T.C. MARMARA ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

KAMU HUKUKU ANABİLİM DALI

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

YÜKSEK LİSANS TEZİ

İSMAİL ÇAĞLAR

İstanbul, 2022

T.C. MARMARA ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

KAMU HUKUKU ANABİLİM DALI

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

YÜKSEK LİSANS TEZİ

İSMAİL ÇAĞLAR

DANIŞMAN: Dr. Öğr. Üyesi Kerim ÇAKIR

İstanbul, 2022

ÖZET

Gelişim hızını günden güne artıran teknoloji, artık hayatımızın her alanını etkilemekte ve bizleri de içinden geçtiği bu değişime tabi kılmaktadır. Ancak söz konusu değişim ve gelişim döngüsünün içerisinde kendisine yer bulmaya çalışan insanoğlu, sahip olduğu bazı değerlerin kullanılmasına rıza göstermek zorunda kalmıştır. Bu değerlerin başında gelen ve yeni dünyanın petrolü olarak görülen en önemli kavram ise bilgidir. Bilgi, artık günümüzde onu elinde bulunduran kişiler açısından bir güç kaynağı olarak kabul görmekte ve bu nedenledir ki kendisine sahip olma noktasında insanları cezbetmektedir. Çalışmamızın konusunu oluşturan ana kavram olan kişisel veriler ise bugünün dünyasında en çok elde edilmek istenen bilgi çeşididir. Zira insana ait verilere sahip olmak, onun davranışlarını şekillendirmek açısından son derece önemlidir.

Özellikle 21. yüzyıl başlarında bilişim sistemlerinin daha etkin hale gelmeye başlamasıyla özel hayatın bir parçası olan kişisel verilere ulaşım kolaylaşmış ve bu verilerin aktarımı, depolanması ile paylaşılması gittikçe yaygınlaşmıştır. Küreselleşen dünyada kişisel verilerin kullanımının bu şekilde artması, bilgi güvenliği konusunda çeşitli endişeler uyandırmış ve bu durum birçok hukuki problemi de beraberinde getirmiştir. Tüm bu gelişmelerin sonunda ise kişisel verilerin korunması ile ilgili endişeleri gidermek ve temel hakların içerisinde büyük bir öneme sahip olan kişisel verilerin korunması hakkını güvence altına almak amacıyla devletler, kendi ulusal mevzuatlarında ve birlikte hareket ederek uluslararası hukuk düzleminde bazı düzenlemeler yapmışlardır.

Kişisel verilerin korunması amacıyla tüm dünyada başlayan ve günümüzde halen devam etmekte olan kodifikasyon hareketlerine Türk kanun koyucusu da kayıtsız kalmamıştır. Bu kapsamda yapılan en geniş düzenleme ise başlı başına kişisel verileri konu alan 6698 sayılı Kişisel Verilerin Korunması Kanunu olmuştur. Bununla birlikte söz konusu kanundan daha önce yürürlüğe giren 5237 sayılı yeni Türk Ceza Kanunu'nda özel olarak kişisel verileri konu alan üç suç tipi düzenlenmiştir. Çalışmamızın konusunu oluşturan verileri hukuka aykırı olarak verme veya ele geçirme suçu da bu üç suç arasında yer almıştır. Eserimizde öncelikle tezimizin konusunu oluşturan suç tipinin daha iyi analiz edilebilmesi için kişisel verilere ilişkin önemli kavramlara değinilmiş ardından söz konusu suç, doktrindeki görüşler ve yargı kararları bağlamında incelenmeye çalışılmıştır.

Anahtar Kelimeler: Teknoloji, kişisel veriler, verileri hukuka aykırı olarak verme veya ele geçirme suçu

SUMMARY

Increasing the speed of development day by day, technology now affects every aspect of our lives and makes us subject to this change that it has. However, human beings trying to find a place for themselves in this change and development cycle have to give consent to the use of some values that they have. The most important concept among these values and seen as the oil of the new world is information. Information is now accepted as a source of power for the people who hold it, and for this reason, it motivates people at the point of possessing it. Personal data, which is the main concept that constitutes the subject of our study, is the most desired type of information in today's world. Because having data that belongs to human is extremely important in terms of shaping his behavior.

Especially at the beginning of the 21st century, with the information systems becoming more effective, accessing to personal data which is a part of private life, has become easier and the transfer, storage and sharing of this data has become increasingly common. The increase in the use of personal data in the globalizing world has raised some concerns about information security and this situation has brought many legal problems. At the end of all these developments, in order to eliminate the concerns about the protection of personal data and to secure the right to the protection of personal data, which has great importance among the fundamental rights, the states have made some regulations in their national legislation and field of international law cooperatively.

The Turkish legislator has not ignored the codification movements that started and are still continuing today all over the world for the protection of personal data. The most extensive regulation made in this context is the Law on the Protection of Personal Data (LPPD, Numbered 6698), which regulates mainly personal data. In addition to this, in the new Turkish Penal Code Numbered 5237, which entered into force before LPPD, three types of offenses regarding specifically personal data were regulated. The offence of Illegally Obtaining or Giving Data, that constitutes the subject of our study, is among these three crimes. In our study, first of all, important concepts related to personal data are mentioned in order to better analyze the type of

crime that is subject of our thesis, and then this crime is tried to be examined in the context of opinions in the doctrine and judicial decisions.

Keywords: Technology, Personal Data, Offence of Illegally Obtaining or Giving Data

ÖNSÖZ

Kişisel verilerin hayatımıza egemen olması neticesinde birçok ülke mevzuatında çeşitli düzenlemeler yapılmış ve farklı suç tipleri ihdas edilmiştir. Söz konusu gelişmelerden ulusal hukuk sistemimiz de etkilenmiştir. Nitekim Yeni Türk Ceza Kanunu'nun 2005 yılında yürürlüğe konulmasıyla birlikte 765 sayılı eski Ceza Yasamızda düzenlenmeyen ve kişisel verileri konu alan verileri yayma veya ele geçirme suçu hayatımıza girmiştir. Söz konusu suç, 5237 sayılı Türk Ceza Kanunu'nun ikinci kitabının Kişilere Karşı Suçlar başlıklı ikinci kısmının Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar başlıklı dokuzuncu bölümünde düzenlenmekte olup her geçen gün yargı kararlarında daha çok yer almaya başlamıştır. Bu nedenledir ki işbu çalışma ile hukuk uygulayıcılarımıza karşılaştıkları somut olayların çözümünde bir nebze olsun yardımcı olmak hedeflenmiştir.

Çalışmamızda öncelikle suç teorisi açısından ikinci bölümde yapacağımız açıklamaların daha iyi anlaşılabilmesi adına kişisel veri kavramı, ulusal ve uluslararası düzenlemeler boyutunda incelenmiştir. Bu kapsamda ilk olarak veri kavramından yola çıkarak açıklamalar yapılmış ve akabinde kişisel veri kavramı ile yakından ilişkili olan veri işleme faaliyeti, kişisel verilerin korunması hakkı, açık rıza ve ilgili kişi gibi kavramlara değinilmiştir. Bahsi geçen başlıklar incelenirken başta Kişisel Verilerin Korunması Kanunu temel alınmakla birlikte Avrupa Genel Veri Koruma Tüzüğü (GDPR) ve ülkemizin de taraf olduğu 108 no'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Gerçek Kişilerin Korunmasına Dair Sözleşme göz önünde bulundurulmuştur.

Eserimizin ikinci bölümde ise Türk Ceza Kanunu'nun 136. maddesinde yer alan verileri hukuka aykırı olarak verme veya ele geçirme suçu incelenmiştir. Bu bağlamda söz konusu suçun unsurları ayrı ayrı başlıklar altında doktrindeki görüşler ve yargı kararları da dikkate alınarak açıklanmaya çalışılmıştır.

TEŞEKKÜR

Bu çalışmanın hazırlanmasında benden maddi ve manevi desteklerini esirgemeyen sevgili anne ve babama, büyük bir sabırla her zaman yardımcı olan ağabeyime teşekkürlerimi sunmayı bir borç bilirim.

İlk tanıştığım günden bugüne dek beni yetiştiren ve gayreti ile bana yol gösteren saygıdeğer danışman hocam Dr. Öğr. Üyesi Kerim Çakır'a eserime sunduğu katkılarından ötürü minnettarım.

İsmail ÇAĞLAR

ANKARA-2021

İÇİNDEKİLER

ÖZET **I**

SUMMARY **II**

ÖNSÖZ **IV**

TEŞEKKÜR **V**

İÇİNDEKİLER **VI**

KISALTMALAR **XI**

GİRİŞ 1

1. BÖLÜM: MEVZUAT İLE YARGI KARARLARI KAPSAMINDA KİŞİSEL VERİ KAVRAMI 5

1. Kişisel Veri 6

1.1. Genel Olarak 6

1.2.Tanım 7

1.2.1. Kimliği Belirli veya Belirlenebilir Olma 7

1.2.2. Gerçek Kişiye İlişkin Olma 9

1.2.3. Her Türlü Bilgi Niteliğinde Olma 14

2. Özel Nitelikli Kişisel Veri 16

2.1. Irk 18

2.2. Etnik Köken 19

2.3. Siyasi Düşünce 20

2.4. Felsefi İnanç 21

2.5. Din, mezhep, diğer inanç 21

2.6. Kılık ve kıyafet 22

2.7. Dernek, vakıf, sendika üyeliği 23

2.8. Sağlık Verisi 23
2.9. Cinsel hayat 25
2.10. Ceza mahkumiyeti ve güvenlik tedbiri 26
2.11. Biyometrik veri 27
2.12. Genetik veri 29
3. Kişisel Verilerin İşlenmesi 30
4. Kişisel Verilerin Korunması Hakkı 33
4.1. Ekonomik Hak Görüşü 33
4.1.1. Mülkiyet Hakkı Görüşü 34
4.1.2. Fikri Mülkiyet Hakkı Görüşü 35
4.2. Özel Hayatın Gizliliği Görüşü 36
5. Türk Hukukunda Kişisel Veriler 38
5.1. Anayasa 38
5.2. Türk Borçlar ve Türk Medeni Kanunu 39
5.3. İş Kanunu 40
5.4. Türk Ceza Kanunu 42
5.5. 6698 Sayılı Kişisel Verilerin Korunması Kanunu 43
6. Özel Bir Kanun Olarak 6698 Sayılı Kişisel Verilerin Korunması Yasası 44
6.1. Genel Olarak 44
6.2. Amaç 45
6.3. Kapsam 45
6.4 Tanımlar 47
6.4.1. Açık Rıza ve İstisnaları 48
6.4.2. Kişisel Verilerin İşlenmesi 48
6.4.4. İlgili Kişi ve Hakları 49

