ve 137), YÜKSEK LİSANS TEZİ, İstanbul, 2021.

Kişisel verilerin değerinin gün geçtikte artması, bu değerın daha hassas bir şekilde korunması gerekliliğini doğurmuştur. Bu anlamda gerek ulusal gerekse uluslararası alanda çok sayıda çalışmalar gerçekleştirilmiş, kişisel verilerin güvence altına alınmasını amaçlayan birtakım yasal düzenlemeler oluşturulmuştur.

Esasında kişisel verilerin korunması ihtiyacı asırlar öncesinde hasıl olmuştur. Ancak özellikle 20. yüzyılda bireylere ait bilgilerin gerek kamu gerekse özel sektörde otomatik yöntemler aracılığıyla işlenmesi ve bu işlemenin bireyler üzerinde ayrımcılık, mağduriyet gibi birtakım olumsuz sonuçlar doğurması, korumanın yeniden şekillenmesi gerektiğini ortaya çıkarmıştır. Bilhassa 2000’li yıllarla birlikte bireylere ait bilgiler bir bütün olarak ele alındığında, bu bilgilerin yepyeni ve önemli değerler taşıdığı su götürmez bir gerçek olmuştur. Nitekim artık kişisel verilerin korunması hakkı yalnızca özel hayatın gizliliği ile değil, birçok hak ile ilişkilendirilmekte, hatta bağımsız bir hak olarak nitelendirilmektedir. Diğer yandan bu bilgilerin ifşası, teknolojik gelişmelerin de sağladığı kolaylıkla günümüzde daha önceki dönemlere göre oldukça basittir. Dolayısıyla günümüz koşullarında, insan haklarına dayanan bir değer olan kişisel verilerin daha hassas bir şekilde korunması gerekir. Bunun için de kişisel verilerin ifşası ve koruduğu değerın ihlalinin yaptırıma bağlanması gereklidir.

Bu tez çalışmasının amacı, 5237 sayılı Türk Ceza Kanunu’nun 136. maddesinde düzenlenen verileri hukuka aykırı olarak verme veya ele geçirme suçunu ve suçun nitelikli hallerini 6698 sayılı Kişisel Verilerin Korunması Kanunu kapsamında incelemektir. Bu bağlamda çalışmada; çok da yeni olmamakla birlikte Türk mevzuatına yakın tarihte dahil olan kişisel verilerin korunması hakkının ulusal ve uluslararası alanda nasıl düzenlendiği, bu hakkın bilhassa Türk ceza hukuku, ceza muhakemesi hukuku ve diğer bazı hukuk dalları arasındaki ilişkisi incelenerek verileri hukuka aykırı olarak verme veya ele geçirme suçunun nasıl ele alınması gerektiği değerlendirilmeye çalışılmıştır.

**Anahtar Sözcükler:** Kişisel veri, kişisel verilerin korunması, KVKK, Türk Ceza Kanunu, kişisel verilerin verilmesi, kişisel verilerin yayılması, kişisel verilerin ele geçirilmesi.



## ABSTRACT

YAĞLIDERE, UMUT EMRE. *ILLEGALLY OBTAINING OR GIVING DATA (TURKISH PENAL CODA NO 5237) WITHIN THE SCOPE OF THE LAW ON PROTECTION OF PERSONAL DATA NO 6698*, MASTER'S THESIS, İstanbul, 2021.

The increase in the value of personal data day by day, necessitated the protection of this value more sensitively. In this sense, lots of studies have been carried out in the national and international arena and many legal regulations aiming to protection of personal data have established.

In fact, the need to protect personal data emerged centuries ago. However, especially in the 20th century, the processing of personal data by automatic methods in both the public and private sectors and the negative consequences of this processing on individuals, revealed that the data protection regulations needs to be reshaped. It is an indisputable fact that the personal has new and important values belonging to individuals is considered as a whole with the 2000s. On the other hand, the results that emerge in case of the disclosure of this information are not the same when we compare today's and before. Therefore, in today's conditions, personal data, which is a value based on human rights, needs to be protected more sensitively. In order to achieve this, the disclosure of personal data or the violation of the value it protects must also be sanctioned.

The aim of this thesis is to examine the crime of illegally obtaining or giving personal data regulated in Article 136 of the Turkish Penal Code No. 5237 and the qualified forms of the crime within the scope of the Law on Protection of Personal Data No. 6698. In this study, it has been tried to evaluate how the concept of personal data, which has recently been included in the Turkish legislation, is regulated nationally and internationally, it's relation with other regulations in the Turkish criminal law, and how the crime of illegally giving or seizing personal data should be approached.

**Keywords:** Personal data, protection of personal data, KVKK, Turkish Penal Code, deliver of personal data, publishes of personal data, acquisition of personal data.

## TEŞEKKÜRLER

Bu çalışmanın hazırlanması sürecinde değerli vaktini benimle paylaşmaktan çekinmeyen; görüş, eleştiri ve tavsiyeleri ile bana yön gösteren kıymetli danışman hocam Dr. Öğr. Üyesi Aysun Altunkaş'a; tez jürimde yer alarak beni onurlandıran ve değerli vaktini ayırarak çalışmamızı değerlendiren Prof. Dr. Tuğrul Bayazıt Katoğlu ve Dr. Öğr. Üyesi Elif Küzeci'ye teşekkürlerimi sunarım.

Ayrıca avukatlık mesleğimin başında değerli tecrübelerini benden esirgemeyen Av. Filiz Saraç ve abim Av. Deniz Erdem Yağlıdere'ye, kişisel verilerin korunması alanında çalışma ve tecrübe edinme fırsatını tanıyan Av. Rıza Saka'ya, çalışmanın gözden geçirilmesi sürecinde desteklerini esirgemeyen meslektaşlarım Av. Ömer Faruk Topcu, Av. Esat Gül ve çalışmada emeği geçen tüm arkadaşlarıma teşekkürlerimi sunarım.

Son olarak, hayatımın her aşamasında bana destek olan canım aileme teşekkürlerimi sunarım.



*Babaanneme, Anneanneme, Dedeme ve Poyraz'a...*

## KISALTMALAR

108 sayılı Sözleşme	: 28.1.1981 tarihli ve 108 sayılı Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Avrupa Konseyi Sözleşmesi
2002/58/EC sayılı Yönerge	: 2002/58/EC sayılı Özel Yaşamın ve Elektronik İletişimin Korunması Yönergesi
29. Madde Çalışma Grubu	: Article 29 Data Protection Working Party
5235 sayılı Kanun	: Adli Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanun
622 sayılı Kanun Hakkında Kanun	: 6222 sayılı Sporda Şiddet ve Düzensizliğin Önlenmesi
6991 sayılı Kanun	: 04.04.2017 tarihli ve 30028 sayılı Resmî Gazete’de yayımlanan 6991 sayılı Türkiye Cumhuriyeti ile Sırbistan Cumhuriyeti Arasında Suçluların İadesine Dair Anlaşma ve Anlaşmada Değişiklik Yapılmasına İlişkin Notaların Onaylanmasının Uygun Bulunduğu Hakkında Kanun
765 sayılı TCK	: 765 sayılı Türk Ceza Kanunu
95/46/EC Sayılı Direktif	: 24.10.1995 tarihli ve 1995/46/EC sayılı Kişisel Verilerin İşlenmesi ve Serbestçe Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Direktif
A.Ş.	: Anonim Şirketi
AB	: Avrupa Birliği
ABAD	: Avrupa Birliği Adalet Divanı
Adli Sicil Kanunu	: 5352 sayılı Adli Sicil Kanunu
AİHM	: Avrupa İnsan Hakları Mahkemesi
AİHS	: Avrupa İnsan Hakları Sözleşmesi
AK	: Avrupa Konseyi
Anayasa	: T.C. 1982 Anayasası
ASK	: 5352 sayılı Adli Sicil Kanunu
AVK	: 1136 sayılı Avukatlık Kanunu
AY	: T.C. 1982 Anayasası



AYM	: Anayasa Mahkemesi
Beyanname	: İnsan Hakları Evrensel Beyannamesi
Bkz.	: Bakımız
BM/Örgüt	: Birleşmiş Milletler
C.	: Cilt
c.	: Cilt sayısı
CCTV	: Close Circuit Television (Kapalı Devre Kamera Sistemleri)
CGİK	: 5275 sayılı Ceza ve Güvenlik Tedbirlerinin İnfazı Hakkında Kanun
CMK	: 5271 sayılı Ceza Muhakemesi Kanunu
Çev	: Çeviren
DNA	: Deoksiribo Nükleik Asit
E.	: Esas
ed.	: Editör
EUROJUST	: The European Union's Judicial Cooperation Unit (Avrupa Birliği Yargısal İşbirliği Birimi)
EUROPOL	: The European Police Office (Avrupa Polis Ofisi)
Dn	: dipnot
GDPR	: General Data Protection Regulation (Avrupa Veri Koruma Tüzüğü)
GPRS Servisi)	: General Packet Radio Service (Genel Paket Radyo Servisi)
ICO	: Information Commissioner's Office (Birleşik Krallık Veri Koruma Otoritesi)
IP	: Internet Protocol (İnternet Protokolü)
İade Anlaşması	: Türkiye Cumhuriyeti ile Sırbistan Cumhuriyeti Arasında Suçluların İadesine Dair Anlaşma
İş Kanunu	: 4857 sayılı İş Kanunu
Jandarma Kanunu	: 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanunu
K.	: Karar
KEP	: Kayıtlı Elektronik Posta

Kurul	: Kişisel Verileri Koruma Kurulu
KVKK	: 6698 sayılı Kişisel Verilerin Korunması Kanunu
m.	: Madde
MOBESE	: Mobil Elektronik Sistem Entegrasyonu
Mük.	: Mükerrer
OECD	: Organization for Economic Cooperation and Development (Ekonomik Kalkınma ve İşbirliği Örgütü)
par.	: Paragraf
PVSK	: 2559 sayılı Polis Vazife ve Salâhiyet Kanunu
Rehber İlkeler	: Ekonomik İşbirliği ve Kalkın Örgütü tarafından hazırlanan Özel Yaşamın Gizliliğinin ve Sınır Ötesi Kişisel Veri Akışının Korunmasına İlişkin Rehber İlkeler
s.	: Sayfa
S.	: Sayı
SGK	: Sosyal Güvenlik Kurumu
SHTK	: 3359 sayılı Sağlık Hizmetleri Temel Kanunu
ss.	: Sayfa sayısı
TBB	: Türkiye Barolar Birliği
TBK	: 6098 sayılı Türk Borçlar Kanunu
TBMM	: Türkiye Büyük Millet Meclisi
TCK	: 5237 sayılı Türk Ceza Kanunu
TDK	: Türk Dil Kurumu
TMK	: 4721 sayılı Türk Medeni Kanunu
TTK	: 6102 sayılı Türk Ticaret Kanunu
UYAP	: Ulusal Yargı Ağı Platformu
vb.	: ve benzeri
vd.	: ve devamı
VUK	: 213 sayılı Vergi Usul Kanunu
YCGK	: Yargıtay Ceza Genel Kurulu
WHO	: World Health Organization (Dünya Sağlık Örgütü)

## GİRİŞ

Bireylerin özel hayatlarının korunmasının önemi, esasen yüz yıllar öncesinde ortaya çıkmıştır. Bu önem, özellikle II. Dünya Savaşı'ndan sonra bireylere yapılan ayrımcılık, ötekileştirme, farklı muamele gösterme gibi olumsuzluklar nedeniyle bir hayli artmıştır.

Son yıllarda bilgisayar ve iletişim teknolojilerinde görülen gelişmeler sonucunda devletler; kendilerine verilen yükümlülükleri yerine getirmek ve kamu hizmetini yürütmek amacıyla daha önceden çoğunlukla fiziki ortamda kullanmış olduğu sistemlerini dijital ortama taşımıştır. Özel sektörde de hız, zaman, maliyet, teknolojik gelişmelere uyum sağlama vb. etkenler gözetilerek bir dijitalleşme adımı atılmıştır. Diğer yandan bireyler haberleşme, iletişim kurma, etkileşimde bulunma, alışveriş yapma, müzik dinleme, video izleme, haber takip etme, anı ölümsüzleştirme gibi gayelerle teknolojik imkânları özel yaşantılarına eskiye göre daha fazla dahil etmeye başlamıştır. Tüm bunların bir sonucu olarak artık insanoğluna ait bilgiler sanal dünyaya taşınmaktadır. Bir hukuk devletinin görevi de teknolojik imkanlar ve bu imkanların getirdiği riskler karşısında; kişilere ait bilgilerin, dolayısıyla kişinin kendisinin korunmasını hedefleyen normları oluşturmak ve uygulamaktır.

1950'lerin sonundan itibaren uluslararası alanda kişisel verilerin koruma altına alınması amacıyla çeşitli düzenlemelerin ortaya çıktığı, ülkemizde ise bu çalışmaların son yıllarda yapıldığı görülmektedir. Nitekim ülkemizde 1982 Anayasası, 5237 sayılı Türk Ceza Kanunu, 6698 sayılı Kişisel Verilerin Korunması Kanunu gibi yasal düzenlemelerle son yıllarda kişisel verilerin korunması hakkı ve buna bağlı değerler koruma altına alınmaktadır. Çalışmanın I. bölümünde kişisel verinin ve ilgili diğer kavramların ülkemizde ve uluslararası alanda kabul görmüş tanımları, kişisel verilerin korunmasının hukuksal gelişim süreci ve kişisel verilerin korunmasında güdülen amaç ele alınmıştır. Çalışmanın II. bölümünde ülkemizde kişisel verilerin korunmasının ceza hukuku, ceza muhakemesi hukuku, infaz hukuku ve ilgili bazı hukuk dallarıyla ilişkisi incelenmiştir. Çalışmanın III. bölümünde ise 5237 sayılı Türk Ceza Kanunu'nun 136. maddesinde düzenlenen verileri hukuka aykırı olarak verme veya ele geçirme suç tipinin incelemesi yapılmış, bu suçun uygulama alanı ile ilgili mahkeme kararları ve öğretideki görüşler değerlendirmeye çalışılmıştır.

# I. BÖLÜM: GENEL BİLGİLER

## 1. GENEL KAVRAMLAR

### 1.1. Kişisel Veri

#### 1.1.1. Kişisel Verinin Tanımı

Türk hukukunda kişisel veri kavramı 07.06.2016 tarihli Resmî Gazete’de yayımlanarak yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu’nun<sup>1</sup> “Tanımlar” başlıklı 3. maddesinin 1. fıkrasının d bendinde “*Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi*” olarak tanımlanmıştır. Aynı doğrultuda, 26.09.2004 tarihli Resmî Gazete’de yayımlanarak yürürlüğe giren 5237 sayılı Türk Ceza Kanunu’nun<sup>2</sup> “*Kişisel verilerin kaydedilmesi*” suçunu düzenleyen 135. maddesinin gerekçesinde de “*gerçek kişiye ilişkin her türlü bilginin*” kişisel veri olarak kabul edilmesi gerektiği belirtilmiştir. Anayasa Mahkemesi’nin<sup>3</sup> istikrar kazanmış tanımına göre ise kişisel veri “*Belirli veya kimliği belirlenebilir olmak şartıyla bir kişiye ilişkin bütün bilgiler*” olarak ifade edilmektedir<sup>4</sup>.

Kişisel verinin uluslararası alanda kabul görmüş diğer önemli kaynaklardaki tanımının da Türk hukukundaki tanımla benzer olduğu görülmektedir. Konuyla ilgili ilk uluslararası düzenleme olan ve Ekonomik İşbirliği ve Kalkınma Teşkilatı (*Organization for Economic Co-operation and Development*)<sup>5 6</sup> tarafından yayımlanan 23.09.1980 tarihli Kişisel Verilerin Sınıraşan Trafığı ve Verilerin Korunmasına İlişkin Rehber İlkeler’in

<sup>1</sup> Resmî Gazete Tarihi: 7.4.2016, Sayı: 29677. Çalışmanın devamında “KVKK” olarak isimlendirilecektir.

<sup>2</sup> Resmî Gazete Tarihi: 26.9.2004, Sayı: 25611. Çalışmanın devamında “TCK” olarak isimlendirilecektir.

<sup>3</sup> Çalışmanın devamında “AYM” olarak isimlendirilecektir.

<sup>4</sup> AYM’nin 2014/7256 başvuru numaralı ve 27.02.2019 tarihli kararı, erişim için bkz.: <https://kararlarbilgibankasi.anayasa.gov.tr/BB/2014/7256>, erişim tarihi: 07.08.2021; AYM’nin 2013/2941 başvuru numaralı ve 11.05.2016 tarihli kararı, erişim için bkz.: <https://kararlarbilgibankasi.anayasa.gov.tr/BB/2013/2941?BasvuruNoYil=2013&BasvuruNoSayi=2941>, erişim tarihi: 07.08.2021; AYM’nin 2014/90 E., 2014/180 K. sayılı ve 04.12.2014 tarihli kararı, erişim için bkz.: <https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2014/180?EsasNo=2014%2F90>, erişim tarihi: 07.08.2021.

<sup>5</sup> Çalışmanın devamında “OECD” olarak isimlendirilecektir.

<sup>6</sup> Türkiye Cumhuriyeti, OECD’nin bir üyesidir.

(Guidelines on the Protection of Privacy and Transborder Flows of Personal Data)<sup>7</sup> 1. maddesinin b bendine göre kişisel veri “Tanımlanmış veya tanımlanabilir bir bireye ilişkin herhangi bir bilgi” olarak ifade edilmiştir<sup>8</sup>. Uluslararası düzeyde bağlayıcılığa sahip ilk kaynak olan 28.1.1981 tarihli ve 108 sayılı Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Avrupa Konseyi Sözleşmesi’nin (The Convention of the Protection of Individuals with regard to Automatic Processing of Personal Data No. 108)<sup>9</sup> 2. maddesinin a bendinde kişisel veri “Kimliği belirli veya belirlenebilir bir gerçek kişi hakkındaki tüm bilgiler” olarak tanımlanmıştır<sup>10</sup>.

Avrupa Birliği<sup>11</sup> düzenlemeleri içerisinde bulunan 24.10.1995 tarihli ve 1995/46/EC sayılı Kişisel Verilerin İşlenmesi ve Serbestçe Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Direktif’in (Protection of Individuals with regard to the Processing of Personal Data and on Free Movement of Such Data)<sup>12</sup> 2. maddesinin a bendinde ise kişisel veri “Belirlenmiş veya belirlenebilir gerçek kişiye ilişkin herhangi bir bilgi” olarak tanımlanmıştır<sup>13</sup>. Ayrıca madde metninin devamında belirlenebilir olma durumu, “Fizyolojik, zihinsel, ekonomik, kültürel veya sosyal kimliğine özel bir veya daha fazla faktöre veya bir kimlik numarasına atf başta olmak üzere doğrudan veya dolaylı olarak belirlenebilir olma” ifadeleriyle açıklığa kavuşturulmuştur.

95/46/EC sayılı Direktif’in yerini alan Avrupa Birliği Veri Koruma Tüzüğü’nün (General Data Protection Regulation)<sup>14</sup> 4. maddesinin 1. fıkrasına göre kişisel veri, “Tanımlanmış veya tanımlanabilir bir gerçek kişiye ilişkin her türlü bilgi” olarak belirtilmiştir<sup>15</sup>. Madde metninin devamında tanımlanabilir olma ifadesi “İsim, kimlik numarası, lokasyon, çevrim

<sup>7</sup> Çalışmanın devamında “Rehber İlkeler” olarak isimlendirilecektir.

<sup>8</sup> Rehber İlkeler’e erişim için bkz.: <https://www.oecd.org/digital/ieconomy/oecdguidelinesontheprivacyandtransborderflowsofpersonaldata.htm#guidelines>, erişim tarihi: 07.08.2021.

<sup>9</sup> Çalışmanın devamında “108 sayılı Sözleşme” olarak isimlendirilecektir.

<sup>10</sup> 108 sayılı Sözleşme’ye erişim için bkz.: <https://rm.coe.int/1680078b37>, erişim tarihi: 10.08.2021. Ayrıca Türkçe çevirisi için bkz.: <https://insanhaklarimerkezi.bilgi.edu.tr/media/uploads/2016/03/29/KisiselVerilerinOtomatikIslemeTabiTutulmasiKarsisindaBireylerinKorunmasiSozlesmesi.pdf>, erişim tarihi: 10.08.2021.

<sup>11</sup> Çalışmanın devamında “AB” olarak isimlendirilecektir.

<sup>12</sup> Çalışmanın devamında “95/46/EC sayılı Direktif” olarak isimlendirilecektir.

<sup>13</sup> 95/46/EC sayılı Direktif’e erişim için bkz.: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN>, erişim tarihi: 07.08.2021.

<sup>14</sup> Çalışmanın devamında “GDPR” olarak isimlendirilecektir.

<sup>15</sup> GDPR’a erişim için bkz.: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1374-1-1>, erişim tarihi: 07.08.2021.

*içi tanımlayıcı, fiziksel, fizyolojik, genetik, ruhsal, ekonomik, kültürel veya toplumsal kimliğine özgü bir ya da daha fazla sayıda faktöre atıfta bulunularak doğrudan veya dolaylı olarak tanımlanabilme” şeklinde detaylandırılmıştır.*

Sonuç olarak; görüleceği üzere ulusal ve uluslararası kaynaklar dikkate alındığında kişisel verinin tam olarak ne anlama geldiğinin ve nelerin kişisel veri olabileceğinin net bir yanıtı bulunmamaktadır<sup>16</sup>. Ancak genel anlamda kişisel veri “*belirli ya da belirlenebilir nitelikteki bir kişiye ilişkin her türlü bilgi*” olarak tanımlanabilir<sup>17</sup>. Bu tanımdan yola çıkılarak, bir kişiye ait kişisel veri türlerinin oldukça fazla olduğu söylenebilir. Örneğin kişinin kimlik numarası, sosyal güvenlik numarası, adresi, e-posta adresi, e-posta adresinin şifresi, telefon numarası, hobileri, kredi kartı bilgileri, banka bilgileri, malî bilgileri, tuttuğu takımı, evinin bedeli, kulüp üyeliği bilgileri, sosyal medya kullanıcı ve hesap bilgileri, alışkanlıkları, sesi, görüntüsü, katıldığı etkinlikleri, tercihleri, sosyal, ekonomik, duygusal veya fiziksel benliğine ilişkin bilgileri, dış görünüşü, bedenindeki belirleyici bilgileri (dövme, ben gibi), kanaati, tercihleri ve gündelik yaşantıları, yolculuk kayıtları, reçetede yer alan ilaç bilgileri, internet protokolü (IP) adresi, internet kullanım alışkanlıklarına ilişkin bilgileri birer kişisel veri olabilir<sup>18</sup>. Önemle belirtmek gerekir ki

<sup>16</sup> **Dülger**, Murat Volkan, *Kişisel Verilerin Korunması Hukuku*, Hukuk Akademisi Yayıncılık, 3. Baskı, İstanbul, Haziran 2020, (**Dülger**, *Kişisel Verilerin Korunması*), s. 61.

<sup>17</sup> **Küzeci**, Elif, *Kişisel Verilerin Korunması*, Turhan Kitapevi, Yenilenmiş ve Gözden Geçirilmiş Üçüncü Bası, Ankara, Şubat 2019, (**Küzeci**, *Kişisel Verilerin Korunması*), s. 9.

<sup>18</sup> **Küzeci**, *Kişisel Verilerin Korunması*, s. 315; **Ayözger Öngün**, A. Çiğdem, *Kişisel Verilerin Korunması Hukuku (Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil)*, Beta Yayınevi, İstanbul, 2019, s. 98; **Koç**, Buğrahan, *Tıp Alanında Kişisel Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme Suçu*, Yayımlanmamış Yüksek Lisans Tezi, T.C. İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, İstanbul, 2019, s. 3; **Erarslan Türkmen**, Sevgi, *Özel Nitelikli Kişisel Verilerin İşlenmesinde Açık Rızanın Aranmadığı Haller*, On İki Levha Yayıncılık, İstanbul 2019, s. 16; **Sert**, Şeyma, *Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması*, Seçkin Yayıncılık, Şubat 2019, Ankara, s. 24-25; **Akgül**, Aydın, *Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması*, Beta Yayınevi, İstanbul, 2014, s. 8-9; **Henkoğlu**, Tülay, *Bilgi Güvenliği ve Kişisel Verilerin Korunması*, Yetkin Yayınları, Ankara, 2015, s. 28; **Aksoy**, Hüseyin Can, *Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması*, Çakmak Yayınevi, Ankara 2010, s. 1; **Özdemir**, Hayrunnisa, “*Haberleşmenin Gizliliği ve Kişisel Veriler*”, Erzincan Üniversitesi Hukuk Fakültesi Dergisi, 13(1-2), 2009, ss. 285-303, (**Özdemir**, *Haberleşmenin Gizliliği*), s. 290; **Şimşek**, Oğuz, *Anayasa Hukukunda Kişisel Verilerin Korunması*, Beta Yayınevi, Ankara, 2008, s. 121; **Başalp**, Nilgün, *Kişisel Verilerin Korunması ve Saklanması*, Yetkin Yayınları, Ankara, 2004, (**Başalp**, *Kişisel Verilerin Korunması*), s. 22; **Akkurt**, Sinan Sami, “*Kişisel Veri Kavramının Hukuki Niteliğine İlişkin Yaklaşımlara Mukayeseli Bir Bakış*”, *Kişisel Verileri Koruma Dergisi*, Cilt: 2, Sayı: 1, ss. 20-32, s. 21; **Dülger**, *Kişisel Verilerin Korunması*, s. 61; **Yılmaz**, Sabire Sanem, *Tıp Alanında Kişisel Verilerin Korunması*, Seçkin Yayıncılık, Güncellenmiş 5. Baskı, Ankara, 2021, (**Yılmaz**, *Kişisel Veriler*), s. 53; **Aşıkoğlu**, Şehriban İpek, *Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri*, On İki Levha Yayınları, 1. Baskı, İstanbul, Kasım 2018, s. 5-6; **Turan**, Metin, *Karşılaştırmalı Hukukta Kişisel Verilerin Korunması*, Seçkin Yayıncılık, Güncellenmiş 2. Baskı, Ankara, Nisan 2019, s. 35; **İmançlı**, Canan, *Kişisel Sağlık Verilerinin*

örneklene kişisel verilerin, bir kısmının bireyin kişiliğine ilişkin bilgiler olduđu, bir kısmının ise bireyin bilişim topluluğundan kaynaklı hizmetlerin kullanımı sonucunda kendisiyle ilişkilendirilen ya da ilişkilendirilebilen bilgiler olduđu görölmektedir<sup>19</sup>. Bu anlamda ileride ortaya çıkacak teknolojik gelişmelerin de etkisiyle, kişisel veri türlerinin artabileceği söylenebilir.

### 1.1.2. Kişisel Verinin Unsurları

Hangi bilgilerin kişisel veri olarak sınıflandırılacağına net bir yanıtının bulunmamasının karşısında bazı unsurlar vardır ki bu unsurlar kişisel veri kavramının sınırlarını daraltarak bu kavramın daha belirgin hale gelmesini sağlamaktadır. Diğer bir ifadeyle kişisel verinin barındırdığı birtakım unsurlar vardır ve bu unsurlar onu alelade verilerden ayırt etmektedir<sup>20</sup>.

Kişisel verinin ulusal ve uluslararası alandaki tanımına bakıldığında, üç unsurunun bulunduğu görölmektedir<sup>21</sup>. Bunlar “bilginin varlığı”, “bilginin gerçek kişiye ilişkin olması” ve “kimliği belirli veya belirlenebilir kişinin varlığı”dır<sup>22</sup>. Bu unsurlar karşılanmadığı takdirde kişisel veriden söz edilemez.

---

*Korun(a)mamasından Doğan Özel Hukuk Sorumluluğu*, On İki Levha Yayıncılık, 1. Baskı, İstanbul, Nisan 2020, s. 38.

<sup>19</sup> **Dülger**, *Kişisel Verilerin Korunması*, s. 61.

<sup>20</sup> **Mutlu**, Muhammet Sefa, *Kişisel Verilerin Soruşturma Evresinde İşlenmesi ve İnsan Hakları Kapsamında Korunması*, Seçkin Yayıncılık, Ocak 2020, s. 31.

<sup>21</sup> 95/46/EC sayılı Direktif’in 29. maddesi ile veri koruma kurallarının uygulanmasında birlikteliği sağlamak ve uygulamada ortaya çıkan sorunları incelemek adına Avrupa Birliği Komisyonu’na görüş bildirmek ve tavsiyede bulunmak üzere kurulan Working Party 29 - Çalışma Grubu’nun (Çalışmanın devamında 29. Madde Çalışma Grubu olarak isimlendirilecektir.) 04/2007 sayılı görüşüne göre kişisel verinin “kimliği belirli veya belirlenebilir olan”, “gerçek bir kişi”, “ile ilgili”, “her türlü bilgi” olarak dört unsuru bulunmaktadır. 29. Madde Çalışma Grubu’nun 04/2007 sayılı görüş yazısına (*on the concept of personal data*) erişim için bkz.: [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf), erişim tarihi: 10.06.2021.

<sup>22</sup> *Sert*’e göre kişisel verilerin “veri” ve “kimliği belirli veya belirlenebilir bir kişi” olarak iki unsuru bulunmaktadır. **Sert**, s. 25; *Koç*’a göre kişisel verilerin unsurları “kimliği belirli veya belirlenebilir kişi”, “kişiyi belirli kılmayı sağlayacak bilgi” ve “bu kişi ile bilgi arasında kurulacak ilgi” olarak üçe ayrılmaktadır. **Koç**, s. 16. Ancak nihayetinde ortaya çıkan sonuç “belirli veya belirlenebilir bir kişiye ait her türlü bilgi” etrafında toplanmaktadır.

### 1.1.2.1. Bilginin Varlığı

Kişisel verinin ilk unsuru bilgidir. Bilgi, Türk Dil Kurumu<sup>23</sup> tarafından “*İnsan aklının erebileceği olgu, gerçek ve ilkelerin bütünü, bilgi, malumat*” olarak tanımlanmıştır<sup>24 25</sup>. Kişiyeye ait olan ve kişinin teşhis edilmesine olanak sağlayan bilgilerin kişisel veri olduğu bilinmektedir<sup>26</sup>. Burada önemle belirtmek gerekir ki bilgi ve veri kavramları her ne kadar birbirlerinden farklı olsa da öğretilerde bu kavramlar birbirlerinin yerine kullanılabilir<sup>27</sup>. Nitekim bu kavramların kişisel verilerin korunmasıyla ilişkili olarak birbirlerinin yerine geçer şekilde kullanılmaları bir sakınca yaratmamaktadır<sup>28</sup>.

Bir bilginin kişisel veri olarak kabul edilmesi için, o bilginin mutlaka gizli olmasına gerek yoktur<sup>29</sup>. Nitekim belirleyici olan, bilginin kendisidir. Ayrıca gizli veya gizli olmayan bilgi gibi bir ayrım yapılmamalıdır. Örneğin, aşağıda ele alınacak olan diğer iki unsurun da varlığı halinde kişinin fiziksel görünümü, uzun saçlı veya kısa saçlı olması, saçının

<sup>23</sup> Çalışmanın devamında “TDK” olarak isimlendirilecektir.

<sup>24</sup> TDK, Güncel Türkçe Sözlük, erişim için bkz.: <https://sozluk.gov.tr/>, erişim tarihi: 01.06.2021.

<sup>25</sup> Ayrıca bilgi, 24.10.2003 tarihli ve 25269 sayılı Resmî Gazete’de yayımlanan 4982 sayılı Bilgi Edinme Hakkı Kanunu’nda “*Kurum ve kuruluşların sahip oldukları kayıtlarda yer alan bu Kanun kapsamındaki her türlü veri*” olarak; 30.11.2007 tarihli ve 26716 sayılı Resmî Gazete’de yayımlanan İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik, 24.10.2007 tarihli ve 26680 sayılı Resmî Gazete’de yayımlanan Telekomünikasyon Kurumu Tarafından Erişim Sağlayıcılara ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik ile 11.04.2007 tarihli ve 30035 sayılı ve Resmî Gazete’de yayımlanan İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik’in ilgili maddelerinde “*verinin anlam kazanmış biçimi*” olarak tanımlanmıştır. Veri ise TDK tarafından “*Bir araştırmanın, bir tartışmanın, bir muhakemenin temeli olan ana öge, muta, done*” şeklinde; yukarıda anılan diğer Yönetmeliklerde “*Bilgisayar tarafından üzerinde işlem yapılabilen her türlü değer*” şeklinde, 18.11.2005 tarihli ve 25997 sayılı Resmî Gazete’de yayımlanan 5429 sayılı Türkiye İstatistik Kanunu’nda “*Anket veya idarî kayıtlar yoluyla elde edilen nicel ve/veya nitel istatistikî bilgiler*” şeklinde tanımlanmıştır. Bu tanımlardan yola çıkarak verinin işlenmemiş; ancak bilgiye dönüştürülmesi mümkün olan doneler olduğunu söylemek mümkündür. Aynı yönde görüş için bkz: **Avcıoğlu**, Nur Halet, *Türk Hukukunda Kişisel Verilerin Korunması Hakkı*, Yayımlanmamış Yüksek Lisans Tezi, T.C. Konya Karatay Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Yüksek Lisans Programı, Konya, 2018.

<sup>26</sup> **Köse Aysun**, Melike, *Kişisel Verilerin Kaydedilmesi Suçu (TCK m. 135)*, Seçkin Yayıncılık, Ankara, 2018, s. 26.

<sup>27</sup> Çalışma genelinde bilgi ve veri kavramları aynı anlamda kullanılacaktır. Bilgi, bilginin hammaddesi olarak enformasyon ve enformasyonun hammaddesi olarak veri kavramları ile ilgili detaylı bilgiye erişim için bkz.: **Küzeci**, *Kişisel Verilerin Korunması*, s. 9-12; **Uygun**, Murat, *Avrupa Birliğinin 95/46 Sayılı Veri Koruma Yönergesi Işığında Kişisel Verilerin Korunması*, Yayımlanmamış Yüksek Lisans Tezi, T.C. Gazi Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk Anabilim Dalı, Ankara, 2010, s. 46 vd.

<sup>28</sup> **Küzeci**, *Kişisel Verilerin Korunması*, s. 12.

<sup>29</sup> **Taştan**, Furkan Güven, *Türk Sözleşme Hukukunda Kişisel Verilerin Korunması*, On İki Levha Yayıncılık, 2. Baskı, İstanbul, Kasım 2017, s. 42; **Aşıkoğlu**, s. 8; **Sert**, s. 26-27.



rengi, bisikletinin markası, sosyal medyada paylaştığı bir fotoğrafı veya gizli tuttuğu banka kartı şifresi bu kişinin kişisel verisi olabilir<sup>30</sup>.

Diğer yandan bilginin doğru, yanlış, tam veya kanıtlanmış olup olmamasının da bir önemi yoktur<sup>31</sup>. Nitekim hem 1982 Anayasası'yla<sup>32</sup> hem de KVKK'yla<sup>33</sup> kişiye kendisiyle ilgili kişisel verilerin düzeltilmesini talep hakkı tanınmıştır. Dolayısıyla Anayasa ve KVKK'nın koruma alanının, kişilerin yanlış veya eksik verilerini de kapsadığı söylenebilir<sup>34</sup>. Örneğin bir şirketin tuttuğu borç defterinde kişinin borcunun 1.000 Türk lirası olarak yazıldığı; ancak gerçekte 1.500 Türk lirası olduğu varsayımında eğer ki yanlış bilgi içeren borç da ilgili kişiye ulaşmak için yeterli ise, bu durumda bilginin yanlış olması kişisel verinin unsurları açısından önem arz etmeyecektir.

Kişiyle ilgili nesnel bilgilerin yanında görüş ve değerlendirme gibi öznel bilgiler de o bilginin kişisel veri olup olmaması açısından belirleyici değildir<sup>35</sup>. TDK'ya göre öznel "*Özneyle ilişkili olan, öznedeki oluşan, nesnelere gerçeğine değil, bireyin düşünce ve duygularına dayanan, enfüsi, subjektif, nesnel karşıtı*", nesnel ise "*Nesne ile ilgili, nesneye ilişkili, öznel karşıtı*" anlamına gelmektedir<sup>36</sup>. Bu doğrultuda örneğin bir çalışanın işe kaç gün geldiği onun nesnel bir bilgisi iken, aynı çalışan hakkında iş yerindeki müdürü ya da amiri tarafından yapılan işe uygunluk değerlendirmesi onun öznel bir bilgisidir. Bu bilgilerin ikisi de çalışanın kişisel verisidir.

Diğer yandan bir bilginin kişisel veri olup olmadığına ilişkin değerlendirmenin, o bilginin biçiminden veya saklandığı alandan bağımsız olarak yapılması gerekir<sup>37</sup>. Dolayısıyla

<sup>30</sup> Aksoy, s. 14.

<sup>31</sup> Aşikoğlu, s. 9; Sert, s. 27; Bozkurt Yüksel, Armağan Ebru, *Bulut Bilişimde Kişisel Verilerin Korunması (Personal Data Protection on Cloud Computing)*, Yetkin Yayınları, 2016, s. 88.

<sup>32</sup> Anayasa'nın 20. maddesinin 3. fıkrası: "*Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında ... bunların düzeltilmesini veya silinmesini talep etme ... kapsar.*"

<sup>33</sup> KVKK'nın 11. maddesinin 1. fıkrasının d bendi: "*Herkes, veri sorumlusuna başvuruda bulunarak kendisiyle ilgili kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme ... hakkına sahiptir.*"

<sup>34</sup> Akdağ, Hale, *Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması*, Adalet Yayınevi, Ankara 2013, s. 10-13; Aksoy, s. 14-15.

<sup>35</sup> Özcan, Göknil, *Bankacılık İş ve İşlemlerinde Kişisel Verilerin Korunması*, On İki Levha Yayıncılık, 1. Baskı, İstanbul, Ocak 2020, s. 9; İmançlı, s. 42; Sert, s. 27; Dülger, *Kişisel Verilerin Korunması*, s. 155-156; Bozkurt Yüksel, s. 88.

<sup>36</sup> TDK, Güncel Türkçe Sözlük, erişim için bkz.: <https://sozluk.gov.tr/>, erişim tarihi: 19.06.2021.

<sup>37</sup> Aşikoğlu, s. 9.

bilginin sayısal, çizgisel, görsel veya işitsel olması ya da doküman üzerinde veya elektronik ortamda saklanması, o bilginin kişisel veri olma özelliğini etkilememektedir<sup>38</sup>.

29. Madde Çalışma Grubu da 04/2007 sayılı görüş yazısında (*on the concept of personal data*) bilgiyi geniş yorumlayarak “*her türlü bilginin (any information)*” varlığını bilgi unsuru açısından yeterli görmüştür<sup>39</sup>.

AYM, konuyla ilgili olarak “*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, eposta adresi, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler kişisel veri kapsamındadır.*” yorumunu yapmış; takip eden başlıklarda ele alınacak olan “*bilginin gerçek kişiye ilişkin olması*” ve “*kimliği belirli veya kimliği belirlenebilir kişinin varlığı*” şartlarının sağlanması durumunda her türlü bilginin kişisel veri olabileceğini belirtmiştir<sup>40</sup>.

### 1.1.2.2. Bilginin Gerçek Kişiye İlişkin Olması

KVKK'nın “*Tanımlar*” başlıklı 3. maddesinin 1. fıkrasının d bendinde kişisel veri “... *gerçek kişiye ilişkin her türlü bilgi*” olarak tanımlanmıştır. Dolayısıyla kişisel verinin ikinci unsuru, bilginin gerçek kişiye ilişkin olmasıdır<sup>41</sup>. Bilginin kişiye *ilişkin* olması, bilginin o kişi ile ilgili olmasını ifade eder<sup>42</sup>. 29. Madde Çalışma Grubu'na göre bir bilgi eğer ki kişinin kimliğine, karakterine veya davranışlarına gönderme yapıyorsa veya bu

<sup>38</sup> **Küzeci**, *Kişisel Verilerin Korunması*, s. 315; **Aşıkoğlu**, s. 9; **İmançlı**, s. 42.

<sup>39</sup> 29. Madde Çalışma Grubu'nun 04/2007 sayılı görüş yazısı (*on the concept of personal data*), s. 6.

<sup>40</sup> AYM'nin 2013/122 E., 2014/74 K. sayılı ve 09.04.2014 tarihli kararı, erişim için bkz.: <https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2014/74?EsasNo=2013%2F122>, erişim tarihi: 07.08.2021.

<sup>41</sup> Önemle belirtmek gerekir ki KVKK'nın 2000 ve 2008 yıllarına ait tasarılarında ilk olarak tüzel kişilerin bilgileri de kişisel veri olarak tanımlanmış; ancak yasalaşırken tüzel kişiler kapsam dışında bırakılmıştır.

<sup>42</sup> **Taştan**, 42; **Eraslan Türkmen**, s. 17.

bilgi kişinin nasıl muamele göreceğini ya da nasıl değerlendirileceğini belirlemede kullanılıyorsa kişiye ilişkindir<sup>43</sup>.

Yukarıda anılan madde metnindeki tanıma göre tüzel kişilerin bilgileri KVKK kapsamında kişisel veri olarak kabul edilmemektedir<sup>44</sup>. KVKK'nın 2008 ve 2014 tarihli tasarılarında tüzel kişilerin bilgilerinin de kişisel veri olabileceği düzenlenmiş; ancak tasarılar yasalaşırken tüzel kişilerin bilgileri kapsam dışında bırakılmıştır<sup>45</sup>.

Diğer yandan 95/46/EC sayılı Direktif'te "gerçek kişi (*natural person*)" ifadesi kullanılmasına karşın; AB üye devletlerinin, iç hukukta benimsediği veri koruma kanunları aracılığıyla 95/46/EC sayılı Direktif'in uygulama alanını geniş tutarak tüzel kişilerin bilgilerini de kişisel veri olarak kabul etmelerinin önünde bir engel bulunmamaktaydı<sup>46</sup>. Örneğin İsviçre<sup>47</sup> ve İzlanda'nın<sup>48</sup> verilerin korunmasına ilişkin düzenlemelerinde tüzel kişilerin bilgilerinin de koruma altına alındığı görülmektedir<sup>49</sup>. Ayrıca 2002/58/EC sayılı Özel Yaşamın ve Elektronik İletişimin Korunması

---

<sup>43</sup> 29. Madde Çalışma Grubu, 10107/05/EN-WP 105 numaralı çalışması (*Working document on data protection issues related to RFID technology*), s. 8, erişim için bkz.: [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp105\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp105_en.pdf), erişim tarihi: 08.08.2021.

<sup>44</sup> Ayrıca önemle belirtmek gerekir ki 24.07.2012 tarihli ve 28363 sayılı Resmî Gazete'de yayımlanan Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik'in 3. maddesinde kişisel veri "Belirli veya kimliği belirlenebilir gerçek ve tüzel kişilere ilişkin bütün bilgiler" olarak tanımlanmaktayken; 04.12.2020 tarihli ve 31324 sayılı Resmî Gazete'de yayımlanan Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik'in üçüncü maddesinde kişisel veri "Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi" olarak tanımlanmıştır.

<sup>45</sup> **Küzeci**, Kişisel Verilerin Korunması, s. 316; **Börekçi**, Eşref Barış, *Kişisel Verileri Verme, Yayma veya Ele Geçirme Suçu*, On İki Levha Yayıncılık, 1. Baskı – İstanbul, Kasım 2020, s. 6; **Üzeltürk**, Sultan, *1982 Anayasası ve İnsan Hakları Avrupa Sözleşmesine Göre Özel Hayatın Gizliliği Hakkı*, Beta Yayıncılık, İstanbul, 2004, s. 103.

<sup>46</sup> **Aksoy**, s. 19.

<sup>47</sup> İsviçre Federal Veri Koruma Kanunu (*Federal Act of Data Protection*), İngilizce çevirisine erişim için bkz.:

[https://fedlex.data.admin.ch/filestore/fedlex.data.admin.ch/eli/cc/1993/1945\\_1945\\_1945/20190301/en/pdf-a/fedlex-data-admin-ch-eli-cc-1993-1945\\_1945\\_1945-20190301-en-pdf-a.pdf](https://fedlex.data.admin.ch/filestore/fedlex.data.admin.ch/eli/cc/1993/1945_1945_1945/20190301/en/pdf-a/fedlex-data-admin-ch-eli-cc-1993-1945_1945_1945-20190301-en-pdf-a.pdf), erişim tarihi: erişim tarihi: 27.06.2021. Kanun'un 3. maddesinin b bendinde veri süjesi "verisi işlenen gerçek veya tüzel kişi" olarak tanımlanmıştır.

<sup>48</sup> İzlanda Veri Koruma Kanunu (*The Data Protection Act*), İngilizce çevirisine erişim için bkz.: <https://www.personuvernd.is/information-in-english/greinar/nr/438/forum>, erişim tarihi: 27.06.2021. Kanun'un 6. maddesinin 3. paragrafında kanun hükümlerinin tüzel kişilerin finansal ve kredi itibarı ile ilgili verilerinin işlenmesi halinde de uygulanacağı düzenlenmektedir.

<sup>49</sup> **Küzeci**, Kişisel Verilerin Korunması, s. 324-325; **Akgül**, s. 14. Avrupa İnsan Hakları Sözleşmesi'nin "Özel Hayata ve Aile Hayatına Saygı" başlıklı 8. maddesi bağlamında, tüzel kişiler de koruma görmektedir. Bunun yanında 95/46/EC sayılı Direktif'le, taraf ülkelere tüzel kişilerin bilgilerinin de kişisel veri olarak tanınıp tanımayacağı konusunda serbestlik tanınmıştır. 95/46/EC sayılı Direktif'in 24. maddesi: "Kendilerini ilgilendiren verileri işlemeye dair tüzel kişilerin korunmasına ilişkin mevzuat, bu Direktiften etkilenmez."

Direktifi'nde (*Directive on Privacy and Electronic Communications*)<sup>50</sup> de tüzel kişilerin bilgileri koruma kapsamına alınmıştır<sup>51</sup>. Ancak burada önemle belirtmek gerekir ki 2002/58/EC sayılı Direktif, kişisel verilerin korunmasına yönelik ilkeleri telekomünikasyon sektöründe benimseyen bir düzenlemedir. 2002/58/EC sayılı Direktif'in 1. maddesinin 2. fıkrasına göre; “tüzel kişiliğe sahip abonelerin yasal çıkarlarının korunması” söz konusudur. Bu anlamda koruma kapsamına tüzel kişilerin de dahil edilmesindeki amaç, abonelerin tüzel kişi olması halinde yasal çıkarlarının korunmasıdır ve bu düzenlemeye bakıldığında AB'nin veri koruma sisteminin bütününde tüzel kişilerin koruma kapsamına alındığını söylemek mümkün değildir<sup>52</sup>. Nitekim Avrupa Birliği Adalet Divanı<sup>53</sup>, 09.11.2010 tarihli bir kararında<sup>54</sup> tüzel kişilerin kişisel verilerin korunması hakkında yararlanamayacağına hükmetmiştir. GDPR'da da buna paralel bir şekilde yalnızca gerçek kişilerin kişisel verisi olabileceği düzenlenmiştir<sup>55</sup>.

Diğer yandan, TCK'nın 135. maddesinin gerekçesinde “Gerçek kişiyle ilgili her türlü bilgi, kişisel veri olarak kabul edilmelidir.” ifadelerine yer verilerek kişisel verinin gerçek kişiye ilişkin olması gerektiği belirtilmiştir. Farklı görüşte yazarlar, kişisel verinin kapsamının TCK'da belirtilmemiş olması nedeniyle suçun mağdurunun hem gerçek kişi hem de tüzel kişi olabileceğini savunmaktadır<sup>56</sup>. Kanaatimce insan hakkını korumayı temel felsefe olarak belirleyen ve kaynağını temel hak ve özgürlüklerden alan kişisel verilerin korunması düzenlemelerinin tüzel kişileri de koruması, bu düzenlemelerin doğası ile bağdaşmamaktadır<sup>57 58</sup>. Kaldı ki anılan suçla ihlal edilen menfaat, diğer bir ifadeyle kişisel verilerin korunması hakkı, gerçek kişilere tanınmış bir haktır. Ne var ki

<sup>50</sup> Çalışmanın devamında “2002/58/EC sayılı Direktif” olarak isimlendirilecektir.

<sup>51</sup> 2002/58/EC sayılı Direktif'e erişim için bkz.: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN>, erişim tarihi: 07.08.2021.

<sup>52</sup> Aynı yönde görüş için bkz.: **Küzeci**, *Kişisel Verilerin Korunması*, s. 317.

<sup>53</sup> Çalışmanın devamında “ABAD” olarak isimlendirilecektir.

<sup>54</sup> ABAD, *Volker ve Markus Schecke ve Hartmut Eifert v. Land Hessen*, Birleştirilmiş Davalar, Dava No: C-92/09 ve C-93/09, 09.11.2010, erişim için bkz.: <https://curia.europa.eu/juris/document/document.jsf?docid=79001&doclang=en>, erişim tarihi: 10.08.2021.

<sup>55</sup> **Voigt**, Paul/**Bussche**, Axelvondem, *The EU General Data Protection Regulation (GDPR)*, SpringerLink, İsviçre, 2017, s. 21.

<sup>56</sup> Bu yönde görüş için: **Akgül**, s. 15; **Şen**, Ersan, *Ceza Hukuku Perspektifinden Güncel Olaylara Bakış*, Yorumluyorum – 1, Seçkin Yayıncılık, Ankara, 2011, (**Şen**, *Ceza Hukuku*), s. 202.

<sup>57</sup> Aynı yönde görüş için bkz.: **Küzeci**, *Kişisel Verilerin Korunması*, s. 317; **Dülger**, *Kişisel Verilerin Korunması*, s. 171.

<sup>58</sup> Tüzel kişilerin verilerinin kişisel verilerin korunması mevzuatı çerçevesinde korunmasının olumlu ve olumsuz yanları için bkz.: **Walden**, I. N. / **Savage**, R. N., “Data Protection and Privacy Laws: Should Organizations Be Protected?”, *International and Comparative Law Quarterly*, 1988, Cilt 37, Sayı 2, ss. 337-347, s. 341 vd.

AYM, henüz KVKK yürürlüğe girmeden önce vermiş olduğu 04.12.2014 tarihli bir kararında Anayasa'nın 20. maddesinin 3. fıkrasında yer alan “Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir” hükmünde gerçek-tüzel kişi ayrımı yapılmaması nedeniyle tüzel kişilerin de koruma kapsamında olduğunu belirtmiştir<sup>59</sup>. Ancak ilgili kararın karşıoy gerekçesinde de belirtildiği üzere, “herkes” ifadesinin gerçek-tüzel kişi özelinde değil, vatandaşlık, dil, din veya cinsiyet temelinde istisna olmaksızın her birey olacak şekilde anlaşılması gerekmektedir. Sonuç olarak, KVKK'nın yürürlüğe girmesiyle birlikte tüzel kişilerin bilgilerinin kişisel veri olarak nitelendirilip nitelendirilemeyeceği tartışmaları da son bulmuştur.

Konu ile ilgili bir diğer önemli husus, ticari sır niteliğindeki bilgilerin akıbetidir. Ticari sır genel anlamda “Bağımsız bir değeri olan veya iktisadi faaliyetlerde sahibi lehine bir rekabet avantajı sağlayan, aleni olmayan (sadece sınırlı bir çevrede bilinen) ve sahibinin gizli kalmasını istediği her türlü bilgi” olarak tanımlanabilir<sup>60</sup>. Bu itibarla kişisel verilerin korunması düzenlemeleri özel hayatı korumaktadır ve tüzel kişiler açısından bir özel hayat söz konusu olmadığından, kişisel verilerin korunmasından değil, ticari sırların (gizliliğin) korunmasından söz edilebilir<sup>61</sup>. Nitekim KVKK'nın 1. maddesine göre de KVKK'nın amaçlarından birisinin “Kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ...” olduğu belirtilmiştir.

Tüzel kişilerin bilgileri aracılığıyla gerçek bir kişiye ulaşılması mümkünse bu bilgiler de kişisel veri olarak kabul edilmektedir<sup>62</sup>. Örneğin isim.soyisim@şirketismi.com olan bir e-posta adresi şirket bilgisiyken, aynı zamanda e-posta adresini kullanan kişiyi belirlenebilir kılması halinde bir kişisel veri olacaktır. Kişisel Verileri Koruma Kurumu da buna benzer bir ifadeyle bir şirketin ticaret unvanı ya da adresi gibi tüzel kişiliğe ilişkin

<sup>59</sup> AYM'nin 2013/83 E., 2014/183 K. sayılı ve 04.12.2014 tarihli kararına erişim için bkz.: <https://www.lexpera.com.tr/resmi-gazete/metin/anayasa-mahkemesinin-4-12-2014-tarihli-ve-e-2013-84-k-2014-183-sayili-karari>, erişim tarihi: 24.09.2021.

<sup>60</sup> **Bilge**, Mehmet Emin, *Ticari Sırların Korunması*, Asil Yayın, 2. Baskı, Ankara 2005, s. 5.

<sup>61</sup> **Tezcan**, Durmuş, “*Bilgisayar Karşısında Özel Hayatın Korunması*”, Anayasa Yargısı 8, Anayasa Mahkemesinin 29.Kuruluş Yıldönümü Sempozyumu, 25 – 27 Nisan 1991, Ankara, ss. 385-392, s. 389.

<sup>62</sup> Aynı yönde bkz.: **Başalp**, *Kişisel Verilerin Korunması*, s. 26; **Küzeci**, *Kişisel Verilerin Korunması*, s. 318; **Şimşek**, Oğuz, s. 123; **Aksoy**, s. 19-20, **Taştan**, s. 29-30; **Dülger**, *Kişisel Verilerin Korunması*, s. 172; **Özcan**, s. 10; 29. Madde Çalışma Grubu'nun 04/2007 sayılı görüş yazısı (*on the concept of personal data*), s. 23-24.

bilgilerin kişisel veri sayılmayacağını belirtmiş; ancak bu bilgilerin gerçek bir kişiyle ilişkilendirilebilecekleri durumları hariç tutmuştur<sup>63</sup>.

Açıklığa kavuşturulması gereken bir diğer husus ise ölü ve cenine ilişkin bilgilerin kişisel verilerin korunması alanına dahil olup olamayacağı hususudur. 4721 sayılı Türk Medeni Kanunu'nun<sup>64</sup> 28. maddesi uyarınca “*Kişilik, çocuğun sağ olarak tamamıyla doğduğu anda başlar ve ölümlle sona erer.*” Dolayısıyla kişinin tam ve sağ olarak doğumuyla birlikte kişisel verilerinin korunması hakkı gündeme gelecektir. Kişilik ölümle ortadan kalktığından dolayı kural olarak ölümle birlikte kişisel verilerin korunması hakkı sona erecektir<sup>65</sup>. Dolayısıyla kural olarak ölmüş kimselerin kişisel verilerin korunması hakkı yoktur. Ancak bu kuralın istisnası olarak Kişisel Sağlık Verileri Hakkında Yönetmelik'in<sup>66</sup> 11. maddesinde ölmüş kişilerin de sağlık verisine sahip olabileceği belirtilmiştir<sup>67</sup>. GDPR'da ise ölmüş kişilerin kişisel verilerinin korunması ile ilgili düzenleme yapılabilmesi konusunda üye devletlere imkân tanınmıştır<sup>68</sup>. Örneğin İngiltere Veri Koruma Kanunu'nda (Data Protection Act) yalnızca hayatta olan kişilerin kişisel verilerinin korunacağını düzenlenmişken<sup>69</sup>, Kanada Gizlilik Kanunu'nda (Privacy Act) ölmüş kişilerin kişisel verilerinin ölüm tarihinden itibaren 20 yıllık süre ile “*kişisel veri*” olarak nitelendirileceği belirtilmiştir<sup>70</sup>.

---

<sup>63</sup> Kişisel Verileri Koruma Kurumu, *6698 Sayılı Kişisel Verilerin Korunması Kanununun Uygulanmasına Yönelik Soru Cevaplar*, s. 17-18, erişim için bkz.: <https://www.kvkk.gov.tr/yayinlar/6698%20SAYILI%20K%C4%B0%C5%9E%C4%B0SEL%20VER%C4%B0LER%20KORUNMASI%20KANUNUNUN%20UYGULANMASINA%20Y%C3%96NEL%20SORU%20VE%20CEVAPLAR.pdf>, erişim tarihi: 19.06.2021.

<sup>64</sup> 08.12.2001 tarihli ve 24604 sayılı Resmî Gazete'de yayımlanan 4721 sayılı Türk Medeni Kanunu. Çalışmanın devamında “TMK” olarak isimlendirilecektir.

<sup>65</sup> **Doğan**, Buse, *Kişisel Verilerin İşlenme Şartları Bağlamında Açık Rıza*, Yayımlanmamış Yüksek Lisans Tezi, T.C. İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk Anabilim Dalı, İstanbul, 2019, s. 27.

<sup>66</sup> 21.06.2019 tarihli ve 30808 sayılı sayılı Resmî Gazete'de yayımlanan Kişisel Sağlık Verileri Hakkında Yönetmelik.

<sup>67</sup> Anılan yönetmeliğin ilgili maddesi:

“Ölünün sağlık verilerine erişim

**MADDE 11 – (1)** Ölmüş bir kimsenin sağlık verilerini almaya, veraset ilamını ibraz etmek suretiyle murisin yasal mirasçıları münferit olarak yetkilidir.”

(2) Ölmüş bir kimsenin sağlık verileri, en az 20 yıl süre ile saklanır.

<sup>68</sup> **Develioğlu**, Hüseyin Murat, *6698 Sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku*, On İki Levha Yayıncılık, İstanbul, 2017, s. 32.

<sup>69</sup> İngiltere Veri Koruma Kanunu'nun (Data Protection Act) 3. maddesinin 2. fıkrası. İlgili kanuna erişim için bkz.: <https://www.legislation.gov.uk/ukpga/2018/12/section/3/enacted>, erişim tarihi: 08.08.2021.

<sup>70</sup> Kanada Gizlilik Kanunu'nun (Privacy Act) 3. maddesi. İlgili kanunun İngilizce çevirisine erişim için bkz.: <https://laws-lois.justice.gc.ca/eng/acts/p-21/fulltext.html>, erişim tarihi: 08.08.2021.

Son olarak, hayatta olsun ya da olmasın gerçek bir kişi ile ilişkilendirilemeyen bilgiler anonim bilgi olarak kabul edilmiş ve KVKK'da koruma altına alınmamıştır<sup>71</sup>. KVKK'nın 3. maddesinin 1. fıkrasının b bendine göre anonim hale getirme “*Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesini*” ifade etmektedir. Dolayısıyla anonim hale getirilen bir bilgi artık gerçek kişiyle ilişkilendirilemiyorsa, kişisel verinin unsurlarından “*bilginin gerçek kişiye ilişkin olması*” ve “*kimliği belirli veya belirlenebilir kişinin varlığı*” unsuru sağlanamayacak, artık bir kişisel veriden söz edilemeyecektir.

### **1.1.2.3. Kimliği Belirli veya Belirlenebilir Kişinin Varlığı**

Kişisel verinin son unsuru, kimliği belirli veya belirlenebilir kişinin varlığıdır. Şöyle ki öncelikle bir bilgi var olmalı, sonrasında bu bilgi gerçek bir kişiye ilişkin olmalı, nihayetinde bu gerçek kişinin kimliği belirli veya belirlenebilir olmalıdır. Bir bilginin, kullanılması makul olan tüm araçların kullanılması sonucunda herhangi bir kişiyi belirlenebilir kılması durumunda bu unsur sağlanmış olur<sup>72</sup>.

Kişinin belirli olması, kişinin ayırt edilebilmesidir<sup>73</sup>. Bir bilgiden, basit ve olağan bir bağlantıyla bilginin bağlantılı olduğu kişinin kim olduğu anlaşılabilir ise *belirli bir kişiden* bahsedilebilir<sup>74</sup>. Örneğin ad, soyadı, kimlik numarası veya adres içeren bilgiler kullanılarak bir kişinin kimliği doğrudan ortaya çıkarılabiliyorsa bu durumda anılan bilgiler belirli bir kişiye ilişkin olur<sup>75</sup>.

<sup>71</sup> Aşkoğlu, s. 11; Aydoğdu, Yasin, “*Kamu İdaresinde Kişisel Verilerin Korunması*”, Selçuk Üniversitesi Hukuk Fakültesi Dergisi, 2021, Cilt: 29, Sayı: 1, ss. 263-293, s. 267.

<sup>72</sup> Aksoy, s. 24; Aşkoğlu, s.18; İmançlı, s. 48.

<sup>73</sup> İtişgen, Rezzan, “*Türk Ceza Hukukunda Kişisel Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme Suçu*”, Türkiye Adalet Akademisi Dergisi, 6 (23), 2015, ss. 179-202, s. 183.

<sup>74</sup> Börekçi, s. 12; Sert, s. 31.

<sup>75</sup> Şimşek, Oğuz, s. 122.

Belirlenebilir olma ise kişinin dolaylı veya doğrudan bir ilişkilendirme ile tanımlanabilmesidir<sup>76 77</sup>. Diğer bir ifadeyle ilgili kişinin kimliği doğrudan açığa çıkmıyor; ancak bazı ek bilgilerle ilgili kişi belirli kılınıyorsa bu durumda belirlenebilir bir kişinin varlığından söz edilebilir<sup>78</sup>. Örneğin ikamet ettiği apartman, daire numarası gibi bilgilerden kişinin kimliği belirlenebiliyorsa bu bilgiler kişisel veri olacaktır. Başka bir örnekte; yüz kişinin katılım sağladığı bir toplantı salonunda yalnızca bir kişi yeşil bir takım elbise giymişse, bu toplantı salonunda herhangi birisinin “yeşil takım elbiseli kişi” şeklinde seslenmesi kişinin kimliğini belirlenebilir kılacaktır. Yine, çalışanların katılım sağladığı bir iş toplantısında şirketin genel müdüründen bahsedildiği takdirde toplantıya katılım sağlayan kişilerin gözünde şirketin genel müdürü olan kişi canlanacağından, bu bilgi de bir kişisel veri olacaktır. ABAD, *Breyer v. Almanya* davasında internete her yeni bağlantı yapıldığında değişkenlik gösteren IP adresinin, hizmet sağlayıcı tarafından ek bilgiler kullanılarak (örneğin bir siber saldırıya ilişkin cezai süreç çerçevesinde delil toplanması gibi) ilgili kişinin belirlenebileceğini, bu nedenle IP adresinin kişiyi belirlenebilir kıldığını belirtmiştir<sup>79</sup>. KVKK’nın gerekçesine göre de kişinin adı, soyadı, doğum tarihi gibi kesin teşhisini sağlayan bilgilerin yanında fiziki, sosyal, ailevi, ekonomik vb. özelliklerine ilişkin bilgileri de (örneğin taşıt numarası, özgeçmiş, resim, sosyal güvenlik numarası gibi) kişiyi dolaylı olarak belirlenebilir kılması sebebiyle kişisel veri olabilir<sup>80</sup>.

Belirli veya belirlenebilir olmanın her somut olaya göre ayrıca değerlendirilmesi gerekmektedir<sup>81</sup>. Diğer bir anlatımla, bir bilgi, bir kişi açısından doğrudan ilgili kişiyi belirli veya belirlenebilir kılabilirken; başka bir kişi açısından hiçbir anlam ifade etmeyebilir. Bu durumda herhangi bir kişiyi ifade etmeyen bir bilginin kişisel veri olarak

<sup>76</sup> Ergün, İsmail, *Siber Suçların Cezalandırılması ve Türkiye’de Durum*, Adalet Yayınevi, Ankara, 2008, s. 114; Erarslan Türkmen, s. 17.

<sup>77</sup> Çekin, Mesut Serdar, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku*, On İki Levha Yayıncılık, 2. Baskı, İstanbul, Ekim 2019, s. 42 vd.: Çekin’e göre belirlenebilirlik hususunda yapılan tartışmalar neticesinde mutlak ve nispi olmak üzere iki tür belirlenebilirlik görüşü ortaya atılmıştır. Mutlak belirlenebilirliğe göre, bir verinin kişisel veri niteliğine haiz olup olmadığı belirlenirken bu verinin başkaca bir kişinin elindeki veri ile birlikte anıldığında verinin bir kişiyle bağlantılandırılması esas alınmalı; nispi belirlenebilirlikte ise, sadece veriyi işleyen kişinin kimliği ve bilgisi esas alınmalıdır.

<sup>78</sup> Ayözger Öngün, s. 11; Sert, s. 32-33.

<sup>79</sup> ABAD, *Patrick Breyer / Almanya*, Dava No: C-582/14, 19.10.2016, erişim için bkz.: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0582>, erişim tarihi: 05.10.2021.

<sup>80</sup> KVKK’nın 3. maddesinin gerekçesi. Gerekçeye erişim için bkz.: <https://www2.tbmm.gov.tr/d26/1/1-0541.pdf>, erişim tarihi: 09.08.2021.

<sup>81</sup> Yılmaz, *Kişisel Veriler*, s. 56.



nitelendirilmesi doğru olmayacaktır. Diğer yandan, yaygın bir ada ve soyada sahip olan bir kişiye ilişkin olarak, yalnızca bu bilgilere yer verilmesi, onu her zaman için belirlenebilir kılmayacaktır<sup>82</sup>. Örneğin elli kişinin katılım sağladığı bir sınavda aynı ada ve soyada sahip üç öğrencinin olduğu varsayımında, sınav sonucu ilan edilirken bu öğrencilerin yalnızca adına ve soyadına yer verilmesi, ilgili kişiyi belirli veya belirlenebilir kılmak için yeterli olmayacaktır. Dolayısıyla somut örnekte ilgili kişinin yalnızca adı ve soyadı, onu belirli veya belirlenebilir kılmayacağından, kişisel veri olarak nitelendirilmeyecektir. Ancak bu bilgileri destekleyici bilgilerin de bulunması durumunda kişinin adı veya soyadı kişisel veri olarak nitelendirilebilir.

### 1.1.3. Özel Nitelikli Kişisel Veriler

Özel nitelikli kişisel veriler KVKK'nın “*Özel nitelikli kişisel verilerin işlenme şartları*” başlıklı 6. maddesinin 3. fıkrasında sınırlı sayıda (*numerus clausus*) belirtilmiştir. Buna göre “*Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri*” özel nitelikli kişisel veridir. Bu bilgilerin, üçüncü kişiler tarafından öğrenilmesi durumunda ilgili kişi hakkında ayrımcılık yapılmasına veya ilgili kişinin mağdur olabilmesine sebebiyet verebilecek nitelikte olduğu görülmektedir<sup>83 84</sup>.

<sup>82</sup> **Küzeci**, Kişisel Verilerin Korunması, s. 9.

<sup>83</sup> Kişisel Verileri Koruma Kurumu, *Özel Nitelikli Kişisel Verilerin İşlenme Şartları*, s. 2, erişim için bkz.: <https://kvkk.gov.tr/SharedFolderServer/CMSFiles/fae2e7c8-f24f-457f-a71d-2d5ed599cf15.pdf>, erişim tarihi: 20.06.2021; KVKK 6. maddesinin gerekçesi, gerekçeye erişim için bkz.: <https://www2.tbmm.gov.tr/d26/1/1-0541.pdf>, erişim tarihi: 15.08.2021; **Dülger**, Murat Volkan, *Bilişim, Kişisel Verilerin Korunması ve İnternet İletişimi Mevzuatı*, Seçkin Yayıncılık, 4. Baskı, İstanbul, 2018, (**Dülger**, Bilişim), s. 665; **Özdemir**, Hayrunnisa, *Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması*, Seçkin Yayıncılık, Ankara, 2009, (**Özdemir**, Elektronik Haberleşme), s. 126; **Akgül**, s. 18; **Başalp**, Kişisel Verilerin Korunması, s. 43; **Özcan**, s. 14; **Dursun**, Yonca, *Kişisel Verilerin Korunması Kanunu Kapsamında İşçinin Korunması*, Seçkin Yayıncılık, 1. Baskı, Ocak 2021, s. 28.

<sup>84</sup> 29. Madde Çalışma Grubu'nun 20.04.2011 tarihli Özel Veri Kategorisine İlişkin Tavsiye Belgesi'nde (*Advice Paper on Special Categories of Data “Sensitive Data”*) birtakım verilerin özel nitelikli kişisel veri olarak düzenlenmesine sebep olan nedenin, bu türden verilerin kötüye kullanımının insanlar üzerinde diğer “normal” veri türlerinin kötüye kullanımından daha uzun süreli ve geri dönüşü olmayan nitelikte etki bırakabileceğini belirtmiştir, erişim için bkz.: [https://ec.europa.eu/justice/article-29/documentation/other-document/files/2011/2011\\_04\\_20\\_letter\\_artwp\\_mme\\_le\\_bail\\_directive\\_9546ec\\_annex1\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf), s. 12, dn. 5, erişim tarihi: 19.06.2021.

Özel nitelikli kişisel verilerin korunmasına ilişkin gereklilik büyük ölçüde II. Dünya Savaşı ve sonrasında ortaya çıkmıştır. Bu dönemde kişilerin belirli bir ırk, renk, uyruk veya kökene sahip olduğu için ayrımcılık görmesi, kişilerin birtakım bilgilerinin diğer bilgilerine oranla daha hassas bir şekilde korunması ihtiyacını ortaya çıkarmış, dolayısıyla da özel nitelikli kişisel verilerin korunmasına yönelik ek düzenlemeler yapılmasını zorunlu kılmıştır<sup>85</sup>.

Her ne kadar TCK'nın 136 ve 137. maddelerinde ayrıma gidilirse de 135. maddesinin 2. fıkrasında “*kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine, hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin verilerinin kaydedilmesi*” durumunda verilecek cezanın artırılacağı düzenlenmiştir. Bu bağlamda özel nitelikli kişisel verilerin özel olmayan nitelikteki kişisel verilere nazaran daha çok korunmaya çalışıldığını söylemek mümkündür<sup>86</sup>. Nitekim KVKK'da bu bilgilerin kullanılma koşulları diğer bilgilerin kullanılma koşullarına kıyasla daha dar tutulmuştur<sup>87</sup>. Özel nitelikli kişisel verilerin korunmasında ek koşullar getirilmesindeki temel düşünce, diğer kişisel verilere kıyasla ilgili kişiye daha fazla zarar verme durumunun mevcut olmasıdır<sup>88</sup>.

Uluslararası düzenlemelerde ise “*özel nitelikli kişisel veri*” kavramının yerine “*özel veri kategorisi*”, “*hassas bilgi*”, “*özel türde bilgi*”, “*hassas kişisel veri*” kavramlarının kullanıldığı görülmektedir<sup>89</sup> 90. Örneğin ırksal köken, siyasi düşünce, din veya diğer inançları ortaya koyan, sağlık, cinsel hayat veya ceza mahkumiyeti ile ilgili olan kişisel

---

<sup>85</sup> **Erarslan Türkmen**, s. 43-44.

<sup>86</sup> Federal Almanya Anayasa Mahkemesi 1983 yılında vermiş olduğu bir kararında kişisel verilerin tamamının önemli olduğunu, bunların “önemliler” ve “daha az önemliler” şeklinde bir sınıflandırmaya tabi tutulmasının yanlış olduğunu, başlangıçta tehlike taşımayan bir bilginin, geçirdiği işlemler neticesinde önemli bir bilgi haline gelebileceğini, ayrıca, kişisel veriler arasında bu şekilde bir ayırım yapıldığı takdirde özel nitelikli olmayan kişisel verilerin tam korunmadığı sonucunun ortaya çıkabildiği, basit bir bilginin otomatik işleme sistemleri ile oldukça hassas bir nitelik kazanabileceğini, bu nedenle özel nitelikli kişisel verilere diğer verilere kıyasla ek güvence getirilemeyeceğini belirtmiştir. Akt: **Küzeci**, *Kişisel Verilerin Korunması*, s. 245-246.

<sup>87</sup> KVKK'nın 6. maddesinin 3. fıkrasına göre “*Sağlık ve cinsel hayat dışındaki özel nitelikli 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 finansmanın planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir.*”

<sup>88</sup> **Korkmaz**, İbrahim, “*Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme*”, TBB Dergisi 2016 (124), (**Korkmaz**, Değerlendirme), ss. 81-152, s. 113.

<sup>89</sup> **Akgül**, s. 17-18.

<sup>90</sup> KVKK'daki terminoloji açısından farklılık olmaması için çalışmanın devamında bu tür bilgiler “*özel nitelikli veri*” olarak isimlendirilecektir.

veriler 108 sayılı Sözleşme'nin 6. maddesinde “*Özel veri kategorileri*” başlığı altında düzenlenmiştir. Diğer yandan 95/46/EC sayılı Direktif'in “*Özel İşleme Kategorileri-Verilerin özel işleme kategorileri*” başlıklı 8. maddesinde kişilerin sağlık durumu, cinsel yaşamı, sendika üyeliği, dini veya felsefi inançları, siyasi görüşü, ırk veya etnik kökeni ile ilgili verilere yer verildiği görülmektedir. Son olarak GDPR'ın “*Özel veri kategorilerindeki kişisel verilerin işlenmesi*” başlıklı 9. maddesinde ırk veya etnik köken, siyasi görüşler, din veya felsefi inançlar, sendika üyeliği, genetik ve biyometrik veriler, sağlık, cinsel yaşam ve cinsel yönelim kategorilerinin bulunduğu görülmektedir.

ABAD'ın 06.11.2003 tarihli *Lindqvist v. İsveç* kararında “*hassas*” kişisel verilerin yorumlanmasının geniş bir şekilde yapılması gerektiği belirtilmiştir<sup>91</sup> <sup>92</sup>. Buna karşın henüz KVKK yürürlüğe girmeden önce AYM tarafından verilmiş 2015 yılına ait bir kararda “...*biyometrik yöntemlerle kimlik doğrulaması yapılması suretiyle elde edilen bilgilerin kişisel veri olduğu; ancak 108 sayılı Sözleşme'nin 6. maddesi uyarınca çok hassas verilerden olmadığı...*” belirtilmiştir<sup>93</sup>. Ancak KVKK'nın yürürlüğe girmesiyle birlikte biyometrik verinin bir özel nitelikli kişisel veri olarak sınıflandırılmasında şüphe bulunmamaktadır. Nitekim Kişisel Verileri Koruma Kurulu da 01.12.2020 tarihli ve 2020/195 sayılı<sup>94</sup>, 27.02.2020 tarihli ve 2020/167 sayılı<sup>95</sup>, 31.05.2019 tarihli ve

<sup>91</sup> ABAD, *Bodil Lindqvist v. İsveç*, Dava No: C-101/01, 6.11.2003, karara erişim için bkz.: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62001CJ0101&from=EN>, erişim tarihi: 19.06.2021.

<sup>92</sup> Karara konu olayda Bodil Lindqvist, sadece kendisinin ve iş yerinden arkadaşlarının bağlantı adresi verilmek suretiyle erişebildiği kişisel hobi amaçlı bir internet sitesi kurmuş, bu internet sitesinde çalıştığı iş yeri ile ilgili bilgilerin yanında, arkadaşlarının adları ve çalıştıkları iş yerleri gibi kişisel verilere de yer vermiştir. Bodil Lindqvist, bir arkadaşına ait sağlık bilgilerini de internet sitesinde paylaşmış; ancak geri bildirimler üzerine bu içeriği kaldırmıştır. Aleyhine açılan davada Bodil Lindqvist, internet sitesinin ticari kaygı gütmeyeceğini ve kişisel amaçlı olduğunu belirtse de davayı gören bölge mahkemesi Avrupa Adalet Divanı'ndan görüş talep etmiştir. Avrupa Adalet Divanı ise vermiş olduğu görüşte “kişisel verilerin internet ortamında belirsiz sayıda kişilere işlenmesinin kişisel faaliyet kapsamına giremeyeceğini” belirtmiştir. Ayrıca söz konusu dava ile ilgili detaylı bilgi için bkz.: **Gültekin Várkonyi**, Gizem, “*Avrupa Birliği Genel Veri Koruma Tüzüğü Kapsamında Gerçek Kişilerin Kişisel Sosyal Robot Kullanımından Doğabilecek Sorumlulukları*”, *Kişisel Verileri Koruma Dergisi*, Cilt: 2, Sayı: 2, ss. 19-29, s. 24 ve 25.

<sup>93</sup> AYM'nin 2014/180 E., 2015/30 K. sayılı ve 19.03.2015 tarihli kararı, erişim için bkz.: <https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2015/30?EsasNo=2014%2F180>, erişim tarihi: 15.08.2021.

<sup>94</sup> Kişisel Verileri Koruma Kurulu'nun “*Belediyede memur olarak görev yapan ilgili kişinin, veri sorumlusu bünyesinde işe giriş çıkış takibinin biyometrik veri işlenerek yapılması*” ile ilgili 01.12.2020 tarihli ve 2020/915 sayılı karar özetine erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/6872/2020-915>, erişim tarihi: 20.06.2021.

<sup>95</sup> Kişisel Verileri Koruma Kurulu'nun “*Spor salonu hizmeti sunan veri sorumlusunun, üyelerinin giriş-çıkış kontrolünü biyometrik veri işleyerek yapması*” ile ilgili 27.02.2020 tarihli ve 2020/167 sayılı karar özetine erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/6738/2020-167>, erişim tarihi: 20.06.2021.

2019/165<sup>96</sup> sayılı kararlarında parmak izi tanıma, avuç içi tarama, el geometrisi tanıma, iris tanıma, yüz tanıma, retina tanıma, DNA tanıma gibi yöntemlerle elde edilen biyometrik bilgilerin özel nitelikli kişisel veri olduğunu belirtmiştir. Diğer yandan Kişisel Verileri Koruma Kurulu, “*Biyometrik imza verisinin kullanılmasına ilişkin görüş talebi*” ile ilgili olarak yayınlamış olduğu 27.08.2020 tarihli ve 2020/649 sayılı kararında fizyolojik nitelikli ve davranışsal biyometrik veri ayrımına gitmiş; bu ayrımda fizyolojik nitelikli biyometrik verileri, “*insan vücudunun benzersiz özelliklerini içeren veriler (örneğin iris, retina, parmak izi gibi)*” olarak tanımlamış; davranışsal biyometrik verileri ise “*...zaman, ruh hali, yaş ve benzeri faktörlere göre değişebilen dinamik yapıda özelliklere ilişkin veriler (örneğin yürüyüş biçimi, klavyeye basış şekli, akıllı cihazları kullanırken uyguladığı basınç ve basış şekli, araba sürüş biçimi gibi)*” olarak tanımlamıştır<sup>97</sup>. Kurul, kararın devamında biyometrik imzayı “*...analizinde, biyometrik imza esnasında uygulanan basıncın miktarı, yazma açısı, kalemin hızı ve ivmesi, harflerin oluşumu, imzanın yönü ve benzer diğer kişinin sahip olduğu benzersiz dinamik özellikler kullanılması sebebiyle*” davranışsal biyometrik veri olarak kabul etmiştir<sup>98</sup>. Önemle belirtmek gerekir ki “*biyometrik veri*” ifadesinin tanımını KVKK’da yer almamaktadır. Ancak GDPR’ın 4. maddesinin 14. fıkrasına göre “*Biyometrik veri; yüz görüntüsü veya daktiloskopik veri gibi benzersiz tanıtıcılarla bir bireyin fiziksel, psikolojik veya davranışsal özelliklerine ilişkin olan tüm verileri*” ifade etmektedir.

Özel nitelikli kişisel verilerin sınırlı bir şekilde belirtilmesi, konuya ilişkin olarak tereddütlerin tam anlamı ile ortadan kalkmasını sağlamamaktadır<sup>99</sup>. Bu doğrultuda özel nitelikli kişisel veriler açısından üzerinde durulması gereken bir diğer konu, bu kategoriye dâhil olan veri türlerinin nasıl değerlendirilmesi gerektiğidir. Örneğin bir kişinin gözlüklü bir fotoğrafı o kişinin sağlık durumuna yönelik bir bilgi içerebilir<sup>100</sup>. Bu durumda

---

<sup>96</sup> Kişisel Verileri Koruma Kurulu’nun “*Spor salonu hizmeti sunan veri sorumlularının, üyelerinin giriş-çıkış kontrolünü biyometrik veri işleyerek yapması*” ile ilgili 31.05.2019 tarihli ve 2019/165 sayılı karar özetine erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/5496/2019-81-165>, erişim tarihi: 20.06.2021.

<sup>97</sup> Kişisel Verileri Koruma Kurulu’nun “*Biyometrik imza verisinin kullanılmasına ilişkin görüş talebi*” ile ilgili ile ilgili 27.08.2020 tarihli ve 2020/649 sayılı karar özetine erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/6815/2020-649>, erişim tarihi: 20.06.2021.

<sup>98</sup> Kişisel Verileri Koruma Kurumu’nun biyometrik verileri ele aldığı başka bir rehberi için ayrıca bkz.: *Biyometrik Verilerin İşlenmesinde Dikkat Edilmesi Gereken Hususlara İlişkin Rehber*, erişim adresi: <https://kvkk.gov.tr/SharedFolderServer/CMSFiles/bd06f5f4-e8cc-487e-abe1-d32dc18e2d7e.pdf>, erişim tarihi: 29.09.2021.

<sup>99</sup> **Dülger**, *Kişisel Verilerin Korunması*, s. 178.

<sup>100</sup> **Küzeci**, *Kişisel Verilerin Korunması*, s. 244 ve 352.

yapılacak değerlendirmede kanaatimizce somut olay çerçevesinde kişisel verinin niteliğinin yanında işlenme amacının da dikkate alınması gerekir. Örneğin söz konusu fotoğraftan eğer ki kişinin gözlük kullanımına ve dolayısıyla sağlığına ilişkin bir sınıflandırma yapılıyor ise bu durumda özel nitelikli kişisel verinin varlığından söz edilebilir. Benzer bir şekilde başka bir örnekte, iş başvurusu yapan bir kişinin isminin “Muhammet” olduğu varsayımında, kişinin ismi, onun dini inancı hakkında bilgi verebilecek nitelikte olabilir. Bu durumda kişinin ismi ile ilgili olarak dini inancına yönelik çıkarımlarda bulunuluyor veya bu yönde veri işleniyor ise özel nitelikli kişisel veriden bahsetmek mümkün olacaktır<sup>101</sup>. Avrupa Konseyi de bir kişinin video görüntüsünün kayda alınmasına ilişkin somut olayda, eğer kişinin hassas verilerinin açığa çıkarılması amacı güdülyorsa hassas veri işlemenin, ancak yalnızca güvenlik amacı güdülyorsa hassas olmayan veri işlemenin söz konusu olduğunu belirtmiştir<sup>102</sup>.

Özel nitelikli kişisel veriler açısından ele alınması gereken bir diğer önemli konu, yalnızca Türk hukukunda özel nitelikli kişisel veri olan “*kılık ve kıyafete ilişkin*” bilgilerdir. Bu kategoriye ait kişisel veriler gerçekten belirsizdir<sup>103</sup>. TDK’da kılık kavramı “*Bir kimsenin giyinişi, dış görünüşü, üst baş*” olarak; kıyafet kavramı “*Giysi*” olarak; kılık kıyafet kavramı ise “*Üst baş ve dış görünüş, kisve*” olarak tanımlanmıştır<sup>104</sup>. Görüleceği üzere kılık ve kıyafete ilişkin bilgilerin kapsamı oldukça geniştir. Dolayısıyla KVKK’nın özel nitelikli kişisel verilerin işlenmesine yönelik katı kuralları dikkate alındığında bu kuralların kılık ve kıyafete ilişkin her türlü bilgi açısından uygulanması, günlük yaşantıda amacını aşan bir yorumlamaya sebebiyet verebilir. Örneğin bir hazır giyim firmasının müşterilerinin alışverişlerine yönelik bilgilerin kılık ve kıyafete ilişkin bilgiler olarak sınıflandırılması veya bir işverenin çalışanına koruyucu kıyafet ve donanım teslim ederken, çalışanın beden ölçüsünü “*medium*”, “*large*” şeklinde işlemesi halinde özel nitelikli kişisel verilerin gündeme gelmesi gerçekten özel nitelikli kişisel verilerin korunması amacını aşar nitelikte olacaktır<sup>105</sup>. Kanaatimizce kılık ve kıyafete ilişkin

---

<sup>101</sup> Dülger, Kişisel Verilerin Korunması, s. 180.

<sup>102</sup> Avrupa Konseyi’nin Kişisel Verilerin Otomatik İşlenmesine İlişkin Kişilerin Korunmasına İlişkin Sözleşmede Değişiklik Yapan Protokole İlişkin Açıklayıcı Rapor’u (*Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*), erişim için bkz.: <https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a>, erişim tarihi: 18.09.2021.

<sup>103</sup> Dülger, Kişisel Verilerin Korunması, s. 180.

<sup>104</sup> TDK, Güncel Türkçe Sözlük, erişim için bkz.: <https://sozluk.gov.tr/>, erişim tarihi: 09.08.2021.

<sup>105</sup> Dülger, Kişisel Verilerin Korunması, s. 180.

kişisel verilerin özel nitelikli kişisel veri grubundan çıkarılmasına ilişkin KVKK'da bir değişiklik yapılması veya Kişisel Verileri Koruma Kurulu tarafından tereddütlere yer vermeyecek şekilde kılık ve kıyafete ilişkin bilgilerden ne anlaşılması gerektiğine yönelik bir karar yayınlanması; kılık ve kıyafete ilişkin verilerin işleme süreçleriyle ilgili kural ve şartların herkes tarafından kolaylıkla anlaşılması adına oldukça yerinde olacaktır.

Son olarak, yetkili merciler tarafından yapılacak değerlendirmelerde kişisel verilerin özel nitelikli olsun veya olmasın her somut olay çerçevesinde “*ihlal edildiği takdirde ortaya çıkan risk ve sonuçlar*”ın esas alınması gerektiğini, buradan hareketle “*özel nitelikli - diğer*” ayrımının yanı sıra bilginin türü, bununla ulaşılabilecek diğer bilgiler ve somut olayda ihlalin yarattığı etki gibi kriterlerin gözetilmesi gerektiğini düşünmekteyiz<sup>106</sup>. Pek tabii yukarıdaki kişisel veriler, kişinin etnik kökeni, felsefi inancı, dini veya mezhebi, sağlığı<sup>107</sup> yönünden sınıflandırılmasına veya ayrımcılık görmesine sebebiyet veriyorsa özel nitelikli kişisel veri olarak yorumlanmalıdır<sup>108</sup>.

## 1.2. Kişisel Verinin İşlenmesi

### 1.2.1. Kişisel Verinin İşlenmesinin Tanımı

Kişisel verinin işlenmesi KVKK'nın 3. maddesinin 1. fıkrasının e bendinde “*Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin<sup>109</sup> parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem.*”

<sup>106</sup> Benzer yönde görüş için bkz.: **Küzeci**, Kişisel Verilerin Korunması, s. 250.

<sup>107</sup> Örneğin bir işverenin çalışanına koruyucu kıyafet vermesi; hamile bir çalışanına hamileler için üretilmiş bir kıyafet temin etmesi durumunda özel nitelikli kişisel verilerden sağlık verisinin gündeme gelmesi muhtemeldir.

<sup>108</sup> **Dülger**, Kişisel Verilerin Korunması, s. 180.

<sup>109</sup> KVKK'nın 3. maddesinin 1. fıkrasının h bendinde veri kayıt sistemi “*Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistem*” olarak tanımlanmıştır.

olarak tanımlanmıştır. Kişisel Sağlık Verileri Hakkında Yönetmelik'in<sup>110</sup> 4. maddesinin 1. fıkrasının 1 bendinde de aynı tanım bulunmaktadır. Bu doğrultuda, kişisel verinin işlenmesinden, KVKK'da sayılan işleme tür ve örnekleriyle sınırlı olmaksızın, bir kişisel veri üzerinde gerçekleştirilecek her türlü işlem anlaşılmaktadır<sup>111</sup>.

95/46/EC sayılı Direktif'in 2. maddesine göre işleme “...otomatik ya da otomatik olmayan her türlü yöntemi içermekte olup kişisel verilerin toplanması, elde edilmesi, kaydedilmesi, organize edilmesi, saklanması, değiştirilmesi, okunması, sorulması, kullanılması, transfer yoluyla başkalarına verilmesi, yayılması ya da hazır bulundurulması için yapılan işlemlerle bunların yanı sıra verilerin birleştirilmesi ya da ilişkilendirilmesi ve hatta bloke edilmesi, silinmesi ya da yok edilmesi suretiyle gerçekleştirilen her türlü işlemi...” ifade etmektedir<sup>112</sup>. 95/46/EC sayılı Direktif'in yerini alan GDPR'a göre ise işleme, “Kişisel veri ya da bir takım kişisel veriler üzerinde; otomatik olsun ya da olmasın aktarım, yayma veya diğer yollarla elde edilebilir hale getirme, sıraya koyma, birleştirme, sınırlama, silme veya yok etme suretiyle toplama, kayıt etme, düzenleme, yapılandırma, depolama, uyumlaştırma, değiştirme, geri kazanma, danışma, kullanma, açıklama gibi herhangi bir işlemde ya da bir takım işlemlerde bulunma...”yı ifade etmektedir<sup>113</sup>.

Burada öncelikle otomatik işleminin üzerinde durulması gerekmektedir. KVKK'da ve mehz alınan Direktif'te otomatik işlemeye dair herhangi bir tanım bulunmamaktadır. Rehber İlkeler'de otomatik işleme “İnsan müdahalesi ya da yardımı konusundaki ihtiyacı asgari seviyeye indiren, kendi aralarında bağlantılı ve etkileşimli elektrikli veya elektronik bir sistem tarafından gerçekleştirilen veri işleme...” olarak tanımlanmıştır<sup>114</sup>

---

<sup>110</sup> 21.06.2019 tarihli ve 30808 sayılı sayılı Resmî Gazete'de yayımlanan Kişisel Sağlık Verileri Hakkında Yönetmelik, erişim için bkz.: <https://www.resmigazete.gov.tr/eskiler/2019/06/20190621-3.htm>, erişim tarihi: 29.09.2021.

<sup>111</sup> **Taştan**, s. 46; **Başalp**, Kişisel Verilerin Korunması, s. 33; **Çekin**, s. 46.

<sup>112</sup> 95/46/EC sayılı Direktif'in erişim için bkz.: <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>, erişim tarihi: 12.08.2021.

<sup>113</sup> GDPR'a erişim için bkz.: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1374-1-1>, erişim tarihi: 12.08.2021.

<sup>114</sup> OECD Kişisel Verilerin Sınırşan Trafiği ve Verilerin Korunmasına İlişkin Rehber İlkeler (*Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*), erişim için bkz.: <https://www.oecd.org/digital/ieconomy/oecdguidelinesontheprivacyandtransborderflowsofpersonaldata.htm#part1>, erişim tarihi: 12.08.2021.

<sup>115</sup>. 108 sayılı Sözleşme’de de otomatik işleme “*Bir bütün veya parçalar halinde otomatik araçlarla gerçekleştirilmesi halinde aşağıdaki işlemleri içerir; verileri saklama, bu veriler üzerinde mantıksal ve/veya aritmetik işlemlerin gerçekleştirilmesi, verilerin değiştirilmesi, silinmesi, verilerin saklama yerlerinden geri alınarak/kurtarılarak yeniden kullanılması veya yayınlanması.*” şeklinde tanımlanmıştır<sup>116</sup>. Diğer yandan, KVKK’nın gerekçesinde “*Günümüzde bu veriler ... bilişim sistemleri üzerinden otomatik yollarla sıkça kullanılmaktadır.*” ifadelerine yer verilmiştir. Bu anlamda otomatik işlemenin esasında bilişim sistemleri üzerinden gerçekleştirilen faaliyetler olduğu anlaşılmaktadır<sup>117</sup>.

*Otomatik olmayan işleme* ise otomatik işleme dışında kalanlardır. Otomatik olmayan veri işlemenin KVKK kapsamına dahil olabilmesi için veri kayıt sisteminin bir parçası olması gerekmektedir. Örneğin; gelişigüzel şekilde yazılmış ve bir kenara atılmış bilgiler açısından KVKK hükümlerinin uygulama alanı olmayacaktır<sup>118</sup>. Nitekim söz konusu işleme otomatik olmayan yöntemlerle yapılmasına karşın, herhangi bir veri kayıt sisteminin parçası değildir.

### 1.2.2. Kişisel Verinin İşlenmesinde Benimsenen Genel İlkeler

Kişisel verinin işlenmesinde benimsenen genel ilkeler, bütün veri işleme süreçlerinde uyulması gereken ilkelerdir<sup>119</sup>. KVKK’nın “*Genel ilkeler*” başlıklı 4. maddesine göre kişisel veriler işlenirken “*hukuka ve dürüstlük kurallarına uygun olunmalı*”, “*belirli, açık ve meşru amaçlar için işleme yapılmalı*”, “*işleme amacıyla bağlantılı, sınırlı ve ölçülü olunmalı*”, “*muhafaza için mevzuatta süre öngörülen veya işleme amacıyla orantılı süre*

---

<sup>115</sup> Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin Korunması Kanunu’na İlişkin Uygulama Rehberi*, KVKK Yayınları No:1, Aralık 2019, Ankara, s. 54, erişim için bkz.: <https://kvkk.gov.tr/Icerik/2030/Rehberler>, erişim tarihi: 30.05.2021.

<sup>116</sup> 108 Sayılı Sözleşme’ye erişim için bkz.: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108?module=treaty-detail&treatynum=108>, erişim tarihi: 12.08.2021.

<sup>117</sup> Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin Korunması Kanunu’na İlişkin Uygulama Rehberi*, s. 54.

<sup>118</sup> Kişisel Verileri Koruma Kurumu, *6698 sayılı Kişisel Verilerin Korunması Kanunu Hakkında Doğru Bilinen Yanlılar*, KVKK Yayınları No:13, Nisan 2020, Ankara, s. 14, erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/6722/6698-Sayili-Kisisel-Verilerin-Korunmasi-Kanunu-Hakkinda-Dogru-Bilinen-Yanlislar>, erişim tarihi: 22.08.2021.

<sup>119</sup> **Küzeci**, *Kişisel Verilerin Korunması*, s. 335.



*belirlenmeli ve uyulmalı” ve “veriler doğru ve güncel tutulmalı”*dır. Anılan ilkeler birbirleri ile ilişkili, adeta birbirine kaynak olan ilkelerdir ve birbirlerini tamamlayıcı fonksiyonlara sahiptir<sup>120</sup>. Hatta öyle ki, kimi zaman bu ilkelerin birbirinden ayırt edilebilmesi de güçtür<sup>121</sup>. Kişisel verinin özel nitelikli olup olmaması, genel ilkelere uygun olma açısından önemli değildir. Kişisel veri özel nitelikli olsa da olmasa da işlenirken genel ilkelere uygun davranılması gerekmektedir. Bu ilkelere aykırı hareket edildiği takdirde veri işleme faaliyeti de hukuka aykırı olacaktır<sup>122</sup>.

Kişisel verinin işlenmesinde benimsenen genel ilkeler, kişisel verilerin korunmasını düzenleyen ulusal ve uluslararası belgelerde farklılık gösterebilse de temel anlamda birbiri ile paralellik göstermektedir<sup>123</sup>. KVKK’da bulunan genel ilkeler büyük ölçüde 108 sayılı Sözleşme ve 95/46/EC sayılı Direktif’e uygun şekilde düzenlenmiştir<sup>124</sup>.

### **1.2.2.1. Hukuka ve Dürüstlük Kurallarına Uygun Olma**

Kişisel verinin işlenmesinde benimsenen genel ilkelerden ilki *“hukuka ve dürüstlük kurallarına uygun olma”*dır. Bu ilke, ilerleyen başlıklarda yer alan diğer genel ilkelere kaynaklık etmesi ve bu ilkeleri de kapsamaması nedeniyle birincil ilke olarak değerlendirilmektedir<sup>125</sup>. Hukuka uygunluk ve dürüstlük kriterleri ayrı ayrı ele alınmalıdır.

Hukuka uygunluktan anlaşılması gereken, yalnızca konuya ilişkin özel norm niteliğindeki hükümlere değil; genel olarak hukuk normlarına ve evrensel hukuk ilkelerine uygunluktur<sup>126</sup>. Dolayısıyla hukuka uygunluk kavramının kapsamı oldukça geniş olup, mevzuata uygunluk da bu kapsama dahil edilebilir<sup>127</sup>. Örneğin çalışmanın II. bölümünde

---

<sup>120</sup> **Oğuz**, Sefer, “*Kişisel Verilerin Korunması Hukukunun Genel İlkeleri*”, Bilgi Ekonomisi ve Yönetim Dergisi, 2018, 13:2, ss. 121-138, s. 129.

<sup>121</sup> **Küzeci**, *Kişisel Verilerin Korunması*, s. 199.

<sup>122</sup> **Çekin**, s. 61.

<sup>123</sup> **Dülger**, *Kişisel Verilerin Korunması*, s. 260.

<sup>124</sup> *Kişisel Verileri Koruma Kurumu, Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler*, s. 1, erişim için bkz.: <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/32ff74f6-9798-405a-b3d2-b42d28423fde.pdf>, erişim tarihi. 16.08.2021.

<sup>125</sup> **Küzeci**, *Kişisel Verilerin Korunması*, s. 200; **Akgül**, s. 126; **Özdemir**, *Elektronik Haberleşme*, s. 137.

<sup>126</sup> **Küzeci**, *Kişisel Verilerin Korunması*, s. 200; **Dülger**, *Kişisel Verilerin Korunması*, s. 263; *Kişisel Verileri Koruma Kurumu, Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler*, s. 2.

<sup>127</sup> *Kişisel Verileri Koruma Kurumu, Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler*, s. 2.

detaylıca ele alınan ve kendine özgü (*sui generis*) bir hukuka uygunluk nedeni niteliğinde olan KVKK'nın veri işleme şartlarına aykırılık da hukuka aykırılığı beraberinde getirmektedir.

Dürüstlük kuralına uygunluk değerlendirmesi yapılırken ise kişisel verinin işleme amacı, şekli ve işlenmenin kendisinin dürüstlük kuralına uygun olup olmaması gibi birden fazla etkenin gözetilmesi gerekmektedir<sup>128</sup>. Veri işleme sürecinin en başından en sonuna kadar devam eden tüm aşamalarında, ilgili kişinin menfaatlerinin, çıkarlarının ve makul beklentilerinin orantılılık prensibi çerçevesinde dikkate alınması gerekmektedir<sup>129</sup>. Bilhassa tarafların çatışan menfaatleri söz konusu olduğunda menfaatlerin dengelenmesi açısından dürüstlük kurallarına uygun olunması oldukça önemlidir<sup>130</sup>.

KVKK'daki dürüstlük kurallarına uygun olma ilkesi, TMK'nın 2. maddesinde<sup>131</sup> düzenlenen dürüstlük kuralının karşılığı olarak ifade edilebilir ise de<sup>132</sup>; bu ilke yalnızca medeni hukuk anlamında değil, hukukun tüm dallarında geçerli bir ilkedir<sup>133</sup>. Örneğin açık rıza ile elde edilen kişisel verinin, rıza kapsamı dışındaki amaçlar için herhangi bir bilgilendirme yapılmadan işlenmesi dürüstlük kuralına aykırılık teşkil edecektir.

Kişisel Verileri Koruma Kurulu 01.10.2019 tarihli ve 2019/294 sayılı kararında “*Veri sorumlusunun kimlik görüntüsünün muhafaza edilmesine rağmen kayıt altına alınmadığı yönünde ilgili kişiye cevap vermesinden dolayı şeffaf olmadığı, bu nedenlerle de dürüstlük kuralına aykırı veri işleme faaliyetinde bulunduğu...*” ifadelerine yer vererek şeffaf olmamayı da bir dürüstlük kuralı ihlali olarak nitelendirmiştir<sup>134</sup>. Dolayısıyla dürüstlük

<sup>128</sup> Erarşlan Türkmen, s. 92-93.

<sup>129</sup> Taranto, Lill, “*Data Protection Principles*”, European Privacy: Law and Practice for Data Protection Professionals, ed.: Eduardo Ustran, IAPP publication, USA, 2012; s.58; Bygrave, Lee A., *Data Privacy Law An International Perspective*, Oxford University Press, The United Kingdom, 2014, s. 147; Küzeci, *Kişisel Verilerin Korunması*, s. 201-213; Akdağ, s. 72; Aşıkoğlu, s. 75. Köse Aysun, s. 84.

<sup>130</sup> Küzeci, *Kişisel Verilerin Korunması*, s. 201-202; Çekin, s. 64; Doğan, s. 44.

<sup>131</sup> TMK m. 2: “*Herkes, haklarını kullanırken ve borçlarını yerine getirirken dürüstlük kurallarına uymak zorundadır. Bir hakkın açıkça kötüye kullanılmasını hukuk düzeni korumaz.*”

<sup>132</sup> Özdemir, *Elektronik Haberleşme*, s. 138; Akdağ, s. 71-72; Taştan, s. 49; Dülger, *Kişisel Verilerin Korunması*, s. 264 vd.

<sup>133</sup> Çekin'e göre ise TMK'nın 2. maddesindeki dürüstlük kuralı ile KVKK'daki dürüstlük kuralı eş anlamlı olmayıp; veri sorumlularının işleme faaliyetinde KVKK'dan doğan haklarını adil kullanmaları gereklidir. Çekin, s. 64; Erarşlan Türkmen, s. 92.