6.4.5. Veri Sorumlusu ve Yükümlülükleri 51
6.4.6. Veri İşleyen 53
6.5. Kişisel Verilerin İşlenmesinde Uyulması Gereken Genel İlkeler 54
6.6. Verilerin İşlenme Şartları 58
6.6.1. Kişisel Verilerin İşlenme Şartları 59
6.6.1.1. Açık Rıza 59
6.6.1.2. Kanunlarda Açıkça Öngörülme 61
6.6.1.3. Hayat veya Beden Bütünlüğünün Korunması 63
6.6.1.4. Sözleşmenin Kurulması veya İfası 63
6.6.1.5. Hukuki Yükümlülüğün Yerine Getirilmesi 64
6.6.1.6. Verinin Alenileştirilmiş Olması 65
6.6.1.7. Hakkın Tesisi, Kullanılması veya Korunması 66
6.6.1.8. Veri Sorumlusunun Meşru Menfaati 66
6.6.2. Özel Nitelikli Kişisel Verilerin İşlenme Şartları 67
7. Kişisel Verilere İlişkin Uluslararası Düzenlemeler 69
7.1. Genel Olarak 69
7.2. OECD 70
7.3. BM 70
7.4. 108 Sayılı Sözleşme 71
7.5. Avrupa İnsan Hakları Sözleşmesi (AİHS) 72
7.6. Avrupa Genel Veri Koruma Tüzüğü (GDPR) 73
2. BÖLÜM: VERİLERİ HUKUKA AYKIRI OLARAK VERME VEYA ELE GEÇİRME SUÇU 76
1. Genel Olarak 77
2. Madde Metni, Gerekçesi ve Yapılan Değişiklikler 80

3. Korunan Hukuki Değer 82

4. Suçun Unsurları 83

4.1. Maddi Unsurlar 85

4.1.1. Fiil 85

4.1.1.1. Verme 88

4.1.1.2. Yayma 89

4.1.1.3. Ele Geçirme 92

4.1.2. Fail 97

4.1.3. Mağdur 98

4.1.4. Konu 99

4.1.5. Nitelikli Haller 100

4.1.5.1. Suçun konusunun CMK Uyarınca Kayda Alınan Beyan ve Görüntüler Olması 100

4.1.5.2. Suçun Yetkisini Kötüye Kullanan Kamu Görevlisi Tarafından İşlenmesi 102

4.1.5.3.Suçun Bir Meslek ve Sanatın Sağladığı Kolaylıktan Yararlanılarak İşlenmesi 104

4.2. Manevi Unsur 105

4.3. Hukuka Aykırılık Unsuru 107

4.3.1. Hukuka Uygunluk Nedenleri 108

4.3.1.1. Mağdurun Rızası 109

4.3.1.2. Kanun Hükmünün İcrası 109

4.3.1.3. Hayat veya Beden Bütünlüğünün Korunması İçin Zorunluluk 111

4.3.1.4. Bir Sözleşmenin Kurulması veya İfasında Gereklilik 112

4.3.1.5. Hakkın Tesisi, Kullanılması ve Korunması İçin Zorunluluk 112

4.3.1.6.Veri Sorumlusunun Hukuki Yükümlülüğünü Yerine Getirmesi 113

4.3.1.7. Veri Sorumlusunun Menfaatleri Açısından Zorunluluk 114

4.3.1.8. Sağlık ve Cinsel Hayata İlişkin Verilerin İşlenmesi 114

4.3.1.9. İlgili Kişinin Verilerini Alenileştirmesi 115

5. Suçun Özel Görünüş Biçimleri 116

5.1. Teşebbüs 116

5.2. İştirak 117

5.3. İçtima 118

6. Yaptırım 122

7. Soruşturma Usulü 122

8. Yetkili ve Görevli Mahkeme 123

SONUÇ 124

KAYNAKÇA 130

KISALTMALAR

108 Sayılı Sözleşme : Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi

AB : Avrupa Birliği

ABAD : Avrupa Birliği Adalet Divanı

AGO : Adli Görüşme Odası

AİHM : Avrupa İnsan Hakları Mahkemesi

AİHS : Avrupa İnsan Hakları Sözleşmesi

AYM : Anayasa Mahkemesi

Bkz. : Bakınız

BM : Birleşmiş Milletler

C. : Cilt

CMK : Ceza Muhakemesi Kanunu

COVID-19 : Koronavirüs hastalığı (Şiddetli akut solunum yolu sendromu koronavirüsü 2)

ÇİM : Çocuk İzlem Merkezi

dn : Dipnot

E.T. : Erişim Tarihi

EUROJUST : Avrupa Birliği Yargısal İşbirliği Kurumu

EUROPOL : Avrupa Polis Teşkilatı

GDPR : Avrupa Genel Veri Koruma Tüzüğü

KVKK : Kişisel Verilerin Korunması Kanunu

KURUL : Kişisel Verileri Koruma Kurulu

KURUM: : Kişisel Verileri Koruma Kurumu

MERNİS : Merkezi Nüfus İdare Sistemi

m. : Madde

OECD : Ekonomik Kalkınma ve İşbirliği Örgütü

PVSK : Polis Vazife ve Salahiyet Kanunu

RG : Resmi Gazete

s. : Sayfa

S. : Sayı

TAAD : Türkiye Adalet Akademisi Dergisi

TBK : Türk Borçlar Kanunu

TBB : Türkiye Barolar Birliği

TBMM : Türkiye Büyük Millet Meclisi

TCK : Türk Ceza Kanunu

TDK : Türk Dil Kurumu

TMK : Türk Medeni Kanunu

UNESCO : Birleşmiş Milletler Eğitim, Bilim ve Kültür Örgütü

vd. : ve devamı

VERBİS :Veri Sorumluları Sicili Bilgi Sistemi

GİRİŞ

Bilgi, eski zamanlardan günümüze dek insan hayatında önemli bir yer edinmiştir. Kendisine sahip olma noktasında insanoğlunu cezbeden bilgi, kimi zaman bir güç kaynağı şeklinde görülmüş kimi zaman ise bireylerin özel hayatı açısından kilit rol oynayan unsurlardan biri olarak kabul edilmiştir. Özellikle 21. yüzyılda ivme kazanan bilişim sistemleri ile birlikte artık günlük yaşamın vazgeçilmez kavramları arasında sayılan bilgi, bu denli fazla kullanılması sonucu birçok farklı şekle bürünmüştür. Çalışmamızın çevresinde şekillendiği ve bilginin de en önemli türlerinden birisini oluşturan olgu ise kişisel veridir. Ulusal mevzuatımızda ve uluslararası düzenlemelerde kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi olarak tanımlanan kişisel veri, devlet kurumları yanında özel sektördeki kuruluşlar tarafından da işlem hayatında her geçen gün daha fazla kullanılmaktadır. Teknolojinin sağladığı imkanların çeşitlenmesi ile söz konusu veriler artık anlık olarak işlenebilmekte ve hızlıca yayılabilmektedir. Bu noktada özel hayatın gizliliği ile ilgili endişeler gündeme gelmekte ve bireylerin temel haklarının korunabilmesi amacıyla çeşitli düzenlemeler yapılmaktadır. Kişisel verilerin korunması hakkı özelinde insan hakları bağlamında meydana gelen gelişmelere Türk kanun koyucusu da kayıtsız kalmamıştır. Öncelikle çalışmamızın konusunu da oluşturan verileri hukuka aykırı olarak verme veya ele geçirme suçunun yanı sıra başkaca suç tipleri Türk Ceza Kanunu'nda düzenlenmiş, diğer bazı yasalarda ise verilerin korunmasına ilişkin hükümler hayata geçirilmiş ve nihayet Kişisel Verilerin Korunması Kanunu ihdas edilerek bireylerin kişisel verileri açısından geniş güvenceler sağlanmıştır.

Kişisel veri, modern dünyanın vazgeçilmez unsurlarındandır. İnsana dair bilgilerin elde edilmesi, biriktirilmesi, çeşitli amaçlarla kullanılması ise tarihin eski dönemlerinden günümüze dek süregelmiş ve halen devam etmektedir. Sanayi Devrimi'yle büyük bir ivme kazanan teknolojik gelişmeler 20. yüzyılın ikinci yarısında internet ve bilgisayar kullanımının dünya genelinde yaygınlaşmasıyla daha da hız kazanmıştır. Teknolojinin bu denli hızlı gelişmesi sonucunda kişisel veri kullanımı da büyük bir artış göstermiş ve kolaylaşmıştır. Günümüzde kişisel veriler ülke sınırları kalkmışçasına dünya çapında toplanmakta, aktarılmakta ve çeşitli yöntemlerle işlenmektedir. Kişisel verilerin kolayca kullanılabilmesine ortam hazırlayan teknolojik gelişmeler bir yandan işlem hayatının, ticaretin, iletişimin ve bilgi akışının hızını artırırken diğer yandan bu verilerin korunması noktasında çeşitli problemleri de beraberinde getirmiştir. Söz konusu bilgilerin sızdırılması, elde ediliş amacı dışında kullanılması ve kişisel

veriler kullanılarak suç işlenmesi sonucu veri sahiplerinin zarar görmesi bunlardan sadece birkaçıdır. Bu bağlamda Bilgi ve Teknoloji Çağı olarak isimlendirilen 21. yüzyılda kişisel verilerin elde edilmesi ve işlenmesinin artık kaçınılmaz ve kolay olması sonucu ortaya çıkan birçok hak ihlali vardır. Kişisel verilerin korunması hakkı özelinde kişilik hakkının korunması ise demokratik bir hukuk devleti olmanın gerekliliklerindendir. Bunun sonucunda ise ulusal ve uluslararası alanda çeşitli veri koruma kuralları ihdas edilmiştir. Günümüzde ülkemizde ve diğer birçok ülkede kişisel verilerin korunması amacıyla çıkarılmış çeşitli veri koruma kanunları mevcuttur.