<sup>134</sup> *Kişisel Verileri Koruma Kurulu'nun 01.10.2019 tarihli ve 2019/294 sayılı karar özetine erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/6556/2019-294>, erişim tarihi: 20.06.2021.*

kurallarına uygun olma ilkesi şeffaflığı da içerisinde barındıran bir ilke olarak değerlendirilmelidir<sup>135</sup>.

Kişisel Verileri Koruma Kurulu bu ilke ile ilgili olarak başka bir kararında; “*Şirket tarafından ilgili kişinin telefon numarasına aynı içerikteki mesajların farklı tarihlerde birden fazla gönderilmesini veri sorumlusunun sahip olduğu hakkın kötüye kullanımı olarak değerlendirilmesi ve bu durumun hukuka ve dürüstlük kurallarına uygun olma ilkesine aykırılık teşkil etmesi hususları göz önünde tutularak..*” ifadelerine yer vererek bu ilkenin hakkın kötüye kullanımı ile ilişkisine değinmiş, hakkın kötüye kullanımını hukuka ve dürüstlük kurallarına uymama olarak nitelendirmiştir<sup>136</sup>. Dolayısıyla dürüstlük kuralı, hakkın kötüye kullanılmamasını da içerisinde barındırmaktadır<sup>137</sup>. Diğer yandan, TCK’da yer alan hakkın kullanılması hukuka uygunluk nedeninin de bir sonucu olarak hakkın kötüye kullanılmaması gerekmektedir. Kişisel Verileri Koruma Kurulu’nun bu kararından yola çıkılarak, kişisel verinin işlenmesi için geçerli bir hukukî neden bulunsa dahi dürüstlük kurallarına aykırı bir şekilde veri işlemenin KVKK’ya da aykırı olduğu sonucuna ulaşılması mümkündür<sup>138</sup>.

Yine Kişisel Verileri Koruma Kurulu Facebook aleyhine vermiş olduğu bir kararda “*Açık rızanın özgür irade ile açıklanması gerekirken, ilgili kişinin açık rızasının alınmasının, bir ürün veya hizmetin sunulmasının ya da ürün veya hizmetten yararlandırılmasının ön şartı olarak ileri sürülmesini*” hukuka ve dürüstlük kurallarına aykırılık olarak nitelendirmiştir<sup>139</sup>.

### 1.2.2.2. Belirli, Açık ve Meşru Amaçlar İçin İşleme

Benimsenen genel ilkelerden ikincisi “*belirli, açık ve meşru amaçlar için işleme*”dir. Bu ilke uyarınca, kişisel veri işlenirken keyfî davranışlarda bulunulmasından

<sup>135</sup> Develioğlu, s. 44-45.

<sup>136</sup> Kişisel Verileri Koruma Kurulu’nun 31.05.2019 tarihli ve 2019/159 sayılı karar özetine erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/5494/2019-159>, erişim tarihi: 20.06.2021.

<sup>137</sup> Özdemir, Elektronik Haberleşme, s. 138.

<sup>138</sup> Göçmen Uyarer, Sinem, *Kişisel Verilerin Korunması kanunu ve Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması*, Seçkin Yayıncılık, Güncellenmiş 2. Baskı, Ankara 2020, s. 124.

<sup>139</sup> Kişisel Verileri Koruma Kurulu’nun 11.04.2019 tarihli ve 2019/104 sayılı karar özetine erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/5450/2019-104>, erişim tarihi: 20.06.2021.

kaçınılmalıdır<sup>140</sup>. Kişisel verinin işlenmesindeki amaçlar bir bakıma işleme sürecinin varlık sebebini ihtiva etmektedir<sup>141</sup>. Kişisel verinin elde edilmesi, kullanılması, arşivlenmesi ve hatta silinmesi de bir veri işleme olduğundan, bu ilke kişisel veri işleme süreçlerinin tamamını kapsamaktadır<sup>142</sup>. Kişisel veri işleme amaçlarının belirsiz olması ya da yeterince açık olmaması, kişilerin kişisel verileri üzerindeki denetim ve kontrol yetkisini azaltacağından, anılan ilke kişisel verinin işlenmesi konusunda uyulması gereken en önemli ilkeler arasında yer almaktadır<sup>143</sup>. Ancak bu ifadeden, diğer genel ilkelerin önemsiz olduğu sonucuna ulaşılmamalıdır.

Bu ilke kapsamında, elde edilen kişisel verinin işleme amacının niteliğinin değerlendirilmesi gerekmektedir. Kişisel veri işleme amacı belirli, somut, anlaşılır ve ilgili kişiyi tereddüde düşürmeyecek şekilde olmalıdır<sup>144</sup>. Kişiyi şüpheye düşürebilecek muğlak veya kapsamı çok geniş olan amaçlarla kişisel veri işlenmemelidir. Örneğin bir işverenin “*özlük dosyası oluşturmak*” amacıyla çalışanından almış olduğu kişisel verilere yönelik olarak; bu bilgileri tek tek hangi amaçla aldığını (SGK bildirimlerinin yapılması, acil durum yönetim süreçlerinin yürütülmesi, eğitim kayıtlarının tutulması, iş sağlığı ve güvenliği mevzuatından kaynaklanan yükümlülüklerin yerine getirilmesi gibi) belirtmesi gerekmektedir. Başka bir örnekte, bir firmanın “*reklam ve pazarlama amaçlı*” veya “*araştırma amaçlı*” kişisel veri işlediği durumlarda reklam ve pazarlamanın veya araştırmanın neyi hedeflediğini açıklaması gerekmektedir<sup>145</sup>.

Diğer yandan kişisel veriler, ilk işleme amacıyla uyumsuz bir şekilde ve ileride ortaya çıkabilecek muhtemel veri işleme süreçleri için işlenmemelidir<sup>146</sup>. Örneğin bir kargo firmasının, taşınan eşyanın teslim edilmemesi halinde göndericiye geri dönüş yapıp göndericiyi durumdan haberdar edebilmek için aldığı cep telefonu numarasını satış veya

---

<sup>140</sup> **Börekçi**, s. 49.

<sup>141</sup> 29. Madde Çalışma Grubu'nun 03/2013 sayılı görüş yazısı (*on purpose limitation*), erişim için bkz.: [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf), erişim tarihi: 20.06.2021, s. 11; **Yücedağ**, Nafiye, “*Kişisel Verilerin Korunması Kanunu Kapsamında Genel İlkeler*”, *Kişisel Verileri Koruma Dergisi*, Cilt:1, Sayı:1, ss. 47-63, (**Yücedağ**, Genel İlkeler), s. 49.

<sup>142</sup> **Küzeci**, *Kişisel Verilerin Korunması*, s. 202.

<sup>143</sup> **Göçmen Uyarer**, s. 126; **Şimşek**, Oğuz, s. 83.

<sup>144</sup> **Şimşek**, Oğuz, s. 84.

<sup>145</sup> **Çekin**, s. 66.

<sup>146</sup> *Kişisel Verileri Koruma Kurumu, Kişisel Verilerin Korunması Kanunu Hakkında Sıkça Sorulan Sorular*, KVKK Yayınları, Mart 2018, Ankara, s. 45, erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/4196/Kisisel-Verilerin-Korunmasi-Kanunu-Hakkinda-Sikca-Sorulan-Sorular>, erişim tarihi: 21.08.2021; **Kuner**, Christopher, *European Data Protection Law (Corporate Compliance and Regulation)*, Oxford, Second Edition, 2007, s. 100; **Küzeci**, *Kişisel Verilerin Korunması*, s. 203.

pazarlama amacıyla kullanması, göndericiye reklam amaçlı iletiler göndermesi, veri işleme amacının verinin toplandığı andaki belirsizliğini ve eksikliğini göstermektedir. Nitekim bu örnekte gönderici, verilerinin toplandığı anda bunların reklam amaçlı kullanılacağını bilmemektedir.

Son olarak, kişisel veri meşru amaçlar için işlenmelidir. Amacın meşru olması, işlenen kişisel verinin, işleme amacıyla bağlantılı ve gerekli olması anlamına gelmektedir<sup>147</sup>. Örneğin bir e-ticaret sitesinin, sunmuş olduğu mal ve hizmeti müşterisine ulaştırabilmesi adına müşterisinin adını, soyadını, adresini işlemesi meşru amaç kapsamında değerlendirilebilirken; kan grubu ya da anne kızlık soyadını işlemesi bu kapsamda değerlendirilemeyecektir<sup>148</sup>. Başka bir örnekte; şoför olarak çalışan bir kişinin ehliyet bilgisinin işlenmesi meşru kabul edilebilirken; dini veya felsefi inancı ile ilgili kişisel verilerinin işlenmesi meşru kabul edilemeyecektir<sup>149</sup>.

Kişisel Verileri Koruma Kurulu, “*Şikâyetçinin müşterisi olduğu Bankaya kendisine ait iş ve işlemlerde ulaşılması adına vermiş olduğu telefon numarası bilgisinin, eşine ulaşılmasında yardımcı olunabilmesi adına işlenmesi*”ni belirli, açık ve meşru amaçlar için işleme ilkesine aykırı bulmuştur<sup>150</sup>. Yine Kurul, yayınlamış olduğu başka bir kararda, işlemin gerektirmediği kişisel veri içeren bir belgenin müşteriden istenilmesini belirli, açık ve meşru amaç barındırmaması sebebiyle KVKK’ya aykırı bulmuştur<sup>151</sup>.

<sup>147</sup> KVKK 4. maddenin gerekçesi. Gereğe erişim için bkz.: <https://www2.tbmm.gov.tr/d26/1/1-0541.pdf>, erişim tarihi: 15.08.2021.

<sup>148</sup> Kişisel Verileri Koruma Kurumu, *Örneklerle Kişisel Verilerin Korunması Rehberi*, KVKK Yayınları No:29, Haziran 2019, Ankara, s. 7, erişim için bkz.: <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/a23bfe08-9b3a-4c2f-8a97-a259dcc0e667.PDF>, erişim tarihi: 15.08.2021.

<sup>149</sup> **Özer Deniz**, Miray, “*İşçilerin Özel Nitelikli Kişisel Verilerinin Korunması ve Bundan Doğan Sorumluluk*”, Türkiye Adalet Akademisi Dergisi, Yıl: 12, Sayı: 45, Ocak 2021, ss. 355-378, s. 361.

<sup>150</sup> Kişisel Verileri Koruma Kurulu’nun 18.09.2019 tarihli ve 2019/277 sayılı karar özetine erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/5545/2019-277>, erişim tarihi: 21.06.2021.

<sup>151</sup> Karar tarihi ve numarası anılan kararda belirtilmemiştir. Ancak ilgili karara erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/5417/Kanunda-Yer-Alan-Genel-Ilkelere-Aykiri-Sekilde-Kisisel-Veri-Islenmesi-Hukuka-ve-Durustluk-Kurallarına-Uygun-Oлма-ile-Belirli-Acık-Ve-Mesru-Amaçlar-Icin-Isleme-Ilkelere-Aykiri-Kisisel-Veri-Islenmesi>, erişim tarihi: 21.06.2021.

### 1.2.2.3. İşleme Amacıyla Bağlantılı, Sınırlı ve Ölçülü Olma

Kişisel verinin işlenmesinde benimsenen bir diğer ilke, “İşleme amacıyla bağlantılı, sınırlı ve ölçülü olma”dır. İşleme amacını aşar nitelikte, diğer bir ifade ile gereksiz bir şekilde bilgi toplanması, bu bilginin işleme amacı ile bağlantılı olmayacak bir şekilde kullanılması veya bağlantılı olacak şekilde sınırlandırılmaması genel ilkelere aykırılık teşkil etmektedir.

Bu ilkeye göre, belirlenen amacın gerçekleştirilmesi için kişisel veriyi işlemenin gerekli olup olmadığı ayrıntılı bir şekilde incelenmeli, yalnızca amacın gerçekleşmesi için gerekli olan veriler işlenmelidir<sup>152</sup>. Diğer bir ifade ile hedefe ulaşabilmek açısından, kişisel veriyi işlemek gerekli olmalıdır<sup>153</sup>. Bu ilke, işlenecek veri ile veri işlemede güdülen amaç arasındaki illiyet bağının sağlanmasını hedeflemektedir<sup>154</sup>.

İşleme amacıyla bağlantılı, sınırlı ve ölçülü olma ilkesi aslında üç açıdan ele alınmalıdır. Öncelikle toplanan veri ile veri işleme amacı arasında bağlantının bulunması gerekmektedir. Örneğin bir marketten içecek almak isteyen birisine e-posta adresinin sorulması, amaç ile bağlantılı değildir. İkincil olarak amaçla sınırlı verilerin işlenmesi gerekmektedir. Diğer bir ifade ile amacın gerçekleşmesi için yeterli ölçüde veri işlenmelidir. Örneğin iş başvurularında henüz adaylık statüsünde bulunan bir kişiden nüfus cüzdanı fotokopisinin talep edilmesi, amacın gerçekleşmesi bakımından fazla bilginin talep edilmesi anlamına gelebilir. Son olarak veri işlemenin toplanan veri ile ölçülü olması gerekmektedir. Örneğin bir şirketin, doğrudan doğruya ibadet alanının içerisini kayıt altına alan bir kamera ile veri işlemesi, ölçülü olmayacaktır.

Kişisel Verileri Koruma Kurulu, yukarıda da yer verilen spor salonuna giriş-çıkış yapılmasında biyometrik verilerin işlenmesini konu alan kararında ölçülülük ilkesinin gözetilerek minimum düzeyde veri talep edilmesi gerektiğini vurgulamış, biyometrik verilerin spor salonuna giriş-çıkış takibi amacıyla toplanmasını ölçülülük ilkesine aykırı bulmuştur<sup>155</sup>. Yine Kurul başka bir kararında sadakat programı kapsamında kullanıcı adı

<sup>152</sup> Bygrave, s. 163; Develioğlu, s. 47; Çekin, s. 72; Küzeci, Kişisel Verilerin Korunması, s. 208; Taştan, s. 51.

<sup>153</sup> Başalp, Kişisel Verilerin Korunması, s. 38; Akdağ, s. 77; Köse Aysun, s. 86-87.

<sup>154</sup> Başalp, Kişisel Verilerin Korunması, s. 38; Mutlu, s. 90.

<sup>155</sup> Kişisel Verileri Koruma Kurulu'nun “Spor salonu hizmeti sunan veri sorumlusunun, üyelerinin giriş-çıkış kontrolünü biyometrik veri işleyerek yapması” ile ilgili 27.02.2020 tarihli ve 2020/167 sayılı karar özetine erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/6738/2020-167>, erişim tarihi: 20.06.2021; Kişisel

ve parola bilgilerinin deęiřtirmek isteyen bir kullanıcıdan *kimlik doęrulama iřlemi için daha az verinin iřlenmesi mümkünken* arkalı önlü kimlik görüntüsünün talep edilmesini ölçülülük ilkesine aykırı bulmuřtur<sup>156</sup>.

Anılan ilke GDPR’da veri minimizasyonu ilkesi (*data minimization*) olarak da ifade edilmektedir<sup>157</sup>. Veri minimizasyonu, kiřisel verinin iřlenmesinde yeterli ve minimum miktarla veri kullanma olarak tanımlanabilir<sup>158</sup>. Veri minimizasyonu ilkesi KVKK’da doğrudan bulunmasa da Kiřisel Verileri Koruma Kurulu’nun kararlarında yer verdięi bir ilkedir. Örneęin, Kiřisel Verileri Koruma Kurulu vermiř olduęu bir kararında “*Mahkemeye veri sorumlusundan ilgili kiři hakkında bazı kiřisel verilerin talep edilmesi ve veri sorumlusunun gereęinden fazla kiřisel veri aktarımında bulunması*”nı veri minimizasyonu ilkesine aykırı görmüřtür<sup>159</sup>.

Veri ekonomisi olarak da adlandırılabilen bu ilkeyle, gerekli olandan fazla miktardaki kiřisel verinin iřlenmesinin önüne geçilmektedir<sup>160</sup>. Kiřisel veri iřlemede ilgili kiřinin çıkarlarını tehlikeye düřürecek bir řekilde orantısızlık bulunmamalıdır<sup>161</sup>. Dolayısıyla kiřisel verinin iřlenmesine iliřkin bir sınırlama getirilmektedir<sup>162</sup>. Böylelikle ilgili kiřilerin mümkün olabildięi ölçüde en az riskle karřılařması amaçlanmaktadır<sup>163</sup>.

---

Verileri Koruma Kurulu’nun “*Spor salonu hizmeti sunan veri sorumlularının, üyelerinin giriř-çıkıř kontrolünü biyometrik veri iřleyerek yapması*” ile ilgili 31.05.2019 tarihli ve 2019/165 sayılı karar özetine eriřim için bkz.: <https://www.kvkk.gov.tr/Icerik/5496/2019-81-165>, eriřim tarihi: 20.06.2021.

<sup>156</sup> Kiřisel Verileri Koruma Kurulu’nun “*Bir havayolu tařımacılık řirketinin (veri sorumlusu) sunduęu sadakat programını kullanan ilgili kiřinin kullanıcı adı ve parola bilgilerinin deęiřtirme talebi karřısında ilgili kiřiden arkalı önlü kimlik görüntüsü talep eden veri sorumlusu*” ile ilgili 01.10.2019 tarihli ve 2019/294 sayılı karar özetine eriřim için bkz.: <https://www.kvkk.gov.tr/Icerik/6556/2019-294>, eriřim tarihi: 15.08.2021.

<sup>157</sup> ICO, *Guide to GDPR*, eriřim için bkz.: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/>, eriřim tarihi: 21.06.2021.

<sup>158</sup> **Kuner**, s. 74.

<sup>159</sup> Karar adı ve tarihi Kurul tarafından belirtilmemiřtir. Karara eriřim için bkz.: <https://www.kvkk.gov.tr/Icerik/5413/Islenme-Amacinin-Gerektirdiginden-Fazla-Kisisel-Veri-Islenmesi-Aktarilmasi-Veri-Minimizasyonu-Ilkesine-Aykirilik->, eriřim tarihi: 21.06.2021.

<sup>160</sup> **Küzeci**, *Kiřisel Verilerin Korunması*, s. 208.

<sup>161</sup> **Solove**, Daniel J., “*The New Vulnerability: Data Security and Personal Information*”, GW Law Faculty Publications & Other Works, Faculty Scholarship, 2008, ss. 111-136, s. 117.

<sup>162</sup> **Taranto**, s. 86; **Ařıkoęlu**, s. 75;

<sup>163</sup> **Korkmaz**, İbrahim, *Kiřisel Verilerin Türk Ceza Kanunu Kapsamında Korunması*, Ankara, Seçkin Yayıncılık, 2019, (**Korkmaz**, Ceza Hukuku), s. 118.

#### 1.2.2.4. Mevzuatta Öngörülen veya İşlendikleri Amaç İçin Gerekli Olan Süre Kadar Muhafaza Edilme

Benimsenen genel ilkelerden bir diğeri, “*Mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme*”dir. Bu ilkeye göre; belirli bir amaca yönelik işlenen bir kişisel verinin saklanması ya da imha edilmesi için mevzuatta bir süre varsa, bu süreye uyulması gerekmektedir. Örneğin vergi hukukunda faturaların saklanması için belirli süreler öngörülmüştür<sup>164</sup>. Yine ticaret hukukunda bazı evrakların saklanması için belirli süreler bulunmaktadır<sup>165</sup>. Ek olarak, iş güvenliği mevzuatı açısından sağlık kayıtlarının saklanması için belirli asgari süreler bulunmaktadır<sup>166</sup>. Bu durumda kişisel verinin saklanması açısından mevzuattaki süreler uygulanmalıdır. Eğer kişisel verinin saklanması için mevzuatta belirlenen bir süre mevcut değilse, bu durumda kişisel veri işleme amacı ile orantılı bir süre belirlenmeli<sup>167</sup> ve bu sürenin sonunda kişisel veriler imha edilmelidir. Nitekim KVKK’nın 4. maddesinin gerekçesinde de “*Bir verinin daha fazla saklanması için geçerli bir sebep olmaması durumunda, o veri silinecek veya anonim hale getirilecektir. Gelecekte kullanma ihtimalinin varlığına dayanarak veri*

<sup>164</sup> 12.01.1961 tarihli ve 10705 sayılı Resmî Gazete’de yayımlanan 213 sayılı Vergi Usul Kanunu’nun 253. maddesine göre: “*Bu Kanuna göre defter tutmak mecburiyetinde olanlar, tuttukları defterlerle üçüncü kısımda yazılı vesikaları, ilgili buldukları yılı takibeden takvim yılından başlayarak beş yıl süre ile muhafaza etmeye mecburdurlar.*”

<sup>165</sup> 14.02.2011 tarihli ve 27846 sayılı Resmî Gazete’de yayımlanan 6102 sayılı Türk Ticaret Kanunu’nun 82. maddesine göre her tacir “*ticari defterlerini, envanterleri, açılış bilançolarını, ara bilançolarını, finansal tablolarını, yıllık faaliyet raporlarını, topluluk finansal tablolarını ve yıllık faaliyet raporlarını ve bu belgelerin anlaşılabilirliğini kolaylaştıracak çalışma talimatları ile diğer organizasyon belgelerini on yıl süre ile saklamalıdır.*”

<sup>166</sup> 29.12.2012 tarihli ve 28512 sayılı Resmî Gazete’de yayımlanan İş Sağlığı ve Güvenliği Hizmetleri Yönetmeliği’nin 7. maddesi uyarınca “*İşveren, işten ayrılma tarihinden itibaren en az 15 yıl süreyle çalışanların kişisel sağlık dosyalarını saklar.*”

<sup>167</sup> 30.12.2017 tarihli ve 30286 sayılı Resmî Gazete’de yayımlanan Veri Sorumluları Sicili Hakkında Yönetmelik’in 9. maddesinin 4. fıkrası uyarınca, işlenen amaç için gerekli süre belirlenirken

“*a) İlgili veri kategorisinin işlenme amacı kapsamında veri sorumlusunun faaliyet gösterdiği sektörde genel teamül gereği kabul edilen süre,*

*b) İlgili veri kategorisinde yer alan kişisel verinin işlenmesini gerekli kılan ve ilgili kişiyle tesis edilen hukuki ilişkinin devam edeceği süre,*

*c) İlgili veri kategorisinin işlenme amacına bağlı olarak veri sorumlusunun elde edeceği meşru menfaatin hukuka ve dürüstlük kurallarına uygun olarak geçerli olacağı süre,*

*ç) İlgili veri kategorisinin işlenme amacına bağlı olarak saklanmasının yaratacağı risk, maliyet ve sorumlulukların hukukten devam edeceği süre,*

*d) Belirlenecek azami sürenin ilgili veri kategorisinin doğru ve gerektiğinde güncel tutulmasına elverişli olup olmadığı,*

*e) Veri sorumlusunun hukuki yükümlülüğü gereği ilgili veri kategorisinde yer alan kişisel verileri saklamak zorunda olduğu süre,*

*f) Veri sorumlusu tarafından, ilgili veri kategorisinde yer alan kişisel veriye bağlı bir hakkın ileri sürülmesi için belirlenen zamanaşımı süresi” dikkate alınmalıdır.*



*saklanamayacaktır.*” ifadeleri yer almaktadır. Dolayısıyla a) kişisel verinin işleme amacının ortadan kalkması, b) kişisel verinin işlenmesindeki amaca ulaşma bakımından elverişsiz olması veya c) kişisel veri işleme ile hedeflenen amacın gerçekleşmesi halinde kişisel verinin işlenmesi ile işleme amacı arasındaki nedensellik bağı kesileceğinden, artık kişisel verinin imha<sup>168</sup> edilmesi gerekmektedir<sup>169</sup>. Örneğin siyasi seçim öncesinde bir bölgede bireylerin siyasi tercihini araştıran bir anket şirketi, elde ettiği kişisel verileri seçim sonrasında imha etmelidir<sup>170</sup>. Nitekim artık kişisel veri işleme ile hedeflenen amaç gerçekleşmiştir. Bundan sonraki aşamalar için ilgili kişi, kendisinden toplanan kişisel verilerinin toplanma amacına ulaşıldıktan sonra bilgisi olmaksızın daha önceki toplama amacı dışında başka bir amaç için işlenmeyeceği hususunda güven sahibi olmalıdır<sup>171</sup>.

Mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkesi, TCK’nın 138. maddesinde düzenlenen *“verileri yok etmeme”* suçu ile de yakından ilgilidir. İlgili maddeye göre *“Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediğinde bir yıldan iki yıla kadar hapis cezası verilir.”* Her ne kadar madde metninde *“verileri yok etmeme”* ifadesi belirtilmiş olsa da maddenin gerekçesinden *“veri”* ifadesiyle anlatılmak istenin *“kişisel veri”* olduğu anlaşılmaktadır. Dolayısıyla kişisel verinin imha edilmesi gerekiyorken imha edilmemesi durumunda suçun diğer unsurlarının da varlığı halinde TCK’nın 138. maddesinin uygulanması söz konusu olabilir.

---

<sup>168</sup> İmha; kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi işlemi ifade etmektedir. 28.10.2017 tarihli ve 30224 sayılı Resmî Gazete’de yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik’in 8. maddesine göre *“Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemi”*, 9. maddesine göre *“Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemi”*, 10. maddesine göre *“Kişisel verilerin anonim hale getirilmesi, kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesini”* ifade etmektedir.

<sup>169</sup> **Küzeci**, Kişisel Verilerin Korunması, s. 215; **Taştan**, s. 52; **Korkmaz**, Değerlendirme, s. 104, **ICO**, Guide to GDPR, s. 39-45.

<sup>170</sup> **Börekeçi**, s. 51.

<sup>171</sup> **Şimşek**, Oğuz, s. 85.

### 1.2.2.5. Doğru ve Gerektiğinde Güncel Olma

Kişisel verinin işlenmesinde benimsenen ilkelerden bir diğeri “*Doğru ve gerektiğinde güncel olma ilkesi*”dir. Bu ilke ile amaçlanan, kişisel verinin gerçeğe uygun bir halde ve eksiksiz bir şekilde işlenmesidir<sup>172</sup>. Kişisel verinin doğru olması, kişinin temel hak ve özgürlüklerinin yanında ekonomik menfaati ve manevi bütünlüğünün korunmasını da sağlar<sup>173</sup>. Doğru olmayan kişisel veriler düzeltilmediği veya imha edilmediği takdirde hem kişisel veriyi talep edenin (veri sorumlusunun) hem de ilgili kişinin menfaatlerinin ve ekonomik çıkarlarının zarar görme riski doğabilir<sup>174</sup>. Örneğin müşteri eğiliminin saptanması, istatistikî bilgilerin oluşturulması, kamusal bir işlemin gerçekleştirilmesi, kârlılık oranının artırılması gibi birçok konuda eğer ki doğru olmayan bilgiler esas alınıyorsa ortaya çıkacak sonuç da doğru olmayacak, yanlış bilgilerden hareketle verilecek kararlar zararlara sebep olabilecektir<sup>175</sup>. Ancak esasen bu durum, insan hakkı açısından ilgili kişi aleyhine daha ciddi sonuçlar doğurur. Örneğin bir iş yeri hekimince, çalışanın bulaşıcı hastalığa sahip olduğuna dair tutulan bir kayıt, o çalışanın ayrımcılığa uğramasına sebep olabilir<sup>176</sup>.

Kişisel verinin güncel olmasından kasıt, kişisel verinin artık doğru bir veri olmaması durumunda güncellenmesi gerektiğidir<sup>177</sup>. Burada cevaplanması gereken iki önemli soru vardır. Güncelliğin “*gerektiğinde*” olması nasıl anlaşılmalıdır? Kişisel veriyi doğru ve güncel tutması gereken kimdir? Esasında, “*gerektiğinde*” güncel olma, veri sorumlusunun kendisine yüklenen bir yükümlülüktür. Ancak bu yükümlülüğün “*veri sorumlusunun ilgili kişilerin içerisinde bulunduğu yeni durumları zorla ve sürekli olarak araştırması*” olarak kabul edilmesi makul değildir<sup>178</sup>. Dolayısıyla ilgili kişilerin, kişisel verilerinde bir değişiklik olması halinde bunu veri sorumlusuna bildirmeleri, veri sorumlusunun ise ilgili kişilerin bilgilerini güncelleyebileceği kanallar oluşturması gerekmektedir. Burada bir bakıma veri sorumlusunun aktif özen yükümlülüğü

---

<sup>172</sup> Doğan, s. 45.

<sup>173</sup> Akgül, s. 132; Yücedağ, Genel İlkeler, s. 50.

<sup>174</sup> Develioğlu, s. 48; Küzeci, Kişisel Verilerin Korunması, s. 213; Yücedağ, Genel İlkeler, s. 50; Doğan, s. 46.

<sup>175</sup> Küzeci, Kişisel Verilerin Korunması, s. 213.

<sup>176</sup> Orak, Beşir, *Kişisel Sağlık Verilerinin Korunması*, Yetkin Yayınları, 1. Baskı, Nisan 2020, s. 58.

<sup>177</sup> Erarslan Türkmen, s. 96.

<sup>178</sup> Küzeci, Kişisel Verilerin Korunması, s. 214.

bulunmaktadır<sup>179</sup>. Nitekim Kişisel Verileri Koruma Kurulu 22.12.2020 tarihli ve 2020/966 sayılı bir kararında doğru ve gerektiğinde güncel olma ilkesinin önemine değinerek “*Veri sorumlusunun bu ilke açısından ilgili kişiye verilerini güncelleyebileceği kanallar oluşturması gerektiği*”ni belirtmiştir<sup>180</sup>. Gerçekten, veri sorumlusu tarafından ilgili kişilere bu hususta kendi verilerinin doğruluğunu denetleyici imkanlar verilmelidir<sup>181</sup>. Yukarıdaki açıklamalar doğrultusunda şu sonuca varılabilir: Verileri doğru ve güncel tutması gereken kişi veri sorumlusudur. Ancak veri sorumlusunun sürekli ilgili kişiyle iletişim kurarak bu verilerin güncelliğini takip etmesi ya da ilgili kişi tarafından kendisine iletilen bilgilerin doğruluğu kontrol etmesi objektif olarak her durum için kabul edilemez. Dolayısıyla veri sorumlusu tarafından ilgili kişiye verilerinin güncelliğini ve doğruluğunu denetleyebilme imkânı sağlayan kanalların oluşturulması söz konusudur. Örneğin bir bankanın, cep telefonu uygulamasını kullanan kişinin uygulamaya girmesinden sonra ona “*Kayıtlı cep telefonu numaranız / e-posta adresiniz doğru mu?*” şeklinde belirli aralıklarla bildirim göndermesi bu imkânı sağlamak adına etkili bir yöntemdir.

Önemle belirtmek gerekir ki bazen somut olayın şartları, bilginin “*güncel olmamasını*” gerektirebilir. Örneğin bir yargılama sürecinde delillerin muhafaza edilmesi amacıyla verilerin güncellenmemesi veya güncel olmayan verilerin de saklanması gerekebilir<sup>182</sup>. Başka bir örnekte, zaman damgalı ve arşivleme amacı güdülen saklanan verilerin güncellenmemesi haklı kabul edilebilir<sup>183</sup>. Bu durumda güncel olmanın gerekliliği, mevcut olayın şartlarına göre değişebilmektedir<sup>184</sup>. O halde söylenebilir ki, bir kişisel verinin doğru bir şekilde tutulması *her zaman için* zorunlu iken, güncel bir şekilde tutulması *gerektiğinde* zorunludur<sup>185</sup>.

Kişisel verinin doğru ve gerektiğinde güncel olması, ilgili kişi hakkında başkalarının yanlış bir izlenime sahip olmaması ve bu izlenim nedeniyle ilgili kişi hakkında karar

---

<sup>179</sup> Kişisel Verileri Koruma Kurumu, Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler, s. 6.

<sup>180</sup> Kişisel Verileri Koruma Kurulu’nun 22.12.2020 tarihli ve 2020/966 sayılı ilke kararına erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/6858/2020-966>, erişim tarihi: 21.06.2021.

<sup>181</sup> **Erarslan Türkmən**, s. 96; **Taştan**, s. 50. “*Bir şirketin belirli aralıklarla müşterisine gönderdiği beyanlarda/iletelerde bu bilgilere yer vermesi ve müşteriyi yanlış olan bilgileri düzeltme yolları hakkında yönlendirmesi*” bu denetleyici imkanlara örnek verilebilir, **Küzeci**, Kişisel Verilerin Korunması, s. 214.

<sup>182</sup> **Çekin**, s. 72.

<sup>183</sup> **Aşıkoğlu**, s. 77.

<sup>184</sup> **Aşıkoğlu**, s. 77.

<sup>185</sup> **Dülger**, Kişisel Verilerin Korunması, s. 293.

alınmaması açısından da önemlidir<sup>186</sup>. Nitekim AİHM, avukat olan ve öğrenciyken yazdığı mektuplar nedeniyle mahkûm olan davacının Romanya İstihbarat Servisi tarafından kendisi hakkında tutulan bilgilerin gerçek olmadığını iddia ettiği bir olayda, istihbarat servisi tarafından elli yıldan uzun bir süre ile tutulan bilgilerin yanlış tutulmasını, davacının itibarını zedelemesi nedeniyle AİHS'in 8. maddesinin ihlali olarak görmüştür<sup>187</sup>.

### 1.3. Kişisel Veri İşleme Sürecindeki Süjeler

#### 1.3.1. İlgili Kişi

İlgili kişi, KVKK'nın 3. maddesinin 1. fıkrasının ç bendinde “*Kişisel verisi işlenen gerçek kişi*” şeklinde tanımlanmıştır. İlgili kişi esasen korumanın konusudur<sup>188</sup>. İlgili kişi kavramının karşılığı olarak 95/46/EC sayılı Direktif'te ve GDPR'da “*veri öznesi (data subject)*” ifadeleri kullanılmaktadır<sup>189</sup>.

Kişisel verinin işlenmesi aynı zamanda TCK'nın 136. maddesi açısından suç teşkil ediyorsa bu durumda mağdur ve ilgili kişi aynı olacaktır<sup>190</sup>. Kişisel verinin işlenmesi sürecinde yer alan bu süje için çalışmanın devam eden bölümlerinde konu ile bağlantılı ve uygun bir şekilde ilgili kişi, veri öznesi veya mağdur ifadeleri de tercih edilecektir.

#### 1.3.2. Veri Sorumlusu

Kişisel veri işleme sürecindeki bir diğer süje veri sorumlusudur. Veri sorumlusu, veri işleme faaliyetinin neden ve nasıl yapılacağını, kişisel verinin toplanma yöntemini,

---

<sup>186</sup> Yücedağ, Genel İlkeler, s. 50.

<sup>187</sup> AİHM *Rotaru v. Romania* kararı, başvuru no: 28341/95, karar tarihi: 04.05.2000, karara erişim için bkz.: [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-58586%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-58586%22]}), erişim tarihi: 15.08.2021.

<sup>188</sup> Küzeci, Kişisel Verilerin Korunması, s. 15.

<sup>189</sup> Bygrave, s. 17; Voigt – Bussche, s. 260.

<sup>190</sup> Börekçi, s. 22.

toplanacak kişisel veri türlerini, kişisel verinin işleme amaçlarını, kiminle paylaşılacağını, ne kadar süreyle saklanacağını belirleyen kişidir<sup>191</sup>.

Veri sorumlusu KVKK'nın 3. maddesinin 1. fıkrasının 1 bendinde “*Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi*” şeklinde tanımlanmıştır. 95/46/EC sayılı Direktif ile GDPR'a bakıldığında veri sorumlusunun karşılığı olarak “*data controller*” teriminin kullanıldığı, bu terimin de “*Tek başına veya başkalarıyla birlikte kişisel verilerin işlenmesine ilişkin amaçlar ve yöntemleri belirleyen gerçek veya tüzel kişi, kamu kuruluşu, kurumu veya diğer herhangi bir organ*” şeklinde tanımlandığı görülmektedir<sup>192</sup>.

### 1.3.3. Veri İşleyen

Veri sorumlusu kişisel verileri bizzat işleyebileceği gibi veri işleme sürecinde üçüncü kişilerden de yardım alabilir. Örneğin veri sorumlusu bir şirket, kişisel verilerin arşivlenmesi sürecini arşiv hizmeti sunan başka bir firmaya gördürebilir. Bu hizmeti alan kişi veri sorumlusu, hizmeti veren kişi ise veri işleyendir. Ancak “*hizmet alan her zaman için veri sorumlusu, hizmet veren ise her zaman için veri işleyendir*” şeklinde bir genelleme yapılmamalıdır. Nitekim bir veri işleyen, aynı zamanda veri sorumlusu da olabilir. Örneğin bir muhasebe firması, hizmet verdiği kişi bakımından veri işleyen sıfatıyla hareket etmekteyken, kendi çalışanları bakımından veri sorumlusudur<sup>193</sup>.

Veri işleyen kavramı KVKK'nın 3. maddesinin 1. fıkrasının 2 bendinde “*Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi*” olarak tanımlanmıştır<sup>194</sup>. Dolayısıyla veri sorumlusu ile veri işleyenin

<sup>191</sup> Kişisel Verileri Koruma Kurumu, *Veri Sorumlusu ve Veri İşleyen*, s. 2, erişim için bkz.: <https://kvkk.gov.tr/SharedFolderServer/CMSFiles/31d9c444-27a5-4a75-95b1-1ca9bdb81ea5.pdf>, erişim tarihi: 21.09.2021.

<sup>192</sup> Voigt – Bussche, s. 17.

<sup>193</sup> Kişisel Verileri Koruma Kurumu, *Veri Sorumlusu ve Veri İşleyen*, s. 4.

<sup>194</sup> Benzer tanım GDPR'ın 4. maddesinin 8. fıkrasında da yapılmıştır.

belirlenmesindeki temel ayırt edici unsurun “yetki” ve “adına işleme” olduğu söylenebilir<sup>195</sup>.

## 2. KİŞİSEL VERİLERİN KORUNMASININ HUKUKSAL GELİŞİMİNİN TARİHİ SÜRECİ

### 2.1. Genel Olarak

Her ne kadar kişisel verilerin korunmasına ilişkin hukukî sorunlar özellikle son yüzyılda gündeme gelse de kişilerin kendisine ait bilgilerinin gizli kalmasına veya korunmasına yönelik düşünceleri, diğer bir ifade ile mahremiyeti ve mahremiyetine bağlı çekinceleri oldukça eskiye dayanmaktadır<sup>196</sup>.

Günümüzden neredeyse 2500 yıl öncesinde dahi, sır saklama meselesinin önemli olduğu görülmektedir<sup>197</sup>. Kuşkusuz buna verilecek en iyi örnek, eski Yunan hukukunda bulunan ve değişikliğe uğrasa da halen geçerliliğini koruyan Hipokrat Yemini'dir. Hipokrat Yemini; sağlık çalışanlarının, mesleklerini onurla icra edeceklerine, hastalarının onuruna ve haklarına saygı göstereceklerine, hastaları arasında dil, din, ırk, inanç nedeniyle herhangi bir ayrımcılık yapmayacaklarına ve insan haklarını çiğnemeyeceklerine yönelik bir yemin metni olmasının yanı sıra, hastalarının kendilerine açtığı sırları gizli tutacaklarına yönelik de bir yemin metnidir<sup>198</sup>. Bu anlamda yemin metninin içerisinde insan onuru, insan yaşamı, ayrımcılık yapmama ve sır saklama gibi kişisel verilerin korunmasıyla yakından ilgili değerler de yer almaktadır<sup>199</sup>.

---

<sup>195</sup> **Küzeci**, Kişisel Verilerin Korunması, s. 319.

<sup>196</sup> **Çekin**, s. 5; **Şimşek**, Oğuz, s. 5; **Akgül**, s. 163.

<sup>197</sup> **Yılmaz**, Kişisel Veriler, s. 35.

<sup>198</sup> Türk Tabipleri Birliği'nin de kabul ettiği ve kullandığı Dünya Tabipler Birliği Cenevre Bildirgesi Hekimlik Andı'nın tamamına erişim için bkz.: [https://www.ttb.org.tr/userfiles/files/hekimlik\\_andi.pdf](https://www.ttb.org.tr/userfiles/files/hekimlik_andi.pdf), erişim tarihi: 22.06.2021.

<sup>199</sup> **Yılmaz**, Kişisel Veriler, s. 36; **Şimşek**, Oğuz, s. 5 vd.; **Kolenoğlu**, Mustafa, *Sağlık Mesleği Mensuplarının Sır Saklama ve Suçu Bildirmeme (ihbar) Yükümlülüğü*, Yayımlanmamış Yüksek Lisans Tezi, T.C. İstanbul Üniversitesi Adli Tıp Enstitüsü Sosyal Bilimler Anabilim Dalı, s. 17; **Yağhdere**, Umut Emre, “Sağlık Hukuku Açısından Sır Saklama Yükümlülüğüne Genel Bir Bakış”, Veri Güvenliği ve Kişisel Verileri Koruma Derneği Bülteni, E-Dergi, 1. Sayı, İstanbul, (**Yağhdere**, Sır Saklama Yükümlülüğü), s. 43.

Yakın geçmişte ise teknolojik gelişmelerin kolaylığıyla devlet kurumlarının bireylere ait bilgi bankaları oluşturmaya başladığı görülmektedir. Bunun neticesinde de devletlerin kişisel veriler üzerindeki hakimiyetini sınırlandırıcı tedbirlere ihtiyaç duyulmuştur. Avrupa'daki hukukî düzenlemelere bakıldığında kişisel verilerin korunması alanına dair ilk düzenlemenin temellerinin 1970 yılında "Hessen Planı" etkisinde<sup>200</sup> oluşturulduğu görülmektedir. Bu kapsamda Avrupa'da ilk olarak Almanya'nın Hessen Eyaletine ait 07.10.1970 tarihli Kişisel Verilerin Korunması Kanunu yürürlüğe girmiştir<sup>201</sup>. Bunu takiben İsveç'te yalnızca bilgisayar aracılığı ile işlenen kişisel verilerin korunmasını kapsayan İsveç Veri Koruma Kanunu kabul edilmiştir<sup>202</sup>. Bu sırada Amerika Birleşik Devletleri'nde 31.12.1974 tarihinde Gizlilik Kanunu kabul edilmiştir<sup>203</sup>. Almanya'da ise federal düzeyde ilk düzenleme 28.01.1977 tarihli Federal Veri Koruma Kanunu olmuştur<sup>204</sup>. Devamında Fransa'da 06.01.1978 tarihinde Veri İşleme ve Hürriyetler Kanunu, Avusturya'da ise 18.10.1978 tarihli Federal Kişisel Verilerin Korunması Kanunu 01.01.1980 tarihinde yürürlüğe girmiştir<sup>205</sup>. Bu düzenlemeleri takiben uluslararası alanda da kişisel verilerin korunması ele alınmış; devletlerin uyacağı kurallar oluşturulmaya başlanmıştır. Bu kuralların bazıları devletler için bağlayıcıyken, bazıları yalnızca tavsiye niteliğindedir.

## 2.2. Uluslararası Düzenlemeler

Uluslararası alanda doğrudan kişisel verilerin korunmasına özgülenmiş önemli düzenlemeler bulunmaktadır. Bu düzenlemeler OECD, Avrupa Konseyi, Birleşmiş Milletler Örgütü<sup>206</sup> gibi uluslararası kuruluşlar tarafından yapılmıştır. Diğer yandan 95/45EC sayılı Direktif ile GDPR da uluslararası uygulama alanı bulmuştur.

---

<sup>200</sup> Hessen Planı, merkezi bir veri bankası kurulması planıdır. Bu dönemde Hessen Planı'nın özel hayatın gizliliği hakkı üzerindeki olası sonuçları üzerinde çalışmalar gerçekleştirilmiştir.

<sup>201</sup> Akgül, s. 167.

<sup>202</sup> Akgül, s. 167; Aşıkoğlu, s. 33.

<sup>203</sup> Erişim için bkz.: <https://www.justice.gov/opcl/privacy-act-1974>, erişim tarihi: 30.09.2021.

<sup>204</sup> Çekin, s. 6.

<sup>205</sup> Çekin, s. 6; Saka, Rıza / Çağlayan, Ramazan / Koca, Mahmut, *Avrupa Birliği Hukuku, İdare Hukuku ve Ceza Hukuku Açısından, Kişisel Verilerin İmhası*, Seçkin Yayıncılık, 1. Baskı, 2021 Ocak, s. 22.

<sup>206</sup> Çalışmanın devamında "Örgüt" olarak isimlendirilecektir.

### 2.2.1. OECD Düzenlemeleri

Kişisel verilerin korunmasına dair uluslararası alanda ilk düzenlemenin OECD tarafından hazırlanan Rehber İlkeler olduğu görülmektedir. Rehber İlkeler'in bağlayıcılığı bulunmamaktadır. Ancak bu ilkeler kişisel verilerin korunması hususunun üye devletler için iç hukuklarında yer alacak düzenlemelerde dikkate alınması ile sınır ötesi veri trafiğinin haksız yere engellenmemesi konusunda tavsiye niteliği taşımaktadır<sup>207</sup>. Rehber İlkeler'de, kişisel veri akışının yeni ekonomik ve sosyal alanlar yarattığı, bu akış sırasında bireyin mahremiyet hakkının devletler arasında gözetilerek uyumlu kurallar geliştirilmesinin faydalı olacağı belirtilmiştir<sup>208</sup>. Metinde yer alan temel ilkeler; sınırlı toplama ilkesi, veri kalitesi ilkesi, amacın belirliliği ilkesi, sınırlı kullanım ilkesi, veri güvenliği ilkesi, açıklık ilkesi, bireysel katılım ilkesi ve hesap verilebilirlik ilkesi olarak sıralanabilir<sup>209</sup>.

Rehber İlkeler, uluslararası alanda yapılan ilk önemli girişimin ürünü olması sebebiyle oldukça önemlidir. Nitekim kişisel verilerin korunmasının uluslararası alanda tartışılan bir konu haline gelmesi üzerine, Rehber İlkeler'le bu konuya bir çözüm arayışı getirilmeye çalışılmıştır<sup>210</sup>. Diğer yandan bu ilkelerin belirlenmesinde çeşitli kıtalardan temsilciler de rol oynamıştır. Dolayısıyla kişisel verilerin korunmasına ve işlenmesine yönelik konularda geniş kapsamlı bir uzlaşmayı da barındırması açısından bu ilkeler önemlidir<sup>211</sup>.

Rehber İlkeler her ne kadar bağlayıcı olmasa da devletlere ve topluluklara yön verme anlamında OECD dünyada güçlü bir teşkilattır<sup>212</sup>. Dolayısıyla bu ilkeler, kişisel verilerin korunması alanıyla ilgili bazı ulusal ve uluslararası metinlerin kabul edilmesinde, bu metinlerin içeriğinin oluşturulmasında ve kişisel verilerin korunmasıyla ilgili bir farkındalığın meydana gelmesinde etkili olmuştur<sup>213</sup>. Örneğin Kuzey Amerika'da kanunen bir zorunluluk bulunmamasına rağmen birçok firma bu ilkelere uyacağını beyan

<sup>207</sup> **Küzeci**, *Kişisel Verilerin Korunması*, s. 114; **Köse Aysun**, s. 41-42.

<sup>208</sup> **Hızarcı**, Emine, *6698 sayılı Kişisel Verilerin Korunması Kanununun AB Veri Koruma Hukuku Işığında Değerlendirilmesi*, Yetkin Yayınları, Ankara 2020, s. 21.

<sup>209</sup> Rehber İlkeler, 2. Kısım, 7, 8, 9, 10, 11, 12, 13 ve 14. madde.

<sup>210</sup> **Küzeci**, *Kişisel Verilerin Korunması*, s. 115.

<sup>211</sup> **Küzeci**, *Kişisel Verilerin Korunması*, s. 115.

<sup>212</sup> **Hızarcı**, s. 20.

<sup>213</sup> **Küzeci**, *Kişisel Verilerin Korunması*, s. 115; **Dülger**, *Kişisel Verilerin Korunması*, s. 87.



etmiştir<sup>214</sup>. Ülkemizde de KVKK'nın gerekçesinde belirtilen ilkelere atıfta bulunulması, Rehber İlkeler'in ulusal düzenlemelere hala etki ettiğinin bir göstergesi niteliğindedir<sup>215</sup>. Rehber İlkeler, güncel koşullar gözetilerek 2013 yılında yeniden ele alınmıştır<sup>216</sup>. Düzenlemeye eskisinden farklı olarak gizlilik stratejileri, gizlilik yönetim programları ile veri sızıntılarını bildirme yükümlülüğü dahil edilmiş, denetim mekanizmalarının önemine vurgu yapılmıştır<sup>217</sup>.

### 2.2.2. Avrupa Konseyi Düzenlemeleri

Avrupa Konseyi'nde kişisel verilerin korunması alanıyla ilişkili birden çok düzenlemenin bulunduğu görülmektedir. Bunlardan ilki her ne kadar ayrı ve bağımsız bir hak olarak kişisel verilerin korunması hakkı ele alınmasa da Avrupa İnsan Hakları Sözleşmesi'dir<sup>218</sup>. Sözleşme 04.11.1950 tarihinde kabul edilip 03.09.1953 tarihinde yürürlüğe girmiştir. Avrupa İnsan Hakları Mahkemesi<sup>219</sup> kişisel verilerin korunması hakkını AİHS'in 8. maddesinde düzenlenen “*özel ve aile hayatına saygı hakkı*” çerçevesinde ele almaktadır. AİHS'in 8. maddesi şu şekilde düzenlenmiştir:

#### ***“MADDE 8 Özel ve aile hayatına saygı hakkı***

- 1. Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.*
- 2. Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın*

<sup>214</sup> ABD Teknoloji ve Gizlilik Danışma Kurulu'nun Terörizmle Mücadelede Gizliliği Korunması Raporu (*Report of the Technology and Privacy Advisory Committee -Safeguarding Privacy in the Fight Against Terrorism*), Mart 2004, ABD, erişim için bkz.: <https://cdt.org/wp-content/uploads/security/usapatriot/20040300tapac.pdf>, erişim tarihi: 19.09.2021.

<sup>215</sup> **Küzeci**, Kişisel Verilerin Korunması, s. 116; **Dülger**, Kişisel Verilerin Korunması, s. 87.

<sup>216</sup> OECD *Privacy Framework*, erişim için bkz.: [https://www.oecd.org/sti/ieconomy/oecd\\_privacy\\_framework.pdf](https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf), erişim tarihi: 19.09.2021.

<sup>217</sup> **Küzeci**, Kişisel Verilerin Korunması, s. 117.

<sup>218</sup> Çalışmanın devamında “AİHS” olarak isimlendirilecektir. AİHS'e erişim için bkz.: [https://www.echr.coe.int/documents/convention\\_tur.pdf](https://www.echr.coe.int/documents/convention_tur.pdf), erişim tarihi: 19.09.2021.

<sup>219</sup> Çalışmanın devamında “AİHM” olarak isimlendirilecektir.

*veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir.”*

Madde metninden anlaşılacağı üzere özel ve aile hayatına saygı kapsamında dört alan korunmaktadır. Bu alanlar özel hayat, aile hayatı, kişinin ev yaşamı ve yazışmaları olarak sıralanabilir. Devletin bu hak kapsamında kişilerin özel hayatına, aile hayatına, yazışmalarına ve ev hayatına müdahale etmemek yönünde negatif ve müdahale edilmesini önlemek yönünde pozitif yükümlülüğü bulunmaktadır<sup>220</sup>. Özel hayatın gizliliği ile kişisel verilerin korunması arasındaki ilişki kapsamlı bir şekilde ileride<sup>221</sup> ele alınacağından, burada detaylandırılmayacaktır.

Avrupa Konseyi bünyesinde doğrudan kişisel verilerin korunmasını ele alan düzenlemelerden ilki 108 sayılı Sözleşme'dir<sup>222</sup>. Anılan sözleşme 28.01.1981 tarihinde imzaya açılmış, 01.10.1985 tarihinde yürürlüğe girmiştir. Türkiye de bu sözleşmenin taraflarından birisidir<sup>223</sup>. KVKK'nın genel gerekçesinde, Türkiye'de bu türden bir düzenlemeye neden ihtiyaç duyulduğu detaylı bir şekilde açıklanmış, bu açıklamalar yapılırken 108 sayılı Sözleşme'ye atıf bulunmuş ve 108 sayılı Sözleşme'nin Türkiye tarafından imzalandığı vurgulanmıştır<sup>224</sup>. Bunun yanında KVKK'nın Kişisel Verileri Koruma Kurumu ile Kişisel Verileri Koruma Kurulu'nu ele alan 19. ve 21. maddelerinin gerekçelerinde de 108 sayılı Sözleşme'ye atıfta bulunulmuştur.

108 sayılı Sözleşme, tıpkı Rehber İlkeler gibi 18.05.2018 tarihinde güncel gelişmeler ışığında değişikliğe uğramıştır<sup>225</sup>. Sözleşmenin yeni hali “108+” olarak isimlendirilmiştir. Yapılan değişiklikte özellikle bilişim teknolojilerinin getirdiği yeniliklere uyum sağlama ihtiyacını karşılamaya yönelik adımların atıldığı

<sup>220</sup> Göçmen Uyarer, s. 53.

<sup>221</sup> Çalışmanın III. bölüm, 2.2.2.1. başlığı.

<sup>222</sup> Avrupa Konseyi'nin 108 sayılı Sözleşme düzenlemesinden önce 1973 ve 1974 yıllarında “*Özel Sektörde Elektronik Veri Bankaları Karşısında Bireylerin Özel Yaşamlarının Korunmasına İlişkin Karar*” ve “*Kamu Sektöründe Elektronik Veri Bankaları Karşısında Bireylerin Özel Yaşamlarının Korunmasına İlişkin Karar*” ile otomatik veri bankalarında bulunan kişisel verilerin korunmasına yönelik iki kararı bulunmaktadır.

<sup>223</sup> 108 sayılı Sözleşme, 6669 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun ile TBMM tarafından onaylanmış, 07.03.2016 tarihli ve 29656 sayılı Resmî Gazete'de yayımlanarak iç hukukumuzda dahil edilmiştir.

<sup>224</sup> KVKK'nın gerekçesine erişim için bkz: <https://www2.tbmm.gov.tr/d26/1/1-0541.pdf>, erişim tarihi: 19.09.2021.

<sup>225</sup> Değişikliğe ilişkin erişim için bkz.: <https://www.coe.int/en/web/data-protection/convention108/modernised>, erişim tarihi: 19.09.2021.

görülmektedir<sup>226</sup>. Bunun yanında şeffaflık, ihlallerin bildirilmesi, tasarımda gizlilik gibi konularda GDPR'a paralel bir şekilde yeni düzenlemeler ele alınmıştır.

Ayrıca 108 sayılı Sözleşme'ye ek olarak 01.07.2004 tarihinde Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'ne Ek 181 nolu Denetleyici Makamlar ve Sınıraşan Veri Akışına İlişkin Protokol (*Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Regarding Supervisory Authorities and Transborder Data Flows*)<sup>227</sup> getirilmiştir. Anılan ek protokolde özellikle veri işleme faaliyetlerinin denetlenme koşullarına ve sınıraşan veri akışına yönelik yeni düzenlemelere yer verilmiştir.

Avrupa Konseyi'nin kişisel verilerin korunmasını ele alan başka bir düzenlemesi Biyoloji ve Tıbbın Uygulanması Bakımından İnsan Hakları ve İnsan Haysiyetinin Korunması Sözleşmesi (*Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine*)<sup>228</sup> 01.12.1999 tarihinde yürürlüğe girmiştir. Sözleşme Türkiye tarafından 03.12.2003 tarihinde uygun bulunup onaylanmıştır<sup>229</sup>. Başta insan onurunun üstün tutulması olmak üzere insan haklarına dayalı yaklaşımı hedefleyen sözleşme, tıbbın kötüye kullanılmaması ile teknolojik gelişmelerin tıbbı ve ekseninde bulunan insana zarar vermesi gibi kaygılarla hazırlanmıştır<sup>230</sup>.

Avrupa Konseyi tarafından kişisel verilerin koruma altına alındığı diğer bir düzenleme ise 23.11.2001 tarihli Siber Suç Sözleşmesi (*Convention on Cybercrime*)'dir<sup>231</sup>. İlgili sözleşme, bilişim suçlarıyla ilgili taraf devletlerin düzenlemelerinin ve bağlantılı hükümlerinin uyumlu hale getirilmesini, siber suçların ve elektronik delil içeren diğer suçların soruşturma ile kovuşturulmasına yönelik uluslararası muhakeme kullarının

---

<sup>226</sup> Dülger, Kişisel Verilerin Korunması, s. 92.

<sup>227</sup> 181 nolu ek protokole erişim için bkz.: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/181>, erişim tarihi: 17.06.2021.

<sup>228</sup> Sözleşmeye erişim için bkz.: <http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168007cf98>, erişim tarihi: 16.06.2021.

<sup>229</sup> 09.12.2003 tarihli ve 25311 sayılı Resmî Gazete'de yayımlanan 5013 sayılı Biyoloji ve Tıbbın Uygulanması Bakımından İnsan Hakları ve İnsan Haysiyetinin Korunması Sözleşmesi: İnsan Hakları ve Biyotıp Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun. Erişim için bkz.: <https://www.resmigazete.gov.tr/eskiler/2003/12/20031209.htm#8>, erişim tarihi: 16.06.2021.

<sup>230</sup> Yılmaz, Kişisel Veriler, s. 137.

<sup>231</sup> Sözleşmeye erişim için bkz.: <http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561>, erişim tarihi: 16.06.2021.

yeknesaklaştırılmasını ve uluslararası adli yardım ile işbirliği alanında hızlı ve etkili bir sistem oluşturulmasını amaçlamaktadır<sup>232</sup>.

### 2.2.3. Birleşmiş Milletler Örgütü Düzenlemeleri

Birleşmiş Milletler Örgütü II. Dünya Savaşı'nın yıkıcı etkilerine karşı 24.10.1945 tarihinde 51 devlet tarafından kurulmuş ve günümüzde 193 üyesi bulunan bir örgüttür<sup>233</sup>. Üye devletler Birleşmiş Milletler Şartı'ndan<sup>234</sup> doğan yükümlülükleri kabul etmişlerdir<sup>235</sup>. Birleşmiş Milletler Şartı'nın 1. maddesinin 3. fıkrasına göre Örgüt'ün belirlenen dört amacından birisi; ırk, cinsiyet, dil ya da din ayrımı gözetmeksizin herkesin insan haklarına ve temel özgürlüklerine saygı gösterilmesinin geliştirilip desteklenmesidir. Bu anlamda Örgüt'ün kurulması, insan haklarının korunması alanında dünya genelinde atılan ilk adımdır<sup>236</sup>.

Örgüt'ün kuruluşundan üç yıl sonra 10.12.1948 tarihinde kabul edilen İnsan Hakları Evrensel Beyanname'si'nin<sup>237</sup> 12. maddesinde; “*hiç kimsenin özel hayatına, ailesine, meskenine, yazışmasına karşı bir tecavüze maruz bırakılamayacağı ve herkesin bu karışma ve tecavüzlere karşı kanun ile korunmaya hakkı olduğu*” belirtilmiştir. Yine, 23.03.1976'da kabul edilen Bireysel ve Siyasal Haklar Uluslararası Sözleşmesi'nin<sup>238</sup> 17. maddesinde, Beyanname'nin 12. maddesine paralel bir şekilde özel hayatın gizliliğinin korunması ele alınmıştır.

Özel hayatın gizliliğinin korunmasının dışında Birleşmiş Milletler Genel Kurulu'nun 14.12.1990 tarihinde kabul ettiği Bilgisayarla İşlenen Kişisel Veri Dosyalarına İlişkin

---

<sup>232</sup> Aliusta, Cahit / Benzer, Recep, “Avrupa Siber Suçlar Sözleşmesi ve Türkiye'nin Dahil Olma Süreci”, Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, Cilt:4, No:2, 2018, ss. 35-42, s. 38.

<sup>233</sup> Üye devletler ile ilgili bilgiler için bkz.: <https://www.un.org/en/about-us/member-states>, erişim tarihi: 19.09.2021.

<sup>234</sup> Birleşmiş Milletler Şartı'nın Türkçe metnine erişim için bkz.: [https://inhak.adalet.gov.tr/Resimler/SayfaDokuman/2212020141836bm\\_01.pdf](https://inhak.adalet.gov.tr/Resimler/SayfaDokuman/2212020141836bm_01.pdf), erişim tarihi: 19.09.2021.

<sup>235</sup> Küzeci, Kişisel Verilerin Korunması, s. 117.

<sup>236</sup> Küzeci, Kişisel Verilerin Korunması, s. 117.

<sup>237</sup> Çalışmanın devamında “Beyanname” olarak isimlendirilecektir. Erişim için bkz.: <https://www.hsk.gov.tr/Eklentiler/Dosyalar/9a3bfe74-cdc4-4ae4-b876-8cb1d7eeae05.pdf>, erişim tarihi: 19.09.2021.

<sup>238</sup> Sözleşmeye erişim için bkz.: [https://diabgm.adalet.gov.tr/arsiv/sozlesmeler/coktarafilisoz/bm/bm\\_05.pdf](https://diabgm.adalet.gov.tr/arsiv/sozlesmeler/coktarafilisoz/bm/bm_05.pdf), erişim tarihi: 19.09.2021.

Yönlendirici İlkeler (*Guidelines Concerning Computerized Personal Data Files*)'de<sup>239</sup> de kişisel verilerin korunması alanına yönelik düzenlemeler yer almaktadır. Buna göre ulusal hukuk sistemlerinde tanınması gereken ilkeler; i) yasal ve dürüst yollarla toplama ve işleme ilkesi, ii) verilerin doğruluğu ilkesi, iii) amacın belirliliği ilkesi, iv) ilgili kişinin erişimi ilkesi, v) ayrımcılık yapmama ilkesi, vi) veri güvenliği ilkesi, vii) denetim ve yaptırım, viii) verilerin sınır ötesi akışı olarak sıralanabilir.

Anılan ilkeler, denetim yapılmasına yönelik bağımsız ve yetkili kurumların oluşturulmasını öngören ilk uluslararası hukuk kaynağı olması açısından önemlidir<sup>240</sup>. Ancak hukuksal açıdan üye devletleri bağlayıcı olmaması, diğer bir ifade ile yalnızca tavsiye niteliğinde olması sebebiyle ilkeler beklenen etkiyi yaratmamıştır<sup>241</sup>.

#### **2.2.4. Avrupa Birliği Düzenlemeleri: 95/46/EC Sayılı Direktif ve GDPR**

Avrupa Birliği tarafında ise ilk önemli düzenleme, Türk hukukunda yürürlükte olan KVKK'nın da esas aldığı 95/46/EC sayılı Direktif'tir. 95/46/EC sayılı Direktif uyarınca Avrupa Birliği üye devletlerinin, kişisel verilerin korunması alanında yasal düzenlemelere sahip olması zorunlu kılınmıştır<sup>242</sup>.

Kişisel verilerin korunmasına ilişkin usul ve esasların günümüz koşulları ile paralellik sağlanması ve mahremiyete yönelik çeşitli koruma açıklıklarının giderilmesi amacıyla<sup>243</sup> 14.04.2016 tarihinde GDPR onaylanmış ve 25.05.2018 tarihinde 95/46/EC sayılı Direktif'in yerine yürürlüğe girmiştir. GDPR her ne kadar bir Avrupa Birliği düzenlemesi olsa da üye devletler arasında yapılan ticari ve iş anlaşmalarında bu düzenlemeye uyum sağlanması aranmıştır<sup>244</sup>.

<sup>239</sup> İlkeler erişim için bkz.: <http://hrlibrary.umn.edu/instree/q2grcpd.htm>, erişim tarihi:16.06.2021.

<sup>240</sup> Şimşek, Oğuz, s. 16; Küzeci, Kişisel Verilerin Korunması, s. 119-120; Doğan, s. 7.

<sup>241</sup> Küzeci, Kişisel Verilerin Korunması, s. 120.

<sup>242</sup> Saka / Çağlayan / Koca, s. 22.

<sup>243</sup> Saka / Çağlayan / Koca, s. 23.

<sup>244</sup> Yılmaz, Süleyman / Çavuşoğlu, Gökçe Filiz, *Kişisel Verileri Koruma Hukuku*, Yetkin Yayınları, Ankara, 2020, s. 24.

Esasen GDPR, 95/46/EC sayılı Direktif'e göre daha kapsamlıdır ve farklı hükümler içermektedir. Düzenleme farklılıklarının bir kısmı aşağıdaki şekilde sıralanabilir:

a) Etki alanının genişletilmesi (m. 3): Her ne kadar GDPR hükümleri Avrupa Birliği tarafından hayata geçirilse de GDPR'ın etki alanı Avrupa Birliği sınırlarından daha geniştir. Eğer veri kontrolörü veya veri işleyen Avrupa Birliği sınırları içerisindeki faaliyeti kapsamında veri işliyorsa faaliyetin nerede gerçekleştiğine bakılmaksızın GDPR uygulama alanı bulur. Diğer yandan; Avrupa Birliği sınırları içerisindeki bir kişiye ürün veya hizmet sunulması veya bu sınırlar içerisindeki bir kişinin davranışlarının izlenmesi halinde de GDPR uygulanacaktır. Bu anlamda sınırların bu denli geniş çizildiği bir uygulama alanına sahip olması nedeniyle bu yenilik önemlidir.

b) Unutulma hakkı (m. 17): Bu hakla, ilgili kişiye kişisel verilerinin silinmesi ile yayınlanmasının ve potansiyel üçüncü kişilere aktarılmasının önlenmesi konularında talep etme hakkı verilmiştir<sup>245</sup>. Kişisel Verileri Koruma Kurulu'nun vermiş olduğu kararlarda da unutulma hakkının ele alındığı görülmektedir<sup>246</sup>. Kişisel verilerin üçüncü kişiler tarafından sınırsız bir şekilde saklanmasının önüne geçilmesi adına bu hakkın tanınması önemlidir<sup>247</sup>.

c) İhlal bildirim (m. 33): Veri işleme faaliyetleri dolayısıyla bir veri ihlalinin gündeme gelmesi ve bu ihlalin ilgili kişi açısından risk oluşturması durumunda veri ihlalinin öğrenildiği andan itibaren 72 saat içerisinde yetkin denetim makamına bildirilmesi gerekmektedir. Her ne kadar KVKK'da yer almasa da Kişisel Verileri Koruma Kurulu 2019 yılında yayımlanmış olduğu bir kararla veri sorumlularının yaşadığı ihlalleri ihlalin öğrenilmesinden itibaren 72 saat içerisinde Kurul'a bildirmelerini zorunlu kılmıştır<sup>248</sup>. İhlali bildirim yükümlülüğü, kişisel verilerin korunmasına ilişkin yükümlülüklerin ciddiye alınması amacıyla getirilmiş önemli bir yeniliktir.

---

<sup>245</sup> **Dülger**, Kişisel Verilerin Korunması, s. 108. Unutulma hakkı ile ilgili olarak ayrıca bkz.: **Saka / Çağlayan / Koca**, s. 215-233.

<sup>246</sup> Kişisel Verileri Koruma Kurulu'nun "Kişilerin ad ve soyadı ile arama motorları üzerinden yapılan aramalarda çıkan sonuçların indeksten çıkarılmasına yönelik talepler" ile ilgili 23.06.2020 tarihli ve 2020/481 sayılı kararına erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/6776/2020-481>, erişim tarihi: 29.09.2021.

<sup>247</sup> Unutulma hakkına yönelik eleştiriler için bkz.: **Yavuz**, Can, *İnternetteki Arama Sonuçlarından Kişisel Verilerin Kaldırılması*, Seçkin Yayıncılık, Güncellenmiş ve Genişletilmiş 3. Baskı, Ankara 2020, s. 263 vd.

<sup>248</sup> Kişisel Verileri Koruma Kurulu'nun 24.01.2019 tarihli ve 2019/10 sayılı kararına ilişkin duyuruya erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirimi>, erişim tarihi: 29.09.2021.

ç) Veri koruma etki değerlendirmesi (m. 35): Özellikle otomatik metotların kullanıldığı veri işleme faaliyetleri eğer ki gerçek kişilerin temel hak ve özgürlükleri açısından yüksek risk teşkil ediyorsa veya bu risk muhtemelse, söz konusu riskin etkileri konusunda analiz çalışmasının yapılması gerekmektedir. Özellikle büyük ölçekli ve hassas verilerin işlenmesinde etki değerlendirmesinin önemli olduğu belirtilmektedir<sup>249</sup>. Türk hukukunda veri koruma etki değerlendirmesine ilişkin herhangi bir düzenleme bulunmamaktadır.

d) Veri koruma görevlisi (m. 37): Yargı faaliyetinin yürütülmesi durumu hariç olmak üzere eğer ki veri işleme faaliyeti; i) bir kamu kurum veya kuruluşunca gerçekleştiriliyorsa; ii) veri işleyicisi ve veri kontrolörünün temel faaliyetleri işin doğası gereği büyük ölçüde veri işlemeyi gerektiriyorsa; iii) temel faaliyetler hassas verilerin işlenmesi üzerine kuruluysa veri kontrolörü veya veri işleyicisi, bir veri koruma görevlisi belirlemek durumundadır. Veri koruma görevlisinin veri koruma alanında yeterli uzmanlık bilgisine sahip olması gereklidir. Bu anlamda GDPR, özel ve idari kurumların kişisel verilerin korunması alanında yeterli bilgi ve donanımı haiz kişiler ile çalışmasını hedeflemektedir. Dolayısıyla kişisel verilerin korunmasına yönelik sistematüğün oluşturulması açısından bu yenilik önemlidir.

### 2.3. Türk Hukukundaki Düzenlemeler

Türk hukukunda kişisel verilerin korunmasına yönelik düzenlemeler, uluslararası düzenlemelerden çok sonra yapılmıştır. Bu başlık altında kişisel verilerin korunmasıyla ilgili Türk hukukunda yer alan yasal düzenlemeler *kronolojik* sırayla ele alınacaktır.

Kişisel verilerin korunması, Türk hukukunda ilk kez 2004 yılında “*Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğın Korunması Hakkında Yönetmelik*”<sup>250</sup> ile düzenlenmiştir. Bunu takiben 2005 yılında yürürlüğe giren TCK’nın

<sup>249</sup> T.C: Kalkınma Bakanlığı İktisadi sektörler ve koordinasyon genel müdürlüğü Bilgi Toplumu Dairesi Başkanlığı, Çalışma Raporu – 6, Ayşe Nur Akıncı, Avrupa Birliği Genel Veri Koruma Tüzüğü’nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi, s. 17, erişim için bkz.: [http://www.bilgitoplumu.gov.tr/wp-content/uploads/2017/07/AB\\_Veri\\_Koruma\\_Tuzugu.pdf](http://www.bilgitoplumu.gov.tr/wp-content/uploads/2017/07/AB_Veri_Koruma_Tuzugu.pdf), erişim tarihi: 22.06.2021.

<sup>250</sup> 06.02.2004 tarihli ve 25365 sayılı Resmî Gazete’de yayımlanan söz konusu yönetmelik 24.07.2012 tarihli ve 28363 sayılı Resmî Gazete’de yayımlanan Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğın Korunması Hakkında Yönetmelik’le yürürlükten kalkmıştır.

“Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar” başlıklı dokuzuncu bölümünde kişisel verilerin korunmasıyla ilgili üç suç tipi düzenlenmiştir. Bu suç tipleri TCK’nın 135. maddesinde “*Kişisel verilerin kaydedilmesi*”, 136. maddesinde “*Verileri hukuka aykırı olarak verme veya ele geçirme*” ve 138. maddesinde “*Verileri yok etmeme*” olarak yer almaktadır. Ancak bu suç tiplerinde yer alan teknik kavramlar nedeniyle uygulamaya ilişkin birtakım sıkıntılar yaşanmıştır.

2010 yılında Anayasa’nın “Özel Hayatın Gizliliği” başlıklı 20. maddesine yapılan ekleme<sup>251</sup> ile kişisel veriler ilk defa anayasal güvence altına alınmış, kişisel verilerin korunması hakkı da temel bir hak olarak düzenlenmiştir<sup>252</sup>. Anılan düzenleme şu şekildedir:

*“Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir”*<sup>253</sup>.

İlgili düzenlemede kişisel verilerin korunması alanında uluslararası düzenlemelere paralel bir şekilde bilgi edinme hakkı, düzeltme ve silme hakkı ile amaca bağlılık ve orantılılık ilkelerine yer verilmesi yerinde olmuştur<sup>254</sup>. Buna karşın terminoloji açısından “*kişisel verilerin korunmasını isteme hakkı*” yerine “*kişisel verilerin korunması hakkı*” ifadesinin tercih edilmesinin daha isabetli olacağını düşünmekteyiz. Nitekim kişisel veriler, ilgili kişinin isteğinden bağımsız olarak da korunmalıdır<sup>255</sup>. Diğer yandan, yapılan eklemede kişisel verilerin işlenmesini denetleme altına alacak tam bağımsız bir otoritenin varlığı öngörülmemiştir<sup>256</sup>. Ancak bağımsız bir otoritenin kurulması yönünde Anayasa’da

<sup>251</sup> 07.06.2010 tarihli ve 5982 sayılı Türkiye Cumhuriyeti Anayasasının Bazı Maddelerinde Değişiklik Yapılması Hakkında Kanun’un 2. maddesiyle Anayasa’nın 20. maddesine ek 3. fıkra getirilmiştir. Böylelikle kişisel verilerin korunması hakkı ilk defa anayasal güvence altına alınmıştır.

<sup>252</sup> **Akgül**, s. 222; **Çekin**, s. 8-9; **Taştan**, s. 23.

<sup>253</sup> Erişim için bkz.: <https://www.mevzuat.gov.tr/MevzuatMetin/1.5.2709.pdf>, erişim tarihi: 23.09.2021.

<sup>254</sup> **Ayözger Öngün**, s. 95; **Börekçi**, s. 42.

<sup>255</sup> **Küzeci**, *Kişisel Verilerin Korunması*, s. 283.

<sup>256</sup> ABAD’ın bağımsızlığın koşuluna ve otoritenin sınırlarına ilişkin kararları için bkz.: ABAD, *Avrupa Komisyonu v. Avusturya Cumhuriyeti*, Dava No: C-614/10, tarih: 16.10.2012, dava raporuna erişim için bkz.: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62010CJ0614&from=en>, erişim tarihi: 23.09.2021; ABAD, *Avrupa Komisyonu, Avrupa Komisyonu v. Macaristan*, Dava No: C-288/12, tarih: 08.04.2021, dava özetine erişim için bkz.: <https://ec.europa.eu/anti->



doğrudan hüküm bulunmaması, bu otoritenin kurulamayacağı anlamına gelmemektedir<sup>257 258</sup>.

Diğer yandan Anayasa'nın 13. maddesinde temel hak ve özgürlüklerin Anayasa'nın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlandırılabilceği belirtilmiştir. Oysa Anayasa'nın 20. maddesinin 3. fıkrasına ilişkin düzenlemede bu hakka ilişkin özel bir sınırlama sebebi öngörülmemiştir. Her ne kadar Anayasa'nın 13. maddesinin devamında sınırlamanın "*Anayasa'nın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamayacağı*" düzenlenmiş ise de -diğer bir ifadeyle sınırlamanın sınırları belirtilmiş ise de<sup>259</sup>- 2010 yılında eklenen bu düzenleme mevcut haliyle kişisel verilerin korunmasının önünde bir engel yaratabilecek niteliktedir<sup>260</sup>. Nitekim bu husus hakkın sınırlandırılmasına ilişkin özel sebeplerin kanun düzeyine indirilmesine yol açmaktadır<sup>261 262</sup>. *Küzeci*, konuya ilişkin olarak haklı bir şekilde şu ifadeleri kullanmaktadır: "*Kişisel verilerin korunması Anayasa ile güvence altına alınmış bir temel hak olduğuna göre, bu hakkın sağlanması kural, sınırlanması istisna olacaktır. Aksi yaklaşım, yani yasal düzenlemeler ile belirlenen ölçüsüz sınırlama nedenleri, hakkın tanınmasını anlamsız kılabilir. Bu ise temel ilkelere aykırı olacağı gibi, kişisel verilerin korunmasına ilişkin anayasal hükmün kâğıttan bir kaplana dönüşmesine neden olabilir*"<sup>263</sup>.

Anayasa'nın 20. maddesine yapılan eklemeye kişisel verilerin korunmasına ilişkin usul ve esasların kanunla düzenleneceği belirtilse de 6698 sayılı Kişisel Verilerin Korunması Kanunu, kişisel verilerin korunmasının anayasal bir hak olarak düzenlenmesinin neredeyse altı yıl sonrasında, 07.04.2016 tarihinde yürürlüğe girmiştir<sup>264</sup>. Dolayısıyla

---

[fraud/sites/default/files/caselaw\\_2001\\_2015\\_en.pdf](http://fraud/sites/default/files/caselaw_2001_2015_en.pdf), s. 21; ayrıca C-614/10 nolu dava özetine erişim için bkz.: s. 17, erişim tarihi: 23.09.2021.

<sup>257</sup> **Küzeci**, Kişisel Verilerin Korunması, s. 283.

<sup>258</sup> Türkiye'de KVKK'nın yürürlüğe girmesiyle birlikte Kişisel Verileri Koruma Kurumu kurulmuştur.

<sup>259</sup> **Arslan**, Zühtü, "*Temel Hak ve Özgürlüklerin Sınırlanması: Anayasa'nın 13. Maddesi Üzerine Bazı Düşünceler*", Anayasa Yargısı, Cilt: 19, Ankara 2002, ss. 139-155, s. 140.

<sup>260</sup> **Küzeci**, Kişisel Verilerin Korunması, s. 283.

<sup>261</sup> **Üzeltürk Tahmazoğlu**, Sultan, "*Kişisel Verilerin Korunması Hakkında Anayasa Değişikliği*", Legal Hukuk Dergisi, Sayı: 93, Eylül 2010, ss. 3151-3156, s. 3155.

<sup>262</sup> Her ne kadar Anayasa'da hakkın kanunla sınırlandırılabilceği ve sınırlandırmanın sınırları belirtilmiş olsa da bu durumun yarattığı riske somut örnek olarak, çalışmanın II. bölüm 4.2.4. başlığında ele alınan istisna durumları ve Kişisel Verileri Koruma Kurulu'nun Covid-19 ile ilgili vermiş olduğu karar gösterilebilir.

<sup>263</sup> **Küzeci**, Kişisel Verilerin Korunması, s. 284.

<sup>264</sup> Önemle belirtmek gerekir ki Türkiye'de kişisel verilerin korunmasına özgü kanun çıkarılmasına yönelik çalışmalar 1989 yılında başlamıştır. Kişisel verilerin korunmasına ilişkin bir kanun tasarısı hazırlamak

2010 yılından KVKK'nın yürürlüğe girmesine kadar olan süre zarfında kişisel verilere ilişkin hukukî meselelerde hukuka uygunluğun veya aykırılığın nasıl belirleneceği önemli bir konu olmuştur. Yukarıda belirtildiği üzere AİHM, kişisel verilerin korunması hakkını AİHS'in 8. maddesinde ele almaktadır. Dolayısıyla arada geçen sürede karar verici mercilerin birincil kaynak olarak AİHM içtihadından yararlanması gerekmiştir. Diğer yandan 95/46/EC sayılı Direktif ve uygulamaları ile ABAD kararları da yargıçlara yön göstermiştir. Nitekim kişisel veri, 2008 yılında AYM tarafından uluslararası düzenlemelerdekine benzer şekilde “belirli veya belirlenebilir kişilerle ilgili her türlü bilgi” olarak tanımlanmıştır<sup>265</sup>. Yine, AYM tarafından 2015 yılında, TCK'nın 136. maddesinin “kişisel verilerle ilgili bir tanım ve sınırlandırma yapılmaması” sebebiyle Anayasa'nın 38. maddesine aykırılığı ileri sürülerek iptal istemine yönelik davada, 108 sayılı Sözleşme, Rehber İlkeler, 95/46/EC sayılı Direktif, AİHS ve AİHM kararlarına atıfta bulunularak, kişisel verinin tespitinde bu kaynaklardan yararlanılması gerektiği belirtilmiştir<sup>266</sup>.

KVKK ile amaçlanan; kişisel verilerin işlenmesinde temel hak ve özgürlüklerin korunması, kişisel verileri işleyenlerin disiplin altına alınması, kişilerin mahremiyetinin korunması ve kişisel verilerin güvenliğinin sağlanmasıdır<sup>267</sup>. Bunun yanında, Türk vatandaşların Schengen ülkelerine girişindeki vize muafiyeti için yapılan görüşmeler esnasında AB'nin sunmuş olduğu şartlar arasında kişisel verilere ilişkin genel bir kanun yapılmasının ön şart olarak ileri sürülmesi, AB uyum çalışmalarının sürdürülmesi, Anayasa'ya getirilen eklemeye istinaden kişisel verilerin korunması hakkının

---

üzere ise ilk komisyon 13.09.1995'te kurulmuş; ancak bu komisyon çalışmalarını tamamlayamamıştır. Bunu takiben 2000 yılında oluşturulan ikinci komisyon üç yıllık çalışmasının ardından Kişisel Verilerin Korunması Kanun Tasarısı'nı hazırlamıştır. Ancak bu tasarı yasalaşmamıştır. Ardından 2011 yılında yeni bir tasarı taslağı gündeme gelse de yine bir sonuca varılamamıştır. 2014 yılında yeni bir tasarı bir kez daha Türkiye Büyük Millet Meclisi'ne (TBMM) sevk edilmiş; ancak bu tasarı TBMM'de görüşülmeyle hükümsüz kalmıştır.

<sup>265</sup> AYM'nin 2006/167 E., 2008/86 K., sayılı ve 20.03.2008 tarihli kararı, erişim için bkz.: <https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2008/86?EsasNo=2006%2F167>, erişim tarihi: 28.06.2021.

<sup>266</sup> AYM'nin 2015/32 E., 2015/102 K. sayılı ve 12.11.2015 tarihli kararı, erişim için bkz.: <https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2015/102?EsasNo=2015%2F32>, erişim tarihi: 05.10.2021.

<sup>267</sup> Kişisel Verileri Koruma Kurumu, *6698 Sayılı Kişisel Verilerin Korunması Kanununun Amacı ve Kapsamı*, s. 2, erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/4185/6698-Sayili-Kisisel-Verilerin-Korunmasi-Kanununun-Amaci-ve-Kapsami#:~:text=bu%20h%C3%BCkme%20g%C3%B6re%20ama%C3%A7%20ki%C5%9Fisel,uyacaklar%C4%B1%20usul%20ve%20esaslar%C4%B1%20d%C3%BCzenlemektir>, erişim tarihi: 28.06.2021.

sınırlandırılacağı bir düzenlemenin bulunmaması, EUROPOL ve EUROJUST ile işbirliği yapılamaması, TCK'da kişisel verilere ilişkin düzenlenen suç tiplerini tamamlayıcı bir düzenlemenin mevcut olmaması gibi sebepler de KVKK'nın yürürlüğe girmesinde etkili olmuştur<sup>268</sup>.

KVKK'nın yürürlüğe girmesinin ardından, kişisel verilerin korunmasıyla doğrudan ilgili olan birtakım yönetmelikler hazırlanmıştır. Bu yönetmeliklerden ilki; Kişisel Verileri Koruma Kurumu tarafından çıkarılan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'tir<sup>269</sup>. Bu yönetmeliğin amacı, 2. maddesinde *“Tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin usul ve esasları belirlemek”* olarak ifade edilmiştir.

Kişisel Verileri Koruma Kurumu tarafından çıkarılan diğer bir yönetmelik, Kişisel Verileri Koruma Kurulu Çalışma Usul ve Esaslarına Dair Yönetmelik'tir<sup>270</sup>. Bu yönetmelikle Kurul'un çalışma usul ve esasları, görevleri, yetkileri ve sorumlulukları belirlenmiştir.

Kişisel Verileri Koruma Kurumu tarafından çıkarılan son yönetmelik, Veri Sorumluları Sicili Hakkında Yönetmelik'tir<sup>271</sup>. İlgili yönetmelikle veri sorumlularının internet tabanlı bir sicile kaydolarak bünyelerinde barındırdığı veri kategorilerini, bunları işleme amaçlarını, saklama sürelerini, bunların hangi kişi grubuna ait olduğunu, ne kadar süreyle saklanacağını ve güvenliğini sağlamaya yönelik almış olduğu tedbirleri bildireceği bir sistem oluşturulmuştur. Esasen uygulamada veri sorumlularının genellikle alelade bir şekilde doğru ya da yanlış bilgilerle bildirim yaptığı görüldüğünden, bu sicilin şeffaflığı sağlamak yönündeki amacına ulaştığının söylenmesi güçtür.

---

<sup>268</sup> **Başalp**, Nilgün, *“Avrupa Birliği Veri Koruması Genel Regülasyonu'nun Temel Yenilikleri”*, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, C.XXI, S.1, 2015, ss. 77-105, (**Başalp**, Temel Yenilikler), s. 80; **Küzeci**, Kişisel Verilerin Korunması, s. 305-306.

<sup>269</sup> 28.10.2017 tarihli ve 30224 sayılı Resmî Gazete'de yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik.

<sup>270</sup> 16.11.2017 tarihli ve 30242 sayılı Resmî Gazete'de yayımlanan Kişisel Verileri Koruma Kurulu Çalışma Usul ve Esaslarına Dair Yönetmelik.

<sup>271</sup> 30.12.2017 tarihli ve 30286 sayılı Resmî Gazete'de yayımlanan Veri Sorumluları Sicili Hakkında Yönetmelik.

Kişisel verilerin korunmasıyla ilgili olan bir diğer yönetmelik, Sağlık Bakanlığı tarafından çıkarılan *Kişisel Sağlık Verileri Hakkında Yönetmelik*'tir<sup>272</sup>. Bu yönetmelik ile Sağlık Bakanlığı'nın merkez ve taşra teşkilatı birimleri ile bunlara bağlı olarak faaliyet göstermekte olan sağlık hizmeti sunucuları ile bağlı ve ilgili kuruluşları tarafından yürütülen süreç ve uygulamalarda kişisel sağlık verilerinin işlenmesine ilişkin uyulacak usul ve esasların düzenlenmesi amaç edinilmiştir.

### 3. KİŞİSEL VERİLERİN KORUNMASINDA GÜDÜLEN AMAÇ

Teknolojinin bu denli hızlıca ilerlemesinin sonuçlarından birisi olarak, günümüzde idari ve özel kurumlar birçok kişinin bilgilerine ulaşabilmektedir. Kişisel veriler de bu bilgiler arasında bulunmaktadır. Esasında, teknolojinin henüz son yıllardaki kadar gelişmediği dönemlerde dahi kişisel veri toplamak, veriyi toplayan kişi açısından ilgili kişiyi tanımak için oldukça önemli olmuştur<sup>273</sup>. Bu veri toplama isteğinin, diğer bir ifade ile “*bilme*” isteğinin temelinde; sosyal yaşam açısından insani bir duygu olarak merak<sup>274</sup>, iş hayatı açısından personel verimliliğinin artırılması, ticari hayat açısından kârlılığın ve avantajın artırılması veya edimlerin yerine getirilmesinin sağlanması, idare hukuku açısından gerekli planlama, yönetim ve güvenliğin sağlanması, sağlık hukuku açısından ise gerekli sağlık hizmetinin sunulması bulunabilir<sup>275</sup>. Dolayısıyla kişisel verilerin günümüzden önce de önemli bir kaynak, bilgiye ulaşmak için güçlü bir araç olduğu söylenebilir. Bu nedenle kişisel verilerin korunması, tüm zamanlar için elzemdir. Ancak özellikle son zamanlarda teknolojinin insan yaşamına daha fazla dahil olmasıyla birlikte kişisel verilerin bilişim alanındaki gelişmeler karşısında korunmasının önemi bir hayli artmıştır. Nitekim uygulamada veri koruma otoriteleri tarafından verilen kararlar ve bu kararlara konu olan ihlaller düşünüldüğünde, kişisel verilerin bilişim alanındaki gelişmeler karşısında korunmasının önemi ve gerekliliği daha da açık hale gelmektedir.

<sup>272</sup> 21.06.2019 tarihli ve 30808 sayılı sayılı Resmî Gazete’de yayımlanan *Kişisel Sağlık Verileri Hakkında Yönetmelik*.

<sup>273</sup> **Köse Aysun**, s. 40.

<sup>274</sup> **Küzeci**, *Kişisel Verilerin Korunması*, s. 20.

<sup>275</sup> **Küzeci**, *Kişisel Verilerin Korunması*, s. 20; **Köse Aysun**, s. 40.

KVKK'nın ilk maddesine göre “*Kanun'un 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.*” Dolayısıyla kişisel verilerin korunmasında güdülen amaçların temelinde özel hayatın gizliliğinin ve kişilerin temel hak ve özgürlüklerin korunmasının bulunduğu söylenebilir. Madde gerekçesine bakıldığında ise kişisel verilerin korunmasıyla kişinin mahremiyet hakkının ve bilgi güvenliği hakkının da korunmasının hedeflendiği görülmektedir<sup>276</sup>. Nitekim belirtilen amaçlar KVKK'nın mehz aldığı 95/46/EC sayılı Direktif ile de örtüşmektedir. Ancak unutulmamalıdır ki kişisel verilerin korunması hakkı, esasında özel yaşamın gizliliği hakkının yanı sıra birçok hak ile yakından ilişkilidir<sup>277</sup>. Örneğin ifade özgürlüğü, haberleşme özgürlüğü, bilgilerin geleceğini belirleme özgürlüğü, bilgi edinme gibi haklar kişisel verilerin korunması hakkıyla da ilişkilidir<sup>278</sup>. Nitekim bir düşünce veya haberleşmeye konu bilgiler kişisel veri olabilir. Diğer yandan ilgili kişi, anayasal hakkı olan bilgi edinme hakkını kullanarak birtakım bilgileri talep edebilir. Buna ek olarak kişinin kişisel verileri üzerindeki denetim yetkisi ise kişinin bilgilerinin geleceğini belirleme özgürlüğü olarak değerlendirilebilir.

---

<sup>276</sup> Kişisel Verileri Koruma Kurumu, *Madde ve Gerekçesi ile Kişisel Verilerin Korunması Kanunu (Bilgi Notu) ve Kişisel Verilerin Korunmasına İlişkin Terimler Sözlüğü*, KVKK Yayınları, Mart 2019, Ankara, s. 7, erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/5388/Madde-ve-Gerekçesi-ile-Kisisel-Verilerin-Korunmasi-Kanunu-Bilgi-Notu-ve-Kisisel-Verilerin-Korunmasina-Iliskin-Terimler-Sozlugu>, erişim tarihi: 29.09.2021.

<sup>277</sup> **Küzeci**, *Kişisel Verilerin Korunması*, s. 58.

<sup>278</sup> **Küzeci**, *Kişisel Verilerin Korunması*, s. 58.

## II. BÖLÜM: KVKK’NIN CEZA HUKUKU, CEZA MUHAKEMESİ HUKUKU VE DİĞER HUKUK DALLARIYLA İLİŞKİSİ

### 1. GENEL OLARAK

Kişisel verilerin korunması birçok hukuk dalı ile ilişkili bir alandır. Ancak KVKK’nın ceza hukuku ve ceza muhakemesi hukuku ile ilişkisine bakıldığında bu ilişkinin KVKK’nın diğer alanlarla olan ilişkisinden pozitif anlamda ayrışan yönünün bulunduğu görülmektedir. Bunun nedenlerinden birisi, TCK’da kişisel verilerin korunmasına yönelik olarak spesifik suç tiplerinin düzenlenmiş olmasıdır<sup>279</sup>. Üstelik bu düzenlemeler henüz KVKK yürürlüğe girmeden önce yapılmıştır. Diğer yandan, ceza muhakemesi ve infaz işlemleri kapsamında yürütülen işlemlerde kişilerin mahrem bilgilerinin işlenmesi, KVKK’nın ceza muhakemesi hukukunda ne kadar önemli bir rol oynadığını göstermektedir.

Kişisel verilerin korunmasına ilişkin olarak Türk Ceza Hukuku bakımından ilk düzenlemeler TCK’da görülmektedir. Esasında 765 sayılı mülga Türk Ceza Kanunu’nda<sup>280</sup> kişisel verilerin korunmasına ilişkin bir düzenleme bulunmamasına karşın; yargı mercilerinin kişisel verilerin korunması hakkını “*Sırrın Masuniyeti Aleyhinde Cürümler*” başlıklı beşinci faslının 195 vd. maddelerinde yer alan *haberleşmenin ihlali* (195. madde), *haberleşme kağıtlarını ortadan kaldırma* (196. madde), *haberleşmenin ifşası* (197. madde), *haberleşmenin ifşasının belirli kişiler tarafından işlenmesi* (198. madde) suç tipleri kapsamında değerlendirdikleri görülmektedir<sup>281</sup>.

TCK’nın yürürlüğe girmesiyle 765 sayılı TCK’dan farklı olarak *kişisel verilerin kaydedilmesi* (135. madde), *verileri hukuka aykırı olarak verme veya ele geçirme* (136. madde), *nitelikli haller* (137. madde) ve *verileri yok etmeme* (138. madde) suçları düzenlenmiştir. TCK’nın yürürlüğe girdiği 2005 yılı ile KVKK’nın yürürlüğe girdiği 2016 yılı arasında geçen on bir yılda karşılaşılan en önemli sorunlardan birisi, “*kişisel*

<sup>279</sup> Sınar, Hasan, “*Kişisel Verileri Hukuka Aykırı Olarak Verme, Yayma veya Ele Geçirme Suçu (TCK Md. 136)*”, *Kişisel Verileri Koruma Dergisi*, Cilt: 2, Sayı: 1, ss. 33-62, s. 34.

<sup>280</sup> 13.03.1926 tarihli 320 sayılı Resmî Gazete’de yayımlanan 765 sayılı Türk Ceza Kanunu. Çalışmanın devamında “765 sayılı TCK” olarak isimlendirilecektir.

<sup>281</sup> Göçmen Uyarer, s. 99.

veri” gibi temel bir kavramı tanımlayan ulusal bir düzenlemenin bulunmamasıdır<sup>282</sup>. Bu zaman zarfında mahkemeler tasarı çalışmaları ile uluslararası ve yabancı ülke mevzuatından yararlanarak kişisel verilerle ilgili unsurları aramaya çalışmışlardır<sup>283</sup>. Nihayet 2016 yılında kişisel verilerle ilgili pek çok kavram tanımlanmış ve bu verilerin işlenmesine yönelik temel esaslar belirlenmiştir<sup>284</sup>. Dolayısıyla neyin kişisel veri sayılabileceği, kişisel verinin hangi şartlar altında işlenebileceği, hangi durumlarda kaydedilebileceği, üçüncü kişilere hangi şartlarda aktarılabilceği, ne zaman yok edileceği, hukuka uygunluk nedenlerinin sınırlarının nasıl ele alınacağı gibi konular açısından KVKK oldukça önemli bir düzenlemedir. Nitekim KVKK’nın gerekçesinde de “Ülkemizde kişisel verilerin korunmasını sağlayacak bir kanunun yürürlüğe girmesini gerektiren değişik sebepler bulunmaktadır. Öncelikle, 5237 sayılı Türk Ceza Kanununun 135 ve devamı maddelerinde, kişisel verilerin hukuka aykırı olarak elde edilmesi, kaydedilmesi veya ifşa edilmesi fiilleri suç olarak düzenlenmiş ve yaptırıma bağlanmıştır. Bununla birlikte, kişisel verilerin işlenmesine yönelik özel bir kanunun bulunmaması sebebiyle, bu fiillerin ne zaman hukuka aykırı ne zaman hukuka uygun olduğunun belirlenmesinde tereddütlerin yaşandığı görülmektedir.” ifadelerine yer verilerek bu durumun önemine değinilmiştir<sup>285</sup>.

KVKK, kişisel verilerin korunması alanına yönelik özel bir kanundur. TCK ise KVKK’ya göre daha genel nitelikte bir kanun olmasının yanında, kişisel verilerin korunması alanına yönelik özel hükümler içermektedir. Bu anlamda KVKK, kişisel verilerin korunmasıyla ilgili olarak daha önceden TCK’da düzenlenen suç tiplerine kendi özel hükümleriyle ışık tutmaktadır. Ele alınan bu iki kanun, kişisel verilerin korunmasına yönelik spesifik suç tiplerinin nasıl yorumlanması gerektiği açısından birbirlerinin tamamlayıcısıdır. Bu doğrultuda, KVKK’nın “Suçlar” başlıklı 17. maddesinde ve “Kabahatler” başlıklı 18.

---

<sup>282</sup> **Küzeci**, Kişisel Verilerin Korunması, s. 405.

<sup>283</sup> Bu durumun suçta ve cezada kanunilik ve belirlilik ilkesine aykırı olduğu hususu Yargıtay’ın 2014 tarihli muhalefet şerhlerine de yansımıştır: “İtiraz gerekçelerimiz; Türk Ceza Kanunu’nda kişisel verilerle ilgili bir tanım ve sınırlandırmanın yapılmaması nedeniyle kişisel verilerle ilgili maddeler suçta ve cezada kanunilik ilkesini ihlal ettiğinden Anayasa’ya aykırı oldukları, tanım yapılmasının sınırlarını suçta ve cezada kanunilik ve belirlilik ilkesi nazara alınarak...”. Yargıtay 12. Ceza Dairesi’nin 2014/607 E., 2014/16665 K. sayılı ve 07.07.2014 tarihli kararı, (Lexpera), erişim tarihi: 26.09.2021; Yargıtay 12. Ceza Dairesi’nin 2013/27402 E., 2014/15379 K. sayılı ve 23.06.2014 tarihli kararı, (Lexpera), erişim tarihi: 26.09.2021.

<sup>284</sup> **Küzeci**, Kişisel Verilerin Korunması, s. 406.

<sup>285</sup> KVKK’nın genel gerekçesi, erişim için bkz.: <https://www2.tbmm.gov.tr/d26/1/1-0541.pdf>, erişim tarihi: 15.08.2021.

maddesinde ceza hukukunu ilgilendiren bazı düzenlemelere yer verilmiştir. Ancak ne var ki bu düzenlemeler birtakım soru işaretlerini de beraberinde getirmiştir<sup>286</sup>.

Diğer yandan, kişisel verilerin işlenmesi kavramı KVKK'nın 3. maddesinin 1. fıkrasının e bendinde “...elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem” olarak tanımlanmıştır. Dolayısıyla TCK'nın 135. maddesinde yer alan kişisel verilerin kaydedilmesi suç tipine karşılık veri işleme kavramı içerisinde verilerin “kaydedilmesi”, TCK'nın 137. maddesinde yer alan verilerin yok etmeme davranışına karşılık ise verilerin “depolanması, muhafaza edilmesi” ifadeleri kullanılabilir. Çalışmada ele alıp incelenen, TCK'nın 136. maddesinde yer alan kişisel verileri verme, yayma veya ele geçirme suç tipine benzeyen ise veri işleme kavramı içerisinde verilerin “açıklanması, aktarılması, elde edilmesi” ifadeleridir<sup>287</sup>.

Kişisel verilerin korunmasına ilişkin düzenlemeler ceza muhakemesini de yakından ilgilendirmektedir. Nitekim ceza muhakemesi yoluyla kişisel verilerin işlenmesi, temelinde insan haklarına bir müdahale niteliği oluşturmakta; ancak maddi gerçeğe ulaşma amacı bu müdahaleyi hukuka uygun hale getirmektedir. Soruşturma veya kovuşturmanın gereği gibi yerine getirilebilmesi için, diğer bir ifadeyle maddi gerçeğe ulaşılabilmesi için şüpheli veya sanığın birtakım işlemlere karşı koymama şeklinde bir “katlanma yükümlülüğü” bulunmaktadır<sup>288</sup>. Ancak ne var ki, maddi gerçeğe insan haklarına saygılı bir şekilde ulaşılması gerekmektedir<sup>289</sup>. Nitekim modern ceza muhakemesi kuralları, insan hakları ile maddi gerçeğe ulaşma amacı arasında bir denge kurmaya çalışmaktadır<sup>290</sup>. Bu anlamda kişisel verilerin korunması hakkının da bir insan hakkı olması boyutuyla ceza muhakemesine dahil olması kaçınılmazdır.

---

<sup>286</sup> **Küzeci**, *Kişisel Verilerin Korunması*, s. 379-380.

<sup>287</sup> Esasen bu durum kanunilik ilkesi açısından sakıncalı olup, suç incelemesinin yapıldığı III. bölüm 1.1. başlığında konuya ilişkin çekinceler aktarılmıştır.

<sup>288</sup> **Centel**, Nur / **Zafer**, Hamide, *Ceza Muhakemesi Hukuku*, Beta Yayınları, 16. Baskı, İstanbul 2019, s. 182 ve 194; **Sarıgül**, Ali Tanju, “Şüpheli ve Sanığın Ceza Muhakemesi İşlemlerine Katlanma Yükümlülüğüne Getirilen Sınır-Nemo Tenetur Seipsum Accusare İlkesi”, *TBB Dergisi* 2021 (153), ss. 39-64, s. 42; **İnci**, Z. Özen, “Şüpheli ve Sanığa Rağmen Bir Ceza Muhakemesi Hukuku Mu? Şüpheli ve Sanığın Ceza Muhakemesi İşlemlerine Katlanma Yükümlülüğü ve Bu Yükümlülüğün Sınırları Hakkında Düşünceler”, *Hacettepe Hukuk Fakültesi Dergisi*, 7 (2), 2017, ss. 119-168, s. 122.

<sup>289</sup> **İnci**, s. 126.