Kişisel veriler alanında meydana gelen gelişmelerden geri kalmamak adına ülkemizde de birtakım düzenlemeler yapılmıştır. Bu kapsamda aslında uzun süredir kanunlaştırma çalışmaları devam eden ancak nihayete erdirilemeyen Kişisel Verilerin Korunması Kanunu 2016 yılında yürürlüğe girmiştir. Böylece artık gündelik yaşamımızda ciddi bir yeri olan ve kişilerin özel hayatını yakından ilgilendiren kişisel veriler konusu kanuni bir altyapıya kavuşmuştur. Ayrıca söz konusu kanunun uygulanmasında önemli bir yer tutan Kişisel Verileri Koruma Kurumu da ülkemizin, yeni ihdas edilen bu kanuna alışmasında kilit bir rol oynamıştır. Kişisel verilerin korunması noktasında ilginç olan husus ise KVKK'nin yürürlüğe girmesinden yaklaşık on yıl kadar öncesinde kişisel verilere ilişkin olarak 5237 sayılı Türk Ceza Kanunu'nda kişisel verileri konu alan suç tiplerinin düzenlenmiş olmasıdır. Bu durum kişisel verilere ilişkin özel bir yasa olmamasına rağmen bu verilerin konu edildiği suç tiplerinin hüküm altına alınmış olması sonucunu doğurmuş ve belirlilik açısından çeşitli endişeleri de beraberinde getirmiştir. Nitekim verileri hukuka aykırı olarak verme veya ele geçirme suçuyla ilgili Anayasa Mahkemesine yapılan iptal başvurusunda da aynı gerekçelere değinilmiş ancak Yüksek Mahkeme kişisel veri kavramının uygulamada netleşeceğini ifade ederek söz konusu başvuruyu reddetmiştir. Çalışmamızda söz konusu iptal başvurusu ve bu başvuruya ilişkin ret kararı ayrıntısıyla incelenmiştir.

Kişisel verileri hususi olarak konu alan suç tipleri 5237 sayılı Türk Ceza Kanunu'nun 135 ila 140'ıncı maddeleri arasında düzenlenmiştir. Bu suçlar sırasıyla kişisel verilerin kaydedilmesi (135. madde), verileri hukuka aykırı olarak yayma veya ele geçirme (136. madde) ve son olarak verileri yok etmeme (138. madde) suçlarıdır. Saymış olduğumuz bu suçlar yeni Ceza Kanunumuzun yürürlüğe girmesiyle kanunda yerini almış ve böylelikle teknolojik gelişmeler göz ardı edilmeyerek kişisel veriler açısından önemli bir düzenlemeye imza atılmıştır. Nitekim 5237 Sayılı Yasanın genel gerekçesinde yer alan *"Ceza mevzuatı çağın gereklerini ve yeniden oluşan milli ve insanlığın değerlerini vurgulayan, insan haklarını ve toplumsal güvenliği*

korumayı hedefleyen bir suç ve ceza siyasetine dayandırılmalıdır." ifadesi de teknolojinin Türk Ceza Kanunu'nun hazırlanması sürecini açıkça etkileyen faktörlerden biri olduğunu belirtmektedir. Aynı şekilde genel gerekçede, çağdaş teknolojinin insan hayatına getirdiği modern araçların küreselleşmenin (globalleşmenin) bir ölçüde işlenmesine neden olduğu suçlara ve uygulamaların ortaya çıkardığı yeni suç şekillerine 765 Sayılı Yasa'nın aksine yeni TCK'de yer verildiği vurgulanmıştır. Bu suç tiplerinden birisi de verileri hukuka aykırı olarak verme veya ele geçirme suçudur.

Çalışmamızın ana konusunu oluşturan verileri hukuka aykırı olarak verme veya ele geçirme suçu, Türk Ceza Kanunu'nun 136. maddesinde düzenlenmiştir. Söz konusu maddenin gerekçesinde de belirtildiği üzere hukuka uygun olarak kaydedilmiş olsun veya olmasın, kişisel verileri hukuka aykırı olarak başkalarına vermek, yaymak veya ele geçirmek bağımsız bir suç olarak tanımlanmıştır. Bu düzenleme ile en başta Anayasamızın 20. maddesi ve AİHS'in 8. maddesinde güvence altına alınan kişisel verilerin korunması hakkı özelinde özel hayatın gizliliği korunmuş olmaktadır. Kişisel verilerin korunması hakkı artık özel hayatın gizliliği başlığı altında incelenen ve yargı kararlarında da açıkça kabul edilen bir haktır. Zira teknolojinin hızlı gelişimi veri sahibi kişilerin, bu verileri elinde bulunduran veya işleyen kişilere karşı korunmasını zorunlu kılmıştır. Nitekim kişisel verileri hukuka aykırı olarak ele geçirilen kişilerin yaşamış olduğu mağduriyetler her geçen gün artmaktadır. Tam bu noktada ise kişisel verilerin korunması hakkı hukuka aykırı veri işleme faaliyetlerine karşı bir koruma kalkanı olmaktadır.

Eserimizin ilk bölümünde öncelikle veri kavramından yola çıkılarak kişisel verinin unsurları ayrıntısıyla incelenmiş akabinde özel nitelikli kişisel veriler, kişisel verilerin işlenmesi, kişisel verilerin korunması hakkı, açık rıza, ilgili kişi, veri işleyen ve veri sorumlusu kavramları 6698 sayılı Kişisel Verilerin Korunması Kanunu başta olmak üzere ulusal ve uluslararası mevzuat kapsamında açıklanmıştır. Daha sonra kişisel verileri konu alan diğer kanuni düzenlemelere değinilmiş ve sonrasında uluslararası hukuk düzleminde kişisel verilerin korunması amacıyla hayata geçirilen regülasyonlara yer verilmiştir. Bu bağlamda özellikle Avrupa Genel Veri Koruma Tüzüğü (GDPR) ve 108 no'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Gerçek Kişilerin Korunmasına Dair Sözleşme'ye dikkat çekilmiştir. Çalışmamızın ikinci bölümünde ise Türk Ceza Kanunu'nda özel olarak kişisel verileri konu alan suç tiplerinden olan verileri hukuka aykırı olarak verme veya ele geçirme suçu incelenmiştir.

Kişisel verilerin hukuka aykırı olarak verilmesi, yayılması veya ele geçirilmesi suçu iki fıkra halinde düzenlenmekle birlikte madde metninde ilk olarak suçun temel şekli yer almış ardından

ikinci fıkrada nitelikli hale yer verilmiştir. Söz konusu madde bir kez yaptırım değişikliği ve bir kez de yeni fıkra eklenmesi olmak üzere toplamda iki değişikliğe uğramıştır. Çalışmamızda öncelikle madde metninin geçirmiş olduğu değişiklikler incelenmiş ardından suçla korunan hukuki değer konusu, doktrindeki farklı görüşler de dikkate alınarak açıklanmıştır. Devam eden başlıklarda sırasıyla suçun maddi unsurları, manevi unsurları, hukuka aykırılık unsuru ve hukuka uygunluk nedenleri, suçun özel görünüş halleri, soruşturma usulü ve yaptırım konuları güncel yargı kararları ve öğretideki farklı bakış açıları bağlamında irdelenmiştir. Konular incelenirken madde gerekçeleri ve Meclis komisyonlarına ait raporlar da dikkate alınmıştır. Yeri geldikçe mukayeseli hukuk anlamında farklı ülke uygulamalarına değinilmiş ve yabancı mahkeme kararlarından bahsedilmiştir. Ayrıca Avrupa İnsan Hakları Mahkemesinin ve Kişisel Verileri Koruma Kurulumuzun kararlarına da ilgili kısımlarda yer verilmiştir.

1. BÖLÜM: MEVZUAT İLE YARGI KARARLARI KAPSAMINDA KİŞİSEL VERİ KAVRAMI

1. Kişisel Veri

1.1. Genel Olarak

Teknolojinin gelişmesiyle birlikte bilişim sistemlerindeki çeşitliliğin artması ve bilgiye daha fazla ihtiyaç duyulması sonucu veri kavramı hayatımızda önemli bir yer edinmiştir. TDK' de *"Bilgi, data"* olarak tanımlanan veri[1], *"Bir bilginin ya da bu bilgiye ilişkin görünüm ya da ögelerden kimilerinin, genellikle otomatik olarak işlenmesine uygun biçimde uzlaşmalı gösterimi"* şeklinde ifade edilmektedir.[2] Istılahi manası hakkında fikir birliği bulunmayan ve çeşitli tanımlamalara konu olan veri kavramı, enformasyon ve bilgi kavramlarıyla ilişkili tutularak anlamlandırılmaktadır. Yirminci yüzyılın sonlarına doğru farklı bilim insanları tarafından *"data"* (veri)[3] kavramı hakkında değişik tasnifler ortaya konmuş ve en nihayetinde teorisyen Russell Lincoln Ackoff sırasıyla *"wisdom"*, *"understanding"*, *"knowledge"*, *"information"* ve *"data"* kavramlarını belirli bir hiyerarşik zincire bağlı olarak açıklamıştır. Ackoff'a göre bu kavramlar birbirlerinin içlerinden türeyerek bir sonraki basamağı oluşturmaktadır ve "*data*" yani veri kavramına gelince bu kavram, nesnelerin ve olayların varlıklarını temsil etmekle birlikte söz konusu terimlerin içinde bulundukları bağlamı da kapsamaktadır. Ayrıca Ackoff, verinin, bir gözlemin ürünü olduğunu ve madenler gibi kullanılabilir bir forma dönüştürülmediği sürece herhangi bir değeri olmadığını da belirtmiştir.[4] Kenneth C. Laudon ve Jane P. Laudon ise veri kavramını henüz insanların anlayıp

---

[1] TDK, **Büyük Türkçe Sözlük**

[2] **Büyük Larousse Sözlük ve Ansiklopedisi**, 23. Cilt, s.12164; 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un Tanımlar başlıklı ikinci maddesinde veri *"Bilgisayar tarafından üzerinde işlem yapılabilen her türlü değer"* olarak tanımlanmıştır. Ancak bu tanımlama bilgisayar sistemleri özelinde yapılmış olduğundan konumuz açısından yeterli aydınlatmayı yapmamaktadır. Zira veri kavramının, bilişim sistemlerine indirgenerek açıklanması durumunda gerçek kapsamı oldukça daraltılmış olacaktır.