<sup>290</sup> **Karakehya**, Hakan, “Dolaylı Maddi Gerçek: Ceza Muhakemesinde Yargılama Makamının Maddi Gerçeğe Deliller Aracılığıyla Ulaşma Zorunluluğu Üzerine”, *Türkiye Adalet Akademisi Dergisi*, yıl: 7,



İdarenin gerek önleyici gerek koruyucu gerekse istihbari faaliyetleri çerçevesinde de bireylerin mahrem bilgileri işlenebilmektedir. İdarenin görev ve sorumluluklarını yerine getirebilmesi için bazı veri işleme süreçlerinin şeffaflık içermeden gerçekleştirilmesi gerekmektedir. Bu anlamda idarenin birtakım faaliyetlerinde KVKK hükümlerinin uygulanmaması yönünde istisna tutulmuştur. İstisnai durumlar yalnızca idarenin işlemleriyle de sınırlı değildir.

Çalışmanın bu bölümünde öncelikle KVKK'nın uygulanacağı haller, KVKK ile TCK'nın 5. maddesi arasındaki ilişki ve KVKK'nın "Suçlar" ve "Kabahatler" başlıklı 17. ve 18. maddeleri ele alınacaktır. Daha sonrasında KVKK'nın uygulanmayacağı haller ve bu hallerde hukuka uygunluk tespitinde hangi hükümlerin uygulanacağı incelenecektir. Akabinde, kendine özgü (*sui generis*) hukuka uygunluk nedeni olan KVKK'daki veri işleme şartları incelenecek, bu şartların TCK'daki hukuka uygunluk nedenleriyle karşılaştırması yapılacaktır. Sonrasında KVKK'nın önleyici kolluk faaliyetleri, ceza muhakemesi işlemleri ve cezaların infaz işlemleriyle arasındaki ilişki incelenecek ve KVKK açısından suçluların iadesine ilişkin hükümler ele alınacaktır. Son olarak ise, TCK'nın 136. maddesinde yer alan "Verileri hukuka aykırı olarak verme veya ele geçirme" suç tipinin incelemesine geçmeden hemen öncesinde TCK'nın 135 ve 138. maddelerinde yer alan suç tiplerinden bahsedilecektir.

## 2. KVKK'NIN UYGULANACAĞI HALLER VE KVKK'NIN TCK'NIN 5. MADDESİYLE İLİŞKİSİ

### 2.1. KVKK'nın Uygulanacağı Haller

Çalışmanın daha önceki bölümünde belirtildiği üzere veri işleme "*Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, ... gibi veriler*

---

sayı: 27, Temmuz 2016, ss. 59-82, s. 61; **Boga**, Betül Gamze, *Ceza Muhakemesinde Kişisel Verilerin Korunması*, Yayımlanmamış Yüksek Lisans Tezi, T.C. Necmettin Erbakan Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Kamu Hukuku Bilim Dalı, Konya 2021, s. 83

üzerinde gerçekleştirilen her türlü işlemi” ifade etmektedir. Bu itibarla, KVKK’nın uygulanacağı haller şu şekilde sınırlandırılabilir:

1. Kişisel verilerin tamamen veya kısmen otomatik olan yollarla işlenmesi.
2. Kişisel verilerin herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenmesi.

Veri kayıt sistemi, Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik’te<sup>291</sup> “*Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi*” olarak tanımlamaktadır.

Diğer yandan, KVKK’nın uygulanabilmesi için 28. maddesinin 1. fıkrasında yer alan tam istisna durumlarının da bulunmaması gerekmektedir. Bunun yanında, 28. maddenin 2. fıkrasında yer alan kısmî istisna durumlarında ise KVKK’nın aydınlatma yükümlülüğünün düzenlendiği 10. maddesi, zararın giderilmesini talep etme hakkı hariç olmak üzere ilgili kişinin haklarının düzenlendiği 11. maddesi ve Veri Sorumluları Siciline kayıt yükümlülüğünün düzenlendiği 16. maddesi haricindeki hükümlerinin uygulanmasına devam edilmektedir.

## **2.2. KVKK’nın TCK’nın 5. Maddesiyle İlişkisi**

KVKK, kişisel verilerin korunması alanına özgü, özel bir kanundur. Bu doğrultuda kişisel verilerin işlenmesi açısından hukuka uygunluğun da sınırlarını belirlemektedir. TCK ise kişisel verilerin korunmasıyla ilgili birtakım suç tiplerini içerisinde barındıran genel bir kanundur. Bir veri işlemeyi (davranışı) hukuka uygun hale getiren nedenler, KVKK’da ve TCK’da farklı isim ve şartlar altında düzenlenmiştir. Bu nedenler KVKK’da a) açık rıza, b) bir verinin işlenmesinin kanunlarda öngörülmesi, c) fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukukî geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, ç) bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, d) veri

---

<sup>291</sup> 28.10.2017 tarihli ve 30224 sayılı Resmî Gazete’de yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik.

sorumlusunun hukukî yükümlülüğünü yerine getirebilmesi için zorunlu olması, e) ilgili kişi tarafından alenileştirilmiş kişisel verilerin işlenmesi, f) bir hakkın tesisi, kullanılması veya korunması için zorunlu olması, g) ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması, ğ) kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından işlenmesi şeklinde düzenlenmiştir.

TCK'daki hukuka uygunluk nedenleri ise a) ilgilinin rızası, b) kanun hükmünü icra, c) yetkili merciin emrini yerine getirme, ç) zorunluluk hali, d) hakkın kullanılması, e) meşru menfaat olarak sıralanabilir. KVKK'da ve TCK'da yer alan her bir hukuka uygunluk nedeni detaylı bir şekilde çalışmanın devamında ele alınacaktır. Bu başlıkta, TCK'nın "Özel kanunlarla ilişki" başlıklı 5. maddesi dikkate alındığında KVKK tarafından ayrıca bir hukuka uygunluk nedeni (veya nedenleri) getirilip getirilemeyeceği, getirilebilir ise bu hukuka uygunluk nedeninin (veya nedenlerinin) hangi nitelikte olacağı incelenecektir.

TCK'nın "Özel kanunlarla ilişki" başlıklı 5. maddesine göre TCK'nın genel hükümleri, özel ceza kanunları ve ceza içeren kanunlardaki suçlar hakkında da uygulanır. Bu itibarla ilk başta KVKK'nın uygulama alanına bakılmaksızın, hukuka uygunluk değerlendirilmesinde KVKK'nın özel hükümlerinin değil, TCK'nın genel hükümlerinin uygulanması gerektiği düşünülebilir. Ancak burada TCK'nın ilgili maddesinin zamansal etki alanı ve KVKK'nın yürürlük tarihi gözetilerek bir sonuca varılması gerekmektedir. 5252 sayılı Türk Ceza Kanununun Yürürlük ve Uygulama Şekli Hakkında Kanun'un<sup>292</sup> geçici 1. maddesine göre "Diğer kanunların, 5237 sayılı Türk Ceza Kanununun Birinci Kitabında yer alan düzenlemelere aykırı hükümleri, ilgili kanunlarda gerekli değişiklikler yapıncaya ve en geç 31 Aralık 2008 tarihine kadar uygulanır." Dolayısıyla 01.01.2009 tarihinden itibaren; TCK'nın 5. maddesinin yürürlük tarihinden önce kabul edilmiş olan ve TCK'nın genel hükümlerine aykırı olan hükümler uygulanamayacaktır<sup>293</sup>. Diğer

<sup>292</sup> 13.11.2004 tarihli ve 25642 sayılı Resmî Gazete'de yayımlanan 5252 sayılı Türk Ceza Kanununun Yürürlük Ve Uygulama Şekli Hakkında Kanun. Çalışmanın devamında "5252 sayılı Kanun" olarak isimlendirilecektir.

<sup>293</sup> **Türay**, Aras, "5237 Sayılı Türk Ceza Kanunu'nun 5. Maddesine İlişkin Bir İnceleme", T.C. Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, Özel Sayı: Prof. Dr. Nur Centel'e Armağan, Yıl: 2013, Cilt: 19, Sayı: 2, ss. 1727-1747, s. 1734.

yandan, konuya normlar hiyerarşisi bakımından yaklaşıldığında, TCK'nın 5. maddesinin KVKK'nın hukuka uygunluk nedenlerini düzenleyen maddelerinden teknik anlamda bir farkı bulunmamaktadır. Nitekim her iki norm da “kanun” düzeyindedir. Bu durumda, TCK'nın 5. maddesinin, yürürlük tarihinden sonra kabul edilen kanunlar üzerinde *lex posterior derogat priori* ilkesi gereğince bir etkisinin olmayacağı kabul edilmelidir<sup>294</sup>. KVKK da 2016 yılında yürürlüğe girdiğine göre, KVKK'nın uygulanacağı durumlarda hukuka uygunluk nedenlerinin saptanmasında KVKK'nın ilgili hükümlerine gidilmelidir.

Peki KVKK'daki hukuka uygunluk nedenleri hangi nitelikte olacaktır? Esasen KVKK'daki hukuka uygunluk nedenlerinin kullanılması, TCK'daki hakkın kullanılması hukuka uygunluk nedenine benzemekle birlikte; KVKK'daki hukuka uygunluk nedenleri tam olarak TCK'daki hakkın kullanılması çerçevesinde ele alınmamalıdır. Nitekim hak, hukuk tarafından korunan menfaat anlamına gelir<sup>295</sup>. Kişisel verilerin korunmasında hak, ilgili kişiye aittir ki bu hak kişisel verilerin korunması hakkı olarak ele alınmaktadır. Buna karşılık, kişisel verilerin korunması hakkını ihlal eden kişiye bir hak tanındığından bahsedilemez. Nitekim kişisel verilerin korunmasına ilişkin düzenlemelerde “Yasaklanmadıkça her şey serbesttir” prensibi değil, “İzin verilmedikçe her şey yasaktır” prensibi geçerlidir<sup>296</sup>. Bu doğrultuda, zaman zaman örtüşebilmekle birlikte, KVKK'da yer alan hukuka uygunluk nedenlerinin tamamen TCK'daki hakkın tesisi çerçevesinde ele alınması mümkün görünmemektedir.

Diğer yandan, bu nedenlerle TCK'daki kanun hükmünü yerine getirme arasındaki ilişkinin de saptanması gerekmektedir. Esasen kanun hükmünün yerine getirilmesini hakkın kullanılmasından ayıran, onun görev veya yetki niteliğinde olmasıdır<sup>297</sup>. Bu itibarla KVKK'daki bazı veri işleme faaliyetlerinin bir görevden veya yetkiden kaynaklandığı söylenebilir ise de bu faaliyetlerin tamamı görev veya yetki çerçevesinde gerçekleştirilmemektedir. Dolayısıyla, KVKK'da yer alan hukuka uygunluk nedenlerinin

---

<sup>294</sup> Centel, Nur / Zafer, Hamide / Çakmut, Özlem, *Türk Ceza Hukukuna Giriş*, Beta Yayınları, Yenilenmiş ve Gözden Geçirilmiş 11. Bası, İstanbul, 2020, s. 81; Türay, s. 1735.

<sup>295</sup> Özen, Mustafa, *Ceza Hukuku Genel Hükümler Dersleri*, Adalet Yayınevi, Ankara, 2020, s. 407.

<sup>296</sup> Kişisel Verileri Koruma Kurumu, *Kişisel Veri Güvenliği Rehberi*, KVKK Yayınları, Ankara, Ocak 2018, s. 9, erişim için bkz.: [https://www.kvkk.gov.tr/yayinlar/veri\\_guvenligi\\_rehberi.pdf](https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf), erişim tarihi: 03.10.2021.

<sup>297</sup> Özbek, Veli Özer / Doğan, Koray / Bacaksız, Pınar, *Türk Ceza Hukuku Genel Hükümler, Seçkin Yayıncılık, Güncellenmiş ve Gözden Geçirilmiş 11. Baskı*, Ankara 2020, (Özbek / Doğan / Bacaksız, Genel Hükümler), s. 283.

TCK'daki kanun hükmünü yerine getirmenin tamamen bir yansıması olduğunun söylenmesi de doğru olmayacaktır.

Sonuç olarak, TCK'nın 5. maddesi karşısında özel bir kanun olan KVKK ile, TCK'daki genel hükümlerde yer alanlardan farklı hukuka uygunluk nedenleri getirilebilir. Bu hukuka uygunluk nedenleri kimi zaman TCK'daki genel hukuka uygunluk nedenlerinin bir görünümü olabilse de çoğunlukla kendine özgü (*sui generis*) niteliktedir. KVKK'nın uygulama alanı bulduğu hallerde, hukuka uygunluk nedenlerinin tespit edilmesi bakımından KVKK'daki hukuka uygunluk nedenlerinin incelenmesi gerekmektedir.

### **3. KVKK'NIN 17. VE 18. MADDELERİNE İLİŞKİN DEĞERLENDİRMELER**

#### **3.1. Genel Olarak**

KVKK hükümlerine uyulmaması halinde karşılaşılabilecek “Suçlar” ve “Kabahatler” KVKK'nın 17. ve 18. Maddelerinde aşağıdaki şekilde hüküm altına alınmıştır:

##### ***“Suçlar***

**MADDE 17-** (1) *Kişisel verilere ilişkin suçlar bakımından 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununun 135 ila 140 ıncı madde hükümleri uygulanır.*

(2) *Bu Kanunun 7 nci maddesi hükmüne aykırı olarak; kişisel verileri silmeyen veya anonim hâle getirmeyenler 5237 sayılı Kanunun 138 inci maddesine göre cezalandırılır.*

##### ***Kabahatler***

**MADDE 18-** (1) *Bu Kanunun;*

a) *10 uncu maddesinde öngörülen aydınlatma yükümlülüğünü yerine getirmeyenler hakkında 5.000 Türk lirasından 100.000 Türk lirasına kadar,*

b) *12 nci maddesinde öngörülen veri güvenliğine ilişkin yükümlülükleri yerine getirmeyenler hakkında 15.000 Türk lirasından 1.000.000 Türk lirasına kadar,*

- c) 15 inci maddesi uyarınca Kurul tarafından verilen kararları yerine getirmeyenler hakkında 25.000 Türk lirasından 1.000.000 Türk lirasına kadar,
- ç) 16 ncı maddesinde öngörülen Veri Sorumluları Siciline kayıt ve bildirim yükümlülüğüne aykırı hareket edenler hakkında 20.000 Türk lirasından 1.000.000 Türk lirasına kadar idari para cezası verilir.”

Ne var ki bu hükümlerin uygulanmasıyla ilgili birtakım belirsizlikler bulunmaktadır. Bu belirsizlikler KVKK'nın 17. maddesi için cezanın niteliği ve derecelendirilmesi, hükmün uygulanacağı davranış ve işlemlerin kapsamı, cezayı artıran sebepler ve hükümlerin uygulanabilme zamanı, KVKK'nın 18. maddesi içinse yaptırıma konu aykırılıklar ve yaptırımın derecelendirilmesi şeklinde sıralanabilir. Bu başlıkta, sözü edilen belirsizliklere yönelik değerlendirmelerde bulunulacaktır.

## **3.2. KVKK'nın 17. Maddesine İlişkin Değerlendirmeler**

### **3.2.1. Cezanın Niteliği ve Derecelendirilmesi Açısından**

KVKK'da cezanın niteliği konusunda bir sınıflandırma yapılmadığı, herhangi bir derecelendirmeye başvurulmadığı görülmektedir. Dolayısıyla örneğin iş yerinde çalışan bir kişinin, müşteri ziyaretinde müşterisiyle çekildiği bir fotoğrafı herhangi bir kötü niyet taşımadan internet ortamında KVKK'ya aykırı bir şekilde paylaşması ile aynı kişinin iş yerinin tüm müşteri bilgilerini belirli bir bedel karşılığında satması arasında cezanın niteliği açısından KVKK'da bir fark gözetilmemiştir. Ne var ki, cezanın alt veya üst sınırı açısından yapılacak değerlendirme yargıcın takdirinde olup, TCK'nın “*Cezaların belirlenmesi*” başlıklı 61. maddesine göre değerlendirme yapılacaktır<sup>298</sup>.

Bunun yanında TCK'nın 140. maddesinde her ne kadar ilgili maddelerde tanımlanan suçların işlenmesi dolayısıyla tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunacağına ilişkin hüküm yer olsa da bu güvenlik tedbirlerinin caydırıcılığı ile hürriyeti bağlayıcı bir ceza olan hapis cezasının caydırıcılığı eşit değildir. Bu anlamda

<sup>298</sup> **Küzeci**, Kişisel Verilerin Korunması, s. 379.

hem suçların ve cezaların belirliliği ilkesi açısından hem de caydırıcılık noktasındaki eşitsizlik açısından KVKK'nın 17. maddesindeki düzenlemenin eksik bir düzenleme olduğunu söylemek mümkündür<sup>299</sup>.

AB uygulamasında ise GDPR'da ayrı bir cezaî yaptırım düzenlenmediği; ancak üye devletlere bu alanda takdir yetkisi tanındığı görülmektedir<sup>300</sup>. Üye devletler tarafından cezaî yaptırımın benimsenmesi halinde ise cezaların etkili, caydırıcı ve cezalandırıcı olması istenmiş<sup>301</sup>; bunun yanında aynı suçtan iki kez yargılanmama ilkesinin gözetilmesi gerektiği belirtilmiştir<sup>302</sup>.

### 3.2.2. Hükümün Uygulanacağı Davranış ve İşlemlerin Kapsamı Açısından

Anayasa'nın 38. maddesine göre “Hiç kimse, işlendiği zaman yürürlükte bulunan kanunun suç saymadığı bir fiilden dolayı cezalandırılmaz.” Yine TCK'nın 2. maddesine göre de “Kanunun açıkça suç saymadığı bir fiil için kimseye ceza verilemez ve güvenlik tedbiri uygulanamaz. Kanunda yazılı cezalardan ve güvenlik tedbirlerinden başka bir ceza ve güvenlik tedbirine hükmolunamaz. İdarenin düzenleyici işlemleriyle suç ve ceza konulamaz. Kanunların suç ve ceza içeren hükümlerinin uygulanmasında kıyas yapılamaz. Suç ve ceza içeren hükümler, kıyasa yol açacak biçimde geniş yorumlanamaz.” TCK'nın 135 vd. maddelerindeki kaydetme, verme, yayma, ele geçirme ve verileri yok etmeme davranışları bir veri işleme türü olarak düzenlenmiştir. Dolayısıyla bu davranışların gerçekleşmesi halinde TCK'daki suç tiplerinin inceleneceği açıktır. Ancak KVKK'da yer alan veri işleme türlerinin tamamı ceza kanunlarında düzenlenmemiştir. Eğer kanunda bir davranış suç olarak düzenlenmemişse, o davranış suç olarak ele alınamaz<sup>303</sup>. Suça da ancak kanunda gösterilen ceza uygulanabilir<sup>304</sup>.

<sup>299</sup> Küzeci, Kişisel Verilerin Korunması, s. 379.

<sup>300</sup> Küzeci, Kişisel Verilerin Korunması, s. 379.

<sup>301</sup> GDPR'nın 84. maddesinde ve başlangıç hükümlerinin 152. paragrafında bu durum “effective, proportionate and dissuasive” olarak ifade edilmiştir.

<sup>302</sup> GDPR'nın başlangıç hükümlerinin 149. paragrafında “ne bis in idem” (aynı suçtan iki kez yargılanmama) ilkesine uyulması gerektiği belirtilmiştir.

<sup>303</sup> Hakeri, Hakan, *Ceza Hukuku Genel Hükümler*, Adalet Yayınevi, 24. Baskı, Ankara, 2021, s. 12; Özen, s. 69.

<sup>304</sup> Özbek / Doğan / Bacaksız, Genel Hükümler, s. 214. Özgenç, İzzet, *Türk Ceza Hukuku Genel Hükümler*, Seçkin Yayıncılık, Gözden Geçirilmiş ve Güncellenmiş 16. Bası, Ankara 2020, s. 65.

Dolayısıyla ceza kanunlarında yer almayan ancak veri işleme türü olan davranışlar açısından hangi hükümlerin uygulanacağı bir soru işaretidir. Bu doğrultuda bir kıyas metodu geliştirilmesi ise kıyas yasağına aykırılık teşkil edecektir. Nitekim kıyas, kanunda açıkça yazılı olmayan bir davranışın, kanunda suç olarak gösterilen bir davranışa benzetilerek cezalandırılması anlamına gelmekte olup, buna olanak tanımak suçta ve cezada kanunilik ilkesi ile bağdaşmayacaktır<sup>305</sup>. Bu doğrultuda önerimiz, TCK'nın 135 vd. maddelerinde yer alan suç tanımlarının veri işleme tanımıyla paralel bir şekilde değiştirilmesidir.

### 3.2.3. Cezayı Artıran Sebepler ile Özel Nitelikli Kişisel Veriler Açısından

KVKK'nın "*Özel nitelikli kişisel verilerin işleme şartları*" başlıklı 6. maddesinin 3. fıkrasında özel nitelikli kişisel veriler sınırlı sayıda (*numerus clausus*) belirtilmiştir. Buna göre "*Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri*" özel nitelikli kişisel veridir. TCK'nın 135. maddesinin 2. fıkrasına göre "*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.*" Görüleceği üzere burada sayılan kişisel veri türleri ile özel nitelikli kişisel veriler arasında bir dengesizlik bulunmaktadır. Özel nitelikli olmayan "*ahlaki eğilim*" kategorisindeki kişisel verilere TCK'nın 135. maddesinde yer verilirken; özel nitelikli olan etnik köken, mezhep ve diğer inançlar, kılık ve kıyafet, dernek ya da vakıf üyeliği, ceza mahkumiyeti, güvenlik tedbirleri, biyometrik ve genetik veri kategorisinde olan kişisel verilere TCK'nın 135. maddesinde yer verilmemiştir. Böylelikle aynı kategoride ve aynı düzenlemeye tabi olan kişisel veriler için farklı bir cezai yaptırım benimsenmesi gibi orantısız bir sonuç ortaya çıkmıştır<sup>306</sup>. Bu nedenle, TCK'nın ilgili maddesinin KVKK'nın

<sup>305</sup> Centel / Zafer / Çakmut, s. 53.

<sup>306</sup> Küzeci, Kişisel Verilerin Korunması, s. 381.



özel nitelikli kişisel verileri düzenleyen maddesi doğrultusunda değiştirilmesi gerektiği kanaatindeyiz.

### **3.2.4. Hükümlerin Uygulanabilme Zamanı Açısından**

KVKK 07.06.2016 tarihinde yürürlüğe girmiştir. Ne var ki KVKK'nın uygulanması açısından farklı süreler öngörülmüştür. Nitekim KVKK'nın geçici 1. maddesinin 3. fıkrasına göre *“Bu Kanunun yayımı tarihinden önce işlenmiş olan kişisel veriler, yayımı tarihinden itibaren iki yıl içinde bu Kanun hükümlerine uygun hâle getirilir.”* Diğer yandan KVKK'nın 32. maddesinin 1. fıkrasının a bendine göre *“Kanunun 8 inci, 9 uncu, 11 inci, 13 üncü, 14 üncü, 15 inci, 16 ncı, 17 nci ve 18 inci maddeleri yayımı tarihinden altı ay sonra yürürlüğe girer.”* Dolayısıyla kişisel verilere ilişkin suçlar bakımından TCK'nın 135 vd. maddelerinin hükümlerinin uygulanacağını belirtildiği 17. madde, KVKK'nın yayımlanmasından altı ay sonra yürürlüğe girmiştir. Bu zaman aralığında kişisel verilere ilişkin suçlar bakımından hangi maddenin uygulanacağı belirtilmemiştir. Her ne kadar meclis görüşmelerinde KVKK'nın 17. maddesine bu hususa ilişkin olarak TCK'daki 135 vd. maddelerinin aynen korunacağı yönünde hüküm eklenmesi hususu konuşulsa da bu şekilde bir hüküm eklenmesine gerek duyulmamış, yalnızca ilgili maddelere atıfta bulunulmuştur<sup>307</sup>. Bu durumda KVKK yürürlüğe girmeden önce ne yapılıyor ise arada kalan zaman diliminde de aynısının yapılması söz konusu olmuştur.

## **3.3. KVKK'nın 18. Maddesine İlişkin Değerlendirmeler**

### **3.3.1. Yaptırıma Konu Aykırılıklar Açısından**

KVKK'nın 18. maddesinin ilk olarak idari para cezasına konu olan aykırılıklar açısından ele alınması gerekmektedir. İdari para cezasına konu olan aykırılıklar aydınlatma

<sup>307</sup> TBMM Tutanak Dergisi, 26. Dönem, Cilt: 12, Yasama Yılı: 1, 60. Birleşim, 7. Oturum, 23.03.2016, s. 397 ve 399, erişim için bkz.: <https://www5.tbmm.gov.tr/tutanaklar/TUTANAK/TBMM/d26/c012/tbmm26012060.pdf>, erişim tarihi. 22.09.2021.

yükümlülüğünü yerine getirmeme, veri güvenliğine ilişkin yükümlülükleri yerine getirmeme, Kişisel Verileri Koruma Kurulu kararlarını yerine getirmeme ile Sicile kayıt ve bildirim yükümlülüğüne aykırı hareket etme olarak belirtilmiştir. Bu yönüyle birtakım hukuka aykırılıkların idari para cezasına tabi tutulmadığı görülmektedir. Örneğin daha önceki bölümde incelenen KVKK'nın genel ilkelerine aykırılık halinde bir yaptırım uygulanacağı öngörülmemiştir<sup>308</sup>. Dolayısıyla genel ilkelere aykırı hareket edildiği takdirde ne olacağı belirsizdir. Diğer yandan, KVKK'nın 12. maddesinde “*Veri sorumlusu; a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek, c) Kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.*” hükmü yer almaktadır. Ancak gerekli tedbirlerin neler olduğu KVKK'da değil, Kişisel Veri Güvenliği Rehberi'nde belirtilmiştir<sup>309</sup>. Bunun bir sonucu olarak, belirtilen tedbirler kapsamında yer alan bazı durumlar idari para cezasının konusu olurken, bazı durumlar açısından idari para cezasının uygulanması söz konusu olmayacaktır<sup>310</sup>. Dolayısıyla yaptırımın hangi hukuka aykırılık durumunda uygulanıp uygulanmayacağı belirsizliği, belirlilik ilkesine zarar verici niteliktedir<sup>311</sup>. Bu doğrultuda önerimiz, hukuka aykırılık halinde buna denk gelen yaptırımın sınırlarının net bir şekilde çizildiği bir düzenlemenin KVKK'ya dahil edilmesidir.

### 3.3.2. Yaptırımın Derecelendirilmemesi Açısından

İdari para cezasının alt ve üst sınırlarının neye göre belirleneceği KVKK'da belirtilmemiştir. Bunun yerine madde gerekçesinde bu belirlemenin kabahatin haksızlık içeriği ile failin kusuru ve ekonomik durumu alınarak yapılacağı ifade edilmiştir. Ekonomik durumun ölçütleri açısından ise herhangi bir kriter öngörülmemiştir. Dolayısıyla idari para cezalarının alt ve üst sınırının nasıl belirleneceğine ilişkin bir belirsizlik mevcuttur<sup>312</sup>. Bu konuya ilişkin olarak, hükmedilecek idari para cezasında

<sup>308</sup> **Küzeci**, Kişisel Verilerin Korunması, s. 375.

<sup>309</sup> Kişisel Verileri Koruma Kurumu, *Kişisel Veri Güvenliği Rehberi*.

<sup>310</sup> **Küzeci**, Kişisel Verilerin Korunması, s. 375.

<sup>311</sup> **Küzeci**, Kişisel Verilerin Korunması, s. 375.

<sup>312</sup> **Küzeci**, Kişisel Verilerin Korunması, s. 376.

kriter olan hususların madde metninde belirtilmesinin şeffaflığın sağlanması adına gerekli olduğunu düşünmekteyiz<sup>313</sup>.

Diğer yandan, yaptırımın davranış esas alınarak mı yoksa ilgili kişi sayısı esas alınarak mı belirleneceği hususu da net değildir<sup>314</sup>. Örneğin bir şirketin veri tabanında yer alan 10.000 kişiye ait kişisel verilerin ihlale konu olduğu varsayımında yaptırım, davranış temel alınarak belirlenip üst sınıra mı yaklaşacaktır, yoksa bir kişi açısından değerlendirme yapıp para cezası tutarı 10.000 ile mi çarpılacaktır?<sup>315</sup> İdari para cezası miktarlarının yüksek tutulması, cezaların caydırıcı ve etkili olması açısından önemli olmakla birlikte bu miktarların aynı zamanda orantılı ve öngörülebilir olması gerekmektedir<sup>316</sup>. Bu doğrultuda, idari yaptırım uygulanırken esas alınacak ölçütlerin orantılı bir şekilde belirlenmesi ve TCK'nın 61. maddesinde olduğu gibi bu ölçütlere KVKK'da yer verilmesi gerektiğini düşünmekteyiz.

#### 4. KVKK'NIN UYGULANMAYACAĞI HALLER VE BU HALLERDE İZLENİLECEK YÖNTEM

##### 4.1. Genel Olarak

KVKK'nın uygulanmayacağı haller kişi, 28. madde istisna halleri ve kişisel verinin tutulduğu yer bakımından olmak üzere üç farklı şekilde ele alınabilir. Esasen kişi bakımından uygulanmama alanları çalışmanın I. bölümünde incelendiğinden, bu başlık altında KVKK'nın istisnai durumlarını düzenleyen 28. maddesindeki istisna halleri ve

<sup>313</sup> Aynı yönde görüş için bkz.: **Küzeci**, Kişisel Verilerin Korunması, s. 376.

<sup>314</sup> **Küzeci**, Kişisel Verilerin Korunması, s. 376.

<sup>315</sup> Örneğin 31.03.2005 tarihli ve 25772 (Mük.) sayılı Resmî Gazete'de yayımlanan 5326 sayılı Kabahatler Kanunu'nun 15. maddesinin 1 ve 2. fıkralarında bu durum açıktır:

*“İçtima Madde 15- (1) Bir fiil ile birden fazla kabahatin işlenmesi halinde bu kabahatlere ilişkin tanımlarda sadece idarî para cezası öngörülmüşse, en ağır idarî para cezası verilir. Bu kabahatlerle ilgili olarak kanunda idarî para cezasından başka idarî yaptırımlar da öngörülmüş ise, bu yaptırımların her birinin uygulanmasına karar verilir. (2) Aynı kabahatin birden fazla işlenmesi halinde her bir kabahatle ilgili olarak ayrı ayrı idarî para cezası verilir. Kesintisiz fiille işlenebilen kabahatlerde, bu nedenle idarî yaptırım kararı verilinceye kadar fiil tek sayılır.”*

<sup>316</sup> **Küzeci**, Kişisel Verilerin Korunması, s. 376.

kişisel verinin tutulduğu yer bakımından uygulanmaması üzerinde durulacaktır. Ancak yine de kişi bakımından uygulama alanına yönelik kısa açıklamalarda bulunulacaktır.

KVKK'nın kişi bakımından uygulama alanı, gerçek kişilerin kişisel verilerinin işlenmesiyle sınırlandırılmıştır. Nitekim KVKK'nın 2. maddesinde yer alan "*Bu kanun hükümleri, kişisel verileri işlenen gerçek kişiler ile bu verileri ... işleyen gerçek ve tüzel kişiler hakkında uygulanır.*" hükmünden, tüzel kişilerin verilerinin işlenmesi durumunda KVKK hükümlerinin uygulanmayacağı anlaşılmaktadır.

Yine ilgili hükümden yola çıkılarak KVKK'nın a) Tamamen veya kısmen otomatik olan yollarla kişisel veri işlenmesi b) Herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla kişisel veri işlenmesi hallerinde uygulanacağı sonucuna ulaşılmaktadır. Dolayısıyla konu bakımından, herhangi bir veri kayıt sisteminin parçası olunmadığı ve aynı zamanda otomatik olmayan yollarla kişisel veri işlendiği durumlarda KVKK hükümleri uygulanmayacaktır.

Diğer yandan 28. maddede tam ve kısmî istisna halleri düzenlenmiştir. Buna göre 28. maddenin 1. fıkrasında yer alan hallerde KVKK'nın hiçbir hükmünün uygulanmaması, 2. fıkrasında yer alan hallerde ise KVKK'nın birtakım hükümlerinin uygulanmaması söz konusu olacaktır.

## **4.2. Tam İstisna Halleri (m. 28/1)**

KVKK'nın tam istisna halleri 28. maddenin 1. fıkrasında düzenlenmiştir. Buna göre anılan fıkrada yer alan hallerden herhangi birisinin mevcut olması durumunda KVKK'nın hiçbir hükmü uygulanmayacaktır.

### **4.2.1. Kişinin Kendisiyle veya Aynı Konutta Yaşayan Aile Bireyleriyle İlgili Kişisel Verileri İşlemesi**

Tam istisna hallerinden ilki; "*Kişisel verilerin, üçüncü kişilere verilmemek ve veri güvenliğine ilişkin yükümlülüklere uyulmak kaydıyla gerçek kişiler tarafından tamamen*

*kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında işlenmesi”dir.*

AB hukukunda bu istisnai halin benzeri “*kişinin kişisel amaçlarla*” işlediği kişisel veriler açısından düzenlenmiştir<sup>317</sup>. Ancak AB hukukunda, Türk hukukundaki gibi *yalnızca kişinin kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili olma durumu* şeklinde bir sınırlama değil, *maddi çıkar olmadan kişisel amaçlarla veya ev içi etkinliklerde (household activity) gerçekleştirilen kişisel veri işleme süreçleri* şeklinde bir sınırlama yapılmıştır<sup>318</sup>. Dolayısıyla KVKK’daki “*kendisiyle ilgili*” ifadesi ile AB hukukundaki “*kişisel amaçlarla*” ifadesinin farklılığı dikkat çekmektedir. Örneğin bir kişinin telefon defteri tuttuğu ve bu yolla kişisel veri işlediği durumda bu kişi, AB’deki düzenlemeden muaf tutulacak; ancak KVKK kapsamında sorumlu olacaktır<sup>319</sup>.

KVKK hükmü ile AB hukukundaki düzenlemelerin farklılaştığı diğer bir husus, kişi bakımından sınırlamadır. AB hukukunda istisna kapsamı “*aynı konutta beraber yaşayanlar*” bakımından düzenlenirken; KVKK’da “*aynı konutta yaşayan aile fertleriyle ilgili faaliyetler*” bakımından düzenlenmiştir. Aile ferdinin tespitinde TMK hükümlerinin uygulanması gerekmektedir. Önemle belirtmek gerekir ki GDPR’da kişisel ve ev içi etkinlikleri; haberleşme, sosyal ağlarda yer alma, çevrim içi etkinliklerde bulunma gibi konuları kapsamaktadır<sup>320</sup>. Dolayısıyla örneğin bir aile ferdi olmayan ancak aynı evi paylaşan kişilerin internete bağlandıkları durumlarda KVKK hükümleri uygulanmaya devam edecektir<sup>321</sup>.

Bu istisna halinin uygulanabilmesi için kişisel verilerin üçüncü kişilere verilmemesi ve veri güvenliğine ilişkin yükümlülükler aykırı hareket edilmemesi gerekmektedir<sup>322</sup>. Ancak yukarıda verilen örnekte, aile ferdi olsun veya olmasın, aynı evi paylaşan kişilerin aynı ağdan internete bağlandığı durumlarda internet protokolü (IP) adresi, lokasyon gibi birtakım bilgilerin üçüncü kişilere aktarılması söz konusu olacaktır. Dolayısıyla anılan istisna hükmü, bu kişiler açısından nasıl bir yol izleneceği sorusunu da beraberinde getirmektedir<sup>323</sup>. Kanaatimizce bu ayrıksı durumun da istisna maddesine dahil olması

<sup>317</sup> 95/46/EC sayılı Direktif’in 3. maddesinin 2. fıkrası ve GDPR’ın 2. maddesinin 2. fıkrasının d bendi.

<sup>318</sup> **Küzeci**, Kişisel Verilerin Korunması, s. 329; **Çekin**, s. 28.

<sup>319</sup> **Küzeci**, Kişisel Verilerin Korunması, s. 329.

<sup>320</sup> GDPR, Giriş par. 18.

<sup>321</sup> **Küzeci**, Kişisel Verilerin Korunması, s. 329.

<sup>322</sup> **Dülger**, Kişisel Verilerin Korunması, s. 349.

<sup>323</sup> **Küzeci**, Kişisel Verilerin Korunması, s. 329.

gerekirdi. Nitekim aksi durumda aynı modemden internete bağlanan kişilerin, bu modemi kullanan diğer kişileri aydınlatma yükümlülüğü bulunacaktır ki bu süreç, birlikte yaşamının doğal sonucuna aykırı olacaktır.

#### 4.2.2. İstatistik, Araştırma ve Planlama Amacıyla Kişisel Verilerin İşlenmesi

Tam istisna hallerinden ikincisi, “*Kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi*”dir. Burada a) resmi istatistik amacıyla işleme ve b) araştırma, planlama ve istatistik gibi amaçlarla işleme şeklinde ikili bir ayırım yapıldığı görülmektedir.

Resmî istatistik amacıyla işlemlerin tamamı KVKK’dan muaf tutulmuş; bu işlemler için herhangi bir anonimleştirme şartı aranmamıştır. İstatistiki bilgilerin toplanması, devletin planlama yapma ve politika belirleme gibi temel görevlerini yerine getirmesi bakımından oldukça önemlidir<sup>324</sup>. Ancak bu önemin karşısında, kişisel verilerin korunması ve güncel tutulmasının gerektiği de açıktır. Örneğin bir kişi, kişisel verilerinin toplanması ve işlenmesinde özel yasaların kendisini korumayacağını bilmesi halinde tam ve doğru bilgiyi vermeyebilir<sup>325</sup>. Bu durum da devletin gerçekleştireceği planlamaların aslında yanlış kaynaklar esas alınarak yapılacağı ve dolayısıyla gerçekten etkili bir sonuç veremeyeceği sonucunu beraberinde getirir.

Diğer yandan, kişisel verilerin araştırma, planlama ve istatistik gibi amaçlarla işlenmesi durumuna yönelik olarak “*gibi*” ifadesinin kullanıldığı görülmektedir. Dolayısıyla istisna kapsamında olan amaçların yalnızca sayılanlardan ibaret olmadığı, bu amaçlara benzer amaçların da aynı istisna kapsamında ele alınabileceği anlaşılmaktadır<sup>326</sup>. Mevcut şekliyle “*gibi*” ifadesi geniş yorumlanmaya çok müsaittir<sup>327</sup>. Öte yandan fıkra bulunan araştırma, planlama ve istatistik amaçların da neyi hedeflediğinin madde metninde belirtilmesi, kişisel verilerin korunması ruhuna uygunluğun ve şeffaflığın sağlanması açısından yerinde olacaktır.

<sup>324</sup> **Küzeci**, Kişisel Verilerin Korunması, s. 330.

<sup>325</sup> **Küzeci**, Kişisel Verilerin Korunması, s. 330.

<sup>326</sup> **Dülger**, Kişisel Verilerin Korunması, s. 351.

<sup>327</sup> Aynı yönde görüş için bkz.: **Küzeci**, Kişisel Verilerin Korunması, s. 330.

Son olarak, bu istisna halinin resmi istatistik dışında uygulanabilmesi için kişisel verilerin anonim hale getirilerek işlenmesi gerekmektedir. Anonim hale getirme, veri işlemeden önce yapılmalıdır. Bunun yanında, kişisel veriler anonimleştirildiğinde zaten “*kişisel*” veri olma vasfını kaybedeceğinden, madde metninde aranan anonim hale getirme kriteri anlam karışıklığı yaratabilmektedir.

#### **4.2.3. Sanat, Tarih, Edebiyat veya Bilimsel Amaçlarla ya da İfade Özgürlüğü Kapsamında Kişisel Verilerin İşlenmesi**

KVKK'nın bir diğer tam istisna hali “*Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi*”dir.

Burada ifade özgürlüğü üzerinde ayrıca durulması gerekir. Nitekim ifade özgürlüğü ile kişisel verilerin korunması hakkı kimi zaman birbirine paralel, kimi zamansa birbiriyle yarışan haklardır<sup>328</sup>. Dolayısıyla bu iki hakkın arasında mutlaka bir dengenin kurulması gerekmektedir<sup>329</sup>. Kişisel Verileri Koruma Kurulu'nun ifade özgürlüğü kapsamında vermiş olduğu önemli kararlar bulunmaktadır. Bu kararlardan ilkinde Kurul, kişinin babasının kanser tedavisi nedeniyle bir süre önce görevine ara verdiğine ilişkin köşe yazısında yayınlanan bir haberin kaldırılması talebiyle ilgili başvuruda “... *özel nitelikli kişisel veri niteliğindeki sağlık verisinin söz konusu köşe yazısına konu edilerek yayımlanmasında halihazırda kamu yararı bulunmadığı, bu itibarla çatışan haklar bakımından kişilik haklarının ifade özgürlüğüne üstün geldiği kanaatine varıldığından...*” ifadelerine yer vererek çatışan haklar bakımından kişilik haklarını, dolayısıyla bununla bağlantılı olarak somut olayda kişisel verilerin korunması hakkını ifade özgürlüğünden daha üstün görmüştür<sup>330</sup>. Kurul'un bu iki hak arasındaki dengenin oluşturulmasında kamu yararı kriterinden yararlandığı görülmektedir. Ancak yalnızca

<sup>328</sup> **Küzeci**, Kişisel Verilerin Korunması, s. 331.

<sup>329</sup> **Böreççi**, s. 127.

<sup>330</sup> Kişisel Verileri Koruma Kurulu'nun 09.12.2019 tarihli ve 2019/372 sayılı karar özetine erişim için bkz: <https://kvkk.gov.tr/Icerik/6663/2019-372>, erişim tarihi: 19.09.2021.

karardaki bilgilerden yola çıkılarak söz konusu kamu yararının veya dengenin tespitinde hangi kriterleri kullandığı hakkında yorum yapılması sağlıklı olmayacaktır. Nitekim anılan kararda somut olayın iç yüzü, köşe yazısının tamamı, köşe yazısının ne zaman yayımlandığı gibi hususlar belirtilmemiştir. Ancak en azından, söz konusu kişisel verilerin sağlığa ilişkin olması durumunda bu iki hak arasında kurulacak dengenin, kişisel verilerin korunması hakkı lehine olabilir. Kurul başka bir kararında “*unutulma hakkı*”nı ele almış ve kişilerin ad ve soyadı ile arama motorları üzerinden yapılan aramalarda çıkan sonuçların indeksten çıkarılmasına ilişkin değerlendirmede dikkate alınacak kriterleri duyurmuştur<sup>331</sup>. Buna göre; “a) ilgili kişinin kamusal yaşamda önemli bir rol oynayıp oynamadığı, b) arama sonuçlarının öznesinin çocuk olup olmadığı, c) bilginin içeriğinin doğru olup olmadığı, ç) bilgilerin kişilerin çalışma hayatı ile ilişkili olup olmadığı, d) arama sonuçlarında yer alan bilginin ilgili kişi hakkında hakaret, onur kırıcı, iftira niteliği taşıyıp taşımadığı, e) arama sonuçlarında yer alan bilginin özel nitelikli kişisel veri niteliği taşıyıp taşımadığı, f) arama sonuçlarında ulaşılan bilginin güncel olup olmadığı, g) arama sonucunda ulaşılan bilginin kişi hakkında önyargıya sebep olup olmadığı, ğ) arama sonucunda yer alan bilginin kişi açısından bir risk doğurup doğurmadığı, h) bilginin kişinin kendisi tarafından yayımlanıp yayımlanmadığı, ı) orijinal içeriğin gazetecilik faaliyeti kapsamında işlenen verileri kapsayıp kapsamadığı, i) ilgili kişiye ilişkin bilgilerin yayımlanmasında yasal bir zorunluluk bulunup bulunmadığı ve j) ilgili kişiye ilişkin bilginin ceza gerektiren bir suçla ilgisi olup olmadığı” hususlarının değerlendirmeye alınması gerekmektedir.

Diğer yandan, kişisel verilerin sanat, tarih, edebiyat veya bilimsel amaçlarla işlenmesi de tam istisna hali olarak düzenlenmiştir. KVKK’nın bu istisna haline yönelik olarak da bir anayasal koruma alanı bulunmaktadır. Önemle belirtmek gerekir ki kişisel verilerin sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi halinde her durumda istisnadan söz edilememektedir. Nitekim söz konusu veri işlemenin milli savunmayı, milli güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini ve kişilik haklarını ihlal etmemesi gerekmektedir<sup>332</sup>. Bu anlamda dengenin yalnızca kişisel verilerin korunması hakkı ile ifade özgürlüğü arasında değil, bu

<sup>331</sup> Kişisel Verileri Koruma Kurulu’nun 23.06.2020 tarihli ve 2020/481 sayılı karar özetine erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/6776/2020-481>, erişim tarihi: 19.09.2021.

<sup>332</sup> Çekin, s. 29; Dülger, Kişisel Verilerin Korunması, s. 352.



istisna durumunda yer alan tüm veri işleme faaliyetleri ile milli savunma, milli güvenlik, kamu güvenliği, kamu düzeni, ekonomik güvenli, özel hayatın gizliliği ve kişilik hakları arasında da kurulması gerektiği söylenebilir.

#### 4.2.4. Önleyici, Koruyucu ve İstihbari Faaliyetler Kapsamında Kişisel Verilerin İşlenmesi

“Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi” durumunda da KVKK’nın hiçbir hükmü uygulanmamaktadır. İlgili maddenin gerekçesinde “...suç gelirlerinin aklanması, terörizmin finansmanının önlenmesi ve mali suçların araştırılması konusunda yetkili birim tarafından yürütülen faaliyetler kapsamında...” yapılan veri işlemlerin bu istisna hal özelinde değerlendirileceği belirtilmiştir<sup>333</sup>.

Önleyici ve koruyucu faaliyetler sağlık alanına ilişkin olabildiği gibi, suçun önlenmesi, ceza kanunlarında suç olarak belirlenmiş olan davranışların veya kabahatlerin, bu davranışlar henüz gerçekleşmeden önce belli birimler tarafından önlenmesi faaliyetlerine ilişkin de olabilir<sup>334</sup>. Bu faaliyetleri gerçekleştirecek kişiler ise polis, jandarma gibi kolluk güçleridir<sup>335</sup>. Milli İstihbarat Teşkilatı<sup>336</sup> tarafından yayımlanan ve MİT tarihçesinin anlatıldığı kaynakta “İstihbarat (intelligence), plânlama, araştırma, deliller toplama, çeşitli aklı ve tecrübe ilmi metotlar ile onları değerlendirip bir sonuç istihsal edip, kullanma faaliyetlerini içine alan bir manaya sahip bulunmaktadır.” ifadeleri kullanılmıştır<sup>337</sup>. Önleyici, koruyucu ve istihbari faaliyetlerin belirsizliği ve öngörülemezliği bir yana, bu faaliyetler “kapsamında” kişisel veri işlenmesinin KVKK’dan tam istisna nedeni olması, kişisel verilerin korunması hakkının özüne zarar

<sup>333</sup> Gerekçeye erişim için bkz.: <https://www2.tbmm.gov.tr/d26/1/1-0541.pdf>, erişim tarihi: 19.09.2021

<sup>334</sup> Seyhan, Kazım / Eryılmaz, Bedri M., “Gelişmiş Ülkeler ve Türkiye Uygulamasında Suç Önleme Stratejileri”, Liberal Düşünce Dergisi, Bahar 2004, ss. 5-34, s. 7.

<sup>335</sup> Athi, Turan, “Kişisel Verilerin Önleyici, Koruyucu ve İstihbari Faaliyetler Amacıyla İşlenmesi”, Necmettin Erbakan Üniversitesi Hukuk Fakültesi Dergisi, C: 2, S: 1, 2019, ss. 4-22, s. 11.

<sup>336</sup> Çalışmanın devamında “MİT” olarak isimlendirilecektir.

<sup>337</sup> İter, Erdal, Millî İstihbarat Teşkilatı Tarihçesi, MİT Basım Evi, Ocak 2002, s. 1.

verebilecek niteliktedir. Nitekim Kişisel Verileri Koruma Kurulu 28.09.2021 tarihinde Covid-19 PCR testi sonucu ve aşı bilgisi uygulamalarına ilişkin yapmış olduğu kamuoyu duyurusunda, Çalışma ve Sosyal Güvenlik Bakanlığı'nın "*Covid-19 aşısı olmayan işçilerden zorunlu olarak haftada bir kez PCR testi yaptırmalarının işyeri/işveren tarafından istenebileceği ve test sonuçlarının gerekli işlemler yapılmak üzere kayıt altında tutulacağına*" ilişkin 02.09.2021 tarihli yazısını sağlık riskine yönelik koruyucu ve önleyici tedbirler kapsamında değerlendirmiştir<sup>338</sup>. Böylelikle ilgili istisna halini düzenleyen fıkradaki "*kapsamında*" ifadesiyle, kişisel verilerin korunması hakkının kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından hazırlanmış bir "*yazı*" ile sınırlandırılmasının önü açılmıştır.

#### **4.2.5. Soruşturma, Kovuşturma, Yargılama veya İnfaz İşlemlerinde Kişisel Verilerin İşlenmesi**

Son olarak, "*Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi*" durumunda da KVKK'nın tam istisna hali söz konusu olacaktır. İlgili fıkradan anlaşılacağı üzere bu istisna hali, yargı makamları veya infaz mercileri tarafından gerçekleştirilen veri işleme faaliyetlerine ilişkindir.

AB hukukunda suçların önlenmesi, soruşturulması, kovuşturulması ya da infazı alanlarında geçerli olmak üzere 05.05.2016 tarihinde Kişisel Verilerin Yetkili Otoritelerce Suçların Önlenmesi, Soruşturulması, Ortaya Çıkarılması veya Kovuşturulması veya Cezaların İnfazı Amacıyla İşlenmesiyle İlgili Gerçek Kişilerin Korunmasına ve Bu Verilerin Serbest Dolaşımına İlişkin 2016/680 sayılı Direktif

<sup>338</sup> Kişisel Verileri Koruma Kurulu'nun 28.09.2021 tarihli ve 2021/980 sayılı kararına ilişkin duyuruya erişim için bkz.: <https://kvkk.gov.tr/Icerik/7055/COVID-19-PCR-TEST-SONUCU-VE-ASI-BILGISI-UYGULAMALARINA-ILISKIN-KAMUOYU-DUYURUSU>, erişim tarihi: 29.09.2021.

yürürlüğe girmiştir<sup>339</sup> <sup>340</sup>. Bu ve bir önceki başlıkta ele alınan istisna hallerinde kişisel verilerin yetkili makamlar tarafından keyfi bir şekilde işlenmesinin önüne geçilmesi için, benzer kuralların getirilmesi gerekmektedir<sup>341</sup>. Aksi durumda tıpkı İstanbul İl Emniyet Müdürlüğü'nün İstanbul Sağlık Müdürlüğü'nden “ivedi” ve “gizli” ibareleriyle 01.01.2017 ile 31.05.2019 tarihleri arasında şehirde kürtaj yaptıran kadınların bilgisini talep etmesi gibi insan haklarına, tıbbi etik kurallarına ve özellikle de kişisel verilerin korunması hakkına uygun düşmeyecek olayların yaşanması her zaman için ihtimal dahilinde olacaktır<sup>342</sup>. Kişisel verilerin soruşturma, kovuşturma gibi alanlarda korunmaması, kişisel verilerin korunmasına yönelik yapılan düzenlemelerin yalnızca göstermelik olduğu yönünde bir sonuç doğuracaktır<sup>343</sup>.

### 4.3. Kısmî İstisna Halleri (m 28/2)

KVKK'nın kısmî istisna halleri 28. maddenin 2. fıkrasında düzenlenmiştir. Bu hallerde 1. fıkradaki gibi tam bir istisna durumu söz konusu değildir. Nitekim kısmî istisna hallerinde yalnızca KVKK'nın aydınlatma yükümlülüğünün düzenlendiği 10. maddesi, zararın giderilmesini talep etme hakkı hariç olmak üzere ilgili kişinin haklarının düzenlendiği 11. maddesi ve Veri Sorumluları Siciline kayıt yükümlülüğünün düzenlendiği 16. maddesinin uygulanmaması söz konusudur.

<sup>339</sup> 2008/977 Aİİ sayılı Konsey Çerçeve Kararı yerine geçen 27.04.2016 tarihli ve 2016/680 sayılı Direktif'e (Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA) erişim için bkz.: [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L\\_.2016.119.01.0089.01.ENG](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0089.01.ENG), erişim tarihi: 19.09.2021.

<sup>340</sup> 2016/680 sayılı Direktif'e ilişkin detaylı bilgi için bkz.: İstanbul Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü, Avrupa Parlamentosu ve Konseyi'nin 2016/680 Sayılı ve 27 Nisan 2016 Tarihli Kişisel Verilerin Yetkili Otoritelerce Suçların Önlenmesi, Soruşturulması, Ortaya Çıkarılması veya Kovuşturulması veya Cezaların İnfazı Amacıyla İşlenmesiyle İlgili Gerçek Kişilerin Korunmasına ve Bu Verilerin Serbest Dolaşımına İlişkin ve 2008/977/JHA Sayılı Konsey Çerçeve Kararı'nı Yürürlükten Kaldıran Direktif Hakkında Bilgi Notu, erişim için bkz.: <https://itlaw.bilgi.edu.tr/media/2019/7/29/law-enforcement-directive-bilgi-notu.pdf>, erişim tarihi: 19.09.2021.

<sup>341</sup> Aynı yönde görüş için bkz.: **Küzeci**, Kişisel Verilerin Korunması, s. 332.

<sup>342</sup> İlgili haber için bkz.: <https://t24.com.tr/haber/istanbul-emniyet-mudurlugu-kurtaj-yaptiran-30-40-yas-araligi-kadınların-listesini-istedi.838733>.

<sup>343</sup> **Mutlu**, s. 146.

### 4.3.1. Kişisel Veri İşlemenin Suç İşlenmesinin Önlenmesi veya Suç Soruşturması İçin Gerekli Olması

KVKK'nın kısmî istisna hallerinden ilki, “*Kişisel veri işlemenin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması*”dır. Suç işlenmesini önlemek veya suç soruşturmasını yürütebilmek üzere görevli kişilerin, bu amaçlarla gerçekleştirdikleri kişisel veri işleme faaliyetlerinde KVKK hükümleri kısmen uygulanmamaktadır. Nitekim soruşturma sürecinde yer alan kolluk gücünden, şüpheliyi kişisel verilerinin işlenmesi konusunda bilgilendirmesi beklenmemelidir. Suçlunun veya suçun ortaya çıkarılması ile kişinin kişisel verilerinin işlenmesi sürecine yönelik bilgilendirilmesi arasında bir menfaat dengesinde, suç araştırması ön planda olacaktır<sup>344</sup>.

### 4.3.2. Kişinin Kendisi Tarafından Alenileştirilmiş Kişisel Verilerin İşlenmesi

Kısmî istisna hallerinden ikincisi, “*İlgili kişi tarafından alenileştirilmiş kişisel verilerin işlenmesi*”dir. Bu istisna halinin söz konusu olabilmesi için kişisel verilerin ilgili kişinin kendisi tarafından alenileştirilmesi gerekmektedir. Dolayısıyla kişisel verilerin üçüncü kişiler tarafından alenileştirilmesinde bu istisna hali söz konusu olmayacaktır. Bunun yanında alenileştirme iradesinin açıkça anlaşılması gerekmektedir<sup>345</sup>. Örneğin kişinin herkesin erişimine açık bir şekilde sosyal medya hesabında fotoğrafını paylaşması durumunda bu istisna hali söz konusu olacaktır<sup>346</sup>. Ancak paylaşılan fotoğrafın farklı amaçlar doğrultusunda kullanılması durumunda artık alenileştirme istisna halinden söz edilemeyecektir<sup>347</sup>.

Burada aynı kişinin herkesin erişimine değil, sınırlı kişilerin erişimine açık bir şekilde fotoğraf paylaşmasının alenileştirme kapsamında olup olmayacağının da ayrıca tespit

<sup>344</sup> Dülger, Kişisel Verilerin Korunması, s. 359.

<sup>345</sup> Dülger, Kişisel Verilerin Korunması, s. 359.

<sup>346</sup> Kişisel Verileri Koruma Kurumu, 6698 Sayılı Kişisel Verilerin Korunması Kanun'unun Amacı ve Kapsamı, s. 15, erişim için bkz.: <https://kvkk.gov.tr/yayinlar/6698%20SAYILI%20K%C4%B0%C5%9E%C4%B0SEL%20VER%C4%B0LER%C4%B0N%20KORUNMASI%20KANUN%E2%80%99UNUN%20AMACI%20VE%20KAPSA MI.pdf>, erişim tarihi: 19.09.2021.

<sup>347</sup> Kişisel Verileri Koruma Kurumu, Kişisel Verilerin Korunması Kanunu'na İlişkin Uygulama Rehberi, s. 44.

edilmesi gerekmektedir. Bu durumda ilk aşamada alenileştirmenin sınırlı kişiler için gerçekleştirildiği düşünülebilir. Ancak TDK'ya göre alenileşmek, “*Herkesçe bilinir duruma gelmek*”tir<sup>348</sup>. Dolayısıyla kişisel verilerin sınırlı kişilerin erişimine açılmasında bir alenileştirme durumu söz konusu değildir. Bu nedenle kişinin, sosyal medya hesabından sınırlı kişilerin erişimine açık bir şekilde fotoğraf paylaşması durumunda alenileştirme istisna halinden söz edilebilmesi mümkün değildir. Öte yandan, aynı kişinin sosyal medyada hesabını gizli olarak ayarladığı başka bir örnekte eğer ki kişi profil fotoğrafı kullanmışsa, kişiye profil fotoğrafı kullanıp kullanmama gibi bir seçeneğin sunulmasından dolayı bu kişisel veri için alenileştirme söz konusu olacaktır.

#### **4.3.3. Kişisel Veri İşlemenin Denetleme veya Düzenleme Görevlerinin Yürütülmesi ile Disiplin Soruşturma veya Kovuşturması İçin Gerekli Olması**

KVKK'nın kısmî istisna hallerinden bir tanesi de “*Kişisel veri işlemenin kanunun verdiği yetkiye dayanılarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olması*”dır. Bu kısmî istisna halinin uygulanabilmesi için kişisel veri işlemenin kanunun verdiği yetki kapsamında görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca yapılması gerekmektedir. Diğer yandan işlenen kişisel verinin ilgili faaliyet için gerçekten gerekli olup olmadığının da araştırılması, anılan istisna hükmü dahilinde işlem yapılıp yapılamayacağının tespitinde önemlidir. Nitekim soruşturma veya kovuşturma geçiren bir kişinin, gerekli olup olmadığına bakılmaksızın her türlü bilgisinin işlenmesi, bu istisna hali kapsamında değerlendirilmeyecektir.

<sup>348</sup> TDK, Güncel Türkçe Sözlük, erişim için bkz.: <https://sozluk.gov.tr/>, erişim tarihi: 05.10.2021.

#### **4.3.4. Kişisel Verilerin Bütçe, Vergi ve Mali Konulara İlişkin Olarak Devletin Ekonomik ve Mali Çıkarlarının Korunması Kapsamında İşlenmesi**

KVKK'nın son kısmî istisna hali, “*Kişisel veri işleminin bütçe, vergi ve mali konularla sınırlı olmak kaydıyla devletin ekonomik ve mali çıkarlarının korunması için gerekli olması*”dır. Dolayısıyla devletin ekonomik güvenliği kapsamında yetkili kurum ve kuruluşlar tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetlerde kişisel veri işlenmesinin tam istisna; devletin ekonomik, mali, bütçe ve vergi güvenliği ve çıkarlarına ilişkin faaliyetlerde kişisel veri işlenmesinin ise kısmî istisna kapsamında bulunduğu söylenebilir<sup>349</sup>.

#### **4.4. KVKK'nın Kişisel Verinin Tutulduğu Yer Bakımından Uygulanmaması**

Kişisel verilerin işlenmesi, eğer ki otomatik olmayan yollarla gerçekleşiyorsa ve aynı zamanda herhangi bir veri kayıt sisteminin parçası değilse KVKK anlamında bir veri işlemeyi söz edilemeyecektir. Dolayısıyla bu durumlarda KVKK hükümleri uygulanmayacaktır.

Veri kayıt sistemi, belirli kriterlere göre kişisel verilerin düzenlendiği sistemi ifade etmektedir. Bu itibarla, bir bakkalın müşterilerinin borçlarını yazdığı veresiye defteri tutmasında belirli kriterler yer aldığından, veri kayıt sisteminden bahsedilebilir. Diğer yandan bir kişinin, hoşlanmadığı bir kimsenin cep telefonu numarasını halka açık bir alanda spreyle duvara yazması durumunda bir veri kayıt sisteminden söz edilemeyecektir. Nitekim anılan örnekte kişisel verilerin belirli bir kriter baz alınarak işlenmesi söz konusu değildir. Bununla birlikte, bir veri kayıt sisteminin parçası olmadan işlenen kişisel verilerin KVKK'ya tâbi olmaması durumu, söz konusu kişisel verilerin gelişigüzel bir şekilde kullanılacakları sonucunu da doğurmamaktadır<sup>350</sup>.

<sup>349</sup> Dülger, Kişisel Verilerin Korunması, s. 361.

<sup>350</sup> Kişisel Verileri Koruma Kurumu, 6698 sayılı Kişisel Verilerin Korunması Kanunu Hakkında Doğru Bilinen Yanlılar, s. 14.

#### 4.5. KVKK'nın Uygulanmadığı Hallerde Hukuka Uygunluk Tespitinde İzlenilecek Yöntem

Çalışmanın II. bölümün başında, KVKK ile TCK arasındaki ilişki incelenerek iki kanun hükümlerinin hangi nitelikte olduğu belirtilmişti<sup>351</sup>. Bu başlıkta, KVKK'nın uygulanmaması halinde hukuka uygunluk tespiti için hangi hükümlerin uygulanması gerektiği meselesi ele alınacaktır. Bu mesele, üç farklı açıdan incelenebilir:

1. Tam istisna hallerinde kanun koyucu, KVKK'nın hiçbir hükmünün uygulanmayacağını belirtmiştir. Diğer bir ifadeyle kanun koyucu tam istisna hallerinde veri işlemeyi belirli sınırlar çerçevesinde serbest bırakmıştır. Bu durumda KVKK'nın hukuka uygun kıldığı bir veri işlemeyi söz edilebilir. Dolayısıyla bu veri işleminin hukuka uygun olup olmadığını belirleyecek norm yine KVKK'da yer almaktadır. Dolayısıyla hukuka uygunluğun belirlenmesinde yine KVKK hükümlerinin uygulanması söz konusu olacaktır.
2. Kısmî istisna hallerinde ise yalnızca bilgilendirme, ilgili kişinin hakları ve Sicile kayıttan istisna hali söz konusu olmakta; KVKK'nın hukuka uygunluk nedenleri ile genel ilkelerine uyumlu olma yükümlülüğü devam etmektedir. Diğer bir ifadeyle sayılanlar hariç olmak üzere KVKK hükümleri hala geçerlidir. Dolayısıyla bu durumda da KVKK'da düzenlenen hukuka uygunluk nedenleri uygulanacaktır.
3. Eğer ki bir kişisel veri otomatik olmayan yollarla işleniyor ve aynı zamanda bu işleme veri kayıt sisteminin bir parçası değil ise, bu durumda KVKK hükümlerinin uygulama alanı olmayacaktır. Nitekim burada veri işleme faaliyeti KVKK anlamında bir veri işleme faaliyeti değildir. Dolayısıyla bu durumda hukuka uygunluk tespiti için TCK'da yer alan hukuka uygunluk nedenlerinden yararlanılması söz konusu olacaktır. Ancak önemle belirtmek gerekir ki KVKK'da kişisel verilerin işleme koşulları ve bu işlemede uyulacak genel ilkelerin belirlenmesinin yanı sıra, bu süreçte yer alan kavramlar da açıklığa kavuşturulmuştur. Dolayısıyla soruşturma ve kovuşturma aşamalarında özellikle

---

<sup>351</sup> Çalışmanın II. bölüm 2.2. başlığı.

neyin kişisel veri olarak sınıflandırılabilirliği hususunda KVKK hükümlerinden yararlanılması gerekmektedir.

## 5. VERİ İŞLEME ŞARTLARININ GENEL HUKUKA UYGUNLUK NEDENLERİYLE KARŞILAŞTIRILMASI

### 5.1. Genel Olarak

KVKK'daki veri işleme şartlarının (dolayısıyla hukuka uygunluk nedenlerinin) kişisel verilerle ilgili suçlar bakımından kendi özgü (*sui generis*) hukuka uygunluk nedeni olduğundan yukarıda bahsedilmişti. TCK'nın 135 vd. maddelerindeki suçlar kişisel verilerle ilgilidir. Dolayısıyla kişisel verilerin işlenmesine yönelik usul ve esasları belirleyen özel bir kanun olan KVKK'nın hükümlerinin, bu suçlardaki hukuka uygunluğun tespit edilmesinde uygulanması gerekmektedir.

Kişisel verilerin işleme şartları KVKK'nın 5. ve 6. maddelerinde düzenlenmiştir. Anılan şartlar, TCK'nın 135 vd. maddeleri açısından -dolayısıyla da çalışmanın konusunu oluşturan verileri hukuka aykırı olarak verme veya ele geçirme suçu açısından- oldukça önemlidir. Çünkü bu şartların varlığı halinde KVKK kapsamına giren davranış için hukuka uygunluk nedenlerinin varlığından söz edilebilecektir.

KVKK'nın 5. maddesinde özel nitelikli olmayan kişisel verilerin işleme şartları düzenlenmiştir. Anılan maddenin 1. fıkrasına göre ilgili kişinin açık rızası olmaksızın kişisel verilerin işlenmesi yasaktır. Ancak maddenin 2. fıkrasında bulunan şartlardan herhangi birinin varlığı halinde kişinin açık rızası aranmaksızın kişisel verilerin işlenmesi mümkündür<sup>352</sup>. Bu şartlar aşağıdaki şekilde sıralanabilir:

- Bir verinin işlenmesinin kanunlarda açıkça öngörülmesi (m. 5/2-a),

<sup>352</sup> Kişisel Verileri Koruma Kurulu'nun 08.07.2019 tarih ve 2019/206 sayılı kararda veri işleme şartlarının mevcut olduğu durumlarda ilgili kişiden açık rıza alınmasının ilgili kişiyi yanlıtıcı nitelikte olduğunu belirtmiştir. Çünkü bu durum hakkın kötüye kullanımı niteliğinde değerlendirilmektedir. Nitekim ilgili kişi tarafından verilen rıza istenildiği zaman geri alınabilir. İlgili kişinin, rızasını geri alması halinde faaliyetin sonlandırılacağını düşünmesinin karşısında, diğer veri işleme şartlarından herhangi birisi varsa veri işleme faaliyeti sonlandırılmayacak ve veri işlemeye devam edilecektir. İlgili karara erişim için bkz.: <https://kvkk.gov.tr/Icerik/6709/2019-206>, erişim tarihi: 29.05.2021.



- Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukukî geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması (m. 5/2-b),
- Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması (m. 5/2-c),
- Veri sorumlusunun hukukî yükümlülüğünü yerine getirebilmesi için zorunlu olması (m. 5/2-ç),
- İlgili kişi tarafından alenileştirilmiş kişisel verilerin işlenmesi (m. 5/2-d),
- Bir hakkın tesisi, kullanılması veya korunması için zorunlu olması (m. 5/2-e),
- İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması (m. 5/2-f).

KVKK'nın 6. maddesinde ise özel nitelikli kişisel verilerin işleme şartları düzenlenmiştir. Bu kapsamda *“Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri”* özel nitelikli kişisel veridir. Anılan maddenin 3. fıkrasında özel nitelikli kişisel verilerin nasıl işlenebileceği düzenlenmiştir. Buna göre *“Sağlık ve cinsel hayat dışındaki özel nitelikli 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 de anlaşılacağı üzere; kanun koyucu özel nitelikli kişisel veriler arasında sağlık ve cinsel hayata ilişkin veriler ile diğer özel nitelikli kişisel veriler olarak ikili bir ayrıma gitmiş, sağlık ve cinsel hayata ilişkin verilerin açık rıza dışında işleme koşullarını kişi ve amaç yönünden sınırlandırmıştır.

Çalışmanın devamında öncelikle açık rıza, sonrasında özel nitelikli olmayan kişisel verilerin işleme şartları, daha sonrasında ise özel nitelikli kişisel verilerin işleme şartları ele alınacaktır. Sistematik açıdan ise öncelikle KVKK'daki kişisel veri işleme şartı hakkında bilgiler verilecek, sonrasında söz konusu kişisel veri işleme şartının

TCK'nın genel hükümlerinde hangi hukuka uygunluk nedeniyle ilişkili olduğu belirtilerek bunlar arasındaki ilişki ortaya çıkarılacaktır. Ancak her bir hukuka uygunluk nedeni başlığında tekrar olmaması açısından en başta şu hususun belirtilmesinde fayda bulunmaktadır: KVKK'nın uygulama alanı bulduğu hallerde, hukuka uygunluk nedenlerinin tespit edilmesi bakımından KVKK'daki hukuka uygunluk nedenlerinin incelenmesi gerekmektedir. TCK'nın 5. maddesinde yer alan hüküm, gerek yürürlük tarihi itibarıyla gerekse normlar hiyerarşisi nedeniyle KVKK'nın TCK'dan farklı bir hukuka uygunluk nedeni getirebilmesinin önünde engel değildir.

## 5.2. Açık Rıza

### 5.2.1. Açık Rıza Kavramı

Kişisel verilerin (ve özel nitelikli kişisel verilerin) ilgili kişinin açık rızası olmaksızın işlenmesi yasaktır. Rıza, açıklanma şekli bakımından açık ve örtülü olmak üzere ikiye ayrılır<sup>353</sup>. KVKK'nın "*Tanımlar*" başlıklı 3. maddesinin 1. fıkrasının a bendinde "*Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza*" olarak açık rızaya yer verilmiştir. Dolayısıyla KVKK'da örtülü rıza bir veri işleme şartı olarak kabul edilmemektedir. Nitekim Kişisel Verileri Koruma Kurumu'nun yayınlamış olduğu Açık Rıza Rehberi'nde açık rızanın Avrupa Birliği'nde yalnızca özel nitelikli kişisel verilerin işlenmesi için arandığı; ancak ülkemizde her türlü kişisel verinin işlenmesi için arandığı belirtilmektedir<sup>354</sup>. Burada eklemek gerekir ki KVKK'nın 3. maddesinin gerekçesinde "*Açık rıza, 95/46/EC sayılı Direktif dikkate alınarak tanımlanmaktadır. Buna göre, açık rıza ilgili kişinin kendisiyle ilgili veri işlenmesine, özgürce, konuyla ilgili yeterli bilgi sahibi olarak, tereddüde yer bırakmayacak açıklıkta ve sadece o işlemle sınırlı olarak verdiği onay beyanı şeklinde anlaşılmalıdır*" ifadelerine yer verilmiştir<sup>355</sup>. Buna karşılık, 95/46/EC sayılı Direktif'te yalnızca özel nitelikli kişisel verilerin işlenmesi

<sup>353</sup> Özen, s. 424; Centel / Zafer / Çakmut, s. 334; Hakeri, s. 327.

<sup>354</sup> Kişisel Verileri Koruma Kurumu, *Açık Rıza*, s. 4, erişim için bkz.: <https://www.kvkk.gov.tr/yayinlar/A%C3%87IK%20RIZA.pdf>, erişim tarihi: 15.08.2021.

<sup>355</sup> KVKK gerekçesine erişim için bkz.: <https://www2.tbmm.gov.tr/d26/1/1-0541.pdf>, erişim tarihi: 09.08.2021.

için açık rıza aranmakta; diğer kişisel verilerin işlenmesi için örtülü rıza kabul edilmektedir<sup>356 357</sup>.

Kanaatimizce 95/46/EC sayılı Direktif'teki düzenlemeye benzer bir şekilde KVKK'da da özel nitelikli kişisel verilerin işlenmesi için "açık rıza", özel nitelikli olmayan kişisel verilerin işlenmesi için "rıza"nın geçerli olabileceği bir değişiklik yapılması gerekmektedir. Böylelikle veri işleme sürecine yönelik katı kuralların ilgili kişinin hak ve özgürlüklerine zarar vermeyecek ölçüde gevşetilmesinin uygulama açısından daha yerinde olacağını düşünmekteyiz. Ancak önemle belirtmek gerekir ki 95/46/EC sayılı Direktif'le benzer bir rıza metodunun benimsenmesi halinde, ilgili kişiye veri işleme amacıyla yöneltilen bir talepte ilgili kişinin sessiz kalması, iradesini yansıtan başkaca bir unsur bulunmadığı takdirde kesin bir kabul olarak anlaşılmamalıdır<sup>358</sup>.

Kişisel Verileri Koruma Kurulu yakın tarihli bir kararında açık rızanın, kişinin sahibi olduğu verinin işlenmesine kendi isteği ile ya da karşı taraftan gelen istek üzerine onay vermesi anlamını taşıdığını belirtmiştir<sup>359</sup>. Yine Kişisel Verileri Koruma Kurulu önceki tarihli bir kararında açık rızanın, rıza veren kişinin "olumlu irade beyanını" içermesi gerektiğini belirtmiştir<sup>360</sup>.

İlgili kişinin açık rızası, kişisel verilerin işlenmesinin yasak olması ilkesine bir istisna<sup>361</sup>, kişisel verilerin işlenmesinin bir şartı<sup>362</sup> ve kesin işlem yasağını ortadan kaldıran bir

<sup>356</sup> Ayrıntılı bilgi için bkz.: **Küzeci**, Kişisel Verilerin Korunması, s. 232.

<sup>357</sup> Bu anlamda bir görüşe göre açık rıza ibaresinden anlaşılması gereken esasında örtülü rızayı da içine alan bir rıza kavramıdır. **Braun**, Cihan Avcı, "Kişisel Verilerin İşlenmesindeki Rıza", Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, C. XV, 2018/1, ss. 13-33, s. 19.

<sup>358</sup> **Başalp**, Kişisel Verilerin Korunması, s. 40.

<sup>359</sup> Kişisel Verileri Koruma Kurulu'nun 27.02.2020 tarihli ve 2020/173 sayılı karar özetine erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/6739/2020-173>, erişim tarihi: 18.08.2021.

<sup>360</sup> Kişisel Verileri Koruma Kurulu'nun 08.07.2019 tarihli ve 2019/206 sayılı karar özetine erişim için bkz.: <https://kvkk.gov.tr/Icerik/6709/2019-206>, erişim tarihi: 18.08.2021.

<sup>361</sup> **Başalp**, Kişisel Verilerin Korunması, s. 44; **Kaya**, Cemil, "Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, C. LXIX, No:1-2, 2011, s. 317-334, s. 323, erişim için bkz.: <https://dergipark.org.tr/tr/download/article-file/97634>, erişim tarihi: 20.08.2021. **Erarslan Türkmen**, s. 116.

<sup>362</sup> **Voigt/Bussche**, s. 93; **Lambert**, Paul, *Understanding the New European Data Protection Rules*, New York, CRC Press Taylor & Francis Group, 2018, s. 78; **Çekin**, s. 73; **ICO**, Guide to GDPR, erişim için bkz.: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/>, erişim tarihi: 20.08.2021; 29. Madde Çalışma Grubu'nun 15/2011 sayılı görüş yazısı (*on the definition of consent*), s. 2, erişim için bkz.: [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf), erişim tarihi: 20.08.2021.

hukuka uygunluk nedeni<sup>363</sup> olarak düzenlenmiştir. Açık rıza ile aynı zamanda kişiye kişisel verileri üzerinde denetim yapma imkânı verilmektedir<sup>364</sup>.

KVKK'daki tanımdan yola çıkılarak açık rızanın belirli bir konuya ilişkin olma, bilgilendirmeye dayalı olma ve özgür irade ile açıklanmış olma şeklinde üç ana geçerlilik unsurunun bulunduğu söylenebilir<sup>365</sup>. Bu unsurlardan en az birinin eksikliği halinde açık rıza geçerli olmayacaktır<sup>366</sup>.

### 5.2.3. Açık Rızanın Geçerlilik Unsurları

KVKK anlamında hukuken geçerli bir açık rızanın söz konusu olabilmesi için gerekli **ilk unsur**, açık rızanın özel bir konuya ilişkin ve o konuyla sınırlı bir şekilde verilmiş olmasıdır<sup>367</sup>. Diğer bir ifadeyle “*Kişisel verilerimin işlenmesine rıza gösteriyorum.*” veya “*Her türlü ticari işlem, her türlü bankacılık işlemi ve her türlü veri işleme faaliyeti için kişisel verilerimin işlenmesine rızam vardır.*” şeklinde amacı belirsiz ve ucu açık bir ifade, geçerli bir açık rıza olarak kabul edilemez<sup>368</sup>. Açık rızanın belirli bir konuya ilişkin olması için doktrinde “*battaniye rıza*” şeklinde tanımlanan<sup>369</sup> ve belirli bir konu veya amaç bakımından sınırlandırılmayan ifadeler yerine örneğin, “*Almış olduğum ürünün benzerleri ile ilgili olarak reklam ve pazarlama yapılması amacıyla tarafıma SMS gönderilmesine, cep telefonu numaramın bu amaçla işlenmesine açık rıza gösteriyorum.*”

<sup>363</sup> **Yücedağ**, Nafiye, “*Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu'nun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri*”, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, C. LXXV, S.2, 2017, ss. 765-789, (**Yücedağ**, Hukuka Uygunluk Sebepleri), s.772.

<sup>364</sup> **Zor**, Abdülhamid, *Veri Sorumlusunun Yükümlülükleri ve Bu Yükümlülükleri İhlalinden Doğan Özel Hukuk Sorumluluğu*, On İki Levha Yayıncılık, 1. Baskı, İstanbul, Ekim 2020, s. 136.

<sup>365</sup> **Çekin**, s. 74; Kişisel Verileri Koruma Kurumu, *Açık Rıza*, s. 4, 5 ve 6.

<sup>366</sup> **Uçak**, Murat, “*Kişisel Verilerin Hukuka Uygun İşlenmesinde Çocuğun Rızası*”, Kişisel Verileri Koruma Dergisi, Cilt: 3 Sayı: 1, 2021, ss. 41-60, s. 49.

<sup>367</sup> **Dülger**, Kişisel Verilerin Korunması, s. 224.

<sup>368</sup> Kişisel Verileri Koruma Kurumu, *Açık Rıza*, s. 4; Kişisel Verileri Koruma Kurumu, *Soru Cevaplar*, s. 25; Kişisel Verileri Koruma Kurumu, *Sıkça Sorulan Sorular*, s. 27; Ayrıca bkz.: Kişisel Verileri Koruma Kurumu, *Açık Rıza Alırken Dikkat Edilecek Hususlar*, erişim için <https://kvkk.gov.tr/Icerik/2037/Acik-Riza-Alirken-Dikkat-Edilecek-Hususlar>, erişim tarihi: 21.06.2021.

<sup>369</sup> **Dülger**, Kişisel Verilerin Korunması, s. 224; GDPR yürürlüğe girdikten sonra 29. Madde Çalışma Grubu'nun yerini alan Avrupa Veri Koruma Kurulu (European Data Protection Board)'nun 05/2020 sayılı rehberi (*Guidelines 05/2020 on consent under Regulation 2016/679*), s. 18, erişim için bkz.: [https://edpb.europa.eu/sites/default/files/files/file1/edpb\\_guidelines\\_202005\\_consent\\_en.pdf](https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf), erişim tarihi: 21.06.2021; **Taştan** bu tür rızalar için “*torba rıza*” kavramını kullanmaktadır, bkz.: **Taştan**, s. 158.

şeklinde daha belirgin ifadeler kullanılmalıdır. Diğer yandan, açık rıza vermesi için ilgili kişiye yöneltilen sorularda da belirginlik olmalıdır. Örneğin “*Bütün kişisel verilerinizin işlenmesine açık rıza gösteriyor musunuz?*” şeklinde yöneltilen bir soruya ilgili kişinin olumlu cevap vermesi, sorunun belirli bir konuya ilişkin ve yeterince açık olma şartlarını taşımadığından hukuken geçerli olmayacaktır<sup>370</sup>. Dolayısıyla verilecek açık rıza ve açık rıza almaya yönelik sorular, veri işleme amacı ile sınırlı ve belirli bir konuya ilişkin olmalıdır.

Kişisel Verileri Koruma Kurulu 27.02.2020 tarihli ve 2020/173 sayılı kararında “*Sipariş verdiğinizde Gizlilik Bildirimini, Kullanım ve Satış Koşullarını ve Çerez Bildirimini kabul etmiş olursunuz.*” ifadesini “*battaniye rıza*” olarak kabul etmiş, konu ve işlem yönüyle sınırlandırılmaması sebebiyle bu ifadenin kullanılmasını hukuka aykırı bulmuştur<sup>371</sup>.

Geçerli bir açık rızadan bahsedilebilmesi için gerekli **ikinci unsur**, açık rızanın bilgilendirmeye dayalı olmasıdır<sup>372</sup>. Bilgilendirme yapılmasının şart koşulmasının amacı, kişinin iradesinin sağlıklı bir şekilde ortaya konulmasını sağlamaktır<sup>373</sup>. Eğer ilgili kişi hangi işlem için açık rıza verdiğini bilmezse bu durumda özgür ve açık bir beyandan söz edilebilmesi mümkün olmayacaktır<sup>374</sup>. Dolayısıyla ilgili kişiye, verdiği açık rızanın sınırları anlatılmalı ve bu açık rızanın kapsamı geniş tutulmamalıdır<sup>375</sup>.

Bilgilendirmenin kapsamı KVKK’nın 10. maddesinde asgari olarak sayılmıştır. Buna göre ilgili kişiye asgari olarak “*veri sorumlusunun kimliği, kişisel verilerin hangi amaçlarla işleneceği, işlenen kişisel verinin kimlere ve hangi amaçla aktarılacağı, kişisel veri toplamanın hukuki sebebi ve yöntemi, ilgili kişinin hakları*” konularında bilgilendirme yapılmalıdır<sup>376</sup>. Diğer yandan doğruyu yansıtmak kaydıyla ilgili kişiye

<sup>370</sup> **Dülger**, *Kişisel Verilerin Korunması*, s. 224; benzer yönde bkz.: **Küzeci**, *Kişisel Verilerin Korunması*, s. 234.

<sup>371</sup> *Kişisel Verileri Koruma Kurulu’nun 27.02.2020 tarihli ve 2020/173 sayılı karar özetine erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/6739/2020-173>, erişim tarihi: 21.06.2021.*

<sup>372</sup> **Küzeci**, *Kişisel Verilerin Korunması*, s. 234.

<sup>373</sup> **Subaşı**, İlhan, *Hekimin Aydınlatma Yükümlülüğü, Aydınlatılmış Onam, Tazminat Sorumluluğu*, Seçkin Yayıncılık, Ankara, 2016, s. 41, **Doğan**, s. 104.

<sup>374</sup> **Dülger**, *Kişisel Verilerin Korunması*, s. 225.

<sup>375</sup> **Hızarci**, s. 35.

<sup>376</sup> Avrupa Veri Koruma Kurulu’nun 05/2020 sayılı rehberinde bilgilendirmenin asgari olarak veri sorumlusunun kimliği, rıza istenen her bir veri işleme faaliyetinin amacı, hangi (tür) verinin toplanacağı ve kullanılacağı, rızayı geri alma hakkının mevcut olduğu, otomatik karar almaya konu varsa buna ilişkin bilgi ve yurt dışına transfer halinde uygunluk kararı ve gerekli önlemlerin bulunmaması halinde söz konusu olabilecek riskler konularını içermediğini belirtmektedir, Guidelines 05/2020 on consent under Regulation 2016/679, s. 15 ve 16.

yönelik olarak başkaca bilgilendirme yapılabilir. Ancak bu bilgilendirmenin objektif bir şekilde yapılması, bilgilendirme yapılırken karışıklığa mahal verebilecek ifadelerin ve ilgili kişi için anlamlı olmayan bilgilerin kullanılmasından kaçınılması gerekmektedir<sup>377</sup>.

Bilgilendirme anlaşılır, açık ve sade bir şekilde kişi henüz açık rızasını vermeden (en geç kişisel verilerin işlendiği sırada) yapılmalıdır<sup>378</sup>. Bilgilendirme yapılırken dürüstlüğe aykırı davranışlardan kaçınılmalıdır<sup>379</sup>.

Geçerli bir açık rızadan bahsedilebilmesi için **son unsur** ilgili kişinin özgür iradesinin varlığıdır. Hata, aldatma, cebir, korku, baskı vb. durumlarda verilen rıza hukuken geçerli değildir<sup>380</sup>.

Özgür irade ile açık rıza verilebilmesi için gerçekten kişiye seçim hakkının tanınması gerekmektedir<sup>381</sup>. Diğer bir anlatımla kişi, kendisini rıza vermeye mecbur hissetmemelidir ve rıza vermediği durumda kendisinin bir hizmetten mahrum bırakılmaması, olumsuz bir sonuca maruz kalmaması gerekmektedir<sup>382</sup>.

Taraflar eşit konumda değilse veya taraflardan biri, diğeri üzerinde etkiliyse bu durumda özgür irade unsurunun sağlanıp sağlanmadığı konusuna titizlikle yaklaşılmalıdır<sup>383</sup>. Örneğin işçi işveren ilişkilerinde işçi sözleşmenin zayıf tarafıdır ve işveren tarafından kişisel verilerinin işlenmesine yönelik talep edilen açık rızasını verirken her zaman için özgür iradesiyle hareket etmeyebilir<sup>384</sup>. Bu noktada taraflardan birinin zayıf konumda olduğu durumlarda işçinin rıza göstermediği takdirde olumsuz sonuçlarla karşılaşmaması için işveren tarafından işçiye güvence verilmelidir<sup>385</sup>.

Burada değinilmesi gereken önemli bir husus, açık rızanın genel işlem şartları kapsamında alınıp alınamayacağıdır. Açık rızanın sözleşmeden ayrı bir beyanla alınması

---

<sup>377</sup> Kişisel Verileri Koruma Kurumu, *Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi*, Nisan 2019, Ankara, s. 23, erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/5394/Aydinlatma-Yukumlulugunun-Yerine-Getirilmesi-Rehberi>, erişim tarihi: 27.08.2021.

<sup>378</sup> Kişisel Verileri Koruma Kurumu, *Açık Rıza*, s. 4.

<sup>379</sup> Örneğin küçük puntolar kullanılmamalıdır.

<sup>380</sup> **Çekin**, s. 80; **Beytar**, Erbil, *İşçinin Kişiliğinin ve Kişisel Verilerinin Korunması*, On İki Levha Yayınları, İstanbul, 2018, s. 156; s. 23; **Doğan**, s. 108.

<sup>381</sup> **Doğan**, s. 108.

<sup>382</sup> **Çekin**, s. 81; **Doğan**, s. 108.

<sup>383</sup> Kişisel Verileri Koruma Kurumu, *Açık Rıza*, s. 6

<sup>384</sup> **Uncular**, Selen, *İş İlişkisinde İşçinin Kişisel Verilerinin Korunması*, Seçkin Yayıncılık, Güncellenmiş ve Genişletilmiş 2. Baskı, Ankara, Ekim 2018, s. 143.

<sup>385</sup> **Dülger**, *Kişisel Verilerin Korunması*, s. 227.

yerine aynı genel işlem şartları çerçevesinde alınması, veri işleme sürecini her iki taraf için de kolaylaştırabilir. Genel işlem şartları içerisinde alelade ve fark edilmeyecek bir ifadeyle bilgilendirme yapılması ve böylelikle açık rızanın alınması hukuken geçerli değildir<sup>386</sup>. Ancak bu, her durumda genel işlem koşulları ile açık rıza almanın imkânsız olduğu anlamına gelmemelidir<sup>387</sup>. Açık rıza, dürüstlük kuralları çerçevesinde yeterince açık, sade, anlaşılır ve şeffaf bir bilgilendirme sonrasında tereddüde yer vermeyecek bir şekilde açıklanıyorsa geçerli olmalıdır<sup>388</sup>.

Özgür irade unsurunda değinilmesi gereken diğer bir önemli husus ise hizmetin açık rıza şartına tabi tutulup tutulamayacağıdır. Kişisel Verileri Koruma Kurulu, “*Bir hizmetin verilmesinin açık rıza şartına bağlanmış olmasının açık rızayı sakatlayacağını, bu durumun hukuka ve dürüstlük kuralına uygun olmadığını*” belirtmiştir<sup>389</sup>. Kurul’un kişisel verilerin korunması yönündeki hassasiyetine katılmakla beraber, bazı durumlarda KVKK hükümleri gereğince hizmet vermenin kişinin açık rızasına tabi olduğunu da belirtmek isteriz. Diğer bir anlatımla, bazı durumlarda KVKK’nın katı kurallarının bir sonucu olarak, ilgili kişilerin açık rıza vermemesi durumunda hizmet verilememektedir. Bunun bir örneği yine Kişisel Verileri Koruma Kurulu’nun başka bir kararında görülmektedir<sup>390</sup>. Şöyle ki anılan kararda bir sigorta şirketi, sağlık sigortası poliçesi kapsamında sağlık bilgilerinin işlenmesi için ilgili kişiden açık rıza istemektedir. Nitekim sağlık bilgilerinin ilgili kişinin açık rızası bulunmaksızın işlenmesi yasak olmakla birlikte 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 ilgili kişinin açık rızası bulunmaksızın işlenebilir. Bu durumda sağlık sigortası poliçesinin yenilenmesi sürecinde açık rıza için kişi ve amaç unsuru sağlanamadığından, ilgili kişiden açık rıza alınması gerekmektedir. Ancak ilgili kişi açık rıza göstermezse sigorta şirketinin sunmuş olduğu hizmetten yararlanamamaktadır.

---

<sup>386</sup> Çekin, s. 84.

<sup>387</sup> Çekin, s. 84.

<sup>388</sup> Çekin, s. 84.

<sup>389</sup> Kişisel Verileri Koruma Kurulu’nun internet adresinde yer verilen bu karara ait tarih veya karar numarası bulunmamaktadır. Karara erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/5412/Acik-Rizanın-Hizmet-Sartina-Baglanmasi>, erişim tarihi: 23.08.2021.

<sup>390</sup> Kişisel Verileri Koruma Kurulu’nun 03.09.2020 tarihli ve 2020/667 sayılı karar özetine erişmek için bkz.: <https://www.kvkk.gov.tr/Icerik/6878/2020-667>, erişim tarihi: 23.08.2021.

Dolayısıyla hizmetin verilmesi ilgili kişinin açık rızasına tabi tutulmaktadır. Bu çerçevede “*hizmetin açık rıza şartına tabi tutulmaması gerektiği*” noktasındaki çelişkilerin giderilmesi gerekmektedir. Diğer yandan, Kişisel Verileri Koruma Kurulu’nun “*hizmetin açık rıza şartına tabi tutulmaması gerektiği*” yönündeki tutumuna da katılmadığımızı belirtmek isteriz. Kanaatimizce hizmetin verilmesi ile açık rıza gösterilmesi arasında denge esas alınarak, mevcut duruma ilişkin birtakım araştırmalar yapılmalıdır. Örneğin bu hizmeti veren kişi tekel konumunda mıdır? Bu hizmetin ilgili kişi tarafından alınmaması durumunda ilgili kişinin aleyhine olacak şekilde telafisi güç zararlar meydana gelir mi? İlgili kişiyi bu hizmetten yararlanmaya zorlayan bir etken var mı? Bu sorulara verilecek yanıt üzerine kişisel verilerin türü ya da niteliği dikkate alınarak hizmet, açık rıza şartına tabi tutulabilmelidir. Örneğin kullanıcılarına tamamen ücretsiz olan, internet tabanlı ve gelirini kullanıcılara yönelik profillemeye sonucunu kullanıcılara gönderdiği reklamlardan (çerezlerden) elde eden bir cep telefonu uygulamasını düşünelim. Kullanıcıların karşısına uygulamayı kullanırken çerezler yardımıyla reklam çıkarılması, diğer bir ifadeyle kullanıcıların hareketleri esas alınarak profillemeye yapılması, yine kullanıcıların açık rızasına tabidir. Ancak kullanıcılar açık rıza göstermezse bu uygulamayı kullanamayacaktır. Açık rıza gösterildiği takdirde ise açık rızanın gerçekten özgür irade ile gösterilip gösterilmediği tartışma konusu olacaktır. Bu durumda somut olayın koşullarına göre değerlendirme yapılmalı, söz konusu uygulamanın muadillerinin olup olmadığı incelenmelidir. Eğer ki aynı işlevi görece bir uygulama yine ücretsiz bir şekilde kullanıcılarına profillemeye yapmadan bu hizmeti sunabiliyorsa bu durumda kişinin özgür iradesinin varlığından söz edilebilmelidir<sup>391</sup>.

Özgür irade unsuruyla ilgili olarak değinilmesi gereken diğer bir önemli husus ise, açık rıza verme sürecinde ilgili kişiyi etkileyecek davranışlar sergilenmesinin açık rızayı geçersiz kılıp kılmayacağıdır. Kanaatimizce açık rıza isteyen kişi, ilgili kişiyi zorlamaya varmayacak şekilde makul bir ölçüde etkilemeye çalışabilir. Örneğin, ürün pazarlayan bir şirketin, pazarlama için ilgili kişinin kişisel verilerine ihtiyaç duyması ve kararsız olan ilgili kişiye bu sürecin olumlu ve avantajlı yönlerini anlatması makul kabul edilebilir<sup>392</sup>.

---

<sup>391</sup> Benzer örnek için bkz.: **Küzeci**, Kişisel Verilerin Korunması, s. 234.

<sup>392</sup> **Dülger**, Kişisel Verilerin Korunması, s. 227.



Ancak açık rıza isteyen, ilgili kişinin olumsuz yanıt vermesinin ardından onu ikna etmeye çalışmamalıdır.

Bu başlık altında incelenecek son husus, ilgili kişinin açık rıza vermesi halinde kendisine ek avantajlar ya da menfaatler sağlanmasının açık rızanın geçerliliğini etkileyip etkilemeyeceğidir. Burada bir hizmetin sağlanması değil, bir avantajın sağlanması söz konusudur. Dolayısıyla avantajın sağlanmasının açık rızaya tabi olduğu durumda açık rıza gösterilmemesi halinde hizmetin hiç verilmemesi ya da ilgili kişinin özgür iradesinin etkilenmesi söz konusu değildir. Nitekim burada karşılıklı bir menfaat ve sözleşme söz konusudur<sup>393</sup>. İlgili kişiye açık rızasını vermesi halinde ek menfaatler sağlanacağı söylenebilir. Ancak tıpkı yukarıda belirtildiği üzere bu söylemler ilgili kişiyi rahatsız edecek ve taciz boyutuna varacak şekilde ısrarcı bir düzeyde olmamalıdır<sup>394</sup>. Nitekim Kişisel Verileri Koruma Kurulu 25.03.2019 tarihli ve 2019/82 sayılı kararında “*Müşterinin Sadakat Kart Programına üye olmadığı durumda Şirketin sunduğu ürüne ve kişiye özel fırsat dünyasından faydalanamadığı ancak bu durumun hiçbir şekilde herhangi bir müşterinin Şirketin sunduğu alışveriş ortamından faydalanmasını engellemediği dolayısıyla, veri sorumlusu Şirket tarafından hizmet sunumu kapsamında Sadakat Kart Programına katılımın müşteriler açısından zorunlu tutulmadığı, söz konusu Programa üye olmayan müşterilere hizmet sunulmaması gibi bir durum ortaya çıkmadığı dikkate alındığında....*” ifadeleriyle ek menfaat sağlanmasını hukuka uygun bulmuştur<sup>395</sup>. Yine Kurul 08.07.2019 tarihli ve 2019/206 sayılı başka bir kararında “*Veri sorumlusu bünyesinde sunulan indirim ve avantajların yalnızca üyelere sunulmasının bir ürün veya hizmetin sunulmasının ya da ürün veya hizmetten yararlandırılmasının açık rıza şartına dayandırılması anlamına gelmediğini*” belirtmiştir<sup>396</sup>.

---

<sup>393</sup> Dülger, Kişisel Verilerin Korunması, s. 236.

<sup>394</sup> Dülger, Kişisel Verilerin Korunması, s. 234-235.

<sup>395</sup> Kişisel Verileri Koruma Kurulu’nun 25.03.2019 tarihli ve 2019/82 sayılı karar özetine erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/5463/-Bir-market-zincirinin-sadakat-kart-uygulamasina-iliskin-ihbar-ve-sikayetler-hakkinda-Kisisel-Verileri-Koruma-Kurulunun-25-03-2019-tarihli-ve-2019-82-sayili-Karari>, erişim tarihi: 25.08.2021.

<sup>396</sup> Kişisel Verileri Koruma Kurulu’nun 08.07.2019 tarihli ve 2019/206 sayılı karar özetine erişim için bkz.: <https://kvkk.gov.tr/Icerik/6709/2019-206>, erişim tarihi: 18.08.2021.

#### 5.2.4. Açık Rızanın Hukukî Niteliği

Açık rızanın hukukî niteliğinin belirlenmesi, ona bağlanacak hukukî sonuçlar bakımından önem arz etmektedir. Öncelikle belirtmek gerekir ki, KVKK'daki açık rıza ile TCK'daki rıza arasında hukukî nitelik farkı bulunmamaktadır. Dolayısıyla doktrinde rızanın hukukî niteliğine yönelik ileri sürülen görüşler, KVKK'daki açık rızanın hukukî niteliği için de geçerlidir. Rızanın hukukî niteliğine yönelik olarak doktrinde hukukî işlem, hukukî işlem benzeri, maddî fiil, hukuksal korumadan vazgeçme şeklinde farklı görüşler bulunmaktadır<sup>397</sup>.

Hukukî işlem teorisi kendi içerisinde özel hukuk alanına ait hukukî işlem ve kamu hukuku alanına ait hukukî işlem olarak ayrılmaktadır. Hukukî işlem, genel itibarıyla hukukî bir sonuç doğurmaya yönelik irade açıklamalarıdır<sup>398</sup>. Hukuk düzeni, bu irade açıklamalarına dayanarak irade açıklamasına uygun hukukî sonucu gerçekleştirir<sup>399</sup>. Rızanın hukukî işlem olduğu görüşü; hukukî işlem olan rızanın sübjektif sonuç doğurmasının karşısında ceza hukuku alanında geçerli olan rızanın objektif sonuç doğurduğu, hukukî işlem anlamında her zaman için bir hukukî sonucun doğmasına karşın ceza hukukunda rızanın her zaman hukukî bir değişiklik ortaya çıkarmadığı, hukukî işlem anlamındaki rızanın rıza gösteren tarafı katlanma yükümlülüğü altına sokmasına karşın ceza hukukunda böyle bir yükümlülüğün bulunmadığı, kamu hukuku alanında geçerli olan hukukî işlemlerin (idari, yasama, yargısal) hiçbirisiyle rızanın açıklanmasının mümkün olmadığı gerekçeleriyle eleştirilmiştir<sup>400</sup>.

Rızanın hukukî niteliğine yönelik bir diğer görüş, hukukî işlem benzeri görüşüdür<sup>401</sup>. Hukukî işlem benzeri fiillerde, irade doğrudan doğruya fiilî bir sonuca yönelmiş olsa bile hukuk düzeni kendiliğinden bu irade açıklamasına bir hukukî sonuç bağlamaktadır<sup>402</sup>. Dolayısıyla irade açıklaması istenilen bir hukukî sonuca yönelmemektedir<sup>403</sup>.

<sup>397</sup> **Ekici Şahin**, Meral, *Ceza Hukukunda Rıza*, On İki Levha Yayıncılık, 1. Baskı, İstanbul, Ocak 2012, s. 29-50; **Polat**, Alperen, *Sorumluluk Hukukunda Rıza*, On İki Levha Yayıncılık, İstanbul, 2019, s. 11-18.

<sup>398</sup> **Kocayusufpaşaoğlu**, Necip, *Borçlar Hukukuna Giriş, Hukukî İşlem Sözleşme*, Filiz Kitapevi, Cilt: 1, 5. Bası, İstanbul 2010, s. 84; **Ekici Şahin**, s. 51.

<sup>399</sup> **Kocayusufpaşaoğlu**, s. 84.

<sup>400</sup> **Ekici Şahin**, s. 33; **Hakeri**, s. 323.

<sup>401</sup> **Kaneti**, Selim, *Haksız Fiilde Hukuka Aykırılık Sorunu, Kazancı Hukuk Yayınları*, İstanbul, 2007, s. 244; **Çilingiroğlu**, Cüneyt, *Tıbbi Müdahaleye Ceza*, Filiz Kitapevi, İstanbul, 1993, s. 44.

<sup>402</sup> **Doğan**, s. 67.

<sup>403</sup> **Eren**, Fikret, *Borçlar Hukuku Genel Hükümler*, Yetkin Yayınları, 21. Bası, Ankara, 2017, s. 161.

Rızanın hukukî niteliğine yönelik bir diğer görüş, maddî fiil görüşüdür<sup>404</sup>. Maddî fiillerde hukukî sonuç doğrudan “*dış alemde meydana gelen fiilî değişikliğe bağlanmaktadır*”<sup>405</sup>. Bu görüş, rızanın verilmesiyle dış alemde bir değişikliğin meydana gelmeyeceği ve rızanın doğası gereği hukuk alanında bir hukukî sonuç meydana getireceği sebepleriyle eleştirilmiştir<sup>406</sup>.

Son olarak, rızanın hukukî niteliğini hukuksal korumadan vazgeçme ile açıklayan bir görüş bulunmaktadır<sup>407</sup>. Bu görüşe göre rıza, hukuksal değerleri üzerinde serbestçe tasarruf edebileceği kabul edilen bir kişinin, söz konusu hukuksal değerlerine yönelik olarak somut olayda yine hukuk düzeni tarafından sağlanan soyut korumadan vazgeçmesidir<sup>408</sup>. Kanaatimizce rızanın hukukî niteliğine yönelik görüşler içerisinde hukuksal korumadan vazgeçme görüşü daha isabetlidir. Nitekim rıza, kişinin hukuksal değerlerine yönelik karar verebilme ve üzerinde tasarrufta bulunabilme özgürlüğünün bir yansımasıdır<sup>409</sup>. Dolayısıyla Anayasa’nın 12. ve 17. maddeleriyle korunan “*kişinin kişiliğini serbestçe geliştirme hakkı*” kapsamında değerlendirilmelidir<sup>410</sup>. Rıza ile açık rıza arasında bir hukukî nitelik farkı bulunmadığından, açık rızanın hukukî niteliği için de aynı ifadelerin geçerli olduğunu söylemek mümkündür<sup>411</sup>.

### 5.2.5. Açık Rıza Gösterme Ehliyeti

Açık rıza gösterme ehliyetine ilişkin olarak KVKK’da herhangi bir düzenleme bulunmamaktadır. Bu doğrultuda ceza hukuku açısından rızaya ilişkin tespit ve değerlendirmelerin yapılması gerekmektedir. Ceza hukuku açısından da kimlerin bu

<sup>404</sup> **Bucher**, Eugen, Die Ausübung der Persönlichkeitsrechte, insbesondere die Persönlichkeitsrechte des Patienten als Schranken der ärztlichen Tätigkeit, Zürich, 1956, s.108-110 (Akt: **Başara**, Gamze Turan, *Kişiliğin İhlalinden Kaynaklanan Maddî ve Manevî Tazminat ile Haksız Kazancın İadesi*, Turhan Kitapevi, Ankara, 2018, s. 70.)

<sup>405</sup> **Kocayusufpaşaoğlu**, s. 85.

<sup>406</sup> **Çekin**, s. 76.

<sup>407</sup> **Hakeri**, s. 323.

<sup>408</sup> **Hakeri**, s. 323; **Ekici Şahin**, s. 40.

<sup>409</sup> **Ekici Şahin**, s. 41.

<sup>410</sup> **Hakeri**, s. 323; **Ekici Şahin**, s. 40

<sup>411</sup> Açık rızanın verilmesiyle ortaya çıkan hukukî sonucun hukuka aykırı olan kişisel veri işlemenin hukuka uygun hale getirilmesi olması nedeniyle, açık rızayı bir hukukî işlem olarak değerlendiren farklı görüşler için bkz.: **Çekin**, s. 77; **Doğan**, s. 68.

ehliyetine sahip olduğu ve şartlarının neler olduğu konusunda görüş ayrılıkları bulunmaktadır<sup>412</sup>. Esasen kanun koyucu rıza ehliyetine ilişkin bazı özel düzenlemeler getirmiştir. Örneğin TCK'nın 103. maddesinin 1. fıkrası ve TCK'nın 104. maddesinde yer alan düzenlemelere göre on beş yaşından küçüklerin cinsel özgürlüklerine yönelik rıza ehliyetleri bulunmamaktadır. Ancak kanun koyucunun açıkça düzenlemediği hallerde rıza ehliyetinin tespitinde öğreti ve uygulamanın büyük rolü bulunmaktadır. Yargıtay kişiyi hürriyetinden yoksun kılma suçunun cinsel amaçlarla işlenmesi durumunda TCK'nın 103. maddesini esas alarak bir kıyas yapsa da bu husus rıza ehliyetinin belirlenmesi açısından isabetli değildir<sup>413</sup>.

Rıza ehliyetinin belirlenmesine yönelik a) hukukî işlem ehliyetine ilişkin kuralların uygulanması, b) kusur ehliyetine ilişkin kuralların uygulanması, c) ayırt etme yeteneğine göre belirlenmesi olmak üzere üç farklı şekilde görüş bulunmaktadır.

Rıza ehliyetinin belirlenmesinde hukukî işlem ehliyetine ilişkin kuralların uygulanması, açık rızanın bir hukukî işlem olmaması nedeniyle mümkün görünmemektedir. Açık rızanın bir hukukî işlem olması görüşüne yönelik eleştiriler genel anlamda ehliyet açısından da geçerlidir.

Rıza ehliyetinin belirlenmesinde kusur ehliyetine ilişkin kuralların uygulanması gerektiğini savunan görüşe göre, rıza ehliyetine ilişkin kesin bir yaş sınırının belirlenmesi doğru değildir<sup>414</sup>. Bu görüşe göre on iki – on sekiz yaş grubunda bulunanların rızalarının geçerliliği konusunda her somut olay özelinde ayrıca değerlendirme yapılmalıdır<sup>415</sup>. Yaşı on ikiden küçük olanların ve on sekizden büyük olanların kural olarak rıza gösterme yeteneğinin bulunduğu ise şüphe yoktur<sup>416</sup>. Bu görüş; rıza ehliyetinin kişinin kendi hukuksal değerlerine yönelik bir değerlendirme yapması ve kendi menfaatlerini gözetebilmesi esasına dayanmasına karşın; kusur ehliyetinin başkalarının hukuksal değerlerine yönelik saygı göstermeyi esas almasından dolayı eleştirilmiştir<sup>417</sup>. Ayrıca örneğin on iki yaşını tamamlamamış bir çocuğun algılaması bir gün sonra on iki yaşını

---

<sup>412</sup> Ekici Şahin, s. 132.

<sup>413</sup> Ekici Şahin, s. 134.

<sup>414</sup> Centel / Zafer / Çakmut, s. 334.

<sup>415</sup> Centel / Zafer / Çakmut, s. 334; Hakeri, s. 326.

<sup>416</sup> İstisna olarak akıl hastalığı, sağır-dilsizlik veya geçici nedenle kusur yeteneği bulunmayan kimselerin rızaları geçerli değildir.

<sup>417</sup> Ekici Şahin, s. 146.

tamamlamış halinden farklı olmayacağından, bu görüşü desteklemek mümkün görünmemektedir<sup>418</sup>.

Rızaya ehliyetinin ayırt etme gücüne göre belirlenmesi gerektiğini savunan göre göre ise her somut olay kendi içerisinde ayrıca değerlendirilmelidir<sup>419</sup>. Kanaatimizce üçüncü görüş daha isabetlidir. Bu itibarla rızaya ehliyetin her somut olay çerçevesinde dürüst ve şeffaflık ilkeleri dahilinde, ilgili kişinin vermiş olduğu rızanın sonuçlarını öngörebilecek nitelikte olup olmadığının incelenmesi gerekir<sup>420</sup>. İlgili kişi, açık rıza verdiği somut faaliyetin sonuçlarını öngörebilecek nitelikte değilse yasal temsilcilerinin açık rızalarının alınması gerekmektedir.

### 5.2.6. Çocukların Rızası

Çocukların rızası ile ilgili olarak KVKK'da özel bir düzenleme bulunmamaktadır. Mevzuatın 95/46/EC sayılı Direktif'te de çocukların rızası ile ilgili ayrı bir bölüme yer verilmemişti. Bu nedenle eleştiriler üzerinde GDPR'la birlikte çocuklara yönelik özel düzenlemeler getirilmiştir<sup>421</sup>. GDPR'ın 8. maddesine göre; bilgi toplumu hizmetlerine erişimlerde eğer çocuk 16 yaşından küçükse; çocuk üzerinde velayet hakkı bulunan kişi tarafından veri işlemeye rıza gösterilmesi veya onaylanması halinde hukuken geçerli bir veri işlemeden bahsedilir. Bu durumda 16 yaşından küçüklerin vermiş olduğu rıza, yasal temsilcinin onaylanması ile hukuka uygun olacaktır. Anılan maddenin devamında üye devletlere bu yaş sınırını 13 yaşa kadar indirme imkânı tanınmıştır<sup>422</sup>.

Çocukların kişisel verilerinin işlenmesi sonucunda doğacak riskleri bilmesi yetişkinlere göre zordur. Diğer yandan, internet çağında yaşadığımız gerçeği de düşünülürse, çocuk yaşta kendisi hakkında mahrem nitelikte verileri paylaşan bir kişinin bu paylaşımından

<sup>418</sup> **Ekici Şahin**, s. 149.

<sup>419</sup> **Amelung**, Knut, "Über die Einwilligungsfähigkeit I", in ZStW 95, 1992, ss. 525-558, s. 558 (Akt: **Ekici Şahin**, s. 148, dn. 125).

<sup>420</sup> **Toroslu**, Nevzat / **Toroslu**, Haluk, *Ceza Hukuku Genel Kısım*, Savaş Yayınları, Ankara, Eylül 2019, s. 190; **Ekici Şahin**, s. 150; **Centel / Zafer / Çakmut**, s. 334; **Çekin**, s. 87.

<sup>421</sup> GDPR'ın 8. ve 38. resitali, erişim için bkz.: <https://gdpr-info.eu/recitals/no-8/>, <https://gdpr-info.eu/recitals/no-38/>, erişim tarihi: 22.08.2021.

<sup>422</sup> **Determann**, Lothar, *Kişisel Verilerin Korunması Uygulama Kılavuzu – Şirketlerin Uluslararası Mevzuata Uyumu*, On İki Levha Yayıncılık, 1. Baskı, İstanbul, Ocak 2020, Çeviri: Av. Hilal Temel, s. 183.

doğan kötü sonuçlarla ömür boyu yüzleşmesi muhtemel olacaktır<sup>423</sup>. Bu nedenle GDPR’da çocuklara yönelik korumacı bir yaklaşım getirilmesi yerinde olmuştur.

Çocukların neden daha özel bir koruma alanına sahip olması gerektiği GDPR’ın 38. resitalinde belirtilmiştir<sup>424</sup>. Buna göre; “Çocuklar, kişisel verilerin işlenmesine ilişkin riskler, sonuçlar ve ilgili önlemler ile hakları hususlarında daha az farkındalığa sahip oldukları için kişisel verilerinin işlenmesinde özel bir korumaya layıktırlar.” Özel bir korumanın gerektiği hallerde örnekler ise resitalin ikinci cümlesinde belirtilmiştir. Buna göre “Çevrimiçi pazarlama faaliyetleri, sosyal kişilik yaratma veya kullanıcı profili oluşturma ya da çocuklara doğrudan hizmet vermeyi amaçlayan uygulamaların kullanılması esnasında çocukların kişisel verilerinin toplanması işlemlerinde ...” çocukların bilhassa korunması gerekir<sup>425</sup>. GDPR’da çocuklara ilişkin düzenlemeler yapılırken Amerika Birleşik Devletleri’ndeki Çocukların Çevrimiçi Platformlarda Mahremiyetinin Korunmasına İlişkin Kanun’dan<sup>426</sup> (*Children’s Online Privacy Protection Act of 1998*) yararlanılmıştır<sup>427</sup>.

Çocukların kişisel verilerinin özel bir koruma alanına sahip olması gerektiği ile ilgili sonuca ayrıca GDPR’da bulunan “Veri Koruma Etki Değerlendirmesi” sürecinde rastlanılmaktadır. Şöyle ki, GDPR’ın 35. maddesine göre gerçek kişilerin haklarına ve özgürlüklerine yönelik yüksek risk oluşturması muhtemel kişisel verileri işleme faaliyetlerinde etki değerlendirmesinin yapılması gerekir. GDPR’ın 75. resitalinde ise bu faaliyetlere örnek olarak gösterilen veri işleme süreçlerinde çocukların kişisel verilerinin işlendiği faaliyetler de yer almaktadır<sup>428</sup>.

Gelişen çevrimiçi teknolojinin de etkisiyle birlikte toplumun savunmasız kesimini oluşturan çocuklar interneti küçük yaşta kullanmaya başlamakta ve kötü niyetli kimseler tarafından açık hedef hâline gelmektedir<sup>429</sup>. Bu nedenle çocuklara yönelik veri işleme faaliyetlerinde (özellikle çevrimiçi ortamdaki faaliyetlerde) veri sorumlularına ek yükümlülükler getirilmesinin yerinde olacağını düşünmekteyiz. Veri işleme faaliyetinin

<sup>423</sup> Çekin, s. 87; Dülger, Kişisel Verilerin Korunması, s. 231; benzer yönde Akdağ, s. 134.

<sup>424</sup> GDPR’ın 38. resitaline erişim için bkz.: <https://gdpr-info.eu/recitals/no-38/>, erişim tarihi. 22.08.2021.

<sup>425</sup> Uçak, s. 47.

<sup>426</sup> Erişim için bkz.: <https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule>, erişim tarihi: 30.09.2021.

<sup>427</sup> Uçak, s. 47.

<sup>428</sup> GDPR’ın 75. resitaline erişim için bkz.: <https://gdpr-info.eu/recitals/no-75/>, erişim tarihi. 22.08.2021.

<sup>429</sup> Guidelines 05/2020 on consent under Regulation 2016/679, s. 29; Uçak, s. 50.

ve sonuçlarının çocuklar tarafından daha kolay anlaşılabilmesi için görsel iletişimin artırılması, animasyon kullanılması, çocuklar ya da yasal temsilcileri tarafından açık rıza gösterilen veri işleme süreçleri ile ilgili olarak açık rıza ve veri işleme devam ettiği sürece periyodik aralıklarla hatırlatma yapılması (örneğin hâlâ açık rıza gösteriyor musunuz şeklinde sorulması) gibi zorunlulukların getirilmesi bu yükümlülüklerle örnek olabilir.

Çocukların rızasına ilişkin olarak KVKK'da ayrıca bir düzenleme bulunmamaktadır. Bu noktada, rızanın ehliyetinin belirlenmesine yönelik bir önceki başlıkta yer alan açıklamaların burası için de geçerlidir. Ancak özellikle, çocuklara yönelik gerçekleştirilen tüm bu süreçlerde, kişisel verilerin korunması hakkının yasal temsilciye değil, çocuklara verildiği unutulmamalıdır<sup>430</sup>.

### 5.2.7. Açık Rıza ile İlgili Diğer Hususlar

Açık rıza herhangi bir şekil şartına tabi tutulmamıştır. Bu nedenle kişi açık rızasını sözlü veya yazılı bir şekilde ilgisine iletebilir. Kişisel Verileri Koruma Kurumu da yayınlamış olduğu rehberde açık rızanın yazılı şekilde alınmasına gerek olmadığını belirtmiştir<sup>431</sup>. Ancak açık rızanın varlığını ispat yükü veri sorumlusundadır.

Açık rızanın geri alınıp alınamayacağı hususunda da KVKK'da özel bir düzenleme bulunmamaktadır. Ancak yine Kişisel Verileri Koruma Kurumu yayınlamış olduğu rehberde “*Açık rıza geri alınabilir. Geri alma işlemi ileriye etkilidir.*” ifadelerini kullanmıştır<sup>432</sup>. Dolayısıyla ilgili kişinin açık rızasının bulunduğu zamana ait veri işleme faaliyetlerinin sonuçlarının ortadan kaldırılması beklenemez<sup>433</sup>. Açık rıza geri alınmaya dek *açık rızaya bağlı gerçekleştirilen veri işleme süreci* hukuka uygun olacaktır. Diğer bir ifade ile açık rıza geri alınmaya dek yapılan işlemler için hukuka uygunluk nedeninin varlığından söz edilebilir. Öte yandan, Kişisel Verilerin Silinmesi, Yok Edilmesi veya

<sup>430</sup> **Küzeci**, Kişisel Verilerin Korunması, s. 238.

<sup>431</sup> Kişisel Verileri Koruma Kurumu, *Açık Rıza*, s. 1.

<sup>432</sup> Kişisel Verileri Koruma Kurumu, *6698 Sayılı Kişisel Verilerin Korunması Kanununun Uygulanmasına Yönelik Soru Cevaplar*, s. 17-18.

<sup>433</sup> **Braun** s. 17; **Dülger**, Kişisel Verilerin Korunması, s. 238.

Anonim Hale Getirilmesi Hakkında Yönetmelik'in<sup>434</sup> 5. maddesinin 2. fıkrasının d bendine göre “*Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştirildiği hallerde ilgili kişinin rızasını geri alması ...*” durumunda söz konusu kişisel verilerin işlenmesi için gerekli şartlarının ortadan kalktığı kabul edilmektedir<sup>435</sup>.

Açık rızanın geri alınmasının bir sonucu olarak açık rızaya dayalı veri işleme faaliyetinin hukukî bir dayanağı artık kalmayacağından, anılan veri işleme faaliyeti durdurulmalıdır. Örneğin hali hazırda bir müşterisinin cep telefon numarasına açık rızası doğrultusunda reklam amacı güden SMS gönderen bir firma, eğer müşteri açık rızasını geri alırsa artık söz konusu veri işleme faaliyetini gerçekleştiremeyecektir.

Açık rızanın geri alınması, verilmesi kadar kolay olmalıdır<sup>436</sup>. Açık rızanın geri alınmasını zorlaştırıcı prosedürler uygulanmamalıdır.

Açık rızanın geri alınması hakkından önceden feragat edilmesi, TMK'nın 23. maddesinde yer alan “(1) Kimse, hak ve fiil ehliyetlerinden kısmen de olsa vazgeçemez. (2) Kimse özgürlüklerinden vazgeçemez veya onları hukuka ya da ahlâka aykırı olarak sınırlayamaz.” hükümleri gereğince mümkün değildir<sup>437</sup>.

Son olarak, açık rıza dışındaki veri işleme şartlarının varlığına rağmen ilgili kişiden açık rıza alınarak kişisel veri işlenmesi durumunun değerlendirilmesi gerekir. Yalnızca KVKK metni yorumlandığında, açık rıza dışındaki veri işleme şartlarının varlığına rağmen veri işlemeye yönelik açık rıza alınmasına engel bir durum bulunmamaktadır. Nitekim KVKK'nın 5. maddesinin 2. fıkrasında “*Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür.*” ifadesi bulunmaktadır. Ancak Kişisel Verileri Koruma Kurulu vermiş olduğu kararlarında konuyu ayrıntılı bir şekilde ele almış ve veri işleme şartlarının varlığına rağmen ilgili kişiden açık rıza alınmasını hukuka aykırı bulmuştur. Kurul vermiş olduğu bir kararda “*Diğer kişisel veri işleme şartlarının varlığı durumunda açık rıza alınmasının ilgili kişinin yanıtılması ve yanlış yönlendirilmesi dolayısıyla veri sorumlusunca hakkın kötüye*

---

<sup>434</sup> 28.10.2017 tarihli ve 30224 sayılı Resmî Gazete’de yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik.

<sup>435</sup> Çekin, s. 85.

<sup>436</sup> Dülger, Kişisel Verilerin Korunması, s. 230.

<sup>437</sup> Aynı yönde görüş için bkz.: Dülger, Kişisel Verilerin Korunması, s. 238; Braun, s. 17.



*kullanılması anlamına geleceği ...” ifadelerini kullanmıştır<sup>438</sup>. Gerçekten; veri işleme şartlarının bulunmasına rağmen ilgili kişiden açık rıza alınması, ilgili kişiyi yanlış yönlendirebilir. Nitekim açık rıza istenildiği an geri alınabilir. Bu durumda ilgili kişide - açık rızasını geri aldığı takdirde veri işleme faaliyetinin son bulacağı- yönünde bir algı oluşabilir. Ancak eğer veri işleme faaliyeti bir hukukî yükümlülüğten kaynaklı ise (veya mevcut durumun koşullarına göre diğer veri işleme şartlarından kaynaklı ise) bu durumda söz konusu kişiler verilerin işlenmesine devam edilmesi gerekecektir. Dolayısıyla bu durumda açık rıza istenilmesi, ilgili kişiyi yanlış yönlendirebilir.*

### 5.2.8. TCK'daki İlgilinin Rızasıyla Arasındaki İlişki

İlgilinin rızası TCK'nın 26. maddesinin 2. fıkrasında düzenlenmiştir. Buna göre *“Kişinin üzerinde mutlak surette tasarruf edebileceği bir hakkına ilişkin olmak üzere, açıkladığı rızası çerçevesinde işlenen fiilden dolayı kimseye ceza verilmez.”*

İlgilinin rızasının bir hukuka uygunluk nedeni olarak değerlendirilebilmesi için birtakım geçerlilik şartlarının sağlanması gerekir. **İlk şart**, kişinin üzerinde serbestçe tasarruf edebileceği bir hukuksal değer bulunmasıdır<sup>439</sup>. Rızanın hem hukuka uygunluk nedeni olma fonksiyonunu yerine getirdiği hem de tipikliğin gerçekleşmesine engel olduğu durumlarda mutlak surette kişinin tasarruf edebileceği hukuksal bir değere ilişkin olması gerekir<sup>440</sup>. İlgilinin rızasının bir hukuka uygunluk nedeni olarak değerlendirilebilmesi için **ikinci şart**, rızayı gösteren kişinin, bu iradeyi göstermeye ehil olmasıdır<sup>441 442</sup>. **Üçüncü şart**, rızanın açıklanmasıdır<sup>443</sup>. İlgilinin rızası, en geç davranışın gerçekleştiği anda var

<sup>438</sup> Kişisel Verileri Koruma Kurulu'nun internet adresinde yer verilen bu karara ait tarih veya karar numarası bulunmamaktadır. Karara erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/5412/Acik-Rizinin-Hizmet-Sartina-Baglanmasi>, erişim tarihi: 23.08.2021.

<sup>439</sup> **Ekici Şahin**, s. 111; **Centel / Zafer / Çakmut**, s. 334; **Özen**, s. 442; **Özbek / Doğan / Bacaksız**, Genel Hükümler, s. 332.

<sup>440</sup> Mutlak tasarruf edilebilen hukuksal değerler, sınırlı tasarruf edilebilen hukuksal değerler ve tasarruf edilemeyen değerler hakkında detaylı bilgi için bkz.: **Ekici Şahin**, s. 111-124; **Özen**, s. 442-428.

<sup>441</sup> **Soyaslan**, Doğan, *Ceza Hukuku Genel Hükümler*, Yetkin Yayınları, Güncellenmiş 9. Baskı, Ankara, 2020, s. 379; **Ekici Şahin**, s. 132 vd; **Centel / Zafer / Çakmut**, s. 333-334; **Börekçi**, s. 99; **Özbek / Doğan / Bacaksız**, Genel Hükümler, s. 341-342.

<sup>442</sup> Rızaya ehliyet konusunda TCK'da genel bir hüküm bulunmadığı için, ehliyetin belirlenmesinde öğreti ve uygulamanın büyük rolü bulunmaktadır.

<sup>443</sup> **Ekici Şahin**, s. 167; **Centel / Zafer / Çakmut**, s. 334-335; **Özen**, s. 429; **Hakeri**, s. 327; **Özbek / Doğan / Bacaksız**, Genel Hükümler, s. 342.

olmalıdır<sup>444</sup>. Kural olarak rıza, fiil işleninceye kadar geri alınabilmekle birlikte; başlangıçta var olan rıza, icra hareketlerine başladıktan sonra geri alınırsa, geri alma anından önce gerçekleştirilen hareketler suç olarak nitelendirilmez. Rızanın şüpheye mahal vermemek kaydıyla açık veya örtülü bir şekilde açıklanması mümkündür<sup>445</sup>. **Dördüncü şart** ise rızanın özgür ve sağlıklı bir iradeye dayanmasıdır<sup>446</sup>. Son olarak rızanın ahlaka ve genel adap törelerine aykırı olmaması gerekir<sup>447</sup>.

Kişisel verilere ilişkin suçlarda hukuka uygunluk değerlendirmesi yapılırken KVKK'da yer alan açık rızanın unsurlarının incelenmesi gerekir. KVKK'daki açık rıza ile TCK'daki ilgilinin rızasının birbiri ile örtüştüğü ve örtüşmediği noktalar bulunur. Örneğin, açık rıza gösterme ehliyeti bakımından KVKK'da ve TCK'da özel bir hüküm belirlenmemiştir. Bu doğrultuda, öğretinin çabaları ve uygulama sonucunda açık rıza gösterme ehliyetine yönelik birtakım görüşler ortaya çıkmıştır. Diğer yandan, ilgilinin rızasının, kişinin üzerinde mutlak suretle tasarruf edebileceği bir hakka ilişkin olduğu hususu TCK'da belirtilmişken, KVKK'da bu durum özel olarak belirtilmemiştir. Esasen bu durumun kişisel verilerin korunması düzenlemelerinin ruhuna uygun olduğu söylenebilir. Rızanın açıklama şekli bakımından KVKK yalnızca açık rızayı kabul ederken, TCK'daki ilgilinin rızanın açık veya örtülü bir şekilde belirtilmesi mümkündür<sup>448 449</sup>. Diğer yandan KVKK'daki rızanın mutlaka bilgilendirmeye dayalı olması gerekirken, TCK'daki rızada böyle bir şart bulunmamaktadır<sup>450</sup>. Ancak esasında TCK'daki rızanın sağlıklı bir iradeye dayanması gerekliliği bu anlamda ilgilinin bilgilendirilmesiyle ilişkilendirilebilir<sup>451</sup>. Son olarak, ilgilinin rızasının ahlaka ve genel adap törelerine aykırı olmaması durumu KVKK'nın genel ilkeleri içerisinde "*Hukuka ve dürüstlük kuralına uygun işleme ilkesi*" kapsamında ele alınabilir.

<sup>444</sup> **Börekçi**, s. 99; **Soyaslan**, s. 381, **Özen**, s. 430; **Özbek / Doğan / Bacaksız**, Genel Hükümler, s. 342.

<sup>445</sup> **Akdağ**, s. 113; **Özbek / Doğan / Bacaksız**, Genel Hükümler, s. 342; **Centel / Zafer / Çakmut**, s. 334; **Özen**, s. 429. "Katı irade açıklaması teorisi" rızanın açıklanmasına ilişkin olarak mutlaka bir şekil şartının bulunması gerektiğini, "İradenin yönü teorisi" rızanın açıklanmasının her zaman için şart olmadığını, "Sınırlı irade açıklama teorisi" ise rızanın davranışla da olsa açıklanması kabul etmektedir. Bu üç teori arasındaki görüş ayrılıkları ve eleştiriler için bkz.: **Ekici Şahin**, s. 167 vd.

<sup>446</sup> **Ekici Şahin**, s. 185; **Centel / Zafer / Çakmut**, s. 335.

<sup>447</sup> **Centel / Zafer / Çakmut**, s. 337; **Soyaslan**, 381.

<sup>448</sup> **Özbek / Doğan / Bacaksız**, Genel Hükümler, s. 342; **Centel / Zafer / Çakmut**, s. 334; **Özen**, s. 429; **Hakeri**, s. 327; **Börekçi**, s. 101.

<sup>449</sup> *Braun'a* göre KVKK'nın açık rıza ile ilgili kısmının gerekçesinde 95/46/EC sayılı Direktif'in esas alındığı belirtildiğinden açık rıza yerine örtülü rıza da kullanılabilir. **Braun**, s. 19.

<sup>450</sup> **Börekçi**, s. 103.

<sup>451</sup> **Ekici Şahin**, s. 187.

### 5.3. Kanunlarda Açıkça Öngörülme (m. 5/2-a) ile Hukukî Yükümlülüğün Yerine Getirilmesi (m. 5/2-ç)

#### 5.3.1. Kanunlarda Açıkça Öngörülme (m. 5/2-a)

Kanunlarda bir verinin işlenebileceğine yönelik bir hüküm yer alıyorsa “*Kanunlarda açıkça öngörülme*” veri işleme şartından bahsedilebilir. Burada önemle üzerinde durulması gereken iki konu vardır. Bu konulardan ilki “*kanun*” ifadesinin, ikincisi ise “*açıkça öngörülme*” ifadesinin tercih edilmesi ve bunların sonuçlarıdır.

Kanun koyucu tarafından “*kanun*” ifadesinin kullanılmış olması oldukça önemlidir. Kararname, yönetmelik gibi idarenin genel düzenleyici işlemleriyle veya genel bir yetkiyle kişisel veri işlenmesi durumunda kanunlarda açıkça öngörülme veri işleme şartından söz edilemeyecektir<sup>452</sup>. Diğer bir anlatımla “*kanun*” ifadesinin geniş yorumlanmaması, dolayısıyla ilgili kanun dayanak alınarak hazırlanan yönetmelik, genelge, talimat vb. diğer yazılı metinlerin bu veri işleme şartına dahil edilmemesi gerekmektedir<sup>453</sup>. “*Kanun*” ifadesi dar yorumlanmalıdır. Genel ifadelerle veri işleme konusunda bir yükümlülük doğuran düzenlemeler bu veri işleme şartındaki “*kanun*” ifadesinin karşılığı olamaz. Ancak bu durumda bir sonraki başlıkta ele alınan “*hukuki yükümlülüğün yerine getirilmesi*” veri işleme şartından söz edilebilir.

Üzerinde durulması gereken ikinci önemli konu ise “*açıkça öngörülme*” durumudur. Anılan veri işleme şartı dahilinde işlem yapılabilmesi için söz konusu kanun hükmünden hangi verinin ne amaçla işlendiğinin anlaşılması gerekmektedir<sup>454</sup>. Örneğin fatura düzenlenirken asgari olarak hangi bilgilerin fatura üzerinde yer alması gerektiği 213 sayılı Vergi Usul Kanunu’nun<sup>455</sup> 230. maddesinde açıkça belirtilmiştir. Bu bilgiler arasında “*Faturanın düzenlenme tarihi seri ve sıra numarası, faturayı düzenleyenin adı, varsa ticaret unvanı, iş adresi, bağlı olduğu vergi dairesi ve hesap numarası, müşterinin adı, ticaret unvanı, adresi, varsa vergi dairesi ve hesap numarası*” yer almaktadır. Yine,

<sup>452</sup> **Küzeci**, Kişisel Verilerin Korunması, s. 342; **Dülger**, Kişisel Verilerin Korunması, s. 392 vd.; **Doğan**, s. 68.

<sup>453</sup> **Dülger**, Kişisel Verilerin Korunması, s. 392 vd.

<sup>454</sup> **Dülger**, Kişisel Verilerin Korunması, s. 392 vd.

<sup>455</sup> 12.01.1961 tarihli ve 10705 sayılı Resmî Gazete’de yayımlanan 213 sayılı Vergi Usul Kanunu Çalışmada “VUK” olarak isimlendirilecektir.

örneğin 4857 sayılı İş Kanunu'nun<sup>456</sup> 75. maddesine göre işveren, çalıştırdığı işçinin kimlik bilgileri ile yasal olarak düzenlemek zorunda olduğu her türlü belge ve kayıtları özlük dosyasında tutmak zorundadır. Belirtmek gerekir ki bu örnekte işçinin kimlik bilgilerinin işlenmesi kanunlarda açıkça öngörülme şartı kapsamında değerlendirilebilirken, işverenin yasal olarak düzenlemek zorunda olduğu her türlü belge ve kayıtlar için her durumda bu veri işleme şartının uygulanacağını söyleyebilmesi güçtür. Nitekim söz konusu belge ve kayıtların içerisinde hangi kişisel verilerin bulunduğu hususu ayrıca başka bir kanunda açıkça düzenlenmemişse, bu durumda aşağıda yer alan hukukî yükümlülüğün yerine getirilmesi veri işleme şartının uygulanması söz konusu olacaktır.

### 5.3.2. Hukukî Yükümlülüğün Yerine Getirilmesi (m. 5/2-ç)

Kişisel verilerin işlenmesinde bir diğer veri işleme şartı, veri sorumlusunun hukukî yükümlülüğünü yerine getirebilmesi için veri işlemenin zorunlu olmasıdır. Hukukî yükümlülüğün kanunlardan doğmuş olması şart değildir. Esasında bu veri işleme şartı, kanunlarda öngörülme ve ilerideki başlıkta ele alınacak olan sözleşmenin kurulması ya da ifasına ilişkin veri işleme şartlarının dışında kalan hukukî yükümlülükler içindir<sup>457</sup>. Kişisel verilerin işlenmesinin gerekçesi açık bir kanun hükmünün dışında bir yönetmelik veya başkaca bir hukukî belge, emir, karar, düzenleme, talimat vb. hukukî yükümlülüğü gerektiren bir sebep ise bu durumda veri sorumlusunun hukukî yükümlülüğünden bahsedilebilir<sup>458</sup>. Örneğin mahkeme emirlerinin ya da resmî makam tarafından verilen talimatların yerine getirilmesinde hukukî yükümlülüğünden bahsedilebilir. Bir şirketin çalışanına maaş ödeyebilmesi için banka hesap numarası, bakmakla yükümlü olduğu kişiler, eşinin çalışıp çalışmadığı, sosyal sigorta numarası gibi bilgilerini işlemesi hukukî yükümlülük çerçevesinde değerlendirilebilir.

<sup>456</sup> 10.06.2003 tarihli ve 25134 sayılı Resmî Gazete'de yayımlanan 4857 sayılı İş Kanunu. Çalışmanın devamında "İş Kanunu" olarak isimlendirilecektir.

<sup>457</sup> **Dülger**, Kişisel Verilerin Korunması, s. 402; **Taştan**, s. 170.

<sup>458</sup> **Yücedağ**, Hukuka Uygunluk Sebepleri, s. 778; **Doğan**, s. 72; **Uncular**, s. 151.

Bu veri işleme şartında dikkat edilmesi gereken önemli bir nokta, verilerin işlenmesinin zorunlu olmasıdır. Dolayısıyla burada hukukî yükümlülüğün gerekliliğinin yanında bir de zorunluluk unsuru var olmalıdır<sup>459</sup>.

Hukukî yükümlülüğün kaynağının yalnızca Türk hukuku olmasının gerekip gerekmediğinin de belirtilmesinde fayda bulunmaktadır<sup>460</sup>. 95/46/EC sayılı Direktif uygulamasında genel kabul gören görüş, başkaca ülke mevzuatından kaynaklı hukukî yükümlülüklerin bu veri işleme şartı kapsamında kabul edilmemesi gerektiği yönündedir<sup>461</sup>. Ancak ABAD; *Parliament v. Council* kararında Amerika Birleşik Devletleri hukukundan kaynaklı bir yükümlülüğü (*havayolu şirketinin yolculara ait kişisel verileri ABD İç Güvenlik Birimine aktarması yükümlülüğü*) bu kapsamda kabul etmiştir<sup>462</sup>. Kanaatimizce bu durumda her somut olay bazında ayrı bir değerlendirme yapılması gerekmektedir<sup>463</sup>.

### 5.3.3. TCK'daki Kanunun Hükmünü İcra ve Yetkili Merciiin Emrini Yerine Getirme Arasındaki İlişkisi

Kanunun hükmünü icra ve yetkili merciiin emrini yerine getirme TCK'nın 24. maddesinde aşağıdaki şekilde düzenlenmiştir:

*“Madde 24- (1) Kanunun hükmünü yerine getiren kimseye ceza verilmez.*

*(2) Yetkili bir merciden verilip, yerine getirilmesi görev gereği zorunlu olan bir emri uygulayan sorumlu olmaz.*

*(3) Konusu suç teşkil eden emir hiçbir surette yerine getirilemez. Aksi takdirde yerine getiren ile emri veren sorumlu olur.*

<sup>459</sup> Mutlu, s. 128.

<sup>460</sup> Doğan, s. 73.

<sup>461</sup> Doğan, s. 73; 29. Madde Çalışma Grubu'nun 06/2014 sayılı görüş yazısı (*legitimate interest*), s. 24, erişim için bkz.: [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf), erişim tarihi: 15.08.2021.

<sup>462</sup> Küzeci, *Kişisel Verilerin Korunması*, s. 345; Doğan, s. 73.

<sup>463</sup> Aynı yönde görüş için bkz.: Kuner, s 76; Doğan, s. 73.

(4) Emrin, hukuka uygunluğunun denetlenmesinin kanun tarafından engellendiği hallerde, yerine getirilmesinden emri veren sorumlu olur.”

Görüleceği üzere TCK'nın 24. maddesindeki hukuka uygunluk nedeni, görevin kanundan veya amirin emrinden kaynaklanmasına göre ikiye ayrılmaktadır<sup>464</sup>. Burada yer alan genel hukuka uygunluk nedenlerinin KVKK'daki “kanunlarda açıkça öngörülme” ve “hukuki yükümlülüğün yerine getirilmesi” veri işleme şartlarıyla benzeştiği ve farklılaştığı noktaların bulunduğu görülmektedir.

Kanun hükmünü icraya yönelik yapılacak değerlendirme açısından belirtmek gerekir ki TCK'daki “kanun” ifadesi KVKK'daki “kanun” ifadesinin aksine geniş yorumlanmakta ve hukuk kuralı anlamına gelmektedir<sup>465</sup>. Dolayısıyla ceza hukukuna ilişkin olmayan diğer yazılı hukuk kuralları da hukuka uygunluk nedeni olarak değerlendirilebilir<sup>466</sup>. Bu anlamda TCK'daki kanun hükmünü icra hukuka uygunluk nedeninin *hangi kişisel verinin işleneceğinin kanun metninde belirtilip belirtilmemesine göre* KVKK'daki kanunlarda açıkça öngörülme veya hukukî yükümlülüğün yerine getirilmesi veri işleme şartlarıyla örtüşebileceği ifade edilebilir.

Yetkili merciin emrinin uygulanması açısından ise, bu hukuka uygunluk nedeninin doğrudan KVKK'daki veri işleme şartlarına benzediğinin belirtilmesi tam olarak mümkün değildir. Nitekim yetkili merciin emrinin uygulanması hukuka uygunluk nedeninden yararlanılabilmesi için bir emrin bulunması, emri verenin yetkili olması, emrin hukuka uygun olması, emrin yerine getirilmesinin zorunlu olması gerekmektedir<sup>467</sup>. Bir emrin bulunması noktasında ise ast-üst ilişkisinin varlığı aranmaktadır<sup>468</sup>. KVKK'daki veri işleme şartında böyle bir ayırım gözetilmemiştir. Diğer yandan KVKK'da emrin hukuka uygun olması gerektiği yönünde araştırma yapılmasına gerek duyulmamaktadır. Son olarak KVKK'daki veri işleme şartında gereklilik unsuru aranmakta iken, TCK'daki düzenlemede zorunluluk unsuru aranmaktadır.

<sup>464</sup> **Toroslu / Toroslu**, s. 159.

<sup>465</sup> **Centel / Zafer / Çakmut**, s. 309; **Hakeri**, s. 274; **Soyaslan**, s. 382; Aksi yönde görüşler ve “Kanun” ifadesinin “kanun kuralı” veya “hukuk kuralı” şeklinde yorumlanmasının sonuçları için bkz.: **Özen**, s. 381.

<sup>466</sup> **Centel / Zafer / Çakmut**, s. 309;

<sup>467</sup> **Korkmaz**, Ceza Hukuku, s. 414; **Centel / Zafer / Çakmut**, s. 311. **Özbek / Doğan / Bacaksız**, Genel Hükümler, s. 396-400.

<sup>468</sup> **Özbek / Doğan / Bacaksız**, Genel Hükümler, s. 396.

Burada yine, KVKK kapsamına giren veri işleme faaliyetlerine yönelik olarak hukuka uygunluğun tespitinde KVKK'daki veri işleme şartlarına yönelik hükümlerinin uygulanması, KVKK kapsamına girmeyen faaliyetlerde ise TCK'daki hukuka uygunluk nedenlerinin uygulanması gerekmektedir.

#### 5.4. Fiili İmkânsızlık ve Zorunluluk Hali (m. 5/2-b)

##### 5.4.1. KVKK'daki Düzenleme

Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukukî geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması durumunda da kişisel veriler, ilgili kişinin rızası aranmaksızın işlenebilir<sup>469</sup>. Dolayısıyla bu veri işleme şartının uygulanmasında dikkat edilmesi gereken unsurların **ilki**; ilgili kişinin fiili imkânsızlık nedeniyle açık rızasını açıklayamayacak durumda olması ya da rızasına hukukî geçerlilik tanınmayan bir durumda bulunmasıdır<sup>470</sup>. **İkinci** unsur ise ilgili kişinin ya da üçüncü bir kişinin hayatı ya da beden bütünlüğünün korunması için veri işlenmesinin zorunluluğudur.

Bu veri işleme şartı, hayatın olağan akışı dahilinde olmayarak gerçekleştirilecek durumları kapsamaktadır<sup>471</sup>. Örneğin bir kişinin kaybolması durumunda elektronik cihazından en son alınan konum sinyalinin kontrol edilmesi ve kişinin yerinin tespitinin yapılması durumunda fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan kişinin hayatı veya beden bütünlüğünün korunması için veri işlenmesi zorunludur<sup>472</sup>. Bu durumda kişinin bilgileri açık rızası bulunmaksızın işlenebilir. Başka bir örnekte; trafik kazası geçiren ve durumu ağır olan bir kimsenin hastane yetkilileri tarafından yakınlarına ulaşabilmek amacıyla kimlik ve iletişim bilgilerinin işlenmesi, müdahale yapabilmek amacıyla kan grubu ve diğer sağlık bilgilerinin işlenmesi için yine

<sup>469</sup> **Başalp**, Kişisel Verilerin Korunması, s. 121; **Dülger**, Kişisel Verilerin Korunması, s. 394 vd.; **Yılmaz / Çavuşoğlu**, s. 89.

<sup>470</sup> **Küzeci**, Kişisel Verilerin Korunması, s. 343.

<sup>471</sup> **Önder**, Nesibe, "6698 Sayılı Kanun'un Öngörmüş Olduğu Kişisel Veri İşleme Şartları Nelerdir?", Veri Güvenliği ve Kişisel Verileri Koruma Derneği Bülteni, E-Dergi, 1. Sayı, İstanbul, s. 33.

<sup>472</sup> Kişisel Verileri Koruma Kurumu, *Örneklerle Kişisel Verilerin Korunması Rehberi*, s. 12.

ilgili kişinin açık rızasına gerek duyulmamaktadır<sup>473</sup>. Nitekim bu örnekte de bilinci yerinde olmayan bir kimsenin hayatının korunması söz konusudur.

Örneklerdeki gibi yaşamsal durumlarda kişisel verilerin işlenmesine yönelik olarak açık rıza alma prosedürleri kişilerin hayatını ya da vücut bütünlüğünü telafisi olmayacak şekilde tehlikeye atabileceğinden, anılan veri işleme şartında açık rızaya gerek bulunmamasına ilişkin düzenleme son derece yerindedir<sup>474</sup>.

Fiili imkânsızlık veri işleme şartının uygulanabilmesi için hayat ve beden bütünlüğü menfaatlerinin açık ve mevcut bir tehlike altında bulunması gerekir. Örneğin bir tatil beldesinde denize giren kişilerin boğulma riskleri karşısında plajı çeken kamera görüntülerinin sık aralıklarla kurtarma merkezine aktarılması genel anlamda kişilerin hayat ve beden bütünlüğünü korumayı amaçlasa da; bir zorunluluktan veya kişiden açık rıza alınmasının önündeki bir engelden söz edilemeyeceğinden bu örnekte fiili imkânsızlık veri işleme şartı kapsamında veri işlenemeyecektir<sup>475</sup>.

Bu veri işleme şartında önemli olan başka bir hususa değinilmesinde fayda vardır. Şöyle ki; KVKK'nın 5. maddesinin gerekçesinde -ki ilgili madde özel nitelikli olmayan kişisel verilerin işleme şartlarını belirler- bu veri işleme şartı için "*Kan grubu, geçirilen hastalıklar ve ameliyatlar, kullanılan ilaçlar gibi verilerin*" işlenebileceği belirtilmiştir. Ancak bu veriler sağlığa ilişkin kişisel verilerdir. Sağlığa ilişkin kişisel verilerin işlenmesi KVKK'nın 6. maddesinde düzenlenmiş olup; kişinin açık rızası ile işlenebilir. 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. Dolayısıyla KVKK'daki veri işleme şartları, bilhassa sağlığa ilişkin kişisel verilerin işleme şartları, her fiili imkânsızlık halinde kişilerin sağlığa ilişkin kişisel verilerinin açık rıza bulunmaksızın işlenmesine izin vermemektedir. Her ne kadar tıbbî teşhis veya tedavi amacı mevcut olsa da 6. maddede kişi yönünden de bir sınırlama olduğundan, örneğin acil bir durumda sağlık personeli bu tedaviyi yapabilirken ve kişinin sağlık bilgilerini

---

<sup>473</sup> Yılmaz/Çavuşoğlu, s. 90; Kişisel Verileri Koruma Kurumu, *Örneklerle Kişisel Verilerin Korunması Rehberi*, s. 12.

<sup>474</sup> Göçmen Uyarer, s. 131-132.

<sup>475</sup> Dülger, *Kişisel Verilerin Korunması*, s. 396.



araştırabilirken; sağlık personeli olmayan ancak geçmişte acil durum eğitimi almış normal bir vatandaşın kişinin sağlık bilgilerini araştırması KVKK'ya aykırı olacaktır. Üzerinde yıllarca çalışılan kanunun bir maddesinin gerekçesi ile başka bir maddesinin metninin uyuşmaması önemli bir eksikliklerdir. Bu doğrultuda sağlığa ilişkin kişisel verilerin fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukukten geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması durumunda işlenebileceğine ilişkin madde metninde değişikliğe gidilmesinde fayda bulunmaktadır.

#### **5.4.2. TCK'daki Zorunluluk Hali ile İlişkisi**

KVKK'daki fiili imkânsızlık hali, TCK'nın 25. maddesinin 2. fıkrasında düzenlenen zorunluluk hali ile örtüşmektedir. Anılan maddeye göre *“Gerek kendisine gerek başkasına ait bir hakka yönelik olup, bilerek neden olmadığı ve başka suretle korunmak olanağı bulunmayan ağır ve muhakkak bir tehlikeden kurtulmak veya başkasını kurtarmak zorunluluğu ile ve tehlikenin ağırlığı ile konu ve kullanılan vasıta arasında orantı bulunmak koşulu ile işlenen fiillerden dolayı faile ceza verilmez.”*

KVKK'daki kişisel veri işleme şartı ile TCK'daki zorunluluk hali arasındaki ilişkiye geçmeden önce, zorunluluk halinin hukukî niteliğinin tespit edilmesi yerinde olacaktır. TCK'da yer alan zorunluluk halinin bir hukuka uygunluk nedeni olarak mı yoksa kusurluluğu etkileyen bir hal olarak mı değerlendirilmesi gerektiği noktasında öğretide görüş farklılıkları bulunmaktadır. Şöyle ki; zorunluluk hali TCK'nın *“Ceza Sorumluluğunu Kaldıran veya Azaltan Nedenler”* bölümünde yer almaktadır. Zorunluluk halinin düzenlendiği 25. maddenin gerekçesinde *“Kusurluluğu ortadan kaldıran bir neden olarak zorunluluk hali”* ifadesine yer verilmiştir. Diğer yandan 5271 sayılı Ceza Muhakemesi Kanunu'nun<sup>476</sup> 223. maddesinin 2. fıkrasının b bendinde *“Suçun zorunluluk hali etkisiyle işlenmiş olması halinde kusurunun bulunmaması dolayısıyla sanık hakkında ceza verilmesine yer olmadığı”* kararı verileceği hüküm altına alınmıştır. Bu çerçevede

<sup>476</sup> 17.12.2004 tarihli ve 25673 sayılı Resmî Gazete'de yayımlanan 5271 sayılı Ceza Muhakemesi Kanunu. Çalışmanın devamında “CMK” olarak isimlendirilecektir.

zorunluluk halinin a) hukuka uygunluk nedeni olduğu<sup>477</sup>, b) kusuru etkileyen bir neden olduğu<sup>478</sup> ve c) somut olayın özelliğine göre her ikisinin de olabileceği<sup>479</sup> yönünde üç farklı görüş ortaya atılmıştır. Bu anlamda zorunluluk halinin hukukî niteliğinin belirlenmesi güç bir hale gelmiştir<sup>480</sup>. Esasında bu yalnızca bir kavram tartışması olmayıp; nihayetinde hukukî sonuçları itibarıyla önemli olan bir meseledir<sup>481</sup>. Nitekim birisinde davranış suç olmaktan çıkarken, ötekinde hukuka aykırılık vasfı korunarak failin içinde bulunduğu durumun özel olması nedeniyle cezalandırılmaması söz konusu olmaktadır<sup>482</sup> <sup>483</sup>. Ancak zorunluluk halinin hukukî nitelendirilmesinin tespitinde hukukun bir bütün olduğu unutulmamalıdır. Nitekim bir hukuk sistemi oluşturulabilmesinin ön koşulu olarak, bu sisteme konu olacak hukukun birlik ve düzen barındırması gerekir<sup>484</sup>. Bir davranışın hukuka aykırı olup olmadığı noktasında bir yargıya varıldığı takdirde bu yargı tüm hukuk düzeni açısından geçerli olmalıdır<sup>485</sup>. Dolayısıyla hukukun herhangi bir dalında bir davranışın hukuka uygunluğu kabul edilmişse, artık aynı sonuç bütün hukuk düzeni açısından kabul edilmelidir<sup>486</sup>. Nitekim TBK'nın "*Hukuka aykırılığı kaldıran haller*" başlıklı 63. maddesinde "*Zarar görenin rızası, daha üstün nitelikte özel veya kamusal yarar, zarar verenin davranışının haklı savunma niteliği taşıması, yetkili kamu makamlarının müdahalesinin zamanında sağlanamayacak olması durumunda kişinin hakkını kendi gücüyle koruması veya zorunluluk hâllerinde de fiil, hukuka aykırı sayılmaz.*" hükmü yer almaktadır. Dolayısıyla zorunluluk halinin bir bütün olarak ele alınmasının sonucunda hukuk düzeninde ceza hukukuna aykırılık – medeni hukuka aykırılık – borçlar hukukuna

<sup>477</sup> Centel / Zafer / Çakmut, s. 326.

<sup>478</sup> Hakeri, s. 368; Özen, s. 481; Özgenç, s. 437-439.

<sup>479</sup> Kangal, Zeynel T., *Ceza Hukukunda Zorunluluk Durumu*, Seçkin Yayıncılık, 1. Baskı, Ankara, Mart 2010, (Kangal, Zorunluluk), s. 48.

<sup>480</sup> Özbek, Veli Özer / Doğan, Koray, "*Zorunluluk Halinin (TCK m. 25/2) Hukuki Niteliği*", Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi Cilt: 9, Sayı 2, 2007, ss. 195-222, s. 195.

<sup>481</sup> Özbek / Doğan, s. 195.

<sup>482</sup> Özbek / Doğan, s. 195.

<sup>483</sup> Almanya hukukunda zorda kalma hali, Alman Ceza Kanunu'nun 34. ve 35. maddelerinde hukuka uygunluk nedeni (m. 34) ve kusurluluğu ortadan kaldıran sebep (mazeret sebebi, m. 35) olarak iki farklı şekilde düzenlenmiştir. Kanunun İngilizce metnine erişim için bkz.: [https://www.gesetze-im-internet.de/englisch\\_stgb/englisch\\_stgb.html#p0191](https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#p0191), erişim tarihi: 25.09.2021.

<sup>484</sup> Önok, R. Murat / Önay, Işıl, "*Hukuk Düzeninin Birliği İlkesi Çerçevesinde Zorunluluk Hâlinin Hukukî Niteliği*", İstanbul Hukuk Mecmuası, 77 – 2, ss. 847-895, s. 851.

<sup>485</sup> Katoğlu, Tuğrul, *Ceza Hukukunda Hukuka Aykırılık*, Seçkin Yayıncılık, Ankara 2003, (Katoğlu, Hukuka Aykırılık), s. 35-36.

<sup>486</sup> Katoğlu, Hukuka Aykırılık, s. 23-24; Toroslu / Toroslu, s. 158; Toroslu, Nevzat, *Ceza Hukukunda Zaruret Hali*, Sevinç Matbaası, Ankara – 1968, s. 76; Önok / Önay, s. 854.

aykırılık halleri bütün hukuk düzeni için sonuç doğuracaktır. *Katoğlu*'na göre her eylem öncelikle ilgili olduğu hukuk dalına aykırılık teşkil etmekte; ancak hukuk düzeninin bir bütün oluşundan dolayı bu aykırılık bütün hukuk düzeni açısından sonuç doğurmaktadır<sup>487</sup>. Bu bilgiler ışığında, TCK'nın 25. maddesinin 2. fıkrasında düzenlenen zorunluluk halinin yalnızca hukuka uygunluk nedeni veya yalnızca kusuru etkileyen bir neden olduğunun söylenmesi güç görünmektedir. Bu nedenle, zorunluluk halinin ikili karakteri bulunduğu ifade edilebilir.

Zorunluluk halinin hukukî niteliğinin belirlenmesinden sonra, KVKK'daki veri işleme şartı ile TCK'daki düzenlemenin karşılaştırılmasının yapılması gerekir. İlk olarak, KVKK'daki veri işleme şartı "*hayat veya beden bütünlüğünün korunması*" durumunda açık rıza olmaksızın veri işlemeyi meşru kılarken, TCK'daki zorunluluk hali de "*ağır ve muhakkak bir tehlikeden kurtulmak veya başkasını kurtarmak*" için gerçekleştirilen davranışı kapsar. İkinci olarak, KVKK'nın genel ilkelerinden "*işleme amacıyla bağlantılı, sınırlı ve ölçülü veri işleme*" ilkesinin bir yansıması, TCK'daki zorunluluk halinde "*tehlikenin ağırlığı ile konu ve kullanılan vasıta arasında orantı bulunmak koşulu*"nda görülmektedir. Son olarak, KVKK'daki düzenlemede "*kişinin kendisi ya da bir başkasının*" ifadesiyle ilgili kişi ve bir başka üçüncü kişi yararına veri işleme meşru kılınırken, aynı şekilde TCK'daki zorunluluk halinde de "*gerek kendisine gerek başkasına ait bir hakka yönelik*" ifadesine yer verilerek kişinin kendisine veya üçüncü bir kişiye ait hakka yönelik davranışın meşru kılındığı belirtilmiştir. Dolayısıyla her iki düzenleme de ilgili kişinin yanında üçüncü kişileri de kapsamaktadır.

##### **5.5. Bir Sözleşmenin Kurulması veya İfası (m. 5/2-c)**

Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması durumunda da kişisel veriler açık rıza bulunmaksızın işlenebilir. Kurulan ya da ifa edilen sözleşmenin yazılı olması şart değildir<sup>488</sup>.

<sup>487</sup> **Katoğlu**, Hukuka Aykırılık, s. 35.

<sup>488</sup> **Dülger**, Kişisel Verilerin Korunması, s. 397.

Anılan veri işleme şartının **ilk unsuru**, sözleşmenin taraflarının verilerinin işlenmesidir. Sözleşme ile ilgisi bulunsa dahi eğer verisi işlenen kişi sözleşmenin tarafı değilse bu veri işleme şartından yararlanılamaz<sup>489 490</sup>. Örneğin bir işverenin alt işveren ile anlaşması durumunda; alt işverenin çalışanları esasında asıl işverenin işlerini yapacaktır. Ancak ortada a) asıl işveren ile alt işveren arasında ve b) alt işveren ile çalışanı arasında kurulan iki sözleşme bulunacaktır. Dolayısıyla asıl işverenin; alt işverenin çalışanın ödeme bilgilerini muhafaza etmesine dayalı veri işleme faaliyetinde bu veri işleme şartından söz edilemeyecektir. Nitekim burada sözleşmenin tarafı olmayan üçüncü bir kişinin bilgilerinin işlenmesi söz konusu olacaktır. Ancak yukarıda ele alınan hukukî yükümlülüğün yerine getirilmesi (KVKK m. 5/2-ç) ve aşağıda ele alınacak meşru menfaat (KVKK m. 5/2-f) kapsamında bir veri işlemeden söz edilebilir. Aynı örnekte işveren ile alt işveren arasındaki sözleşmeye işveren ve alt işveren tarafından imza atılması ise bu veri işleme şartı kapsamında değerlendirilecektir.

Tüzel kişilikler arasında kurulan sözleşmelerde kişisel veri işlenmesinin bu veri işleme şartı dahilinde değerlendirilip değerlendirilemeyeceğinin de açıklığa kavuşturulması gerekir. Tüzel kişiler arasında kurulan sözleşmelerde doğrudan tüzel kişilerin değil, yetkililerinin imzası bulunmaktadır. Dolayısıyla imzayı atan yetkili, sözleşmenin bir tarafı değildir. Sözleşmenin tarafı olan, tüzel kişinin kendisidir<sup>491</sup>. Bu durumda sözleşmenin *taraflarına* ait kişilerin kişisel verileri işlenmeyeceğinden, anılan istisna hükmü kapsamında değerlendirme yapmak mümkün değildir. Bu durumda ilerleyen başlıklarda ele alınacak *veri sorumlusunun meşru menfaatinden* bahsedilebilir<sup>492</sup>.

Ele alınan veri işleme şartının **ikinci unsuru**, veri işlemenin sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olmasıdır. Gerçekten, gerçekleştirilen veri işleme faaliyeti sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili değilse anılan veri işleme şartından yararlanılamaz. Burada önemli olan, sözleşmenin konusunu oluşturan asıl ve yan edimlerin yerine getirilmesi amacıyla kişisel verinin işlenmesinin

---

<sup>489</sup> Doğan, s. 70.

<sup>490</sup> Aksi yönde görüş için bkz.: Çekin, s. 93; Aşıkoğlu, s. 83. Aşıkoğlu'na göre bu maddenin lafzi bakımından veri sorumlusunun sözleşmenin tarafı olması şartı aranmamaktadır. Bunun nedeni sözleşmenin ifası için veri işlemenin üçüncü bir kişi tarafından da yapılabilmesidir. Örneğin bir mesafeli satış sözleşmesinde malı teslim eden kişinin taşıma şirketi olması durumunda, taşıma şirketi sözleşmenin tarafı olmamasına rağmen anılan veri işleme şartı kapsamında kişisel veriler işlenmektedir.

<sup>491</sup> Yücedağ, Hukuka Uygunluk Sebepleri, s.778.

<sup>492</sup> Yücedağ, Hukuka Uygunluk Sebepleri, s.778; Doğan, s. 71.

gerekliliğidir<sup>493</sup>. Dolayısıyla işlenecek kişisel verilere sözleşmede yer verilmesine gerek duyulmamakla birlikte, edimlerin yerine getirilmesi kapsamında gerçekleştirilecek kişisel veri işleme faaliyetlerinde bu veri işleme şartı söz konusu olacaktır. Ancak sözleşme ile uzaktan ya da yakından ilgili olan her kişisel verinin işlenmesi mümkün değildir. Örneğin işçi ve işveren arasındaki iş sözleşmesinin kurulması aşamasında tarafların adı, soyadı, imzası ve kimlik numarası bilgilerinin sözleşmeyle kayıt altına alınması *sözleşmenin kurulması*, işçinin mesai takibinin yapılması sürecinde mesai saatlerinin kayıt altına alınması ise *sözleşmenin yerine getirilmesi* kapsamında değerlendirilebilir. Nitekim 6098 sayılı Türk Borçlar Kanunu'nun<sup>494</sup> 419. maddesine göre de “*İşveren, işçiye ait kişisel verileri, ancak işçinin işe yatkınlığıyla ilgili veya hizmet sözleşmesinin ifası için zorunlu olduğu ölçüde kullanabilir.*” Ancak aynı işverenin; işçisinin tatilden sonra performans düşüklüğü yaşadığını düşünmesi sebebiyle nerede tatil yaptığını sorgulaması sözleşmenin ifası ya da kurulması ile doğrudan doğruya ilgili olmayacaktır. Kişisel veriler yalnızca merak giderme veya işçi üzerinde psikolojik baskı kurma amacıyla işlenmemelidir<sup>495</sup>. Başka bir örnekte, bir e-ticaret sitesinden ürün satın alan bir kimsenin sipariş detaylarının kayıt altına alınması sözleşmenin ifası açısından doğrudan doğruya ilgili olmasına karşın; aynı sipariş detaylarının sonraki aşamalarda reklam ve promosyon amaçlı kullanılması artık sözleşmenin ifası ya da kurulmasıyla doğrudan doğruya ilgili olmayacaktır.

Kişisel Verileri Koruma Kurulu, konuyla ilgili bir kararında “*Müşterilerin/yolcuların yaptığı seyahatlerin şoförler tarafından puanlanmasına ve bu puanların ortalamasının alınmasına dayanan veri işleme faaliyetinin, Kanununun 5 inci maddesinin 2 inci fıkrasının (c) bendinde yer alan “Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması” şartı kapsamında sözleşmenin ifasına ilişkin ana kurucu öge olmadığı veya sözleşmenin ifasıyla doğrudan doğruya bir ilişkisinin var olmaması sebebiyle...*” ifadelerine yer vermiş ve sözleşmenin ana kurucu ögesi olma ile sözleşmeyle doğrudan doğruya olma ölçütlerinin bu veri işleme şartında bulunması gerektiğini belirtmiştir<sup>496</sup>.

<sup>493</sup> Dülger, Kişisel Verilerin Korunması, s. 399.

<sup>494</sup> 04.02.2011 tarihli ve 27836 sayılı Resmî Gazete’de yayımlanan 6098 sayılı Türk Borçlar Kanunu. Çalışmanın devamında “TBK” olarak isimlendirilecektir.

<sup>495</sup> Özer Deniz, s. 361.

<sup>496</sup> Kişisel Verileri Koruma Kurulu’nun 27.01.2020 tarihli ve 2020/65 sayılı karar özetine erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/6717/2020-65>, erişim tarihi: 25.08.2021.

Anılan veri işleme şartının **üçüncü unsuru** ise gerekliliktir. Kanun koyucu, sözleşmenin kurulması ya da ifası için kişisel verinin işlenmesinin “*gerekli*” olması durumunda açık rıza olmaksızın kişisel verilerin işlenebileceğini düzenlemiştir. Örneğin kiracı ile malik arasında kurulan sözleşmede evin adres bilgilerinin veya tarafların adının, soyadının, imzasının yer alması bu veri işleme şartı dahilinde değerlendirilir. Sözleşmenin kurulması veya ifası için gerekli olmadığı halde sözleşme süreçleri ile ilgili olan bir verinin işlenmesi ise bu kapsamda değerlendirilemez.

Açıklığa kavuşturulması gereken bir diğer konu, sözleşmenin kurulması veya ifasının doğrudan doğruya taraflara ait özel nitelikli kişisel verilerin işlenmesini gerektirmesi durumunda hangi veri işleme şartının geçerli olduğudur. Örneğin bir mankenlik ajansı ile anlaşma yapan bir müşterinin fotoğraf ve videolarının yakın çekimi sırasında biyometrik verilerinin işlenmesi gerekebilir. Ancak her türlü fotoğraf ya da video çekimi sırasında biyometrik verinin işlenmesi söz konusu olmayacaktır. Nitekim biyometrik veriler için KVKK’da ayrıntılı bir düzenleme bulunmamakla birlikte, GDPR’ın 4. maddesinde bu veriler “*Yüz görüntüleri veya daktiloskopik veriler gibi bir gerçek kişinin özgün bir şekilde teşhis edilmesini sağlayan veya teyit eden fiziksel, fizyolojik veya davranışsal özelliklerine ilişkin olarak spesifik teknik işlemeden kaynaklanan kişisel veriler*” olarak tanımlanmıştır<sup>497</sup>. Aynı şekilde GDPR’ın 51. resitalinde de “*Fotoğrafların işlenmesinin doğrudan biyometrik veri olarak nitelendirilemeyeceği, yalnızca gerçek bir kişinin benzersiz bir şekilde tanımlanmasına veya doğrulanmasına izin veren belirli bir teknik yöntemle işlendiğinde, bu verilerin biyometrik verilerin tanımı kapsamında kabul edileceği açıklamalarına yer verildiği, dolayısıyla bir verinin biyometrik veri kapsamında değerlendirilebilmesi için o verinin sadece o kişiyi tanımlayabilme ya da doğrulayabilme özelliğine sahip olmasının kriter alındığının değerlendirildiği*” belirtilmiştir<sup>498</sup>. Bu durumda eğer ki örnekte işlenen kişisel veriler biyometrik veri değilse zaten KVKK’nın 5. maddesinin 2. fıkrasının c bendindeki veri işleme şartı uygulanacaktır. Ancak eğer ki bu kişisel veriler biyometrik veri olarak sınıflandırılır ise KVKK’ya göre açık rızanın alınması gündeme gelecektir. Bu durumda Kişisel Verileri Koruma Kurulu’nun kararlarında değindiği “*hizmetin açık rıza şartına bağlı tutulmaması*” kuralı nedeniyle uygulama açısından bir çıkmaza girilecektir. Kanaatimizce sözleşmenin kurulması veya

<sup>497</sup> GDPR’ın 4. maddesine erişim için bkz.: <https://gdpr-info.eu/art-4-gdpr/>, erişim tarihi: 27.08.2021.

<sup>498</sup> GDPR 51. resitale erişim için bkz.: <https://gdpr-info.eu/recitals/no-51/>, erişim tarihi: 27.08.2021

ifasının doğrudan doğruya taraflara ait özel nitelikli kişisel verilerin işlenmesini gerektirmesi durumunda özel nitelikli kişisel verilerin işlenmesine ve muhafazasına ilişkin gerekli tedbirlerin alınması kaydıyla KVKK'nın 5. maddesinin 2. fıkrasının c bendindeki veri işleme şartının uygulanması gerekir.

KVKK'da yer alan bu kişisel veri işleme şartı TCK'daki herhangi bir hukuka uygunluk nedeniyle benzerlik göstermemektedir.

### 5.6. İlgili Kişi Tarafından Alenileştirilmiş Olma (m. 5/2-d)

KVKK'da yer alan bir diğer veri işleme şartı, ilgili kişi tarafından kamuoyuna açıklanmış ya da alenileştirilmiş kişisel verilerin işlenmesidir. Alenileştirmenin bir hukuka uygunluk nedeni olabilmesi için gerekli **ilk unsur**, ilgili kişi tarafından yapılmasıdır. Başkası tarafından alenileştirilmiş bilgilerin işlenmesi halinde bu veri işleme şartından söz edilemez<sup>499</sup>. Örneğin bir işverenin, internet sitesinde çalışanlarına ait özgeçmiş bilgilerini yayınlaması durumunda ilgili kişinin kendisinin bu alenileştirmeyi yaptığı söylenemez<sup>500</sup>. Dolayısıyla bu durumda bir hukuka uygunluk nedeninin varlığından da bahsedilemez.

**İkinci unsur**, kişisel verilerin alenileştirme amacı ile bağlantılı ve orantılı bir şekilde işlenmesidir<sup>501</sup>. Başka bir anlatımla, ilgili kişinin kişisel verisini alenileştirirken taşıdığı amaç ile bu veriyi daha sonradan kullanan kişinin kullanımına yönelik amacı birbiri ile bağlantılı ve orantılı olmalıdır. Örneğin bir avukatın kendi internet sitesinde iletişim bilgilerine yer vermesi ve potansiyel müvekkillerinin avukatlık hizmeti dahilinde kendisi ile iletişime geçmesi halinde alenileştirmedeki bağlantılı ve orantılı olma prensibi gerçekleşir. Aynı örnekte, yeni iş kurmuş kişilere belirli bir ücret karşılığında kendini tanıtmaya imkânı veren bir televizyon kanalının avukatı arayıp ücret karşılığında stüdyoya davet etmesi halinde, bağlantılı ve orantılı olma prensibinin varlığından söz edilemeyecektir.

<sup>499</sup> **Dülger**, Kişisel Verilerin Korunması, s. 405.

<sup>500</sup> **Dülger**, Kişisel Verilerin Korunması, s. 405.

<sup>501</sup> **Küzeci**, Kişisel Verilerin Korunması, s. 346.

Alenileştirme veri işleme şartı kapsamında kişisel verinin hukuka uygun olarak işlenebilmesi için gerekli **üçüncü unsur**, alenileştirme iradesinin varlığıdır. İlgili kişi, kişisel verilerini bilerek ve isteyerek alenileştirmelidir<sup>502</sup>.

KVKK'nın 5. maddesinin gerekçesinde “İlgili kişi tarafından alenileştirilen ve bu haliyle herkes tarafından bilinebilecek hale gelen bu tür verilerin işlenmesinde, korunması gereken hukuki yararın ortadan kalktığı kabul edilmektedir.” İfadelerine yer verilmiştir<sup>503</sup>. Ancak bu ifadelere katılmadığımızı belirtmek isteriz. Nitekim kişisel verilerin alenileştirilmesi halinde de korunması gereken hukukî yarar devam etmektedir. Kaldı ki KVKK'nın istisna hükümlerini düzenleyen 28. maddesinin 2. fıkrasında “İlgili kişinin kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi” durumu KVKK'nın birtakım hükümlerinin uygulanmayacağı haller arasında düzenlenmiştir. KVKK'nın genel ilkeleri, söz konusu uygulanmayacak hükümler arasında yer almamaktadır. Dolayısıyla genel ilkeler tarafından da korunan bir kişisel veri için korunması gereken hukukî yararın ortadan kalktığı savunmak isabetli değildir. Örneğin bir kişinin hobi amaçlı oluşturup kullanmış olduğu internet sitesinde kendisiyle iletişim kurulması amacıyla telefon numarasına yer vermesi, artık bu telefon numarasının korunmasındaki hukukî yararın ortadan kalktığını göstermez. Eğer hukukî yararın ortadan kalktığı kabul edilirse, telefon numarasının üçüncü kişiler tarafından reklam ve promosyon amaçlı aranarak pazarlama yapılmamasının veya alelade bir şekilde internet forumlarında paylaşılmamasının önünde bir engel kalmayacaktır.

## **5.7. Bir Hakkın Tesisi, Kullanılması veya Korunması (m. 5/2-e)**

### **5.7.1. KVKK'daki Düzenleme**

Kişisel veriler bir hakkın tesisi, kullanılması veya korunması için zorunlu olması halinde de açık rıza bulunmaksızın işlenebilir. Kanun koyucu tesis edilecek, kullanılacak veya korunacak hakkın kaynağı ya da türü açısından bir ayırım gözetmemiştir<sup>504</sup>. Kişisel

---

<sup>502</sup> Doğan, s. 74.

<sup>503</sup> Gereğe erişim için bkz.: <https://www2.tbmm.gov.tr/d26/1/1-0541.pdf>, erişim tarihi: 15.08.2021.

<sup>504</sup> Dülger, Kişisel Verilerin Korunması, s. 411-412.



Verileri Koruma Kurumu, *Örneklerle Kişisel Verilerin Korunması Rehberi*'nde “*Veri sorumlularınca ilgili kişilere bir hakkın tesis edilmesi, kullandırılması veya ilgili kişilerin haklarının korunması için gerekli olması halinde kişisel veri işlenebilecektir.*” ifadelerine yer vermiştir<sup>505</sup>. Bu anlamda anılan rehber uyarınca “*ilgili kişilere bir hak tesis edilmesi*”, “*bir hakkın ilgili kişilere kullandırılması*” veya “*ilgili kişilerin haklarının korunması*” için kişisel verinin işlenebileceği sonucuna ulaşılmaktadır. Ancak madde metninde hakkın kime tesis edileceği, kim için kullandırılacağı veya kimi ya da neyi koruyacağına dair özel bir düzenleme bulunmamaktadır. Ayrıca ilgili maddenin gerekçesinde de “*Bir şirketin kendi çalışanı tarafından açılan bir davada ispat için bazı verileri kullanması veya kısıtlı bir kişinin haklarının korunması amacıyla vasinin veya kayyımın, kısıtlının mali bilgilerini tutması hukuka uygun sayılacaktır.*” örneğine yer verildiği görülmektedir. Dolayısıyla madde metninden ve gerekçesinden, yalnızca ilgili kişiye ait değil, üçüncü kişilere ait bir hakkın tesisi, kullanılması veya korunması için de kişisel verinin işlenebileceği yorumu yapılabilmektedir. Dolayısıyla anılan rehber ile ilgili madde metni ve gerekçesi birbiri ile örtüşmemektedir.

Bu veri işleme şartına en tipik örnek olarak, bir davada taraflara veya üçüncü kişilere ait kişisel verilerin işlenmesi verilebilir<sup>506</sup>. Ancak önemle belirtmek gerekir ki; yargılama aşamasında delil olarak sunulan bir kişisel verinin hukuka aykırı yöntemlerle elde edilmemesi, ilgili kişinin özel hayatının gizliliğine, kişisel verilerinin korunması hakkına ve diğer temel hak ve hürriyetlerine aykırı işlemlerde bulunulmaması gerekmektedir<sup>507</sup>. Yargıtay'ın bu konuda çelişkili kararları bulunmaktadır. Örneğin Yargıtay 9. Hukuk Dairesi bir kararında işverenin, çalışanın whatsapp konuşmalarını delil göstererek iş sözleşmesini feshettiği bir olayda whatsapp konuşmalarının gizlilik içeren kişisel veri niteliğinde olduğunu belirterek, nasıl ve ne şekilde temin edildiği anlaşılamayan yazışmaların delil gösterilerek iş sözleşmesinin feshedilmesinin haksız olduğuna hükmetmiştir<sup>508</sup>. Ancak Yargıtay'ın özellikle son yıllardaki kararlarında, başka suretle delil elde edilmesi imkânının bulunmaması nedeniyle, son çare olarak hukuka aykırı bir şekilde işlenen kişisel verileri delil olarak kabul ettiği görülmektedir. Bu tutum,

<sup>505</sup> Kişisel Verileri Koruma Kurumu, *Örneklerle Kişisel Verilerin Korunması Rehberi*, s. 16.

<sup>506</sup> Gerekçeye erişim için bkz.: <https://www2.tbmm.gov.tr/d26/1/1-0541.pdf>, erişim tarihi: 15.08.2021.

<sup>507</sup> Doğan, s. 76.

<sup>508</sup> Yargıtay 9. Hukuk Dairesi'nin 10.01.2019 tarihli, 2018/10718 E. ve 2019/559 K. sayılı kararı, (Yargıtay Bilgi Bankası), erişim tarihi 25.08.2021.

Anayasa'nın 38. maddesinde yer alan “*Kanuna aykırı olarak elde edilmiş bulgular, delil olarak kabul edilemez.*” hükmü ile bağdaşmamaktadır.

### 5.7.2. TCK'daki Hakkın Kullanılması ile İlişkisi

TCK'nın 26. maddesinin 1. fıkrasında “*Hakkını kullanan kimseye ceza verilmez.*” hükmüyle, hakkın kullanılması bir hukuka uygunluk nedeni olarak düzenlenmiştir<sup>509</sup>. Eğer ki hukuk kuralı bir davranışa izin veriyorsa, aynı anda bu hareketi suç sayamaz<sup>510</sup>.

Maddenin gerekçesinde “*Bir hakkı kullanan kimsenin hukuka aykırı bir şekilde hareket etmiş sayılamayacağı, bilinen bir gerçektir. Bir hak, kanun, tüzük, yönetmelik, genelge gibi nizamlara dayanabilir ve hukuken tanınmış ve düzenlenmiş olmak kaydıyla, bir mesleğin icrasından da doğabilir. Burada hakkın doğrudan doğruya kullanılabilir olması aranacaktır. Eğer hak, bir mercie başvurarak kullanılabilirse, artık buradaki hak kapsamında kabul olunmayacaktır.*” ifadelerine yer verilmiştir. Dolayısıyla hem madde metninden hem de gerekçesinden yola çıkıldığında, hukuka uygunluk nedeni olarak hakkın kullanılmasının birtakım şartları barındırması gerektiği söylenebilir. Bunlardan **ilk şart**, hakkın varlığı ve kişiye hukuk düzeni tarafından tanınmasıdır<sup>511</sup>. **İkinci şart**, hakkın hiçbir mercii aracılığına gerek bulunmaksızın doğrudan doğruya kullanılabilir olmasıdır<sup>512</sup>. Örneğin hakkın kullanılması için öncelikle yargı kararıyla tespit edilmesi gerekiyorsa bu durumda doğrudan doğruya kullanılabilirlikten bahsedilemez<sup>513</sup>. **Üçüncü şart**, hakkın sınırlar dışında, nedensellik bağından ari ve kötüye kullanılmamasıdır<sup>514</sup>.

KVKK'da düzenlenen hukuka uygunluk nedeni ile TCK'da düzenlenen genel hukuka uygunluk nedeni karşılaştırıldığında isim olarak benzerliğin bulunduğu; ancak TCK'daki hakkın kullanılmasına ilişkin şartların hiçbirisinin doğrudan doğruya KVKK'daki

<sup>509</sup> Özgenç, s. 324.

<sup>510</sup> Centel / Zafer / Çakmut, s. 342.

<sup>511</sup> Özbek / Doğan / Bacaksız, Genel Hükümler, s. 312; Özgenç, s. 324; Centel / Zafer / Çakmut, s. 342; Özen, s. 407; Hakeri, s. 312.

<sup>512</sup> Özbek / Doğan / Bacaksız, Genel Hükümler, s. 312; Özgenç, s. 324; Centel / Zafer / Çakmut, s. 342; Özen, s. 407; Hakeri, s. 312.

<sup>513</sup> Centel / Zafer / Çakmut, s. 343.

<sup>514</sup> Soyaslan, s. 369; Özbek / Doğan / Bacaksız, Genel Hükümler, s. 312. Centel / Zafer / Çakmut, s. 343; Özen, s. 407.

düzenlemede yer almadığı görülmektedir. Bu anlamda TCK'daki düzenleme KVKK'daki düzenlemeye göre daha belirgin bir şekilde ele alınmıştır. Ancak ne var ki, TCK'nın 5. maddesinde yer alan hüküm ile KVKK'nın yürürlük tarihleri ve normlar hiyerarşisindeki yerleri esas alındığında, KVKK'nın uygulanacağı hallerde, hukuka uygunluk nedenlerinin tespit edilmesi bakımından KVKK'daki hukuka uygunluk nedenlerinin incelenmesi gerekmektedir. Bu itibarla TCK'daki hakkın kullanılmasına ilişkin hükümler ancak KVKK'nın uygulanmayacağı bazı durumlarda söz konusu olabilecektir.

### **5.8. Meşru Menfaat (m. 5/2-f)**

Kişisel verilerin işleme şartlarında incelenecek olan son hukuka uygunluk nedeni meşru menfaattir. KVKK'nın 5. maddesinin 2. fıkrasının f bendine göre "*İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması*" halinde ilgili kişinin açık rızası aranmamaktadır. Dolayısıyla öncelikle bir menfaat bulunmalı, sonrasında bu menfaat meşru olmalıdır. Diğer yandan veri işleme, ilgili kişinin temel hak ve özgürlüklerine zarar vermemelidir. Son olarak veri işleme zorunlu olmalıdır.

Burada ilk olarak meşru menfaat kavramı üzerinde durulmalıdır. Madde gerekçesinde her ne kadar "*...örneğin bir şirket sahibi, çalışanlarının temel hak ve özgürlüklerine zarar vermemek kaydıyla, onların terfileri, maaş zamları yahut sosyal haklarının düzenlenmesinde ya da işletmenin yeniden yapılandırılması sürecinde görev ve rol dağıtımında esas alınmak üzere çalışanların kişisel verilerini işleyebilecektir. Burada, işletmenin yeniden yapılandırılması ya da ehliyetli ve liyakatli çalışanların terfi almaları, veri sorumlusu statüsündeki şirket sahibinin meşru menfaati cümlesindedir...*" şeklinde örnekleme yoluna gidilmiş ise de bu örnekleme meşru menfaat kavramından ne anlaşılması gerektiği ile ilgili tam olarak bilgi vermemektedir. Öte yandan Kişisel Verileri Koruma Kurumu'nun veri işleme şartlarını konu edindiği rehberde "*...veri sorumlusunun elde edeceği fayda; meşru, ilgili kişinin temel hak ve özgürlüğü ile yarışabilecek yeterli düzeyde etkin, belirli ve halihazırda mevcut olan bir menfaatine ilişkin olmalıdır.*"

ifadelerine yer verilmiştir<sup>515</sup>. Bu anlamda ileride meydana gelebilecek, belirsiz ya da alelade bir menfaatin madde kapsamının dışında tutulduğu açıktır. Veri sorumlusunun meşru menfaati, KVKK'nın amacına ve ruhuna uygun bir şekilde yorumlanmalı<sup>516</sup>, aynı şekilde diğer veri işleme şartlarının mevcut olmaması durumunda başvurulabilecek son çare olarak görülmemelidir<sup>517</sup>.

Belirtmek gerekir ki meşru menfaat kavramı 95/46/EC sayılı Direktif ve GDPR'da da yer almaktadır<sup>518</sup>. Özellikle 29. Madde Çalışma Grubu meşru menfaat kavramını çok kapsamlı bir şekilde ele almıştır. Gruba göre veri sorumlusunun meşru menfaati, gerçekleştirilecek veri işleminin sonucunda elde edeceği faydaya yönelik olmalı ve veri işleme amacından daha geniş yorumlanmalıdır<sup>519</sup>. Diğer yandan veri sorumlusunun meşru menfaati ile ilgili kişinin temel hak ve özgürlükleri arasında bir dengeyin sağlanması gerekmektedir<sup>520</sup>. Başka bir anlatımla menfaatler dengesi testi yapılmalıdır<sup>521</sup>. Denge testi yapılırken veri sorumlusunun faaliyet gösterdiği sektör ve kişisel verilerin korunmasına yönelik almış olduğu önlemler de dikkate alınmalıdır<sup>522</sup>.

Veri sorumlusunun meşru menfaati ile ilgili kişinin temel hak ve özgürlükleri arasındaki denge sağlanırken gözetilecek unsurlara KVKK'da yer verilmemiştir<sup>523</sup>. Bu nedenle meşru menfaat veri işleme şartı; kavramın sahip olduğu belirsizlik ve kişisel verilerin korunması hakkının özüne zarar verebilecek nitelikte olması sebebiyle eleştirilmektedir<sup>524</sup>. Nitekim meşru menfaat kavramının belirsizliği, temel hak ve özgürlüklere sınırlama getirmesi, özel hayata bir müdahale olduğu, kişisel verilerin korunması hakkının orantısız bir şekilde sınırlandırdığı ve hakkın özüne zarar verdiği gerekçeleriyle anılan hükmün Anayasa'nın 2, 13, 20 ve 90. maddelerine aykırılığı iddia edilerek iptali istenmiş; Anayasa Mahkemesi ise iptal istemini reddederek anılan

<sup>515</sup> Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin İşlenme Şartları*, s. 14,

<sup>516</sup> Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin İşlenme Şartları*, s. 14.

<sup>517</sup> Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin İşlenme Şartları*, s. 16-17.

<sup>518</sup> 95/EC/46 sayılı Direktif'in 7. maddesinin f bendi ve GDPR'ın 6. maddesinin 1. fıkrasının f bendi.

<sup>519</sup> 29. Madde Çalışma Grubu'nun 06/2014 sayılı (*legitimate interest*) görüş yazısı, s. 24.

<sup>520</sup> 29. Madde Çalışma Grubu'nun 06/2014 sayılı (*legitimate interest*) görüş yazısı, s. 23.

<sup>521</sup> **Doğan**, s. 77.

<sup>522</sup> **Kuner**, s. 245.

<sup>523</sup> KVKK'nın bu hükmü için açılan iptal davasında AYM, "veri sorumlusu ile ilgili kişinin menfaat dengesinin gözetilmesi" gerektiğini belirtmektedir. AYM'nin 2016/125 E., 2017/143 K. sayılı ve 28.09.2017 tarihli kararı. Karara erişim için bkz.: <https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2017/143?EsasNo=2016%2F125>, erişim tarihi: 30.08.2021.

<sup>524</sup> **Doğan**, s. 79.

maddeye göre meşru menfaat kavramının belirsiz olduğunun söylenemeyeceğini, zira bu kavramın kişilerin temel hak ve özgürlüklerine zarar getirilmemesi şartıyla ve menfaat dengesi gözetilerek değerlendirilmesi gereken bir kavram olduğunu, bu veri işleme şartının esas düzenleme olmadığını, hak ve menfaat kayıplarını önlemek amacıyla getirildiğini, ihlali veya kötüye kullanımı halinde zaten şikayete tabi olduğunu belirtmiştir.

Kişisel Verileri Koruma Kurulu 25.03.2019 tarihli ve 2019/78 sayılı kararında bu veri işleme şartının tespit edilmesinde, belirsizliğin giderilmesine yardımcı olacak şekilde, birtakım hususların değerlendirilmesi gerektiğini belirtmiştir<sup>525</sup>:

- *“Kişisel verinin işlenmesi sonucunda elde edilecek menfaat ile ilgili kişinin temel hak ve hürriyetlerinin yarışabilir düzeyde olması,*
- *Söz konusu menfaate ulaşılabilmesi bakımından kişisel veri işlenmesinin zorunluluk arz etmesi,*
- *Meşru menfaatin halihazırda mevcut, belirli ve açık olması,*
- *İlgili kişinin temel hak ve hürriyetleri ile yarışabilir nitelikte olan meşru menfaatin elde edilmesi halinde bir yarar sağlanacak olması ve kişisel veri işlenmeksizin başkaca bir yol ve yöntemle bu yararın ortaya çıkmasının mümkün olmaması,*
- *Meşru menfaat belirlenirken söz konusu yararın çok sayıda kişiyi etkilemesi, yalnızca kâr elde edilmesi ya da ekonomik yararın sağlanması amacına yönelik olmaması, iş süreçlerini ya da bir işleyişi kolaylaştırması (örneğin bir birim ya da az sayıda personel nezdinde değil, kurumsal olarak geneli etkileyecek şekilde) gibi şeffaf ve hesap verilebilir nitelikleri haiz kriterlerin esas alınması,*
- *Bu açıdan ilgili kişinin başta kişisel verilerinin korunması olmak üzere temel hak ve hürriyetlerinin zarar görmesini engellemek amacıyla öngörülebilir, açık ve yakın her türlü tehlikeden uzak tutulması,*

---

<sup>525</sup> Kişisel Verileri Koruma Kurulu'nun 25.03.2019 tarihli ve 2019/78 sayılı karar özetine erişim için bkz.: <https://kvkk.gov.tr/Icerik/5434/2019-78>, erişim tarihi: 21.06.2021.

- *Kişisel verilerin bir veri kayıt sisteminde amaçla sınırlı olarak hukuka uygun işleyişinin temini ile zararı ve ihlalleri engellemek için her türlü teknik ve idari tedbirin alınması,*
- *Kişisel verilerin işlenmesinde genel ilkelere uygunluğun sağlanması,*
- *Bu kapsamda, kişinin temel hak ve hürriyetleri ile veri sorumlusunun meşru menfaatinin karşılaştırılarak denge testinin yapılması.”*

Bu kriterlerin meşru menfaat veri işleme şartı kapsamında değerlendirme yapılırken özenle ve dikkatle irdelenmesi gerekir. Diğer yandan değerlendirmede KVKK'nın amacına ve ruhuna uygun bir yorumlama yapılmalı ve meşru menfaatin kapsamı geniş yorumlanmamalıdır<sup>526</sup>. Bu kavramın geniş yorumlanmasının hakkın özüne zarar verebilme tehlikesi taşıdığı unutulmamalıdır<sup>527</sup>.

Önemle belirtmek gerekir ki bu veri işleme şartı dahilinde işlem yapılabilmesi için veri işleme zorunlu olmalıdır. Eğer meşru menfaat, kişisel veri işlenmeden başka bir yöntemle elde edilebiliyorsa kişisel veri işlenmemelidir<sup>528</sup>. Diğer bir anlatımla meşru menfaat, diğer veri işleme şartlarının bulunmadığı durumlarda “*son çare (a last resort), zayıf halka (the weakest link) veya açık kapı (open door)*” olarak görülmemelidir<sup>529</sup>. Nitekim meşru menfaat, her türlü veri işleme faaliyetini meşrulaştırmamaktadır<sup>530</sup>.

Meşru menfaat, tıpkı sözleşmenin kurulması veya ifası kişisel veri işleme şartı gibi, TCK'daki herhangi bir hukuka uygunluk nedeniyle benzerlik göstermemektedir.

## 5.9. Özel Nitelikli Kişisel Verilerin İşlenme Şartları

KVKK'nın 6. maddesinin 2. fıkrasında “*Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili*

<sup>526</sup> Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin İşlenme Şartları*, s. 16.

<sup>527</sup> **Küzeci**, *Kişisel Verilerin Korunması*, s. 347.

<sup>528</sup> **Çekin**, s. 98 vd.

<sup>529</sup> 29. Madde Çalışma Grubu'nun 06/2014 sayılı (*legitimate interest*) görüş yazısı, s. 3 ve 9.

<sup>530</sup> Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin İşlenme Şartları*, s. 17.

verileri ile biyometrik ve genetik verileri” özel nitelikli kişisel veriler olarak düzenlenmiştir.

Anılan maddenin 3. fıkrasında özel nitelikli kişisel verilerin hangi veri işleme amacı dahilinde işlenebileceği yer almaktadır. Bu bağlamda “Sağlık ve cinsel hayat dışındaki özel nitelikli 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 de anlaşılacağı üzere; kanun koyucu özel nitelikli kişisel veriler arasında sağlık ve cinsel hayata ilişkin veriler ile diğer özel nitelikli kişisel veriler olarak ikili bir ayrıma gitmiş, sağlık ve cinsel hayata ilişkin verilerin işlenme amaçlarını kişi ve amaç yönünden sınırlandırmıştır. Esasen bu hükmün Adalet Komisyonu’nda kabul edilen ilk şekli şu şekildeydi: “(1) Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefî inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir. (2) Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır. (3) Birinci fıkrada sayılan kişisel veriler, ilgili kişinin açık rızası aranmaksızın aşağıdaki hallerde işlenebilir: a) Kanunlarda açıkça öngörülmesi. b) Kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından işlenmesi. (4) Özel nitelikli kişisel veriler, ikinci ve üçüncü fıkrada sayılan hallerde, Kurul tarafından belirlenen yeterli önlemlerin alınması şartıyla işlenebilir.” Ancak hüküm, özellikle sağlık ve cinsel hayata yönelik kişisel verilerin yeterli ölçüde korunmadığı gerekçesiyle eleştiriye uğramıştır<sup>531</sup>.

<sup>531</sup> TBMM Tutanak Dergisi, Cilt: 12, 59. Birleşim, 8. Oturum, 22.03.2016, erişim için bkz.: <https://www5.tbmm.gov.tr/tutanaklar/TUTANAK/TBMM/d26/c012/tbmm26012059.pdf>, erişim tarihi. 19.09.2021.

Aşağıda öncelikle sağlık ve cinsel hayat dışındaki kişisel verilerin işleme şartları, sonrasında ise sağlık ve cinsel hayata ilişkin kişisel verilerin işleme şartları ele alınacaktır.

### 5.9.1. Sağlık ve Cinsel Hayat Dışındaki Kişisel Verilerin İşlenmesi

Sağlık ve cinsel hayat dışındaki özel nitelikli kişisel veriler kural olarak ilgili kişinin açık rızası ile işlenebilir. Ancak bu veriler istisnai olarak, kanunlarda öngörülen hallerde ilgili kişinin açık rızası bulunmasa da işlenebilir. Her ne kadar burada da kural açık rıza, istisna kanunlarda öngörülme gibi gözükmese de Kişisel Verileri Koruma Kurulu'nun yayınlamış olduğu 08.07.2019 tarih ve 2019/206 sayılı kararı doğrultusunda kişisel verinin işlenmesine dair kanunda öngörülme halinin bulunduğu durumlarda ilgili kişilerden açık rıza alınması, ilgili kişileri *-rıza göstermediğim takdirde kişisel verilerim işlenmeyecek-* düşüncesine sevk ettiğinden, yanıltıcı nitelikte değerlendirilmektedir<sup>532</sup>.

Özel nitelikli olmayan kişisel verilerin işleme şartlarında *“Kanunlarda açıkça öngörülme”* bulunmaktaydı. Ancak bu maddede *“açıkça”* ifadesi terk edilerek yalnızca *“Kanunlarda öngörülme”* ifadesine yer verilmiştir. Dolayısıyla özel nitelikli olmayan kişisel verilerin işlenmesi sürecinde, kanun haricindeki bir düzenleme hukuka uygunluk nedeni sayılamazken, özel nitelikli kişisel verilerin işlenmesinde eğer veri işleme kanunda yer alan bir düzenlemenin zorunlu sonucu ise<sup>533</sup> ilgili kişiden açık rıza alınmadan veri işlenmesi bir hukuka uygunluk nedeni olarak değerlendirilebilecektir. Bunun bir sonucu olarak, *“kanunlarda öngörülme”* anlamında özel nitelikli kişisel verilerin işlenmesindeki hukuka uygunluk nedenlerinin, özel nitelikli olmayan kişisel verilerdekine göre genişletildiğinin söylenmesi mümkündür<sup>534</sup>. Bu doğrultuda özel nitelikli olmayan kişisel verilerin işlenmesinde *“açıkça”* kanun hükmünün aranmasına karşın; özel nitelikli kişisel verilerin işlenmesinde *“kanunlarda öngörülen haller”* gibi ucu açık ve muğlak bir ifade kullanılması yerinde olmamıştır. Diğer yandan bu durumun

<sup>532</sup> Kişisel Verileri Koruma Kurulu'nun 08.07.2019 tarih ve 2019/206 sayılı karar özetine erişim için bkz.: <https://kvkk.gov.tr/Icerik/6709/2019-206>, erişim tarihi: 28.06.2021.

<sup>533</sup> **Dülger**, Kişisel Verilerin Korunması, s. 423.

<sup>534</sup> **Yücedağ**, Hukuka Uygunluk Sebepleri, s. 772.



kanun koyucunun özel nitelikli kişisel verilere ayrıcalıklı bir koruma alanı yarattığı gerçeğiyle de örtüşmemektedir.

Sağlık ve cinsel hayat haricindeki özel nitelikli kişisel verilerin işlenmesinde kanunlarda öngörülme şartına örnek olarak 2559 sayılı Polis Vazife ve Salâhiyet Kanunu'nun<sup>535</sup> 5. maddesi uyarınca silah ruhsatı, sürücü belgesi, pasaport veya pasaport yerine geçen belge almak için başvuruda bulunan kişilerin parmak izinin alınması, 5352 sayılı Adli Sicil Kanunu'nun<sup>536</sup> 4. maddesi uyarınca Türk mahkemeleri tarafından vatandaş veya yabancı hakkında verilmiş ve kesinleşmiş mahkûmiyet hükümlerinin adlî sicile kaydedilmesi, çalışanların 6356 sayılı Sendikalar ve Toplu İş Sözleşmesi Kanunu<sup>537</sup> kapsamında çalışanların sendikal işlerinin gerçekleştirilmesi ve sendika bilgilerinin özlük dosyasında tutulması verilebilir<sup>538</sup>.

### **5.9.2. Sağlık ve Cinsel Hayata İlişkin Kişisel Verilerin İşlenmesi**

Kişisel veriler, işlenmelerinin hukukî sebepleri esas olarak bir piramide benzetilirse, piramidin en üstünde sağlık ve cinsel hayata ilişkin kişisel veriler, bir altında diğer özel nitelikli kişisel veriler, en altta ise özel nitelikli olmayan kişisel verilerin bulunduğu söylenebilir. Ancak bu piramidin en üstünde sağlık ve cinsel hayata ilişkin kişisel verilerin yer alması, bir kişinin dini inancı veya siyasi görüşünün daha az önemli olduğu anlamına gelmez. Nitekim bu benzetme yalnızca veri işleme hukukî sebeplerinin getirmiş olduğu sınırlandırma esas alınarak yapılmıştır. Nitekim özel nitelikli olmayan kişisel verilerin işlenmesi için kanun koyucu tarafından sekiz hukukî sebep belirlenmişken; özel nitelikli kişisel verilerin işlenmesi için kanunlarda öngörülme veya açık rıza şeklinde iki hukukî sebep belirlenmiştir. Sağlık ve cinsel hayata ilişkin kişisel verilerin işlenmesi için ise özel amaçlarla birlikte belirli kişiler veya açık rıza öngörülmüştür.

<sup>535</sup> 14.07.1934 tarihli ve 2751 sayılı Resmî Gazete'de yayımlanan 2559 sayılı Polis Vazife ve Salâhiyet Kanunu. Çalışmanın devamında "PVS" olarak isimlendirilecektir.

<sup>536</sup> 01.06.2005 tarihli ve 25832 sayılı Resmî Gazete'de yayımlanan 5352 sayılı Adli Sicil Kanunu. Çalışmanın devamında "Adli Sicil Kanunu" olarak isimlendirilecektir.

<sup>537</sup> 07.11.2012 tarihli ve 28640 sayılı Resmî Gazete'de yayımlanan 6356 sayılı Sendikalar ve Toplu İş Sözleşmesi Kanunu.

<sup>538</sup> Kişisel Verileri Koruma Kurumu, *Özel Nitelikli Kişisel Verilerin İşlenme Şartları*, s. 5.

Sağlık ve cinsel hayata ilişkin verilerin açık rıza bulunmaksızın işlenmesinde kanun hükmünün bir kişisel veri işleme şartı olarak ele alınmadığı<sup>539</sup>, bu verilerin işlenmesi için “kişi” ve “belirli amaçlar” olmak üzere iki kriter getirildiği görülmektedir. Bu anlamda anılan kişisel verilerin işlenmesi için yasal bir dayanağa ihtiyaç duyulmaması, kişisel verilerin korunmasını zayıflatmaktadır<sup>540</sup>.

Aşağıda ilk olarak amaç yönünden, sonrasında ise kişi yönünden işlemeye ilişkin kurallar ele alınacak ve değerlendirilecektir.

### 5.9.2.1. Amaç Yönünden İşleme

KVKK'nın sağlık ve cinsel hayata yönelik işlenmesini ele alan 6. maddesinde yer alan amaçlar;

- a) kamu sağlığının korunması,*
- b) koruyucu hekimlik,*
- c) Tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi,*
- d) Sağlık hizmetleri ile finansmanının planlanması ve yönetimi”*

olarak sıralanabilir. Dolayısıyla sağlık ve cinsel hayata yönelik kişisel veriler yalnızca bu amaçlardan birisinin varlığı halinde -eğer kişi yönünden de uygunluk sağlanıyorsa- ilgili kişinin açık rızası olmaksızın işlenebilir.

<sup>539</sup> İmançlı'ya göre sağlık ve cinsel hayata yönelik bilgiler ancak kanunlarda öngörülen hallerde ve ayrıca maddede belirtilen amaçlarla ve kişiler tarafından işlenebilir. Diğer bir anlatımla, “kanunlarda öngörülme” ifadesi yalnızca sağlık ve cinsel hayat dışındaki özel nitelikli kişisel veriler için değil, aynı zamanda sağlık ve cinsel hayata ilişkin özel nitelikli kişisel verilere de ilişkin olarak değerlendirilmelidir. İmançlı, s. 128.

<sup>540</sup> Dülger, Kişisel Verilerin Korunması, s. 351; İmançlı, s. 128.

### 5.9.2.1.1. Kamu Sağlığının Korunması

Kamu sağlığı, tüm nüfusun sağlığını korumaya odaklanan bir kavramdır<sup>541</sup>. Dolayısıyla kamu sağlığı kapsamında, bir hastalık veya yaralanmanın iyileştirilmesinden ziyade eğitim politikalarının geliştirilmesi, uygulanması, hizmetlerin yönetilip, araştırmalar yapılması sonucunda sağlık sorunlarının oluşmasının ve yeniden ortaya çıkmasının önlenmesi amaçlanmaktadır<sup>542</sup>. Salgınların önlenmesi, çevrenin, iş yerlerinin, konutların, besinin ve suyun korunması, kamunun sağlık durumunun izlenmesi, topluluk eylem programlarının harekete geçirilmesi, doğal afetlere karşı harekete geçilmesi, tıbbi tedavilerin kalitesinin, erişilebilirliğinin ve hesap verebilirliğinin sağlanması, yüksek riskli ve ulaşılmaması zor kişilerin hizmet ihtiyaçlarının karşılanması gibi faaliyetler kamu sağlığının korunması olarak değerlendirilebilir<sup>543</sup>. Dolayısıyla kamu sağlığının korunması, bireysel anlamda bir korunmayı değil, bir bütün olarak tüm nüfusun sağlığının korunmasını ifade etmektedir<sup>544</sup>.

1593 sayılı Umumi Hıfzıssıhha Kanunu'nda<sup>545</sup>, kamu sağlığının korunmasına yönelik birçok tedbir düzenlenmiştir. Örneğin kanunun 57. maddesinde kolera, veba, lekeli humma, karahumma gibi hastalıkların bildirilmesinin zorunlu olduğu<sup>546</sup>, 67. maddesinde bu hastalıkların tedavisinin sağlanması bakımından hekimlerin hastaların yanına veya

---

<sup>541</sup> “Kamu sağlığının misyonu, bir başka deyişle, toplumun sağlığını teşvik eden koşulları sağlamaktır.”, **Novick**, Lloyd F. / **Morrow**, Cynthia B., “Defining Public Health: Historical And Contemporary Developments”, Public Health Administration: Principles For Population-Based Management, Ed. Lloyd F. Novick vd., Sudbury, Jones and Bartlett Publishers, 2005, s.3-33, s.2 (Akt: **Erarslan Türkmen**, s. 173, dn. 127.).

<sup>542</sup> Pfizer Public önderliğinde kurulan Halk Sağlığı Okulları Birliği (*Association of Schools of Public Health*) tanımına erişim için bkz.: <https://web.archive.org/web/20050307160406/http://www.whatispublichealth.org/about/index.html>, erişim tarihi: 30.08.2021.