[3] Data kelimesi "datum" kavramının çoğulu olarak kullanılmaktadır. Bkz. "Datum." Merriam-Webster.com Dictionary, Merriam-Webster, (13.10.2020 tarihinde erişildi.); "Datum" Cambridge.org Dictionary, Cambridge, https://dictionary.cambridge.org/dictionary/english/datum (14.10.2020 tarihinde erişildi.)

[4] Russell Lincoln Ackoff, **From Data to Wisdom**, Journal of Applied Systems Analysis 3-9, 1989. Ackoff'un belirttiği bu hiyerarşik ilişki DIKW Piramidi olarak da adlandırılmaktadır.; Benzer ve farklı yaklaşımlar için bkz. Chaim Zins, **Conceptual Approaches for Defining Data, Information, and Knowledge**, Journal of the American Society For Information Science and Technology, 58(4):479–493, 2007; G. Donald Allen Department of Mathematics, Texas A&M University, **Hierarchy of Knowledge – from Data to Wisdom**, International Journal of Current Research in Multidisciplinary (IJCRM) ISSN: 2456-0979, Vol.2 pg. 15-23; Bernstein, Jay H., **"The Data-Information-Knowledge-Wisdom Hierarchy and its Antithesis"** (2009). City University of New York (CUNY) Academic Works.; Piramidin en üst basamağına ahlak kavramının konulması hakkında bkz. Gu, Ji-Fa. (2013). **Data, Information, Knowledge, Wisdom and Meta-Synthesis of Wisdom-Comment on Wisdom Global and Wisdom Cities**. Procedia Computer Science

kullanabileceği bir forma dönüşmemiş olan ve meydana gelen olayları/olguları temsil eden saf gerçekler olduğunu öne sürmüştür.[5]

Yukarıdaki tanımlamaya uygun olarak gözlemlerimiz sonucunda elde edilen ve farkına vardığımız saf gerçeğin sembolü olarak nitelenebilecek veri kavramı birçok farklı forma bürünebilmektedir. İşte çalışmamızın ilk bölümünün konusu olan kişisel veri kavramı da verinin günümüzde en çok karşılaştığımız türleri arasında kendisine yer bulmaktadır. Bu bağlamda, takip eden başlıklarda kişisel veri kavramı, ilişkili bulunduğu diğer kavramlarla birlikte başta 6698 sayılı Kişisel Verilerin Korunması Kanunu olmak üzere ulusal ve uluslararası mevzuat, doktrin görüşleri ve güncel yargı kararları kapsamında ele alınacaktır.

1.2.Tanım

Kişisel veri, mevzuatımızda *"Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi"* olarak tanımlanmaktadır.[6]-[7]-[8] Öncelikle belirtmeliyiz ki basit gibi görünen bu tanımlama aslında oldukça önemli ayrıntıları ihtiva etmektedir. Bu sebeple konumuzun daha iyi anlaşılması için söz konusu tanımı ögelerine ayırarak incelemekte fayda vardır ve bu ögeler, a) Kimliği belirli veya belirlenebilir olma b) Gerçek kişiye ilişkin olma c) Her türlü bilgi olabilme şeklinde sınıflandırılabilecektir.

1.2.1. Kimliği Belirli veya Belirlenebilir Olma

Öncelikle verinin kişisel veri vasfını taşıması için kimliği belirli veya belirlenebilir bir kişiye ilişkin olması gerekmektedir. Belirli bir kişi kavramı, kimliği somut bir şekilde ortada olan yani kim olduğunun tespit edilmesi için herhangi bir işleme/aşamaya ihtiyaç bulunmayan kişiyi ifade etmektedir. Buna karşın belirlenebilir nitelikte olmak ise bireyin kimliğinin somutlaştırılması

[5] Kenneth C. Laudon, Jane P. Laudon, **Management Information Systems: Managing the Digital Firm**,12 th Edition, s.15. Yazarlar ayrıca information ve data kavramının anlaşılması açısından şu örneği vermektedirler: Bir süpermarkette her gün okunan barkod sayılarının toplamı data olarak kabul edilecek olursa bu datanın anlamlı hale gelen bir türü ise satılan deterjan ürünlerinin toplamı veya bu ürünlerin toplam satış maliyeti olacak ve böylelikle data kavramı anlamlı ve işe yarar hale gelerek "information" formuna bürünecektir.

[6] 6698 Sayılı Kişisel Verilerin Korunması Kanunu m. 3/1-d, Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi m.2/a ve Avrupa Genel Veri Koruma Tüzüğü(GDPR) m.4/1'de de kişisel veri kavramı aynı şekilde tanımlanmaktadır.

[7] Çalışmamızın devamında; 6698 Sayılı Kişisel Verilerin Korunması Kanunu **"KVKK"**; Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi **"108 Sayılı Sözleşme"** ve Avrupa Genel Veri Koruma Tüzüğü **"GDPR"** olarak anılacaktır.

[8] Tanımdaki ilişkili ibaresinin yapılan tanımlamadaki değişkenlik gösteren tek kavram olduğu ve çoktan aza doğru olacak şekilde veri öznesi ile veri arasındaki ilişkinin dercelendirilmesi ve bu kavramın nasıl anlaşılması gerektiği hakkında bkz. Malgieri, Gianclaudio, **Property and (Intellectual) Ownership of Consumers' Information: A New Taxonomy for Personal Data** (April 20, 2016). Privacy in Germany - PinG, n. 4, 2016, 133 ff

için karşımıza çıkan olayda elde bulunan verinin bazı aşamalardan geçmesi gerektiği anlamına gelmektedir.

6698 sayılı KVKK'nin Tanımlar başlıklı 3. maddesinin gerekçesinde veri öznesi için aranan kimliği belirli veya belirlenebilir olma unsuru açısından bir ölçüt getirilmiştir. Buna göre kişinin kesin teşhisini araya başka bir işlem girmeksizin sağlayan bilgiler yanında ilgili birey ile ilişkilendirilme faaliyeti sonucu o kimsenin tespit edilebilir hale getirilmesine olanak sağlayan bilgilerin de kişisel veri kavramını karşıladığı ifade edilmiştir.[9] Bilginin belirli veya belirlenebilir bir kişiye ait olması unsuru ile hedeflenen amaç aslında sahip olunan bu bilginin kullanılması sonucu o kişinin toplumun diğer bireylerinden ayrılması, ayırt edilebilir hale getirilmesidir.[10] Ayırt edicilik niteliği ile kast edilen ise o kişiye toplumdaki diğer kişilerden faklı şekilde davranılması olarak anlaşılmalıdır.[11] Aynı doğrultuda belirtmek gerekir ki sahip olunan bilginin ilgili olduğu kişiyi diğerlerinden ayıracak nitelikte bir kişisel veri olup olmadığı somut olay özelinde değerlendirilmesi gereken bir hususdur. Nitekim bu veri, karşılaşılan herhangi bir hadisede kişisel veri vasfını taşırken diğer bir durumda taşımama ihtimalini de bünyesinde barındırmaktadır. Örneğin kişinin küçük bir yörede rahatça tanınmasını sağlayan lakabı, yirmi milyona yaklaşan nüfusu dikkate alındığında İstanbul gibi bir şehirde anlam ifade etmeyecektir. Aynı şekilde ülkemizde sıkça kullanılan bir ismi taşıyan kişi ile ilgili olarak sadece isminin bilindiği durumda da o kişinin kimliğinin belirlenebilmesi imkanı olmayacaktır. Ancak bu kişinin çalıştığı iş yerinde o ismi sadece kendisinin taşıdığı varsayımında mevcut isim belirlenebilirliği de aşarak artık belirli bir kişiye ilişkin bir bilgi olacaktır. Zira o isim zikredildiğinde başka bir işleme ihtiyaç olmaksızın kişinin kimliği ortaya çıkacak ve kim olduğu sadece adı aracılığıyla tespit edilecektir. Görüldüğü üzere bir verinin kişisel nitelik taşıyıp taşımadığının belirlenmesi sırasında bulunulan bağlama göre yorum yapılarak bir sonuca varılması gerekmektedir. Bununla birlikte mevcut şartlar yanında dikkate değer diğer bir husus

---

[9] Türkiye Büyük Millet Meclisi, **Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu**, Madde Gerekçeleri, s.7. Raporda belirli veya belirlenebilir olmaya ilişkin olarak sadece bireyin adı, soyadı, doğum tarihi ve doğum yeri gibi onun kesin teşhisini sağlayan bilgilerin değil, aynı zamanda kişinin fiziki, ailevi, ekonomik, sosyal ve sair özelliklerine ilişkin bilgilerin de kişisel veri olduğu, bir kişinin belirli veya belirlenebilir olması hususunun mevcut verilerin herhangi bir şekilde bir gerçek kişiyle ilişkilendirilmesi suretiyle o kişinin tanımlanabilir hale getirilmesini ifade ettiği yani verilerin; kişinin fiziksel, ekonomik, kültürel, sosyal veya psikolojik kimliğini ifade eden somut bir içerik taşıması veya kimlik, vergi, sigorta numarası gibi herhangi bir kayıtla ilişkilendirilmesi sonucunda kişinin belirlenmesini sağlayan tüm halleri kapsadığı belirtilmiştir. Ayrıca isim, telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler gibi verilerin de dolaylı da olsa kişiyi belirlenebilir kılabilme özellikleri nedeniyle kişisel veri olduğu ifade edilmiştir.