<sup>543</sup> **Novick**, Lloyd F. / **Morrow**, Cynthia B., s. 2, (Akt: **Erarslan Türkmen**, s. 175-176, dn. 132).

<sup>544</sup> **Erarslan Türkmen**, s. 175; **Dülger**, Kişisel Verilerin Korunması, s. 428.

<sup>545</sup> 06.05.1930 tarihli ve 1489 sayılı Resmî Gazete’de yayımlanan 1593 sayılı Umumi Hıfzıssıhha Kanunu.

<sup>546</sup> “Memleket dahilinde sari ve salgın hastalıklarla mücadele, Madde 57 - Memleket dahilinde sari ve salgın hastalıklarla mücadele Madde 57 – Kolera, veba (Bübon veya zatürree şekli), lekeli humma, karahumma (hummayı tiroidi) daimi surette basil çıkaran mikrop hamilleri dahi - paratifoit humması veya her nevi gıda maddeleri tesemmümatı, çiçek, difteri (Kuşpalazı) - bütün tevkiatı dahi sari beyin humması (İltihabi sahayı dimağii şevkii müstevli), uyku hastalığı (İltihabi dimağii sari), dizanteri (Basilli ve amipli), lohusa humması (Hummai nifası) ruam, kızıl, şarbon, felci tifti (İltihabi nuhai kuddamii sincabii haddi tifti), kızamık, cüzam (Miskin), hummai racia ve malta humması hastalıklarından biri zuhur eder veya bunların birinden şüphe edilir veyahut bu hastalıklardan vefiyat vuku bulur veya mevtin bu hastalıklardan biri sebebiyle husule geldiğinden şüphe olunursa aşağıdaki maddelerde zikredilen kimseler vak'ayı haber vermeğe mecburdurlar. Kudurmuş veya kuduz şüpheli bir hayvan tarafından ısırılmaları, kuduza müptela hastaların veya kuduzdan ölenlerin ihbarı da mecburidir.”

evine girebileceği<sup>547</sup>, 88. maddesinde ise Türkiye’de yaşayan herkese çiçek aşısı uygulanacağı<sup>548</sup> düzenlenmiştir.

#### 5.9.2.1.2. Koruyucu Hekimlik

Koruyucu hekimlik, kamu sağlığına benzer bir şekilde toplum düzeyinde, klinik hekimliğe gelinmeden önceki aşamada, diğer bir ifade hastalıkların henüz risk düzeyindeyken önlenmesine yönelik faaliyetleri ifade etmektedir<sup>549</sup>. Dolayısıyla koruyucu hekimlik, bir hastalığın seyrinin ilerlemesini sınırlayan tüm önlemleri içermektedir<sup>550</sup>. Bu doğrultuda koruyucu hekimlik kavramı açıklanırken üç koruma modeline yer verilmektedir<sup>551</sup>. Bir hastalığın ortaya çıkmasının önlenmesi için uygulanan *birincil koruma* bireyin çevresinin, su kaynaklarının, soluduğu havanın kullanımı ile bireylerin bulaşıcı hastalığa karşı bağışıklık kazandırılması gibi önlemleri içerirken; herhangi bir evrede hastalığın durdurulduğu ya da komplikasyonların önlendiği *ikincil koruma* bulaşıcı hastalığın hastalıktan etkilenmeyen kişilere yayılmasının önlenmesi, terapi yapılması ve rehabilitasyon işlemlerini; *tersiyer koruma* ise hastalığa bağlı olarak gelişebilecek sakatlık ve kalıcı bozuklukların en aza indirgenmesini ve rehabilitasyon hizmetlerini içermektedir<sup>552</sup>.

Yukarıda anılan süreçlerin haricinde sağlık kurum ve kuruluşları (ve/veya yetkilendirdiği başkaca kişiler) tarafından gerçekleştirilen aşılama, temizlik, beslenme aktiviteleri,

---

<sup>547</sup> “Madde 67 – 57 nci maddede zikrolunan sari ve salgın hastalıklar vakaları hakkında tetkikat yapan tabip bu tetkikatı kolaylaştırmak üzere hastanın yanına girmeye ve hastayı ve icabına göre evin sair sakinlerini muayeneye ve hastalığın sureti zuhur ve seyrine dair izahat ve malumat talebine salahiyyettardır. Bu hususta mümaneatı görülenler bu kanunda zikredilen ahkamı mahsusa mucibince cezalandırılır.”

<sup>548</sup> “Madde 88 - Türkiye dahilinde her fert çiçek aşısı ile mükerrenen aşılamağa mecburdur. Bu aşının, icrası tarzı ve vesikaların ne suretle ita olunacağı ve aşılmasının fennen geri bırakılması icap eden kimseler 87 nci maddede yazılan yönetmelikte zikredilir.”

<sup>549</sup> **Erarslan Türkmen**, s. 176-177; **Basan**, Nuri Mehmet / **Bilir**, Nazmi, “Koruyucu Sağlık Hizmetlerinde Önleme Çelişkisi ve Nedenleri”, TAF Preventive Medicine Bulletin, C.XV, No:1, 2016, ss. 44-50, s. 45. erişim için bkz.: <https://docplayer.biz.tr/50144710-Koruyucu-saglik-hizmetlerinde-onleme-celiskisi-ve-nedenleri.html>, erişim tarihi: 22.06.2021.

<sup>550</sup> **Clarke**, E.A., “What is Preventive Medicine?”, Official Publication of The College of Family Physicians of Canada, C.XX, No:11, 1974, ss. 65-68, s. 65.

<sup>551</sup> **Clarke**, s. 65.

<sup>552</sup> **Erarslan Türkmen**, s. 177.

kirlilikle mücadele, altyapı çalışmaları, sağlık taramaları gibi çalışmalar da koruyucu hekimlik faaliyetleridir<sup>553</sup>.

### 5.9.2.1.3. Tıbbi Teşhis, Tedavi ve Bakım Hizmetlerinin Yürütülmesi

Tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi ifadesinden anlaşılması gereken kamu sağlığı ve koruyucu hekimliğin aksine, bireysel anlamda kişilerin iyileştirilmesine yönelik müdahale ve işlemlerin yapılması faaliyetleridir<sup>554</sup>.

Tıbbi teşhis, bir hastalığın tanısının ortaya konulmasıdır<sup>555</sup>. Başka bir ifade ile tıbbi teşhis, bir kişinin semptomlarının ve belirtilerinin hangi hastalık veya durumu ifade ettiğinin belirlenmesi sürecidir<sup>556</sup>. Esasında kişi öncelikle bir şikayetle sağlık kurumuna gelmekte, sağlık kurumundaki hekim hastadan şikayetine ve semptomlarına ilişkin bilgileri almakta, sonrasında ise tanılama süreci başlamakta ve son olarak da hastanın tedavisi gerçekleştirilmektedir<sup>557</sup>. Dolayısıyla tıbbi teşhis kronolojik olarak tedavi ve bakım hizmetlerinden önce gelmektedir<sup>558</sup>.

Tedavi hizmetleri, sağlık durumu bozulan kişilerin eski sağlık düzeylerine ulaşmalarını sağlamak üzere verilen sağlık hizmetlerini ifade etmekte olup; kendi içinde ilk başvuru ve ayakta tedaviyi kapsayan *birinci basamak*, yatarak tedaviyi kapsayan *ikinci basamak* ve üst düzeyde uzmanlaşmış ve yüksek teknoloji kullanılan merkezler aracılığı ile tedaviyi kapsayan *üçüncü basamak* tedavi hizmetleri olmak üzere üçe ayrılmaktadır<sup>559</sup>.

Bakım hizmetleri ise sağlığın korunması, hastalığın önlenmesi ve hastalığın tedavisi ile sağlık hizmetlerinin sağlanmasını ifade etmektedir<sup>560</sup>. Örneğin hasta hakkında sağlık

---

<sup>553</sup> Üçok, Kağan, “Koruyucu Hekimlik ve Acil İlk Yardımda Pratik Bilgiler”, Bizim Ereğli, No:3, Konya, Konya Ereğli Halk Eğitimi Merkezi ve Akşam Sanat Okulu Yayını, 1991, ss. 13-15, s. 13.

<sup>554</sup> Dülger, Kişisel Verilerin Korunması, s. 430.

<sup>555</sup> Erarslan Türkmen, s. 179.

<sup>556</sup> Erişim için bkz.: [https://en.wikipedia.org/wiki/Medical\\_diagnosis](https://en.wikipedia.org/wiki/Medical_diagnosis), erişim tarihi: 30.08.2021.

<sup>557</sup> Balogh, Erin P. / Miller, Bryan T. / Ball, John R., “National Academies of Sciences, Engineering and Medicine”, Improving Diagnosis in Health Care, Ed. Washington DC, The National Academies Press, 2015, s. 2.

<sup>558</sup> Erarslan Türkmen, s. 179.

<sup>559</sup> Akdur, Recep, Türkiye’de Sağlık Hizmetleri ve Avrupa Topluluğu Ülkeleri ile Kıyaslanması, Ankara Üniversitesi Basımevi, 3. Baskı, Ankara, 2000, s. 6.

<sup>560</sup> Mosby’s Medical Dictionary, erişim için bkz.: <https://medical-dictionary.thefreedictionary.com/medical+care>, erişim tarihi: 30.08.2021.

durumu değerlendirmesi yapılması, hastalığın iyileştirilmesi, hastalığın önlenmesi, yayılmasının engellenmesi gibi süreçler evde bakım hizmetlerinin işlevleri arasındadır<sup>561</sup>.

#### 5.9.2.1.4. Sağlık Hizmetleri ile Finansmanının Planlanması ve Yönetimi

Sağlık hizmetleri, kişileri koruyucu ve rehabilite edici hizmetler ile hastalıkları iyileştirici hizmetleri ifade etmektedir<sup>562</sup>. Bu anlamda sağlık hizmetleri, kamu sağlığının sağlanması ve korunmasında en önemli etkenlerden birisidir<sup>563</sup>. Sağlık hizmetlerinin temel esasları, Sağlık Hizmetleri Temel Kanunu'nda<sup>564</sup> düzenlenmiştir. SHTK'nin "*Temel Esaslar*" başlıklı 3. maddesinin f bendi uyarınca "*Herkesin sağlık durumunun takip edilebilmesi ve sağlık hizmetlerinin daha etkin ve hızlı şekilde yürütülmesi maksadıyla, Sağlık Bakanlığı ve bağlı kuruluşlarınca gerekli kayıt ve bildirim sistemi kurulur. Bu sistem, e-Devlet uygulamalarına uygun olarak elektronik ortamda da oluşturulabilir. Bu amaçla, Sağlık Bakanlığınca, bağlı kuruluşları da kapsayacak şekilde ülke çapında bilişim sistemi kurulabilir.*"

Sağlık hizmetlerinin finansmanının planlanması ve yönetimi de esasında SHTK kapsamında ele alınmalıdır. Nitekim sağlık hizmetlerinin doğru ve etkili bir şekilde yürütülmesinin yolu, finansmanının planlanması ve yönetiminden geçer<sup>565</sup>. Dünya Sağlık Örgütü'ne (*World Health Organization - WHO*) göre sağlık hizmetlerinin finansmanı; insanların sağlık ihtiyaçlarına erişebilmeleri için gereken paranın tahsisi, biriktirilmesi ve mobilizasyonu ile ilgili hizmetleri içermekte olup, bu finansmanın amacı fonlamanın

<sup>561</sup> Childs, Alfred W., "*The Functions of Medical Care*", Public Health Reports, C. XC, No: 1, 1975, (10-14), s. 10, (Akt: **Erarslan Türkmen**, s. 180, dn. 150).

<sup>562</sup> **Fişek**, Nusret, "*Sağlık Hizmetleri ve İşçi Sağlığı Ailelerinin Sağlık Sorunları*", Modern Yönetim Semineri, Türk-İş Yayınları, No: 144, 1982, erişim için bkz.: [https://www.ttb.org.tr/n\\_fisek/kitap\\_1/33.html](https://www.ttb.org.tr/n_fisek/kitap_1/33.html), erişim tarihi: 30.08.2021.

<sup>563</sup> **Şimşek**, Zeynep, "*Sağlığı Geliştirmenin Tarihsel Gelişimi ve Örneklerle Sağlığı Geliştirme Stratejileri*", TAF Preventive Medicine Bulletin, C. XII, No: 3, 2013, ss. 343-358, s. 346, erişim için bkz.: <https://docplayer.biz.tr/7908362-Sagligi-gelistirmenin-tarihsel-gelisimi-ve-orneklerle-sagligi-gelistirme-stratejileri.html>, erişim tarihi: 30.08.2021.

<sup>564</sup> 15.05.1987 tarihli ve 19461 sayılı Resmî Gazete'de yayımlanan 3359 sayılı Sağlık Hizmetleri Temel Kanunu. Çalışmanın devamında "SHTK" olarak isimlendirilecektir.

<sup>565</sup> **Uğurluoğlu**, Özgür / **Çelik**, Yusuf, "*Sağlık Sistemleri Performans Ölçümü, Önemi ve Dünya Sağlık Örgütü Yaklaşımı*", Hacettepe Sağlık İdaresi Dergisi, C. VIII, No: 1, 2005, ss. 3-29, s. 6; **Şimşek**, Zeynep, s. 349; **Uğurluoğlu**, Ece / **Özgen**, Hacer, "*Sağlık Hizmetleri Finansmanı ve Hakkaniyet*", Hacettepe Sağlık İdaresi Dergisi, C. XI, No: 2, 2008, ss. 133-160, s. 134.

mümkün kılınması ile tüm bireylerin sağlık hizmetlerine etkili bir şekilde erişilmesini sağlamaktır<sup>566</sup>.

Sağlık hizmetleri ile finansmanının planlanması ve yönetimi süreçleri Türk hukukunda Sağlık Bakanlığı, bağlı teşkilatı, özel hastaneler, Sosyal Güvenlik Kurumu, merkezi yönetim bütçesi gibi kuruluşlar tarafından sağlık hizmetlerinin sunulabilmesi için organizasyonun sağlanması sürecini ifade eder<sup>567</sup>.

### 5.9.2.2. Kişi Yönünden İşleme

Sağlık ve cinsel hayata ilişkin kişisel veriler ilgili kişinin açık rızası bulunmaksızın; yalnızca sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından işlenebilir. Dolayısıyla kişi yönünden ele alınacak değerlendirmede sır saklama yükümlüsü ile yetkili kurum ve kuruluşlar olarak iki faktör bulunmaktadır.

#### 5.9.2.2.1. Sır Saklama Yükümlüsü

Arapça kökenli bir sözcük olan “sır” TDK tarafından “*Varlığı veya bazı yönleri açığa vurulmak istenmeyen, gizli kalan, gizli tutulan şey*” olarak tanımlanmaktadır<sup>568</sup>. Mevzuatımızda ise sır kavramının kesin bir tanımı olmamakla birlikte “*İşitmek, görmek veya hissetmek suretiyle mazhar olunan, manevi bir varlığı haiz bir kavram*” olduğu belirtilmektedir<sup>569</sup>. Diğer yandan sırrın “*bir ya da daha fazla kişiden bilgi gizleme niyeti*” olduğu düşünülebilir<sup>570</sup>. Nihayetinde sır; “*herkes tarafından bilinmeyen ve açıklanması*

---

<sup>566</sup> Dünya Sağlık Örgütü (World Health Organization), “Health Systems Financing”, Haziran 2008, s. 2, erişim için bkz.: [https://www.who.int/healthinfo/statistics/toolkit\\_hss/EN\\_PDF\\_Toolkit\\_HSS\\_Financing.pdf](https://www.who.int/healthinfo/statistics/toolkit_hss/EN_PDF_Toolkit_HSS_Financing.pdf), erişim tarihi: 30.08.2021.

<sup>567</sup> Dülger, Kişisel Verilerin Korunması, s. 431; İmançlı, s. 150.

<sup>568</sup> TDK, Güncel Türkçe Sözlük, erişim için bkz.: <https://sozluk.gov.tr/>, erişim tarihi: 30.08.2021.

<sup>569</sup> Erem, Faruk, “Ceza Hukukunda Meslek Sırrı”, Ankara Üniversitesi Hukuk Fakültesi Dergisi, C. I, No: 1, 1943, ss. 35-72, s. 36, erişim için bkz.: <https://dergipark.org.tr/tr/download/article-file/635609>, erişim tarihi: 30.08.2021.

<sup>570</sup> Slepian, Michael L. / Chun, Jinseok S. / Mason, Malia F., “The Experience of Secrecy”, Journal of Personality and Social Psychology, C. CXIII, No: 1, 2017, ss. 1-33, s. 2, erişim için bkz.:

*sahibinin şeref ve menfaatine zarar verme tehlikesi gösteren hususlar”* olarak tanımlanabilir<sup>571</sup>. Dolayısıyla sırrın başkaları tarafından bilinmemesi ve sır sahibinin bilginin gizli kalması yönündeki iradesi olarak iki unsuru bulunmaktadır<sup>572</sup>.

Mevzuatımızda çeşitli meslek gruplarına veya kuruluşlarına vakıf olduğu sırların korunmasına ilişkin olarak birtakım yükümlülükler getirilmiş olup, bu yükümlülükler genel anlamda sır saklama yükümlülüğü olarak adlandırılmaktadır<sup>573</sup>. Örneğin Tıbbi Deontoloji Nizamnamesi'nin<sup>574</sup> 4. maddesinde “*Tabip ve dış tabibi, meslek ve sanatının icrası vesilesiyle muttali olduğu sırları, kanuni mecburiyet olmadıkça, ifşa edemez. Tıbbi toplantılarda takdim edilen veya yayınlarda bahis konusu olan vakalarda, hastanın hüviyeti açıklanamaz.*” hükmü bulunmaktadır. Hasta Hakları Yönetmeliği'nin 20. maddesinde “*İlgili mevzuat hükümleri ve/veya yetkili mercilerce alınacak tedbirlerin gerektirdiği haller dışında; kişi, sağlık durumu hakkında kendisinin, yakınlarının ya da hiç kimsenin bilgilendirilmemesini talep edebilir. Bu durumda kişinin kararı yazılı olarak alınır. Hasta, bilgi verilmemesi talebini istediği zaman değiştirebilir ve bilgi verilmesini talep edebilir*” hükmü düzenlenmiştir. Türk Eczacıları Deontoloji Tüzüğü'nün<sup>575</sup> 4. maddesinde “*Eczacı, meslek ve sanatının icrası sırasında öğrendiği sırları, kanuni zorunluluk olmadıkça, ifşa edemez.*” hükmü yer almaktadır. Diğer yandan 1136 sayılı Avukatlık Kanunu'nun<sup>576</sup> 36. maddesinde “*Avukatların, kendilerine tevdi edilen veya gerek avukatlık görevi, gerekse, Türkiye Barolar Birliği ve barolar organlarındaki görevleri dolayısıyla öğrendikleri hususları açığa vurmaları yasaktır.*” denilerek avukatların sır saklama yükümlülüğü, 5411 sayılı Bankacılık Kanunu'nun<sup>577</sup> 73. maddesinde “*Kurul başkan ve üyeleri ile Kurum*

[http://www.columbia.edu/~ms4992/Pubs/2017\\_Slepian-Chun-Mason\\_Secrecy\\_JPSP.pdf](http://www.columbia.edu/~ms4992/Pubs/2017_Slepian-Chun-Mason_Secrecy_JPSP.pdf), erişim tarihi: 30.08.2021.

<sup>571</sup> **Donay**, Süheyl, *Meslek Sırrının Açıklanması Suçu*, İstanbul, Sulhi Garan Matbaası Varisleri Kollektif Şirketi, 1978, s. 4; **Karasu**, Sinem, *Hekimin Sır Saklama Yükümlülüğü*, Vedat Kitapçılık, İstanbul, 2009, s. 44; **Özdemir**, Hayrunnisa, “*Hadım Etme ve Hekimin Sır Saklama Yükümlülüğü*”, Gazi Üniversitesi Hukuk Fakültesi Dergisi, C. XIV, Y. 2010, Sa. 1, (**Özdemir**, Sır Saklama), ss. 125-164, s. 138; **Büyükcay**, Yusuf, “*Hekimin Sır Saklama Yükümlülüğü*”, Atatürk Üniversitesi Erzincan Hukuk Fakültesi Dergisi, C. VIII, S. 1-2 (2004), ss. 383-396, s. 386.; **Kolenoğlu**, s. 15.; **Türkmen**, Ali, *Hasta ve Hekim Hukuku*, Adalet Yayınevi, 2. Baskı, Ankara 2013, s. 98; **Yağlıdere**, Sır Saklama Yükümlülüğü, s. 42.

<sup>572</sup> **Donay**, s. 5; **Karasu**, s. 44-45; **Uşan**, Fatih, *İş Sırrının Korunması (Sır Saklama ve Rekabet Yasağı)*, Ankara, Seçkin Yayıncılık, 2003, s. 3; **Erbaş**, Rahime, *Türk Hukukunda ve Karşılaştırmalı Hukukta Sağlık Mesleği Mensuplarının Suçu Bildirme Yükümlülüğü*, On İki Levha Yayıncılık, İstanbul Ceza Hukuku ve Kriminoloji Arşivi Yayını, No: 4, İstanbul, 2015, s. 13; **Yılmaz**, Kişisel Veriler, s. 42-43.

<sup>573</sup> **Erarslan Türkmen**, s. 161.

<sup>574</sup> 19.02.1960 tarihli ve 10436 sayılı Resmî Gazete’de yayımlanan Tıbbi Deontoloji Nizamnamesi.

<sup>575</sup> 27.07.1968 tarihli ve 12961 sayılı Resmî Gazete’de yayımlanan Türk Eczacıları Deontoloji Tüzüğü.

<sup>576</sup> 07/04/1969 tarihli ve 13168 sayılı Resmî Gazete’de yayımlanan 1136 sayılı Avukatlık Kanunu. Çalışmanın devamında “AVK” olarak isimlendirilecektir.

<sup>577</sup> 01.11.2005 tarihli ve 25983 (Mük.) sayılı Resmî Gazete’de yayımlanan 5411 sayılı Bankacılık Kanunu.



personeli, Fon Kurulu başkan ve üyeleri ile Fon personeli görevleri sırasında öğrendikleri bankalara ve bunların bağlı ortaklık, iştirak, birlikte kontrol edilen ortaklıkları ve müşterilerine ait sırları bu Kanuna ve özel kanunlarına göre yetkili olanlardan başkasına açıklayamaz ve kendilerinin veya başkalarının yararlarına kullanamazlar. Kurumun dışarıdan destek hizmeti aldığı kişi ve kuruluşlar ile bunların çalışanları da bu hükme tâbidir. Bu yükümlülük görevden ayrıldıktan sonra da devam eder.” ifadelerine yer verilerek bankacılıkla ilgili bazı unvan ve göreve sahip olan kişilerin sır saklama yükümlülüğü, 1512 sayılı Noterlik Kanunu’nun<sup>578</sup> 54. maddesinde “Noter ve noterlik katipleri, görevleri dolayısıyla öğrendikleri sırları, kanunların emrettiği haller dışında açıklayamazlar.” denilerek noterler ve katiplerinin sır saklama yükümlülüğü, 3568 sayılı Serbest Muhasebeci Mali Müşavirlik ve Yeminli Mali Müşavirlik Kanunu’nun<sup>579</sup> 43. maddesinde “Meslek mensupları ve bunların yanlarında çalışanlar, işleri dolayısıyla öğrendikleri bilgi ve sırları ifşa edemezler, çeşitli kanunlarla muhbirlerle tanınan hak ve menfaatlerden faydalanamazlar.” denilerek meslek mensuplarının ve çalışanlarının sır saklama yükümlülüğü, 6102 sayılı Türk Ticaret Kanunu’nun<sup>580</sup> 613. maddesinde “Ortaklar, şirket sırlarını korumakla yükümlüdür. Bu yükümlülük şirket sözleşmesi veya genel kurul kararıyla kaldırılamaz.”, 626. maddesinde “Müdürler ve yönetimle görevli kişiler, görevlerini tüm özeni göstererek yerine getirmek ve şirketin menfaatlerini, dürüstlük kuralı çerçevesinde, gözetmekle yükümlüdürler.”, 404. maddesinde “Denetçi ve özel denetçi, bunların yardımcıları ile denetleme yapmasına yardımcı olan temsilcileri, denetimi dürüst ve tarafsız bir şekilde yapmak ve sır saklamakla yükümlüdür.” ifadeleriyle şirket ortaklarının, müdürlerinin, yönetimle görevli kişilerin ve denetçilerin sır saklama yükümlülüğü düzenlenmiştir. Ayrıca işverenler açısından İş Kanunu’nun 75. maddesinin 2. fıkrasında “İşveren, işçi hakkında edindiği bilgileri dürüstlük kuralları ve hukuka uygun olarak kullanmak ve gizli kalmasında işçinin haklı çıkarı bulunan bilgileri açıklamamakla yükümlüdür.” hükmü ile İş Sağlığı ve Güvenliği Kanunu’nun<sup>581</sup> 15. maddesinin 2. fıkrasında “Sağlık muayenesi

---

<sup>578</sup> 05.02.1972 tarihli ve 14090 sayılı Resmî Gazete’de yayımlanan 1512 sayılı Noterlik Kanunu.

<sup>579</sup> 13.06.1989 tarihli ve 20194 sayılı Resmî Gazete’de yayımlanan 3568 sayılı Serbest Muhasebeci Mali Müşavirlik ve Yeminli Mali Müşavirlik Kanunu.

<sup>580</sup> 14.02.2011 tarihli ve 27846 sayılı Resmî Gazete’de yayımlanan 6102 sayılı Türk Ticaret Kanunu.

<sup>581</sup> 30.06.2012 tarihli ve 28339 sayılı Resmî Gazete’de yayımlanan 6331 sayılı İş Sağlığı ve Güvenliği Kanunu.

*yaptırılan çalışanın özel hayatı ve itibarının korunması açısından sağlık bilgileri gizli tutulur.” hükmü düzenlenmiştir.*

Sağlık ve cinsel hayata ilişkin kişisel verilerin sır saklama yükümlülükleri tarafından belirtilen amaçlarla işlenmesi veri işleme şartında ilk açıklığa kavuşturulması gereken husus, sır saklama yükümlüsünün kimler olabileceğidir. Yukarıda belirtilen hukukî düzenlemelerde adı geçen kişiler açık rıza bulunmaksızın kişilerin sağlık ve cinsel hayatına ilişkin kişisel verileri işleyebilir mi? Gerçekten, sır saklama yükümlüsünün kimler olabileceği konusunda KVKK’da açık bir hüküm bulunmamaktadır. KVKK’nın 6. maddesinin iptali istemiyle açılan davada AYM, sır saklama yükümlülüğü altında bulunan kişilerin yalnızca hekimler olmadığını “*Sır saklama yükümlülüğü altında olan kişiler ise avukat, hekim veya mali müşavir gibi kendi kanunlarında görevleri dolayısıyla edindikleri bilgileri zamanla sınırlı olmaksızın açığa vurmaları yasak olan ve bu yasağın ihlali halinde hukuki ve cezai sorumluluğu olan kişilerdir*” ifadeleri ile açıklamıştır<sup>582</sup>. Ancak bu verilerin KVKK’daki amaç yönünden sınırlama kriterlerine bakıldığında; madde metninden anlaşılması gerekenin sağlık mesleği mensupları, sağlık kurumları, Sosyal Güvenlik Kurumu personeli gibi sağlık hizmeti ile finansmanının planlaması alanında faaliyet gösteren kişi veya kurumlar olduğu sonucuna ulaşılmaktadır<sup>583</sup>. Nitekim bir avukatın, bankacının, mali müşavirin kamu sağlığının korunması, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması gibi faaliyetlerde asli olarak rol almadığı açıktır. İşverenlerin iş sağlığı ve güvenliği mevzuatındaki yükümlülüklerinden bahisle kamu sağlığının korunması kapsamında hareket ettiği düşünülebilir ise de<sup>584</sup> tam anlamıyla bunu söylemek güçtür.

Öte yandan sağlık sektöründe faaliyet gösteren her kişinin sır saklama yükümlüsü olarak hareket edip edemeyeceğine yönelik olarak da mevzuatımızda açık bir düzenleme yoktur. Bu anlamda çeşitli yorum yöntemleriyle cevaba ulaşmak gerekmektedir. TCK’nın 280. maddesinde düzenlenen “*Sağlık mesleği mensuplarının suçu bildirmemesi suçu*”nun gerekçesinde suçu ihbar yükümlülüğünün “*Bir tıbbi tahlil laboratuvarında görev yapan kişiler*” açısından da mevcut olduğu belirtilmiştir. Dolayısıyla anılan suçta ihbarla

<sup>582</sup> AYM’nin 2016/125 E., 2017/143 K. sayılı ve 28.09.2017 tarihli kararı. Karara erişim için bkz.: <https://www.resmigazete.gov.tr/eskiler/2018/01/20180123-15.pdf>, erişim tarihi: 30.08.2021.

<sup>583</sup> **Dülger**, Kişisel Verilerin Korunması, s. 424.

<sup>584</sup> **İmançlı**, s. 155.

yükümlü kişilerin sınırları yalnızca hekim, tabip, diş tabibi, eczacı, ebe, hemşire, sağlık hizmeti veren diğer kişi ve meslek gruplarını dahil edecek şekilde çizilmemiştir<sup>585</sup>. Buradan hareketle hekimin mahiyetinde çalışan stajyer, asistan, tıbbi sekreter ve hastabakıcı da sırrı saklamakla yükümlüdür<sup>586</sup>. Bu itibarla sır saklama yükümlülüğünün, somut olayın koşullarına göre değerlendirme yapılarak ilgili tıbbi teşhis, tedavi, bakım hizmetleri, sağlık hizmetleri ile finansmanının planlanması ve yönetimi sürecine dahil olan, hasta ile ilgili bilgi ve belgelere görevi gereği ulaşan kişiler bakımından uygulanması gerektiğini düşünmekteyiz<sup>587</sup>.

Diğer yandan örneğin bir avukatın müvekkilinin sağlık bilgileri ile ilgili olarak sürdürdüğü bir davada, müvekkilinin sağlığı ile ilgili bilgileri vekaletin sona ermesinden itibaren üç yıl süre ile saklaması zorunludur<sup>588</sup>. Bu anlamda avukatın sır saklama yükümlüsü olduğu açıktır. Dolayısıyla kişi bakımından sınırlama kriterlerinden “sır saklama yükümlüsü” durumu karşılanmaktadır. Ancak bu örnekte, amaç yönünden sınırlama kriterleri karşılanmamaktadır. Dolayısıyla ilgili kişinin açık rızası olmaksızın avukatın müvekkiline ait sağlık bilgilerini söz konusu uyuşmazlıkta işlemesi KVKK hükümleri dikkate alındığında yasaktır. Eğer ki müvekkil, açık rızasını geri çeker ise bu durumda avukat, müvekkilinin sağlık bilgilerini işleyemeyecek ve AVK'nın 39. maddesinden doğan dosya saklama yükümlülüğünü yerine getiremeyecektir. Bu anlamda sır saklama yükümlüsünün dışında, amaç yönünden sınırlama kriterlerinde de mevcut uygulama sorunları göz önüne alınarak KVKK'da bir düzenleme yapılması gerekmektedir. Burada önemle belirtmeliyim ki Kişisel Verileri Koruma Kurulu bir iş davasıyla ilgili olarak işverenin işçiye ait sağlık bilgilerini mahkemeye delil olarak sunduğu bir olayda “*Diğer yandan 6100 sayılı Hukuk Muhakemeleri Kanununun 219 uncu maddesinin 1 inci fıkrası uyarınca, tarafların, kendilerinin veya karşı tarafın delil*

---

<sup>585</sup> Yağlıdere, Umut Emre, “Sağlık Mesleği Mensuplarının Suçu Bildirmemesi Suçu”, T.C. Kadir Has Üniversitesi Hukuk Fakültesi Dergisi, Cilt: 6, Sayı: 1, Haziran 2018, Prof. Dr. Mustafa Dural Anısına, Özel Sayı – III, (Yağlıdere, Suçu Bildirmeme), ss. 59-79, s. 65.

<sup>586</sup> Yağlıdere, Suçu Bildirmeme, s. 65.

<sup>587</sup> Bu kişilerin sır saklama yükümlüsü olduğu yönünde görüş için bkz.: Zeytin, Zafer, “Hekimin Sır Saklama Yükümlülüğü”, Orijinal Araştırma, Türkiye Klinikleri J Med Ethics 2006, Sayı: 14, ss. 77-82, s. 80.

<sup>588</sup> “AVK Madde 39 - Avukatın dosya saklaması ve hapis hakkı: Madde 39 – Avukat, kendisine tevdi olunan evrakı, vekaletin sona ermesinden itibaren üç yıl süre ile saklamakla yükümlüdür. Şu kadar ki, evrakın geri alınması müvekkile yazı ile bildirilmiş olduğu hallerde saklama yükümlülüğü, bildirme tarihinden itibaren üç ayın sonunda sona erer. Avukat, ücreti ve yapmış olduğu giderleri kendisine ödenmedikçe, elinde bulunan evrakı geri vermekle yükümlü değildir.”

olarak dayandıkları ve ellerinde bulunan tüm belgeleri mahkemeye ibraz etmek zorunda olduğu, bununla birlikte, anılan Kanunun 220 nci maddesinin 3 üncü fıkrası uyarınca, belgeyi ibraz etmesine karar verilen tarafın, kendisine verilen sürede belge ibraz edilmez ve aynı sürede, delillerle birlikte ibraz edilmemesi hakkında kabul edilebilir bir mazeret gösterilmez ya da belgenin elinde bulunduğu inkâr edilirse, mahkemenin, duruma göre belgenin içeriği konusunda diğer tarafın beyanını kabul edebileceği” ifadelerine yer vererek söz konusu veri işlemeyi KVKK’nın istisna hükümlerinde bulunan “Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi” kapsamında ele almıştır<sup>589</sup>. Ancak bu karar şu yönüyle eksiktir: İlgili istisna maddesi kişisel verilerin yargı makamları tarafından işlenmesi halini ele almıştır. Mahkemenin bu bilgileri istisna hükmü kapsamında işlediği açıktır. Ancak kişisel verilerin aktarılması da bir veri işleme olduğundan, esasen somut olayda iki farklı veri işleme mevcuttur. Birincisi mahkemenin bu bilgileri işlemesi, ikincisi ise işverenin bu bilgileri mahkemeye aktarmasıdır. Belirtilen ikinci veri işlemenin bir yargı makamı olmayan işveren tarafından gerçekleştirilmesi sebebiyle bir istisna hali söz konusu olmayacaktır. Eğer ki somut olayda işveren tarafından yapılan veri işleme KVKK’ya uygun olarak nitelendirilecekse -ki görüşümüz bu yönde bir düzenleme yapılmasının gerekli olduğu yönündedir- bu durumda KVKK’nın ilgili maddesinde acilen bir düzenleme yapılması zorunludur.

Son olarak, sağlık verilerinin iş hukuku kapsamında işlenmesinde ortaya çıkan problemlere değinmek gerekir. Bir çalışanın sağlık bilgilerinin iş sağlığı ve güvenliği mevzuatı çerçevesinde iş yeri hekimi tarafından işlenmesi, KVKK’nın 6. maddesinin 3. fıkrasında yer alan amaç ve sınırlama kriterlerine uymaktadır. Ancak iş yeri hekimi çalıştırmayan işyerlerindeki durum belirsizdir. Ayrıca İş Kanunu’nun 25. maddesi uyarınca işverenin haklı sebeple derhal fesih hakkını kullanılabilmesi için, çalışanın sağlık bilgilerinin iş yeri hekimi haricindeki kişiler<sup>590</sup> tarafından işlemesi gerekecektir<sup>591</sup>. Yine, işverenin İş Kanunu’nun 30. maddesi uyarınca elli veya daha fazla kişi çalıştırılan iş yerlerinde engelli çalıştırma yükümlülüğü bulunmaktadır. Dolayısıyla gerek fesih gerekse mevzuattan kaynaklı yükümlülükler çerçevesinde işveren, çalışanına ait sağlık

<sup>589</sup> Kişisel Verileri Koruma Kurulu’nun 18.02.2020 tarihli ve 2020/138 sayılı karar özetine erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/6887/2020-138>, erişim tarihi: 25.09.2021.

<sup>590</sup> Örneğin avukat, insan kaynakları personeli gibi.

<sup>591</sup> Doğan, s. 90.

verilerini işlemek durumundadır. Uygulamada bu bilgiler insan kaynakları süreçlerinin yerine getirilmesi amacıyla istihdam edilen insan kaynakları uzmanları tarafından işlenmektedir. Bu süreçlerin iş yeri hekimine devredilmesi halinde dahi istihdam ve fesih işlemlerinin gereği olarak sağlık bilgilerinin iş yeri hekimi haricindeki kişiler tarafından da işlenmesi gerekmektedir. Bunun dışında, işverenin çalışanını gözetme borcu bulunmaktadır. Bu borca dayalı olarak işveren, çalışanına ait birtakım kişisel verilerini işlemesi gerekebilir<sup>592</sup>. Örneğin işveren, engeli olan bir çalışanı için uygun çalışma düzenini oluşturmakla yükümlü olup; bu yükümlülüğünü yerine getirmek için onun birtakım sağlık bilgilerini bilmesi gerekir<sup>593</sup>. Dolayısıyla çalışanın sağlık verilerinin işlenmesine açık rıza göstermemesi halinde bu tür faaliyetlerin aksayacağı düşünülmektedir<sup>594</sup>.

Özetle, esasında sır saklama yükümlüsünün kim olduğuna ilişkin olarak KVKK'da yeni bir düzenleme yapılması oldukça faydalı olacaktır. Nitekim bu haliyle “*sır saklama yükümlülüğü altında bulunan kişiler*” kavramının kapsamı çok belirsizdir. Diğer yandan sır saklama yükümlüsünün dışında, amaç yönünden sınırlama kriterlerinde de mevcut uygulama sorunları göz önüne alınarak yukarıda belirtilen şekilde bir düzenleme yapılması gerekir.

#### **5.9.2.2.2. Yetkili Kurum veya Kuruluşlar**

KVKK'nın 6. maddesinin gerekçesinde, Sağlık Bakanlığı, sağlık kuruluşu veya Sosyal Güvenlik Kurumu'nun, maddenin 3. fıkrasında yer alan amaçlarla işledikleri ve tuttıkları sağlık ve cinsel hayata ilişkin kişisel verilerin açık rıza bulunmaksızın işleyebileceği belirtilmiştir<sup>595</sup>. Ancak bu ifade yine de yetersiz kalmıştır. Çünkü yetkili kurum ve kuruluşlar ifadesinden ne anlaşılması gerektiği ve hangi dayanak ile “*yetkili*” olunabileceği konuları yeterince net değildir<sup>596</sup>. Sağlık ve cinsel hayata ilişkin bilgilerin

<sup>592</sup> **Belge**, Ayşe Merve, “*Özellikle Kişisel Verilerin Korunması Kanunu Çerçevesinde İşçilerin Kişisel Verilerinin İhlali ve Korunması Yolları*”, Dokuz Eylül Hukuk Fakültesi Dergisi, Prof. Dr. Ertaş'a Armağan, C.19, Özel Sayı, ss. 1025-1051, s.1039; **İmançlı**, s. 218-219.

<sup>593</sup> **Özer Deniz**, s. 367.

<sup>594</sup> Aynı yönde bkz.: **Taştan**, s. 175.

<sup>595</sup> KVKK'nın 6. maddesinin gerekçesi.

<sup>596</sup> Aynı yönde görüş için bkz.: **Doğan**, s. 90.

açık rıza bulunmadan işlenmesini gerektirecek veri işleme amaçları zaten hali hazırda oldukça geniş ve muallaktır. Bir de bunun üzerine “yetkili” kavramının belirsizliği eklenince kişinin en mahrem bilgilerinin açık rızası bulunmaksızın işlenmesi, kişinin temel hak ve özgürlüklerine bir müdahale boyutunda olabilecektir. Önemle belirtmek gerekir ki 95/46/EC sayılı Direktif’in 8. maddesinin 3. maddesinde “... amaçları için üye devletlerin yasal düzenlemelerine göre mesleki olarak sır saklama yükümlülüğü bulunan sağlık personeli veya eşdeğer seviyede sır saklama yükümlülüğü altında bulunan bir başka kişi” ifadelerine yer verilerek yetkili kişilerin kim olduğu açıklığa kavuşturulmuştur. Dolayısıyla KVKK’da da bu soru işaretlerini giderici bir düzenleme yapılması gerekmektedir.

Bununla birlikte, yetkili ifadesinden yalnızca kamu kurumlarının anlaşılması gerekmediği açıktır<sup>597</sup>. Nitekim madde metninde yetkili kurum veya kuruluşun kamu kurumu olması gerektiği yönünde ayrıca bir sınırlama yapılmamıştır.

### 5.9.3. Özel Nitelikli Kişisel Verilerin İşlenmesinde Ek Güvenlik Tedbirleri

Özel nitelikli kişisel verilerin işlenmesi sürecinde ayrıca Kişisel Verileri Koruma Kurulu tarafından belirlenmiş olan yeterli önlemlerin alınması, KVKK’nın 6. maddesinin 4. fıkrası uyarınca zorunludur. Anılan önlemler Kişisel Verileri Koruma Kurulu’nun 31.01.2018 tarihli ve 2018/10 sayılı kararında belirtilmiştir. Buna göre özel nitelikli kişisel verilerin işleme süreçlerine yönelik olarak aşağıdaki idari ve teknik tedbirlerin yerine getirilmesi zorunludur<sup>598</sup>:

*“a) Özel nitelikli kişisel verilerin korunması, saklanması ve işlenmesine yönelik özel politika ve prosedürler benimsenmesi,*

*b) Özel nitelikli kişisel verilerin işlenmesinde rol alan personelin düzenli olarak KVKK ve bilgi güvenliği konularını içeren eğitimler görmesi,*

<sup>597</sup> İmançlı, s. 159.

<sup>598</sup> Kişisel Verileri Koruma Kurulu’nun 31.01.2018 tarihli ve 2018/10 sayılı kararının tamamına erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/4110/2018-10>, erişim tarihi: 22.06.2021.

c) Verilere erişim yetkisi bulunan kişilerin belirlenmesi, bu yetkilerin düzenli aralıklarla kontrol edilmesi, görev değişikliği ya da işten ayrılmalarda bu yetkilerin derhal kaldırılması,

ç) Dijital ortam güvenliğinin sağlanması için ek çalışmalar yapılması (örneğin verilerin kriptografik yöntemler kullanılarak muhafaza edilmesi, veriler üzerinde gerçekleştirilen işlem ve hareketlere ait kayıtların tutulması, uzaktan erişimde iki kademeli kimlik doğrulama sistemi kullanılması, verilere yazılım aracılığı ile erişiliyorsa kullanıcı yetkilendirmelerinin yapılması, yazılımın güvenlik testlerinin düzenli bir şekilde yapılması gibi),

d) Fiziksel ortam güvenliği için ek önlemlerin alınması (örneğin verilerin elektrik kaçağı, yangın, su baskını gibi durumlara karşı korunaklı alanda muhafaza edilmesi, yetkisiz giriş çıkışların engellenmesi gibi),

e) Verilerin dijital ortamda aktarımı halinde kurumsal e-posta adresi veya kayıtlı elektronik posta (KEP) hesabı kullanılması, aktarımın şifreli bir şekilde gerçekleştirilmesi, fiziki aktarımların “gizlilik dereceli belgeler” formatında gerçekleştirilmesi.”

Bu doğrultuda, özel nitelikli kişisel verilerin işlenmesinin KVKK'nın 6. maddesi kapsamında bir hukuka uygunluk nedeni olarak değerlendirilebilmesi için yukarıdaki önlemlerin de alınması gerekmektedir. Belirtilen önlemlerin Devlet Denetleme Kurulu'nun 27.11.2013 tarihinde yayımladığı rapordaki<sup>599</sup> önlemler ile paralel olduğu görülmektedir.

---

<sup>599</sup> Devlet Denetleme Kurulu'nun 27.11.2013 tarihli ve 2013/3 sayılı “Kişisel Verilerin Korunmasına İlişkin Ulusal ve Uluslararası Durum Değerlendirmesi ile Bilgi Güvenliği ve Kişisel Verilerin Korunması Kapsamında Gerçekleştirilen Denetim Çalışmaları” adlı denetim raporunun bir kısmına erişim için bkz.: [https://www.ttb.org.tr/images/stories/file/2015/ddk\\_rapor.pdf](https://www.ttb.org.tr/images/stories/file/2015/ddk_rapor.pdf), erişim tarihi: 19.09.2021.

## 6. KVKK’NIN ÖNLEYİCİ KOLLUK FAALİYETLERİ, CEZA MUHAKAMESİ İŞLEMLERİ VE CEZALARIN İNFAZ İŞLEMLERİYLE İLİŞKİSİ

Önleyici kolluk, ceza muhakemesi ve cezaların infaz işlemleri ile KVKK arasında tıpkı TCK ile KVKK arasında olduğu gibi özel bir ilişki bulunmaktadır. Nitekim önleyici tedbirlerin alınması, delillerin elde edilmesi, muhafaza edilmesi gibi işlemlerin tamamında bir kişisel veri işleme silsilesi vardır ve genellikle bu silsilede kişilerin mahrem bilgileri bulunmaktadır.

Esasen KVKK’nın istisnai hallerini düzenleyen 28. maddesinin 1. fıkrasının b bendine göre “*Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi.*” ve d bendine göre “*Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi.*” durumlarında KVKK’dan tam istisna hali söz konusudur. Dolayısıyla bir tam istisna hali bulunsa da kolluk, ceza muhakemesi ve infaz işlemlerinin KVKK ile yakından ilişkisi olduğu gerçeği değişmemektedir.

Bu başlık altında KVKK açısından yapılacak incelemeler a) Önleyici kolluk faaliyetleri, b) Ceza muhakemesi işlemleri, c) Ceza infaz işlemleri olmak üzere üç kategori altında toplanabilir.

### 6.1. KVKK’nın Önleyici Kolluk Faaliyetleriyle İlişkisi

Önleyici kolluk faaliyetleri açısından ele alınacak işlemler kimlik sorma, kimlik tespiti, parmak izinin kaydı, elektronik gözetim sistemleri, telekomünikasyon yoluyla iletişimin denetlenmesi ve teknik araçlarla izlemedir. Kimlik sorma, yalnız kanunda belirtilen durumlarda başvurulabilen bir kişisel veri toplama yöntemidir<sup>600</sup>. Kimlik sorma PVSK’nin 4. ve 5. maddelerinde düzenlenmiştir. Kimlik sorulan kişinin kimliğini ibraz

<sup>600</sup> **Yenisey**, Feridun, *Kolluk Hukuku*, Beta Yayınları, 2. Baskı, İstanbul, 2015, s. 77; **Can**, Neslihan, *Kolluk ve Adli Makamlar Tarafından İşlenen Kişisel Verilerin Korunması*, On İki Levha Yayıncılık, 1. Baskı, İstanbul, Şubat 2021, 167.



edememesi, açıklamada bulunmaktan kaçınması veya gerçeğe aykırı beyan vermesi durumunda kişinin kimliğinin tespit edilmesi gerekir<sup>601</sup>. Kimlik tespitinde ise kişiyi başkalarından ayıran özelliklerin (örneğin parmak izi) belirlenmesi ve kayda alınması yöntemleriyle bir kişisel veri toplama işlemi bulunur<sup>602</sup>. Kimlik tespiti PVSK'nin 5. maddesinde, CMK'nın 81. ve 147. maddesinde ve 5275 sayılı Ceza ve Güvenlik Tedbirlerinin İnfazı Hakkında Kanun'un<sup>603</sup> 21. maddesinin 3. fıkrasında düzenlenmiştir.

Diğer yandan, PVSK'nin 5. maddesinde, kişinin parmak izinin hangi hallerde alınabileceği belirtilmiştir. Buna göre *“Polis, a) Gönüllü, b) Her çeşit silah ruhsatı, sürücü belgesi, pasaport veya pasaport yerine geçen belge almak için başvuruda bulunan, c) Başta polis olmak üzere, genel veya özel kolluk görevlisi ya da özel güvenlik görevlisi olarak istihdam edilen, ç) Türk vatandaşlığına başvuruda bulunan, d) Sığınma talebinde bulunan veya gerekli görülmesi halinde, ülkeye giriş yapan sair yabancı, e) Gözaltına alınan, kişilerin parmak izini alır.”* KVKK kapsamında bir biyometrik veri olan parmak izi bilgisi PVSK'nin 5. maddesinde görülen hallerde işlenebilir. Burada gönüllülük esasına dayalı veri işlemeden ayrıca söz edilmesi gerekir. Nitekim madde gerekçesinde gönüllü olan kişilerin aydınlatılmış rızaları üzerine parmak izi verisinin işlenmesi gerektiği belirtilmiştir<sup>604</sup>. KVKK kapsamındaki açık rızanın belirli konuya ilişkin, bilgilendirilmeye dayalı ve özgür iradeyle açıklanan rıza beyanı olduğu düşünüldüğünde, bu kriterlerin gönüllülük esasında tam olarak sağlandığı söylenemez. Nitekim gönüllülük esasında verilen parmak izinin hangi konu ve amaçla toplandığına dair ilgili maddede bir düzenleme bulunmamaktadır. Diğer yandan kişinin kamu gücü karşısında özgür iradesiyle hareket edip edemediği şüphe yaratabilir<sup>605</sup>. Bu anlamda ilgili maddenin açık rıza kriterlerine uygun bir şekilde yeniden düzenlenmesi gerekmektedir.

Önleyici kolluk faaliyetlerinde kişisel verilerin özellikle işlendiği bir diğer süreç, elektronik gözetim sürecidir. Elektronik gözetim *“Hakkında veri toplananları etkileme veya idare etme amacıyla tanımlanmış ya da tanımlanmamış herhangi bir kişisel verinin*

---

<sup>601</sup> Can, s. 168.

<sup>602</sup> Can, s. 168; Ömeroğlu, Ömer, *“Ceza Muhakemesinde Şüpheli ve Sanığın Fiziki Kimlik Tespiti”*, TBB Dergisi, 2014 – 115, ss. 61-102, s. 63.

<sup>603</sup> 29.12.2004 tarihli ve 25685 sayılı Resmî Gazete’de yayımlanan 5275 sayılı Ceza ve Güvenlik Tedbirlerinin İnfazı Hakkında Kanun. Çalışmanın devamında “CGİK” olarak isimlendirilecektir.

<sup>604</sup> Erişim için bkz.: <https://www5.tbmm.gov.tr/sirasayi/donem22/yil01/ss1437m.htm>, erişim tarihi. 26.09.2021.

<sup>605</sup> Can, s. 181.

toplanması ve işlenmesi” şeklinde tanımlanabilir<sup>606</sup>. Günümüzde kamusal alanlarda elektronik gözetim sistemlerine yer verilerek insanların suç işlemekten çekinecekleri ve böylelikle suçların önlenebileceği düşüncesi bulunmaktadır<sup>607</sup>. Suçluluğun önlenmesinde etkili olan bu gözetimin genellikle CCTV (*Close Circuit Television*) aracılığıyla yapıldığı gözlemlenmektedir. Diğer yandan, Emniyet Genel Müdürlüğü’nün kullandığı MOBESE (Mobil Elektronik Sistem Entegrasyonu) üzerinde durulması gerekir. MOBESE, coğrafi bilgi sistemleri ve bilgi yönetim sistemleri ile entegre bir şekilde çalışan ve GPRS (*General Packet Radio Service*) teknolojisini kullanan bir yazılımdır<sup>608</sup>. Bu sistem taşıtların plakalarının okunup sahibi ile bağlantı kurulabilmesi ile kritik noktalarda gözetim yapılabilmesi için önemli bir araçtır<sup>609</sup>. Günümüzde bu sistem optik ve teknik araçların kullanılması suretiyle veri toplanması işlevini görmektedir<sup>610</sup>. Dolayısıyla bir veri işlemenin gündeme gelmesi sebebiyle, Anayasa’nın 13. maddesindeki sınırlama ölçütlerine uygun bir şekilde, kanun esasına dayanarak, gözetlemenin usul ve esaslarının açık ve net bir şekilde çizilmesi gerekir<sup>611</sup>. Örneğin bu sistemlerin nerelerde kullanılabilmesi, kamera kayıtlarının ne kadar süre ile hangi ortamlarda saklanabileceği, kamera kayıtlarına kimlerin erişebileceği, gözetimin kimler tarafından gerçekleştirilebileceği gibi hususların belirlenmesi bu açıdan önemlidir<sup>612</sup>. Elektronik gözetimin uygulandığı bir diğer süreç, araç plakasının okunmasıdır. Araç plakasının okunması, araçların plaka tanıma sistemlerinin sabit bir kamera ile izlenmesi ve otomatik biçimde plakaların kaydedilmesi anlamına gelmektedir<sup>613</sup>. Bu yöntem pek çok kişinin tespit edilebilmesinde kullanılabilir<sup>614</sup>. Esasında bu sistem trafik ihlallerinin tespitinde de uygulanabilmektedir. Ancak bu durumda, yapay zekâ teknolojilerinden

---

<sup>606</sup> Lyon, David, *Günlük Hayatı Kontrol Etmek, Gözetlenen Toplum*, Kalkedon Yayınları, İstanbul, 2006, Çeviri: Gözde Soykan, s. 13, 14, (Akt: **Dülger**, *Kişisel Verilerin Korunması*, s. 68.).

<sup>607</sup> **Özbek**, Veli Özer / **Doğan**, Koray / **Bacaksız**, Pınar, *Ceza Muhakemesi Hukuku*, Seçkin Yayıncılık, 12. Baskı, Ankara 2019, (**Özbek / Doğan / Bacaksız**, *Ceza Muhakemesi*) s. 176.

<sup>608</sup> **Can**, s. 188.

<sup>609</sup> **Özbek / Doğan / Bacaksız**, *Ceza Muhakemesi*, s. 174.

<sup>610</sup> **Özbek / Doğan / Bacaksız**, *Ceza Muhakemesi*, s. 174.

<sup>611</sup> Aynı yönde bkz.: **Can**, s. 189; **Yılmaz**, Sabire Sanem, “*Video Gözetimi, Yapay Zekâ ve Kişisel Verilerin Korunması Hakkı*”, (**Yılmaz**, *Gözetim*), erişim için bkz.: <https://www.hukukihaber.net/video-gozetimi-yapay-zeka-ve-kisisel-verilerin-korunmasi-hakki-makale,7001.html>, erişim tarihi: 26.09.2021.

<sup>612</sup> **Derdiman**, Cengiz R. / **Tataroğlu**, Nihan, “*Devletin Gözetimi ile İnsan Haklarının Uyumlaştırılması Sorunu ve Çözüm Önerileri*”, İstanbul Üniversitesi Hukuk Fakültesi Dergisi, Cilt: 7, Sayı: 1, 2016, ss. 247-293, s. 278; **Özbek / Doğan / Bacaksız**, *Ceza Muhakemesi*, s. 178.

<sup>613</sup> **Can**, s. 193.

<sup>614</sup> **Yenisey**, s. 330.

faaydalanılarak *trafik ihlali yapmayan kişilerin kayıt altına alınmaması* yönünde bir sistem geliştirilip kişisel veri ihlallerinin de önüne geçilebilmelidir<sup>615</sup>.

Önleyici kolluk faaliyetlerinde incelenmesi gereken bir diğere husus telekomünikasyon aracılığıyla iletişim denetlenmesidir. PVSK'nin ek 7. maddesinin 2. fıkrası ve Jandarma Kanunu'nun<sup>616</sup> ek 5. maddesinin 1. fıkrası uyarınca polis ve jandarma telekomünikasyon yoluyla iletişimin tespit edilmesi, dinlenmesi, sinyal bilgilerinin değerlendirilmesi ile kayda alınması yetkilerini haizdir.

Diğere yandan PVSK'nın ek 7. maddesinin 6 fıkrası ve Jandarma Kanunu'nun ek 5. maddesinin 5. fıkrasına göre ilgili maddelerde belirtilen katalog suçların önlenmesi amacı güdülerek polis ve jandarmaya teknik araçlarla izleme yetkisi tanınmıştır. Ancak iki düzenlemede de izleme haricinde kayıt yapılabileceği düzenlenmemiştir<sup>617</sup>. Bu durumda polis ve jandarma önleyici amaçlarla yalnızca izleme yapabilecek, ayrıca bu izlediklerini kayıt altına alamayacaktır<sup>618</sup>.

Bir devletin önleyici, koruyucu ve istihbarî faaliyetler yürütmesi gerek devletin yükümlülükleri gerekse kişilerin çıkarları açısından oldukça elzemdir. Her ne kadar bu durumlar önleyici kolluk ya da istihbarî faaliyetler kapsamında değerlendirilebilir ise de (diğere bir ifadeyle KVKK'dan tam olarak istisna hali oluşmuş ise de) KVKK'da yer alan *“işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma”* ile *“dürüstlük kuralına uygun olma”* başta olmak üzere genel ilkelerin de gözetilmesi gerektiğini düşünmekteyiz. Nitekim bu husus anılan faaliyetlerin gerçekleşmesini engellemeyecek ve kişisel verilerin korunmasını destekleyecektir<sup>619</sup>. Aksi durumda tıpkı ABD'de gerçekleşen Ulusal Güvenlik Dairesi skandalı gibi bir durumla karşılaşılabilir, yasadışı ya da amacına ulaşmada çok fazla yarar sağlamayan bir veri işleme gündeme gelebilir<sup>620</sup>.

---

<sup>615</sup> Yılmaz, Gözetim.

<sup>616</sup> 12.03.1983 tarihli ve 17985 sayılı Resmî Gazete'de yayımlanan 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanunu. Çalışmanın devamında “Jandarma Kanunu” olarak isimlendirilecektir.

<sup>617</sup> Can, s. 204.

<sup>618</sup> Can, s. 204.

<sup>619</sup> Küzeci, Kişisel Verilerin Korunması, s. 332.

<sup>620</sup> Ulusal Güvenlik Dairesi skandalı ile ilgili ayrıntılı bilgi için bkz.: [https://en.wikipedia.org/wiki/Edward\\_Snowden](https://en.wikipedia.org/wiki/Edward_Snowden), ayrıca bkz.: [https://www.bbc.com/turkce/haberler/2014/01/140123\\_nsa\\_istihbarat](https://www.bbc.com/turkce/haberler/2014/01/140123_nsa_istihbarat), erişim tarihi: 19.09.2021.

## 6.2. KVKK'nın Ceza Muhakemesi İşlemleriyle İlişkisi

Ceza muhakemesi işlemlerinin de kişisel verilerle ayrılmayan bir bağı vardır. Nitekim kişisel veriler, ceza muhakemesi işlemlerinde devlet eliyle işlenmektedir ve bu veri işleminin şüphesiz ki kişisel verilerin korunması hakkına zarar vermeyecek bir şekilde gerçekleştirilmesi gerekmektedir.

CMK'nın 81. maddesinin 1. fıkrasına göre üst sınırı iki yıl veya daha fazla olan suçlarda şüpheli veya sanığın fizik kimliğinin tespiti yapılır. Fizik kimliğinin tespitinde kişinin fotoğrafından, beden ölçülerinden, parmak ve avuç izinden, bedeninden ve sesi ile görüntülerinden yararlanılmakta, böylelikle kişinin kişisel verilerinin işlenmesi gündeme gelmektedir. Maddenin 2. fıkrasında “*Kovuşturmaya yer olmadığı kararına itiraz süresinin dolması, itirazın reddi, beraat veya ceza verilmesine yer olmadığı kararı verilip kesinleşmesi hâllerinde ...*” söz konusu kayıtların derhâl yok edileceği hüküm altına alınmıştır. Bu doğrultuda yürütülen ceza muhakemesi sona eren ve suçu işlemediği anlaşılan kişinin verilerinin imha edilmesi, KVKK'daki “*işleme amacıyla bağlantılı, sınırlı ve ölçülü olma*” ile “*mevzuatta öngörülen veya işlendikleri amaçla bağlantılı olan süre kadar muhafaza edilme*” ilkesiyle de paraleldir.

Bu başlık altında değerlendirilmesi gereken bir diğer konu, beden muayenesi, vücuttan örnek alınması ve moleküler genetik incelemedir. Beden muayenesi ve vücuttan örnek alınması CMK'nın 75. ve 76. maddelerinde düzenlenmiştir. Burada 76. madde başlığı ile içeriğinin uyuşmadığı belirtilmelidir. Nitekim madde başlığında “*Diğer kişilerin beden muayenesi ve vücuttan örnek alınması*” ifadesinin kullanılmasına karşın madde içeriğinde bu işlemlerin mağdur üzerinde yapılacağı öngörülmüştür. Diğer yandan Ceza Muhakemesinde Beden Muayenesi ve Fiziki Kimliğin Tespiti Hakkında Yönetmelik'in<sup>621</sup> 8. maddesinde bu işlemlerin diğer kişiler üzerinde de yapılabileceği belirtilmiştir. Dolayısıyla düzenlemeler arasındaki tutarsızlığın, kişisel verilerin korunması açısından sakıncalı olduğunu söylemek gerekir<sup>622</sup>. Ayrıca alınan örneklerin bir delil teşkil etmemesi halinde bunların yok edilmesine yönelik bir düzenleme CMK'da bulunmamakla birlikte; anılan yönetmeliğin 6. maddesinin 1. fıkrasında şüpheli veya

<sup>621</sup> 01.06.2005 tarihli ve 25832 sayılı Resmî Gazete'de yayımlanan Ceza Muhakemesinde Beden Muayenesi ve Fiziki Kimliğin Tespiti Hakkında Yönetmelik.

<sup>622</sup> Aynı yönde görüş için bkz.: **Can**, s. 217.

sanığın vücudundan alınan örneklerin derhal yok edileceği belirtilmektedir. Dolayısıyla diğer kişilerin vücudundan alınan örneklerin yok edilip edilmeyeceğine ilişkin bir düzenleme bulunmamakla birlikte, bu durum ciddi bir eksiklik taşımaktadır<sup>623</sup>.

Genetik inceleme, kişinin genetik özelliklerinin belirlenmesine hizmet eden bir yöntem olarak ifade edilmektedir<sup>624</sup>. Olay yeri incelemesi veya beden muayenesinin akabinde vücuttan alınan örnekler, moleküler genetik incelemeye tabi tutulmaktadır<sup>625</sup>. Bu incelemede genellikle DNA alma – eşleştirme yönteminden yararlanılmaktadır<sup>626</sup>. Türk hukukunda CMK hükümleri uyarınca kişiden alınan doku üzerinde yapılan DNA inceleme sonuçları birer kişisel veridir<sup>627</sup>. Elde edilen kişisel veriler, CMK'nın 80. maddesinin 2. fıkrası uyarınca “*Kovuşturmaya yer olmadığı kararına itiraz süresinin dolması, itirazın reddi, beraat veya ceza verilmesine yer olmadığı kararı verilip kesinleşmesi hâllerinde*” derhâl yok edilir. Ayrıca CMK'nın gerek 78. maddesinde gerekse 80. maddesinde alınan örneklerin amacı dışında kullanılmayacağı belirtilmiştir. Bu anlamda yine yukarıda belirtildiği üzere imha işleminin KVKK'daki “*işleme amacıyla bağlantılı, sınırlı ve ölçülü olma*” ve “*mevzuatta öngörülen veya işlendikleri amaçla bağlantılı olan süre kadar muhafaza edilme*” ilkesiyle paralel olduğunu ifade etmek mümkündür.

Ceza muhakemesinin kişisel verilerin korunmasıyla da ilgili olan bir diğer uygulaması, CMK'nın 116 vd. maddelerinde düzenlenen arama ve el koymadır. Nitekim şüpheli veya sanığın üstündeki, eşyasındaki veya konutundaki arama ve el koyma işlemlerinde kişisel verilere erişilebilir<sup>628</sup>. Ancak CMK'da arama ve el koymaya yönelik olarak avukat ve müvekkili arasındaki mesleki ilişkiye dair el konulan bir şeyin imhası dışında kişisel verilerin korunmasıyla ilgili bir düzenlemeye yer verilmemiştir. Arama ve el koymanın özel bir türü olan bilgisayarda ya da bilgisayar kütüklerinde arama, kopyalama ve el koymada kişisel verilerin korunması çok ciddi önem arz etmektedir. Nitekim bu işlemlerde kişilerin fotoğraflarına, sağlık kayıtlarına ve diğer önemli bilgilerine

---

<sup>623</sup> Can, s. 218.

<sup>624</sup> Özbek, Veli Özer, “*Tıp Ceza Hukukunda DNA İncelemesi*”, V. Türk-Alman Tıp Hukuku Sempozyumu, Ankara, Türkiye Barolar Birliği Yayını, 2008, (Özbek, Tıp Ceza Hukuku), s. 1076.

<sup>625</sup> Ünver, Yener / Hakeri, Hakan, *Ceza Muhakemesi Hukuku*, Cilt: 1, Adalet Yayınevi, 15. Baskı, Ankara 2019, s. 619.

<sup>626</sup> Can, s. 211.

<sup>627</sup> Yokuş Sevük, Handan, “*Tıp Ceza Hukukunda Kişisel Verilerin Açıklanması*”, V. Türk-Alman Tıp Hukuku Sempozyumu, Ankara, Türkiye Barolar Birliği Yayını, 2008, s. 797.

<sup>628</sup> Can, s. 225.

erişilebilir. Önemle belirtmek gerekir ki CMK'nın 134. maddesinin 1. fıkrasında Cumhuriyet savcısının kararı ile bu tedbir uygulandığında, hâkim kararı onaylamamış ise kopyaların ve çözümlerin imha edilebileceği düzenlenmiş ise de beraat veya kovuşturmayaya yer olmadığı kararında ne olacağı hükme bağlanmamıştır. Bu yönüyle kişisel verilerin korunmasının önünde bir engel bulunmaktadır<sup>629</sup>.

Ceza muhakemesinde kişisel verilerin işlendiği bir diğer süreç, özel soruşturma yöntemlerinden telekomünikasyon yoluyla iletişimin denetlenmesi ve gizli soruşturmacı görevlendirmesidir. Telekomünikasyon yoluyla iletişimin denetlenmesi CMK'nın 135 vd. maddelerinde düzenlenmiştir. Buna göre bazı suçlarda yapılan soruşturma ve kovuşturmada hâkim veya gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısının kararıyla şüpheli veya şüphelinin iletişimi dinlenebilir, kayda alınabilir ve sinyal bilgileri değerlendirilebilir. Bu yöntemin uygulanabilmesi için suç işlendiğine dair kuvvetli şüphe bulunması ve başka şekilde delil elde edilememesi gerekir. Diğer yandan, şüpheli veya sanığın tanıklıktan çekinebilecek kişilerle yaptığı görüşmeler kayda alınamaz. 135. maddenin 3.fıkrasına göre eğer ki kayıt gerçekleştikten sonra bu durum anlaşılırsa, alınan kayıtlar derhâl yok edilir. Görüleceği üzere burada özel iletişimin denetlenmesi, delillerin elde edilmesine yöneliktir<sup>630</sup>. Yine, 5. fıkra göre şüpheli veya sanığın yakalanabilmesi için mobil telefonunun yeri tespit edilebilir. CMK'nın 137. maddesinin 3. fıkrasına göre şüpheli hakkında kovuşturmayaya yer olmadığına dair karar verilmesi veya hâkim onayının alınmaması durumunda, uygulamaya son verilir ve dinlemeye veya saptamaya ilişkin kayıtlar yok edilir. Burada da aslında yukarıda incelediğimiz *“işleme amacıyla bağlantılı, sınırlı ve ölçülü olma”* ve *“mevzuatta öngörülen veya işlendikleri amaçla bağlantılı olan süre kadar muhafaza edilme”* ilkeleriyle bir paralellik mevcuttur. Özel iletişime müdahale edilmesinin gizli yürütülen bir işlem olmasından mütevellit, işlemde hukuka aykırılık olduğu takdirde bunun açığa çıkması zordur<sup>631</sup>. Bu nedenle anılan sürecin titizlikle yürütülmesi, kişilerin haberleşme ve özel hayatın gizliliği hakkı ile kişisel verilerinin korunması hakkına büyük derecede önem gösterilmesi gereklidir.

Gizli soruşturmacı görevlendirmesi CMK'nın 139. vd. maddelerde düzenlenmiştir. Söz konusu madde gereğince gizli soruşturmacı, soruşturma çerçevesinde kişilerin birtakım

---

<sup>629</sup> Can, s. 226.

<sup>630</sup> Küzeci, Kişisel Verilerin Korunması, s. 423.

<sup>631</sup> Küzeci, Kişisel Verilerin Korunması, s. 426.

kişisel verilerine erişilebilir. Bu bilgilerin de soruşturma ile bağlantılı bir şekilde kullanılması gereklidir. Nitekim 139. maddenin 6. fıkrasına göre “*Soruşturmacı görevlendirilmesi suretiyle elde edilen kişisel bilgiler, görevlendirildiği ceza soruşturması ve kovuşturması dışında kullanılamaz. Suçla bağlantılı olmayan kişisel bilgiler derhâl yok edilir.*” Dolayısıyla suçla bağlantılı olmayan kişisel verilerin imha edilmesi ve suçla bağlantılı olanların da yalnızca ceza soruşturması ve kovuşturması için kullanılması KVKK’nın ilkeleriyle de örtüşmektedir.

### **6.3. KVKK’nın Cezaların İnfaz İşlemleriyle İlişkisi**

Son olarak cezaların infaz işlemlerinde de kişisel verilerin korunmasına yönelik düzenlemelerin son derece önemli olduğunu söylemek gerekir. Nitekim adli sicil kayıtlarının tutulması, parmak izi alınması, elektronik izleme, hükümlünün iletişiminin denetlenmesi ve seyirden yasaklama işlemlerinde KVKK kapsamında özel nitelikli kabul edilen bilgilerin devlet eliyle işlenmesi söz konusu olmaktadır.

Adli sicil kayıtları, Adli Sicil Kanunu’nun 2. maddesi uyarınca Adalet Bakanlığı Adli Sicil ve İstatistik Genel Müdürlüğündeki Adli Sicil’de tutulmaktadır. Adli sicile kayıtlı bilgiler kişilerin mahrem derecesindeki bilgilerdir<sup>632</sup>. Bu anlamda söz konusu kişisel verilerin son derece titizlikle korunması gerekir.

Kişilerin adli sicil kayıtları cezanın veya güvenlik tedbirinin infazının tamamlanması, ceza mahkûmiyetini bütün sonuçlarıyla ortadan kaldıran şikâyetten vazgeçilmesi veya etkin pişmanlık durumu, ceza zamanaşımının dolması, genel af durumlarında silinerek arşiv kaydına alınır. Kişinin ölümü halindeyse tamamen silinir. Belirtmek gerekir ki 2011 yılına kadar, bu kayıtların kişinin ölümü halinde ve herhalde seksen yıl süreyle saklanması öngörülüyordu. AYM 2011 yılında vermiş olduğu kararda “... *kişinin belli bir tarihte aldığı herhangi bir mahkûmiyet kararına ilişkin kaydın kişinin ölümüne kadar ya da seksen yıl süreyle muhafaza edilmesi, Anayasa'nın 5. ve 17. maddelerinde belirtilen kişinin maddi ve manevi varlığının geliştirilmesi ilkesi ve cezaların ıslah edici olma amacı*

---

<sup>632</sup> Adli sicile kaydedilecek bilgiler için bkz.: Adli Sicil Kanunu’nun 4. maddesi.

ile bağdaşmamaktadır.” ifadelerine yer vererek hükmü iptal etmiştir<sup>633</sup>. Bu anlamıyla KVKK’nın genel ilkelerindeki “işleme amacıyla bağlantılı, sınırlı ve ölçülü olma” ilkesiyle bir paralellik bulunduğu görülmektedir. Diğer yandan Adli Sicil Kanunu’nda yer alan a) kullanım amacı belirtilerek kimlere verileceğine yönelik düzenleme<sup>634</sup>, b) 18 yaşını doldurmamış kişilere ait adli sicil kayıtlarının ancak soruşturma ve kovuşturma kapsamında değerlendirilmek üzere Cumhuriyet başsavcılıkları, hâkim veya mahkemelerce istenebileceği<sup>635</sup> düzenlemesi de kişisel verilerin önemini vurgulamakta ve ilgilisi haricinde kimseye verilmemesini öngörmektedir.

Diğer yandan CGİK’in 21. maddesinin 3. fıkrası uyarınca ceza infaz kurumuna gelen hükümlülerin tanısı için parmak ve avuç içi izleri, fotoğrafları, kan grupları, vücutlarının dış özellikleri ve ölçüleri işlenmektedir. Burada hükümlünün tanısına yalnızca parmak izinin alınması yetebilecekken diğer bilgilerin de alınmasının<sup>636</sup> KVKK’daki “işleme amacıyla bağlantılı, sınırlı ve ölçülü olma” ilkesiyle bağdaşmadığını belirtmek gerekir. Ayrıca kişinin ceza infaz kurumundan ayrılması halinde bu bilgilerin ne olacağına ilişkin de herhangi bir hüküm bulunmamaktadır<sup>637</sup>. Bu doğrultuda anılan durumun “belirli, açık ve meşru amaçlar için işleme” ve “mevzuatta öngörülen veya işleme amacıyla orantılı süre kadar muhafaza edilme” ilkesiyle de örtüşmediğini belirtmek mümkündür. Dolayısıyla, anayasal düzlemde tanınmış bir hakka konu kişisel verilerin bu şekilde belirsizlik içerisinde işlenmesi hukuk devleti ilkesiyle bağdaşmamaktadır. Kişinin ceza infaz kurumundan ayrılması halinde bilgilerin akıbeti noktasında bir belirliliğin olması gerekirdi.

Kişisel verilerin ceza infaz işlemlerinde işlenmesine bir örnek de elektronik izlemedir. Elektronik izlemeye Türkiye’de ilk kez 2012 yılında “Elektronik İzleme Sistemine Geçişte Denetimli Serbestlik Hizmetlerinin Kurumsal Kapasitesinin Güçlendirilmesi Avrupa Birliği Eşleştirme Projesi”nde başvurulmuştur<sup>638</sup>. Türk hukukunda 5402 sayılı

---

<sup>633</sup> AYM’nin 2008/44 E., 2011/21 K. sayılı ve 20.01.2011 tarihli kararına erişim için bkz.: <https://normkararlarbilgibankasi.anayasa.gov.tr/Dosyalar/Kararlar/KararPDF/2011-21-nrm.pdf>, erişim tarihi: 29.09.2021.

<sup>634</sup> Adli Sicil Kanunu’nun 7. maddesi.

<sup>635</sup> Adli Sicil Kanunu’nun 10. maddesinin 3. fıkrası.

<sup>636</sup> **Can**, s. 256.

<sup>637</sup> **Can**, s. 256.

<sup>638</sup> **Can**, s. 259.



Denetimli Serbestlik Hizmetleri Kanunu'nun<sup>639</sup> 15. maddesine göre şüpheli, sanık ve hükümlülerin toplum içinde izlenmesi, gözetimi ve denetimi elektronik cihazlar vasıtasıyla kişinin rızası alınarak gerçekleştirilebilir. İzlemeye ilişkin kayıtlarının ne kadar süreyle muhafaza edileceğine yönelik herhangi bir hüküm bulunmamaktadır. Bu doğrultuda kanaatimizce “*mevzuatta öngörülen veya işleme amacıyla orantılı süre kadar muhafaza edilme*” ilkesine paralel bir şekilde izlemenin bitmesiyle kişisel verilerin imha edilmesi gerekmektedir.

Ceza infaz süreçlerinde hükümlülerin iletişiminin denetlenmesi yoluyla kişisel verilerin işlenmesi sürecinde de KVKK kapsamında değerlendirme yapılması mümkündür. CGİK'in 66. maddesinin 1. fıkrası uyarınca kapalı ceza infaz kurumlarındaki hükümlülerin yapacağı telefon görüşmeleri idarece dinlenmekte ve kayda alınmaktadır. Ancak bu kayıtların ne kadar süreyle muhafaza edileceği veya bu kayıtlara kimlerin erişebileceğine yönelik herhangi bir düzenleme bulunmamaktadır<sup>640</sup>. Diğer yandan, CGİK'in 68. maddesi uyarınca hükümlülerin alıcı ve gönderici olduğu mektup, faks ve telgrafların okunacağı ve kaydedileceği hükme bağlanmıştır. Son yıllarda mektupların taranarak Ulusal Yargı Ağı Platformu'na (UYAP) kaydedilmesi yönünde bir uygulama başlatılmıştır<sup>641</sup>. Uygulamanın Anayasa'nın 20. maddesine aykırı olduğu gerekçesiyle başvuruda bulunulsa da AYM “... 6698 sayılı Kanun gereğince kişisel verilerinin ilgilinin rızası dışında kaydedilememesi kural olarak kabul edilmiş ise de kamu güvenliği gibi bazı istisnai hâllerde kişinin rızası hilafına verilerin kaydedilebileceği belirtilmiştir. İnfaz kurumları da kamu güvenliği kapsamında infaz kurumunda güvenliğin sağlanması ve suç işlenmesinin önlenmesi amacıyla mahkumların yazışmalarını denetlerken yazışma hakkında birtakım idari ve yargısal işlemler yapılacağından ilgili yazışmanın diğer bilgiler gibi UYAP sistemine kaydedilmesi olağandır.” ifadeleriyle başvuruyu reddetmiştir<sup>642</sup>. Burada AYM'nin kararına katılmadığımızı belirtmek isteriz. Nitekim karşı oy gerekçesinde de ifade edildiği üzere söz konusu müdahalenin hukuka uygun olabilmesi için müdahalenin demokratik bir toplumda gerekli ve ölçülü olması, müdahaleyle ulaşılmak istenilen amaçla müdahale yöntemi arasında bir dengenin

<sup>639</sup> 20.07.2005 tarihli ve 25881 sayılı Resmî Gazete'de yayımlanan 5402 sayılı Denetimli Serbestlik Hizmetleri Kanunu.

<sup>640</sup> **Can**, s. 262.

<sup>641</sup> **Can**, s. 262.

<sup>642</sup> AYM'nin 2017/24776 başvuru numaralı ve 24.05.2018 tarihli kararı, erişim için bkz.: <https://kararlarbilgibankasi.anayasa.gov.tr/BB/2017/24776>, erişim tarihi: 29.09.2021.

bulunması gerekmektedir. Diğer yandan somut olayda yazışmaların ne kadar süreyle muhafaza edileceği ve bu kayıtlara kimlerin erişebileceğinin de belirsiz olması müdahalenin keyfi ve sınırlandırılmamış olduğunu göstermektedir.

Cezaların infaz işlemlerinin KVKK ile ilişkisinde ele alınacak bir diğer konu, seyirden yasaklanmadır. Spor müsabakalarını seyirden yasaklanma idari tedbir (m. 18/7), koruma tedbiri (m. 18/3) ve bir güvenlik tedbiri (m. 18/1) olarak 6222 sayılı Sporda Şiddet ve Düzensizliğin Önlenmesi Kanunu'nda<sup>643</sup> düzenlenmiştir<sup>644</sup>. 6222 sayılı Kanun'un 18. maddesinin 4. fıkrasına göre, "*Koruma tedbiri olarak uygulanan ve güvenlik tedbiri olarak hükmedilen spor müsabakalarını seyirden yasaklama tedbirine ilişkin bilgiler Emniyet Genel Müdürlüğü bünyesinde tutulan bu amaca özgü elektronik bilgi bankasına derhal kaydedilir. Bu bilgi bankasına spor kulüplerinin ve federasyonların erişimi sağlanır. Yasaklanan kişilere ilişkin bilgiler, ilgili spor kulüplerine ve yurt dışında yapılacak müsabaka öncesinde müsabakanın yapılacağı ülkenin yetkili mercilerine bildirilir.*" Görüleceği üzere hakkında tedbir uygulanan kişilerin bilgileri bilgi bankasına kaydedilecek ve bu bilgilere spor kulüpleri ile federasyonlar erişebilecektir. Buna ek olarak bilgiler yurt dışındaki yetkili mercilere aktarılacaktır. Bir sonraki başlıkta detaylıca inceleneceği üzere, KVKK'nın 9. maddesi gereğince kişisel verilerin yurt dışına aktarılabilmesi için birtakım şartların sağlanması gerekmektedir. Bu şartlardan bir tanesi de kişisel verilerin aktarılacağı yabancı ülkede yeterli korumanın bulunmasıdır. 6222 sayılı Kanun'da, KVKK'nın aradığı yeterli koruma düzeyine ilişkin olarak herhangi bir bilgi verilmemektedir<sup>645</sup>. Kanaatimce kişisel verilerin aktarılacağı yabancı ülkenin kişisel verilerin korunması alanında yeterli koruma düzeyine sahip olup olmadığının araştırılması gerekmektedir.

Diğer yandan, bilgi bankasında hangi kişisel verilerin yer alacağı 6222 sayılı Kanun'da belirlenmemiştir. Seyirden yasaklanmaya yönelik bazı durumlar ise Sporda Şiddet ve

---

<sup>643</sup> 14.04.2011 tarihli ve 27905 sayılı Resmî Gazete'de yayımlanan 6222 sayılı Sporda Şiddet ve Düzensizliğin Önlenmesi Hakkında Kanun. Çalışmanın devamında "6222 sayılı Kanun" olarak isimlendirilecektir. Erişim için bkz.: <https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6222.pdf>, erişim tarihi: 29.09.2021.

<sup>644</sup> **Altunbaş**, Aysun / **Ataç**, Asiye Selcen, "6222 Sayılı Kanun Kapsamında Seyirden Yasaklama (m. 18)", Marmara Üniversitesi Hukuk Fakültesi Dergisi, Cilt: 16, Sayı: 1-2, Haziran – Temmuz 2017, ss. 69-109, s. 73.

<sup>645</sup> **Can**, s. 263.

Düzensizliğin Önlenmesine Dair Kanunun Uygulanmasına İlişkin Yönetmelik'te<sup>646</sup> yer almaktadır. İlgili yönetmeliğin 7. maddesinin c bendinde seyirden yasaklanma tedbiri uygulanan kişinin fotoğrafının alınacağı belirtilmiştir. Ayrıca 6222 sayılı Kanun'da ve ilgili yönetmelikte seyirden yasaklamanın sürelerine yer verilirken bilgilerin saklama sürelerine ilişkin herhangi bir bilgi yer almamaktadır. Bu durumda KVKK'nın *“mevzuatta öngörülen veya işleme amacıyla orantılı süre kadar muhafaza edilme”* ilkesi gereğince seyirden yasaklama tedbirinin süreleri baz alınarak işleme amacıyla orantılı makul bir süre belirlenmesi gerekmektedir.

Bunlara ek olarak, 6222 sayılı Kanun'un 18. maddesinin 8. fıkrasında seyirden yasaklanan kişinin taraftarı olduğu takımın müsabakasının yurt içinde yapıldığı durumlarda müsabakanın başlangıç saatinde ve bundan bir saat sonra kolluk birimine başvuracağı, bunun takibinin ise biyometrik yöntemler kullanılarak gerçekleştirilebileceği belirtilmiştir. Ancak yine, biyometrik verinin nasıl işleneceği ve ne kadar süre ile muhafaza edileceğine yönelik herhangi bir düzenleme bulunmamaktadır. Kişinin en mahrem bilgilerinin arasında yer alan biyometrik verisinin bu şekilde alelade bir düzenlemeyle işlenebileceğinin hükme bağlanması doğru olmamıştır.

## **7. KVKK AÇISINDAN SUÇLULARIN İADESİNE İLİŞKİN DÜZENLEMELER**

Suçluların iadesine ilişkin düzenlemeler özü itibarıyla kişisel verilerin işlenmesine yönelik bir hukuka uygunluk nedeni oluşturmaktadır. Nitekim bu düzenlemelerde suçluya ait birtakım bilgi ve belgelerin, dolayısıyla suçluya ait kişisel verilerin başka kişilere/kurumlara aktarılması gündeme gelmektedir. Eğer ki bu aktarım önleyici, koruyucu ve istihbari faaliyetler kapsamında gerçekleşiyorsa veya bir soruşturma, kovuşturma, yargılama ve infaz işlemine yönelikse zaten hali hazırda KVKK'nın 28. maddesinin 1. fıkrasının d ve ç bentleri uyarınca bir tam istisna durumu söz konusu olacaktır. Ancak bunun dışındaki durumlar için kişisel verilerin aktarımına yönelik düzenlemelerin incelenmesi gerekmektedir.

---

<sup>646</sup> 22.12.2012 tarihli ve 28595 sayılı Resmî Gazete'de yayımlanan Sporda Şiddet ve Düzensizliğin Önlenmesine Dair Kanunun Uygulanmasına İlişkin Yönetmelik.

Kişisel verilerin aktarımı, kişisel verilerin işleme türleri arasında yer almakta olup; yurt içi ve yurt dışı veri aktarımı olarak KVKK'da diğer veri işleme türlerinden ayrıca düzenlenmiştir<sup>647</sup>. KVKK'nın 8. maddesinde kişisel verilerin yurt içi aktarımına ilişkin kurallar düzenlenmiştir. Burada yer alan düzenlemenin veri işleme şartları ile aynı olduğunu ifade etmek mümkündür.

KVKK'nın 9. maddesinde ise kişisel verilerin yurt dışına aktarımı düzenlenmiştir. Maddenin 1. fıkrasına göre kişisel verilerin ilgili kişinin açık rızası bulunmaksızın yurt dışına aktarılması yasaktır. Ancak veri işleme şartlarının varlığı halinde ve kişisel verinin aktarılacağı yabancı ülkede a) yeterli korumanın bulunması, yeterli korumanın bulunmadığı durumda ise b) Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kişisel Verileri Koruma Kurulu'nun izninin bulunması halinde kişisel veriler yurt dışına aktarılabilir. Taahhütnamede asgari olarak yer alması gereken hususlar Kişisel Verileri Koruma Kurulu tarafından belirlenmiş ve internet sitesinde yayınlanmıştır<sup>648</sup>. Madde metninde yer alan "yeterli" ifadesinin, 95/46/EC sayılı Direktif'in 25 ve 25. maddelerinde yer alan "adequate" ifadesinin karşılığı olduğu düşünülmektedir<sup>649</sup>.

Diğer yandan, maddenin 3. fıkrasında yeterli korumanın bulunduğu ülkelerin Kişisel Verileri Koruma Kurulu tarafından belirlenerek ilan edileceği hüküm altına alınmıştır. Gerek yeterli korumanın bulunup bulunmadığına karar verilirken gerekse yurt dışına kişisel veri aktarımına izin verilirken maddenin 4. fıkrasındaki kriterler uygulanacaktır. Buna göre; "a) Türkiye'nin taraf olduğu uluslararası sözleşmeler, b) Kişisel veri talep eden ülke ile Türkiye arasında veri aktarımına ilişkin karşılıklılık durumu, c) Her somut kişisel veri aktarımına ilişkin olarak, kişisel verinin niteliği ile işleme amaç ve süresi, ç) Kişisel verinin aktarılacağı ülkenin konuyla ilgili mevzuat ve uygulaması, d) Kişisel verinin aktarılacağı ülkede bulunan veri sorumlusu tarafından taahhüt edilen önlemler değerlendirilecek ve ihtiyaç duyulması halinde ilgili kurum ve kuruluşların görüşü alınacaktır." Diğer yandan Kişisel Verileri Koruma Kurulu 2019 yılında vermiş olduğu bir kararla yeterli korumanın bulunduğu ülkelerin tayininde kullanılmak üzere

<sup>647</sup> **Küzeci**, Kişisel Verilerin Korunması, s. 354.

<sup>648</sup> İlgili taahhütnamelere erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/5255/Taahhutnameler>, erişim tarihi: 18.09.2021.

<sup>649</sup> **Küzeci**, Kişisel Verilerin Korunması, s. 356.

oluşturulan formu yayınlamış, bu doğrultuda karşılıklılık durumunun, ilgili ülkenin kişisel verilerin işlenmesine yönelik mevzuatın, mevzuatın uygulanmasının, bağımsız veri koruma otoritesinin bulunmasının, kişisel verilerin korunması alanıyla ilgili uluslararası antlaşmalara taraf olma ile uluslararası kuruluşlara üye olma durumunun, Türkiye'nin üye olduğu küresel ve bölgesel örgütlere üye olma durumunun ve ilgili ülke ile yürütülen ticaret hacminin yeterli korumaya sahip ülkelerin belirlenmesinde esas alınacak kriterler olduğunu belirtmiştir<sup>650</sup>.

İlgili maddenin 5. fıkrasında kişisel verilerin, uluslararası sözleşme hükümleri saklı kalmak üzere, Türkiye'nin veya ilgili kişinin menfaatinin ciddi bir şekilde zarar göreceği durumlarda, ancak ilgili kamu kurum veya kuruluşunun görüşünün alınarak Kurul'un izniyle yurt dışına aktarılacağı hüküm altına alınmıştır. Bu anlamda uluslararası sözleşme hükümlerinin saklı kalmasından, suçluların iadesine ilişkin sözleşmeler açısından da kişisel verilerin yurt dışı aktarım koşullarına yönelik bir istisna getirildiğinden söz edilebilir. Örneğin; 6991 sayılı Türkiye Cumhuriyeti ile Sırbistan Cumhuriyeti Arasında Suçluların İadesine Dair Anlaşma<sup>651</sup> ve Anlaşmada Değişiklik Yapılmasına İlişkin Notaların Onaylanmasının Uygun Bulunduğu Hakkında Kanun<sup>652</sup> kapsamında İade Anlaşması uyarınca, her iki hukukuna göre alt sınırı bir yıl süreyle hürriyeti bağlayıcı nitelikte bir cezayı veya tutuklama emrini veya daha ağır bir cezayı gerektiren suçlar bakımından yapılacak iadelerde kişisel veri aktarımı bu madde kapsamında değerlendirilecektir. Diğer yandan 6991 sayılı Kanun uyarınca yapılacak kişisel veri aktarımlarında soruşturma, kovuşturma, yargılama ve infaz işlemlerine ilişkin bir veri işleme hali gündeme geldiğinden, buna bağlı olarak KVKK'dan tam istisna olma durumu da söz konusu olacaktır.

---

<sup>650</sup> Kişisel Verileri Koruma Kurulu'nun 02.05.2019 tarihli ve 2019/125 sayılı kararına erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/5469/-Yeterli-korumanin-bulundugu-ulkelerin-tayininde-kullanilmak-uzere-olusturulan-form-hakkindaki-02-05-2019-tarihli-ve-2019-125-sayili-Kurul-Karari>, erişim tarihi: 19.09.2021.

<sup>651</sup> Çalışmanın devamında “İade Anlaşması” olarak isimlendirilecektir. İade anlaşmasının metnine erişim için bkz.: <https://diabgm.adalet.gov.tr/Resimler/Dokuman/30112020152637S%C4%B1rbistan%20iade%20anla%C5%9Fmas%C4%B1%20son..pdf>, erişim tarihi: 26.09.2021.

<sup>652</sup> 04.04.2017 tarihli ve 30028 sayılı Resmî Gazete'de yayımlanan 6991 sayılı Türkiye Cumhuriyeti ile Sırbistan Cumhuriyeti Arasında Suçluların İadesine Dair Anlaşma ve Anlaşmada Değişiklik Yapılmasına İlişkin Notaların Onaylanmasının Uygun Bulunduğu Hakkında Kanun. Çalışmanın devamında “6991 sayılı Kanun” olarak isimlendirilecektir.

Esasen KVKK'nın 9. maddesinin 5. Fıkrasındaki hüküm önceki tasarılarla TBMM'ye gönderilen metinde ve Adalet Komisyonu'ndaki görüşmelerde gündeme gelmemiş; Genel Kurul'a sunulan bir önerge sonrasında kabul edilmiştir<sup>653</sup>. Ancak Türkiye'nin veya ilgili kişinin menfaatinin ciddi bir şekilde zarar göreceği durumların saptanması, hangi durumların ciddi zarara neden olacağı, aktarıma izin verilecek bir alanda anılan hükmün uygulama alanının nasıl olacağı, her bir yurt dışına veri aktarımında bu değerlendirmenin yapılıp yapılmayacağı, görüşü alınacak ilgili kamu kurum veya kuruluşunun nasıl belirleneceği, konuyu ilgilendiren birden fazla kamu kurum veya kuruluşu mevcutsa nasıl bir yol izleneceği gibi konuların yeterince açık olmaması nedeniyle bu hükmün uygulanmasının uygulamada belirsizlikler yaratacağı aşikardır<sup>654</sup>.

Son olarak, ilgili maddenin 6. fıkrasında kişisel verilerin yurt dışına aktarılmasına ilişkin diğer kanunlarda yer alan hükümler saklı tutulmuştur. Örnek olarak 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun'un<sup>655</sup> ilgili hükümleri verilebilir<sup>656</sup>.

## **8. KİŞİSEL VERİLERİN KORUNMASIYLA İLGİLİ TCK'DA YER ALAN SUÇLAR**

TCK'nın 135 vd. maddelerinde kişisel verilerin korunmasıyla ilgili suçlar düzenlenmiştir. Esasen bu çalışmanın konusu, 136. maddede düzenlenen verileri hukuka aykırı olarak verme veya ele geçirme suçu ile 137. maddede düzenlenen nitelikli hallerdir. Ancak suç incelemesine geçmeden hemen önce 135. maddede düzenlenen kişisel verilerin kaydedilmesi suçu ile 138. maddede düzenlenen verileri yok etme suçu hakkında genel bilgilere yer verilmesinin isabetli olacağı düşünülmüştür.

<sup>653</sup> Küzeci, Kişisel Verilerin Korunması, s. 356.

<sup>654</sup> Küzeci, Kişisel Verilerin Korunması, s. 356.

<sup>655</sup> 18.10.2006 tarihli ve 26323 sayılı Resmî Gazete'de yayımlanan 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun.

<sup>656</sup> Küzeci, Kişisel Verilerin Korunması, s. 356.

## 8.1. Kişisel Verilerin Kaydedilmesi Suçu (m. 135)

Kişisel verilerin kaydedilmesi suçu, TCK'nın 135. maddesinde düzenlenmiştir. Buna göre;

*“Madde 135- (1) Hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir.*

*(2) Kişisel verinin, kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması durumunda birinci fıkraya uyarınca verilecek ceza yarı oranında artırılır.”*

Esasen madde metninin şu anki hali, ilk haline göre oldukça farklıdır. Bunun nedeni kişisel verilerin korunması alanının ülkemizde geçirdiği gelişim sürecidir. Kişisel verilerin kaydedilmesine önceki düzenlemede altı aydan üç yıla kadar hapis cezası verilmesi öngörülürken, yeni düzenlemede bir yıldan üç yıla kadar hapis cezasının verilmesi öngörülmüştür. Diğer yandan suçun nitelikli halinin düzenlendiği 2. fıkrada daha önceki düzenlemede kişilerin siyasi, felsefi veya dini görüşleri, ırki kökenleri, ahlaki eğilimleri, cinsel yaşamları ifadeleri bulunurken, yeni düzenlemede KVKK'ya paralel şekilde özel nitelikli kişisel verilerin eklendiği görülmektedir. Ancak yine de KVKK'da yer alan özel nitelikli kişisel verilerin tamamının 2. fıkraya eklenmemesi bir eksiklik olarak görülmektedir<sup>657</sup>.

Madde metninin gerekçesinde, kişilerle ilgili bilgilerin bilgisayar ortamlarına geçirilip muhafaza edilmesi uygulamasının çeşitli kurum ve kuruluşlar tarafından yapıldığı, bu bilgilerin amacı dışında kullanılmasından veya herhangi bir şekilde üçüncü şahısların eline geçerek hukuka aykırı olarak yararlanılmasından dolayı hakkında bilgi toplanan kişilerin büyük zararlara uğrayabildiği belirtilmiştir. Bu suçun en çok işlendiği yer bilişim alanı olmasına karşın, bu suç yalnızca bilişim alanıyla sınırlı değildir<sup>658</sup>. Nitekim gerekçenin devamında suç tanımında kişisel verilerin bilgisayar ortamında veya kâğıt üzerinde kayda alınması arasında bir ayrım bulunmadığı belirtilmiştir. Diğer yandan,

<sup>657</sup> **Küzeci**, Kişisel Verilerin Korunması, s. 409; **Dülger**, Kişisel Verilerin Korunması, s. 700; **Göçmen Uyarer**, s. 187.

<sup>658</sup> **Karagülmez**, Ali, *Bilişim Suçları ve Soruşturma – Kovuşturma Evreleri*, Seçkin Yayıncılık, Genişletilmiş ve Gözden Geçirilmiş 5. Baskı, Ankara, Temmuz 2014, s. 447.

suçun oluşabilmesi açısından kişisel verilerin sistemli bir şekilde kaydedilmesi de şart değildir, kişisel veriler herhangi bir şekilde kaydedilebilir<sup>659</sup>. Son olarak, suçun oluşması açısından söz konusu kişisel verilerin başkasının kullanıma açılması veya yayınlanması da şart değildir<sup>660</sup>. Bu nedenle yalnızca kişisel verilerin kaydedilmesi, suçun oluşması için yeterlidir, ayrıca aleniyete açılması gerekmemektedir<sup>661</sup>.

## 8.2. Verileri Yok Etmeme Suçu (m. 138)

Verileri yok etmeme suçu, TCK'nın 138. maddesinde düzenlenmiştir. Buna göre;

*“Madde 138- (1) Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde bir yıldan iki yıla kadar hapis cezası verilir.*

*(2) (Ek: 21/2/2014-6526/5 md.) Suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması hâlinde verilecek ceza bir kat artırılır.”*

Görüleceği üzere bu madde ile amaçlanan esasen verilerin saklanması için gerekli sebepler ortadan kalktıktan sonra bu verilerin imha edilmesi, verilere erişimin engellenmesi, insanların kendilerini güvende hissedecekleri bir ortam yaratılmasıdır<sup>662</sup>. Nitekim verilerin sürekli olarak sistemde bulunması, insanlarda sürekli olarak izlendiği duygusu yaratır ki bu durum güvensizlik ve nefret duygusunu da tetikler<sup>663</sup>. Diğer yandan gereksinim duyulmayan verilerin imha edilmesi, keyfi uygulamaların da önüne geçmek için gereklidir<sup>664</sup>. Bunun yanında verilerin süresiz bir şekilde tutulmaması, “*kişisel verilerin işlendikleri amaçla bağlantılı olması*” ilkesinin de bir gereğidir<sup>665</sup>. Nitekim muhafaza etme bir veri işlemidir. Ancak diğer yandan, madde metninde *suçun oluşması için kanunların belirlediği sürelerin geçmiş olmasının* aranması, verinin *toplanma*

<sup>659</sup> Küzeci, Kişisel Verilerin Korunması, s. 409.

<sup>660</sup> Dülger, Kişisel Verilerin Korunması, s. 699.

<sup>661</sup> Karagülmez, s. 448.

<sup>662</sup> Göçmen Uyarer, s. 237.

<sup>663</sup> Dülger, Kişisel Verilerin Korunması, s. 752.

<sup>664</sup> Küzeci, Kişisel Verilerin Korunması, s. 411.

<sup>665</sup> Küzeci, Kişisel Verilerin Korunması, s. 411.



*amacının* ortadan kalkması halinde de muhafaza edilebileceği anlamı taşımaktadır ki bu durum söz konusu ilkeye aykırılık olarak değerlendirilebilir<sup>666</sup>.

Suçun oluşması için öncelikle failin herhangi bir hukukî düzenlemeden kaynaklı “*veriyi yok etme*” yükümlülüğünün bulunması, sonrasında ise failin bu düzenlemede yer alan verinin saklanması süresini geçirmiş olması gerekmektedir<sup>667</sup>. Bu yönüyle verileri yok etmeme suçu, KVKK’nın genel ilkelerinden birisi olan “*mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme*” ilkesi ile de yakından ilgilidir. Ancak farklılık olarak, verileri yok etmeme suçunda sistem içerisindeki verilerin yok edilmesi ele alınmıştır. Sistem ifadesi bilişim suçları açısından bilişim sistemini ifade ederken, bilişim dışındaki alanlarda farklı yorumlanabilir<sup>668</sup>. Sistem ifadesinden yalnızca bilişim sistemlerinin değil, bunun yanında bilişim sistemi haricinde kişisel verilerin tutulduğu yerlerin de anlaşılması gerektiği kanaatindeyiz<sup>669</sup>. Nitekim kişiler verilerin işlenmesine yönelik usul ve esasları düzenleyen KVKK’nın, kişisel olmayan verileri yok etmeme suçuna yönelik göndermede bulunması düşünülemez.

Kişisel verilerin imha edilmesine yönelik olarak KVKK’nın 17. maddesinin 2. fıkrasında “*Bu Kanunun 7 nci maddesi hükmüne aykırı olarak; kişisel verileri silmeyen veya anonim hâle getirmeyenler 5237 sayılı Kanunun 138 inci maddesine göre cezalandırılır.*” hükmü yer almaktadır. KVKK’nın 7. maddesi ise şöyle düzenlenmiştir:

*“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.”*

KVKK’nın 7. maddesinde bulunan “*yok etme*” ifadesinin 17. maddenin 2. fıkrasında kullanılmadığı görülmektedir. Böylelikle kişisel verileri yok etmeyen kişiler hakkında TCK’nın 138. maddesinin uygulanıp uygulanmayacağı sorusu akla gelmektedir<sup>670</sup>. Ancak bu durumun yasa koyucunun kanun yapış tekniğinden kaynaklı bir hatasının sonucu olduğunu düşünmekteyiz.

<sup>666</sup> **Küzeci**, *Kişisel Verilerin Korunması*, s. 411.

<sup>667</sup> **Dülger**, *Kişisel Verilerin Korunması*, s. 756.

<sup>668</sup> **Karagülmez**, s. 470.

<sup>669</sup> Aynı yönde görüş için bkz.: **Karagülmez**, s. 470. Aksi yönde görüş için bkz.: **Göçmen Uyarer**, s. 240. *Yazara* göre bu ifade son derece açık olup doğrudan bilişim sistemlerine gönderme yapılmaktadır.

<sup>670</sup> **Küzeci**, *Kişisel Verilerin Korunması*, s. 412;

### III. BÖLÜM: VERİLERİ HUKUKA AYKIRI OLARAK VERME VEYA ELE GEÇİRME SUÇU (TCK m. 136) VE NİTELİKLİ HALİ (TCK m. 137)

#### 1. GENEL OLARAK

##### 1.1. Suç Hakkında Genel Değerlendirmeler

Verileri hukuka aykırı olarak verme veya ele geçirme suçu ve nitelikli hali TCK'nın 136 ve 137. maddelerinde düzenlenmiştir. Suç tipi ile ilgili genel bilgilere yer verilmeden önce, çalışmanın konusu olarak neden bu suç tipinin seçildiği ile ilgili açıklama yapılmasının yerinde olacağı kanaatindeyiz. Esasen, TCK'nın 135 vd. maddelerinde yer alan düzenlemelerin hepsi KVKK anlamında birer veri işleme niteliğindedir. Ancak “*kişisel verilerin aktarılması*” kavramı diğer veri işleme türlerinin aksine KVKK'nın 8. ve 9. maddesinde ayrıca ele alınmıştır<sup>671</sup>. Bu nedenle “*kişisel verilerin aktarılması, açıklanması, elde edilmesi*” veri işleme türlerine benzeyen<sup>672</sup> TCK'nın 136. maddesinde düzenlenen suç tipinin diğer suç tiplerinden ayrı bir şekilde ele alınması gerektiği düşünülmüş, bu sebeple çalışmada TCK'nın 136. maddesindeki suç tipi incelenmek istenmiştir.

Burada aktarım ile ilgili açıklığa kavuşturulması gereken ve ayrıca önemli gördüğümüz bir konunun da belirtilmesinde fayda vardır. Şöyle ki; kişisel verilerin işlenmesi sürecini gerçekleştiren üçüncü kişilere yapılan aktarımların hangi nitelikte olacağını yanıtı KVKK'da net olarak yer almamaktadır. Veri güvenliğine ilişkin yükümlülüklerin düzenlendiği KVKK'nın 12. maddesinin 2. fıkrasına göre “*Veri sorumlusu, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, birinci fıkrafta belirtilen tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumludur.*” Dolayısıyla veri sorumlusu, bu sıfatını kaybetmeden kişisel verilerin

<sup>671</sup> **Küzeci**, Kişisel Verilerin Korunması, s. 354.

<sup>672</sup> Esasen burada kişisel verilerin “aktarılması”, “açıklanması” ve “elde edilmesi” davranışlarının kişisel verilerin “verilmesi”, “yayılması” ve “ele geçirilmesi” davranışlarına benzerliği vurgulanmak istenmiştir. Ancak bu durum “suçların ve cezaların belirliliği ilkesi” açısından herhangi bir riskin bulunmadığı anlamına gelmemelidir. “*Suçların ve cezaların belirliliği ilkesi*” yorumu açısından ayrıca bkz.: **Küzeci**, Kişisel Verilerin Korunması, s. 411.

işlenmesi sürecini üçüncü kişilere gördürebilir<sup>673</sup>. Ancak bu durumda veri sorumlusundan veri işleyene yapılan aktarımların KVKK'nın 8. maddesi kapsamında değerlendirilip değerlendirilemeyeceği hususu belirlenmemiştir. Söz konusu durumda iki muhtemel sonuç ortaya çıkmaktadır. Bu sonuçlardan ilki, veri sorumlusunun kişisel verileri yine kendi adına ve kendi talimatları ile sınırlı olmak kaydıyla veri işleme amacıyla üçüncü kişilere aktardığı durumlar KVKK'nın 8. maddesi kapsamında değerlendirilecektir. Bu durumda veri işleme şartlarının bulunmaması halinde hukuka uygun bir veri aktarımı yapılamayacaktır. Daha isabetli bulduğumuz ikinci bir sonuç ise, veri sorumlusu ile veri işleyen arasındaki aktarım KVKK'nın 8. maddesinden muaf bir şekilde değerlendirilecektir<sup>674</sup>. Bu durumda yapılan aktarımda veri işleme şartlarına bakılmayacaktır. İkinci sonucu destekleyecek bir şekilde, 95/46/EC sayılı Direktif'te ve GDPR'da üçüncü kişi, veri işleyen ile veri sorumlusunun dışında ayrıca tanımlanmıştır. Diğer bir ifade ile veri işleyen, üçüncü kişi niteliğini haiz değildir<sup>675</sup>. 29. Madde Çalışma Grubu'nun raporlarında da veri sorumlusundan veri işleyene aktarımın üçüncü kişilere aktarıma ilişkin getirilen kurallara tabi olmadığı belirtilmektedir<sup>676</sup>. Esasen KVKK'nın tasarısında “*üçüncü kişilere aktarım*” ifadesi yer almaktaysa da daha sonradan karışıklığa mahal vermemesi adına bu ifade madde metninden çıkarılmıştır<sup>677</sup>. Ancak bu ifadenin çıkarılmaması daha isabetli olacaktı. Özetlemek gerekirse, KVKK'daki aktarım şartlarının hangi koşullarda uygulanıp uygulanmayacağına yönelik acilen açık bir şekilde düzenleme yapılmasına ihtiyaç bulunmaktadır. Mevcut durumda veri sorumlusu ile veri işleyenler arasında yapılan aktarımlar KVKK'nın 8. maddesindeki şartlardan muaf tutulmalıdır. Ancak bu muafiyet, kişisel verilerin alelade bir şekilde aktarılmasının önünü

---

<sup>673</sup> Çekin, s. 106.

<sup>674</sup> Aynı yönde görüş için bkz.: Çekin, s. 107.

<sup>675</sup> Çekin, s. 107.

<sup>676</sup> 29. Madde Çalışma Grubu'nun 1/2010 sayılı görüş yazısında (on the concepts of “controller” and “processor”) veri kontrolörü (veri sorumlusu), veri işleyen ve çalışanlarının veri işlemenin iç çekirdeği kabul edildiğini ve üçüncü kişilere ilişkin özel hükümlerin burada uygulanmayacağını şu ifadelerle belirtmektedir: “Controller and processor and their staff are therefore considered as the -inner circle of data processing- and are not covered by special provisions on third parties.”, s. 6. İkinci ihtimali destekler nitelikte, veri işleyenin veri işleme sürecinin yasallığının veri kontrolörü (veri sorumlusu) tarafından verilen yetki ile gerçekleştiği şu ifadelerle belirtilmiştir: “The lawfulness of the processor's data processing activity is determined by the mandate given by the controller.”, s. 25, erişim için bkz.: [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf), erişim tarihi: 19.09.2021.

<sup>677</sup> Göçmen Uyarer, s. 140.

açmamalı, veri işleyen ile veri sorumluları arasında gizlilik ve güvenliğe ilişkin güçlü tedbirlerin alınmasını öngören sözleşmelerin akdedilmesi de zorunlu tutulmalıdır.

Kişisel verilerin aktarımına yönelik olarak holding, grup şirket, şirketler topluluğu gibi yapılanmaların akıbetinin de belirtilmesinde fayda vardır. Kişisel Verileri Koruma Kurulu vermiş olduğu bir kararda “Bir şirketler topluluğu bünyesinde yer alan birden çok veri sorumlusu şirketler arasında veri aktarımı gerçekleştirilmesinin, üçüncü kişiye veri aktarımı olarak değerlendirildiği, bu itibarla aynı şirketler topluluğu bünyesinde yer alan veri sorumluları arasında gerçekleşecek veri aktarımında da 6698 sayılı Kişisel Verilerin Korunması Kanununun 8 inci maddesi hükümlerinin esas alınması gerektiği dikkate alındığında her bir şirketin ayrıca veri sorumlusu olarak değerlendirileceği” ifadelerini kullanarak bu tür yapılanmaların kendi aralarında kişisel veri transferi yapmasını aktarım olarak değerlendirmiştir<sup>678</sup>.

Türk Ceza Kanunu’nun 136. maddesinin 1. fıkrasında kişisel verileri hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişinin iki yıldan dört yıla kadar hapis cezası ile cezalandırılacağı düzenlenmiştir. Maddenin 2. fıkrasında suç tipinin nitelikli hali öngörülmüş; suçun konusunun CMK’nın 236. maddesinin beşinci ve altıncı fıkraları uyarınca kayda alınan beyan ve görüntüler olması durumunda verilecek cezanın bir kat artırılacağı hüküm altına alınmıştır. Anılan düzenleme şu şekildedir:

***“Verileri hukuka aykırı olarak verme veya ele geçirme***

***Madde 136- (1) Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır.***

***(2) Suçun konusunun, Ceza Muhakemesi Kanununun 236 ncı maddesinin beşinci ve altıncı fıkraları uyarınca kayda alınan beyan ve görüntüler olması durumunda verilecek ceza bir kat artırılır.”***

Görüleceği üzere suçun oluşması için kişisel verilerin hukuka uygun olarak toplanıp toplanmadığına veya herhangi bir şekilde kaydedilip kaydedilmediğine bakılmaksızın söz konusu bilgilerin hukuka aykırı olarak verilmesi, yayılması veya ele geçirilmesi

<sup>678</sup> İlgili kararın numarası yayınlanmamıştır. Karar özetine erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/5410/Is-Basvurusu-Surecinde-Islenen-Kisisel-Verilerin-Hukuka-Aykiri-Sekilde-Paylasilmasi>, erişim tarihi: 18.09.2021.

önlenmek istenmiştir<sup>679</sup>. Nitekim maddenin gerekçesinde de “*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*” ifadelerine yer verilmiştir.

Madde başlığı, madde metni ve madde gerekçesi incelendiğinde birkaç uyumsuzluğun bulunduğu görülmektedir. Bu uyumsuzluklardan ilki, başlıkta “*veri*” ifadesinin, metinde ve gerekçede ise “*kişisel veri*” ifadesinin kullanılmasıdır. Veri ile kişisel veri ifadelerinin tanımları teknik anlamda birbirinden farklıdır. Kanun koyucunun verinin değil, kişisel verinin hukuka aykırı olarak verilmesini, yayılmasını veya ele geçirilmesini cezalandırdığı açıktır. Kanaatimce kişisel verilerin korunmasına özgülenmiş bir suçun başlığında “*veri*” yerine “*kişisel veri*” ifadesinin kullanılması, madde başlığı, metni ve gerekçesi arasındaki uyumun sağlanması bakımından daha doğru olacaktır<sup>680</sup>.

Diğer yandan madde metninde ve gerekçesinde “*yayma*” seçimlik hareketinin kullanılmasına karşın; madde başlığında bu ifadeye yer verilmemiştir. *Özbek*'e göre “*verme*”, “*yayma*”yı da kapsar nitelikte düşünülmüş; ancak daha sonradan oluşabilecek bir boşluğun önlenmesi için “*yayma*” ifadesi madde metnine dahil edilmiştir<sup>681</sup>. Sebep ne olursa olsun, madde başlığı, metni ve gerekçesi arasındaki uyumsuzluğun giderilmesi adına “*yayma*” seçimlik hareketinin madde başlığına eklenmesi isabetli olacaktır<sup>682</sup>. Her iki tutarsızlığın da kanun koyucunun kanun yapma tekniğinden kaynaklandığını düşünmekteyiz.

Yukarıda açıklanan sebeplerden dolayı, TCK'nın 136. maddesinde yer alan *verileri hukuka aykırı olarak verme veya ele geçirme* suçu için çalışmanın devamında hukuk tekniği açısından daha doğru görünen *kişisel verileri verme, yayma veya ele geçirme* ve *kişisel verilerin verilmesi, yayılması veya ele geçirilmesi* ifadeleri kullanılacaktır<sup>683</sup>.

<sup>679</sup> **Küzeci**, *Kişisel Verilerin Korunması*, s. 410; **Göçmen Uyarer**, s. 221.

<sup>680</sup> Aynı yönde bkz.: **Böreççi**, s. 56.

<sup>681</sup> **Özbek**, Veli Özer, *Yeni Türk Ceza Kanunu'nun Anlamı (TCK İzmir Şerhi)*, Madde 76-169, C: II, Ankara, 2008, s. 961; **Özbek**, Veli Özer / **Doğan**, Koray / **Bacaksız**, Pınar, *Türk Ceza Hukuku Özel Hükümler*, Seçkin Yayıncılık, Genişletilmiş ve Güncellenmiş 15. Baskı, Ankara 2020, (**Özbek / Doğan / Bacaksız**, *Özel Hükümler*), s. 597.

<sup>682</sup> Aynı yönde bkz.: **Korkmaz**, *Ceza Hukuku*, s. 118.

<sup>683</sup> “Hukuka aykırı olarak” ifadesinin de madde başlığında ve metninde kullanılmasını doğru bulmamakla birlikte, bu konuyla ilgili açıklamalar ve görüşler çalışmanın sistematigi açısından III. bölüm 8.1. başlığında ele alınmıştır.

Son olarak belirtmelidir ki, kişisel verilerin verilmesi, yayılması veya ele geçirilmesi suçu özellikle internet ve bilişim ortamında sıkça işlenebilen bir suçtur<sup>684</sup>. Nitekim günümüzde artık hemen hemen bütün bilgiler internet ve bilişim ortamında bulunabilmekte, güvenlik ihlalleri sebebiyle meydana gelen veri sızıntıları sonucunda üçüncü kişilerin eline geçebilmektedir<sup>685</sup>. Kişisel Verileri Koruma Kurulu'nun internet sitesinde kamuoyuna yaptığı duyurular da bu durum gözlemlenmektedir<sup>686</sup>. Ancak bu suç yalnızca internet ve bilişim ortamları aracılığıyla işlenmemektedir. Diğer bir ifadeyle kişisel verilerin internet ve bilişim ortamları haricinde de verilmesi, yayılması veya ele geçirilmesi söz konusu olabilir. Böylelikle başta dolandırıcılık olmak üzere birçok suçun işlenmesi için bir zemin oluşturulma tehlikesi bulunur<sup>687</sup>. İşte kişisel verileri verme, yayma veya ele geçirmenin suç olarak düzenlenmesi bu nedenle yerinde olmuştur<sup>688</sup>.

## 1.2. 765 Sayılı TCK ile Karşılaştırma

Kişisel verileri verme, yayma veya ele geçirme suçunun ilk kez 5237 sayılı TCK'da mı yoksa 765 sayılı TCK'da mı düzenlendiğine ilişkin görüş farklılıkları bulunmaktadır. Bir görüşe göre bu suç tipi ilk kez 5237 sayılı TCK'da düzenlenmiş olup, 765 sayılı TCK'da bir karşılığı bulunmamaktadır<sup>689</sup>. İkinci görüşe göre ise 765 sayılı TCK'nın 525a maddesinin 1. fıkrası<sup>690</sup>, 5237 sayılı TCK'nın 136. maddesine denk gelmektedir<sup>691</sup>. İkinci görüşün kabul edilmesi halinde *kişisel veriden* değil, her türlü *veriden* söz etmek gerekecektir<sup>692</sup>. Yukarıda belirtildiği üzere veri ile kişisel veri terminolojik anlamda

<sup>684</sup> Karagülmez, s. 451.

<sup>685</sup> Dülger, Kişisel Verilerin Korunması, s. 731.

<sup>686</sup> KVKK'nın "Veri güvenliğine ilişkin yükümlülükler" başlıklı 12. maddesinin 5. fıkrasına göre "Kurulunun gerekli hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir." Bu doğrultuda Kurul'un internet sitesindeki ilanlara bakıldığında Türkiye'de hizmet veren ve geniş kitlelere hitap eden birçok şirket, kurum veya kuruluşun veri ihlallerine maruz kaldığı görülmektedir. Erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/2015/Duyurular>, erişim tarihi: 21.09.2021.

<sup>687</sup> Dülger, Kişisel Verilerin Korunması, s. 731.

<sup>688</sup> Dülger, Kişisel Verilerin Korunması, s. 731.

<sup>689</sup> Korkmaz, Ceza Hukuku, s. 376; Akdağ, s. 128; Yaşar, Osman / Gökcan, Hasan Tahsin / Artuç, Mustafa, *Yorumlu Uygulamalı Türk Ceza Kanunu*, 3. Cilt, 2. Baskı, Adalet Yayınları, Ankara 2014, s. 4444.

<sup>690</sup> Madde 525a/1: "Bilgileri otomatik olarak işleme tabi tutmuş bir sistemden, programları, verileri veya diğer herhangi bir unsuru hukuka aykırı olarak ele geçiren kimseye bir yıldan üç yıla kadar hapis ve birmilyon liradan onbeşmilyon liraya kadar ağır para cezası verilir."

<sup>691</sup> Taşkın, Şaban Cankat, *Bilişim Suçları*, Beta Basım, Birinci Baskı, İstanbul, Kasım 2008, s. 105.

<sup>692</sup> Karagülmez, s. 453.

birbirinden farklıdır. Ayrıca yine ikinci görüşün kabul edilmesi halinde 5237 sayılı TCK'nın 136. maddesinin aksine *yalnızca otomatik yöntemlerle* suç işlenebilecektir. Son olarak, 765 sayılı TCK'daki düzenlemenin bulunduğu bölüm başlığının "*Bilişim Alanında Suçlar*" olmasına karşın TCK'daki düzenlemenin bulunduğu başlık "*Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar*"dır. Dolayısıyla bu tespitler ışığında, ikinci görüşe paralel bir şekilde, 5237 sayılı TCK'daki düzenlemenin 765 sayılı TCK'dan bağımsız olarak yeni bir düzenleme olduğunun ifade edilmesi mümkündür<sup>693</sup>.

## 2. SUÇUN HUKUKÎ KONUSU

### 2.1. Genel Olarak

Suçun hukukî konusunu, suçu öngören norm tarafından korunan ve suç tarafından ihlâl edilen hukukî varlık veya menfaat oluşturmaktadır<sup>694</sup>. Diğer bir anlatımla ceza normu tarafından korunan varlık ya da menfaat, aynı zamanda suçun hukukî konusudur<sup>695</sup>. Dolayısıyla suçun hukukî konusu, devletin koyduğu emir ve yasaklarla güvence altına alınmış olan varlık veya menfaatleri içermektedir<sup>696</sup>. Bu varlık veya menfaatler bireysel, toplumsal veya kamusal nitelikte olabilirler<sup>697</sup>. Bir suç tipiyle korunan varlık veya menfaatin tespit edilebilmesi için öncelikle suçun düzenlendiği yerin incelenmesi gerekmektedir. Ancak bu tek başına yeterli olmayıp; bu suçun gerçekleşmesiyle neden cezai yaptırım uygulanacağına da ayrıca ele alınması gerekmektedir.

Kişisel verileri verme, yayma veya ele geçirme suçu TCK'nın Dokuzuncu Bölümünde "*Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar*" başlığı altında düzenlenmiştir. Bu başlık ise "*Kişilere Karşı Suçlar*" üst başlığı altında bulunmaktadır. Dolayısıyla söz konusu varlık ya da menfaatin bireysel nitelikte olduğu söylenebilir. Ancak yalnızca bu

<sup>693</sup> Aynı yönde görüş için bkz.: **Börekçi**, s. 58.

<sup>694</sup> **Toroslu / Toroslu**, s. 109.

<sup>695</sup> **Frosali**, Raul Alberto, "*Soggetto passivo del reato*", Novissimo digesto italiano, Torino, UTET, 1975, s. 817, (Akt: **Katoğlu**, Tuğrul, "*Ceza Hukukunda Suçun Mağduru Kavramının Sınırları*", Ankara Üniversitesi Hukuk Fakültesi Dergisi, C. 61 (2), 2012, ss. 657-693, (**Katoğlu**, Mağdur Kavramının Sınırları), s. 660, dn. 11).

<sup>696</sup> **Katoğlu**, Mağdur Kavramının Sınırları, s. 675.

<sup>697</sup> **Toroslu / Toroslu**, s. 109.

sınıflandırmanın yapılması, suçla korunan varlık ya da menfaatin ortaya çıkarılması için yeterli değildir. Nitekim kişisel verilerin korunması hakkı birçok hak ile yakından ilişkilidir ve bu hakkın korunmasıyla ortaya çıkan menfaatin belirlenmesi zordur. Bu nedenle, suçun hukukî konusunun ortaya çıkarılması için kişisel verilerin korunması hakkına yönelik görüş ve yaklaşımların incelenmesi gerekmektedir.

## 2.2. Kişisel Verilerin Korunması Hakkına Yönelik Görüş ve Yaklaşımlar

Kişisel verilerin korunması hakkı, geçmişten bugüne birçok temel hak ve özgürlük kapsamında ele alınmış ve doktrinde bu hakkın hangi hakla birlikte değerlendirilmesi gerektiğine ilişkin pek çok tartışma yapılmıştır<sup>698</sup>. Gerçekten, kişisel verilerin korunması hakkı temelinde birçok hak ile yakından ilişkilidir<sup>699</sup>. Bunların başında özel yaşamın gizliliği hakkı ve insan onuru gelir<sup>700</sup>. Nitekim genel kabul gören görüşe göre de kişisel verilerin korunması hakkı insan hakları zemininde özel hayatın gizliliği kapsamında korunmalıdır<sup>701</sup>. Bunun yanında kişisel verilerin korunması hakkı; insan onuru, kişilik hakkı, bilgi edinme hakkı gibi pek çok hak ve kavramla bağlantılıdır. Diğer yandan günümüz koşullarında kişisel verilerin yeni bir değer olarak görülmesinin sonucunda bu hakkın mülkiyet hakkı ya da fikrî haklar kapsamında korunması gerektiğine yönelik görüşler de bulunmaktadır. Bu görüşler esasında ekonomik hak yaklaşımı olarak adlandırılabilir. Kişisel verileri ekonomik bir değer olarak gören ekonomik hak yaklaşımı özellikle Amerika Birleşik Devletleri'nde savunulmaktadır<sup>702</sup>. Bu doğrultuda kişisel verilerin korunması hakkının a) *ekonomik hak yaklaşımı* ve b) *bu hakkı daha çok insan onuru ile bağdaştıran, insan haklarına dayalı yaklaşımlar* olarak ikili bir ayrımla ele alınması mümkündür.

---

<sup>698</sup> Göçmen Uyarer, s. 23.

<sup>699</sup> Küzeci, Kişisel Verilerin Korunması, s. 58.

<sup>700</sup> Küzeci, Kişisel Verilerin Korunması, s. 58.

<sup>701</sup> Göçmen Uyarer, s. 24.

<sup>702</sup> Dülger, Kişisel Verilerin Korunması, s. 78.



### 2.2.1. Ekonomik Hak Yaklaşımı

Ekonomik hak yaklaşımı; birçok kurumun sermayesinin veri olmaya başladığı bir çağda veri güvenliğinin ve kişisel verilerin korunması hakkının ekonomik açıdan analiz edilmesinden doğan bir yaklaşımdır<sup>703</sup>. Ancak insana ait temel değerlerin korunması bağlamında kişisel verilerin korunması ihtiyacını bu görüş ile savunmak mümkün görünmemektedir<sup>704</sup>. Nitekim kişisel verilerin korunmasını ekonomik hak bağlamında ele alan yaklaşımlar; kişisel verinin ekonomik yönüne odaklanmakta ve bu hakkı insan hakları bağlamından uzaklaştırmaktadır<sup>705</sup>.

Ekonomik hak yaklaşımı kendi içerisinde mülkiyet hakkı ve fikrî hak kapsamında değerlendirilmektedir.

#### 2.2.1.1. Mülkiyet Hakkı Görüşü

Kişisel verilerin korunması hakkına yönelik ekonomik yaklaşım içerisindeki görüşlerden ilki “*mülkiyet hakkı*” görüşüdür. Mülkiyet kavramı, Arapça kökenli mülk kavramından türetilmiştir ve “*egemen*”, “*güç*”, “*kuvvet*” anlamlarına gelmektedir<sup>706</sup>. Mülkiyet hakkının kapsamı, malikin şey üzerinde sahip olduğu olanakları belirtmektedir<sup>707</sup>.

Kişisel verilerin mülkiyet hakkı çerçevesinde ele alınması gerektiğini belirten bu görüşe göre kişisel verilerin özünde mülkiyet hakkı bulunmaktadır<sup>708</sup>. Mülkiyet hakkı kişilerin malvarlığına dahildir ve verinin öznesi olan kişi, maliki olduğu şeyler üzerinde kapsamlı bir denetim ve tasarruf hakkına sahiptir<sup>709</sup>. Dolayısıyla bu görüş çerçevesinden

<sup>703</sup> Göçmen Uyarer, s. 23.

<sup>704</sup> Kişisel verinin mülkiyet hakkına konu olamayacağına yönelik diğer görüşler için bkz.: Küzeci, Kişisel Verilerin Korunması, s. 70; Taştan, s. 57; Uygun, s. 6; Erarslan Türkmen, s. 21.

<sup>705</sup> Dülger, Kişisel Verilerin Korunması, s. 78; Göçmen Uyarer, s. 23.

<sup>706</sup> Akça, Kürşat, “Anayasa Mahkemesi Kararlarında Mülkiyet Hakkı”, İnönü Üniversitesi Hukuk Fakültesi Dergisi Özel Sayı Cilt:1, Yıl 2015, ss. 543-596, s. 550.

<sup>707</sup> Tuğrul, Saim, *Kamu Hukuku Açısından Mülkiyet Hakkı ve Sınırlandırılması*, Kazancı Hukuk Yayınları, İstanbul, 2004, s. 14.

<sup>708</sup> Litman, Jessica, “Information Privacy/Information Property”, Stanford Law Review, 2000, Cilt: 52, ss. 1283-1313, s. 1287; Janger, Edward J., “Privacy Property, Information Costs and the Anticommons”, Hastings LJ, 2002, Cilt: 54, ss. 899-929, s. 903; Bartow, Ann, “Our Date, Ourselves: Privacy, Protortization and Gender”, USFL Rev., 1999, Cilt: 34, ss. 633-704, s. 687; Kang, Jerry, “Information Privacy in Cyberspace Transactions”, Stanford Law Review, 1998, ss. 1193-1294, s. 1246.

<sup>709</sup> Doğan, s. 50.

düşünüldüğünde kişi, malik sıfatıyla hareket ederek kullanma, tasarrufta bulunma ve yararlanma gibi haklarını kişisel verileri üzerinde de kullanabilir<sup>710</sup>. Bunun bir sonucu olarak kişi, kişisel verilerinin mülkiyetini bedel karşılığında ticari bir şirketin kullanımına sunabilir veya üçüncü kişiye devredebilir<sup>711</sup>. Diğer bir anlatımla bu görüşe göre kişisel verilerin ticari bir değeri vardır ve alım-satıma konu olması olağandır<sup>712</sup>. Ancak malike tanınan yetkilerin kişisel veri üzerinde kullanılması, kişisel veriyi malikinden soyutlayarak bir meta haline dönüştürür ki bu durum hem genel ilkelere aykırıdır hem de kişisel verilerin kendine has özelliklerinin kaybolmasına neden olur<sup>713</sup>. Ayrıca mülkiyet hakkı malikine devretme, değiştirme, imha etme gibi tasarruf imkanları sağlamaktayken<sup>714</sup> kişisel verilerin korunması mevzuatı ise kişisel verilerin korunmasını amaç edinmektedir. Dolayısıyla bir kişinin kişisel verisini satın alan bir kişiye, verinin esas sahibinin açık rızası olmadan bu verileri başkalarına devretme hakkı verilmesi, kişisel verilerin korunması mevzuatı ile bağdaşmayacaktır<sup>715</sup>. Nitekim bu görüşü eleştiren bazı yazarlara göre kişisel veriler ticareti yapılamayan ve devredilemeyen bir niteliğe sahiptir<sup>716</sup>.

Kimi yazarlar, kişisel verileri mülkiyet hakkı ile ilişkilendirirken, bireyler ile verileri arasında doğal bir bağa işaret etmektedir<sup>717</sup>. Ancak eğer taraflar eşit konumda değilse, veri sahibi mülkiyet hakkından kolayca vazgeçebilecektir<sup>718</sup> ve böylelikle kişisel verilerin korunması hakkının temel anlamda uygulanamayacağı bir durum ortaya çıkacaktır. Dolayısıyla bu görüşe yönelik eleştirilere katılarak, kişisel verilerin korunması hakkının bir mülkiyet hakkı olarak değerlendirilmesinin mümkün olmadığını düşünmekteyiz.

---

<sup>710</sup> Taştan, s. 55.

<sup>711</sup> Litman, s. 1295; Kang, s. 1256; Taştan, s. 55.

<sup>712</sup> Doğan, s. 50, Göçmen Uyarer, s. 24-25

<sup>713</sup> Aksoy, s. 65; Taştan, s. 57.

<sup>714</sup> Mülkiyet hakkı dinamik bir unsur olarak toplumun yapısından önemli ölçüde etkilendiği ve devletten devlete, hatta aynı toplum içerisinde dahi farklılıklar gösterebileceğinden, malike tanıdığı hakların hepsini saymak mümkün görünmemektedir. Aynı yönde görüş için bkz.: Şimşek, Suat, "Mülkiyet Hakkının Kapsamı, Sınırlandırma Nedenleri ve Şartları Açısından 1982 Anayasası ve Avrupa İnsan Hakları Sözleşmesi: Karşılaştırmalı Bir Analiz – I", TBB Dergisi 2010 (91), ss. 181-228, s. 190.

<sup>715</sup> Aksoy, s. 65; Köse Aysun, s. 37.

<sup>716</sup> Singh, Atul, "Protecting Personal Data as a Property Right," ILI Law Review, Winter Issue 2016, s. 126, erişim için bkz.: [https://ili.ac.in/pdf/p9\\_atul.pdf](https://ili.ac.in/pdf/p9_atul.pdf), erişim tarihi: 28.06.2021.

<sup>717</sup> Nadezhda, Purtova, "Property Rights in Personal Data: Learning from the American Discourse", Computer Law & Security Review, Vol. 25, No. 6, 2009, ss. 507-521, s. 507, erişim için bkz.: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1554341](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1554341), erişim tarihi: 28.06.2021.

<sup>718</sup> Küzeci, Kişisel Verilerin Korunması, s. 61.

### 2.2.1.2. Fikrî Hak Görüşü

Kişisel verilerin korunması hakkına yönelik ekonomik yaklaşımlar içerisinde yer alan diğer bir görüş, “*fikrî hak*” görüşüdür. Bu görüşe göre, kişisel verilerin özünde fikrî hak yer almakta olup<sup>719</sup> telif hakkı ve benzerinin sağladığı koruma ile kişisel verilere yaklaşılması gerekmektedir<sup>720</sup>. Bu görüşe göre veri sahibi, eser sahibi gibi hareket ederek kişisel verilerini bir sözleşmeye konu edebilir, bunların kullanım haklarını da sözleşmenin karşı tarafına verebilir<sup>721</sup>. Ayrıca kişisel veriler özel bir gizlilik anlaşmasına konu edilebilir<sup>722</sup>.

Kişisel verilerin fikrî hakka ilişkin olduğuna yönelik görüşe yapılan eleştiriler, genel itibarıyla mülkiyet hakkı görüşüne yönelik yapılan eleştiriler ile aynıdır<sup>723</sup>. Bunun dışında fikrî hak görüşü, telif hakkının ortaya çıkmasında önemli rol oynayan çaba, güç, emek ve zekanın kişisel veriler özelinde bir etkisi olmaması yönüyle de eleştirilmektedir<sup>724</sup>. Diğer yandan fikrî mülkiyet hukukunda ekonomik kaygıların gözetilmesi hususu ön planda iken, kişisel verilerin korunması hakkının temelinde bilgilerin izinsiz bir şekilde dolaştırılmaması amaç edinilmektedir<sup>725</sup>. Kanaatimizce kişisel verilerin korunması hakkının ekonomik açıdan değil, insani bir yaklaşımla insan haklarına dayalı bir şekilde ele alınması gerekmektedir.

### 2.2.2. İnsan Haklarına Dayalı Yaklaşımlar

Özellikle AB ülkelerinde ve öğretilerde baskın olan bu görüşe göre kişisel verilerin korunması hakkının; özel hayatın gizliliği, ifade özgürlüğü, unutulma hakkı, bilgi edinme hakkı, insan onuru, kişilik hakkı gibi hak ve değerlerle iç içe olmasından dolayı ekonomik

---

<sup>719</sup> **Bartow**, s. 685; **Lessig**, Lawrence, “*Privacy as Property*”, Social Research, 2002, Cilt: 69, Sayı 1, ss. 247-269, s. 247 vd.

<sup>720</sup> **Erarslan Türkmen**, s. 22.

<sup>721</sup> **Göçmen Uyarer**, s. 28.

<sup>722</sup> **Samuelson**, Pamela, “*Privacy as Intellectual Property*”, s. 2, erişim için bkz.: [https://people.ischool.berkeley.edu/~pam/papers/privasip\\_draft.pdf](https://people.ischool.berkeley.edu/~pam/papers/privasip_draft.pdf), erişim tarihi: 28.06.2021.

<sup>723</sup> İlgili eleştiriler için bkz.: **Küzeci**, Kişisel Verilerin Korunması, s. 63; **Taştan**, s. 57-58; **Aksoy**, s. 60-61; **Akgül**, s. 64.

<sup>724</sup> **Küzeci**, Kişisel Verilerin Korunması, s. 63; **Aksoy**, s. 67; **Doğan**, s. 51.

<sup>725</sup> **Göçmen Uyarer**, s. 25.

bir haktan ziyade bir insan hakkı olarak ele alınması gerekmektedir<sup>726</sup>. Nitekim çalışmanın I. bölümünde ele alındığı üzere, kişisel verilerin korunmasının gelişim sürecinde rol oynayan uluslararası belgeler, temellerini insan hakları üzerine kurmuştur. Kişisel verilerin ekonomik değerinin olduğu bir gerçektir<sup>727</sup>. Ancak sırf bu yönüyle kişisel verilerin korunması hakkının esasen insan hakkından uzaklaşan mülkiyet hakkı ya da fikrî hak görüşü ile savunmanın doğru olmayacağını düşünmekteyiz. Nitekim kişisel verilerin korunması gerekliliği insancıl bir gerekliliktir. Diğer yandan kişisel verilerin korunması, kişilerin ekonomik ve maddi değerlerinden ziyade temelinde bilhassa kişilerin kendisinin korunması amacını barındırmaktadır. Bu bağlamda insan haklarına dayalı yaklaşımın bir sonucu olarak kişisel verilerin korunması hakkı; özel hayatın korunması hakkı, kişilik hakkı, insan hakkı ve kendi geleceğini belirleme hakkı olarak görülmektedir<sup>728</sup>.

### 2.2.2.1. Özel Hayatın Korunması Hakkı Kapsamında Değerlendirme

Özel hayatın gizliliği, Anayasa'nın 20. maddesinin 3. fıkrasında "*Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz.*" hükmüyle koruma altına alınmıştır. Yine, Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesi uyarınca da "*Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.*"

Diğer yandan TCK'nın 134. maddesiyle özel hayatın gizliliği koruma altına alınmıştır. Anılan maddeye göre "*Kişilerin özel hayatının gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır.*" Her ne kadar KVKK'nın "*Suçlar*" başlıklı 17. maddesinin 1. fıkrasında "*Kişisel verilere ilişkin suçlar bakımından 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanunu'nun 135 ila 140 ıncı madde hükümleri uygulanır.*" hükmü yer alsa da suçun oluşmasıyla ihlal edilen menfaat olarak genel bir değerlendirme yapılarak, bölüm başlığında yer alan *özel hayatın* koruma altına alındığı düşünülebilir.

<sup>726</sup> Küzeci, Kişisel Verilerin Korunması, s. 65.

<sup>727</sup> Küzeci, Kişisel Verilerin Korunması, s. 64.

<sup>728</sup> Önemle belirtmek gerekir ki bu ayırım yapılırken kimi yazarlar insan hakkına daha farklı bir perspektiften bakarak kişisel verilerin korunması hakkını kişilik hakkı olarak ele almış (Örn: **Akgül**, s. 68 vd; **Köse Aysun**, s. 13 vd; **Sert**, s. 53 vd); kimi yazarlar kişinin kendi geleceğini belirleme hakkını kişilik hakkından ayrı bir şekilde incelemiştir (Örn: **Sert**, s. 52).

Anılan düzenlemelere karşın, özel hayat kavramının sınırlarının net bir şekilde çizilemediğini belirtmek gerekir<sup>729</sup>. Nitekim özel hayatın tanımlanmasının zorluğu ve kapsamının belirsizliği, özel hayat ile ilgili olarak sıklıkla dile getirilen bir şikayettir<sup>730</sup>. AİHM kararlarına bakıldığında özel hayatın tanımının yapılmasından özenle kaçınıldığı görülmektedir<sup>731</sup>. Örneğin *Niemietz v. Germany*<sup>732</sup> kararında AİHM, “*Mahkeme, özel hayat kavramının tam olarak tanımlanmasının mümkün olduğu ya da böyle bir gayretin gerekli olduğu kanaatinde değildir.*” ifadelerine yer vermiştir. Özel hayat kavramı ile ilgili olarak AİHM ayrıca, her somut olay çerçevesinde nelerin özel hayat kapsamına girebileceğine ilişkin değerlendirmeler yapmaktadır<sup>733</sup>. Örneğin AİHM, *Von Hannover v. Germany*<sup>734</sup> kararında özel hayat kavramından anlaşılması gerekenin mutlaka kişinin gizli alanına ilişkin bir alan olmadığına ve kişinin diğer insanlar ile kamuya açık alanlardaki ilişkilerinde de somut olayın koşullarına göre özel hayat sınırlarının oluşacağını belirtmiştir. Benzer şekilde *Rotaru v. Romania*<sup>735</sup> kararında kamuya mal olmuş bir bilginin otoriteler tarafından sistematik bir şekilde toplandığı bir olayda kişinin özel hayatı kapsamında değerlendirme yapılabileceğini belirtmiştir. Ayrıca AİHM, vermiş olduğu *Satakunnan Markkinapörssi Oy ve Satamedia Oy v. Finland*<sup>736</sup> kararında kişisel verilerin AİHS’in 8. maddesi kapsamında koruma altına alındığını, kişisel verilerin korunmasının

<sup>729</sup> Göçmen Uyarer, s. 30.

<sup>730</sup> Salihpaşaoğlu, Yaşar, “Özel Hayatın Kapsamı: Avrupa İnsan Hakları Mahkemesi İçtihatları Işığında Bir Değerlendirme,” Gazi Üniversitesi Hukuk Fakültesi Dergisi C. XVII, Y. 2013, Sayı: 3, ss. 227-266, s. 234, erişim için bkz.: <https://dergipark.org.tr/tr/download/article-file/789215>, erişim tarihi: 22.06.2021.

<sup>731</sup> Tanımlama güçlüğüne karşısında öğretide özel yaşam bireyin çevresi ile ilişkileri iç içe geçmiş çemberlere benzetilmiş; bu çemberlerden en dışta olanı kişinin herkesle paylaşabileceği, kamuya açık yaşam alanlarını ifade eden “*genel yaşam alanı*”, çemberlerden ortada olanı kişinin belirli kimselerle ve belirli ölçüde paylaştığı yaşam alanını ifade eden “*kişinin özel yaşam alanı*”, çemberlerden en içte kalanı ise kişinin kendisine saklamak istediği alanları oluşturan “*sır alanı*” olarak ifade edilmiştir. Küzeci, Kişisel Verilerin Korunması, s. 69.

<sup>732</sup> AİHM *Niemietz v. Germany* kararı başvuru numarası: 13710/88, karar tarihi: 16.12.1992, erişim için bkz.: <https://hudoc.echr.coe.int/eng#%7B%22itemid%22:%5B%22001-57887%22%5D%7D>, erişim tarihi: 22.06.2021.

<sup>733</sup> AİHM *Costello-Roberts v. The United Kingdom* kararı, başvuru numarası: 13134/87, karar tarihi: 25.03.1991, erişim için bkz.: <https://hudoc.echr.coe.int/tur#%7B%22itemid%22:%5B%22001-57804%22%5D%7D>, erişim tarihi: 22.06.2021.

<sup>734</sup> AİHM *Von Hannover v. Germany* kararı, başvuru numarası: 59320/00, karar tarihi: 24.09.2004, karara erişim için bkz.: <https://hudoc.echr.coe.int/tur#%7B%22itemid%22:%5B%22001-61853%22%5D%7D>, erişim tarihi: 22.06.2021.

<sup>735</sup> AİHM *Rotaru v. Romania* kararı, başvuru numarası: 28341/95, karar tarihi: 04.05.2000, karara erişim için bkz.: <https://hudoc.echr.coe.int/eng#%7B%22itemid%22:%5B%22001-58586%22%5D%7D>, erişim tarihi: 20.09.2021.

<sup>736</sup> AİHM *Satakunnan Markkinapörssi Oy ve Satamedia Oy v. Finland* kararı, başvuru numarası: 931/13, karar tarihi: 27.06.2016, erişim için bkz.: <https://hudoc.echr.coe.int/tur#%7B%22fulltext%22:%5B%22931/13%22%5D%2C%22itemid%22:%5B%22001-175121%22%5D%7D>, erişim tarihi: 22.06.2021.

da 8. madde kapsamında korunan özel hayata ve aile hayatına saygı hakkına sahip olmaları açısından temel öneme sahip olduğunu belirtmiştir.

Bu anlamda görüldüğü üzere gerek AİHS’te gerek AİHM kararlarında gerekse Anayasa’nın 20. maddesinin 3. fıkrasında, kişisel verilerin korunması hakkı özel hayatın gizliliği hakkı kapsamında ele alınmaktadır. Ancak her bir kişisel veri kişinin özel hayatına konu bir bilgi haline gelmediği gibi, her özel hayata ilişkin değerlendirme içerisinde de kişisel veri bulunmamaktadır. Dolayısıyla kişisel veri yalnızca özel hayatın gizliliği çerçevesinde korunmamaktadır<sup>737</sup>. Sonuç olarak bu iki hakkın birbirinden farklı olduğu noktalar bulunmaktadır<sup>738</sup>. Kişisel verilerin korunması hakkı ilk aşamada özel yaşamın gizliliği hakkı içerisinde değerlendirilebilir ise de teknolojinin gelişmesi sebebiyle artık kişisel verilerin yalnızca özel hayatın gizliliği içerisinde değerlendirilmesine olanak bulunmamaktadır. Diğer bir anlatımla artık kişisel verilerin korunması hakkını doğrudan özel hayatın korunması hakkı olarak görmek tam olarak ihtiyaçları karşılamamaktadır<sup>739</sup>.

#### **2.2.2.2. İnsan Onuru Kapsamında Değerlendirme**

Dünya tarihinde yaşanan ve insanlığa zarar veren her olayın ardından insan haklarına korunmasına ilişkin adımlar atılmıştır<sup>740</sup>. Çünkü insanlık onuru bu tip olaylarda epey yara almıştır ki her olayda temel hak ve özgürlüklere yönelik gelişmeler gerçekleşmiştir. Örneğin AİHS’in ortaya çıkmasında II. Dünya Savaşı’nda yaşanan ve insanlık onuru ile bağdaşmayan olaylar etkili olmuştur. Kişisel verilerin korunması hakkı da buna benzer şekilde, teknolojinin imkanlarının artmasıyla birlikte insan onurunu zedeleyici davranışların arttığı bir ortamda gelişmiştir. Bu nedenledir ki kişisel verilerin korunması hakkının insan onuru ile ilişkilendirildiği görülmektedir<sup>741</sup>. Bunun en belirgin örneği Alman Federal Anayasa Mahkemesi tarafından verilen 15.12.1983 tarihli “Nüfus Sayımı” kararıdır. Şöyle ki; 1982 yılında Almanya’da kabul edilen Alman Nüfus Kanunu

<sup>737</sup> Göçmen Uyarer, s. 31.

<sup>738</sup> Göçmen Uyarer, s. 31.

<sup>739</sup> Küzeci, Kişisel Verilerin Korunması, s. 69.

<sup>740</sup> Göçmen Uyarer, s. 38.

<sup>741</sup> Oğuz Şimşek, s. 114.

vatandaşlara nüfus sayımının yapılmasının yanı sıra vatandaşları kendileri hakkında birçok istatistiki bilgiyi vermeye zorlamaktaydı<sup>742</sup>. Anılan kanunun iptali amacıyla yapılan başvuruda Alman Federal Anayasa Mahkemesi, kişisel verilerin korunması hakkını insan onuru ile ilişkilendiren bir karara imza atarak bireyin kişisel verilerinin sınırsız bir şekilde toplanmasını hem birey hem de toplum bazında tehlikelere sebep olabilecek nitelikte değerlendirmiştir<sup>743</sup>. Bu kararlar birlikte insan onurunun ve kişiliğin korunması hükümleri bir arada değerlendirilerek kişisel verilerin korunması hakkına yeni bir boyut getirilmiş, “*kişinin kendi geleceğini belirleme hakkı*” olarak yeni bir yaklaşım benimsenmiştir<sup>744</sup>. Kişinin kendi geleceğini belirleme hakkı, kişilerin kendilerine ait kişisel verilerinden hangilerinin, kim tarafından ve hangi şartlar dahilinde işlenebileceğine karar verme hakkı olarak ifade edilmiştir<sup>745 746</sup>.

Kişisel verilerin korunması hakkı, insanlık onurunun korunmasında vazgeçilmez bir değerdir. Nitekim kişilerin kendi kişisel verileri üzerinde hak ve denetim yetkisine sahip olmaları insanlık onurunun bir yansımasıdır.

### 2.2.2.3. Kişilik Hakkı Kapsamında Değerlendirme

Kişilik hakkı, “*Kişinin hak ve fiil ehliyetinin yanında hayatı, sağlığı şeref ve haysiyeti, sırları, vücut bütünlüğü, ismi ve diğer değerleri üzerindeki hakların tamamı*” olarak ifade edilebilir<sup>747</sup>. Kişilik hakkı görüşü, kişisel verilerin korunması hakkını kişilik hakkının özel bir görünümü şeklinde kabul etmektedir<sup>748</sup>. Böylelikle kişiler, kendi kişisel verileri üzerinde bir hakimiyet alanı yaratabilecek ve bunu yaparken özgür iradeleriyle hareket edeceklerdir<sup>749</sup>. Anılan hakimiyet alanı kişiye, işlenen kişisel verilerini bilme, bu verilere

<sup>742</sup> Sert, s. 52; Oğuz Şimşek, s. 115.

<sup>743</sup> Küzeci, Kişisel Verilerin Korunması, s. 66-67; Boga, s. 11; Akkurt, s. 25.

<sup>744</sup> Küzeci, Kişisel Verilerin Korunması, s. 66-67.

<sup>745</sup> Aksoy, s. 71; Sert, s. 53.

<sup>746</sup> Kişinin kendi geleceğini belirleme hakkının detaylı bir şekilde ele alındığı çalışma için bkz.: Küzeci, Elif, “*İstatistikî Birimler ve Bilgilerin Geleceğini Belirleme Hakkı*”, Türkiye ve Ortadoğu Amme İdaresi Enstitüsü İnsan Hakları Yıllığı, C: 32, 2014, ss. 53-75, (Küzeci, İstatistikî Birimler).

<sup>747</sup> Kılınc, Doğan, “*Anayasal Bir Hak Olarak Kişisel Verilerin Korunması*”, Ankara Üniversitesi Hukuk Fakültesi Dergisi, 61 – 3, 2012, ss. 1089-1169, s. 1101; Özel, Sibel, *Uluslararası Alanda Medya ve İnternette Kişilik Hakkının Korunması*, Seçkin Yayıncılık, Ankara, 2004, s. 26; Börekçi, s. 27.

<sup>748</sup> Aksoy, s. 47.

<sup>749</sup> Börekçi, s. 27.

göre yaşamını ve geleceğini şekillendirebilme imkânı da tanımaktadır<sup>750</sup>. Dolayısıyla bireyin kişisel verilerinin hukuka aykırı olarak işlenmesi sonucunda kişinin hareket serbestisinin sınırlandırılması suretiyle kişilik hakkına bir müdahale edilmektedir<sup>751</sup>.

Esasen kişisel verilerin korunması hakkı, gündeme geldiği ilk zamanlarda kişiliğe ilişkin bir hak olarak ele alınmıştır<sup>752</sup>. Kişinin özel ve gizlilik alanlarının da kişiliğe ilişkin olması sebebiyle, kişisel verilerin korunması hakkı, kişilik hakkının faydalandığı korumadan yararlanmaktadır<sup>753</sup>.

#### 2.2.2.4. Bilgi Edinme Hakkı Kapsamında Değerlendirme

Bilgi edinme hakkı ile kişisel verilerin korunması arasında hassas bir ilişki bulunmaktadır. Bilgi edinme hakkı, idarenin kararları ile işlem ve eylemleri ile ilgili olarak gerekli bilgi ve belgelerin elde edilmesini ifade etmektedir<sup>754</sup>.

Bilgi edinme hakkı, Anayasa'nın 74. maddesinde düzenlenmiştir. İlgili maddeye göre *“Vatandaşlar ve karşılıklılık esası gözetilmek kaydıyla Türkiye’de ikamet eden yabancılar kendileriyle veya kamu ile ilgili dilek ve şikayetleri hakkında, yetkili makamlara ve Türkiye Büyük Millet Meclisine yazı ile başvurma hakkına sahiptir. Herkes, bilgi edinme ve kamu denetçisine başvurma hakkına sahiptir.”*

24.10.2003 tarihli ve 25269 sayılı Resmi Gazete’de yayımlanan 4982 sayılı Bilgi Edinme Hakkı Kanunu’nun *“Tanımlar”* başlıklı 3. maddesinin a bendine göre bilgi *“Kurum ve kuruluşların sahip oldukları kayıtlarda yer alan ve bu Kanun kapsamındaki her türlü veriyi”*, belge ise *“Kurum ve kuruluşların sahip oldukları bu Kanun kapsamındaki yazılı, basılı veya çoğaltılmış dosya, evrak, kitap, dergi, broşür, etüt, mektup, program, talimat, kroki, plân, film, fotoğraf, teyp ve video kaseti, harita, elektronik ortamda kaydedilen her türlü bilgi, haber ve veri taşıyıcılarını ...”* ifade etmektedir. Yine aynı Kanun’un *“Bilgi verme yükümlülüğü”* başlıklı 5. maddesine göre *“Kurum ve kuruluşlar istisnai haller*

<sup>750</sup> Şimşek, Oğuz, s. 136.

<sup>751</sup> Çekin, s. 14.

<sup>752</sup> Taştan, s. 59; Kişilik hakkının genel kişilik hakkı ve özel hukuk alanındaki kişilik hakkı olarak ayrımı için bkz.: Küzeci, s. 67, dn. 211.

<sup>753</sup> Taştan, s. 59.

<sup>754</sup> Erarslan Türkmen, s. 15.



*dışındaki her türlü bilgi veya belgeyi başvuranların yararlanmasına sunmak ve bilgi edinme başvurularını etkin, süratli ve doğru sonuçlandırmak üzere, gerekli idari ve teknik tedbirleri almakla yükümlüdür.”*

Ayrıca Bilgi Edinme Hakkı Kanunu'nun 21. maddesinde özel hayatın gizliliğine ilişkin hükümler düzenlenmiş; *“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.”* hükmüyle kişisel veriler, üçüncü kişilere karşı korunmak istenmiştir.

KVKK'da bilgi edinme açısından Bilgi Edinme Hakkı Kanunu'na benzer bir düzenlemenin bulunduğu görülmektedir. Şöyle ki, KVKK'nın *“İlgili kişilerin hakları”* başlıklı 11. maddesine göre kişisel verisi işlenen gerçek kişiler veri sorumlusuna başvuruda bulunarak kişisel verilerinin işlenme süreçleri ile ilgili bilgi talep edebilir, bu verilerin işlenme amaçlarını sorgulayabilir, bu verilerinin aktarıldığı üçüncü kişileri öğrenebilir, kişisel verilerinin yanlış veya eksik işlenmesi halinde bunların düzeltilmesini ve verilerinin aktarıldığı üçüncü kişilere bildirilmesini isteyebilir. Diğer yandan, KVKK'nın 10. maddesinin 1. fıkrasının a bendine göre ilgili kişi, *“veri sorumlusunun ve varsa temsilcisinin kimliği”*ni öğrenme hakkına sahiptir<sup>755</sup>.

İki düzenlemenin bireylerin kişisel verileri ile ilgili bilgilerini elde etmesi hususunda ortak yönleri içermesinin yanında, birbirleri ile ayrıldığı noktalar da vardır. Bilgi Edinme Hakkı Kanunu kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarını kapsarken, KVKK verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek veya tüzel veri sorumlularını kapsamaktadır. Yine, iki kanunda tanımlanan haklar arasındaki diğer fark, Bilgi Edinme Hakkı Kanunu kapsamında kişi yalnızca daha önceden toplanmış olan bilgilere erişebilirken; KVKK ile buna ek olarak veriyi barındıran

---

<sup>755</sup> **Kalyon**, Arzu, *Türk Vergi Hukukunda Kişisel Verilerin Korunması*, Seçkin Yayıncılık, Ankara 2021, s. 234.

kimsenin başkaca sorumlulukları<sup>756</sup> düzenlenmiştir<sup>757</sup>. Bu doğrultuda kişisel verilerin korunması hakkını baştan sona bilgi edinme hakkı ile bağdaştırmak güçtür.

### 2.3. Değerlendirme

Kanaatimizce her ne kadar kişisel verilerin korunması hakkı iletişim, bilgi edinme, özel hayatın gizliliğinin korunması, kişilik, haber alma, ifade özgürlüğü gibi birçok hak ile yakından ilişkili olsa da artık günümüz koşullarında kişisel verilerin korunması alanındaki gereksinime yukarıda sayılan hakların korunmasına ilişkin mekanizmalar yanıt verememektedir<sup>758</sup>. Bu anlamda kişisel verilerin korunması hakkının diğer haklar ile bağlantılı da olsa kendine özgü bir hak olduğunu düşünmekteyiz. Sonuç olarak kişisel verilerin korunması hakkı, kaynağını çoğunlukla özel hayatın gizliliği ve insan onuru hakkında bulan, kişilik hakkına dayanan, aynı zamanda diğer birçok hak ile ilişkisi olan kendine özgü bağımsız bir hak olarak nitelendirilmelidir<sup>759</sup>.

Esasen kişisel verileri verme, yayma veya ele geçirme suçunu öngören norm tarafından korunan menfaat, suçun düzenlendiği yer dikkate alındığında “özel hayatın gizliliği”dir. Ancak yukarıda açıklanan sebeplerden dolayı kişisel verilerin korunması hakkını yalnızca özel hayat ile ilişkilendiremediğimizden, diğer bir ifadeyle kişisel verilerin korunması hakkını kendine özgü bağımsız bir hak olarak nitelendirdiğimizden dolayı bu suçu öngören norm tarafından korunan menfaatin de kişisel verilerin korunması hakkı olduğunu düşünmekteyiz.

---

<sup>756</sup> Anılan yükümlülükleri veri güvenliğini sağlama, aydınlatma, veri işleme şartlarına uyma, eğitim düzenleme, çeşitli politika ve prosedürler hazırlama, denetim yapma, saklama ve imhaya ilişkin uygulamalar gerçekleştirme şeklinde sıralayabiliriz.

<sup>757</sup> **Erarlan Türkmen**, s. 15.

<sup>758</sup> Aynı yönde bkz.: **Dülger**, *Kişisel Verilerin Korunması*, s. 81 vd.; **Sınar**, s. 36.

<sup>759</sup> Benzer görüşler için bkz.: **Erarlan Türkmen**, s. 23, **Dülger**, *Kişisel Verilerin Korunması*, s. 102; **Taştan**, s. 59; **Sınar**, s. 36.

### 3. SUÇUN MADDİ KONUSU

Suçun maddi konusu, suç teşkil eden davranışın üzerinde gerçekleştiği kişi veya şeydir<sup>760</sup>. Suçun konusu bazen insan olabileceği gibi, bazen de bir eşya olabilir. Beş duyu organıyla algılanamayan bir durum, suçun konusu olamaz<sup>761</sup>. Dolayısıyla suçun maddi unsuru somuttur<sup>762</sup>.

Kişisel verileri verme, yayma veya ele geçirme suçu açısından ilk aşamada suçun maddi konusunun kişisel veri olduğu ifade edilebilir. Ancak burada şu değerlendirmenin yapılması gerekir. Kişisel veri bir şey midir? Beş duyu organıyla algılanabilir mi? Fiziki bir varlığı var mıdır? Bu sorulara verilecek yanıt “*hayır*” olmalıdır. Aksi görüşün varlığına rağmen, birçok suçun maddi konusu bulunmamaktadır<sup>763</sup>. Maddi konuyu yalnızca maddi veya fiziki bir yapıya sahip olan varlıklar oluşturabilir<sup>764</sup>. Dolayısıyla kişisel verileri verme, yayma veya ele geçirme suçunun maddi konusu yoktur.

### 4. SUÇUN FAİLİ

Ceza hukuku anlamında hukuka aykırı davranışı gerçekleştiren kimseye suçun faili denilmektedir<sup>765</sup>. Suçlar fail bakımından a) herkes tarafından işlenebilen suçlar ve b) belirli bir sığata sahip kişiler tarafından işlenebilen (özgü-mahsus) suçlar olmak üzere ikiye ayrılmaktadır<sup>766</sup>.

Kanundaki tanımına göre bir suç herhangi bir kimse tarafından işlenebilirse bu suç “*genel suç*” ya da “*herkes tarafından işlenebilen suç*” olarak adlandırılmaktadır<sup>767</sup>. TCK’nın 136. maddesinde düzenlenen kişisel verileri verme, yayma veya ele geçirme suçunun faili açısından herhangi bir ayırım veya özellik gözetilmemiştir, bu anlamda herkes suçun faili

<sup>760</sup> **Toroslu / Toroslu**, s. 110; **Katođlu**, Mađdur Kavramının Sınırları, s. 659; **Özen**, s. 295; **Hakeri**, s. 119; **Centel / Zafer / Çakmut**, s. 236.

<sup>761</sup> **Özen**, s. 295.

<sup>762</sup> **Özen**, s. 295.

<sup>763</sup> **Toroslu / Toroslu**, s. 111.

<sup>764</sup> **Toroslu / Toroslu**, s. 111.

<sup>765</sup> **Toroslu / Toroslu**, s. 107; **Özen**, s. 277.

<sup>766</sup> **Toroslu / Toroslu**, s. 107-108; **Özen**, s. 278.

<sup>767</sup> **Sınar**, s. 40.

olabilir<sup>768</sup> <sup>769</sup>. Dolayısıyla kişisel verileri verme, yayma veya ele geçirme suçu herkes tarafından işlenebilen genel suçtur<sup>770</sup>.

Buna karşın TCK'nın "Nitelikli haller" başlıklı 137. maddesinin 1. fıkrasının a bendine göre; kişisel verileri veren, yayan veya ele geçiren kişi eğer kamu görevlisi ise ve bu kamu görevlisi suçu görevinin verdiği yetkiyi kötüye kullanarak gerçekleştirmiş ise kendisine verilecek ceza yarı oranında artırılabacaktır. Yine aynı maddenin b bendine göre eğer ki bu suç belirli bir meslek ve sanatın sağladığı kolaylıktan yararlanılarak işlenmişse ceza yarı oranında artırılabacaktır. Dolayısıyla suçun 137. maddesinde sayılan nitelikli hali, yalnızca 137. maddede sayılan belirli kişiler tarafından işlenebilen bir suçtur. Belirli kişiler tarafından işlenebilen, failin niteliğiyle ilgili belirleme yapan bu tür suçlara özgü suç denilmektedir<sup>771</sup>. Özgü suç kendi içinde "görünüşte özgü suçlar" ve "gerçek özgü suçlar" olarak ikiye ayrılmaktadır. Suçun basit halinin herkes tarafından işlenebilmesine karşın nitelikli halinin yalnızca belirli niteliği taşıyan kişiler tarafından işlenebiliyor olması durumunda görünüşte özgü suç gündeme gelmektedir<sup>772</sup>. Dolayısıyla bu suç tipinin TCK'nın 137. maddesinde düzenlenen nitelikli hali görünüşte özgü suçtur<sup>773</sup>.

Son olarak, tüzel kişilerin bu suçta fail olup olamayacağına saptanması gerekir. TCK'nın "Ceza sorumluluğunun şahsiliği" başlıklı 20. maddesinin 1. fıkrasına göre "Ceza sorumluluğu şahsidir. Kimse başkasının fiilinden dolayı sorumlu tutulamaz." Aynı maddenin 2. fıkrasına göre ise "Tüzel kişiler hakkında ceza yaptırımı uygulanamaz. Ancak, suç dolayısıyla kanunda öngörülen güvenlik tedbiri niteliğindeki yaptırımlar saklıdır." Suçta ve cezada şahsilik ilkesinin bir yansıması<sup>774</sup> olan bu maddenin yanı sıra

---

<sup>768</sup> **Dülger**, Kişisel Verilerin Korunması, s. 732; **Koca**, Mahmut / **Üzülmez**, İlhan, *Türk Ceza Hukuku Özel Hükümler*, Adalet Yayınevi, Gözden Geçirilmiş ve Genişletilmiş 7. Baskı, Ankara 2020, s. 575; **Saka / Çağlayan / Koca**, s. 367-368; **Göçmen Uyarer**, s. 224; **Hafizoğulları**, Zeki / **Özen**, Muharrem, "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" Ankara Barosu Dergisi, Yıl: 67, Sayı: 4, 2009, ss. 9-22; **Epözdemir**, Rezan, "Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme Suçu (TCK m. 136)" Terazi Hukuk Dergisi, Cilt: 14, Sayı: 151, Mart 2019, ss. 528-544, s. 532; **Korkmaz**, Ceza Hukuku, s. 458; **Börekeçi**, s. 67.

<sup>769</sup> Akdağ'a göre "Kişiyile bağlantılandırılması çok zor olan bir veriyle ilgili olarak gerçekleştirilen fiillerde, failin özel yeteneği göz önüne alınmalı ve objektif olarak suç kabul edilemeyecek bir fiilin, failin yeteneği sebebiyle suç kalıbına uygun hale geliyorsa, fail tipik fiili işlemiş kabul edilmelidir.", **Akdağ**, s. 94.

<sup>770</sup> **Börekeçi**, s. 67.

<sup>771</sup> **Özgenç**, s. 188; **Özbek / Doğan / Bacaksız**, Genel Hükümler, s. 213; **Özen**, s. 278.

<sup>772</sup> **Özen**, s. 278.

<sup>773</sup> **Koca / Üzülmez**, s. 575; **Sert**, s. 141.

<sup>774</sup> Bir fiil dolayısıyla tüzel kişilerin cezalandırılması durumunda, bu fiile katkı sağlamayan diğer kişilerin de (örneğin bir anonim şirkette diğer ortakların) zarar göreceği düşüncesinden hareket edilerek suçta ve cezada şahsilik ilkesi arasında bir bağ kurulmaktadır.

TCK'nın “Tüzel kişiler hakkında güvenlik tedbiri uygulanması” başlıklı 140. maddesi de “Yukarıdaki maddelerde tanımlanan suçların işlenmesi dolayısıyla tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur.” şeklinde düzenlenmiştir. Bu itibarla, tüzel kişiler hakkında Anayasa'nın 38. maddesinde ifade edilen “ceza yerine geçen güvenlik tedbirleri” uygulanacaktır. Ancak güvenlik tedbirlerinin de suçtan kaynaklanan cezai sonuçlar olduğu unutulmamalıdır<sup>775</sup>. Güvenlik tedbirlerinin bir suçun karşılığı olarak uygulanmasından dolayı, tüzel kişilerin de fail olarak kabul edilebilmesi mümkündür<sup>776</sup>. Diğer yandan normlar hiyerarşisi bakımından bir inceleme yapıldığında, Anayasa hükmünün TCK'nın 20. maddesinden üstün olduğu açıktır. Bu durumda tüzel kişilerin fail olabilmesinin önünde yasal anlamda bir engel bulunmamaktadır<sup>777</sup>. Yaygın görüşün aksine, bu suçta tüzel kişilerin fail olabileceği düşüncesindeyiz<sup>778</sup>.

## 5. SUÇUN MAĞDURU

Her suçun bir faili olduğu gibi bir de mağduru bulunmaktadır<sup>779</sup>. Mağdur kavramından anlaşılması gereken, suçun konusu davranış ile ihlal edilen ve cezai korumanın konusunu oluşturan varlık ya da menfaatlerin sahipleridir<sup>780</sup>.

Mağdur gerçek kişi olabileceği gibi eğer ki suçun doğası buna izin veriyorsa tüzel kişi de olabilir<sup>781</sup>. Ancak kişisel verileri verme, yayma veya ele geçirme suçunda söz konusu verilerin “kişisel” olması nedeniyle bu suçun mağduru, suçun doğası gereği tüzel kişi olamaz. Tüzel kişiler bu suçta ancak suçtan zarar gören olabilir<sup>782</sup>. TCK'nın 135.

<sup>775</sup> Katoğlu, Mağdur Kavramının Sınırları, s. 667.

<sup>776</sup> Tüzel kişilerin fail olup olamayacağına ilişkin kapsamlı değerlendirmeler için bkz.: Katoğlu, Mağdur Kavramının Sınırları, s. 667-672; Özen, s. 281-287; Özbek / Doğan / Bacaksız, Genel Hükümler, s. 219-225.

<sup>777</sup> Katoğlu, Mağdur Kavramının Sınırları, s. 671.

<sup>778</sup> Aksi yönde görüş için bkz.: Saka / Çağlayan / Koca, s. 368; Sert, s. 106; Kangal, Zeynel T., *Kişisel Verilerin Ceza ve Kabahatler Hukukunda Korunması*, On İki Levha Yayıncılık, 1. Baskı, İstanbul, Eylül 2019, (Kangal, *Kişisel Veriler*), s. 98; Dülger, *Kişisel Verilerin Korunması*, s. 732; Maden, Mehmet, *Ceza Hukukunda Kişisel Verilerin Korunması*, Adalet Yayınevi, Birinci Baskı, Mayıs, Ankara 2021, s. 112; Parlar, Ali / Çobanoğlu, Yekta, *Özel Hayat ve Hayatın Gizli Alanına Karşı Suçlar (TCK 132. – 140. Md)*, Aristo Yayınevi, 1. Baskı, İstanbul, Haziran 2018, s. 328; Börekçi, s. 68.

<sup>779</sup> Toroslu / Toroslu, s. 112; Sınar, s. 40.

<sup>780</sup> Katoğlu, Mağdur Kavramının Sınırları, s. 662; Toroslu / Toroslu, s. 114.

<sup>781</sup> Katoğlu, Mağdur Kavramının Sınırları, s. 672.

<sup>782</sup> Karagülmez, s. 408; Erdoğan, Yavuz, “*Kişisel Verilerin Korunması Bakımından Türk Ceza Kanunu Hükümlerinin Değerlendirilmesi*”, Erciyes Üniversitesi Hukuk Fakültesi Dergisi Prof. Dr. Doğan Soyaslan

maddesinin gerekçesinde gerçek kişiyle ilgili her türlü bilginin kişisel veri olarak kabul edileceği, KVKK'nın 3. maddesinde ise kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilginin kişisel veri olduğu belirtilmiştir. Yargıtay da vermiş olduğu bir kararında tüzel kişilere ilişkin veriler ile ilgili olarak “*Verileri hukuka aykırı olarak verme veya ele geçirme suçunda gerçek kişiye ait bilgilerin “kişisel veri” olarak düzenlenmesi karşısında, servis elemanının çalıştığı şirkete ait hard diskinde bulunan mali bilgiler ve programların kişisel veri olarak kabul edilemeyeceği gözetilmelidir.*” yorumunu yapmıştır<sup>783</sup>. Yargıtay yine başka bir kararında “*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 nazara alındığında, şikayetçi .... Anonim Şirketi'nin sanığa yüklenen verileri hukuka aykırı olarak verme veya ele geçirme suçunun mağduru olmadığı ve suçtan doğrudan zarar görmemesi nedeniyle davaya katılma hakkının bulunmadığı gözetilmeksizin davaya katılmasına karar verilip...*” ifadelerine yer vermiştir<sup>784</sup>. Yukarıda yapılan açıklamalar dikkate alındığında, bu suçta mağdur ilgili kişi sıfatıyla yalnızca kişisel verilerin korunması hakkına sahip olan gerçek kişi olabilir. Tüzel kişiler ise suçtan zarar gören olabilir.

Diğer yandan bu suçun mağduru olabilmek için kişisel verilerin zilyedi ya da maliki olunmasının şart olup olmadığının da açıklığa kavuşturulması gerekmektedir. Bir görüşe göre suçun mağduru ancak kişisel verilerin zilyedi ya da maliki olabilirken<sup>785</sup>; aksi yöndeki görüşe göre ise suçun mağduru olabilmek için kişisel verilerin zilyedi ya da maliki olunup olunmadığının bir önemi yoktur<sup>786</sup>. Örneğin bir bireyin kişisel verilerinin bir veri sorumlusu tarafından hukuka uygun şekilde işlendiği; ancak siber saldırı sonucu üçüncü kişiler tarafından ele geçirildiği varsayımında, TCK'nın 136. maddesi kapsamında mağdur; kişisel verileri elinde barındıran veri sorumlusu değil; kişisel verileri siber saldırı sonucu hukuka aykırı bir şekilde elde edilen, kişisel verilerinin korunması

---

Armağanı, C: VIII, S: 2, Y: 2013, s. ss. 569-632, s. 614; **Börekçi**, s. 74-75. Bu türden bir ayırım yapılmasının “mağdur” kavramı ile yaratacağı karışıklığa dair görüş için ayrıca bkz.: **Katoğlu**, Mağdur Kavramının Sınırları, s. 680 ve 681.

<sup>783</sup> Yargıtay 12. Ceza Dairesi'nin 2013/10672 E. ve 2013/15772 K. sayılı, 10.06.2013 tarihli kararı, (Kazancı İçtihat Bilgi Bankası), erişim tarihi: 28.06.2021.

<sup>784</sup> Yargıtay 12. Ceza Dairesi'nin 2017/1613 E. ve 2018/3978 K. sayılı, 04.04.2018 tarihli kararı, (Lexpera), erişim tarihi: 28.06.2021.

<sup>785</sup> **Taşkın**, s. 106.

<sup>786</sup> **Göçmen Uyarer**, s. 193; **Dülger**, Kişisel Verilerin Korunması, s. 732; **Sınar**, s. 40.

hakkı zarar gören gerçek kişi olacaktır. Veri sorumlusu ise bu örnekte suçtan zarar gören olabilir. Dolayısıyla, ikinci görüşe paralel şekilde kişisel verilerin verilmesi, yayılması veya ele geçirilmesi suçunun mağdurunun belirlenmesinde zilyet ya da malik olmanın öneminin bulunmadığını düşünmekteyiz.

Suçun mağduru üzerine yapılan tartışmalardan üçüncüsü ise ölmüş kişilerin bu suçun mağduru olup olamayacağına ilişkindir. Kural olarak bir kişinin mağdur sıfatını haiz olabilmesi için hareketin yapıldığı anda hayatta olması gerekir<sup>787</sup>. Ancak Kişisel Sağlık Verileri Hakkında Yönetmelik'in<sup>788</sup> 11. maddesi çerçevesinde göre ölmüş kişilerin de kişisel verisinden söz edilebilir. Bu doğrultuda hastaların sağlık verilerine yönelik sırlarının ölümden sonra da açıklanmaması TCK'nın 136. maddesinin koruma amacı ile bağdaşmaktadır<sup>789</sup> <sup>790</sup>. Ancak bu suç, kişilere karşı suçlar başlığı altında düzenlenmektedir. TMK'nın 28. maddesine göre kişilik ölümle sona ermektedir. Kişisel verilerin korunması hakkı da kişilik hakkına dayanan bir hak olduğundan, kişisel verileri verme, yayma veya ele geçirme suçunun mağduru ölmüş kişiler olamayacaktır<sup>791</sup>. Ancak eğer ki koşulları oluşmuşsa bu durumda kişinin hatırasına hakaret suçunu düzenleyen TCK'nın 130. maddesinin 1. fıkrası uygulanabilir<sup>792</sup>. Diğer yandan, ölmüş bir kimseye ait kişisel verilerin verilmesi, yayılması veya ele geçirilmesi halinde bu kişisel verilerden ölmüş kimsenin yakınları da belirli veya belirlenebilir kılınıyorsa bu durumda ölmüş kimsenin yakınları da mağdur olacaktır<sup>793</sup>.

Kişisel verileri verme, yayıma veya ele geçirme suçunun mağduru bakımından ayrıca bir özellik aranmaz. Bu suçun mağdurunun genel anlamda herkes olabileceği söylenebilir<sup>794</sup>.

<sup>787</sup> Artuk, M. Emin / Gökçen, Ahmet / Alşahin, M. Emin / Çakır, Kerim, *Ceza Hukuku Genel Hükümler*, Adalet, Ankara, 2017, (Artuk / Gökçen / Alşahin / Çakır, Genel Hükümler), s. 303. Bu durumun istisnası, TCK'nın 130. maddesinde düzenlenen "Kişinin hatırasına hakaret" suçunda yer almaktadır.

<sup>788</sup> 21.06.2019 tarihli ve 30808 sayılı sayılı Resmî Gazete'de yayımlanan Kişisel Sağlık Verileri Hakkında Yönetmelik.

<sup>789</sup> Yılmaz, Kişisel Veriler, s. 55.

<sup>790</sup> Anılan Yönetmelik'in "Ölünün sağlık verilerine erişim" başlıklı 11. maddesi aşağıdaki gibidir:

"(1) Ölmüş bir kimsenin sağlık verilerini almaya, veraset ilamını ibraz etmek suretiyle murisin yasal mirasçıları münferit olarak yetkilidir. (2) Ölmüş bir kimsenin sağlık verileri, en az 20 yıl süre ile saklanır."

<sup>791</sup> M. Emin Artuk / Ahmet Gökçen / Emin Alşahin / Kerim Çakır, *Ceza Hukuku Özel Hükümler*, Adalet Yayınevi, Yenilenmiş ve Gözden Geçirilmiş 19. Baskı, Ankara 2021, (Artuk / Gökçen / Alşahin / Çakır, Özel Hükümler), 552.

<sup>792</sup> Kangal, Kişisel Veriler, s. 62.

<sup>793</sup> Ancak önemle belirtmek gerekir ki; kişiler ancak kendisi ile ilgili kişisel veriler açısından suçun mağduru olabilirler. Bu kişilere yakın olan kişiler, suçtan zarar gören sıfatını haiz olabilir. Akdağ, s. 92.

<sup>794</sup> Dülger, Kişisel Verilerin Korunması, s. 732; Koca / Üzülmez, 575; Akdağ, s. 92; Göçmen Uyarer, s. 193; Sınar, s. 40.

## 6. SUÇUN MADDİ UNSURU

### 6.1. Davranış

#### 6.1.1. Genel Olarak

Suçun maddi unsurunu oluşturan davranış a) hareket b) ihmal şeklinde *-diğer bir ifadeyle a) yapma b) yapmama-* şeklinde olabilir<sup>795</sup>. Yapma şeklindeki suçlar hareket suçları olarak adlandırılırken, yapmama şeklindeki suçlar ihmâli davranışla gerçekleştirilen suçlar suçlarıdır<sup>796</sup>. Bu başlık altında öncelikle suçun maddi unsuruna yönelik olarak genel açıklamalara yer verilecek, sonrasında ise suç teşkil eden davranışlar<sup>797</sup> ele alınacaktır.

İlk olarak, suç tipinin davranışın türüne göre sınıflandırılması gerekmektedir. Madde metninde belirtilen “*verme*”, “*yayma*” veya “*ele geçirme*” davranışlarından birisinin varlığı, suçun oluşması için yeterlidir. Bu anlamda suç, **seçimlik davranışlı** bir suçtur<sup>798</sup>. Madde metninde belirtilen davranışlardan birkaçının varlığı halinde tek bir suç işlenmiş olunur ve faile tek suçun cezası verilir<sup>799</sup>. Ancak birden fazla davranışın olması, failin cezasının TCK'nın 61. maddesinin 1. fıkrasının a bendi kapsamında tayin edilmesi açısından önem taşıyacaktır<sup>800</sup>. Buna göre seçimlik davranışlar içerisinde birden fazla davranışın gerçekleşmesi durumunda faile verilecek ceza alt sınırdan üst sınıra yaklaşacaktır.

İkincil olarak, suç tipinin davranışın şekline göre incelenmesi gerekmektedir. Bir görüş, bu suç tipinin yalnızca icrai davranışla işlenebileceğini belirtirken<sup>801</sup>, ikinci bir görüş bu suç tipinin ihmali davranışla da işlenebileceğini savunmaktadır<sup>802</sup>. İkinci görüşe göre örneğin kişinin rızası dahilinde yayınlanmış bir kişisel verinin, kişinin rızasının ortadan

<sup>795</sup> **Toroslu / Toroslu**, s. 133 ve 138.

<sup>796</sup> **Toroslu / Toroslu**, s. 138.

<sup>797</sup> İncelenen suç tipinin ihmali davranışla işlenebileceğini düşünmediğimden, çalışmada davranış ve hareket ifadelerini bazı açıklamalarda birbiri yerine kullandığımı belirtmek isterim.

<sup>798</sup> **Akdağ**, s. 129; **Dülger**, *Kişisel Verilerin Korunması*, s. 733; **Maden**, s. 93; **Karagülmez**, s. 451; **İtişgen**, s. 186; **Erdoğan**, s. 610; **Börekçi**, s. 78; **Saka / Çağlayan / Koca**, s. 381; **Göçmen Uyarer**, s. 227.

<sup>799</sup> **Dülger**, *Kişisel Verilerin Korunması*, s. 736; **Börekçi**, s. 78; **Saka / Çağlayan / Koca**, s. 381-382.

<sup>800</sup> **Börekçi**, s. 78.

<sup>801</sup> **Akdağ**, s. 128.

<sup>802</sup> **Erdoğan**, s. 613-614; **Sert**, s. 140.



kalkması halinde yayınlanmaya devam etmesi durumunda suç ihmali davranışla işlenmiş olacaktır<sup>803</sup>. Ancak bu örnekte esasen KVKK'nın 7. ve 17. maddelerinin değerlendirilmesi gerekmektedir. Nitekim açık rıza ile işlenen bir kişisel veri daha önceden hukuka uygun bir şekilde işlenmiş olacaktır. Açık rızanın geri alınmasıyla birlikte artık bu verinin işlenmesi için hukukî sebep ortadan kalkacağından, kişisel verinin işlenmesini gerektirecek amaç da ortadan kalkacaktır. Dolayısıyla kişisel verinin yayınlanmasına devam edilmesi durumunda TCK'nın 136. maddesinin ihmali bir davranışla gerçekleşmesi değil, TCK'nın 138. maddesinin (verileri yok etmeme) ihmali davranışla gerçekleşmesi söz konusu olacaktır<sup>804</sup>. Diğer yandan, ihmâl şu şekilde açıklanabilir: *“Yasada belli bir durumda belli hareketin yapılması emredildiği halde bu yapılmamışsa ihmali hareketten söz edilir. İhmal, herhangi bir hareketin yapılmaması değil, belli özelliği olan bir hareketin yapılmamasıdır. Bu özellik, bir hukuk normu ile bu hareketin yapılmasının emredilmiş olmasıdır. Yani ihmali ihmal yapan, failin yapmayı ihmal ettiği, ancak “yapılması beklenen” harekettir.”*<sup>805</sup>. Daha kısa bir ifadeyle ihmalin esası, kişinin yapmak zorunda olduğu bir hareketi yapmamasıdır<sup>806 807</sup>. Kişisel verileri verme, yayma veya ele geçirme suçunda *“belli özelliği olan bir hareketin yapılmaması”* söz konusu değildir. Diğer yandan, bu suçun ihmal benzeri bir suç olup olmadığı yönündeki incelemede, ihmal benzeri suçların failin neticeye engel olma yükümlülüğü ve olanağı varsa gündeme geleceğinden<sup>808</sup>, buna da TCK'da kasten öldürme ve kasten yaralama suçlarında yer verildiğinden, kişisel verileri verme, yayma veya ele geçirme suçu ihmali davranışla ya da ihmal benzeri davranışla değil, yalnızca **icrai davranışla işlenebilir**.

Hareketin ne şekilde gerçekleştirileceğinin belirtildiği suçlar bağlı hareketli suç niteliğini taşır<sup>809</sup>. Dolayısıyla kişisel verileri verme, yayma veya ele geçirme suçu da **bağlı hareketli bir suçtur**<sup>810</sup>.

<sup>803</sup> Nil Melek **Gültekin**, *Kişisel Verilerin Ceza Hukuku Yönünden Korunması*, Yayınlanmamış Yüksek Lisans Tezi, Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü, 2012, s. 163-164; **Sert**, s. 140.

<sup>804</sup> Aynı yönde görüş için bkz.: **Böreççi**, s. 84.

<sup>805</sup> **Centel / Zafer / Çakmut**, s. 257-258.

<sup>806</sup> **Toroslu / Toroslu**, s. 138.

<sup>807</sup> **Toroslu / Toroslu**, s. 138.

<sup>808</sup> **Centel / Zafer / Çakmut**, s. 261.

<sup>809</sup> **Özen**, s. 246; **Hakeri**, s. 136; **Toroslu / Toroslu**, s. 139.

<sup>810</sup> **Yılmaz**, *Kişisel Veriler*, s. 104.

Madde gerekçesinde “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.” ifadelerine yer verildiği görülmektedir. Bu anlamda verilen, yayılan ya da ele geçirilen kişisel verilerin hukuka uygun veya hukuka aykırı bir şekilde kaydedilmiş olması, suçun oluşumu açısından önemli değildir<sup>811</sup>. Nitekim kaydetme suçu ile kişisel verilerin verilmesi, yayılması veya ele geçirilmesi suçu birbirinden farklı suçlardır. Yargıtay da vermiş olduğu 2016 tarihli bir kararında bu hususu doğrulamaktadır<sup>812</sup>:

*“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 Kanununun 136/1. maddesinde “Verileri hukuka aykırı olarak verme veya ele geçirme” başlığı altında birbirinden bağımsız iki ayrı suç olarak tanımlanmıştır.”*

Yine madde gerekçesi incelendiğinde, kişisel verilerin kaydedilmiş halde olmasının zorunluluk olduğu yönünde bir sonuç ortaya çıkabilir. Nitekim madde gerekçesinde “hukuka uygun olarak kaydedilmiş olsun veya olmasın” ifadesi yer almaktadır. Dolayısıyla madde gerekçesinde kaydetmenin varlığı aranmış; ancak bu kaydetmenin hukuka uygun olup olmadığının araştırılmasına gerek duyulmamıştır. Yargıtay daha önce vermiş olduğu kararlarında kayıt işlemi olmaksızın salt duyu organları aracılığı ile kişisel

<sup>811</sup> Dülger, Kişisel Verilerin Korunması, s. 733 ve 740; Saka / Çağlayan / Koca, s. 382; Börekçi, s. 78; Maden, s. 106.

<sup>812</sup> Yargıtay 12. Ceza Dairesi'nin 2015/4349 E. ve 2016/5349 K. sayılı, 30.03.2016 tarihli kararı, (Yargıtay Bilgi Bankası), erişim tarihi: 30.09.2021.

verilere erişim halinde suçun özel hayatın gizliliğini ihlal suçu kapsamında değerlendirilmesi gerektiğini belirtirken<sup>813</sup>; 2019 yılında vermiş olduğu bir kararda “... kişisel verilerin, üzerinde yazılı olduğu belgenin bulunduğu yerden alınması ya da kaydedilmiş haliyle başka bir nesne üzerine taşınarak (örneğin; yazının başka bir kağıt, defter vb. nesne üzerine geçirilmesi, taşınabilir belleğe veya CD'ye aktarılması gibi işlemlerle) sabitlenmesi, böylece istenildiğinde tekrar kullanılabilmesi olanağını sağlayan her türlü faaliyet, kişisel verileri “ele geçirme” kapsamında değerlendirilebileceği gibi, kişisel verilerin kaydedilmeden önce öğrenilmesi, kişisel verilere salt duyu organları aracılığıyla vakıf olunması da aynı kapsamda değerlendirilmelidir.” ifadelerine yer vererek kişisel verinin kaydedilmeksizin salt duyu organları aracılığıyla vakıf olunması halinde TCK'nın 136. maddesinden hüküm kurulması gerektiğini belirtmiştir<sup>814</sup>. Bu noktada Yargıtay'ın sonraki tarihli kararları daha isabetli görünmektedir. Nitekim madde metnine göre kişisel verilerin kaydedilmesi bir zorunluluk olarak belirtilmemiştir<sup>815</sup>. Bunun yanında, kişisel verilere ne şekilde erişildiğinin de suçun oluşması açısından bir önemi bulunmamaktadır<sup>816</sup>. Ancak bu durum, veri kayıt sisteminin bir parçası olmadan otomatik olmayan yollarla kişisel verilerin işlenmesini gündeme getirebilir. Bunun bir sonucu olarak da hukuka uygunluk nedenlerinin tespiti açısından KVKK'daki veri işleme şartlarının değil, genel hukuka uygunluk nedenlerinin incelenmesi söz konusu olacaktır. Verilen, yayılan veya ele geçirilen kişisel verilerin başkaları tarafından öğrenilip öğrenilmemesi suçun oluşması açısından önemli değildir<sup>817</sup> Kişisel verinin öğrenilmesi imkanının sağlanmasıyla suç oluşur<sup>818</sup>.

---

<sup>813</sup> Yargıtay 12. Ceza Dairesi'nin 2017/12083 E. ve 2018/2539 K. sayılı, 07.03.2018 tarihli kararı, (Kazancı İçtihat Bilgi Bankası), erişim tarihi: 28.06.2021.

<sup>814</sup> Yargıtay 12. Ceza Dairesi'nin 2018/8152 E. ve 2019/4886 K. sayılı, 10.04.2019 tarihli kararı, (Kazancı İçtihat Bilgi Bankası), erişim tarihi: 28.06.2021.

<sup>815</sup> Aynı yönde görüş için bkz.: **Dülger**, Kişisel Verilerin Korunması, s. 736; **Kangal**, Kişisel Veriler, s. 108; **Maden**, s. 100. Aksi yönde görüş için bkz.: **Börekçi**, s. 80.

<sup>816</sup> **Dülger**, Kişisel Verilerin Korunması, s. 736.

<sup>817</sup> **Sınar**, s. 46; **Sert**, s. 139;

<sup>818</sup> **Akdağ**, s. 131.

## 6.1.2. Verme

TDK'ya göre vermek, “*üzerinde, elinde veya yakınında olan bir şeyi birisine eriřtirmek, iletme*” anlamına gelmektedir<sup>819</sup>. Bu anlamda kişisel verilerin ulařtırılması, ulařtırılan kişinin öğrenmesini gerektirmeyip; kişisel veriyi öğrenmemesi durumunda dahi muhatabın hakimiyet alanına girmesiyle vermek davranıřı tamamlanır<sup>820</sup>. Diđer bir anlatımla, kişisel verinin iletildiđi kişinin, kişisel verinin içeriđine vakıf olması řart deđildir; örneđin kişisel verilerin kayıtlı olduđu bir CD'nin teslim edilmesi yöntemiyle de bu suç gerçekteşebilir<sup>821</sup>.

Söz konusu verme davranıřının usul veya řekli aısından bir ayırım bulunmamaktadır<sup>822</sup>. Kişisel veriler taşınabilir bellek, kısa mesaj<sup>823</sup>, e-posta, bulut, posta<sup>824</sup>, yazılı, sözlü<sup>825</sup> veya dijital gibi birçok yöntemle verilebilir<sup>826</sup>. Öđretide kulaktan kulađa kişisel veri aktarılması halinde TCK'nın 136. maddesinin uygulanmaması gerektiđi savunulsa da suçun hukukî konusu gözetildiđinde kulaktan kulađa kişisel veri aktarımında da TCK'nın 136. maddesinin uygulanması gerektiđi kanaatindeyiz<sup>827</sup>.

Kişisel verilerin verildiđi kişinin gerçekte kişi veya tüzel kişi olması, suçun oluřması aısından önemli deđildir. Fail, mađdura ait kişisel verileri gerçekte bir kişiye verebileceđi gibi, tüzel bir kişiye de verebilir<sup>828</sup>.

<sup>819</sup> TDK, Güncel Türke Sözlük, eriřim için bkz.: <https://sozluk.gov.tr/>, eriřim tarihi: 26.06.2021.

<sup>820</sup> **Maden**, s. 98. *Akdađ'a* göre kişinin bu verinin içeriđini algılayıp algılamamasının, suçun oluřması aısından bir önemi bulunmamakla birlikte; algılama olanađının sađlanması suçun oluřması için yeterli olacaktır. **Akdađ**, s. 130. Aynı yönde görüř için bkz.: **Sert**, s. 138; **Sınar**, s. 42; **Kangal**, Kişisel Veriler, s. 106.

<sup>821</sup> **Maden**, s. 98; **Akdađ**, s. 130; **Kangal**, s. 110.

<sup>822</sup> **Kangal**, Kişisel Veriler, s. 107.

<sup>823</sup> Yargıtay 12. Ceza Dairesi 2015/9893 E. ve 2016/12504 K. sayılı, 09.11.2016 tarihli kararında “SMS” yoluyla kişisel verilerin hukuka aykırı olarak üçüncü kişilere gönderimde TCK'nın 136. maddesinin uygulanması gerektiđini belirtmiřtir, (Yargıtay Bilgi Bankası), eriřim tarihi: 28.06.2021.

<sup>824</sup> Yargıtay 11. Ceza Dairesi'nin 2015/8796 E., ve 2017/5266 K. sayılı ve 10.07.2017 tarihli kararında “posta” yoluyla kişisel verilerin hukuka aykırı olarak üçüncü kişilere gönderiminde TCK'nın 136. maddesinin uygulanması gerektiđi belirtilmiřtir, (Yargıtay Bilgi Bankası), eriřim tarihi: 28.06.2021.

<sup>825</sup> **Koca / Üzülmöz**, s. 578.

<sup>826</sup> **Dülger**, Kişisel Verilerin Korunması, s. 737; **Karagülmez**, s. 451; **Erdođan**, s. 611; **Kangal**, Kişisel Veriler, s. 107; **Göçmen Uyarer**, s. 227.

<sup>827</sup> Aynı yönde görüř için bkz.: **Börekçi**, s. 78-79; **Akdađ**, s. 130; **Sert**, s. 138; Aksi yönde görüř için bkz.: **Özbek**, s. 961; **Özbek / Dođan / Bacaksız**, Özel Hükümler, s. 598. *Özbek'e* göre “*verinin bir araç kullanmaksızın kulaktan kulađa aktarılması madde kapsamına girmez, bu halde diđer unsurları da mevcutsa m. 133/3 ya da m. 134/1 düşünölmelidir.*”

<sup>828</sup> Yargıtay Ceza Genel Kurulu, 2017/12-829 E. ve 2017/363 K. sayılı, 04.07.2017 tarihli kararı, (Kazancı Bilgi Bankası), eriřim tarihi: 28.06.2021. Aynı yönde görüř için bkz.: **Dülger**, Kişisel Verilerin Korunması, s. 738; **Sert**, s. 138; **Maden**, s. 99; **Bozkurt**, Habip, Kişisel Verilerin İşlenmesinin Hukuki Boyutu, Yetkin

Doktrinde verme davranışının gerçekleşebilmesi için öncesinde kişisel verinin elde bulundurulması gerektiği savunulmuştur<sup>829</sup>. Ancak günümüzün teknolojik imkanları gözetildiğinde kişilerin hakimiyet alanında olmasa da verilerin aktarılmasına aracılık edilebilir<sup>830</sup>. Diğer bir ifade ile kişi, elde bulundurmadığı bir bilgiyi başkalarına *eriştirebilir*. Nitekim kişisel verilerin öğrenme olanağının sağlanması suçun oluşması için yeterlidir<sup>831</sup>.

### 6.1.3. Yayma

Suçun seçimlik davranışlarından bir diğeri kişisel verileri yaymaktır. Yaymak TDK'ya göre “*Birçok kimseye duyurmak, çevreye dağılmasına sebep olmak*” olarak tanımlanmaktadır<sup>832</sup>. Sözlük anlamına bakıldığında yaymanın vermeyi de kapsadığını söylemek mümkündür. Yaymak ifadesi günlük hayatta daha çok dijital ortamdaki birtakım etkinlikleri nitelemek için kullanılmaktadır<sup>833</sup>.

Esasen Hükümet Tasarısının 198. maddesinde “*ifşa*” kelimesi tercih edilmesine karşın bu kelime, TBMM Adalet Komisyonu tarafından özellikle görüntünün ifşası anlamını taşıdığı ifade edilerek “*yayma*” olarak değiştirilmiştir<sup>834</sup>. Öğretide ise vermek ve yaymak arasındaki fark daha ziyade nicelik yönünden görülmektedir<sup>835</sup>. Ancak en nihayetinde kullanılan ifade açısından kanun koyucunun bir değişikliğe gitmesi ve ifadeleri daha anlaşılabilir kılması daha isabetli olacaktır.

---

Yayımları, Ankara 2021, s. 51. **Karagülmez**, s. 451: *Karagülmez'e* göre madde metninde bu konuda bir sınırlama bulunmamasının yanında, işin esası açısından da bu yorum tarzı isabetli olacaktır. Aksi yönde görüş için bkz.: *Koca'ya* göre kişisel verilerin verilmesi durumunda ortada veriyi veren bir kişi olduğu gibi, bu veriyi alan bir kişinin de bulunmasından mütevellit, verme fiilinin icrası bakımından çok failli suç gündeme geleceğinden; bu durumda failin gerçek kişi olması gerekir. **Koca / Üzülmez**, s. 578.

<sup>829</sup> **Sert**, s. 138.

<sup>830</sup> Aynı yönde görüş için bkz.: **Maden**, s. 98; **Börekçi**, s. 81-92; **Sınar**, s. 43; **Saka / Çağlayan / Koca**, s. 382; **Sınar**, s. 43.

<sup>831</sup> **Akdağ**, s. 130.

<sup>832</sup> TDK, Güncel Türkçe Sözlük, erişim için bkz.: <https://sozluk.gov.tr/>, erişim tarihi: 26.06.2021.

<sup>833</sup> **Küzeci**, Kişisel Verilerin Korunması, s. 411.

<sup>834</sup> **Karagülmez**, s. 452.

<sup>835</sup> *Karagülmez'e* göre verme davranışında başkası tekil yapıdayken, yayma davranışında birden fazla başkasına kişisel verilerin verilmesi söz konusudur. **Karagülmez**, s. 451-452. Akdağ'a göre verinin çok ve belirsiz sayıda kişi tarafından öğrenilmesi imkanının oluşturulması, yaymaktır. **Akdağ**, s. 131. Ancak kişilerin sayısının belirsizliğinin şart olmadığını düşünmekteyim. Nitekim belirli sayıda kişiye toplu bir şekilde kısa mesaj gönderilmesi durumunda da yayma davranışı gerçekleşebilir.

Yukarıdaki ifadelerden bağımsız olarak, yayma davranışı da verme davranışı gibi mektup, internet sitesi, forum, sosyal mecralar gibi birçok yöntemle gerçekleştirilebilir<sup>836</sup>. Yargıtay Ceza Genel Kurulu bir kararında “*Kişisel verileri yayma seçimli hareketi de çeşitli şekillerde gerçekleştirilebilir. İnternet üzerindeki bir web sitesinde kişisel verileri yayınlamak, birçok kişiye elektronik posta ile ya da telefonda kısa mesajla göndermek, yazılı ya da görsel medyada yayınlamak gibi...*” ifadelerine yer vererek yaymanın çeşitli yöntemlerle gerçekleştirilebileceğini belirtmiştir<sup>837</sup>.

Yayılan bir kişisel verinin kamuya açık alanda kaydedilen ses veya görüntü olması durumunda suçun oluşup oluşmadığı noktasında görüş ayrılıkları bulunmaktadır. Bir görüş, söz konusu kişisel verilerin kamuya açık alanda kaydedilen ses veya görüntü olması durumunda suçun niteliğinin değişmeyeceğini ifade ederken<sup>838</sup>, diğer bir görüş bu durumda TCK’nın 30. maddesinin 4. fıkrası uyarınca haksızlık yanılığından faydalanılabileceğini belirtmektedir<sup>839</sup>. İkinci görüşe göre kişi, günlük yaşantısının her anında fotoğraf veya video çekip bu kayıtları yaptığı davranışın suç teşkil ettiğini bilmeden hareket ederek sosyal medya ortamında paylaşabilmektedir<sup>840</sup>. Esasen suçun niteliğinin değişmeyeceği görüşüne katılmaktayız. Nitekim burada üzerinde durulması gereken nokta, kamuya açık alanda çekilen herhangi bir hukuka uygunluk nedeninden yararlanmayan kişisel verilerin yayılması halinde ne olacağı hususudur<sup>841</sup>. Bu anlamda ikinci görüşü savunanların tespitlerine paralel bir şekilde, söz konusu davranışın haksızlık yanılığı kapsamında irdelenmesi, hatanın kaçınılmaz bir hata olup olmadığının araştırılmasının akabinde her somut olayda ayrıca ele alınması gerektiği görüşündeyiz<sup>842</sup>.

Yayma hareketi, daha geniş bir etki alanında gerçekleştiğinden, somut olayın koşullarına göre ortaya çıkacak zarar ya da tehlike açısından da fark bulunması mümkündür<sup>843</sup>.

---

<sup>836</sup> **Dülger**, *Kişisel Verilerin Korunması*, s. 739; **Sınar**, s. 44.

<sup>837</sup> Yargıtay Ceza Genel Kurulu’nun 2017/12-829 E. ve 2017/363 K. sayılı, 04.07.2017 tarihli kararı, (Kazancı Bilgi Bankası), erişim tarihi: 28.06.2021.

<sup>838</sup> *Akdağ’a göre “Kişilerin kamuya açık alanda başkalarının görülmesi hayatın olağan akışının gereğidir. Ancak bu alanlarda kayıtlarının alınması ve ifşa edilmeleri beklendik ve normal kabul edilemez.” Akdağ*, s. 131.

<sup>839</sup> **Sınar**, s. 46.

<sup>840</sup> **Sınar**, s. 46.

<sup>841</sup> Aynı yönde görüş için bkz.: **Börekeçi**, s. 83.

<sup>842</sup> **Sınar**, s. 46.

<sup>843</sup> **Börekeçi**, s. 82; **Taşkın**, s. 107.

Dolayısıyla TCK'nın 61. maddesi uyarınca yine somut olayın koşullarına göre değerlendirme yapılarak cezanın belirlenmesi gerekir.

Son olarak daha önceden de ifade edildiği üzere, yayma davranışına madde metninde yer verilip madde başlığında yer verilmemesini kanun yapma tekniği açısından yerinde bulmamaktayız<sup>844</sup>.

#### 6.1.4. Ele Geçirme

Ele geçirmek TDK'ya göre “*yakalamak, sahibi olmak, gizlenmek istenen bir şeyi elde etmek*” olarak tanımlanmaktadır<sup>845</sup>. Ele geçirme davranışıyla ilgili görüş farklılıkları, verme ve yayma davranışıyla ilgili görüş farklılıklarından daha fazladır. Bunun sebebi, kanun koyucunun “*ele geçirme*” ifadesiyle neyi kast ettiğinin net bir şekilde belirlenememesidir.

Burada incelenmesi gereken ilk husus, ele geçirmenin failin hakimiyet alanında bulunup bulunmaması (ulaşılabilir olup olmaması) gerektiğine yöneliktir. Birinci görüş, ele geçirmenin failin hakimiyet alanı dışındaki kişisel veriler için mümkün olduğunu belirtmektedir<sup>846</sup>. Bu görüşe göre normalde ulaşılabilir bir alanda bulunmayan kişisel verilere yönelik bir ele geçirme söz konusudur<sup>847</sup>. Yargıtay Ceza Genel Kurulu'nun ele geçirmeyle ilgili görüşleri de bahsedilen birinci görüş ile paraleldir<sup>848</sup>: “*Kişisel verilerin ele geçirilmesi seçimlik hareketi; kişisel verilerin kayıtlı olduğu belgelerin alınması ya da kayıtlı olduğu bilişim sisteminden ele geçirilmesi vb. şekillerde gerçekleşebilecektir. Ele geçirme fiili, başkasının hakimiyeti altında bulunan bir kişisel verinin, failin hakimiyeti altına girmesi ile gerçekleşmiş olacaktır.*” Ancak Yargıtay Ceza Genel Kurulu'nun bu karardaki görüşüne ve haliyle birinci görüşe katılmadığımızı ifade etmek isteriz. Nitekim ele geçirme davranışı yalnızca başkasının hakimiyet alanında bulunan bir kişisel verinin failin hakimiyet alanına girmesi ile gerçekleşmiş olmaz. Fail, herhangi bir

<sup>844</sup> Aynı yönde görüş için bkz.: **Böreği**, s. 85.

<sup>845</sup> TDK, Güncel Türkçe Sözlük, erişim için bkz.: <https://sozluk.gov.tr/>, erişim tarihi: 26.06.2021.