[10] Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi**, Aralık 2019, Ankara, s.52

[11] Article 29 Data Protection Working Party, **Opinion 4/2007 on the concept of personal data**, s.83

ise somut vakıada kişinin teşhisi sürecinde kullanılacak araçlardır. Örnek olarak T.C. kimlik numarasını ele aldığımızda bu veri, kendisini bir sisteme kaydedip sonuç elde etme imkanı bulunmayan birisi için herhangi bir anlam ifade etmezken geniş veri tabanı kullanan -örneğin vergi daireleri gibi- kurumlarda tek başına kişinin teşhis edilmesini sağlayabilecektir. Çünkü vergi dairesinde kullanılacak olan sistem, söz konusu numaranın kimlik tespiti noktasında yeterli olması sonucunu doğuracaktır.

Son olarak değinmek gerekirse yukarıda verdiğimiz örneklerin tersi bir durumda yani sahip olunan bilginin ilişkili bulunduğu kişinin tespiti için yetersiz gibi göründüğü hallerde de yine somut vakıanın özellikleri belirleyici rol oynayacaktır. Örneğin on daireden oluşan bir aile apartmanında bekar olarak yaşayan tek bir kişinin olduğunu düşündüğümüzde bu kişinin, sadece medeni hal bilgisi ile birçok insanın yaşadığı apartmanda teşhis edilebilmesi mümkün olacak ve adı/soyadı gibi kimlik tespitinde ilk akla gelen bilgileri bilinmese dahi o birey, diğer apartman sakinlerinden ayırt edilebilecektir. Netice itibarıyla karşılaşılan bir olayda, sahip olunan bir bilginin kişisel veri olup olmadığı tespit edilirken o bilginin önemli/önemsiz yahut gerekli/gereksiz gibi görünmesine aldırış etmeden somut hadisede taşıdığı özellikler, elde bulunan araçlar, teknolojik imkanlar ve son tahlilde içerisinde bulunulan bağlam ve şartlar göz önüne alınarak bir sonuca varılmalıdır.

1.2.2. Gerçek Kişiye İlişkin Olma

Kişisel verinin varlığından söz edilebilmesi için söz konusu verinin gerçek kişiye ilişkin olması gerekmektedir. Medeni Kanunumuzun 28. maddesinde yer alan hükme göre ise kişilik, çocuğun sağ olarak tamamıyla doğduğu anda başlayacaktır. Kanunun aradığı şartlar yerine gelince sübut bulan kişilik ile birlikte bu kavramı oluşturan değerler koruma altına alınacaktır. Örneğin her ne kadar yeni doğan bir çocuk fiil ehliyetinden mahrum olsa da kendisine ilişkin fotoğraf, T.C. kimlik numarası gibi kişisel veriler, hukuk düzeni tarafından korunacaktır.

Dural/Öğüz'e göre kişilik hakkı, kişinin toplum içindeki saygınlığını ve kişiliğini serbestçe geliştirmesini temin eden varlıkların tümü üzerinde sahip olduğu hak olarak tanımlanmaktadır.[12] Söz konusu tanımlamada yer alan ve kişinin kendini geliştirmesini sağlayan varlıklar olarak anlamdırılan değerler, sınırlı bir biçimde sayılamamakla birlikte teknolojik gelişmelere bağlı olarak meydana gelen yenilikler doğrultusunda kapsamını genişletmektedir. Kişisel veriler de

[12] Mustafa Dural/ Tufan Öğüz, **Kişiler Hukuku**, Ekim 2015, Filiz Kitabevi, s.100

bahsi geçen yeniliklerin sonucunda artık hukuk dünyasınca tanınan ve koruma altına alınan kişilik hakkı değerleri arasında kuşkusuz yer almaktadır.[13]

Konuyla yakından ilgili olması hasebiyle özel hayatın gizliliği kavramına burada kısaca değinmekte fayda görüyoruz. Bireyin sahip olduğu hayat alanları kendi kişiliğinin bir yansıması olup bu alanlar kamuya açık alan, özel alan ve gizlilik alanı olarak üçe ayrılmaktadır. Kamuya açık alan, bireyin kendisinin haricinde diğer kişiler tarafından da bilinen konulardan oluşmakta iken özel alan, kişinin belirli kişilere açtığı, sınırlı sayıda kişi tarafından bilinmesini istediği alandır. Son olarak gizli alan ise üçüncü kişilerin giremediği mahrem bir alan olarak kabul edilmektedir. Belirtilen bu üç alandan özel ve gizli alan kişilik hakkı kapsamında korunmakla birlikte söz konusu iki alana yapılacak müdahaleler kişilik hakkına da halel getirecektir.[14]

Kişisel verilerin korunmaya başlama noktasının kişiliğin başlangıcı olarak kabul edilmesinin bir sonucu olarak bu veriler için sağlanan koruma da kişiliğin sona erdiği noktada artık ortadan kalkacaktır. Bu durumda kişiliğin ölüm veya gaiplik ile sona erdiği göz önüne alındığında kişisel verilerin söz konusu iki durumdan birinin ortaya çıkmasıyla artık hukuki korumadan mahrum kalacağı söylenebilecektir.

Kişisel verilerin gerçek kişilere ilişkin veriler olarak kabul edilmesinin sonucunda iki bulgu ortaya çıkmaktadır: i) Tüzel kişilerin ve ii) Kişiliği sona eren bireylerin kişisel verisi olamayacaktır. Bununla birlikte söz konusu iki sonuç hakkında farklı görüşler mevcuttur.

Öncelikle tüzel kişilerin kişisel verisi olup olamayacağına değinmek gerekirse bu konuda KVKK'nin ve GDPR'ın koyduğu ölçüler son derece nettir. Ayrıca Kişisel Verileri Koruma Kurumu da *"İlgili kişi kimdir?"* sorusunu cevaplandırmış ve konuyla ilgili açıklamasında KVKK ile sadece gerçek kişilerin verilerinin korunduğunu belirtmiştir. Ayrıca Kurum, tüzel kişiye ait verinin gerçek bir kişiyi belirli veya belirlenebilir hale getirmesi durumunda bu verilerin de korunacağını ancak burada korunan menfaatin tüzel kişiye değil gerçek kişiye ait olduğunu ve son olarak da kanunun tüzel kişiye ait verilerin korunmasını hiçbir şekilde düzenlemediğini ifade etmiştir.[15] Kişisel Verileri Koruma Kurulunun tüzel kişilerin verilerine ilişkin olarak verdiği bir kararına konu olayda ise bir tüzel kişi diğer bir tüzel kişiye ait elektronik ortamdaki verileri talep etmiştir. Kurul, kendisine konuyla ilgili yapılan başvuruyu gerçek kişilere ait verilerin KVKK kapsamında bulunmasına karşılık tüzel kişilerin verilerinin bu kapsama dahil edilmediğini ve KVKK'nin 11. maddesinde bulunan ilgili kişinin haklarının

[13] Rona Serozan**, Medeni Hukuk Genel Bölüm/Kişiler Hukuku**, 5. Bası, İstanbul 2014, s.446-447
[14] Dural/ Öğüz, s.135-138
[15] Kişisel Verileri Koruma Kurulu, İlgili Kişi Kimdir?, https://www.kvkk.gov.tr/Icerik/2034/Ilgili-Kisi-Kimdir (23.10.2020 tarihinde erişildi.)

yalnızca gerçek kişi tarafından kullanılacağını belirterek tüzel kişiye ait verilere erişilmesi durumunun kanunun değerlendirme alanı dışında olduğuna kanaat getirmiştir.[16]

GDPR açısından konuya yaklaşıldığında ise KVKK ile paralel bir düzenleme yapıldığı görülmektedir. Aynı şekilde Avrupa Komisyonu tarafından yapılan açıklamada *"Veri koruma kuralları şirketler hakkında uygulanacak mı?"* sorusu Komisyon tarafından olumsuz bir şekilde cevaplandırılarak kuralların yalnızca gerçek kişilere uygulanacağı, buna karşın şirket veya diğer herhangi bir tüzel kişilik için bu kuralların uygulanamayacağı ancak tüzel kişiye ilişkin bir bilginin gerçek kişiyi belirlenebilir kılması durumunda bu verilere ilişkin olarak veri koruma kurallarının uygulanacağı beyan edilmiştir. Bu duruma örnek olarak ise tek kişilik bir şirkete ait bilgilerin gerçek kişiye ilişkin olabileceği ihtimali gösterilmiştir.[17]

Kişisel verinin gerçek kişiye ilişkin olması şartı bağlamında ikinci olarak değinmemiz gereken konu ise ölen kişilere ait verilerin akıbetinin nasıl belirleneceğidir. Ölen kişilerin hayatta iken sahibi oldukları kişisel verilerine ilişkin herhangi bir hüküm KVKK'de düzenlenmemekle birlikte Kişisel Verileri Koruma Kurulu önüne gelen bir olayda bu konu hakkında bazı tespitlerde bulunmuştur. Söz konusu karara konu olayda sağ olan eş, ölen eşinin önceden tedavi gördüğü klinikten tüm medikal ve diğer bilgilerini yasal mirasçısı olarak talep etmiş ancak klinik herhangi bir cevap vermemiştir. Bunun üzerine somut vakıa ile ilgili olarak Kurul, KVKK kapsamında kişisel verilerin gerçek kişilere ilişkin bilgiler olduğunu, Medeni Kanunumuzun 28'inci maddesine göre kişiliğin çocuğun sağ olarak tamamıyla doğduğu anda başlayıp ölüm ile sona erdiğini ve bu suretle talep edilen bilgilerin gerçek kişiye ait olmaması nedeniyle KVKK kapsamında yapılacak bir işlemin olmadığı sonucuna varmıştır.[18]

---

[16] Kişisel Verileri Koruma Kurulu, 19/11/2018 tarih ve 2018/131 sayılı Karar Özeti