<sup>846</sup> **Akdağ**, s. 135; **Kangal**, Kişisel Veriler, s. 112-113;

<sup>847</sup> **Kangal**, Kişisel Veriler, s. 113.

<sup>848</sup> Yargıtay Ceza Genel Kurulu, 2017/12-829 E. ve 2017/363 K. sayılı, 04.07.2017 tarihli kararı, (Kazancı Bilgi Bankası), erişim tarihi: 28.06.2021.

sebepden dolayı kendi hakimiyet altında bulunan, ulaşılabilir olan bilgileri ele geçirebilir<sup>849</sup>. Örneğin bir çalışanın kendi hakimiyet alanında bulunan müşteri bilgilerini hukuka aykırı olarak şahsi elektronik cihazına aktarması da ele geçirilmedi<sup>850</sup>. Yargıtay 2014 tarihli bir kararında bilgi teknolojileri müdürü olarak çalışan kişinin müşteri bilgilerini evindeki şahsi bilgisayarına aktarmasını ele geçirme olarak değerlendirmiş, somut olayda failin işi gereği kişisel verilerin saklandığı veri tabanına ulaşılabilir olma imkanını gözetmiştir<sup>851</sup>. Görüş farklılıklarının bulunduğu ikinci husus, kişisel verinin sadece içeriğinin öğrenildiği durumlarda suçun oluşup oluşmayacağıdır. İlk görüş, önemli olanın kişinin normalde ulaşmaması gereken bir bilgiye ulaşmasının engellenmesi olduğunu belirterek öğrenme halinde de suçun sübut bulacağını belirtirken<sup>852</sup>; ikinci görüş ise yalnızca öğrenmenin suçtaki davranışı karşılamayacağını ifade etmektedir<sup>853</sup>. İkinci görüşe göre “*Örneğin bir tıp profesörü olan doktorun hastasına ilişkin sağlık bilgilerini öğrencilerine ders verdiği dokümanların arasında unutması, hocanın asistanının da dokümanları incelerken hastaya ait bilgileri görmesi ve durumu öğrenmesi halinde ele geçirme söz konusu olmaz*”<sup>854</sup>. Tartışmalı olan bu konuya bizce manevi unsur üzerinden yaklaşılmalıdır. Eğer kişinin bu bilgileri öğrenmesi, bilme ve isteme iradesiyle gerçekleşiyorsa, bu durumda öğrenme davranışı karşılayacaktır.

Ele geçirme ile kaydetme arasındaki fark doktrinde ayrıca belirtilmiştir<sup>855</sup>. Buna göre kişisel verilerin kaydedilmesi için ele geçirme dışındaki davranışlardan söz edilmesi gerekmektedir<sup>856</sup>. Yargıtay evli olan sanığın, eşi ile mağdur arasında ilişki olduğunu öğrenmesi ve bunun üzerine mağdur adına sahte sosyal medya hesabı açıp bu hesapta da mağdura ait ve mağdurun özel hayatı kapsamında sayılmayacak günlük kıyafetleri ile yer aldığı bir fotoğrafı yayınlaması üzerine vermiş olduğu bir kararda, kişisel verileri yayma ve ele geçirme suçunun oluştuğunu belirtmiştir<sup>857</sup>.

---

<sup>849</sup> Aynı yönde görüş için bkz.: **Börekçi**, s. 86.

<sup>850</sup> Aynı yönde görüş için bkz.: **Börekçi**, s. 86.

<sup>851</sup> Yargıtay 15. Ceza Dairesi'nin 2013/612 E., 2014/14715 K. sayılı ve 16.09.2014 tarihli kararı, (Yargıtay Bilgi Bankası), erişim tarihi: 28.06.2021.

<sup>852</sup> **Akdağ**, s. 136.

<sup>853</sup> **Dülger**, Kişisel Verilerin Korunması, s. 741.

<sup>854</sup> **Dülger**, Kişisel Verilerin Korunması, s. 741.

<sup>855</sup> **Göçmen Uyarer**, s. 229.

<sup>856</sup> **Özbek**, s. 961.

<sup>857</sup> Yargıtay 12. Ceza Dairesi'nin 2015/4006 E. ve 2015/18748 K. sayılı, 02.12.2015 tarihli kararı, (Yargıtay Bilgi Bankası), erişim tarihi: 28.06.2021.



Ele geçirme her ne kadar KVKK terminolojisi açısından “*devralma, aktarma, elde etme*” ile ifade edilse de kanun koyucunun bu davranışla neyi kast ettiğini saptayabilmek güçtür<sup>858</sup>. TDK’daki tanımlar doğrultusunda yola çıkıldığında ele geçirmenin tanımında yer alan anlamlara denk gelen veri işleme durumunu anlamak da zordur<sup>859</sup>. Diğer yandan, almak ifadesi de TDK’da “*ele geçirmek, fethetmek*” olarak tanımlanmıştır<sup>860</sup>. Bu tanımdan yola çıkıldığında kişisel verilerin verilmesi ve yayılmasının bir sonucu olarak bu verileri alan kişi de ele geçirmeyi gerçekleştirmektedir<sup>861</sup>. Yine bu tanımdan yola çıkılarak, ele geçirmek, başkasına ait kişisel verileri kendine aktarmak olarak da yorumlanabilmektedir<sup>862</sup>.

Son olarak, fiziki varlığı olmayan bir veri için ele geçirme ifadesinin kullanılmasını terminolojik açıdan doğru olmadığını belirtmek isteriz. Nitekim kişisel veri yakalanabilen ya da üçüncü kişi tarafından öğrenildiği takdirde bu kişi tarafından sahip olunan bir şey değildir. Örneğin bir sırrın fiziki varlığından söz edilmesi mümkün değildir. Bu doğrultuda, uygulamada yarattığı görüş ayrılıkları da gözetilerek, ele geçirme ifadesinin yerine başka bir ifade kullanılması gerekmektedir. Örneğin eğer ele geçirmekten kasıt kendine aktarmak ise, ele geçirmek yerine bu ifade kullanılabilir.

## 6.2. Netice

Netice, davranışın dış dünyada meydana getirdiği değişikliği ifade etmektedir<sup>863</sup>. Ceza hukuku anlamında netice, suçun kanuni tanımında yer alan netice olduğundan, hareketin bir sonucu olarak meydana gelen ve fakat suçun kanuni tanımında yer almayan neticeler ceza hukukunu ilgilendirmemektedir<sup>864</sup>. Ceza hukukunda kural olarak sorumluluğun kaynağı hareket olduğundan, neticeye dayalı sorumluluk için kanunda açık bir düzenleme bulunması gerekmektedir<sup>865</sup>.

<sup>858</sup> **Küzeci**, Kişisel Verilerin Korunması, s. 411.

<sup>859</sup> **Küzeci**, Kişisel Verilerin Korunması, s. 411.

<sup>860</sup> TDK, Güncel Türkçe Sözlük, erişim için bkz.: <https://sozluk.gov.tr/>, erişim tarihi: 03.08.2021.

<sup>861</sup> **Börekçi**, s. 85.

<sup>862</sup> **Artuk / Gökçen / Alşahin / Çakır**, Özel Hükümler, s. 548.

<sup>863</sup> **Özen**, s. 252; **Hakeri**, s. 149; **Centel / Zafer / Çakmut**, s. 268.

<sup>864</sup> **Özen**, s. 252; **Hakeri**, s. 149.

<sup>865</sup> **Özen**, s. 252.

Doktrinde çoğunluk görüş, her suçun bir neticesi olduğunu belirtmektedir<sup>866</sup> <sup>867</sup>. Bu görüşe göre bazı neticeler hareketten ayrılamaz, bunlar *neticesi harekete bitişik suçlar*<sup>868</sup>, *sırf davranış suçu*<sup>869</sup>, *neticesiz suçlar*<sup>870</sup> ya da *biçimsel (şekli)*<sup>871</sup> suçlar olarak isimlendirilmektedir. Neticenin zaman ve yer bakımından hareketten sonra ya da başka yerde meydana gelebildiği suçlar ise *neticesi hareketten ayrılabilen suçlar*<sup>872</sup> veya *maddi suçlar*<sup>873</sup> olarak ifade edilmektedir. Dolayısıyla burada ilk aşamada incelenmesi gereken şudur: Kanun koyucu bu suçta dış dünya değişikliğini aramakta mıdır? Diğer bir ifadeyle kişisel verileri verme, yayma veya ele geçirme suçunun oluşması için netice gerekli midir? Suçun oluşması için kanun koyucu tarafından ayrıca bir netice aranmadığından, failin seçimlik hareketlerden herhangi birini gerçekleştirilmesiyle suç tamamlanmış olur. Bu durumda suç, **neticesi harekete bitişik suçtur (sırf hareket suçu)**<sup>874</sup>.

Diğer yandan suçun tehlike suçu mu yoksa zarar suçu mu olduğunun da saptanması gerekmektedir. Suçun oluşması için hukukî anlamda bir zarar meydana gelmesinin arandığı suçlara *zarar suçu*, bunun karşısında yalnızca zarar tehlikesinin meydana gelmesiyle yetinilen suçlara ise *tehlike suçu* denilmektedir<sup>875</sup>. Bu itibarla suçun tamamlanması zamanı temel alınarak suçu oluşturan davranışın suçla korunan varlık veya menfaate zarar verip vermediğinin veya bir tehlikenin doğmasının yeterli görülüp görülmediğinin saptanması gerekmektedir<sup>876</sup>. Tehlike suçlarında, bir zarar bulunmasa dahi kanun koyucu bazı davranışları cezalandırma yoluna gitmiştir. Dolayısıyla zarar olasılığı, davranışın suç olarak tanımlanmasına yeterlidir<sup>877</sup>. Kişisel verileri verme, yayma veya ele geçirme suçunun sübut bulması için bir zararın doğması aranmamaktadır<sup>878</sup>. Bu itibarla kişisel verileri verme, yayma veya ele geçirme suçu, bir

---

<sup>866</sup> **Hakeri**, s. 149; **Centel / Zafer / Çakmut**, s. 268-269; **Özbek / Doğan / Bacaksız**, Genel Hükümler, s. 228.

<sup>867</sup> Diğer görüş için bkz.: **Özen**, dn. 347, s. 252.

<sup>868</sup> **Özgenç**, s. 191; **Özen**, s. 252; **Centel / Zafer / Çakmut**, s. 269.

<sup>869</sup> **Toroslu / Toroslu**, s. 144; **Özgenç**, s. 191; **Özen**, s. 252; **Hakeri**, s. 149.

<sup>870</sup> **Özbek / Doğan / Bacaksız**, Genel Hükümler, s. 228; **Centel / Zafer / Çakmut**, s. 269.

<sup>871</sup> **Özbek / Doğan / Bacaksız**, Genel Hükümler, s. 228; **Centel / Zafer / Çakmut**, s. 269; **Hakeri**, s. 149.

<sup>872</sup> **Centel / Zafer / Çakmut**, s. 269.

<sup>873</sup> **Özbek / Doğan / Bacaksız**, Genel Hükümler, s. 228; **Centel / Zafer / Çakmut**, s. 269; **Hakeri**, s. 149.

<sup>874</sup> **Akdağ**, s. 129; **Özbek**, s. 961, **Maden**, s. 259.

<sup>875</sup> **Centel / Zafer / Çakmut**, s. 270; **Hakeri**, s. 151.

<sup>876</sup> **Toroslu / Toroslu**, s. 144.

<sup>877</sup> **Hakeri**, s. 151, **Centel / Zafer / Çakmut**, s. 268-269.

<sup>878</sup> **Karagülmez**, s. 453.

**tehlike suçudur**<sup>879</sup>. Kanun koyucu, davranışın yapılmasının karine olarak tehlikeyi ortaya çıkardığını kabul etmektedir. Davranışın suçla korunan hukukî menfaati soyut olarak tehlikeye sokmak için elverişli olması halinde soyut tehlike suçlarından bahsedilir<sup>880</sup>. Bu itibarla kişisel verileri verme, yayma veya ele geçirme suçu bir **soyut tehlike suçudur**<sup>881</sup>. Ayrıca suç tipinde yer alan davranış ile tehlike neticesi arasında bir nedensel bağın mevcudiyetinin araştırılması zorunluluğu bulunmamaktadır<sup>882</sup>. Yargıtay Ceza Genel Kurulu da vermiş olduğu bir kararda “*Bu suçta herhangi bir neticenin gerçekleşmesi aranmadığından maddede sayılan seçimlik hareketlerin yapılmasıyla suç oluşacaktır. Bu açıdan TCK’nın 136. maddesindeki “verileri hukuka aykırı olarak verme veya ele geçirme” soyut bir tehlike suçudur.*” ifadelerine yer vermiştir<sup>883</sup>.

Hareketin yapılması veya neticenin<sup>884</sup> gerçekleşmesiyle biten suçlar *ani suç* olarak anılmaktadır<sup>885</sup>. Bu itibarla kişisel verileri verme, yayma veya ele geçirme suçu bir **ani suçtur**.

## 7. SUÇUN MANEVİ UNSURU

Kişisel verileri verme, yayma veya ele geçirme suçu kasten işlenebilen bir suç olup; davranışın taksirli hali kanunda ayıca belirtilmediğinden, özensiz ve dikkatsiz davranışlarla, diğer bir ifadeyle taksirle bu suçun işlenmesi mümkün değildir<sup>886</sup>. Ayrıca TCK’da bu suçun işlenmesinde herhangi bir amaç, saik veya maksat aranmadığından, diğer bir ifade ile özel kast aranmadığından, bu suç genel kast ile işlenebilen bir suçtur<sup>887</sup>. Ancak burada önemle belirtmek gerekir ki Yargıtay’ın birbiri ile çelişen kararları

<sup>879</sup> Akdağ, s. 129; Göçmen Uyarer, s. 227; Taşkın, s. 107; Özbek / Doğan / Bacaksız, Özel Hükümler, s. 598; Özbek, s. 961; İtişgen, s. 187.

<sup>880</sup> Centel / Zafer / Çakmut, s. 272.

<sup>881</sup> Özbek / Doğan / Bacaksız, Özel Hükümler, s. 598; Göçmen Uyarer, s. 227.

<sup>882</sup> Centel / Zafer / Çakmut, s. 271.

<sup>883</sup> Yargıtay Ceza Genel Kurulu’nun 2012/12-1510 E. ve 2014/331 K. sayılı, 17.06.2014 tarihli kararı, (Kazancı İçtihat Bilgi Bankası), erişim tarihi: 28.06.2021.

<sup>884</sup> Hakeri, s. 154.

<sup>885</sup> Centel / Zafer / Çakmut, s. 273.

<sup>886</sup> Dülger, Kişisel Verilerin Korunması, s. 741; Koca / Üzülmez, s. 580; Snar, s. 52; Börekçi, s. 92; Korkmaz, Ceza Hukuku, s. 462; Parlar / Çobanoğlu, s. 329; Göçmen Uyarer, s. 229-230; Maden, s. 115; Kangal, Kişisel Veriler, s. 120.

<sup>887</sup> Akdağ, s. 105; Karagülmez, s. 525; Taşkın, s. 108; Parlar / Çobanoğlu, s. 329; Göçmen Uyarer, s. 229; Maden, s. 115.

bulunmaktadır. Bu çelişki esasen failin asıl niyetinin kişisel verilere yönelik olmadığı; başkaca amaçlara ulaşırken kişisel verileri kullandığı durumlarda suçun oluşup oluşmayacağına ilişkindir<sup>888</sup>. Örneğin Yargıtay bir kararında “... aile birliğine yönelen saldırıyı önleme ve aile içi geçimsizliğin kaynağının katılanın güven sarsıcı olumsuz tutum ve davranışlarını olduğunu ispatlama amacını taşıyan eylemlerinde...” kişisel verilerin hukuka aykırı bir şekilde ele geçirilmesine rağmen amacın farklı olduğu gerekçesiyle yerel mahkeme tarafından verilen beraat hükmünü yerinde bulmuştur<sup>889</sup>. Ancak bunun aksine Yargıtay, bir hafta sonra verdiği kararda “...genel kastla işlenen suçta sanığın saikinin önemli olmadığı, şaka ve benzeri saiklerin kastı kaldırmayacağı, bu durumun cezanın takdirinde ve bireyselleştirilmesinde dikkate alınabileceği gözetilmeksizin, sanığa yüklenen verileri hukuka aykırı olarak verme veya ele geçirme suçu açısından sanığın kastının bulunmadığına dair yasal ve yeterli olmayan gerekçelerle...” ifadelerine yer vererek failin saikinin öneminin bulunmadığını belirtmiştir<sup>890</sup>. Suç tipinin oluşmasında saik aranmadığından, Yargıtay’ın vermiş olduğu yukarıda belirtilen ikinci kararı daha isabetli olmuştur.

Diğer yandan, suçun olası kastla işlenip işlenemeyeceği hususunda tartışmalar bulunmaktadır. Bir görüş; suçun ancak doğrudan kast ile işlenebileceğini savunurken<sup>891</sup>; diğer görüş suçun olası kast ile de işlenebileceği belirtmektedir<sup>892</sup>. Bu tartışmaların sebebi maddede belirtilen “hukuka aykırı olarak” ifadesidir. “Hukuka aykırı olarak” ifadesini tipikliğin bir unsuru olarak bulan görüşe göre<sup>893</sup> fail gerçekleştirdiği davranışın hukuka aykırı olduğunu bilmek zorunda olduğundan, bu suç olası kastla işlenememektedir<sup>894</sup>. Bu ifadenin ayrı bir önem taşımadığını ve dolayısıyla suçun olası kastla da işlenebileceğini düşünmekteyiz.

---

<sup>888</sup> **Dülger**, Kişisel Verilerin Korunması, s. 741

<sup>889</sup> Yargıtay 12. Ceza Dairesi’nin 2018/8313 E. ve 2019/8077 K. sayılı, 03.07.2019 tarihli kararı, (Kazancı İçtihat Bilgi Bankası), erişim tarihi: 28.06.2021.

<sup>890</sup> Yargıtay 12. Ceza Dairesi’nin 2018/8369 E. ve 2019/8318 K. sayılı, 10.07.2019 tarihli kararı, (Yargıtay Bilgi Bankası), erişim tarihi: 28.06.2021.

<sup>891</sup> **Koca / Üzülmez**, s. 580; **Sert**, s. 144; **İtişgen**, s. 191.

<sup>892</sup> **Özbek / Doğan / Bacaksız**, Özel Hükümler, s. 600; **Kangal**, Kişisel Veriler, s. 120.

<sup>893</sup> **Artuk / Gökçen / Alşahin / Çakır**, Özel Hükümler, s. 557; **Centel / Zafer / Çakmut**, s. 307.

<sup>894</sup> **Özgenç**, s. 321-322.

## 8. HUKUKA UYGUNLUK NEDENLERİ

Hukuka aykırılık, kanuni tipte yer alan bir davranışın tüm hukuk düzeniyle uyumsuzluk halinde bulunmasını ifade eder<sup>895</sup>. Bu nedenle hukukun izin verdiği bir davranış, aynı zamanda cezalandırılmaz<sup>896</sup>. Diğer yandan bunun bir sonucu olarak, eğer suç olarak düzenlenen bir harekete başkaca bir kuralla izin verilmişse, bu kuralın şartlarına uygun bir biçimde gerçekleştirilen davranışın hukuka aykırı olduğu sonucuna ulaşılamaz<sup>897</sup>. Bu başlıkta öncelikle madde metninde yer alan “*hukuka aykırı olarak*” ifadesinin ne anlama geldiği ele alınacak, sonrasında KVKK’daki ve TCK’daki hukuka uygunluk nedenleri ile ilgili bilgi verilecektir.

### 8.1. “Hukuka Aykırı Olarak” İfadesinin Anlamı

Bir suç tipinde “*hukuka aykırı olarak*”<sup>898</sup>, “*hukuka aykırı yollarla*”<sup>899</sup>, “*hukuka aykırı diğer davranışlarla*”<sup>900</sup> gibi ifadelerin kullanılması öğretide “*hukuka özel aykırılık*” olarak ifade edilmektedir<sup>901</sup>. Yine öğretide, bu ve benzeri ifadelerin madde metninde özellikle belirtilmesinin nedenleri ve sonuçları hakkında farklı görüşler bulunmaktadır. Bir görüşe göre bu ve benzeri ifadeler, tipikliğe ait bir unsur özelliğidir<sup>902</sup>. Bunun bağladığı sonuca göre ise bazı yazarlar; failin, cezalandırılabilmesi için özellikle hukuka aykırı olarak hareket edip etmediğinin araştırılması ve bunun ispatlanması gerektiğini ifade ederler<sup>903</sup>. Yine aynı sonuca göre bazı yazarlar ise, bununla doğrudan kastın işaret edildiğini belirtirler<sup>904</sup>. Dolayısıyla bu görüşe göre hukuka aykırı olarak vb. ifadelerin yer aldığı maddelerde fail, suçun tüm maddi unsurlarının yanı sıra eğer davranışın da hukuka aykırı olduğunu bilmiyorsa kasıtlı davrandığı kabul edilemez<sup>905</sup>. İkinci bir görüşe göre

<sup>895</sup> Katoğlu, Hukuka Aykırılık, s. 19.

<sup>896</sup> Akdağ, s. 106.

<sup>897</sup> Akdağ, s. 106.

<sup>898</sup> Örneğin TCK m. 91/2, 109/1, 120, 124/1, 124/2, 124/3, 132/2.

<sup>899</sup> Örneğin TCK m. 239/1.

<sup>900</sup> Örneğin TCK m. 235/2.

<sup>901</sup> Katoğlu, Hukuka Aykırılık, s. 122

<sup>902</sup> Artuk / Gökçen / Alşahin / Çakır, Özel Hükümler, s. 557; Centel / Zafer / Çakmut, s. 307.

<sup>903</sup> Artuk / Gökçen / Alşahin / Çakır, Özel Hükümler, s. 557; Centel / Zafer / Çakmut, s. 307.

<sup>904</sup> Özgenç, s. 321-322.

<sup>905</sup> Özgenç, s. 321

ise suç tipinde bu tür ifadelere yer verilmesiyle kanun koyucu öze ilişkin bir özelliği belirtmemekte<sup>906</sup>; hakimlere “*hukuka uygunluk nedeninin var olabileceği*” hususunda uyarıda bulunmaktadır<sup>907</sup>. Dolayısıyla burada kanun koyucunun ifade özensizliğinden bahsedilebilir<sup>908</sup>. Yargıtay vermiş olduğu bir kararda sanığın hukuka aykırılık bilinciyle hareket etmemesini suçun unsurlarının oluşmaması sonucuna bağlamıştır<sup>909</sup>. Kanaatimizce, suç tanımında “*hukuka aykırı olarak*” ifadesinin kullanılması isabetsizdir. Esasen bu durum zaten TCK’nın hataya ilişkin düzenlemelerinde yer almaktadır. Şöyle ki; TCK’nın 30. maddesinin 4. fıkrasına göre “*İşlediği fiilin haksızlık oluşturduğu hususunda kaçınılmaz bir hataya düşen kişi, cezalandırılmaz.*” Dolayısıyla fail davranışı hukuka aykırı bir bilinçle yapmıyorsa bu durum hataya ilişkin hükümlerde çözümlenmelidir. Ayrıca madde metninde veya başlığında “*hukuka aykırı olarak*” vb. ifadelerin kullanılmasına gerek yoktur.

## **8.2. KVKK’daki ve TCK’daki Hukuka Uygunluk Nedenleri**

TCK’nın 5. maddesinin karşısında özel bir kanun olan KVKK’nın, TCK’daki genel hükümlerde yer hukuka uygunluk nedenlerinden farklı nedenler getirebileceği yukarıda belirtilmişti<sup>910</sup>. Bu doğrultuda, özel ve genel norm ilişkisinin bir sonucu olarak KVKK’daki hukuka uygunluk nedenleri ve genel hukuka uygunluk nedenleri şeklinde bir ayırım yapılması mümkündür. KVKK’nın özel bir düzenleme olmasının getirdiği bir sonuç olarak; davranışın KVKK kapsamında bir veri işleme olması durumunda KVKK’daki hukuka uygunluk nedenleri uygulanacaktır. Davranışın KVKK kapsamında bir veri işleme olmaması durumunda ise TCK’daki genel hukuka uygunluk nedenleri uygulanacaktır. Hukuka uygunluk nedenleri çalışmanın sistematığı açısından II. bölümde detaylıca ele alınıp incelendiğinden, bu başlıkta tekrar olmaması için yalnızca hatırlatma yapılacaktır.

---

<sup>906</sup> Akdağ, s. 110.

<sup>907</sup> Dülger, Kişisel Verilerin Korunması, s. 705-707.

<sup>908</sup> Katoğlu, Hukuka Aykırılık, s. 124-125.

<sup>909</sup> Yargıtay 12. Ceza Dairesi’nin 2014/17630 E. ve 2015/1672 K. sayılı, 02.02.2015 tarihli kararı, (Kazancı Bilgi Bankası), erişim tarihi: 28.06.2021.

<sup>910</sup> Çalışmanın II. bölüm 2.2. başlığı.

TCK'da düzenlenen hukuka uygunluk nedenleri ilgilinin rızası, kanun hükmünün veya amirin emrinin yerine getirilmesi, meşru savunma, hakkın kullanılması ve zorunluluk halidir. KVKK'da düzenlenen hukuka uygunluk nedenlerinde ise ikili bir ayırım yapılması mümkündür. Nitekim KVKK'da kişisel veriler ve özel nitelikli kişisel verilerin veri işleme hukukî sebepleri farklı belirtilmiştir. Bu kapsamda kişisel veriler KVKK'nın 5. ve 6. maddelerinde belirtilen hukukî sebeplerin varlığı halinde işlenebilir. Bunlar 5. maddeye göre açık rıza, kanunlarda açıkça öngörülme, fiili imkânsızlık veya zorunluluk hali, sözleşmenin kurulması veya ifası, alenileştirme, bir hakkın tesisi, kullanılması veya korunması, hukukî yükümlülüğün yerine getirilmesi ve meşru menfaattir. Ancak anılan hukuka uygunluk nedenlerinin her birinin kendi içerisinde barındırması gereken kriterler yer almaktadır. 6. maddede ise özel nitelikli kişisel verilere özgü hukuka uygunluk nedenleri belirtilmiştir. Maddeye göre özel nitelikli kişisel veriler ilgilinin açık rızasıyla ya da kanunlarda öngörülmeye işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel verilerin işlenmesinde kanunlarda öngörülme yerine bir de amaç ve kişi yönünden sınırlama getirilmiştir.

Kişisel verileri verme, yayma veya ele geçirme suçu için en önemli hukuka uygunluk nedenlerinden bir tanesi rızadır. Önemli olmasının sebebi, ilgilinin rızasının hiyerarşik olarak diğer hukuka uygunluk nedenlerinden daha üstün durumda olması değil hem Anayasa'da hem TCK'da hem de KVKK'da rızaya yapılan vurgudur<sup>911</sup>.

KVKK'daki hukuka uygunluk nedenleriyle karşılaştırılacak nitelikte olmamasından dolayı daha önceki bölümde yer verilmeyen meşru savunma (yasal savunma) açısından da değerlendirme yapılması isabetli olacaktır. Meşru savunmanın bir hukuka uygunluk nedeni olarak sayılabilmesi için taşıması gereken bazı şartlar bulunur. Öncelikle bir saldırı olmalı, bu saldırı haksız olmalı, saldırının gerçekleştiği değer kişinin doğrudan özgürce tasarruf edebileceği bir değer olmalı, savunma saldırgana karşı yapılmalı, saldırı ile savunma arasında orantı bulunmalıdır<sup>912</sup>. Kişisel verileri verme, yayma veya ele geçirme suçu açısından meşru savunma çok sık rastlanılabilecek bir hukuka uygunluk nedeni değildir<sup>913</sup>.

---

<sup>911</sup> Börekçi, s. 97.

<sup>912</sup> Soyaslan, s. 390 vd., Hakeri, s. 384 vd.

<sup>913</sup> Kangal, Kişisel Veriler, s. 124.

## 9. KUSURLULUĞU ETKİLEYEN HALLER

Kusuru etkileyen haller ile ilgili olarak KVKK'da ayrıca bir düzenleme mevcut değildir. Ancak TCK'nın kusur yeteneğini etkileyen yaş küçüklüğü (31. madde), akıl hastalığı (32. madde), sağır ve dilsizlik (33. madde) ve geçici nedenler, alkol veya uyuşturucu madde etkisi altında olma (34. madde) durumlarına ilişkin genel hükümlerin kişisel verilerin verilmesi, yayılması veya ele geçirilmesi suç tipinde uygulanacağı hususunda şüphe bulunmamaktadır<sup>914</sup>.

TCK'nın 31. maddesine göre fiili işlediği sırada on iki yaşını doldurmamış olan çocukların ceza sorumluluğu bulunmamakla birlikte, bu kişiler hakkında ceza kovuşturması yapılamamaktadır. Ancak bu kişiler hakkında çocuklara özgü güvenlik tedbirleri uygulanabilmektedir. Çocuklara özgü güvenlik tedbirleri 5395 sayılı Çocuk Koruma Kanunu'nda<sup>915</sup> yer almaktadır. Fiili işlediği sırada on iki yaşını doldurmuş olup, on beş yaşını doldurmamış olanlar açısından ise ceza sorumluluğunun belirlenmesinde bu kişilerin işlediği fiilin hukukî anlam ve sonuçlarını algılayıp algılamaması veya davranışlarını yönlendirme yeteneğinin yeterince gelişmiş olup olmaması dikkate alınmaktadır. Eğer çocuk, işlediği fiilin hukukî anlam ve sonuçlarını algılayabiliyor ve bu fiille ilgili olarak davranışlarını yönlendirme yeteneğini haiz ise, cezasında indirim yapılmaktadır. Fiili işlediği sırada on beş yaşını doldurmuş olup da on sekiz yaşını doldurmamış olan çocuklar içinse algılama veya yönlendirme yeteneğine ilişkin bir değerlendirme yapılmamıştır. Ancak bu kişiler hakkında verilecek hapis cezasında indirim yapılmaktadır.

TCK'nın 32. maddesinde göre, akıl hastalığı nedeniyle, işlediği fiilin hukukî anlam ve sonuçlarını algılayamayan veya bu fiille ilgili olarak davranışlarını yönlendirme yeteneği önemli derecede azalmış olan kişilere ceza verilmemekte; ancak bu kişiler hakkında güvenlik tedbirlerine hükmolunmaktadır. Akıl hastalıklarına özgü güvenlik tedbirleri, TCK'nın 57. maddesinde düzenlenmiştir. İşlediği fiille ilgili olarak davranışlarını

---

<sup>914</sup> Kangal, Kişisel Veriler, s. 131.

<sup>915</sup> TCK'nın "Çocuklara özgü güvenlik tedbirleri" başlıklı 56. Maddesinde çocuklara özgü güvenlik tedbirlerinin neler olduğunun ve ne suretle uygulanacaklarının ilgili kanunda gösterileceği belirtilmiştir. İlgili kanun, 15.07.2005 sayılı ve 25876 tarihli Resmî Gazete'de yayımlanan 5395 sayılı Çocuk Koruma Kanunu'dur.



yönlendirme yeteneği azalmış olan<sup>916</sup> kişi hakkında verilecek hapis cezasında indirim yapılmaktadır.

TCK'nın 33. maddesine göre ise fiili işlediği sırada on beş yaşını doldurmamış sağır ve dilsizler hakkında fiili işlediği sırada on iki yaşını doldurmamış olan çocuklara ilişkin hükümler; on beş yaşını doldurmuş olup da on sekiz yaşını doldurmamış olan sağır ve dilsizler hakkında on iki yaşını doldurmuş olup da on beş yaşını doldurmamış olanlara ilişkin hükümler; on sekiz yaşını doldurmuş olup da yirmi bir yaşını doldurmamış olan sağır ve dilsizler hakkında ise on beş yaşını doldurmuş olup da on sekiz yaşını doldurmamış olanlara yönelik hükümler uygulanmaktadır.

Son olarak, TCK'nın 34. maddesi uyarınca, geçici bir nedenle ya da irade dışı alınan alkol veya uyuşturucu madde etkisiyle, işlediği fiilin hukukî anlam ve sonuçlarını algılayamayan veya bu fiille ilgili olarak davranışlarını yönlendirme yeteneği önemli derecede azalmış olan kişilere ceza verilmemektedir. Ancak alkolün veya uyuşturucu maddenin iradi bir şekilde alınması halinde bu etkiyle suç işleyen kişiler hakkında bu hüküm uygulanmayacaktır. Geçici nedenler, akıl hastalığı düzeyine ulaşmayan; ancak geçici nitelikte herhangi bir patolojik nedenin kişinin kusur yeteneğini etkileyen (örneğin hipnotizma, uyur-gezerlik, ateşli hastalık gibi) hallerdir<sup>917</sup>.

## 10. SUÇUN ÖZEL GÖRÜNÜŞ ŞEKİLLERİ

### 10.1. Teşebbüs

Failin işlemek için istediği suçun icra hareketlerine başladığı veya hareketleri tamamladığı, suçun ve kullanılan araçların da elverişli olması halinde failin elinde bulunmayan sebeplerle icra hareketlerinin tamamlanamadığı veya neticenin meydana gelmediği durumlar suça teşebbüs olarak tanımlanır<sup>918</sup>. Kişisel verileri verme, yayma veya ele geçirilmesi suçunda hareket parçalara bölünebiliyorsa suç teşebbüse

<sup>916</sup> Tam ve kısmî akıl hastalığı kavramları ve buna bağlanan sonuçlar için bkz.: **Centel / Zafer / Çakmut**, s. 422-426.

<sup>917</sup> **Özbek / Doğan / Bacaksız**, Genel Hükümler, s. 372.

<sup>918</sup> **Centel / Zafer / Çakmut**, s. 453.

elverişlidir<sup>919</sup>. Örneğin failin kişisel verileri posta yoluyla gönderdiği durumlarda postanın muhatabına ulaşmaması halinde teşebbüsten söz edilebilir<sup>920</sup>. Diğer yandan, failin kişisel verilerin bulunduğu odaya girip kilitli dolabı açmaya çalışması teşebbüs olarak değerlendirilebilir<sup>921</sup>. Yine, örneğin, failin kişisel verilerin yer aldığı veri tabanına ulaştığı; ancak veri tabanı içerisinde herhangi bir bilgiyi edinmeden yakalanması durumunda teşebbüs söz konusu olabilir<sup>922</sup> <sup>923</sup>. Aynı örnekte, eğer ki fail kişisel verinin içeriğini öğrenmeden icra hareketlerine devam etmekten cayarsa TCK'nın 36. maddesi uyarınca gönüllü vazgeçme hükümleri uygulanacaktır<sup>924</sup>. Bu durumda fail, kişisel verileri ele geçirmeye teşebbüsten değil, cayma zamanına kadar gerçekleştirdiği davranış açısından TCK'nın 243. maddesinde yer alan “*Bilişim sistemine girme suçu*” sübut bulduğundan, bu suçtan sorumlu olacaktır<sup>925</sup>. Yargıtay, sanıkların kredi kartlarının manyetik şeritlerini kopyaladığı somut olayda; suç işlemek amacıyla ATM'ye koydukları hafıza kartında kişisel veriler varsa kişisel verilerin verilmesi ve ele geçirilmesi suçunun oluşacağını; ancak hafıza kartında kişisel veriler bulunmuyorsa bu durumda suça teşebbüsün söz konusu olacağını belirtmiştir<sup>926</sup>.

---

<sup>919</sup> Maden, s. 117; Sınar, s. 57; Göçmen Uyarer, s. 232; Koca / Üzülmöz, s. 582; Taşkın, s. 108. Bu suçun hareketlerinin suçun neticesi ile bitişik olduğunu ve bu sebepten teşebbüs elverişli olmadığını savunan görüş için bkz.: Özbek / Doğan / Bacaksız, Özel Hükümler, s. 601; Özbek, s. 962.

<sup>920</sup> Koç, s. 72.

<sup>921</sup> Akdağ, s. 139.

<sup>922</sup> İtişgen, s. 195. Sınar'a göre “*Bu olasılık yalnızca hukuka uygun olarak ele geçirilen kişisel verilerin başkasına verilmesi veya yayılması yönünden geçerlidir. Çünkü eğer söz konusu kişisel veriler önceden hukuka aykırı olarak ele geçirilmişse zaten bu ele geçirme hareketi ile suç tamamlanmış olacağı için sonraki verme veya yayma hareketleri yönünden teşebbüse elverişlilik söz konusu olmaz.*”, Sınar, s. 57; Sınar ile aynı yönde görüş için bkz.: Kangal, Kişisel Veriler, s. 134.

<sup>923</sup> Akdağ'a göre “*bu durumda failin saikine bakılması gerekir. Nitekim failin sisteme giriş amacı kişisel verileri ele geçirmekse ve fail elinde olmayan sebeplerle amacına ulaşamamışsa, tamamlanmış bir sisteme girme suçu değil, teşebbüs aşamasında kalmış bir kişisel verileri ele geçirme söz konusu olur. Tamamlanmış bilişim sistemine girme suçuyla, bilişim sistemindeki veriyi ele geçirmeye teşebbüsü birbirinden ayıracak olan failin manevi unsurudur.*” Akdağ, s. 140.

<sup>924</sup> Sınar, s. 57.

<sup>925</sup> Akdağ, s. 140.

<sup>926</sup> Yargıtay 8. Ceza Dairesi'nin 2016/12565 E. ve 2017/12892 K. sayılı, 20.11.2017 tarihli kararı, (Lexpera), erişim tarihi: 27.09.2021.

## 10.2. İştirak

Kişisel verilerin verilmesi, yayılması veya ele geçirilmesi suçu iştirak açısından bir özellik göstermemektedir. Dolayısıyla bu suçun iştirak halinde işlenebilmesi mümkündür<sup>927</sup>.

Bir suç tipindeki haksızlığı tek başına gerçekleştiren kişi, doğrudan fail olarak ifade edilmektedir<sup>928</sup>. Ancak failliğin müşterek ve dolaylı olmak üzere iki görünümü vardır<sup>929</sup>. TCK'nın 37. maddesinin 1. fıkrasına göre *“Suçun kanuni tanımında yer alan fiili birlikte gerçekleştiren kişilerden her biri, fail olarak sorumlu olur.”* Böylelikle suçun işlenişi üzerinde beraber hakimiyet kurarak suçu işleyen kişiler müşterek fail olarak sorumlu tutulacak ve müşterek faillerin her biri ayrıca cezalandırılacaktır<sup>930</sup>. Suçun iştirak halinde işlenebilmesi için faillerin seçimlik hareketleri birbirleri ile anlaşmalı şekilde icra etmeleri gerekir<sup>931</sup>. Nitekim eğer faillerin birlikte suç işleme kastı bulunmuyorsa her failin bağımsız olarak bu suçu işlediği sayılır<sup>932</sup>. Faillerin sorumluluğunu belirlemek için iradelerine ve anlaşmalarının bulunup bulunmadığına bakılması gerekir<sup>933</sup>. Diğer yandan TCK'nın 37. maddesinin 2. fıkrasına göre *“Suçun işlenmesinde bir başkasını araç olarak kullanan kişi de fail olarak sorumlu tutulur.”* Bu durumda dolaylı faillik söz konusu olacaktır<sup>934</sup>.

Kişisel verileri verme, yayma veya ele geçirme suçunda iştirak durumunun daha iyi anlatılabilmesi için örnek üzerinden gidilmesi faydalı olacaktır: Fail (A), kendisinden para sakladığını düşündüğü eşinin banka hesap döküm özetine erişerek harcamalarını kontrol etmek ve maddi durumunu öğrenmek ister, bu isteğini gerçekleştirmek için yakın arkadaşı (B) ile plan yapar. (B), kendisini (A)'nın eşi olarak tanıtarak bankadan (A)'nın eşine ait altı aylık hesap döküm özetini elde edip kayıtları (A)'ya teslim eder. Bu örnekte (A) ve (B) aynı suçu işlemek için beraber hareket etmektedir ve TCK'nın 37. maddesinin

---

<sup>927</sup> Koca / Üzülmüş, s. 582; Göçmen Uyarer, s. 233; Parlar / Çobanoğlu, s. 329; Kangal, s. 135; Börekçi, s. 160; Göçmen Uyarer, s. 233; Özbek / Doğan / Bacaksız, Özel Hükümler, s. 601.

<sup>928</sup> Hakeri, s. 512.

<sup>929</sup> Hakeri, s. 512.

<sup>930</sup> Hakeri, s. 513.

<sup>931</sup> Göçmen Uyarer, s. 233.

<sup>932</sup> Göçmen Uyarer, s. 233.

<sup>933</sup> Akdağ, s. 141.

<sup>934</sup> Hakeri, s. 519.

1. fıkrası uyarınca müşterek faillikten hüküm kurulması gerekmektedir. Nitekim Yargıtay da aynı fikirdedir<sup>935</sup>.

Aynı örnek üzerinden; bankada çalışan kişiler, (A)'nın eşine ait hesap döküm özetine ilişkin bilgileri (B)'ye vermiş, dolayısıyla (B) tarafından araç olarak kullanılmıştır. Bankada çalışan kişiler doğru kişiyle konuştukları bilinciyle hareket ettikleri için, kişisel verileri verme, yayma veya ele geçirme suçunu işlemeye yönelik özgür iradeleri ve kasıtları yoktur. Dolayısıyla banka yetkililerinin söz konusu suç için cezai sorumluluğu bulunmamaktadır. (B) ise bu örnekte dolaylı fail olacaktır.

Diğer yandan azmettirenin hukukî durumunun da incelenmesi gerekmektedir. Azmettirme, bir kişinin suç işleme kararı almasını ana etken olarak sağlamaktır<sup>936</sup>. TCK'nın 38. maddesinin 1. fıkrası uyarınca "*Başkasını suç işlemeye azmettiren kişi, işlenen suçun cezası ile cezalandırılır.*" Örneğin TCK'nın 136. maddesine uygun olmayan şirket politikaları doğrultusunda çalışanlarını suç işleme kararına iten işveren şirket politikalarını belirleme dolayısıyla azmettiredir<sup>937</sup>. Dolaylı faillikte bir iştirak iradesi bulunmamasına karşın azmettirilende bir iştirak iradesi bulunmaktadır<sup>938</sup>. Faillik ve azmettirmenin dışında kalan; ancak suçun oluşması için nedensellik değeri taşıyan hareketler, şeriklik olan yardım etmeyi ifade etmektedir<sup>939</sup>. Yardım etme, TCK'nın 39. maddesinde düzenlenmiş olup, fiilin işlenmesinde kullanılan araçları sağlama, yol gösterme, kolaylaştırma (maddi yardım) ve suç işlemeye yöneltme (teşvik, kuvvetlendirme, vaat) şeklinde gerçekleşebilir<sup>940</sup>. Kişisel verileri verme, yayma veya ele geçirme suçuna yardım etmek mümkündür. Bu durumda yardım edenin cezasının yarısı indirilecektir.

Kişisel verileri hukuka uygun bir şekilde elinde bulunduran bir kişinin cebir veya tehdit sonucu bunları bir başkasına vermeye veya yaymaya mecbur edilmesi halinde, zorunluluk

---

<sup>935</sup> "*Haberleşme sürecinin taraflarını ve zamanını gösteren bilgiler, "kişisel veri" kapsamında olup, katılan ...'nin ne zaman kiminle hangi sıklıkla ve ne kadar süreyle görüştüğüne ilişkin kişisel verilerinin yazılı olduğu belgeleri hukuka aykırı olarak ele geçiren ve birlikte hareket eden sanıklar hakkında, TCK'nın 37/1. maddesi yollamasıyla aynı Kanun'un 136/1. maddesindeki verileri hukuka aykırı olarak verme veya ele geçirme suçundan dolayı mahkumiyet kararı verilmesine ilişkin yerel mahkemenin kabulünde bir isabetsizlik görülmemiştir.*" Yargıtay 12. Ceza Dairesi'nin 2015/10994 E., 2017/635 K. sayılı ve 01.02.2017, (Yargıtay Bilgi Bankası), erişim tarihi: 28.09.2021.

<sup>936</sup> **Hakeri**, s. 525.

<sup>937</sup> **Börekcı**, s. 164.

<sup>938</sup> **Hakeri**, s. 531.

<sup>939</sup> **Hakeri**, s. 533.

<sup>940</sup> **Hakeri**, s. 534, 536.

halinin bulunmasından dolayı bir hukuka uygunluk nedeninin varlığından bahsedilebilir<sup>941</sup>. Yine, kişisel verileri hukuka uygun bir şekilde elinde bulunduran bir kişinin bunları vermesi veya yayması için hileyle suçun maddi unsurlarında hataya düşmesi halinde kast ortadan kalkacağından, bu kişi sorumlu tutulamayacaktır<sup>942</sup>.

Son olarak, suça iştirak edenlerin nitelikli hallerine ilişkin şartları taşıması durumunda bu kişilerin cezasında artırım uygulanacaktır<sup>943</sup>.

### 10.3. İçtima

Kişisel verilerin korunması hakkının birçok hak ile yakından ilişkili olmasından ve kişisel veri kavramının sınırlarının tam anlamıyla belirlenememesinden dolayı, kişisel verileri verme, yayma veya ele geçirme suçunun incelenmesinde içtima meselesi oldukça önemlidir. Ancak kişisel verileri verme, yayma veya ele geçirme suçunun ilgili diğer suç tipleri ile içtimasına geçmeden önce, TCK'nın 43. maddesi açısından zincirleme suç hükümlerine yönelik inceleme yapılacaktır.

#### 10.3.1. TCK'nın 43. Maddesi Açısından İnceleme

TCK'nın 43. maddesinin 1. fıkrasına göre “*Bir suç işleme kararının icrası kapsamında, değişik zamanlarda bir kişiye karşı aynı suçun birden fazla işlenmesi durumunda, bir cezaya hükmedilir. Ancak bu ceza, dörtte birinden dörtte üçüne kadar artırılır. Bir suçun temel şekli ile daha ağır veya daha az cezayı gerektiren nitelikli şekilleri, aynı suç sayılır.*” Dolayısıyla aynı kişiye karşı farklı zamanlarda bu suçun tanımında yer alan hareketlerin gerçekleştirilmesi halinde TCK'nın 43. maddesinin 1. fıkrasındaki zincirleme suç hükümleri uygulanıp tek bir cezaya hükmedilecek; ancak verilecek ceza dörtte birinden dörtte üçüne kadar artırılacaktır. Örneğin failin sevmediği bir arkadaşının

<sup>941</sup> Kangal, Kişisel Veriler, s. 136.

<sup>942</sup> Kangal, Kişisel Veriler, s. 137.

<sup>943</sup> Dülger, Kişisel Verilerin Korunması, s. 748.

kişisel verilerini ele geçirip bunları üçer günlük periyotlarla sosyal medya hesabından yayması durumunda TCK'nın 43. maddesinin 1. fıkrası hükümleri uygulanacaktır.

TCK'nın 43. maddesinin 2. fıkrasına göre ise; “*Aynı suçun birden fazla kişiye karşı tek bir fiille işlenmesi durumunda da birinci fıkra hükmü uygulanır.*” Dolayısıyla failin tek bir hareketle birden fazla kişinin kişisel verisini hukuka aykırı olarak vermesi, yayması veya ele geçirmesi durumunda da zincirleme suç hükümleri uygulanacak; verilecek ceza dörtte birinden dörtte üçüne kadar artırılabilecektir. Örneğin bir banka görevlisinin müşteri bilgilerini tek bir e-posta ile şahsi e-posta hesabına aktarması durumunda suç, tek bir davranış ile birden fazla kişiye karşı işlenmiş olacaktır<sup>944</sup>. Yargıtay vermiş olduğu bir kararında “*ATM cihazına yerleştirdiği kart kopyalama ve kamera düzenekleri ile cihazda işlem yapan kişilere ait kartların manyetik şerit bilgilerini ve şifrelerini hukuka aykırı olarak ele geçirmekten ibaret eyleminin, zincirleme şekilde verileri hukuka aykırı olarak verme veya ele geçirme suçunu oluşturduğuna dair yerel mahkemenin ...*” ifadelerini kullanmış, somut olayda TCK'nın 43. maddesinin 2. fıkrası hükümlerinin uygulanması gerektiğini belirtmiştir<sup>945</sup>.

### 10.3.2. TCK'da Düzenlenen Diğer Suç Tipleri ile Olan İçtima İlişkisi

Kişisel verileri verme, yayma veya ele geçirme suçuna ilişkin suçların içtimasında özel bir düzenlemenin bulunmaması sebebiyle, suçların içtimasına ilişkin TCK'daki genel hükümlerin uygulanması gerekmektedir<sup>946</sup>.

---

<sup>944</sup> **Börekçi**, s. 149.

<sup>945</sup> Yargıtay 12. Ceza Dairesi'nin 2015/13192 E. ve 2017/3451 K. sayılı, 26.04.2017 tarihli kararı, (Yargıtay Bilgi Bankası), erişim tarihi: 26.06.2021.

<sup>946</sup> **Koca / Üzülmüş**, s. 233; **Korkmaz**, Ceza Hukuku, s. 410.

### 10.3.2.1. Haberleşmenin Gizliliğini İhlal ve Kişiler Arasındaki Konuşmaların Dinlenmesi ve Kayda Alınması Suçları

Haberleşmenin gizliliğini ihlal suçu TCK'nın 132. maddesinde, kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması suçu ise TCK'nın 133. maddesinde aşağıdaki şekillerde düzenlenmiştir:

#### ***“Haberleşmenin gizliliğini ihlal Madde 132-***

*(1) Kişiler arasındaki haberleşmenin gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Bu gizlilik ihlali haberleşme içeriklerinin kaydı suretiyle gerçekleşirse, verilecek ceza bir kat artırılır.*

*(2) Kişiler arasındaki haberleşme içeriklerini hukuka aykırı olarak ifşa eden kimse, iki yıldan beş yıla kadar hapis cezası ile cezalandırılır.*

*(3) Kendisiyle yapılan haberleşmelerin içeriğini diğer tarafın rızası olmaksızın hukuka aykırı olarak alenen ifşa eden kişi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur.*

#### ***Kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması Madde 133-***

*(1) Kişiler arasındaki aleni olmayan konuşmaları, taraflardan herhangi birinin rızası olmaksızın bir aletle dinleyen veya bunları bir ses alma cihazı ile kaydeden kişi, iki yıldan beş yıla kadar hapis cezası ile cezalandırılır.*

*(2) Katıldığı aleni olmayan bir söyleşiyi, diğer konuşanların rızası olmadan ses alma cihazı ile kayda alan kişi, altı aydan iki yıla kadar hapis veya adli para cezası ile cezalandırılır.*

*(3) Kişiler arasındaki aleni olmayan konuşmaların kaydedilmesi suretiyle elde edilen verileri hukuka aykırı olarak ifşa eden kişi, iki yıldan beş yıla kadar hapis ve dörtbin güne kadar adli para cezası ile cezalandırılır. İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur.”*

Bu suçlar ile kişisel verileri verme, yayma veya ele geçirme suçları arasındaki içtima sorununun çözümü konusunda farklı görüşler bulunmaktadır. İlk görüşe göre TCK'nın 132/2., 132/3. ve 133/3. maddelerinde yer alan ifşa etme suç tipi ile kişisel verileri verme,

yayma veya ele geçirme suç tipi örtüşmekte; haliyle fail, tek bir davranış ile her iki suçu işleyebilmektedir<sup>947</sup>. İkinci görüşe göre ise anılan suçlar arasında özel-genel hüküm ilişkisi bulunduğundan, TCK'nın 132/2., 132/3. ve 133/3. maddelerinde belirtilen davranışların gerçekleştiği durumlarda özel normun önceliği gereğince TCK'nın 136. maddesi uygulanmayacaktır<sup>948</sup>.

Ne var ki, bu düzenlemeler arasında genel hüküm – özel hüküm ilişkisinin bulunmadığı düşünülmektedir. Nitekim genel hüküm – özel hüküm ilişkisinin bulunması için, özel hüküm niteliğindeki düzenlemede, genel hükmün bütün unsurlarına yer verilmesi ve bunun yanında ek birtakım koşulların da karşılanmasının aranması gerekir<sup>949</sup>. Diğer bir ifadeyle, özel hüküm olmasaydı genel hüküm uygulanabilecekti sonucuna varılabiliyor ise bu ilişkinin varlığından bahsedilebilir<sup>950</sup>. Yukarıda ele alınan düzenlemeler incelendiğinde bu durum söz konusu olmadığından, anılan maddelerdeki suç tipleri ile kişisel verileri verme, yayma veya ele geçirme suçu arasında fikri içtima hükümleri uygulanmalı ve fail sadece en ağır cezayı gerektiren 136. maddeden sorumlu tutulmalıdır<sup>951</sup>.

### 10.3.2.2. Özel Hayatın Gizliliğini İhlal Suçu

Kişisel verilerin korunması hakkının kaynağını büyük ölçüde özel hayatın gizliliğinden almasından dolayı TCK'nın 134. maddesinde düzenlenen suç tipi ile kişisel verileri verme, yayma veya ele geçirme suç tipi, uygulamada kimi zaman birbirinden ayırt edilmesi zor olan suç tipleridir. Öğretide özel hayatın gizliliğini ihlal suçunun özel hayat ile ilgili suçlar bakımından torba suç olduğu ifade edilmektedir<sup>952</sup>. Buna bağlanan sonuç, özel hayatın gizliliğini koruyan diğer suç tipleri ile TCK'nın 134. maddesi arasında genel hüküm – özel hüküm ilişkisinin kurulması ve özel hüküm olan suç tipindeki şartlar sağlandığı takdirde TCK'nın 134. maddesinden hüküm tesis edilmesidir. Dolayısıyla bu

<sup>947</sup> Korkmaz, Ceza Hukuku, s. 479 vd.; Gültekin, s. 172.

<sup>948</sup> Akdağ, s. 142-143.

<sup>949</sup> Hakeri, s. 588; Özen, s. 732.

<sup>950</sup> Özen, s. 732.

<sup>951</sup> Börekçi, s. 151.

<sup>952</sup> Akyürek, Güçlü, *Özel Hayatın Gizliliğini İhlal Suçu*, Seçkin Yayıncılık, Ankara – 2014, s. 319.



görüŖe göre TCK'nın 136. maddesi özel hüküm olmakta ve uygulama imkânı bulunmadığında TCK'nın 134. maddesine gidilmelidir<sup>953</sup>. Buna karşılık, verilen, yayılan veya ele geçirilen bilgilerin kişisel veri olarak kabul edilmesi durumunda TCK'nın 134. maddesinden değil, TCK'nın 136. maddesinden hüküm kurulması gerekmektedir<sup>954</sup>. Başka bir görüş ise TCK'nın 136. maddesinin uygulanabilmesi için hareketin TCK'nın 134. maddesine girmemesi gerektiğini savunmaktadır<sup>955</sup>. Yargıtay istikrarlı kararlarında eğer bir hareket hem 134. madde hem de 136. madde açısından suç teşkil ediyorsa suçun konusunun “özel hayata ilişkin” olması durumunda 136. maddedeki suçun oluşmayacağını belirtmektedir<sup>956</sup>: “Bir özel hayat görüntüsü ya da sesinin, “kişisel veri” olduğunda kuşku bulunmamakta ise de, kişinin özel hayatına dair görüntüsü ya da sesinin, bilgisi dışında, resim çekme veya kaydetme özelliğine sahip aletle belli bir elektronik, dijital, manyetik yere sabitlenmesi TCK'nın 134/1.maddesinin 2.cümlesinde; rızası dışında ifşa edilmesi, yani; yayılması, açığa vurulması, afişe edilmesi, ilan edilmesi, kamuoyuna duyurulması, aleniyet kazandırılması, özetle içeriği öğrenme yetkisi bulunmayan kişi veya kişilerin bilgisine sunulması TCK'nın 134/2.maddesinde özel hayatın gizliliğini ihlal suçu kapsamında düzenlendiğinden, kişinin özel hayatına dair görüntüsü ya da sesi, yasal anlamda, TCK'nın 136/1.maddesi kapsamında kişisel veri olarak değerlendirilemez.” Ayrıca Yargıtay, 2020 tarihli bir kararında “Kişisel verileri verme, yayma veya ele geçirme suçunun uygulama alanının amaçlanandan fazla genişletilerek, uygulamada belirsizlik ve hemen her eylemin suç oluşturması gibi olumsuz sonuçların doğmaması için, somut olayın özellikleri dikkate alınarak titizlikle değerlendirme yapılması...” ifadelerini kullanarak kişisel verileri verme, yayma veya ele geçirme suçunun dar bir şekilde ele alınması gerektiğini belirtmiştir<sup>957</sup>.

TCK'nın 136. maddesinin var olmasa bile TCK'nın 134. maddesinin uygulanacağını söylemek güçtür<sup>958</sup>. Nitekim artık kişisel verilerin korunması hakkı, özel hayatın gizliliği

---

<sup>953</sup> Börekçi, s. 152.

<sup>954</sup> Kangal, Kişisel Veriler, s. 141; Akyürek, s. 319-320.

<sup>955</sup> Yaşar / Gökcan / Artuç, s. 4444.

<sup>956</sup> Yargıtay 12. Ceza Dairesi'nin 2015/9893 E. ve 2016/12504 K. sayılı 09.11.2016 tarihli kararı, (Yargıtay Bilgi Bankası), erişim tarihi: 28.06.2021. Diğer örnek kararlar için bkz.: Yargıtay 12. Ceza Dairesi'nin 2019/894 E. ve 2020/845 K. sayılı, 22.01.2020 tarihli kararı (Kazancı İçtihat Bilgi Bankası), Yargıtay 12. Ceza Dairesi'nin 2019/1011 E. ve 2020/1112 K. sayılı, 05.02.2020 tarihli kararı, (Yargıtay Bilgi Bankası), erişim tarihi: 28.06.2021.

<sup>957</sup> Yargıtay 12. Ceza Dairesi'nin 2019/973 E. ve 2020/218 K. sayılı, 08.01.2020 tarihli kararı, (Kazancı İçtihat Bilgi Bankası), erişim tarihi: 28.06.2021.

<sup>958</sup> Börekçi, s. 152.

hakkından ayrılmaya başlamıştır. Diğer yandan, suçta kişisel verilerin verilmesi, yayılması veya ele geçirilmesi söz konusu olmasına rağmen TCK'nın 136. maddesinin oluşmadığını söylemek de doğru değildir. Sonuç olarak, tek bir hareket ile her iki suçun oluşması durumunda fikri içtima hükümleri uygulanmalı, fail hakkında en ağır cezayı gerektiren suçtan hüküm kurulmalıdır<sup>959</sup>.

### 10.3.2.3. Kişisel Verileri Kaydetme Suçu

TCK'nın 135. maddesinde düzenlenen kişisel verileri kaydetme suçu ile kişisel verileri verme, yayma veya ele geçirme suçu arasındaki ilişkide, bu suçların geçitli suç kapsamında değerlendirilip değerlendirilemeyeceğine yönelik görüş ayrılığı bulunmaktadır. Bir görüşe göre TCK'nın 136. maddesi ile 135. maddesi arasında geçitli suç ilişkisi vardır<sup>960</sup>. Geçitli suç; her iki suçun aynı hukukî konuyu koruduğu, suçun işlenmesi için hafif olan suçtan geçilen, fail ve mağdurlarının aynı olduğu ve aynı nedensel bağ üzerinde sübut bulunduğu suçlar olarak tanımlanabilir<sup>961</sup>. Ancak kişisel verileri verme, yayma veya ele geçirme suçu, kişisel veriler kaydedilmeden de gerçekleşebileceğinden, geçitli suçun unsurlarının tamamının varlığından söz edilemeyecektir<sup>962</sup>. Örneğin bir kimse, kişisel verileri kaydetmeden de bir başkasına verebilir. Diğer bir görüş geçitli suçu kısmen kabul etmekte; ancak tek hareketle kişisel verinin kaydedilmesi ve verilmesi, yayılması veya ele geçirilmesi halinde fikri içtima hükümlerinin uygulanacağını savunmaktadır<sup>963</sup>. Bu durumda fail hakkında yalnızca yaptırımını ağır olan TCK'nın 136. maddesinden hüküm kurulacaktır.

Geçitli suça katılmayan bir görüş ise kişisel verileri kaydetme suçu ile kişisel verileri verme, yayma veya ele geçirme suçu arasında geçit ilişkisinin kurulmadığını belirterek failin iki suçtan ayrı ayrı cezalandırılması gerektiğini savunmaktadır<sup>964</sup>. Yargıtay'ın iki

<sup>959</sup> Aynı yönde görüş için bkz.: **Börekçi**, s. 153.

<sup>960</sup> **Taşkın**, s. 109; **Soyaslan**, s. 356. Yargıtay'ın da son yıllarda bu görüşe yakın karar verdiği görülmektedir. Örn: Yargıtay 17. Ceza Dairesi'nin 2015/25941 E. ve 2018/126 K. sayılı, 08.01.2018 tarihli kararı, (Yargıtay Bilgi Bankası), erişim tarihi: 28.06.2021.

<sup>961</sup> **Börekçi**, s. 153.

<sup>962</sup> **Börekçi**, s. 153.

<sup>963</sup> **Korkmaz**, Ceza Hukuku, s. 481; **Gültekin**, s. 174

<sup>964</sup> **Şen**, Ersan, *Yeni Türk Ceza Kanunu Yorumu*, Cilt: 1, Vedat Kitapçılık, İstanbul 2006, (**Şen**, Yorum) s. 607.

hareket arasında geçen süreyi esas alarak -doğrudan olmasa da- bu görüşe benzer tutum sergilediği görülmektedir<sup>965</sup>. Kanaatimizce eğer tek bir hareket ile aynı anda hem kişisel verileri kaydetme hem de kişisel verileri verme, yayma veya ele geçirme suçu işlenmişse bu durumda fikri içtima hükümlerine gidilmeli ve fail en ağır cezayı gerektiren suçtan dolayı cezalandırılmalıdır<sup>966</sup>.

#### 10.3.2.4. Hakaret Suçu

Kişisel verileri verme, yayma veya ele geçirme, aynı zamanda hakaret suçunu da oluşturabilir. Dolayısıyla bu durumda bir hareket ile birden fazla suçun oluşumuna sebebiyet verildiğinden, hakaret suçu ile kişisel verileri verme, yayma veya ele geçirme suçu arasında fikri içtima söz konusu olacaktır<sup>967</sup>. Dolayısıyla kişisel verileri verme, yayma veya ele geçirme suçunun yaptırımını daha ağır olduğundan, bu suçtan hüküm kurulacaktır. Nitekim Yargıtay da “... *hakaret suçunun oluştuğu, bir fiili ile birden fazla farklı suçun oluşmasına neden olan sanığın, TCK'nın 44.maddesi gereğince daha ağır cezayı gerektiren verileri hukuka aykırı olarak verme veya ele geçirme suçundan cezalandırılması...*” ifadelerine yer vermiş, anılan iki suç arasında fikri içtima hükümlerinin uygulanması gerektiğini belirtmiştir<sup>968</sup>.

---

<sup>965</sup> Örn: Yargıtay 12. Ceza Dairesi'nin 2017/3570 E. ve 2018/808 K. sayılı, 24.01.2018 tarihli kararı, (Yargıtay Bilgi Bankası), erişim tarihi: 29.06.2021.: “TCK'ya hakim olan gerçek içtima kuralı gereğince, kişisel veri niteliğindeki mağdura ait cep telefonu numarasını, kaydedilmiş haliyle ve hukuka uygunluk nedenlerinin bulunmaması nedeniyle hukuka aykırı olduğunda tereddüt bulunmayan bir yöntemle ele geçirip, iki gün sonra da, mağdurun rızasına aykırı şekilde yayımlayan sanığın birbirinden bağımsız iki farklı eyleminden dolayı iki ayrı mahkumiyet hükmü kurulması gerekirken, yazılı şekilde tek mahkumiyet hükmü kurulması, bozmayı gerektirmiş olup...”.

<sup>966</sup> Aynı yönde bkz: **İtişgen**, s. 197; **Börekçi**, s. 154-155.

<sup>967</sup> **Dülger**, Kişisel Verilerin Korunması, s. 749.

<sup>968</sup> Yargıtay 12. Ceza Dairesi'nin 2018/8300 E. ve 2019/6862 K. sayılı, 29.05.2019 tarihli kararı, (Lexpera), erişim tarihi: 26.06.2021. Benzer yönde karar için bkz.: Yargıtay 12. Ceza Dairesi'nin 2018/8198 E. ve 2019/6187 K. sayılı, 27.02.2019 tarihli kararı, (Yargıtay Bilgi Bankası), erişim tarihi: 26.06.2021.

### 10.3.2.5. Bilişim Sistemine Girme Suçu

TCK'nın 243. maddesinde düzenlenen bilişim sistemine girme suçu ile kişisel verileri verme, yayma veya ele geçirme suçu arasındaki ilişki önemlidir. Çünkü çoğu zaman kişisel veriler bilişim sistemlerine girilerek ele geçirilmektedir<sup>969</sup>. Bu durumda somut olayda TCK'nın 243. maddesi ile TCK'nın 136. maddesi arasında geçitli suç ilişkisi incelenmelidir. Eğer ki bilişim sistemine girme suçu gerçekleştirilmeden kişisel verileri verme, yayma veya ele geçirme suçu gerçekleştirilebiliyor ise fail her iki suçtan ayrı ayrı cezalandırılmalı; aksi durumda fa iki suçtan hangisinin cezası daha ağırsa o suçtan cezalandırılmalıdır<sup>970</sup>.

## 11. SUÇUN NİTELİKLİ HALLERİ

### 11.1. Genel Olarak

Kişisel verileri verme, yayma veya ele geçirme suçunun nitelikli halleri TCK'nın 136. maddesinin 2. fıkrası ile 137. maddesinde düzenlenmiştir. Aşağıda iki madde ayrı ayrı ele alınacaktır.

### 11.2. Mağdurun Dinlenmesi

2019 yılında adli yargı reform paketi olarak yapılan değişiklikle TCK'nın 136. maddesine ağırlaştırıcı bir hal olarak 2. fıkra eklenmiştir<sup>971</sup>. Buna göre suçun konusunun, CMK'nın 236. maddesinin 5. ve 6. fıkraları uyarınca kayda alınan beyan ve görüntüler olması durumunda verilecek ceza bir kat artırılabacaktır.

<sup>969</sup> **Dülger**, Kişisel Verilerin Korunması, s. 748.

<sup>970</sup> Aynı yönde görüş için bkz.: **Dülger**, Kişisel Verilerin Korunması, s. 749.

<sup>971</sup> 24.10.2019 tarihli ve 30928 sayılı Resmî Gazete'de yayımlanan 17.10.2019 tarihli ve 7188 sayılı Ceza Muhakemesi Kanunu ve Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun'un 17. maddesi: 5237 sayılı Kanunun 136 ncı maddesine aşağıdaki fıkra eklenmiştir.

“(2) 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.”

Bu ağırlaştırıcı nedenin incelenmesi için öncelikle “*mağdur ve şikayetçinin dinlenmesi*” başlıklı CMK’nın 236. maddesinin 5. ve 6. fıkrasının ele alınması gereklidir. Maddenin 5. fıkrası; soruşturma veya kovuşturma aşamasında, TCK’nın “*Çocukların cinsel istismarı*” başlıklı 103. maddesinin 2. fıkrasındaki suçtan<sup>972</sup> mağdur olan çocukların beyanlarının ilgili mercilerce alınmasına yönelik olarak yeni bir usul getirmektedir. Bu usule göre mağdur çocuğun beyanları özel merkezlerde yetkililer<sup>973</sup> tarafından alındığı sırada bu anlar sesli ve görüntülü bir şekilde kaydedilecek; kayda ilişkin olarak mağdur çocuğun veya temsilcisinin rızası aranmayacaktır. Maddenin 6. fıkrasında ise TCK’nın “*Cinsel saldırı*” başlıklı 102. maddesinin 2. fıkrasındaki suçun mağdurunun sadece soruşturma aşamasındaki beyanlarının alınmasına ilişkin yeni bir düzenleme getirmektedir. Şöyle ki; soruşturma evresinde ilgili suçun mağdurunun beyanları alınırken, mağdur rıza gösterirse beyanların verildiği anda sesli ve görüntülü kayıt yapılabilecektir. Esasında CMK’nın ilgili düzenlemesi ile amaçlanan, anılan suç mağdurlarına muhakeme aşamalarında, yaşanan olayları tekrar hatırlatmamak, bununla birlikte mağduru korumaktır<sup>974</sup>. TCK’nın ilgili düzenlemesi ile amaçlanan ise davranışı daha ağır bir yaptırıma tabi tutarak hukukî değerini daha çok korunmasını sağlamaktır. Ancak önemle değinmek gerekir ki; TCK’nın anılan düzenlemesiyle amaçlanan ile ortaya çıkan sonuç arasında tutarsızlık bulunmaktadır. Nitekim TCK’nın 136. maddesinin 2. fıkrasında “*beyan ve görüntüler*” ifadesi kullanılmıştır. Bu durumda sadece beyan ya da sadece görüntünün başkalarına verilmesi, yayılması ya da ele geçirilmesi durumunda failin kastı TCK’nın 136. maddesinin 2. fıkrasına yönelikse fail 136/2’ye teşebbüsten sorumlu tutulacaktır. Ancak failin kastı TCK’nın 136. maddesinin 2. fıkrasına yönelik değilse bu durumda fail TCK’nın 136. maddesinin 1. fıkrasından sorumlu tutulacaktır. Dolayısıyla kanun koyucunun anılan beyan ve görüntülere yönelik daha nitelikli bir koruma getirmesi; ancak yalnızca beyan veya yalnızca görüntüye yönelik daha hafif bir yaptırım öngörmesi bir çelişkiyi doğurmaktadır<sup>975</sup>. Dolayısıyla TCK’nın 136. maddesinin 2.

---

<sup>972</sup> TCK’nın 103. maddesinin 2. fıkrası: “*Cinsel istismarın vücuda organ veya sair bir cisim sokulması suretiyle gerçekleştirilmesi durumunda, on altı yıldan aşağı olmamak üzere hapis cezasına hükmolunur. Mağdurun on iki yaşını tamamlamamış olması hâlinde verilecek ceza on sekiz yıldan az olamaz.*”

<sup>973</sup> Soruşturma aşamasında Cumhuriyet savcısı nezaretinde uzmanlar tarafından, kovuşturma aşamasında ise naip hâkim tarafından uzmanlar aracılığıyla.

<sup>974</sup> **Böreççi**, s. 131.

<sup>975</sup> Aynı yönde bkz.: Anıl **Akyıldız**, *Soruşturma Evresinde Gizliliğin İhlali Suçu*, Yayınlanmamış Yüksek Lisans Tezi, Özyeğin Üniversitesi, Sosyal Bilimler Enstitüsü, İstanbul, 2020, s. 146; **Böreççi**, s. 132-133.

fıkrasındaki “*beyan ve görüntüler*” ifadesinin “*beyan veya görüntüler*” olarak değiştirilmesi, kanun koyucunun amaçladığı korumanın yaratılması açısından daha isabetli olacaktır.

### **11.3. Kamu Görevlisi Olma veya Kolaylıktan Yararlanma**

TCK’nın 137. maddesi uyarınca kişisel verileri verme, yayma veya ele geçirme suçunun “*kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle*” veya “*belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle*” işlenmesi durumları suçun nitelikli hali olarak düzenlenmiştir. Aşağıda her iki nitelikli hal ayrı ayrı ele alınacaktır.

#### **11.3.1. Kamu Görevlisi Olma**

TCK’nın 137. maddesinin 1. fıkrasının a bendi uyarınca kişisel verileri verme, yayma veya ele geçirme suçunun “*kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle*” işlenmesi halinde verilecek ceza yarı oranında artırılabilecektir. Kamu görevlisinin tanımının TCK’nın 6. maddesine göre yapılması gerekmektedir. TCK’nın “*Tanımlar*” başlıklı 6. maddesinde kamu görevlisi “*Kamusal faaliyetin yürütülmesine atama veya seçilme yoluyla ya da herhangi bir surette sürekli, süreli veya geçici olarak katılan kişi.*” olarak tanımlanmıştır. TCK’daki kamu görevlisi tanımı, idare hukukundaki kamu görevlisinin tanımına göre daha kapsamlıdır. Dolayısıyla kamu görevlisi, kamusal faaliyete katılan herkes olarak yorumlanmalıdır<sup>976</sup>. Kişinin yürüttü faaliyetin de niteliğine bakılmalı, eğer ki faaliyet kamusal nitelikte ise bu durumda kişi de kamu görevlisi sayılmalıdır. Örneğin noter, avukat, bilirkişiler, yürüttüğü faaliyetler açısından kamu görevlisi olarak değerlendirilecektir<sup>977</sup>. Yargıtay’a göre de kamu görevlisi, kamusal

<sup>976</sup> Göçmen Uyarer, s. 216.

<sup>977</sup> Korkmaz, Ceza Hukuku, s. 434; Kuşkonmaz, Elif Mendos, *Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması*, Yayımlanmamış Yüksek Lisans Tezi, T.C. İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, İstanbul 2013, s. 150; Börekçi, s. 135.

faaliyetin idaresine katılan kişileri kapsamakta olup, askerlik hizmetini ifa eden kişi de kamu görevlisi olarak değerlendirilmektedir.<sup>978</sup>.

Madde metninde düzenlenen ağırlaştırıcı nedenden hüküm kurulabilmesi için hareketin yalnızca kamu görevlisi tarafından gerçekleştirilmesi yeterli değildir. Aynı zamanda kamu görevlisinin görevinden kaynaklanan yetkisini kötüye kullanması gerekmektedir<sup>979</sup>. Dolayısıyla failin kamu görevlisi olmasına karşın suçu işlerken görevinin verdiği yetkiyi kötüye kullanmaması durumunda nitelikli halin oluştuğu söylenemez. Yargıtay da vermiş olduğu bir kararında “*Katılanın evinde özel hayatını ihlal edecek şekilde görüntü ve ses kaydı yaptığı sabit olan sanığın bu eylemlerinin sanığın görevi ile ilgili olmaması*” gerekçesi ile 137. maddeden hüküm kurulmasının isabetsiz olduğunu değerlendirmiştir<sup>980 981</sup>.

### 11.3.2. Meslek veya Sanatın Sağladığı Kolaylıktan Yararlanma

Kişisel verileri verme, yayma veya ele geçirme suçunun bir diğer nitelikli hali TCK'nın 137. maddesinin 1. fıkrasının b bendi uyarınca suçun “*Belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle*” işlenmesidir. Bu durumda yine verilecek ceza yarı oranında artırılacaktır.

Madde metninde veya madde gerekçesinde meslek veya sanatın kapsamı belirtilmemiştir. TDK'ya göre meslek “*Belli bir eğitim ile kazanılan, sistemli bilgi ve becerilere dayalı, insanlara yararlı mal üretmek, hizmet vermek ve karşılığında para kazanmak için yapılan, kuralları belirlenmiş iş.*” şeklinde tanımlanmıştır<sup>982</sup>. Madde metnindeki sanatın ise zanaat olarak yorumlanması gerekir. TDK'ya göre zanaat, “*İnsanların maddeye dayanan gereksinimlerini karşılamak için yapılan, öğrenimle birlikte deneyim, beceri ve*

<sup>978</sup> Yargıtay 12. Ceza Dairesi'nin 2016/1129 E. ve 2017/6742 K. sayılı, 27.09.2017 tarihli kararı (Yargıtay Bilgi Bankası), erişim tarihi: 28.06.2021.

<sup>979</sup> Karagülmez, s. 464; Dülger, Kişisel Verilerin Korunması, s. 732.

<sup>980</sup> Yargıtay 12. Ceza Dairesi'nin 2018/2226 E. ve 2018/8746 K. sayılı, 26.09.2018 tarihli kararı (Yargıtay Bilgi Bankası), erişim tarihi: 28.06.2021.

<sup>981</sup> Konu ile ilgili benzer yönde kararlar için bkz.: Yargıtay 12. Ceza Dairesi'nin 2018/2226 E. ve 2018/8746 K. sayılı, 26.09.2018 tarihli kararı; Yargıtay 15. Ceza Dairesi'nin 2015/1659 E. ve 2018/2748 K. sayılı, 18.04.2018 tarihli kararı, (Lexpera), erişim tarihi: 26.06.2021.

<sup>982</sup> TDK, Güncel Türkçe Sözlük, erişim için bkz.: <https://sozluk.gov.tr/>, erişim tarihi: 26.06.2021.

*ustalık gerektiren iş, sınaat.*” anlamını taşımaktadır<sup>983</sup>. Bu kavramların her somut olaya göre değerlendirilmesi gerekmektedir<sup>984</sup>.

Anılan madde hükmünde “ve” bağlacının kullanıldığı görülmektedir. Bu bağlacın kullanılması neticesinde kişinin her iki niteliğe de sahip olması gerekecektir. Ancak söz konusu nitelikli halin uygulanabilmesi için bunlardan birisinin bulunması yeterlidir<sup>985</sup>. Anlam karışıklığına mahal vermemesi için “*meslek ve sanat*” ifadesinin “*meslek veya sanat*” olarak değiştirilmesi yerinde olacaktır<sup>986</sup>.

Meslek veya sanatın türüne göre ayrı bir düzenleme belirtilmediğinden, her türlü meslek veya sanatın nitelikli hal kapsamına gireceği söylenebilir<sup>987</sup>. Meslek veya sanatın suçu işlemek açısından elverişli de olması gerekir<sup>988</sup>. Kolaylık sağlama ifadesinden ise meslek veya sanatın icrası ile suçun işlenmesi arasında bir nedensellik bağının bulunması gerektiği anlaşılmalıdır<sup>989</sup>. Örneğin bir lunapark işletmecisinin, hız trenindeki kişilerin güvenlik kamerasında denk gelen komik görüntülerini internet ortamında yayınlamasında bu nitelikli hâl oluşacaktır. Başka bir örnekte, özel bir hastanede hasta kayıtlarına girebilen bir hemşirenin bu kayıtları hukuka uygunluk nedeni bulunmadan bir başkasına vermesi halinde nitelikli hâlin uygulanması gerekecektir<sup>990</sup>. Bir insan kaynakları personelinin özlük dosyalarına erişim sağlaması, bir anketörün anket yaptığı kişilerin telefon numarası bilgilerine ulaşması, satış pazarlama departmanında çalışan bir kişinin satış yapılan müşteri bilgilerine erişmesi de bu nitelikli hale örnek verilebilir. Yargıtay da vermiş olduğu bir kararında bir telefon operatörü firmasının alt bayisi olan sanıkların; kendileriyle işlem yapan müşterilere ait bilgilerin örneklerinin hukuka aykırı olarak alınması ve ayrı bir cihaza aktardıkları olayda sanıkların “*belli bir mesleğin sağladığı kolaylıktan yararlandıklarını*” belirtmiştir<sup>991</sup>.

---

<sup>983</sup> TDK, Güncel Türkçe Sözlük, erişim için bkz.: <https://sozluk.gov.tr/>, erişim tarihi: 26.06.2021.

<sup>984</sup> Kuşkonmaz, s. 151.

<sup>985</sup> Özbek / Doğan / Bacaksız, Özel Hükümler, s. 590.

<sup>986</sup> Özbek / Doğan / Bacaksız, Özel Hükümler, s. 590, 591.

<sup>987</sup> Soyaslan, s. 364; Börekçi, s. 144.

<sup>988</sup> Özbek / Doğan / Bacaksız, Özel Hükümler, s. 591.

<sup>989</sup> Özbek / Doğan / Bacaksız, Özel Hükümler, s. 591; Börekçi, s. 145.

<sup>990</sup> Kangal, Kişisel Veriler, s. 119.

<sup>991</sup> Yargıtay 12. Ceza Dairesi'nin 2014/18783 E. ve 2015/2124 K. sayılı, 09.02.2015 tarihli kararı (Yargıtay Bilgi Bankası), erişim tarihi: 28.06.2021.



Ayrıca suçun işlenmesi ile meslek veya sanatın icrası arasında da bir nedensellik bağının bulunması gerekmektedir<sup>992</sup>. Yargıtay bir kararında “*Gazeteci sanığın, mesleğinin icrası dolayısıyla sağladığı kolaylıktan ve avantajdan yararlanarak atılı eylemi gerçekleştirmediği, basın ve yayın araçlarını kullanabilmek ve bu araçların kolaylığından faydalanabilmek için mutlaka gazeteci olunması gerektiği ve suçun gazeteciler tarafından basın ve yayın yoluyla işlenmesinin daima anılan maddenin uygulanması sonucunu doğurmayacağı...*” ifadelerine yer vermiş ve mesleğin icrası ile suçun işlenmesi arasındaki nedenselliğin aranması gerektiğini belirtmiştir<sup>993</sup>.

## 12. YAPTIRIM

TCK’nın 136. maddesinin 1. fıkrasına göre, kişisel verileri veren, yayan veya ele geçiren kişinin, iki yıldan dört yıla kadar hapis cezası ile cezalandırılacaktır. Cezanın alt sınırı 21.02.2014 tarihli ve 6526 sayılı Kanun<sup>994</sup> ile iki yıla çıkarılmıştır<sup>995</sup>. TCK’nın 136. maddesinin 2. fıkrasına göre ise suçun konusunun CMK’nın 236. maddesinin 5. ve 6. fıkraları uyarınca kayda alınan beyan ve görüntüler olması durumunda verilecek ceza bir kat artırılacaktır. Yine, TCK’nın 137. maddesinin 1. fıkrasına göre suçun kamu görevlisi tarafından görevinin verdiği yetkiyi kötüye kullanılarak işlenmesi ya da belli bir meslek ve sanatın sağladığı kolaylıktan yararlanılarak işlenmesi halinde verilecek ceza yarı oranda artırılacaktır.

Failin elektronik haberleşme hizmeti vermek üzere yetkilendirilmiş bulunan işletmecilerin personeli olması durumunda ise, 5809 sayılı Elektronik Haberleşme

---

<sup>992</sup> Kuşkonmaz, s. 151.

<sup>993</sup> Yargıtay 12. Ceza Dairesi’nin 2018/8108 E. ve 2019/3141 K. sayılı ve 06.03.2019 tarihli kararı, (Yargıtay Bilgi Bankası), erişim tarihi: 28.06.2021.

<sup>994</sup> 06.03.2014 tarihli ve 28933 (Mükerrer) sayılı Resmî Gazete’de yayımlanan 21.02.2014 tarihli ve 6526 sayılı Terörle Mücadele Kanunu ve Ceza Muhakemesi Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun.

<sup>995</sup> Değişiklik öncesinde cezanın alt sınırı bir yıl idi.

Kanunu'nun<sup>996</sup> 63. maddesinin 3. fıkrası uyarınca verilecek ceza yarı oranında değil, bir kat oranında artırılabacaktır<sup>997</sup>.

Kişisel verileri verme, yayma veya ele geçirme suçunun işlenmesi dolayısıyla tüzel kişiler hakkında bunlara özgü güvenlik tedbiri uygulanacağı ise TCK'nın 140. maddesinde düzenlenmiştir. Tüzel kişilere özgü güvenlik tedbirleri TCK'nın 60. maddesinde yer almaktadır. Buna göre;

#### ***“Tüzel kişiler hakkında güvenlik tedbirleri***

*Madde 60- (1) Bir kamu kurumunun verdiği izne dayalı olarak faaliyette bulunan özel hukuk tüzel kişisinin organ veya temsilcilerinin iştirakiyle ve bu iznin verdiği yetkinin kötüye kullanılması suretiyle tüzel kişi yararına işlenen kasıtlı suçlardan mahkûmiyet halinde, iznin iptaline karar verilir.*

*(2) Müsadere hükümleri, yararına işlenen suçlarda özel hukuk tüzel kişileri hakkında da uygulanır.*

*(3) Yukarıdaki fıkralar hükümlerinin uygulanmasının işlenen fiile nazaran daha ağır sonuçlar ortaya çıkarabileceği durumlarda, hakim bu tedbirlere hükmetmeyebilir.*

*(4) Bu madde hükümleri kanunun ayrıca belirttiği hallerde uygulanır.”*

Son olarak, kişisel verileri verme, yayma veya ele geçirme suçunda haksız tahrikin uygulama alanı bulması mümkündür<sup>998</sup>. Nitekim mağdurun hakaretine uğrayan bir kişi, bu hakaretin yarattığı öfkeyle mağdura ait kişisel verileri bir başkasına verebilir, yayabilir veya ele geçirebilir. Bu durumda TCK'nın 29. maddesinde düzenlenen haksız tahrike ilişkin hükümler uygulanacak, cezanın dörtte birinden dörtte üçüne kadar indirim yapılacaktır.

<sup>996</sup> 10.11.2008 tarihli ve 27050 sayılı Resmî Gazete'de yayımlanan 5809 sayılı Elektronik Haberleşme Kanunu, erişim için bkz.: <https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5809.pdf>, erişim tarihi: 29.09.2021.

<sup>997</sup> Elektronik Haberleşme Kanunu'nun 63. maddesinin 3. fıkrası: “Elektronik haberleşme hizmeti vermek üzere yetkilendirilmiş bulunan işletmecilerin personelinin, 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununun İkinci Kitabının İkinci Kısımının Dokuzuncu Bölümünde düzenlenen, özel hayata ve hayatın gizli alanına karşı suçları işlemesi halinde haklarında bu bölümde öngörülen cezalara hükmolunur. Ancak 137 nci maddeye göre yapılacak artırım bir kat olarak uygulanır.”

<sup>998</sup> Kangal, Kişisel Veriler, s. 132.

Haksız tahrikin özellikle suçun tahrikte bulunan kişiye karşı işlenmesi gerektiği şartına bağlı olarak, failin kendisine hakaret edene değil de onun yakınlarına ait kişisel verilerini vermesi, yayması veya ele geçirmesi durumunda haksız tahrik hükümleri uygulanmayacaktır<sup>999</sup>.

### 13. SORUŞTURMA VE KOVUŞTURMA

Kişisel verileri verme, yayma veya ele geçirme suçunun soruşturması ve kovuşturması re'sen yapılır. TCK'nın 139. maddesiyle “*Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar*” başlıklı Dokuzuncu Bölümdeki suçların şikâyete tabi tutulacağı düzenlenmiş; ancak bu düzenlemeden “*Kişisel verilerin kaydedilmesi*”, “*Verileri hukuka aykırı olarak verme veya ele geçirme*” ve “*Verileri yok etmeme*” suçları hariç tutulmuştur<sup>1000</sup>. Yapılan bu ikili ayırım kimi zaman yargı mercilerinin de gözünden kaçabilmektedir. Yargıtay vermiş olduğu bir kararında şikâyet konusunu ele almış; mağdur ve sanıkların birbirine karşı sundukları şikâyetleri geri almalarının suçun soruşturma ve kovuşturmasını etkilemeyeceğini belirtmiştir<sup>1001</sup>.

Kanun koyucunun yapmış olduğu bu ayırımın nedenini anlayabilmek için bir suçun takibinin şikâyete tabi olmasındaki gerekçe ve şikâyet şartının gerekliliği incelenmelidir<sup>1002</sup>. Ceza hukukunda işlenen suçlar kamu düzenini ihlal ettiğinden dolayı kural olarak re'sen soruşturulur ve kovuşturulur. Ancak her suç, kamu düzenini aynı şekilde etkilemeyebilir. Yine, kişiler kendisi için özel olan bazı bilgilerini ceza muhakemesinin aktörü olan üçüncü kişilerle paylaşmak istemeyebilir<sup>1003</sup>. Bu durumda kişinin paylaşmak istemediği verilerini ceza muhakemesinin bir konusu haline getirmeye zorlamak, suçla korunan maddi ve manevi varlığının sürdürülebilmesini sağlamakla örtüşmeyebilir<sup>1004</sup>. Ancak kişisel verileri verme, yayma veya ele geçirme suçunda kanun

<sup>999</sup> Kangal, *Kişisel Veriler*, s. 132.

<sup>1000</sup> Bu itibarla “Haberleşmenin gizliliğini ihlal”, “Kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması” ve “Özel hayatın gizliliğini ihlal” suçları şikâyete tabidir.

<sup>1001</sup> Yargıtay 12. Ceza Dairesi'nin 2012/22005 E. ve 2013/24489 K. sayılı, 04.11.2013 tarihli kararı, (Yargıtay Bilgi Bankası), erişim tarihi: 28.06.2021.

<sup>1002</sup> Börekçi, s. 171.

<sup>1003</sup> Börekçi, s. 171.

<sup>1004</sup> Akyürek, s. 331.

koyucu kamu düzenini suçtan zarar görenin yararından üstün görmektedir<sup>1005</sup>. Kanun koyucu bu sebeple ikili bir ayrıma gitmiştir. Ancak kişisel verilerin korunması hakkının kaynağını çoğunlukla özel hayatın gizliliği hakkından almasından hareketle kişisel verilerin korunması alanında toplum yararı ile kişisel yarar arasında kişisel yararın toplum yararına nazaran daha ağır basmalıdır. Bu nedenle re’sen soruşturulan “*Kişisel verilerin kaydedilmesi*”, “*Verileri hukuka aykırı olarak verme veya ele geçirme*” ve “*Verileri yok etmeme*” suçlarının şikâyete tabi olması daha isabetli olacaktır<sup>1006</sup>.

Suçun failinin kamu görevlisi olması durumunda kamu görevlisi hakkında soruşturma başlatılabilmesi için 4483 sayılı Memurlar ve Diğer Kamu Görevlilerinin Yargılanması Hakkında Kanun’un<sup>1007</sup> 3. maddesindeki prosedürün uygulanması gerekmektedir. Buna göre, yetkili merciden soruşturma izni alınmalıdır<sup>1008</sup>.

Suçun soruşturulması şikâyete tabi olmadığından ve ayrıca bu suça CMK’nın “*Uzlaştırma*” başlıklı 253. maddesinde yer verilmediğinden uzlaştırmaya ilişkin hükümler uygulanmaz. Bu durum nitelikli haller için de geçerlidir<sup>1009</sup>. CMK’nın 231. maddesi uyarınca sanık hakkında verilen ceza iki yıl ya da daha az süreli hapis cezası veya adli para cezası ise maddede öngörülen diğer şartlar sağlandığı takdirde hükmün açıklanmasının geri bırakılmasına karar verilebilir<sup>1010</sup>.

#### 14. GÖREVLİ VE YETKİLİ MAHKEME

Kişisel verileri verme, yayma veya ele geçirme suçunun üst sınırı on yıldan fazla hapis cezasını gerektirmediğinden, görevli mahkeme asliye ceza mahkemesidir<sup>1011</sup>. 5235 sayılı Kanun’un 14. maddesinde yer alan; mahkemelerin görevlerinin belirlenmesinde

<sup>1005</sup> **Korkmaz**, Ceza Hukuku, s. 487.

<sup>1006</sup> Aynı yönde görüş için bkz.: **Koca / Üzülmaz**, s. 598; **Börekçi**, s. 173.

<sup>1007</sup> 04.12.1999 tarihli ve 23896 sayılı Resmî Gazete’de yayımlanan 4483 sayılı Memurlar ve Diğer Kamu Görevlilerinin Yargılanması Hakkında Kanun.

<sup>1008</sup> **Göçmen Uyarer**, s. 236.

<sup>1009</sup> **Sarıusta**, s. 168.

<sup>1010</sup> **Sert**, s. 151.

<sup>1011</sup> 07.10.2004 tarihli ve 25606 sayılı Resmî Gazete’de yayımlanan 5235 sayılı Adli Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanun’un (Çalışmanın devamında “5235 sayılı Kanun” olarak isimlendirilecektir.) 11. 12. ve 14. maddeleri uyarınca değerlendirme yapılmıştır.

ağırlaştırıcı nedenler gözetilmeksizin suçun üst sınırının göz önünde bulundurulacağı hükmü gereğince TCK'nın 136. maddesinin 2. fıkrası ve 137. maddesindeki nitelikli hallerin tatbiki durumunda da görevli mahkeme yine asliye ceza mahkemesidir<sup>1012</sup>.

5187 sayılı Basın Kanunu'nun<sup>1013</sup> 27. maddesinin 2. fıkrası gereğince; suçun basılı eserler yoluyla işlenmesi durumunda asliye ceza mahkemesinin birden fazla dairesi bulunması halinde iki numaralı asliye ceza mahkemesi görevlidir.

Yetkili mahkemenin ise CMK'daki yetki kurallarına göre belirlenmesi gerekmektedir. Bu itibarla CMK'nın 12. maddesine göre kural olarak yetkili mahkeme, suçun işlendiği gerçekleştiği yer mahkemesidir. Özellikle bilişim alanındaki teknolojik gelişmeler sebebiyle, sanal dünyada işlenen suçların nerede gerçekleştiğinin tespiti oldukça güçtür<sup>1014</sup>. Hatta bazı durumlarda hareketin bir kısmı Türkiye'de, diğer kısmı yabancı bir ülkede veya Türkiye'nin farklı şehirlerinde gerçekleşebilir<sup>1015</sup>. Bu durumda mesafe suçlarından bahsedilir ve ülkeler arası gerçekleşen mesafe suçlarında, TCK'nın 8. maddesinin 1. fıkrası gereğince "*Filmin kısmen veya tamamen Türkiye'de işlenmesi veya neticenin Türkiye'de gerçekleşmesi halinde suç, Türkiye'de işlenmiş sayılır*"<sup>1016</sup>. Suçun Türkiye'nin farklı yerlerinde işlenmesi durumunda ise doktrinde ülke içinde gerçekleşen mesafe suçlarından bahsedilmekle birlikte; suçun hareketle neticenin meydana geldiği her yerde işlenmiş sayılabileceği belirtilmiştir<sup>1017</sup>. Şayet suçun işlendiği yer belli değilse, bu durumda CMK'nın 13. maddesindeki hükümlere gidilmelidir. Buna göre eğer suçun işlendiği yer belli değilse şüphelinin/sanığın yerleşim yeri mahkemesi yetkili olacaktır. Şüphelinin/sanığın yerleşim yerinin Türkiye'de bulunmadığı durumda yetkili mahkeme, şüphelinin/sanığın Türkiye'deki en son adresinin bulunduğu yer mahkemesi olacaktır. Eğer bu adres de bulunamıyorsa nihayet şüpheli/sanık hakkında ilk usul işleminin yapıldığı yer mahkemesi yetkili olacaktır.

Suçun basın aracılığıyla işlenmesi durumunda ise eserin yayım merkezinin bulunduğu yer mahkemesi yetkili olacaktır. Eser yayım merkezi dışında basılmışsa bu durumda basım yeri mahkemesi yetkili olacaktır.

---

<sup>1012</sup> **Özbek / Doğan / Bacaksız**, Özel Hükümler, s. 602.

<sup>1013</sup> 26.06.2004 tarihli ve 25504 sayılı Resmî Gazete'de yayımlanan 5187 sayılı Basın Kanunu.

<sup>1014</sup> **Börekçi**, s. 177.

<sup>1015</sup> **Gültekin**, s. 159.

<sup>1016</sup> **Centel / Zafer / Çakmut**, s. 158.

<sup>1017</sup> **Centel / Zafer / Çakmut**, s. 157.

Son olarak, suça konu görsel ve işitsel yayın, mağdurun yerleşim yerinde yayılmışsa bu yer mahkemesi de yetkili olacaktır.

## **15. ZAMANAŞIMI**

TCK'nın 66. maddesinin 1. fıkrasının e bendi uyarınca kamu davası, beş yıldan fazla olmamak üzere hapis veya adlî para cezasını gerektiren suçlarda sekiz yılın geçmesiyle düşer. Kişisel verileri hukuka aykırı olarak verme, yayma veya ele geçirme suçunun temel halinin beş yıldan fazla hapis cezasını gerektirmemesi nedeniyle dava zamanaşımı süresi sekiz yıldır. Ancak 137. maddede düzenlenen cezayı ağırlaştırıcı nitelikli halin varlığı durumunda suç beş yıldan fazla hapis cezasını gerektirebilecektir. Bu durumda TCK'nın aynı madde ve fıkrasının d bendi gereğince dava zamanaşımı süresi on beş yıl olacaktır. TCK'nın 68. maddesinin 1. fıkrasının d ve e bentleri gereğince ise beş yıla kadar hapis ve adlî para cezalarında on yıl, beş yıldan fazla hapis cezalarında yirmi yıllık sürenin geçmesiyle ceza, zamanaşımına uğrayacaktır.

## SONUÇ

Kişisel verilerin korunmasına yönelik duyulan ihtiyaç bugünden asırlar öncesine dayanmaktadır. Ancak özellikle II. Dünya Savaşı'ndan sonra devletlerin kişilere ait bilgi bankaları oluşturması ve bu bilgileri işleyerek kişileri sınıflandırması, kişisel verilerin bağlayıcı hukuk normlarıyla korunması gerektiğini ortaya çıkarmıştır. Bunu takiben çeşitli ülkelerde ve uluslararası alanda, kişisel verilerin korunmasına yönelik adımlar atılmış ve kişisel verilerin korunmamasını yaptırıma bağlayan düzenlemeler oluşturulmuştur. En nihayetinde “kişisel veriler” yeni bir değer olarak görülmüş, bunun sonucunda kaynağını özel hayatın gizliliğinden ve insan onuru hakkından bulan, kişilik hakkına dayanan, aynı zamanda diğer birçok hak ile ilişkisi olan kendine özgü bağımsız bir hak olarak “kişisel verilerin korunması hakkı” gündeme gelmiştir.

Türk hukukunda kişisel verilerin korunması hakkı temel bir hak olarak ilk defa 2010 yılında Anayasa değişikliği ile gündeme gelmiştir. Değişikliğin öncesinde TCK'da kişisel verilerin korunmasına yönelik suç tiplerinin yer almasına karşın; bu suç tiplerinin nasıl irdelenmesi gerektiği yönünde teori ve uygulama eksikliği bulunmaktaydı. Nihayet 2016 yılında kişisel verilerin korunmasına ilişkin özel bir kanun olan KVKK yürürlüğe girmiş, teori ve uygulama eksikliğinin giderilmesi yönünde büyük bir adım atılmıştır.

Çalışmada TCK'nın 136. maddesinde yer alan “*Verileri hukuka aykırı olarak verme veya ele geçirme*” suçu incelenmiştir. Ancak bu suçun incelenmesine geçmeden önce; konunun okuyuculara daha anlaşılabilir bir şekilde aktarılabilmesi için ilk olarak kişisel veriler ile ilgili kavramsal açıklamalarda bulunulmuş, kişisel verilerin korunmasının hukuksal gelişiminin tarihi ele alınmıştır. Sonrasında KVKK'nın ceza, ceza muhakemesi ve diğer bazı hukuk dalları ile ilişkisi ortaya konulmuştur. Nihayet, TCK'nın 136. maddesinde yer alan suç tipi farklı görüşlerle birlikte ele alınmıştır. Bunun sonucunda gerek KVKK'da gerekse TCK'da birtakım önemli değişikliklerin yapılması gerektiği fikri oluşmuştur.

İlk olarak, TCK'nın 135 vd. maddelerinde yer alan suç tiplerinin KVKK'ya uygun bir şekilde “*Kişisel verilerin işlenmesi*” olarak tek çatı altında toplanması gerekir. Nitekim KVKK'nın 17. maddesinde kişisel verilere ilişkin suçlar bakımından TCK'nın 135 vd. maddelerinin uygulanacağı belirtilmiş ise de “*kişisel veri işleme*” ifadesi yalnızca kişisel

verilerin kaydedilmesini, verilmesini, yayılmasını, ele geçirilmesini veya silinmesini ifade etmemektedir. Bu doğrultuda, Anayasa’da ve TCK’da yer alan suçta ve ceza kanunilik ilkesinin bir gereği olarak “*kişisel verilerin işlenmesi*” başlı başına bir suç tipi olarak düzenlenmelidir. Böylelikle suçların içtimama ilişkin yargı kararlarının tutarsızlığının da önüne geçilebilir. Diğer yandan TCK’nın 136. maddesi için “*kişisel veriler kaydedilmiş olmalı mı olmamalı mı*” sorusunun cevabına da bir çözüm yaratılmış olacaktır. Belirtilen şekilde bir düzenleme yapılması, TCK’nın 136. maddesinde yer alan “*ele geçirme*” davranışının belirsizliği ve terminolojik olarak uyumsuzluğu nedeniyle de gereklidir. Bu fikrin hayata geçirilmemesi halinde, diğer bir ifadeyle kişisel verilerin verilmesinin, yayılmasının veya ele geçirilmesinin başlı başına bir suç oluşturduğu durumda dahi TCK’nın 136. maddesinde birtakım değişiklikler yapılmalıdır.

TCK’nın 136. maddesinin başlığında “*veri*” ifadesine yer verilirken maddenin metninde ve gerekçesinde “*kişisel veri*” ifadesine yer verilmiştir. Bu anlamda başlık, gerekçe ve metin içerisinde bir uyumsuzluk bulunmaktadır. Nitekim “*veri*” ifadesi ile “*kişisel veri*” ifadesi aynı anlamı taşımamaktadır. Veri, kişisel verinin daha ham halidir. Bu nedenle uyumsuzluğun giderilmesi açısından madde başlığında da “*kişisel veri*” ifadesi kullanılmalıdır.