[17] European Union, **Do the data protection rules apply to data about a company?**, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/do-data-protection-rules-apply-data-about company_en (23.10.2020 tarihinde erişildi.); AİHM'in konuyla ilgili bazı kararları şöyledir: *ClientEarth and PAN Europe v EFSA* C-615/13 P; *Rechnungshof (C-465/00)v Österreichischer Rundfunk and Others and Christa Neukomm (C-138/01) and Joseph Lauermann (C-139/01) v Österreichischer Rundfunk*; *Commission v Bavarian Lager*, C-28/08 P; *Worten,* C-342/12; GDPR'ın gerkçe kısmının 14. maddesinde de söz konusu regülasyonun gerçek kişilere ait verilere ilişkin olup tüzel kişilere ilişkin verileri kapsamadığı açıkça ifade edilmiştir. Bkz. **Regulation (EU) 2016/679 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 and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Recital 14**, Official Journal of the European Union; GDPR'ın tasarı metninin 12. maddesinde regülasyonla sağlanan korumanın yalnızca gerçek kişilere ilişkin kişisel verileri kapsayıp tüzel kişiler ile ilgili verileri kapsamadığı belirtilmiştir. Ayrıca bu kuralın tüzel kişinin isminin bir veya daha fazla gerçek kişinin ismini taşıması durumunda da geçerli olacağı belirtilmiş ancak bu ifade GDPR'ın son haline dahil edilmemiştir. Bkz. **Draft GDPR Adopted by European Parliament**, Article 12, Wednesday, 12 March 2014 - Strasbourg

[18] Kişisel Verileri Koruma Kurulu, 18/09/2019 tarih ve 2019/273 sayılı karar özeti

Avrupa Birliği özelinde ölen kişilerin verilerinin durumuna bakıldığında ise GDPR'ın gerekçesi yol gösterici olacaktır. Bu kapsamda belirtmek gerekirse gerekçede açıkça söz konusu regülasyonun ölen kişilerin verilerine uygulanmayacağı ancak üye devletlerin isterlerse kendi iç hukuklarında konuyla ilgili düzenleme yapabilecekleri belirtilmiştir.[19] Öte yandan Avrupa Birliği'ndeki bazı devletlerin, kendi iç hukuklarında ölen kişilerin verilerine ilişkin bazı hükümler ihdas ettiği görülmektedir. Örneğin, Danimarka Veri Koruma Yasası'nda söz konusu yasanın ve GDPR'ın ölen kişinin ölümünü takiben 10 yıl daha uygulanacağı belirtilmiştir.[20] Macaristan Veri Koruma Yasası'nda ise ölen kişinin, kendi ölümünden sonraki 5 yıl için kendisine kanun kapsamında sayılan bazı hakları kullanabilecek bir kişiyi belirli usuller dahilinde yetkilendirebileceği ve buna ek olarak yakın akrabasının belirli şartlar dahilinde yine ölümden sonra beş yıl boyunca kanunda veri sahibine sayılan bazı hakları kullanabileceği belirtilmiştir.[21] Slovakya Hukuku'nda ise ilgili kişinin, kendisi öldükten sonra yakınları tarafından verilerinin işlenmesi konusunda rıza verebileceği ancak yakın kişilerden en az birinin yazılı onaylamama beyanı vermesi durumunda verilen rızanın geçersiz olacağı öngörülmüştür.[22] Son olarak İtalya örneğine bakılacak olursa İtalya, 2018'de GDPR'a uyum sağlanması amacıyla yürürlüğe koyduğu düzenleme ile ölen kişinin ardından kendi yararına veya ölenin menfaatlerini koruma amacıyla hareket eden kişinin GDPR'ın 15-22. maddeleri arasında sayılan ilgili kişinin haklarını temsilci sıfatıyla veya korunmaya değer ailevi nedenlerden dolayı kullanabileceğini kabul etmiş ancak ölen veri sahibinin yazılı olarak daha önceden rıza göstermemesi gibi bazı istisnalara da yer vermiştir.[23]-[24]

Mevzuatımızda ölen kişilerin verileri ile ilgili herhangi açık bir hüküm bulunmamakla birlikte doktrinde bazı yazarlar müteveffanın ardında bıraktığı verilerin hiçbir şekilde korunmamasını eleştirmektedir. Bu bağlamda somut olaya göre değerlendirme yapılması ve söz konusu verilerin ölenin mirasçıları gibi diğer kişilere ilişkin özellikler taşıması itibarıyla kişisel veri

[19] **GDPR**, Recital Art.27

[20] **Danish Data Potection Act**, Art.2/5

[21] Act CXII of 2011 on the right to informational self-determination and on the freedom of information, Enforcement of rights related to personal data after the death of the data subject, Section 25

[22] Act of 29 November 2017 on personal data protection and amending and supplementing certain Acts Chapter Four Specıfıc Situations Of Lawfull Processing Of Personal Data, Section 78

[23] Francesco Paolo PATTI & Francesca BARTOLINI, **Digital Inheritance and Post Mortem Data Protection: The Italian Reform**, European Review of Private Law 5-2019 [1181–1194], 2019 Kluwer Law International BV, The Netherlands, s.1182, Ayrıca bkz. Art. 2 terdecies, para. 2, Legislative Decree no. 101 of 2018. Maddenin tam İtalyanca metni için bkz. Gazetta Ufficiale, 4 Settembre 2018, Anno 159° - Numero 205

[24] Alman Ceza Kanunu'nda özel bilgilerin açıklanmasına ilişkin suç tipinde ölen kişi ile ilgili sırların onun vefatının ardından herhangi bir yetkilendirme olmaksızın açıklanması suç olarak kabul edilmiştir. Bkz. Strafgesetzbuch (StGB)§ 203 Verletzung von Privatgeheimnissen

niteliğinde olabileceği belirtilmektedir.[25] Zikredilen görüşe göre bu durum, kanunda veri sahibi kavamı yerine veri ilgilisi kavramının tercih edilmesinin bir sonucudur. Zira ölenin sağ iken çekilen fotoğrafında çocuğunun yer alması ya da ırsi olarak alt soya geçen bir hastalığa sahip olması halinde bu hastalığın açıklanması gibi hallerde halen yaşamakta olan gerçek kişilere ilişkin bazı verilerden söz edilebilecektir.[26] Kanaatimizce değinmekte olduğumuz bu görüşler son derece isabetlidir. Aksini kabul durumunda salt ölene ait olduğu gerekçesiyle müteveffa ile birlikte başka kişileri belirli veya belirlenebilir kılan verilerin kişisel veri olarak kabul edilmemesi gibi bir durum ortaya çıkar ki bu sonuç KVKK'nin amacı ve ilgili kişi kavramının kapsamı ile bağdaşmayacaktır. Belirtilmelidir ki yukarıda da değindiğimiz üzere kanunda ilgili kişi kavramı tercih edilerek kişisel verilerin korunacağı alan genişletilmiştir. Bu doğrultuda kişisel verilerin korunması kapsamında gerçek kişilere tanınan hakların kullanılabilmesi için o verinin sahibi olunması aranmamıştır. Neticeten meydana gelen somut olayın özellikleri incelenerek veri öznesi olan kişinin ölmüş olmasının yanı sıra diğer başkaca kişilere ilişkin bir verinin de olup olmadığının tespiti sonucunda daha doğru sonuçlara ulaşılacaktır.[27]-[28]

---

[25] Kişisel Sağlık Verileri Hakkında Yönetmelik'in 11. maddesinin 2'nci fıkrasında ***"****Ölmüş bir kimsenin sağlık verileri, en az 20 yıl süre ile saklanır."* hükmü yer almaktadır.

[26] Murat Volkan Dülger, **Kişisel Verilerin Korunması Hukuku**, Hukuk Akademisi, 3. Baskı, İstanbul 2020, s.173; https://www.hukukihaber.net/kisisel-verilerin-korunmasi-kurulunun-02042020-tarihinde-yayimlanan-2019138-206-273-297-333-ve-202034-41-43-58-65-67-sayili-kararlarina-iliskin-degerlendirme-makale,7651.html; Mesut Serdar Çekin, **Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku**, On İki Levha Yayınları, 3. Baskı, İstanbul 2020, s.44

[27] Avrupa Birliği Veri Koruma Çalışma Grubu'nun görüşüne göre de ölene ait veriler halen yaşamakta olan kişilere ilişkin bilgi verebilmektedir. Örnek olarak ise hemofili hastalığından ölen bir kişinin oğlunun da taşıdığı kromozomlardan ötürü aynı hastalığı taşıyacağı ve bu suretle veri koruma kuralları kapsamına giren bir durumun meydana geleceği belirtilmektedir. Bkz. **Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data**, s.22

[28] Ölen kişinin verileriyle ilgili olarak son yıllarda tartışılan diğer bir konu ise bu verilerin miras olarak mirasçılarına intikal edip etmeyeceği meselesidir. Bu bağlamda miras hukuku kuralları ile özel hayatın gizliliğinin karşı karşıya gelmesi hasebiyle son derece ilginç bir durum ortaya çıkmış ve bu konuda çeşitli görüşler ileri sürülmüştür. Özellikle Alman Federal Mahkemesi'nin konuya ilişkin kararı tartışmaların daha da alevlenmesine yol açmıştır. Mahkemenin önüne gelen olayda ölen kızının ölüm nedenini araştırmak isteyen annesi tarafından kızının Facebook profiline girilmeye çalışılmış ancak Facebook, vefat eden kızın profil sayfasını anıtlaştırmış ve annenin hesaba erişim talebini haberleşmenin gizliliği ve genel işlem şartlarını gerekçe göstererek reddetmiştir. Bunun üzerine olayı mahkemeye taşıyan annenin talebi Eyalet Mahkemesi tarafından kabul edilmiş ancak Facebook Eyalet Yüksek Mahkemesine başvurmuştur. Mahkeme, haberleşmenin gizliliğini hesaba erişim hakkına tercih ederek annenin talebini reddetmiş ve nihayet dava Federal Mahkemenin önüne gelmiştir. Federal Mahkeme ise ölümle birlikte külli halefiyet ilkesi sonucu müteveffanın sosyal medya şirketi ile arasındaki sözleşme ilişkisinin de mirasçılara geçtiğini ve bunun sonucunda haberleşme içeriklerine mirasçılarca ulaşılabileceğini kabul etmiştir. Ayrıntılı açıklamalar için bkz. Çiğdem İleri, **Dijital Miras - Alman Federal Mahkemesi'nin "Facebook" Kararı Üzerine Bir İnceleme**, TBB Dergisi 2020 (146), s.131-134; Nurten İnce Akman, **Mirasbırakanın Dijital Bilgilerinin Mirasçılara Geçişi (Dijital Tereke)**, İnönü Üniversitesi Hukuk Fakültesi Dergisi –İNÜHFD- Cilt:9 Sayı:2 Yıl 2018; Federal Mahkemenin kararının tam metni için bkz. BGH III ZR 183/17 Juli 12, 2018; Ölümden sonra özel hayatın korunması ve dijital miras kavramları hakkında bkz. J. C. Buitelaar, **Post-mortem privacy and informational self-determination**, Tillburg University Ethics and Information Technology 2017, s.129-142; Sidsel Thaarup**, Implementing Post-Mortem Privacy in a Digital Age a thesis on post-mortem data protection**, January 2018, IT University of Copenhagen; Gianclaudio

1.2.3. Her Türlü Bilgi Niteliğinde Olma

Kişisel verinin tanımına bakıldığında üçüncü unsur olarak karşımıza "her türlü bilgi olma" şartı çıkmaktadır. Böylelikle belirtilmelidir ki kişisel veri, her şeyden önce bilginin bir türü olarak kabul edilmektedir. Ayrıca söz konusu koşulun bir sonucu olarak bilginin ne çeşit olacağı noktasında herhangi bir sınırlama yapılmadığını da eklememiz gerekir. Ulusal ve uluslararası mevzuat irdelendiğinde ise kişisel veri kavramının sayma (tahdidi olarak) yoluyla tanımlanmadığı tam aksine önü açık bir tanımlama yoluna gidildiği görülmektedir. Teknolojinin gelişim hızı dikkate alındığında söz konusu tanımlama yönteminin uygun olduğu söylenebilecektir. Zira kişisel verilerin nelerden ibaret olduğunun tek tek belirtilmesi tercih edildiğinde söz konusu tanıma dahil edilmeyen bir veri çeşidinin teknolojinin gelişimiyle hayatımıza girmesi durumunda, yapılan önceki tanımın artık geçerliliğini yitirip mevcut ihtiyacı karşılayamayacağı açıktır.

Türk Dil Kurumunca kurallardan yararlanarak kişinin veriye yönelttiği anlam şeklinde tanımlanan bilgi kavramı, yukarıda değindiğimiz DIKW Piramidi'ndeki "information" kelimesi özelinde düşünüldüğünde insanoğlunun işine yarayan ve anlamlı hale gelmiş veri olarak anlamlandırılabilecektir.[29] Bahse konu kavramların somutlaştırılması açısından örnek vermek gerekirse data kavramını un, su, tuz, yağ olarak düşünürsek information yani bilgi kavramı ise bu malzemelerin anlamlı birlikteliği sonucu meydana gelen ekmeğe benzetilebilecektir.[30]

Kişisel verinin tanımına işlenmiş olan bilgi, ölçülebilir, aktarılabilir, işlenebilir, depolanabilir gibi özelliklere sahip olup değişik durumlarda farklı nitelikler taşıyarak karşımıza

---

Malgieri, R.I.P.: **Rest in Privacy or Rest in (Quasi-)Property? Personal data protection of deceased data subjects between theoretical scenarios and national solutions**; Heather Conway And Sheena Grattan, **The 'New' New Property: Dealing with Digital Assets on Death**; Lilian Edwards and Edina Harbinja, Protecting Post-Mortem Privacy: **Reconsidering The Privacy İnterests of the Deceased in a Digital World**; Serozan ise ölene ait ve parasal nitelik taşıyan ses ve görüntü gibi kişilik değerlerinin ölümden sonra yakınlarına geçmesi ve yakınları tarafından söz konusu değerlerin korunması yollarına başvurulmasının kişilik haklarının kişiye sıkı sıkıya bağlı olma ve mirasçılara geçmeme gibi özelliklerine gölge düşürdüğünü belirtmektedir. Bkz. Rona Serozan, **Medeni Hukuk Genel Bölüm/Kişiler Hukuku**, 5. Bası, İstanbul 2014, s.447

[29] Kenneth C. Laudon, Jane P. Laudon, **Management Information Systems, Managing the Digital Firm**,12 th Edition, s.15; Diğer bir çalışmada bilgi, bulundukları bağlam aracılığıyla birbiriyle ilişkili olup kullanılabilir formda olan veriler olarak tanımlanmıştır. Bkz. Jennex, Murray. (2017). **Big Data, the Internet of Things, and the Revised Knowledge Pyramid. ACM SIGMIS Database: The Database for Advances in Information Systems**. 48. 69-79., s.69; Farklı yazarların DIKW Piramidindeki kavramlar hakkında yaptığı tanımlamalar için bkz. Baskarada, Sasa & Koronios, Andy. (2013). **Data, Information, Knowledge, Wisdom (DIKW): A Semiotic Theoretical and Empirical Exploration of the Hierarchy and its Quality Dimension**, Australasian Journal of Information System; Piramit ile ilgili kısa açıklamalar için bkz. Fricke, Martin, **The Knowledge Pyramid: A Critique of the DIKW Hierarchy**, 2008, University of Arizona

[30] Robertson, Terry Dwain (2013) **"The Data/Information/Knowledge/Wisdom Hierarchy Goes to Seminary"** Advances in the Study of Information and Religion: Vol. 3, Article 7., s.5

çıkabilmektedir.[31] Örneğin söz konusu kavramın bünyesinde kimi zaman subjektiflik ağır basacak iken bu terim kimi zaman objektifliği daha fazla yansıtacaktır. Şöyle ki kişinin kanındaki bir madde objektif özellik taşırken bankacılık sektöründe kredi çekmek isteyen kişi hakkında yapılan kredi verilmesi konusundaki değerlendirmeler (örneğin kişinin güvenilir biri olması gibi) subjektif nitelikteki bilgi kategorisinde kabul edilecektir. Diğer yandan "bilgi" nin kanıtlanmış veya doğru olması gerekmemektedir. Zira veri koruma kuralları, kişiye kendisi hakkındaki yanlış bilgiye erişim ve bu bilgi açısından itiraz etme hakkı da tanımaktadır. Bunun yanında her türlü bilgi kavramına sayısal, alfabetik, grafiksel, ses veya görüntü formuna bürünmüş bilgiler de girmektedir. Nihayet bilgi, fiziken bir kağıdın üzerinde olabileceği gibi bilgisayar gibi elektronik aletlerde de bulunabilecektir.[32]

Kişiyle ilgili bilgi, kişinin sosyal hayatına ilişkin olabileceği gibi iş yaşantısına veya özel hayatına da ilişkin olabilecektir. Örneğin patronunun, çalışanı hakkındaki görüşlerini içeren dosya bu anlamda kişisel veri barındıracaktır.[33]

Yukarıda da belirttiğimiz gibi kişisel veri kavramı sınırlandırıcı bir şekilde tanımlanmamış ve ileride meydana gelebilecek teknolojik gelişmeler göz önünde bulundurularak kapsamı geniş tutulmuştur. Ancak konumuzun daha iyi anlaşılabilmesi ve bahse konu terimin somutlaştırılması açısından çalışmamızın bu kısmında bazı kişisel verileri örnek kabilinden saymak suretiyle açıklamaya çalışacağız. Bu bağlamda ad, soyad, doğum yeri ve tarihi, anne ve baba adı, adli sicil kaydı, yerleşim yeri, eğitim durumu, meslek, banka hesap bilgileri, telefon numarası, elektronik posta adresi, kan grubu, medeni hal, parmak izi, DNA, saç, tükürük, tırnak gibi biyolojik örnekler, cinsel ve ahlaki eğilim, sağlık bilgileri, etnik köken, siyasi, felsefi ve dini görüş, sendikal bağlantılar[34], üye olunan dernekler, alışkanlıklar, sevilen kitaplar, yapılan spor faaliyetleri, alınan cezalar, yargılanılan suçlar, bu suçlara ilişkin bilgi ve kayıtlar[35], kişinin mali varlığı, sahip olduğu hisse ve hesaplar, borçları, yaptığı alışverişler, kredi kartlarına ilişkin veriler[36], motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler[37], internet sitesi çerezleri[38], 5651

---

[31] Jonathan Hey, December 2004, **The Data, Information, Knowledge, Wisdom Chain: The Metaphorical link**, s.7

[32] Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, s.6-9; Aynı yaklaşım için bkz. AİHM, Amann v. Switzerland, No. 27798/95, 16 Şubat 2000, para 65.

[33] **Handbook on European Data Protection Law**, 2018 Edition, Publications Office of the European Union, s.86 Aynı yaklaşım için bkz. AİHM, Amann v. Switzerland, No. 27798/95, 16 Şubat 2000, para 65.

[34] YARGITAY 12. CEZA DAİRESİ E. 2019/3710 K. 2020/1106 T. 5.2.2020

[35] YARGITAY 4. HUKUK DAİRESİ E. 2017/2479 K. 2020/30 T. 14.1.2020

[36] YARGITAY CEZA GENEL KURULU E. 2012/12-1514 K. 2014/312 T. 10.6.2014

[37] TBMM, **Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu**, Madde Gerekçeleri, 3. madde gerekçesi, s.7

sayılı Kanun'un 2. maddesinin (j) bendinde IP adresi, verilen hizmetin başlama ve bitiş zamanı, yararlanılan hizmetin türü, aktarılan veri miktarı, (varsa) abone kimlik bilgileri şeklinde tanımlanan trafik bilgisi[39], kişinin ByLock haberleşme programını kullandığına ilişkin veriler[40], alışveriş alışkanlıkları, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri[41], lokasyon bilgisi[42], göz irisi taraması[43], yöneticisinin kendi çalışanı hakkındaki görüşleri[44], ilgili kişinin arkadaşlarının bilgileri, kredi geçmişi bilgileri[45], biyometrik imza[46], posta kodu, mahalle ve/veya ikamet ettiği şehir[47] başlıca sayılabilecek kişisel veriler arasında yer almaktadır.