Yine madde başlığında yalnızca “*verme*” ve “*ele geçirme*” davranışları bulunurken, madde metninde ve gerekçesinde “*yayma*” davranışına da yer verilmiştir. Bu anlamda ikinci bir uyumsuzluk ortaya çıkmaktadır. “*Yayma*” davranışının da suç olarak düzenlenmesinin karşısında bu davranışa madde başlığında yer verilmemesi kanun yapma tekniği açısından uygun değildir. Bu nedenle, uyumsuzluğun giderilmesi için “*yayma*” davranışına da madde başlığında yer verilmesi yerinde olacaktır. Ancak bu durum suçta ve cezada kanunilik ilkesinin zarar görmesine sebebiyet verebilecek nitelikte de olduğundan, esasen KVKK’daki veri işlemenin tanımına da “*verme*”, “*yayma*” ve “*ele geçirme*” ifadeleri eklenmelidir.

Diğer yandan madde metninde ve başlığında “*hukuka aykırı olarak*” ifadesinin kullanılması, yargı mercilerinin “*failde hukuka aykırı hareket etme bilinci*”ni aramasına sebep olabilmektedir. Bunun bir sonucu olarak fail hakkında ilgili suçu işlemeye yönelik kastının bulunmadığı gerekçesiyle beraat kararı verilebilmektedir. Ancak hukuka aykırı hareket etme bilincinin esasen TCK’nın 30. maddesinde yer alan hata hükümleri



çerçevesinde çözümlenmesi gerekmektedir. Bu noktada, madde başlığından ve metninden “*hukuka aykırı olarak*” ifadesi çıkarılmalıdır.

Diğer bir önerimiz kişisel verilerin özel nitelikli kişisel veri olması halinde verilecek cezanın artırılmasına yöneliktir. Üçüncü kişiler tarafından öğrenildiği takdirde ilgili kişinin ayrımcılığa maruz kalmasına sebebiyet verebilecek kişisel veriler, özel nitelikli kişisel veriler olarak düzenlenmiş ve bunların işlenmesi, diğerlerine göre ayrıcalıklı koşullara bağlanmıştır. Dolayısıyla kişisel verilerin özel nitelikli olması halinde, kişisel verilerin korunması hakkına müdahale edilmesi daha katı kurallara bağlanmıştır. KVKK’nın özel nitelikli kişisel verilere verdiği önem ile paralel bir şekilde, verilen, yayılan veya ele geçirilen kişisel verilerin özel nitelikli kişisel veri olması durumunda fail hakkında verilecek cezanın artırılması yönünde TCK’nın 136. maddesine hüküm eklenmelidir. Ancak bundan önce, kılık ve kıyafete ilişkin kişisel verilerin özel nitelikli grubundan çıkarılması isabetli olacaktır. Nitekim kılık ve kıyafete ilişkin her türlü bilginin özel nitelikli kişisel veri sayılmasının bir sonucu olarak günlük hayatta kullanılan kıyafetlere, giyime, kuşama ilişkin bilgilerin de özel nitelikli kişisel veri olması gerekmekte ve bu bilgilerin işlenmesi yalnızca açık rıza veya kanunlarda öngörülmeyle hukuka uygun olarak gerçekleşebilmektedir. Bu durum, bilhassa özel nitelikli kişisel verilerin korunması amacını aşar nitelikte olacaktır. Diğer yandan, kişisel verinin özel nitelikli olup olmadığının tespitinde somut olayın koşullarına göre hareket edilmelidir. Örneğin bir kişinin fiziksel engel durumuna odaklanmış bir fotoğrafının internet ortamında yayılmasında, kişinin söz konusu fotoğrafı özel nitelikli kişisel veri olarak değerlendirilmelidir.

KVKK’da yer alan veri işleme şartları, aynı zamanda TCK’nın 136. maddesi için birer hukuka uygunluk nedenidir. Hukukun bir bütün olarak ele alınmasının sonucu olarak, KVKK’da yer alan uygunluk nedenlerinin de genel hukuka uygunluk nedenleri ile *mümkün olduğu* ölçüde özel düzenlemenin ruhuna aykırı olmayacak şekilde örtüşmesi gerekmektedir. Bu doğrultuda ilk olarak KVKK’da özel nitelikte olmayan kişisel verilerin işlenmesine yönelik açık rıza veri işleme şartı terk edilerek yerine rıza kavramı tercih edilmelidir. Özel nitelikli kişisel verilerin işlenmesi için ise açık rıza veri işleme şartı olarak kalmaya devam etmelidir. Nitekim özel nitelikli kişisel verilere, diğer kişisel verilere nazaran ilgili kişiyi daha korumacı bir şekilde yaklaşılması gerekir. Bu anlamda özel nitelikli kişisel verilerin diğer kişisel verilere nazaran daha sınırlı ve şüpheye yer

vermeyecek bir açıklıkta işlenmesi kabul edilebilir. Dolayısıyla, mehz alınan 95/46/EC sayılı Direktif'te olduğu gibi yalnızca özel nitelikli kişisel verilerin işlenmesine yönelik faaliyetlerde açık rıza alınmalı, diğer kişisel verilerde ise örtülü rıza da bir hukuka uygunluk nedeni olarak kabul edilmelidir.

Veri işleme şartları açısından değişikliğe uğraması gereken bir diğer kural, özel nitelikli kişisel verilerin işlenmesine ilişkin kuraldır. Özel nitelikli olmayan kişisel verilerin işlenmesi için bir hukuka uygunluk nedeni olan “*kanunlarda açıkça öngörülme*”, özel nitelikli kişisel verilerin işlenmesinde “*kanunlarda öngörülme*” olarak ele alınmıştır. Bu durum, özel nitelikli kişisel veriler söz konusu olduğunda kişisel verilerin korunması hakkına müdahalenin “*ucu açık*” ve “*muğlak*” gerekçelerle yapılmasının önünü açmaktadır. Kişisel verilerin korunması hakkına müdahalenin sınırlarının belirsizlik içerisinde olması çok büyük bir risktir. Dolayısıyla özel nitelikli kişisel verilerin işlenmesi için de “*kanunlarda açıkça öngörülme*” veri işleme şartı kullanılmalı, KVKK'nın ilgili maddesinde bu yönde değişiklik yapılmalıdır.

Özel nitelikli kişisel veriler arasında yer alan sağlık ve cinsel hayata ilişkin bilgiler ise 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 ilgili kişinin açık rızası olmaksızın işlenebilir. Dolayısıyla bu verilerin işlenmesi ilk olarak amaç yönünden sınırlandırılmıştır. Ancak bu sınırlandırma, görünürde bir sınırlandırmadır. Nitekim belirtilen amaçlar gerçekten birçok faaliyeti kapsayıcı niteliktedir. Dolayısıyla “*kanunlarda açıkça öngörülme*” şeklinde bir şart getirilmediği takdirde kişisel verilerin işlenmesinin kanuni bir dayanağı olmadan mümkün olacağı anlamına gelebilecektir ki bu, Anayasa'da yer alan temel hak ve özgürlüklerin kanunla sınırlandırılmasının özüyle bağdaşmayacaktır. Nitekim uygulamada sağlık bilgilerinin yetkili kamu kurum ve kuruluşları tarafından çıkarılan bir “*yazı*” ile dahi işlenebilmesinin önü açıktır. Diğer yandan sağlık ve cinsel hayata ilişkin kişisel verilerin işlenmesi kişi yönünden de sınırlandırılmıştır. Ancak “*sır saklama yükümlüsü*” ve “*yetkili kurum ve kuruluşlar*” ifadelerinin muğlaklığı yine bu hakka yapılacak müdahalenin sınırlarının belirlenememesi nedeniyle risklidir. Dolayısıyla KVKK'nın sağlık ve cinsel hayata ilişkin kişisel verilerin işlenmesini ele alan ilgili maddesine ilk olarak sağlık verilerinin “*kanunlarda açıkça öngörülen*” hallerde

işlenebileceğine yönelik hüküm eklenmeli, sonrasında ise sır saklama yükümlüsü ve yetkili kurum ve kuruluşların kimler olabileceği ile ilgili belirsizlik giderilmelidir.

KVKK'nın “Suçlar” başlıklı ve “Kabahatler” başlıklı 17. ve 18. maddeleri de birçok yönden belirsizlik içermektedir. Örneğin hukuka aykırılık halinde verilecek cezanın niteliği ve derecelendirmesi açısından herhangi bir ayırım gözetilmemiştir. Kaldı ki hukuka aykırılığa denk gelen davranışa uygulanacak ceza da açık bir şekilde belirtilmemiştir. Diğer yandan, kişisel veri işleme tanımında yer alan tüm davranışlar suç olarak düzenlenmemiştir. Dolayısıyla KVKK'nın 17. ve 18. maddeleri suçların ve cezaların belirliliği ilkeleri ile uyuşmamaktadır. Anılan maddelerde bu ilkelere uygun bir şekilde düzenleme yapılmalıdır.

Yukarıda belirtilenlerin dışında, KVKK'nın istisna hükümlerinde de birtakım belirsizlikler bulunmaktadır. Örneğin kişisel verilerin istatistik, araştırma ve planlama gibi amaçlarla işlenmesi istisna halinde, “gibi” ifadesinin netliğe kavuşturulması gereklidir. Diğer yandan, kişisel verilerin kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi de bir istisna hali olarak düzenlenmiştir. Ancak bu ifade, kişisel veriyi işleyen kişilerin kanunla görev ve yetki verilmiş kamu kurum ve kuruluşların yanında başka kişiler olabileceği anlamına gelmektedir. Nitekim burada “kapsamında” ifadesinin geniş yorumlanması, kişisel verilerin korunması hakkının ve söz konusu istisna hükmünün özüne zarar verebilir. Diğer yandan, belirtilen faaliyetlerin kapsamının genişliği, kişisel verinin net olarak hangi faaliyetlerle ilgili olarak işleneceğinin öngörülememesine sebep olmaktadır. Dolayısıyla bu belirsizliğin giderilmesi için söz konusu faaliyetlere ilgili maddede daha açık bir şekilde yer verilmelidir. Bunun dışında, ilgili kişinin devletin gücü karşısında zayıf konumda olduğu dikkate alındığında, tam istisna hallerinde KVKK'nın genel ilkelerini de içine alacak şekilde tamamen bir muafiyet sağlanması, kişisel verilerin korunması hakkının özünü bağdaşmamaktadır. Genel ilkeler arasında yer alan “işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma” ilkesinin istisna hallerinde kısmen uygulanması gereklidir. Özellikle ilgili kişinin temel hak ve özgürlükleri ile devletin yükümlülüklerini yerine getirmesi arasında bir denge kurulmalıdır.

Devlet yükümlülüklerini yerine getirirken önleyici kolluk faaliyetleri, ceza muhakemesi işlemleri ve ceza infaz işlemlerinde kişilerin en mahrem bilgilerini işlemektedir. Bu veri

işleme süreçlerine yönelik yasal düzenlemelerin, KVKK'nın genel ilkeleri ile kimi zaman uyumlu, kimi zamansa uyumsuz olduğu görülmektedir. Örneğin söz konusu veri işleme süreçlerinde özellikle kişisel verinin ne kadar süre ile tutulacağı, nasıl imha edileceği, kişisel veriye kimler tarafından erişim sağlanabileceği gibi hususların düzenlenmediği görülmektedir. Bu nedenle, KVKK'nın genel ilkeleri ile de uyumlu bir şekilde, kişisel verilerin işlenmesini öngören yasal düzenlemelere kişisel veri işleme süreçleri ile ilgili kurallar getirilmelidir.

Bir başka önerimiz, TCK'nın 136. maddesinin 2. fıkrasında ve 137. maddesinin 1. fıkrasının b bendinde yer alan ve bağlaçlarının veya olarak değiştirilmesidir. Kişisel verileri verme, yayma veya ele geçirme suçunun nitelikli hali olarak TCK'nın 136. maddesinin 2. fıkrasında, "*Suçun konusunun, CMK'nın 236. maddesinin beşinci ve altıncı fıkraları uyarınca kayda alınan **beyan ve görüntüler** olması durumunda*" verilecek cezanın artırılacağı düzenlenmiştir. Esasen bu düzenlemeyle kanun koyucunun davranışı daha ağır bir yaptırıma tabi tutarak hukukî değerini daha çok korunmasını sağlamaya çalıştığı açıktır. Ne var ki "*beyan ve görüntüler*" ifadesinin tercih edilmesi, bu amacın tam tersiyle sonuçlanmaktadır. Nitekim yalnızca beyan veya yalnızca görüntünün söz konusu olduğu durumda fail hakkında TCK'nın 136. maddesinin 2. fıkrasından değil, TCK'nın 136. maddesinin 1. fıkrasından hüküm kurulacaktır. Dolayısıyla ilgili maddede yer alan "*beyan ve görüntüler*" ifadesi, amaçla paralel bir şekilde "*beyan veya görüntüler*" olarak değiştirilmelidir. Suçun diğer bir nitelikli hali olan TCK'nın 137. maddesinin 1. fıkrasının b bendinde "*Belli bir **meslek ve sanatın** sağladığı kolaylıktan yararlanmak suretiyle*" işlenmesi halinde cezanın artırılacağı düzenlenmiştir. Ancak anılan madde hükmünde "*ve*" bağlacının kullanılması kişinin her iki niteliğe de sahip olması anlamına gelmektedir. Bu itibarla, anlam karışıklığına mahal verilmemesi adına "*meslek ve sanat*" ifadesi "*meslek veya sanat*" olarak değiştirilmelidir.

Bir diğer önemli husus ise, kişisel verilerin veri sorumlusundan veri işleyene aktarılmasında uygulanacak kurallara ilişkindir. KVKK'nın aktarıma ilişkin 8. maddesi halihazırda veri sorumlusundan veri işleyene yapılan aktarımlarda da uygulanmaktadır. Ticari hayatın ve uygulamanın mevcut koşulları gözetildiğinde aynı faaliyette aynı kişisel verinin işlenmesine yönelik iki ayrı açık rıza almak kabul edilebilir değildir. İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, KVKK'nın 8. maddesindeki şartların veri sorumlusundan veri işleyene yapılan aktarımlar bakımından gözden

geçirilmesi gereklidir. Bu deęişiklięin sonucu, durum, TCK'nın 136. maddesinde düzenlenen kişisel verileri verme, yayma veya ele geçirme suçunun oluşup oluşmadığının tespiti açısından da oldukça önemlidir.

Son olarak, yargı mercilerinin TCK'nın 136. maddesiyle TCK'nın 134. maddesi arasında bir ayırım yaparken kişisel verinin özel hayata ilişkin olması halinde TCK'nın 134. maddesinin uygulanması gerektięi yönünde bir tutum sergiledikleri görülmektedir. Ancak bu durum uzun vadede, kişisel verinin korunmasına özgülennmiş KVKK'nın uygulanmaması yönünde bir sonucu da beraberinde getirebilir. Bu nedenle TCK'nın 134. maddesi ile TCK'nın 135 vd. maddelerinin birlikte ele alındığı suçlarda (örneğin bir kişisel verinin aynı zamanda özel hayata ilişkin bir bilgi olduğu durumlarda) öncelik, TCK'nın 135 vd. maddelerinin uygulanması yönünde olmalıdır.

**KİTAP, MAKALE VE TEZLER**

**Akça**, Kürşat, “*Anayasa Mahkemesi Kararlarında Mülkiyet Hakkı*,” İnönü Üniversitesi Hukuk Fakültesi Dergisi Özel Sayı Cilt:1, Yıl 2015 ss. 543-596.

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

**Akdur**, Recep, *Türkiye’de Sağlık Hizmetleri ve Avrupa Topluluğu Ülkeleri ile Kıyaslanması*, Ankara Üniversitesi Basımevi, 3. Baskı, Ankara, 2000.

**Akgül**, Aydın, *Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması*, Beta Yayınları, İstanbul, 2014.

**Akipek**, Jale / **Akıntürk**, Turgut / **Ateş**, Derya: *Türk Medeni Kanunu Başlangıç Hükümleri Kişiler Hukuku*, Beta Yayınları, c.1, 14. Baskı, İstanbul, 2018.

**Akkurt**, Sinan Sami, “*Kişisel Veri Kavramının Hukuki Niteliğine İlişkin Yaklaşımlara Mukayeseli Bir Bakış*”, *Kişisel Verileri Koruma Dergisi*, Cilt: 2, Sayı: 1, ss. 20-32.

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

**Akyıldız**, Anıl, *Soruşturma Evresinde Gizliliğin İhlali Suçu*, Sosyal Bilimler Enstitüsü Yayınlanmamış Yüksek Lisans Tezi, Özyeğin Üniversitesi, İstanbul, 2020.

**Akyürek**, Güçlü, *Özel Hayatın Gizliliğini İhlal Suçu*, Seçkin Yayıncılık, Ankara – 2014.

**Aliusta**, Cahit / **Benzer**, Recep, “*Avrupa Siber Suçlar Sözleşmesi ve Türkiye’nin Dahil Olma Süreci*”, *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, Cilt:4, No:2, 2018, ss. 35-42.

**Altunkaş**, Aysun / **Ataç**, Asiye Selcen, “*6222 Sayılı Kanun Kapsamında Seyirden Yasaklama (m. 18)*”, *Marmara Üniversitesi Hukuk Fakültesi Dergisi*, Cilt: 16, Sayı: 1-2, Haziran – Temmuz 2017, ss. 69-109.

**Arslan**, Zühtü, “*Temel Hak ve Özgürlüklerin Sınırlanması: Anayasa’nın 13. Maddesi Üzerine Bazı Düşünceler*”, *Anayasa Yargısı*, Cilt: 19, Ankara 2002, ss. 139-155.

**Artuk**, M. Emin / **Gökçen**, Ahmet / **Alşahin**, M. Emin / **Çakır**, Kerim, *Ceza Hukuku Genel Hükümler*, Adalet Yayınevi, Ankara, 2017, (**Artuk / Gökçen / Alşahin / Çakır**, Genel Hükümler).

<sup>1018</sup> Çalışmada yararlanılan ve aynı zamanda internet ortamında bulunan kaynakların erişim tarihleri, ilgili oldukları dipnotlarda belirtilmiştir. Bunun yanında, internet ortamında bulunan tüm kaynaklara 21.11.2021 tarihinde tekrardan erişim sağlanmış, bu kaynakların ulaşılabilirlikleri teyit edilmiştir.

**Artuk**, M. Emin / **Gökçen**, Ahmet / **Alşahin**, M. Emin / **Çakır**, Kerim, *Ceza Hukuku Özel Hükümler*, Adalet Yayınevi, Yenilenmiş ve Gözden Geçirilmiş 19. Baskı, Ankara 2021, (**Artuk / Gökçen / Alşahin / Çakır**, Özel Hükümler).

**Aşıkoğlu**, Şehriban İpek, *Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri*, On İki Levha Yayınları, 1. Baskı, İstanbul, Kasım 2018.

**Atlı**, Turan, “*Kişisel Verilerin Önleyici, Koruyucu ve İstihbari Faaliyetler Amacıyla İşlenmesi*”, Necmettin Erbakan Üniversitesi Hukuk Fakültesi Dergisi, C: 2, S: 1, 2019, ss. 4-22.

**Avcıoğlu**, Nur Halet, *Türk Hukukunda Kişisel Verilerin Korunması Hakkı*, Yayımlanmamış Yüksek Lisans Tezi, T.C. Konya Karatay Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Yüksek Lisans Programı, Konya, 2018.

**Aydoğdu**, Yasin, “*Kamu İdaresinde Kişisel Verilerin Korunması*”, Selçuk Üniversitesi Hukuk Fakültesi Dergisi, 2021, Cilt: 29, Sayı: 1, (263-293).

**Ayözger Öngün**, A. Çiğdem, *Kişisel Verilerin Korunması Hukuku (Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil)*, Beta Yayınevi, İstanbul, 2019.

**Balogh**, Erin P. / **Miller**, Bryan T. / **Ball**, John R., “*National Academies of Sciences, Engineering and Medicine*”, Improving Diagnosis in Health Care, Ed. Washington DC, The National Academies Press, 2015.

**Bartow**, Ann, “*Our Date, Ourselves: Privacy, Protortization and Gender*”, USFL Rev., 1999, Cilt: 34, ss. 633-704.

**Basan**, Nuri Mehmet / **Bilir**, Nazmi, “*Koruyucu Sağlık Hizmetlerinde Önleme Çelişkisi ve Nedenleri*”, TAF Preventive Medicine Bulletin, C.XV, No:1, 2016, ss. 44-50.

**Başalp**, Nilgün, “*Avrupa Birliği Veri Koruması Genel Regülasyonu'nun Temel Yenilikleri*”, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, C.XXI, S.1, 2015, ss. 77-105, (**Başalp**, Temel Yenilikler).

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

**Başara**, Gamze Turan, *Kişiliğin İhlalinden Kaynaklanan Maddi ve Manevi Tazminat ile Haksız Kazancın İadesi*, Turhan Kitapevi, Ankara, 2018.

**Belge**, Ayşe Merve, “*Özellikle Kişisel Verilerin Korunması Kanunu Çerçevesinde İşçilerin Kişisel Verilerinin İhlali ve Korunması Yolları*”, Dokuz Eylül Hukuk Fakültesi Dergisi, Prof. Dr. Ertaş'a Armağan, C.19, Özel Sayı, ss. 1025-1051.

**Beytar**, Erbil, *İşçinin Kişiliğinin ve Kişisel Verilerinin Korunması*, On İki Levha Yayınları, İstanbul, 2018.

**Bilge**, Mehmet Emin, *Ticari Sırların Korunması*, Asil Yayın, 2. Baskı, Ankara 2005.

**Boga**, Betül Gamze, *Ceza Muhakemesinde Kişisel Verilerin Korunması*, Yayımlanmamış Yüksek Lisans Tezi, T.C. Necmettin Erbakan Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Kamu Hukuku Bilim Dalı, Konya 2021.

**Bozkurt Yüksel**, Armağan Ebru, *Bulut Bilişimde Kişisel Verilerin Korunması (Personal Data Protection on Cloud Computing)*, Yetkin Yayınları, 2016.

**Börekçi**, Eşref Barış, *Kişisel Verileri Verme, Yayma veya Ele Geçirme Suçu*, On İki Levha Yayıncılık, 1. Baskı – İstanbul, Kasım 2020.

**Braun**, Cihan Avcı, “*Kişisel Verilerin İşlenmesindeki Rıza*”, Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, C.XV, 2018/1, ss. 13-33.

**Büyükcay**, Yusuf, “*Hekimin Sır Saklama Yükümlülüğü*”, Atatürk Üniversitesi Erzincan Hukuk Fakültesi Dergisi, C. VIII, S. 1-2 (2004), ss. 383-396.

**Bygrave**, Lee A., *Data Privacy Law An International Perspective*, Oxford University Press, The United Kingdom, 2014.

**Can**, Neslihan, *Kolluk ve Adli Makamlar Tarafından İşlenen Kişisel Verilerin Korunması*, On İki Levha Yayıncılık, 1. Baskı, İstanbul, Şubat 2021.

**Centel**, Nur / **Zafer**, Hamide / **Çakmut**, Özlem, *Türk Ceza Hukukuna Giriş*, Yayınları, Yenilenmiş ve Gözden Geçirilmiş 11. Bası, İstanbul, 2020.

**Centel**, Nur / **Zafer**, Hamide, *Ceza Muhakemesi Hukuku*, Beta Yayınları, 16. Baskı, İstanbul 2019.

**Clarke**, E.A., “*What is Preventive Medicine?*”, Official Publication of The College of Family Physicians of Canada, C.XX, No:11, 1974, ss. 65-68.

**Çekin**, Mesut Serdar, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu*, On İki Levha Yayıncılık, 2. Baskı, İstanbul, 2019.

**Çilingiroğlu**, Cüneyt, *Tıbbi Müdahaleye Ceza*, Filiz Kitapevi, İstanbul, 1993.

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

**Derdiman**, Cengiz R. / **Tataroğlu**, Nihan, “*Devletin Gözetimi ile İnsan Haklarının Uyumlaştırılması Sorunu ve Çözüm Önerileri*”, İstanbul Üniversitesi Hukuk Fakültesi Dergisi, Cilt: 7, Sayı: 1, 2016, ss. 247-293.

**Determann**, Lothar, *Kişisel Verilerin Korunması Uygulama Kılavuzu – Şirketlerin Uluslararası Mevzuata Uyumunu*, On İki Levha Yayıncılık, 1. Baskı, İstanbul, Ocak 2020, Çeviri: Av. Hilal Temel.

**Develioğlu**, Hüseyin Murat, *6698 Sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku*, On İki Levha Yayıncılık, İstanbul, 2017.



**Dođan**, Buse, *Kişisel Verilerin İşlenme Şartları Bağlamında Açık Rıza*, Yayımlanmamış Yüksek Lisans Tezi, T.C. İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk Anabilim Dalı, İstanbul, 2019.

**Donay**, Süheyl, *Meslek Sırrının Açıklanması Suçu*, İstanbul, Sulhi Garan Matbaası Varisleri Kollektif Şirketi, 1978.

**Dursun**, Yonca, *Kişisel Verilerin Korunması Kanunu Kapsamında İşçinin Korunması*, Seçkin Yayıncılık, 1. Baskı, Ocak 2021.

**Dülger**, Murat Volkan, *Bilişim, Kişisel Verilerin Korunması ve İnternet İletişimi Mevzuatı*, , Seçkin Yayıncılık, 4.Baskı, İstanbul, 2018, (**Dülger**, Bilişim).

**Dülger**, Murat Volkan, *Kişisel Verilerin Korunması Hukuku*, Hukuk Akademisi Yayıncılık, 3. Baskı, İstanbul, Haziran 2020, (**Dülger**, Kişisel Verilerin Korunması).

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

**Epözdemir**, Rezan, “*Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme Suçu (TCK m. 136)*” Terazi Hukuk Dergisi, Cilt: 14, Sayı: 151, Mart 2019, ss. 528-544.

**Erarslan Türkmen**, Sevgi, *Özel Nitelikli Kişisel Verilerin İşlenmesinde Açık Rızanın Aranmadığı Haller*, On İki Levha Yayıncılık, İstanbul 2019.

**Erbaş**, Rahime, *Türk Hukukunda ve Karşılaştırmalı Hukukta Sağlık Mesleği Mensuplarının Suçu Bildirme Yükümlülüğü*, On İki Levha Yayıncılık, İstanbul Ceza Hukuku ve Kriminoloji Arşivi Yayını, No: 4, İstanbul, 2015.

**Erdoğan**, Yavuz, “*Kişisel Verilerin Korunması Bakımından Türk Ceza Kanunu Hükümlerinin Değerlendirilmesi*”, Erciyes Üniversitesi Hukuk Fakültesi Dergisi Prof. Dr. Dođan Soyaslan Armađanı, C: VIII, S: 2, Y: 2013, ss. 569-632.

**Erem**, Faruk, “*Ceza Hukukunda Meslek Sırrı*”, Ankara Üniversitesi Hukuk Fakültesi Dergisi, C. I, No: 1, 1943, ss. 35-72.

**Eren**, Fikret, *Borçlar Hukuku Genel Hükümler*, Yetkin Yayınları, 21. Bası, Ankara, 2017.

**Ergün**, İsmail, *Siber Suçların Cezalandırılması ve Türkiye’de Durum*, Adalet Yayınevi, Ankara, 2008.

**Fişek**, Nusret, “*Sađlık Hizmetleri ve İşçi Sađlığı Ailelerinin Sađlık Sorunları*”, Modern Yönetim Semineri, Türk-İş Yayınları, No: 144, 1982.

**Göçmen Uyarer**, Sinem, *Kişisel Verilerin Korunması kanunu ve Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması*, Seçkin Yayıncılık, Güncellenmiş 2. Baskı, Ankara 2020.

**Gültekin Várkonyi**, Gizem, “*Avrupa Birliđi Genel Veri Koruma Tüzüğü Kapsamında Gerçek Kişilerin Kişisel Sosyal Robot Kullanımından Doğabilecek Sorumlulukları*”, Kişisel Verileri Koruma Dergisi, Cilt: 2, Sayı: 2, ss. 19-29.

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

**Hafizoğulları**, Zeki / **Özen**, Muharrem, “*Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar*” Ankara Barosu Dergisi, Yıl: 67, Sayı: 4, Güz 2009, ss. 9-22.

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

**Henkoğlu**, Tülay, *Bilgi Güvenliği ve Kişisel Verilerin Korunması*, Yetkin Yayınları, Ankara, 2015.

**Hizarci**, Emine, *6698 sayılı Kişisel Verilerin Korunması Kanununun AB Veri Koruma Hukuku Işığında Değerlendirilmesi*, Yetkin Yayınları, Ankara 2020.

**İmançlı**, Canan, *Kişisel Sağlık Verilerinin Korun(a)mamasından Doğan Özel Hukuk Sorumluluğu*, On İki Levha Yayıncılık, 1. Baskı, İstanbul, Nisan 2020.

**İnci**, Z. **Özen**, “*Şüpheli ve Sanığa Rağmen Bir Ceza Muhakemesi Hukuku Mu? Şüpheli ve Sanığın Ceza Muhakemesi İşlemlerine Katlanma Yükümlülüğü ve Bu Yükümlülüğün Sınırları Hakkında Düşünceler*”, Hacettepe Hukuk Fakültesi Dergisi, 7 (2), 2017, ss. 119-168.

**İtişgen**, Rezzan, “*Türk Ceza Hukukunda Kişisel Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme Suçu*”, Türkiye Adalet Akademisi Dergisi, 6 (23), 2015, ss. 179-202.

**Janger**, Edward J., “*Privacy Property, Information Costs and the Anticommons*”, Hastings LJ, 2002, Cilt: 54, ss. 899-929.

**Kalyon**, Arzu, *Türk Vergi Hukukunda Kişisel Verilerin Korunması*, Seçkin Yayıncılık, Ankara 2021.

**Kaneti**, Selim, *Haksız Fiilde Hukuka Aykırılık Sorunu*, Kazancı Hukuk Yayınları, İstanbul, 2007.

**Kang**, Jerry, “*Information Privacy in Cyberspace Transactions*”, Stanford Law Review, 1998, ss. 1193-1294.

**Kangal**, Zeynel T., *Ceza Hukukunda Zorunluluk Durumu*, Seçkin Yayıncılık, 1. Baskı, Ankara, Mart 2010, (**Kangal**, Zorunluluk).

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

**Karagülmez**, Ali, *Bilişim Suçları ve Soruşturma – Kovuşturma Evreleri*, Seçkin Yayıncılık, Genişletilmiş ve Gözden Geçirilmiş 5. Baskı, Ankara, 2014.

**Karakehya**, Hakan, “*Dolaylı Maddi Gerçek: Ceza Muhakemesinde Yargılama Makamının Maddi Gerçeğe Deliller Aracılığıyla Ulaşma Zorunluluğu Üzerine*”, Türkiye Adalet Akademisi Dergisi, Yıl: 7, Sayı: 27, Temmuz 2016, ss. 59-82.

- Karasu**, Sinem, *Hekimin Sır Saklama Yükümlülüğü*, Vedat Kitapçılık, İstanbul, 2009.
- Katoğlu**, Tuğrul, *Ceza Hukukunda Hukuka Aykırılık*, Seçkin Yayıncılık, Ankara 2003, (**Katoğlu**, Hukuka Aykırılık).
- Katoğlu**, Tuğrul, “*Ceza Hukukunda Suçun Mağduru Kavramının Sınırları*”, Ankara Üniversitesi Hukuk Fakültesi Dergisi, C. 61 (2), 2012, ss. 657-693, (**Katoğlu**, Mağdur Kavramının Sınırları).
- Kaya**, Cemil, “*Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi*”, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, C. LXIX, No:1-2, 2011, ss. 317-334.
- Ketizmen**, Muammer, *Türk Ceza Hukukunda Bilişim Suçları*, Adalet Yayınevi, Ankara 2008.
- Kılınç**, Doğan, “*Anayasal Bir Hak Olarak Kişisel Verilerin Korunması*”, Ankara Üniversitesi Hukuk Fakültesi Dergisi, 61 – 3, 2012, ss. 1089-1169.
- Koca**, Mahmut / **Üzülmez**, İlhan, *Türk Ceza Hukuku Özel Hükümler*, Adalet Yayınevi, Gözden Geçirilmiş ve Genişletilmiş 7. Baskı, Ankara 2020.
- Kocayusufpaşaoğlu**, Necip, *Borçlar Hukukuna Giriş, Hukuki İşlem Sözleşme*, Cilt: 1, Filiz Kitapevi, 5. Bası, İstanbul 2010.
- Koç**, Buğrahan, *Tıp Alanında Kişisel Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme Suçu*, Yayımlanmamış Yüksek Lisans Tezi, T.C. İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, İstanbul, 2019.
- Kolenoğlu**, Mustafa, *Sağlık Mesleği Mensuplarının Sır Saklama ve Suçu Bildirmeme (ihbar) Yükümlülüğü*, Yayımlanmamış Yüksek Lisans Tezi, T.C. İstanbul Üniversitesi Adli Tıp Enstitüsü Sosyal Bilimler Anabilim Dalı, İstanbul, 2009.
- Korkmaz**, İbrahim, “*Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme*”, TBB Dergisi 2016 (124), ss. 81-152, (**Korkmaz**, Değerlendirme).
- Korkmaz**, İbrahim, *Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması*, Ankara, Seçkin Yayıncılık, 2019, (**Korkmaz**, Ceza Hukuku).
- Köse Aysun**, Melike, *Kişisel Verilerin Kaydedilmesi Suçu (TCK m. 135)*, Seçkin Yayıncılık, Ankara, 2018.
- Kuner**, Christopher, *European Data Protection Law (Corporate Compliance and Regulation)*, Second Edition, Oxford, 2007.
- Kuşkonmaz**, Elif Mendos, *Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması*, Yayımlanmamış Yüksek Lisans Tezi, T.C. İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, İstanbul 2013.
- Küzeci** Elif, “*İstatistikî Birimler ve Bilgilerin Geleceğini Belirleme Hakkı*”, Türkiye ve Ortadoğu Amme İdaresi Enstitüsü İnsan Hakları Yıllığı, C: 32, 2014, ss. 53-75, (**Küzeci**, İstatistikî Birimler).

**Küzeci**, Elif, *Kişisel Verilerin Korunması*, Turhan Kitapevi, Yenilenmiş ve Gözden Geçirilmiş Üçüncü Bası, Ankara, Şubat 2019, (**Küzeci**, *Kişisel Verilerin Korunması*).

**Lambert**, Paul, *Understanding the New European Data Protection Rules*, New York, CRC Press Taylor & Francis Group, 2018.

**Lessig**, Lawrence, “*Provacancy as Property*”, *Social Research*, 2002, Cilt: 69, Sayı 1, ss. 247-269.

**Litman**, Jessica, “*Information Privacy/Information Property*”, *Stanford Law Review*, 2000, Cilt: 52, ss. 1283-1313.

**Maden**, Mehmet, *Ceza Hukukunda Kişisel Verilerin Korunması*, Adalet Yayınevi, Birinci Baskı, Mayıs, Ankara 2021.

**Mutlu**, Muhammet Sefa, *Kişisel Verilerin Soruşturma Evresinde İşlenmesi ve İnsan Hakları Kapsamında Korunması*, Seçkin Yayıncılık, Ocak 2020.

**Nadezhda**, Purtova, “*Property Rights in Personal Data: Learning from the American Discourse*”, *Computer Law & Security Review*, Vol. 25, No. 6, 2009, ss. 507-521.

**Oğuz**, Sefer, “*Kişisel Verilerin Korunması Hukukunun Genel İlkeleri*”, *Bilgi Ekonomisi ve Yönetim Dergisi*, 2018, 13:2, ss. 121-138.

**Orak**, Beşir, *Kişisel Sağlık Verilerinin Korunması*, Yetkin Yayınları, 1. Baskı, Nisan 2020.

**Ömeroğlu**, Ömer, “*Ceza Muhakemesinde Şüpheli ve Sanığın Fiziki Kimlik Tespiti*”, *TBB Dergisi*, 2014 – 115, ss. 61-102.

**Önder**, Nesibe, “*6698 Sayılı Kanun’un Öngörmüş Olduğu Kişisel Veri İşleme Şartları Nelerdir?*”, *Veri Güvenliği ve Kişisel Verileri Koruma Derneği Bülteni*, E-Dergi, 1. Sayı, 2020, İstanbul.

**Önok**, R. Murat / **Önay**, Işıl, “*Hukuk Düzeninin Birliği İlkesi Çerçevesinde Zorunluluk Hâlinin Hukukî Niteliği*”, *İstanbul Hukuk Mecmuası*, 77 – 2, ss. 847-895.

**Özbek**, Veli Özer / **Doğan**, Koray / **Bacaksız**, Pınar, *Ceza Muhakemesi Hukuku*, Seçkin Yayıncılık, 12. Baskı, Ankara 2019, (**Özbek / Doğan / Bacaksız**, *Ceza Muhakemesi*)

**Özbek**, Veli Özer / **Doğan**, Koray / **Bacaksız**, Pınar, *Türk Ceza Hukuku Genel Hükümler*, Seçkin Yayıncılık, Güncellenmiş ve Gözden Geçirilmiş 11. Baskı, Ankara 2020, (**Özbek / Doğan / Bacaksız**, *Genel Hükümler*).

**Özbek**, Veli Özer / **Doğan**, Koray / **Bacaksız**, Pınar, *Türk Ceza Hukuku Özel Hükümler*, Seçkin Yayıncılık, Genişletilmiş ve Güncellenmiş 15. Baskı, Ankara 2020, (**Özbek / Doğan / Bacaksız**, *Özel Hükümler*).

**Özbek**, Veli Özer / **Doğan**, Koray, “*Zorunluluk Halinin (TCK m. 25/2) Hukuki Niteliği*”, *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi* Cilt: 9, Sayı 2, 2007, ss. 195-222.

**Özbek**, Veli Özer, “*Tıp Ceza Hukukunda DNA İncelemesi*”, V. Türk-Alman Tıp Hukuku Sempozyumu, Ankara, Türkiye Barolar Birliği Yayını, 2008, (**Özbek**, Tıp Ceza Hukuku).

**Özbek**, Veli Özer, *Yeni Türk Ceza Kanunu'nun Anlamı (TCK İzmir Şerhi)*, Madde 76-169, C: II, Ankara, 2008.

**Özcan**, Göknül, *Bankacılık İş ve İşlemlerinde Kişisel Verilerin Korunması*, 1. Baskı, On İki Levha Yayıncılık, İstanbul, Ocak 2020.

**Özdemir**, Hayrunnisa, “*Haberleşmenin Gizliliği ve Kişisel Veriler*”, Erzincan Üniversitesi Hukuk Fakültesi Dergisi, 13(1-2), 2009, ss. 285-303, (**Özdemir**, Haberleşmenin Gizliliği).

**Özdemir**, Hayrunnisa, “*Hadım Etme ve Hekimin Sır Saklama Yükümlülüğü*”, Gazi Üniversitesi Hukuk Fakültesi Dergisi, C. XIV, Y. 2010, Sa. 1, ss. 125-164, (**Özdemir**, Sır Saklama).

**Özdemir**, Hayrunnisa, *Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması*, Seçkin Yayıncılık, Ankara, 2009, (**Özdemir**, Elektronik Haberleşme).

**Özel**, Sibel, *Uluslararası Alanda Medya ve İnternette Kişilik Hakkının Korunması*, Seçkin Yayıncılık, Ankara, 2004.

**Özen**, Mustafa, *Ceza Hukuku Genel Hükümler Dersleri*, Adalet Yayınevi, Ankara, 2020.

**Özer Deniz**, Miray, “*İşçilerin Özel Nitelikli Kişisel Verilerinin Korunması ve Bundan Doğan Sorumluluk*”, Türkiye Adalet Akademisi Dergisi, Yıl: 12, Sayı: 45, Ocak 2021, ss. 355-378.

**Özgenç**, İzzet, *Türk Ceza Hukuku Genel Hükümler*, Seçkin Yayıncılık, Gözden Geçirilmiş ve Güncellenmiş 16. Bası, Ankara 2020.

**Parlar**, Ali / **Çobanoğlu**, Yekta, *Özel Hayat ve Hayatın Gizli Alanına Karşı Suçlar (TCK 132. – 140. Md)*, Aristo Yayınevi, 1. Baskı, İstanbul, Haziran 2018.

**Polat**, Alperen, *Sorumluluk Hukukunda Rıza*, On İki Levha Yayıncılık, İstanbul, 2019.

**Saka**, Rıza / **Çağlayan**, Ramazan / **Koca**, Mahmut, *Avrupa Birliği Hukuku, İdare Hukuku ve Ceza Hukuku Açısından, Kişisel Verilerin İmhası*, Seçkin Yayıncılık, 1. Baskı, Ocak, 2021.

**Salihpaşaoğlu**, Yaşar, “*Özel Hayatın Kapsamı: Avrupa İnsan Hakları Mahkemesi İçtihatları Işığında Bir Değerlendirme*,” Gazi Üniversitesi Hukuk Fakültesi Dergisi C. XVII, Y. 2013, Sayı: 3, ss. 227-266.

**Sarıgül**, Ali Tanju, “*Şüpheli ve Sanığın Ceza Muhakemesi İşlemlerine Katılma Yükümlülüğüne Getirilen Sınır-Nemo Tenetur Seipsum Accusare İlkesi*”, TBB Dergisi 2021 (153), ss. 39-64.

**Sarıusta**, Kader, *Kişisel Verilerin Ceza Hukuku Yoluyla Korunması*, T.C. Gaziantep Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Ana Bilim Dalı Yüksek Lisans Tezi, Gaziantep, Temmuz 2018.

**Sert**, Şeyma, *Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması*, Seçkin Yayıncılık, Şubat 2019, Ankara.

**Seyhan**, Kazım / **Eryılmaz**, Bedri M., “*Gelişmiş Ülkeler ve Türkiye Uygulamasında Suç Önleme Stratejileri*”, Liberal Düşünce Dergisi, Bahar 2004, ss. 5-34.

**Sınar**, Hasan, “*Kişisel Verileri Hukuka Aykırı Olarak Verme, Yayma veya Ele Geçirme Suçu (TCK Md. 136)*”, *Kişisel Verileri Koruma Dergisi*, Cilt: 2, Sayı: 1, ss. 33-62.

**Singh**, Atul, “*Protecting Personal Data as a Property Right*,” *ILI Law Review*, Winter Issue 2016.

**Slepian**, Michael L. / **Chun**, Jinseok S. / **Mason**, Malia F., “*The Experience of Secrecy*”, *Journal of Personality and Social Psychology*, C. CXIII, No: 1, 2017, ss. 1-33.

**Solove**, Daniel J., “*The New Vulnerability: Data Security and Personal Information*”, *GW Law Faculty Publications & Other Works, Faculty Scholarship*, 2008, ss. 111-136.

**Soyaslan**, Doğan, *Ceza Hukuku Genel Hükümler*, Yetkin Yayınları, Güncellenmiş 9. Baskı, Ankara, 2020.

**Soyaslan**, Doğan, *Ceza Hukuku Özel Hükümler*, Yetkin Yayınları, 8. Baskı, Ankara, 2010.

**Subaşı**, İlhan, *Hekimin Aydınlatma Yükümlülüğü, Aydınlatılmış Onam, Tazminat Sorumluluğu*, Seçkin Yayıncılık, Ankara, 2016.

**Şen**, Ersan, *Ceza Hukuku Perspektifinden Güncel Olaylara Bakış, Yorumluyorum – 1*, Seçkin Yayıncılık, Ankara, 2011, (Şen, Ceza Hukuku).

**Şen**, Ersan, *Yeni Türk Ceza Kanunu Yorumu*, Cilt: 1, Vedat Kitapçılık, İstanbul 2006, (Şen, Yorum).

**Şimşek**, Oğuz, *Anayasa Hukukunda Kişisel Verilerin Korunması*, Beta Yayınevi, Ankara, 2008, (Oğuz Şimşek).

**Şimşek**, Suat, “*Mülkiyet Hakkının Kapsamı, Sınırlandırma Nedenleri ve şartları Açısından 1982 Anayasası ve Avrupa İnsan Hakları Sözleşmesi: Karşılaştırmalı Bir Analiz – I*”, *TBB Dergisi* 2010 (91), ss. 181-228.

**Şimşek**, Zeynep, “*Sağlığı Geliştirmenin Tarihsel Gelişimi ve Örneklerle Sağlığı Geliştirme Stratejileri*”, *TAF Preventive Medicine Bulletin*, C. XII, No: 3, 2013, ss. 343-358.

**Taranto**, Lill, “*Data Protection Principles*”, *European Privacy: Law and Practice for Data Protection Professionals*, ed.: Eduardo Ustran, IAPP publication, USA, 2012.

**Taşkın**, Şaban Cankat, *Bilişim Suçları*, Beta Basım, Birinci Baskı, İstanbul, Kasım 2008.

**Taştan**, Furkan Güven, *Türk Sözleşme Hukukunda Kişisel Verilerin Korunması*, On İki Levha Yayıncılık, 2. Baskı, İstanbul, Kasım 2017.

**Tezcan**, Durmuş, “*Bilgisayar Karşısında Özel Hayatın Korunması*”, Anayasa Yargısı 8, Anayasa Mahkemesinin 29.Kuruluş Yıldönümü Sempozyumu, 25 – 27 Nisan 1991, Ankara, ss. 385-392.

**Toroslu**, Nevzat / **Toroslu**, Haluk, *Ceza Hukuku Genel Kısım*, Savaş Yayınları, Ankara, Eylül 2019.

**Toroslu**, Nevzat, *Ceza Hukukunda Zaruret Hali*, Sevinç Matbaası, Ankara – 1968.

**Tuğrul**, Saim, *Kamu Hukuku Açısından Mülkiyet Hakkı ve Sınırlandırılması*, Kazancı Hukuk Yayınları, İstanbul, 2004.

**Turan**, Metin, *Karşılaştırmalı Hukukta Kişisel Verilerin Korunması*, Seçkin Yayıncılık, Güncellenmiş 2. Baskı, Ankara, Nisan 2019.

**Türkmen**, Ali, *Hasta ve Hekim Hukuku*, Adalet Yayınevi, 2. Baskı, Ankara 2013.

**Uçak**, Murat, “*Kişisel Verilerin Hukuka Uygun İşlenmesinde Çocuğun Rızası*”, Kişisel Verileri Koruma Dergisi, Cilt: 3 Sayı: 1, 2021, ss. 41-60.

**Uğurluoğlu**, Ece / **Özgen**, Hacer, “*Sağlık Hizmetleri Finansmanı ve Hakkaniyet*”, Hacettepe Sağlık İdaresi Dergisi, C. XI, No: 2, 2008, ss. 133-160.

**Uğurluoğlu**, Özgür / **Çelik**, Yusuf, “*Sağlık Sistemleri Performans Ölçümü, Önemi ve Dünya Sağlık Örgütü Yaklaşımı*”, Hacettepe Sağlık İdaresi Dergisi, C. VIII, No: 1, 2005, ss. 3-29.

**Uncular**, Selen, *İş İlişkisinde İşçinin Kişisel Verilerinin Korunması*, Seçkin Yayıncılık, Güncellenmiş ve Genişletilmiş 2. Baskı, Ankara, Ekim 2018.

**Uşan**, Fatih, *İş Sırrının Korunması (Sır Saklama ve Rekabet Yasağı)*, Seçkin Yayıncılık, Ankara, 2003.

**Uygun**, Murat, *Avrupa Birliğinin 95/46 Sayılı Veri Koruma Yönergesi Işığında Kişisel Verilerin Korunması*, Yayımlanmamış Yüksek Lisans Tezi, T.C. Gazi Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk Anabilim Dalı, Ankara, 2010.

**Üçok**, Kağan, “*Koruyucu Hekimlik ve Acil İlk Yardımda Pratik Bilgiler*”, Bizim Ereğli, No:3, Konya, Konya Ereğli Halk Eğitimi Merkezi ve Akşam Sanat Okulu Yayını, 1991, ss. 13-15.

**Ünver**, Yener / **Hakeri**, Hakan, *Ceza Muhakemesi Hukuku*, Cilt: 1, Adalet Yayınevi, 15. Baskı, Ankara 2019.

**Üzeltürk Tahmazoğlu**, Sultan, “*Kişisel Verilerin Korunması Hakkında Anayasa Değişikliği*”, Legal Hukuk Dergisi, Sayı: 93, Eylül 2010, ss. 3151-3156.

**Üzeltürk**, Sultan, *1982 Anayasası ve İnsan Hakları Avrupa Sözleşmesine Göre Özel Hayatın Gizliliği Hakkı*, Beta Yayıncılık, İstanbul, 2004.

**Voigt, Paul / Bussche, Axelvondem**, *The EU General Data Protection Regulation (GDPR)*, SpringerLink, İsviçre, 2017.

**Yağlıdere**, Umut Emre, “*Sağlık Hukuku Açısından Sır Saklama Yükümlülüğüne Genel Bir Bakış*”, Veri Güvenliği ve Kişisel Verileri Koruma Derneği Bülteni, E-Dergi, 1. Sayı, İstanbul (Yağlıdere, Sır Saklama Yükümlülüğü).

**Yağlıdere**, Umut Emre, “*Sağlık Mesleği Mensuplarının Suçu Bildirmemesi Suçu*”, T.C. Kadir Has Üniversitesi Hukuk Fakültesi Dergisi, Cilt: 6, Sayı: 1, Haziran 2018, Prof. Dr. Mustafa Dural Anısına, Özel Sayı – III, ss. 59-79, (Yağlıdere, Suçu Bildirmeme).

**Yaşar, Osman / Gökcan, Hasan Tahsin / Artuç, Mustafa**, *Yorumlu Uygulamalı Türk Ceza Kanunu*, 3. Cilt, 2. Baskı, Adalet Yayınları, Ankara 2014.

**Yavuz, Can**, *İnternetteki Arama Sonuçlarından Kişisel Verilerin Kaldırılması*, Seçkin Yayıncılık, Güncellenmiş ve Genişletilmiş 3. Baskı, Ankara 2020.

**Yenisey, Feridun**, *Kolluk Hukuku*, Beta Yayınları, 2. Baskı, İstanbul, 2015.

**Yılmaz, Sabire Sanem**, “*Video Gözetimi, Yapay Zekâ ve Kişisel Verilerin Korunması Hakkı*”, (Yılmaz, Gözetim), erişim için bkz.: <https://www.hukukihaber.net/video-gozetimi-yapay-zeka-ve-kisisel-verilerin-korunmasi-hakki-makale.7001.html>.

**Yılmaz, Sabire Sanem**, *Tıp Alanında Kişisel Verilerin Korunması*, Seçkin Yayıncılık, Güncellenmiş 5. Baskı, Ankara, 2021, (Yılmaz, Kişisel Veriler).

**Yılmaz, Süleyman / Çavuşoğlu, Gökçe Filiz**, *Kişisel Verileri Koruma Hukuku*, Yetkin Yayınları, Ankara, 2020.

**Yokuş Sevük, Handan**, “*Tıp Ceza Hukukunda Kişisel Verilerin Açıklanması*”, V. Türk-Alman Tıp Hukuku Sempozyumu, Ankara, Türkiye Barolar Birliği Yayını, 2008.

**Yücedağ, Nafiye**, “*Kişisel Verilerin Korunması Kanunu Kapsamında Genel İlkeler*”, Kişisel Verileri Koruma Dergisi, Cilt:1, Sayı:1, ss. 47-63, (Yücedağ, Genel İlkeler).

**Yücedağ, Nafiye**, “*Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu'nun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri*”, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, C. LXXV, S.2, 2017, ss. 765-789, (Yücedağ, Hukuka Uygunluk Sebepleri).

**Zeytin, Zafer**, “*Hekimin Sır Saklama Yükümlülüğü*”, Orijinal Araştırma, Türkiye Klinikleri J Med Ethics 2006, Sayı: 14, ss. 77-82.

**Zor, Abdülhamid**, *Veri Sorumlusunun Yükümlülükleri ve Bu Yükümlülükleri İhlalinden Doğan Özel Hukuk Sorumluluğu*, On İki Levha Yayıncılık, 1. Baskı, İstanbul, Ekim 2020.

**Walden, I. N. / Savage, R. N.**, “*Data Protection and Privacy Laws: Should Organizations Be Protected?*”, International and Comparative Law Quarterly, 1988, Cilt 37, Sayı 2, ss. 337-347.



## ULUSLARARASI BELGE, GÖRÜŞ, SÖZLEŞME, REHBER VE RAPORLAR

1. 24.10.1995 tarihli ve 1995/46/EC sayılı Kişisel Verilerin İşlenmesi ve Serbestçe Dolaşımını Bakımından Bireylerin Korunmasına İlişkin Direktif (*Protection of Individuals with regard to the Processing of Personal Data and on Free Movement of Such Data*), erişim için bkz.: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN>.
2. 28.1.1981 tarihli ve 108 sayılı Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Avrupa Konseyi Sözleşmesi (*The Convention of the Protection of Individuals with regard to Automatic Processing of Personal Data No. 108*), erişim için bkz.: <https://rm.coe.int/1680078b37>
3. 29. Madde Çalışma Grubu'nun 04/2007 sayılı görüş yazısı (*on the concept of personal data*), erişim için bkz.: [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf)
4. 29. Madde Çalışma Grubu, 1/2010 sayılı görüş yazısı (*on the concepts of "controller" and "processor"*), erişim için bkz.: [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf)
5. 29. Madde Çalışma Grubu, 15/2011 sayılı görüş yazısı (*on the definition of consent*), erişim için bkz.: [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf)
6. 29. Madde Çalışma Grubu, 03/2013 sayılı görüş yazısı (*on purpose limitation*), erişim için bkz.: [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf)
7. 29. Madde Çalışma Grubu, 06/2014 sayılı görüş yazısı (*legitimate interest*), erişim için bkz.: [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf)
8. 29. Madde Çalışma Grubu, 20.04.2011 tarihli Özel Veri Kategorisine İlişkin Tavsiye Belgesi (*Advice Paper on Special Categories of Data "Sensitive Data"*), erişim için bkz.: [https://ec.europa.eu/justice/article-29/documentation/other-document/files/2011/2011\\_04\\_20\\_letter\\_artwp\\_mme\\_le\\_bail\\_directive\\_9546ec\\_annex1\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf)
9. 29. Madde Çalışma Grubu, 10107/05/EN-WP 105 numaralı çalışması (*Working document on data protection issues related to RFID technology*), erişim için bkz.: [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp105\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp105_en.pdf)

10. Avrupa Konseyi Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'ne Ek 181 nolu Denetleyici Makamlar ve Sınırşan Veri Akışına İlişkin Protokol (*Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Regarding Supervisory Authorities and Transborder Data Flows*), erişim için bkz.: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/181>
11. Avrupa İnsan Hakları Sözleşmesi (*Convention on Cybercrime*), erişim için bkz.: [https://www.echr.coe.int/documents/convention\\_tur.pdf](https://www.echr.coe.int/documents/convention_tur.pdf)
12. Avrupa Konseyi Biyoloji ve Tıbbın Uygulanması Bakımından İnsan Hakları ve İnsan Haysiyetinin Korunması Sözleşmesi (*Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine*), erişim için bkz.: <http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168007cf98>
13. Avrupa Konseyi Siber Suç Sözleşmesi, erişim için bkz.: <http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561>
14. Avrupa Veri Koruma Kurulu (European Data Protection Board)'nun 05/2020 sayılı rehberi (Guidelines 05/2020 on consent under Regulation 2016/679), erişim için bkz.: [https://edpb.europa.eu/sites/default/files/files/file1/edpb\\_guidelines\\_202005\\_consent\\_en.pdf](https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf)
15. Avrupa Birliği Veri Koruma Tüzüğü (*General Data Protection Regulation*), erişim için bkz.: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1374-1-1>
16. Birleşmiş Milletler Bilgisayarla İşlenen Kişisel Veri Dosyalarına İlişkin Yönlendirici İlkeler, (Guidelines Concerning Computerized Personal Data Files), erişim için bkz.: <http://hrlibrary.umn.edu/instree/q2grcpd.htm>
17. Birleşmiş Milletler Bireysel ve Siyasal Haklar Uluslararası Sözleşmesi, erişim için bkz.: [https://diabgm.adalet.gov.tr/arsiv/sozlesmeler/coktarafli-soz/bm/bm\\_05.pdf](https://diabgm.adalet.gov.tr/arsiv/sozlesmeler/coktarafli-soz/bm/bm_05.pdf)
18. Birleşmiş Milletler İnsan Hakları Evrensel Beyanamesi, erişim için bkz.: <https://www.hsk.gov.tr/Eklentiler/Dosyalar/9a3bfe74-cdc4-4ae4-b876-8cb1d7eeae05.pdf>
19. Birleşmiş Milletler Şartı, erişim için bkz.: [https://inhak.adalet.gov.tr/Resimler/SayfaDokuman/2212020141836bm\\_01.pdf](https://inhak.adalet.gov.tr/Resimler/SayfaDokuman/2212020141836bm_01.pdf)

20. Devlet Denetleme Kurulu'nun 27.11.2013 tarihli ve 2013/3 sayılı “*Kişisel Verilerin Korunmasına İlişkin Ulusal ve Uluslararası Durum Değerlendirmesi ile Bilgi Güvenliği ve Kişisel Verilerin Korunması Kapsamında Gerçekleştirilen Denetim Çalışmaları*” adlı denetim raporu, raporun bir kısmına erişim için bkz.: [https://www.ttb.org.tr/images/stories/file/2015/ddk\\_rapor.pdf](https://www.ttb.org.tr/images/stories/file/2015/ddk_rapor.pdf)
21. ICO, *Guide to GDPR*, erişim için bkz.: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/>
22. Kişisel Verilerin Yetkili Otoritelerce Suçların Önlenmesi, Soruşturulması, Ortaya Çıkarılması veya Kovuşturulması veya Cezaların İnfazı Amacıyla İşlenmesiyle İlgili Gerçek Kişilerin Korunmasına ve Bu Verilerin Serbest Dolaşımına İlişkin 2016/680 sayılı Direktif (*Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA*), erişim için bkz.: [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L\\_.2016.119.01.0089.01.ENG](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0089.01.ENG)
23. OECD Kişisel Verilerin Sınırtaşan Trafiği ve Verilerin Korunmasına İlişkin Rehber İlkeleri (*Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*), erişim için bkz.: <https://www.oecd.org/digital/ieconomy/oecdguidelinesontheprivacyandtransborderflowsofpersonaldata.htm#guidelines>
24. OECD *Privacy Framework*, erişim için bkz.: [https://www.oecd.org/sti/ieconomy/oecd\\_privacy\\_framework.pdf](https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf)
25. T.C. Kalkınma Bakanlığı İktisadi sektörler ve koordinasyon genel müdürlüğü Bilgi Toplumu Dairesi Başkanlığı, Çalışma Raporu – 6, Ayşe Nur Akıncı, Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi, erişim için bkz.: [http://www.bilgitoplumu.gov.tr/wp-content/uploads/2017/07/AB\\_Veri\\_Koruma\\_Tuzugu.pdf](http://www.bilgitoplumu.gov.tr/wp-content/uploads/2017/07/AB_Veri_Koruma_Tuzugu.pdf)
26. ABD Teknoloji ve Gizlilik Danışma Kurulu'nun Terörizmle Mücadelede Gizliliği Korunması Raporu (*Report of the Technology and Privacy Advisory Committee - Safeguarding Privacy in the Fight Against Terrorism*), Mart 2004, ABD, erişim için bkz.: <https://cdt.org/wp-content/uploads/security/usapatriot/20040300tapac.pdf>
27. World Health Organization, “*Health Systems Financing*”, Haziran 2008, s. 2, erişim için bkz.:

[https://www.who.int/healthinfo/statistics/toolkit\\_hss/EN\\_PDF\\_Toolkit\\_HSS\\_Financing.pdf](https://www.who.int/healthinfo/statistics/toolkit_hss/EN_PDF_Toolkit_HSS_Financing.pdf)

## AIHM KARARLARI

1. AIHM *Niemietz v. Germany* kararı, başvuru numarası: 13710/88, karar tarihi: 16.12.1992, erişim için bkz.:  
[https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-57887%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57887%22]})
2. AIHM *Costello-Roberts v. The United Kingdom* kararı, başvuru numarası: 13134/87, karar tarihi: 25.03.1991, erişim için bkz.:  
[https://hudoc.echr.coe.int/tur#{%22itemid%22:\[%22001-57804%22\]}](https://hudoc.echr.coe.int/tur#{%22itemid%22:[%22001-57804%22]})
3. AIHM *Von Hannover v. Germany* kararı, başvuru numarası: 59320/00, karar tarihi: 24.09.2004, karara erişim için bkz.:  
[https://hudoc.echr.coe.int/tur#{%22itemid%22:\[%22001-61853%22\]}](https://hudoc.echr.coe.int/tur#{%22itemid%22:[%22001-61853%22]})
4. AIHM *Rotaru v. Romania* kararı, başvuru numarası: 28341/95, karar tarihi: 04.05.2000, karara erişim için bkz.:  
[https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-58586%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-58586%22]})
5. AIHM *Satakunnan Markkinapörssi Oy ve Satamedia Oy v. Finland* kararı, başvuru numarası: 931/13, karar tarihi: 27.06.2016, erişim için bkz.:  
[https://hudoc.echr.coe.int/tur#{%22fulltext%22:\[%22931/13%22\],%22itemid%22:\[%22001-175121%22\]}](https://hudoc.echr.coe.int/tur#{%22fulltext%22:[%22931/13%22],%22itemid%22:[%22001-175121%22]})

## AYM KARARLARI

1. AYM'nin 2006/167 E., 2008/86 K., sayılı ve 20.03.2008 tarihli kararı, erişim için bkz.:  
<https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2008/86?EsasNo=2006%2F167>, AYM'nin 2008/44 E., 2011/21 K. sayılı ve 20.01.2011 tarihli kararına erişim için bkz.:  
<https://normkararlarbilgibankasi.anayasa.gov.tr/Dosyalar/Kararlar/KararPDF/2011-21-nrm.pdf>

2. AYM'nin 2013/122 E., 2014/74 K. sayılı ve 09.04.2014 tarihli kararına erişim için bkz.: <https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2014/74?EsasNo=2013%2F122>
3. AYM'nin 2013/83 E., 2014/183 K. sayılı ve 04.12.2014 tarihli kararına erişim için bkz.: <https://www.lexpera.com.tr/resmi-gazete/metin/anayasa-mahkemesinin-4-12-2014-tarihli-ve-e-2013-84-k-2014-183-sayili-karari>
4. AYM'nin 2014/180 E., 2015/30 K. sayılı ve 19.03.2015 tarihli kararına erişim için bkz.: <https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2015/30?EsasNo=2014%2F180>
5. AYM'nin 2014/90 E., 2014/180 K. sayılı ve 04.12.2014 tarihli kararına erişim için bkz.: <https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2014/180?EsasNo=2014%2F90>
6. AYM'nin 2015/32 E., 2015/102 K. sayılı ve 12.11.2015 tarihli kararına erişim için bkz.: <https://normkararlarbilgibankasi.anayasa.gov.tr/Dosyalar/Kararlar/KararPDF/2015-102-nrm.pdf>
7. AYM'nin 2016/125 E., 2017/143 K. sayılı ve 28.09.2017 tarihli kararına erişim için bkz.: <https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2017/143?EsasNo=2016%2F125>
8. AYM'nin 2013/2941 başvuru numaralı ve 11.05.2016 tarihli kararına erişim için bkz.: <https://kararlarbilgibankasi.anayasa.gov.tr/BB/2013/2941?BasvuruNoYil=2013&BasvuruNoSayi=2941>.
9. AYM'nin 2017/24776 başvuru numaralı ve 24.05.2018 tarihli kararına erişim için bkz.: <https://kararlarbilgibankasi.anayasa.gov.tr/BB/2017/24776>
10. AYM'nin 2014/7256 başvuru numaralı ve 27.02.2019 tarihli ve kararı, erişim için bkz.: <https://kararlarbilgibankasi.anayasa.gov.tr/BB/2014/7256>

## YARGITAY KARARLARI

1. Yargıtay 8. Ceza Dairesi'nin 2016/12565 E. ve 2017/12892 K. sayılı, 20.11.2017 tarihli kararı (Lexpera)
2. Yargıtay 11. Ceza Dairesi'nin 2015/8796 E., ve 2017/5266 K. sayılı ve 10.07.2017 tarihli kararı (Yargıtay Bilgi Bankası)
3. Yargıtay 12. Ceza Dairesi'nin 2012/22005 E. ve 2013/24489 K. sayılı, 04.11.2013 tarihli kararı (Yargıtay Bilgi Bankası)
4. Yargıtay 12. Ceza Dairesi'nin 2013/10672 E. ve 2013/15772 K. sayılı, 10.06.2013 tarihli kararı (Kazancı İçtihat Bilgi Bankası)
5. Yargıtay 12. Ceza Dairesi'nin 2013/27402 E., 2014/15379 K. sayılı ve 23.06.2014 tarihli kararı (Lexpera)
6. Yargıtay 12. Ceza Dairesi'nin 2014/17630 E. ve 2015/1672 K. sayılı, 02.02.2015 tarihli kararı (Kazancı İçtihat Bilgi Bankası)
7. Yargıtay 12. Ceza Dairesi'nin 2014/18783 E. ve 2015/2124 K. sayılı, 09.02.2015 tarihli kararı (Yargıtay Bilgi Bankası)
8. Yargıtay 12. Ceza Dairesi'nin 2014/607 E., 2014/16665 K. sayılı ve 07.07.2014 tarihli kararı (Lexpera)
9. Yargıtay 12. Ceza Dairesi'nin 2015/10994 E., 2017/635 K. sayılı ve 01.02.2017 (Yargıtay Bilgi Bankası)
10. Yargıtay 12. Ceza Dairesi'nin 2015/13192 E. ve 2017/3451 K. sayılı, 26.04.2017 tarihli kararı (Yargıtay Bilgi Bankası)
11. Yargıtay 12. Ceza Dairesi'nin 2015/4006 E. ve 2015/18748 K. sayılı, 02.12.2015 tarihli kararı (Yargıtay Bilgi Bankası)
12. Yargıtay 12. Ceza Dairesi'nin 2015/4349 E. ve 2016/5349 K. sayılı, 30.03.2016 tarihli kararı (Yargıtay Bilgi Bankası)
13. Yargıtay 12. Ceza Dairesi'nin 2015/9893 E. ve 2016/12504 K. sayılı, 09.11.2016 tarihli kararı (Yargıtay Bilgi Bankası)
14. Yargıtay 12. Ceza Dairesi'nin 2016/1129 E. ve 2017/6742 K. sayılı, 27.09.2017 tarihli kararı (Yargıtay Bilgi Bankası)

15. Yargıtay 12. Ceza Dairesi'nin 2017/12083 E. ve 2018/2539 K. sayılı, 07.03.2018 tarihli kararı (Kazancı İçtihat Bilgi Bankası)
16. Yargıtay 12. Ceza Dairesi'nin 2017/1613 E. ve 2018/3978 K. sayılı, 04.04.2018 tarihli kararı (Lexpera)
17. Yargıtay 12. Ceza Dairesi'nin 2017/3570 E. ve 2018/808 K. sayılı, 24.01.2018 tarihli kararı (Yargıtay Bilgi Bankası)
18. Yargıtay 12. Ceza Dairesi'nin 2018/2226 E. ve 2018/8746 K. sayılı, 26.09.2018 tarihli kararı (Yargıtay Bilgi Bankası)
19. Yargıtay 12. Ceza Dairesi'nin 2018/8108 E. ve 2019/3141 K. sayılı ve 06.03.2019 tarihli kararı (Yargıtay Bilgi Bankası)
20. Yargıtay 12. Ceza Dairesi'nin 2018/8152 E. ve 2019/4886 K. sayılı, 10.04.2019 tarihli kararı (Kazancı İçtihat Bilgi Bankası)
21. Yargıtay 12. Ceza Dairesi'nin 2018/8198 E. ve 2019/6187 K. sayılı, 27.02.2019 tarihli kararı (Yargıtay Bilgi Bankası)
22. Yargıtay 12. Ceza Dairesi'nin 2018/8300 E. ve 2019/6862 K. sayılı, 29.05.2019 tarihli kararı (Lexpera)
23. Yargıtay 12. Ceza Dairesi'nin 2018/8313 E. ve 2019/8077 K. sayılı, 03.07.2019 tarihli kararı (Kazancı İçtihat Bilgi Bankası)
24. Yargıtay 12. Ceza Dairesi'nin 2018/8369 E. ve 2019/8318 K. sayılı, 10.07.2019 tarihli kararı (Yargıtay Bilgi Bankası)
25. Yargıtay 12. Ceza Dairesi'nin 2019/1011 E. ve 2020/1112 K. sayılı, 05.02.2020 tarihli kararı (Yargıtay Bilgi Bankası)
26. Yargıtay 12. Ceza Dairesi'nin 2019/894 E. ve 2020/845 K. sayılı, 22.01.2020 tarihli kararı (Kazancı İçtihat Bilgi Bankası)
27. Yargıtay 12. Ceza Dairesi'nin 2019/973 E. ve 2020/218 K. sayılı, 08.01.2020 tarihli kararı (Kazancı İçtihat Bilgi Bankası)
28. Yargıtay 15. Ceza Dairesi'nin 2013/612 E., 2014/14715 K. sayılı ve 16.09.2014 tarihli kararı (Yargıtay Bilgi Bankası)
29. Yargıtay 15. Ceza Dairesi'nin 2015/1659 E. ve 2018/2748 K. sayılı, 18.04.2018 tarihli kararı (Lexpera)

30. Yargıtay 17. Ceza Dairesi'nin 2015/25941 E. ve 2018/126 K. sayılı, 08.01.2018 tarihli kararı (Yargıtay Bilgi Bankası)
31. Yargıtay 9. Hukuk Dairesi'nin 10.01.2019 tarihli, 2018/10718 E. ve 2019/559 K. sayılı kararı (Yargıtay Bilgi Bankası)
32. Yargıtay Ceza Genel Kurulu'nun., 2012/12-1510 E. ve 2014/331 K., sayılı ve 17.06.2014 tarihli kararı (Kazancı İçtihat Bilgi Bankası)

## KİŞİSEL VERİLERİ KORUMA KURULU KARARLARI

1. Kişisel Verileri Koruma Kurulu'nun "*Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler*" ile ilgili 31.01.2018 tarihli ve 2018/10 sayılı kararına erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/4110/2018-10>
2. Kişisel Verileri Koruma Kurulu'nun "*Açık rızanın hizmet şartına bağlanması*" ile ilgili kararına erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/5412/Acik-Rizanın-Hizmet-Sartina-Baglanması>
3. Kişisel Verileri Koruma Kurulu'nun "*Amazon Turkey Perakende Hizmetleri Limited Şirketi*" ile ilgili 27.02.2020 tarihli ve 2020/173 sayılı karar özetine erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/6739/2020-173>
4. Kişisel Verileri Koruma Kurulu'nun "*Belediyede memur olarak görev yapan ilgili kişinin, veri sorumlusu bünyesinde işe giriş çıkış takibinin biyometrik veri işlenerek yapılması*" ile ilgili 01.12.2020 tarihli ve 2020/915 sayılı karar özetine erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/6872/2020-915>
5. Kişisel Verileri Koruma Kurulu'nun "*Bir bankanın, ilgili kişinin cep telefonu numarasını bankaya verilmiş amacı dışında kullanması*" ile ilgili 18.09.2019 tarihli ve 2019/277 sayılı karar özetine erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/5545/2019-277>
6. Kişisel Verileri Koruma Kurulu'nun "*Bir gazete tarafından ilgili kişinin özel nitelikli kişisel verileri hakkında haber yapılması*" ile ilgili 09.12.2019 tarihli ve 2019/372 sayılı karar özetine erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/6663/2019-372>
7. Kişisel Verileri Koruma Kurulu'nun "*Bir havayolu taşımacılık şirketinin (veri sorumlusu) sunduğu sadakat programını kullanan ilgili kişinin kullanıcı adı ve parola bilgilerini değiştirme talebi karşısında ilgili kişiden arkalı önlü kimlik*



*görüntüsü talep eden veri sorumlusu*” ile ilgili 01.10.2019 tarihli ve 2019/294 sayılı karar özetine erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/6556/2019-294>

8. Kişisel Verileri Koruma Kurulu’nun “*Bir market zincirinin sadakat kart uygulamasına ilişkin ihbar ve şikayetler*” ile ilgili 25.03.2019 tarihli ve 2019/82 sayılı karar özetine erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/5463/-Bir-market-zincirinin-sadakat-kart-uygulamasina-iliskin-ihbar-ve-sikayetler-hakkinda-Kisisel-Verileri-Koruma-Kurulunun-25-03-2019-tarihli-ve-2019-82-sayili-Karari>
9. Kişisel Verileri Koruma Kurulu’nun “*Bir sigorta şirketinin ilgili kişiye vereceği hizmeti açık rıza şartına bağlaması sebebiyle Kuruma iletilen şikâyet*” ile ilgili 03.09.2020 tarihli ve 2020/667 sayılı karar özetine erişmek için bkz.: <https://www.kvkk.gov.tr/Icerik/6878/2020-667>
10. Kişisel Verileri Koruma Kurulu’nun “*Bir varlık yönetim şirketinin ilgili kişiye aynı konu ile ilgili birden çok mesaj gönderimi*” ile ilgili 31.05.2019 tarihli ve 2019/159 sayılı karar özetine erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/5494/2019-159>
11. Kişisel Verileri Koruma Kurulu’nun “*Biyometrik imza verisinin kullanılmasına ilişkin görüş talebi*” ile ilgili ile ilgili 27.08.2020 tarihli ve 2020/649 sayılı karar özetine erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/6815/2020-649>
12. Kişisel Verileri Koruma Kurulu’nun “*Facebook*” hakkında 11.04.2019 tarihli ve 2019/104 sayılı karar özetine erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/5450/2019-104>
13. Kişisel Verileri Koruma Kurulu’nun “*İş Başvurusu Sürecinde İşlenen Kişisel Verilerin Hukuka Aykırı Şekilde Paylaşılması*” ile ilgili kararına erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/5410/Is-Basvurusu-Surecinde-Islenen-Kisisel-Verilerin-Hukuka-Aykiri-Sekilde-Paylasilmasi>
14. Kişisel Verileri Koruma Kurulu’nun “*İşlenme Amacının Gerektirdiğinden Fazla Kişisel Veri İşlenmesi/Aktarılması*” ile ilgili karar özetine erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/5413/Islenme-Amacinin-Gerektirdiginden-Fazla-Kisisel-Veri-Islenmesi-Aktarilmasi-Veri-Minimizasyonu-Ilkesine-Aykirilik->
15. Kişisel Verileri Koruma Kurulu’nun “*Kanunda Yer Alan Genel İlkelere Aykırı Şekilde Kişisel Veri İşlenmesi*” ile ilgili karar özetine erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/5417/Kanunda-Yer-Alan-Genel-Ilkelere-Aykiri-Sekilde-Kisisel-Veri-Islenmesi-Hukuka-ve-Durustluk-Kurallarına-Uygun-Olma-ile-Belirli-Acik-Ve-Mesru-Amaclar-Icin-Isleme-Ilkelerine-Aykiri-Kisisel-Veri-Islenmesi->

16. Kişisel Verileri Koruma Kurulu'nun "*Kişilerin ad ve soyadı ile arama motorları üzerinden yapılan aramalarda çıkan sonuçların indeksten çıkarılmasına yönelik talepler*" ile ilgili 23.06.2020 tarihli ve 2020/481 sayılı kararına erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/6776/2020-481>
17. Kişisel Verileri Koruma Kurulu'nun "*Spor salonu hizmeti sunan veri sorumlusunun, üyelerinin giriş-çıkış kontrolünü biyometrik veri işleyerek yapması*" ile ilgili 27.02.2020 tarihli ve 2020/167 sayılı karar özetine erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/6738/2020-167>
18. Kişisel Verileri Koruma Kurulu'nun "*Spor salonu hizmeti sunan veri sorumlularının, üyelerinin giriş-çıkış kontrolünü biyometrik veri işleyerek yapması*" ile ilgili 31.05.2019 tarihli ve 2019/165 sayılı karar özetine erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/5496/2019-81-165>
19. Kişisel Verileri Koruma Kurulu'nun "*Ulaşım hizmeti sunan bir mobil uygulama kapsamında işlenen kişisel veriler*" ile ilgili 27.01.2020 tarihli ve 2020/65 sayılı karar özetine erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/6717/2020-65>
20. Kişisel Verileri Koruma Kurulu'nun "*Veri sorumluları tarafından kişilerin telefon numarası, e-posta adresi gibi iletişim kanallarına Kanuna aykırı şekilde gönderilen üçüncü kişilere ait kişisel veriler*" ile ilgili 22.12.2020 tarihli ve 2020/966 sayılı ilke kararına erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/6858/2020-966>
21. Kişisel Verileri Koruma Kurulu'nun "*Veri sorumlusu işveren tarafından, iş sözleşmesi tek taraflı olarak feshedilen ve işe iade davası açan ilgili kişiye ait özlük dosyasında yer alan sağlık raporunun dava savunmasında kullanılmak suretiyle mahkemeye sunulması*" ile ilgili 18.02.2020 tarihli ve 2020/138 sayılı karar özetine erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/6887/2020-138>
22. Kişisel Verileri Koruma Kurulu'nun "*Veri sorumlusunun kanuni yükümlülüğünü yerine getirmek için işlediği kişisel verileri meşru menfaat çerçevesinde kullanma talebiyle Kuruma yapmış olduğu başvuru*" ile ilgili 25.03.2019 tarihli ve 2019/78 sayılı karar özetine erişim için bkz.: <https://kvkk.gov.tr/Icerik/5434/2019-78>
23. Kişisel Verileri Koruma Kurulu'nun "*Veri sorumlusunun, web sitesinde kişisel verilerin işlenmesini hizmet şartı olarak talep ettiği ve aydınlatma yükümlülüğünü usulüne uygun yerine getirmediği iddiaları*" ile ilgili 08.07.2019 tarihli ve 2019/206 sayılı karar özetine erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/6709/2019-206>
24. Kişisel Verileri Koruma Kurulu'nun "*Yeterli Korumanın Bulunduğu Ülkelerin Tayininde Kullanılmak Üzere Oluşturulan Form*" ile ilgili 02.05.2019 tarihli ve 2019/125 sayılı kararına erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/5469/->

[Yeterli-korumanin-bulundugu-ulkelerin-tayininde-kullanilmak-uzere-olusturulan-form-hakkindaki-02-05-2019-tarihli-ve-2019-125-sayili-Kurul-Karari](#)

25. Kişisel Verileri Koruma Kurulu'nun 24.01.2019 tarihli ve 2019/10 sayılı kararına ilişkin duyuruya erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirimi>
26. Kişisel Verileri Koruma Kurulu'nun 28.09.2021 tarihli ve 2021/980 sayılı kararına ilişkin duyuruya erişim için bkz.: <https://kvkk.gov.tr/Icerik/7055/COVID-19-PCR-TEST-SONUCU-VE-ASI-BILGISI-UYGULAMALARINA-ILISKIN-KAMUOYU-DUYURUSU>

## KİŞİSEL VERİLERİ KORUMA KURUMU YAYINLARI

1. Kişisel Verileri Koruma Kurumu, *6698 Sayılı Kişisel Verilerin Korunması Kanununun Uygulanmasına Yönelik Soru Cevaplar*, erişim için bkz.: <https://www.kvkk.gov.tr/yayinlar/6698%20SAYILI%20K%C4%B0%C5%9E%C4%B0SEL%20VER%C4%B0LER%C4%B0N%20KORUNMASI%20KANUNUNUN%20UYGULANMASINA%20Y%C3%96NEL%C4%B0K%20SORU%20VE%20CEVAPLAR.pdf>
2. Kişisel Verileri Koruma Kurumu, *6698 sayılı Kişisel Verilerin Korunması Kanunu Hakkında Doğru Bilinen Yanlıklar*, KVKK Yayınları No:13, Nisan 2020, Ankara, erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/6722/6698-Sayili-Kisisel-Verilerin-Korunmasi-Kanunu-Hakkinda-Dogru-Bilinen-Yanlislar>
3. Kişisel Verileri Koruma Kurumu, *6698 Sayılı Kişisel Verilerin Korunması Kanununun Amacı ve Kapsamı*, erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/4185/6698-Sayili-Kisisel-Verilerin-Korunmasi-Kanununun-Amaci-ve-Kapsami#:~:text=Bu%20h%C3%BCkme%20g%C3%B6re%20ama%C3%A7%20ki%C5%9Fisel,uyacaklar%C4%B1%20usul%20ve%20esaslar%C4%B1%20d%C3%BCzenlemektir>
4. Kişisel Verileri Koruma Kurumu, *6698 Sayılı Kişisel Verilerin Korunması Kanun'unun Amacı ve Kapsamı*, erişim için bkz.: <https://kvkk.gov.tr/yayinlar/6698%20SAYILI%20K%C4%B0%C5%9E%C4%B0SEL%20VER%C4%B0LER%C4%B0N%20KORUNMASI%20KANUNUNUN%20AMACI%20VE%20KAPSAMI.pdf>

5. Kişisel Verileri Koruma Kurumu, *Açık Rıza Alırken Dikkat Edilecek Hususlar*, erişim için bkz.: <https://kvkk.gov.tr/Icerik/2037/Acik-Riza-Alirken-Dikkat-Edilecek-Hususlar>
6. Kişisel Verileri Koruma Kurumu, *Açık Rıza*, erişim için bkz.: <https://www.kvkk.gov.tr/yayinlar/A%C3%87IK%20RIZA.pdf>
7. Kişisel Verileri Koruma Kurumu, *Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi*, Nisan 2019, Ankara, s. 23, erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/5394/Aydinlatma-Yukumlulugunun-Yerine-Getirilmesi-Rehberi>
8. Kişisel Verileri Koruma Kurumu, *Biyometrik Verilerin İşlenmesinde Dikkat Edilmesi Gereken Hususlara İlişkin Rehber*, erişim adresi: <https://kvkk.gov.tr/SharedFolderServer/CMSFiles/bd06f5f4-e8cc-487e-abe1-d32dc18e2d7e.pdf>
9. Kişisel Verileri Koruma Kurumu, *Kişisel Veri Güvenliği Rehberi*, KVKK Yayınları, Ankara, Ocak 2018, erişim için bkz.: [https://www.kvkk.gov.tr/yayinlar/veri\\_guvenligi\\_rehberi.pdf](https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf)
10. Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler*, erişim için bkz.: <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/32ff74f6-9798-405a-b3d2-b42d28423fde.pdf>
11. Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin Korunması Kanunu'na İlişkin Uygulama Rehberi*, KVKK Yayınları No:1, Aralık 2019, Ankara, erişim için bkz.: <https://kvkk.gov.tr/Icerik/2030/Rehberler>
12. Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin Korunması Kanunu Hakkında Sıkça Sorulan Sorular*, KVKK Yayınları, Mart 2018, Ankara, erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/4196/Kisisel-Verilerin-Korunmasi-Kanunu-Hakkinda-Sikca-Sorulan-Sorular>
13. Kişisel Verileri Koruma Kurumu, *Madde ve Gerekçesi ile Kişisel Verilerin Korunması Kanunu (Bilgi Notu) ve Kişisel Verilerin Korunmasına İlişkin Terimler Sözlüğü*, KVKK Yayınları, Mart 2019, Ankara, erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/5388/Madde-ve-Gerekcesi-ile-Kisisel-Verilerin-Korunmasi-Kanunu-Bilgi-Notu-ve-Kisisel-Verilerin-Korunmasina-Iliskin-Terimler-Sozlugu>
14. Kişisel Verileri Koruma Kurumu, *Örneklerle Kişisel Verilerin Korunması Rehberi*, KVKK Yayınları No:29, Haziran 2019, Ankara, erişim için bkz.: <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/a23bfe08-9b3a-4c2f-8a97-a259dcc0e667.PDF>

15. Kişisel Verileri Koruma Kurumu, *Özel Nitelikli Kişisel Verilerin İşlenme Şartları*, erişim için bkz.: <https://kvkk.gov.tr/SharedFolderServer/CMSFiles/fae2e7c8-f24f-457f-a71d-2d5ed599cf15.pdf>
16. Kişisel Verileri Koruma Kurumu, *Veri Sorumlusu ve Veri İşleyen*, erişim için bkz.: <https://kvkk.gov.tr/SharedFolderServer/CMSFiles/31d9c444-27a5-4a75-95b1-1ca9bdb81ea5.pdf>

## ULUSAL KANUNLAR

- 13.03.1926 tarihli 320 sayılı Resmî Gazete’de yayımlanan 765 sayılı Türk Ceza Kanunu (mülga)
- 06.05.1930 tarihli ve 1489 sayılı Resmî Gazete’de yayımlanan 1593 sayılı Umumi Hıfzısıhha Kanunu
- 14.07.1934 tarihli ve 2751 sayılı Resmî Gazete’de yayımlanan 2559 sayılı Polis Vazife ve Salâhiyet Kanunu
- 12.01.1961 tarihli ve 10705 sayılı Resmî Gazete’de yayımlanan 213 sayılı Vergi Usul Kanunu
- 07/04/1969 tarihli ve 13168 sayılı Resmî Gazete’de yayımlanan 1136 sayılı Avukatlık Kanunu
- 05.02.1972 tarihli ve 14090 sayılı Resmî Gazete’de yayımlanan 1512 sayılı Noterlik Kanunu
- 12.03.1983 tarihli ve 17985 sayılı Resmî Gazete’de yayımlanan 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanunu
- 15.05.1987 tarihli ve 19461 sayılı Resmî Gazete’de yayımlanan 3359 sayılı Sağlık Hizmetleri Temel Kanunu
- 13.06.1989 tarihli ve 20194 sayılı Resmî Gazete’de yayımlanan 3568 sayılı Serbest Muhasebeci Mali Müşavirlik ve Yeminli Mali Müşavirlik Kanunu
- 04.12.1999 tarihli ve 23896 sayılı Resmî Gazete’de yayımlanan 4483 sayılı Memurlar ve Diğer Kamu Görevlilerinin Yargılanması Hakkında Kanun
- 10.06.2003 tarihli ve 25134 sayılı Resmî Gazete’de yayımlanan 4857 sayılı İş Kanunu
- 24.10.2003 tarihli ve 25269 sayılı Resmî Gazete’de yayımlanan 4982 sayılı Bilgi Edinme Hakkı Kanunu

09.12.2003 tarihli ve 25311 sayılı Resmî Gazete’de yayımlanan 5013 sayılı Biyoloji ve Tıbbın Uygulanması Bakımından İnsan Hakları ve İnsan Haysiyetinin Korunması Sözleşmesi: İnsan Hakları ve Biyotıp Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun

26.06.2004 tarihli ve 25504 sayılı Resmî Gazete’de yayımlanan 5187 sayılı Basın Kanunu

26.09.2004 tarihli ve 25611 sayılı Resmî Gazete’de yayımlanarak yürürlüğe giren 5237 sayılı Türk Ceza Kanunu

07.10.2004 tarihli ve 25606 sayılı Resmî Gazete’de yayımlanan 5235 sayılı Adli Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanun

17.12.2004 tarihli ve 25673 sayılı Resmî Gazete’de yayımlanan 5271 sayılı Ceza Muhakemesi Kanunu

29.12.2004 tarihli ve 25685 sayılı Resmî Gazete’de yayımlanan 5275 sayılı Ceza ve Güvenlik Tedbirlerinin İnfazı Hakkında Kanun

31.03.2005 tarihli ve 25772 (Mük.) sayılı Resmî Gazete’de yayımlanan 5326 sayılı Kabahatler Kanunu

15.07.2005 sayılı ve 25876 tarihli Resmî Gazete’de yayımlanan 5395 sayılı Çocuk Koruma Kanunu

01.06.2005 tarihli ve 25832 sayılı Resmî Gazete’de yayımlanan 5352 sayılı Adli Sicil Kanunu

20.07.2005 tarihli ve 25881 sayılı Resmî Gazete’de yayımlanan 5402 sayılı Denetimli Serbestlik Hizmetleri Kanunu

01.11.2005 tarihli ve 25983 (Mük.) sayılı Resmî Gazete’de yayımlanan 5411 sayılı Bankacılık Kanunu

18.11.2005 tarihli ve 25997 sayılı Resmî Gazete’de yayımlanan 5429 sayılı Türkiye İstatistik Kanunu

18.10.2006 tarihli ve 26323 sayılı Resmî Gazete’de yayımlanan 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun

10.11.2008 tarihli ve 27050 sayılı Resmî Gazete’de yayımlanan 5809 sayılı Elektronik Haberleşme Kanunu

04.02.2011 tarihli ve 27836 sayılı Resmî Gazete’de yayımlanan 6098 sayılı Türk Borçlar Kanunu

04.02.2011 tarihli ve 27836 sayılı Resmî Gazete’de yayımlanan 6098 sayılı Türk Borçlar Kanunu

14.02.2011 tarihli ve 27846 sayılı Resmî Gazete’de yayımlanan 6102 sayılı Türk Ticaret Kanunu

14.02.2011 tarihli ve 27846 sayılı Resmî Gazete’de yayımlanan 6102 sayılı Türk Ticaret Kanunu

14.04.2011 tarihli ve 27905 sayılı Resmî Gazete’de yayımlanan 6222 sayılı Sporda Şiddet ve Düzensizliğin Önlenmesi Hakkında Kanun

30.06.2012 tarihli ve 28339 sayılı Resmî Gazete’de yayımlanan 6331 sayılı İş Sağlığı ve Güvenliği Kanunu

07.11.2012 tarihli ve 28640 sayılı Resmî Gazete’de yayımlanan 6356 sayılı Sendikalar ve Toplu İş Sözleşmesi Kanunu

06.03.2014 tarihli ve 28933 Mükerrer sayılı Resmî Gazete’de yayımlanan Terörle Mücadele Kanunu ve Ceza Muhakemesi Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun

05.11.2014 tarihli ve 29166 sayılı Resmî Gazete’de yayımlanan 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun

7.4.2016 tarihli ve 29677 sayılı Resmî Gazete’de yayımlanan 6698 sayılı Kişisel Verilerin Korunması Kanunu

04.04.2017 tarihli ve 30028 sayılı Resmî Gazete’de yayımlanan 6991 sayılı Türkiye Cumhuriyeti ile Sırbistan Cumhuriyeti Arasında Suçluların İadesine Dair Anlaşma ve Anlaşmada Değişiklik Yapılmasına İlişkin Notaların Onaylanmasının Uygun Bulunduğu Hakkında Kanun

24.10.2019 tarihli ve 30928 sayılı Resmî Gazete’de yayımlanan 17.10.2019 tarihli ve 7188 sayılı Ceza Muhakemesi Kanunu ve Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun

24.10.2019 tarihli ve 30928 sayılı Resmî Gazete’de yayımlanan Ceza Muhakemesi Kanunu ve Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun

## **ULUSAL YÖNETMELİKLER**

06.02.2004 tarihli ve 25365 sayılı Resmî Gazete’de yayımlanan Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğin Korunması Hakkında Yönetmelik

01.06.2005 tarihli ve 25832 sayılı Resmî Gazete’de yayımlanan Ceza Muhakemesinde Beden Muayenesi ve Fiziki Kimliğin Tespiti Hakkında Yönetmelik

11.04.2007 tarihli ve 30035 sayılı Resmî Gazete’de yayımlanan İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik

24.10.2007 tarihli ve 26680 sayılı Resmî Gazete’de yayımlanan Telekomünikasyon Kurumu Tarafından Erişim Sağlayıcılara ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik

30.11.2007 tarihli ve 26716 sayılı Resmî Gazete’de yayımlanan İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik

24.07.2012 tarihli ve 28363 sayılı Resmî Gazete’de yayımlanan Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik (mülga)

22.12.2012 tarihli ve 28595 sayılı Resmî Gazete’de yayımlanan Sporda Şiddet ve Düzensizliğin Önlenmesine Dair Kanunun Uygulanmasına İlişkin Yönetmelik

29.12.2012 tarihli ve 28512 sayılı Resmî Gazete’de yayımlanan İş Sağlığı ve Güvenliği Hizmetleri Yönetmeliği

28.10.2017 tarihli ve 30224 sayılı Resmî Gazete’de yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik

16.11.2017 tarihli ve 30242 sayılı Resmî Gazete’de yayımlanan Kişisel Verileri Koruma Kurulu Çalışma Usul ve Esaslarına Dair Yönetmelik

30.12.2017 tarihli ve 30286 sayılı Resmî Gazete’de yayımlanan Veri Sorumluları Sicili Hakkında Yönetmelik

30.12.2017 tarihli ve 30286 sayılı Resmî Gazete’de yayımlanan Veri Sorumluları Sicili Hakkında Yönetmelik

21.06.2019 tarihli ve 30808 sayılı sayılı Resmî Gazete’de yayımlanan Kişisel Sağlık Verileri Hakkında Yönetmelik

04.12.2020 tarihli ve 31324 sayılı Resmî Gazete’de yayımlanan Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik

## **DiğER**

19.02.1960 tarihli ve 10436 sayılı Resmî Gazete’de yayımlanan Tıbbi Deontoloji Nizamnamesi

2002/58/EC sayılı Özel Yaşamın ve Elektronik İletişimin Korunması Direktifi, (*Directive on Privacy and Electronic Communications*), erişim için bkz.: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN>

27.07.1968 tarihli ve 12961 sayılı Resmî Gazete’de yayımlanan Türk Eczacıları Deontoloji Tüzüğü



ABAD, *Avrupa Komisyonu v. Avusturya Cumhuriyeti*, Dava No: C-614/10, tarih: 16.10.2012, dava raporuna erişim için bkz.: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62010CJ0614&from=en>

ABAD, *Avrupa Komisyonu, Avrupa Komisyonu v. Macaristan*, Dava No: C-288/12, tarih: 08.04.2021, dava özetine erişim için bkz.: [https://ec.europa.eu/anti-fraud/sites/default/files/caselaw\\_2001\\_2015\\_en.pdf](https://ec.europa.eu/anti-fraud/sites/default/files/caselaw_2001_2015_en.pdf)

ABAD, *Volker ve Markus Schecke ve Hartmut Eifert v. Land Hessen*, Birleştirilmiş Davalar, Dava No: C-92/09 ve C-93/09, 09.11.2010, karara erişim için bkz.: <https://curia.europa.eu/juris/document/document.jsf?docid=79001&doclang=en>

ABAD, *Bodil Lindqvist v. İsveç*, Dava No: C-101/01, 6.11.2003, karara erişim için bkz.: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62001CJ0101&from=EN>

ABAD, *Patrick Breyer / Almanya*, Dava no: C-582/14, 19.10.2016, erişim için bkz.: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0582>, erişim

Alman Ceza Kanunu, İngilizce metnine erişim için bkz.: [https://www.gesetze-im-internet.de/englisch\\_stgb/englisch\\_stgb.html#p0191](https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#p0191)

Avrupa Konseyi, *Kişisel Verilerin Otomatik İşlenmesine İlişkin Kişilerin Korunmasına İlişkin Sözleşmede Değişiklik Yapan Protokole İlişkin Açıklayıcı Rapor (Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data)*, erişim için bkz.: <https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a>

Amerika Birleşik Devletleri Çocukların Çevrimiçi Platformlarda Mahremiyetinin Korunmasına İlişkin Kanun (*Children's Online Privacy Protection Act of 1998*), erişim için bkz.: <https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule>

İngiltere Veri Koruma Kanunu (Data Protection Act), erişim için bkz.: <https://www.legislation.gov.uk/ukpga/2018/12/section/3/enacted>

İsviçre Federal Veri Koruma Kanunu (*Federal Act of Data Protection*), İngilizce çevirisine erişim için bkz.: [https://fedlex.data.admin.ch/filestore/fedlex.data.admin.ch/eli/cc/1993/1945\\_1945\\_1945/20190301/en/pdf-a/fedlex-data-admin-ch-eli-cc-1993-1945\\_1945\\_1945-20190301-en-pdf-a.pdf](https://fedlex.data.admin.ch/filestore/fedlex.data.admin.ch/eli/cc/1993/1945_1945_1945/20190301/en/pdf-a/fedlex-data-admin-ch-eli-cc-1993-1945_1945_1945-20190301-en-pdf-a.pdf)

İstanbul Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü, Avrupa Parlamentosu ve Konseyi'nin 2016/680 Sayılı ve 27 Nisan 2016 Tarihli Kişisel Verilerin Yetkili Otoritelerce Suçların Önlenmesi, Soruşturulması, Ortaya Çıkarılması veya Kovuşturulması veya Cezaların İnfazı Amacıyla İşlenmesiyle İlgili Gerçek Kişilerin Korunmasına ve Bu Verilerin Serbest Dolaşımına İlişkin ve 2008/977/JHA Sayılı Konsey Çerçeve Kararı'nı Yürürlükten Kaldıran Direktif Hakkında Bilgi Notu, erişim için bkz.: <https://itlaw.bilgi.edu.tr/media/2019/7/29/law-enforcement-directive-bilgi-notu.pdf>

[İstanbul İl Emniyet Müdürlüğü'nün İstanbul Sağlık Müdürlüğü'nden "ivedi" ve "gizli" ibareleriyle 01.01.2017 ile 31.05.2019 tarihleri arasında şehirde kürtaj yaptıran kadınların bilgisini talep etmesini konu alan haber, erişim için bkz.:](#)

<https://t24.com.tr/haber/istanbul-emniyet-mudurlugu-kurtaj-yaptiran-30-40-yas-araligi-kadinlarin-listesini-istedi,838733>

Kanada Gizlilik Kanunu (*Privacy Act*), erişim için bkz.: <https://laws-lois.justice.gc.ca/eng/acts/p-21/fulltext.html>

Kişisel Verileri Koruma Kurumu'nun yurt dışına aktarım taahhütnamelerine erişim için bkz.: <https://www.kvkk.gov.tr/Icerik/5255/Taahhutnameler>

Milli İstihbarat Teşkilatı'nın istihbarat tanımı, erişim için bkz.: <https://www.mit.gov.tr/tarihce/giris.html>

Pamela Samuelson, *Privacy as Intellectual Property*, erişim için bkz.: [https://people.ischool.berkeley.edu/~pam/papers/privasip\\_draft.pdf](https://people.ischool.berkeley.edu/~pam/papers/privasip_draft.pdf).

Pfizer Public önderliğinde kurulan Halk Sağlığı Okulları Birliği'nin (Association of Schools of Public Health) “kamu sağlığı” tanımına erişim için bkz.: <https://web.archive.org/web/20050307160406/http://www.whatispublichealth.org/about/index.html>

TBMM Tutanak Dergisi, 26. Dönem, Cilt: 12, Yasama Yılı: 1, 59. Birleşim, 8. Oturum, 22.03.2016, erişim için bkz.: <https://www5.tbmm.gov.tr/tutanaklar/TUTANAK/TBMM/d26/c012/tbmm26012059.pdf>

TBMM Tutanak Dergisi, 26. Dönem, Cilt: 12, Yasama Yılı: 1, 60. Birleşim, 7. Oturum, 23.03.2016, erişim için bkz.: <https://www5.tbmm.gov.tr/tutanaklar/TUTANAK/TBMM/d26/c012/tbmm26012060.pdf>

İzlanda Veri Koruma Kanunu (*The Data Protection Act*), İngilizce çevirisine erişim için bkz.: <https://www.personuvernd.is/information-in-english/greinar/nr/438/forum>

Türk Tabipleri Birliği'nin de kabul ettiği ve kullandığı Dünya Tabipler Birliği Cenevre Bildirgesi Hekimlik Andına erişim için bkz.: [https://www.ttb.org.tr/userfiles/files/hekimlik\\_andi.pdf](https://www.ttb.org.tr/userfiles/files/hekimlik_andi.pdf)

Ulusal Güvenlik Dairesi skandalı ile ilgili çalışma için bkz.: [https://en.wikipedia.org/wiki/Edward\\_Snowden](https://en.wikipedia.org/wiki/Edward_Snowden), ayrıca bkz.: [https://www.bbc.com/turkce/haberler/2014/01/140123\\_nsa\\_istihbarat](https://www.bbc.com/turkce/haberler/2014/01/140123_nsa_istihbarat)

## YARARLANILAN BAŞLICA İNTERNET SİTELERİ

Avrupa İnsan Hakları Mahkemesi: <https://hudoc.echr.coe.int/>

Kişisel Verileri Koruma Kurumu: [www.kvkk.gov.tr](http://www.kvkk.gov.tr)

Türk Dil Kurumu Sözlükleri: <https://sozluk.gov.tr/>

Yargıtay Bilgi Bankası: <https://karararama.yargitay.gov.tr/>

Kazancı İctihat Bilgi Bankası: <http://www.kazanci.com/>

Resmî Gazete: <https://www.resmigazete.gov.tr/>

Mevzuat Bilgi Sistemi: <https://mevzuat.gov.tr/>

Lexpera: <https://www.lexpera.com.tr/>

ICO (International Commissioner's Office): <https://ico.org.uk/>

Avrupa Konseyi: <https://www.coe.int/en/web/portal/home>

GDPR: <https://gdpr-info.eu/recitals/>

Türkiye Büyük Millet Meclisi: <https://www.tbmm.gov.tr/>



# ÖZGEÇMİŞ

## Kişisel Bilgiler

Adı Soyadı : Umut Emre Yağlıdere

## Eğitim Durumu

Lisans Öğrenimi : T.C. Kadir Has Üniversitesi - Hukuk Fakültesi (2015)

Yüksek Lisans Öğrenimi : T.C. Kadir Has Üniversitesi

Sosyal Bilimler Enstitüsü

Kamu Hukuku Tezli Yüksek Lisans Programı

Bildiği Yabancı Diller : İngilizce

## İş Deneyimi

Çalıştığı Kurumlar ve Tarihler: 2020 – Halen: Serbest Avukatlık (Bursa Barosu)

2018-2020 – RSK Veri Güvenliği ve Dan. Hiz. A.Ş.

2015-2016 – Stajyer Avukat