2. Özel Nitelikli Kişisel Veri

Kişisel Verilerin Korunması Kanunu'nun 6. maddesinde belirtildiği üzere özel nitelikli kişisel veriler kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik veriler olarak kabul edilmiştir. GDPR'ın tanımlamasına bakıldığında ise KVKK'de yer verilen mezhep, kılık ve kıyafet, dernek ve vakıf üyeliği, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verilerin sayılmadığı ve cinsel yönelimin ise KVKK'den farklı olarak tanımın kapsamına dahil edildiği görülmektedir. Ceza mahkûmiyeti ve güvenlik tedbirlerini ilgilendiren veriler ise GDPR'ın 10. maddesinde ayrıca düzenlenmiştir.

6698 sayılı Yasa'nın 6. maddesinde sayılan verilerin hassas veri olarak değerlendirilmesinin nedeni madde gerekçesinde bu verilerin başkaları tarafından öğrenilmesi durumunda bireyin mağduriyetinin artacak olması ve ilgili kişinin ayrımcılığa/ötekileştirilmeye maruz kalmasının

[38] Directive 2002/58/EC Of The European Parliament And Of The Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Article 25; Handbook on European data protection law 2018 Edition, Publications Office of the European Union, s.89

[39] AYM, E.2014/149, K.2014/151, T. 2/10/2014

[40] AYM, Başvuru Numarası: 2018/23077 Karar Tarihi: 17/9/2020 Resmi Gazete Tarihi: 13 Ekim 2020

[41] AYM, Başvuru Numarası: 2016/4060 Karar Tarihi: 17/9/2020 Resmi Gazete Tarihi: 14 Ekim 2020

[42] GDPR, Art.4; AİHM görsel ve işitsel gözetleme sistemlerinin GPS takibine nazaran daha fazla özel hayata müdahale ettiğini belirtmiştir. Bkz. Case of Uzun V. Germany, (Application no. 35623/05), 2 September 2010

[43] Handbook on European data protection law 2018 Edition, Publications Office of the European Union, s.90

[44] Amann v. Switzerland, No. 27798/95, 16 Şubat 2000, para 65

[45] Kişisel Verileri Koruma Kurulu, 27/02/2020 tarih ve 2020/173 sayılı karar özeti

[46] Kişisel Verileri Koruma Kurulu, 27.08.2020 tarih ve 2020/649 sayılı karar özeti

[47] Kişisel Verileri Koruma Kurulu, 16.04.2020 tarih ve 2020/286 sayılı karar özeti

önlenmesi olarak belirtilmektedir.[48] Özel nitelikli veriler -ihtiva ettikleri bilgi çeşidi açısından- ortaya çıkması durumunda diğer verilere nazaran ilgili kişinin ayrımcılığa uğramasını daha fazla kamçılayacak vasıftadır. Bunun sonucunda ise söz konusu verilerin ihlali durumunda ortaya çıkacak zarar da düşünüldüğünde hassas verilerin korunmasına öncelik tanınacaktır. Zira özel kategorideki verilerin kamuya açık hale gelmesi, kişinin özel hayatı, aile yaşamı, toplum içerisindeki konumu ve iş kariyeri açısından tehlike oluşturabilecektir.[49] Bu bağlamda aynı şekilde çeşitli yargı kararlarında kişilerin bazı verilerinin diğerlerine oranla daha yüksek derecede korunması gerektiği de ifade edilmiştir. Örneğin Danıştay 15. Dairesinin 8.7.2014 tarihli kararına konu olayda, davacı muayene olmak için gittiği hastanede el okutma sistemine girmeden mayene olmak istemiş ancak hastanece avuç içi okuma işlemi yapılmadan söz konusu muayenenin yapılamayacağı cevabı verilmiştir. Danıştay ise, hastanenin cevabına dayanak yapılan Sosyal Güvenlik Kurumu Genel Sağlık Sigortası Genel Müdürlüğünün kılavuzunun bazı maddelerinin iptali ve yürütmesinin durdurulması istemiyle açılan davada hassas verilere ilişkin birtakım tespitlerde bulunmuştur. Şöyle ki, kişinin verilerinden bazıları hassas veri olarak tanımlanmakta ve bu veriler ile bireyin temel hak ve özgürlükleri arasında yakın bir ilişki bulunmaktadır. Bundan dolayıdır ki söz konusu özel nitelikli veriler, kişinin diğer verilerine nazaran daha etkili bir şekilde korunmayı beraberinde getirmektedir.[50] Hassas verilere ilişkin olarak değinilmesi gereken diğer önemli bir karar ise Avrupa İnsan Hakları Mahkemesinin Marper v. Birleşik Krallık davasına ilişkindir. AİHM, mahkum edilmemiş ancak şüpheli sıfatını taşıyan kişilerin DNA izlerinin veritabanına kaydedilmesi ile ilgili olayda suç işlememiş kişilerin suç işlemiş kişilerle aynı muameleye maruz bırakılmasının toplum tarafından kınanma riskini oluşturduğunu ve bundan dolayı özel hayata orantısız şekilde müdahale edildiğini belirterek AİHS'in sekizinci maddesinin somut olayda ihlal edildiğine karar vermiştir.[51] Söz konusu karar, hassas verilerin ifşa edildikleri zaman ait oldukları kişilere ayrımcılık yapılmasına yol açacağını göstermesi açısından son derece mühimdir.

---

[48] Türkiye Büyük Millet Meclisi, **Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu**, Madde Gerekçeleri, 6. madde gerekçesi, s.9; Türkay Henkoğlu, **Hassas Bilgi Varlıklarının Ve Kişisel Verilerin Hukuksal Düzenlemeler İle Korunması Ve Bu Kapsamda Üniversiteler İçin Bilgi Güvenliği Politikasının Geliştirilmesi**, Doktora Tezi, Ankara, 2015, s.18; GDPR'in gerekçe kısmında, bireylerin maddi/maddi olmayan zarar gördükleri veri işleme faaliyetlerinden temel hak ve özgürlükler açısından tehlike doğabileceği ve özellikle hassas verilerin işlenildiği durumların da bu kapsamda olduğu ifade edilmiştir. Bkz. GDPR, Recital para.75

[49] Metin Bulut, **Özel Bir Hukuksal Koruma ve Veri Kategorisi Alanı: Hassas Kişisel Veriler**, 2020/3 Ankara Barosu Dergisi, Hakemli Makale, s.123-124; Veri ihlali durumunda ihlale konu kişisel veriler hassas veri kategorisinde ise ihlal durumunun kişiler üzerindeki etkisi daha ciddi olacaktır. Özellikle hırsızlık, dolandırıcılık, fiziksel ve psikolojik zarar, aşağılanma ve şeref ve saygınlık ihlalinde bu türden etkiler gözlemlenebilecektir. Bkz. Article 29 Data Protection Working Party, **Guidelines on Personal Data Breach Notification Under Regulation 2016/679**, 6 February 2018, s.25

[50] Danıştay 15. Dairesi 08.07.2014 tarih ve 2014/1150 Esas sayılı kararı

[51] AİHM, S. ve Marper v. Birleşik Krallık Davası Kararı (Başvuru no.30562/04 ve 30566/04) para.125

Son olarak belirtmek gerekir ki hassas veriler için kişisel veri kavramının tanımındaki gibi geniş bir kapsam öngörülmeyip sınırlı bir alan belirlenmiştir ve kanunda belirtilen veriler dışında hiçbir veri kıyas yoluyla özel nitelikli veri kategorisine dahil edilemeyecektir.[52] Devam eden başlıklarda veri koruma kanunumuzda sayılan özel nitelikli kişisel veri kategorilerine ilişkin açıklamalara yer verilecektir.

2.1. Irk

Irk kavramı, etnik köken ve ulusal köken terimleriyle birlikte kullanılan bir terim[53] olmakla birlikte adı geçen bu üç terim için ulusal hukuk düzenlerinde genel olarak tam bir tanımlama yapılmamıştır.[54]

Irk, Türk Dil Kurumu tarafından kalıtımsal olarak ortak fiziksel ve fizyolojik özelliklere sahip insanlar topluluğu olarak tanımlanmaktadır.[55] UNESCO'ya göre ise ırk kavramı, biyolojik bir terim olarak Afrika ve Avrupa gibi kalıtsal açıdan farklılıklar gösteren insan topluluklarını ifade etmektedir. Bu şekilde insan grupları arasındaki kalıtsal farklılıklara dayanan ırk terimi, sınıflandırma için bir araç olmasının yanı sıra insanların ırk farklılıklarının kolayca ortaya koyulmasında da rol oynamaktadır.[56]

Irk verisi ile ilgili olarak dikkat çekilmesi gereken önemli bir husus ise söz konusu verinin işlenmesi sırasında gereken güvenlik önlemlerinin alınması ve kişilerin ırk verisinin büyük bir hassasiyetle korunmasıdır. Son yıllarda artan ve ırk ayrımcılığı amacı güden radikal akımların yükselişi dikkate alındığında bu verinin işlenmesi sırasında çok dikkatli olunması gerektiği söylenebilecektir. Zira kişilerin ayrımcılığa karşı korunması için uluslararası alanda birçok önemli adım atılmasına rağmen ırka dayalı ayrımcılık halen etkisini sürdürmektedir. Nitekim

---

[52] Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin Korunması Kanunu Hakkında Sıkça Sorulan Sorular**, KVKK Yayınları, Mart 2018, Ankara, s.22

[53] Örneğin Birleşik Krallık'ta ırk kavramının, renk, uyruk, ulusal ve etnik kökeni içerdiği kabul edilmiştir. Bkz. Equality Act 2010, Section 9

[54] European Commission, **European network of legal experts in gender equality and non-discrimination, The meaning of racial or ethnic origin in EU law: between stereotypes and identities**, s.62; Irk ve etnik köken kavramlarının birlikte incelendiği bir çalışma için bkz. Diego Junior, Silva Santos, Nathalia Palomares, David Normando, Cátia Cardoso, Cátia Cardoso Abdo Quintão, **Race versus ethnicity: Differing for better application**, Dental Press J. Orthod. vol.15 no.3 Maringá jun. 2010

[55] TDK, **Büyük Türkçe Sözlük**; Irk kavramının tarihsel gelişimi için bkz. Ünlütürk, Ö. (2015). **"Irk" Kavramının Tarihsel Gelişimi ve Adli Antropolojide Kullanımı**, Antropoloji , (29) , 93-116

[56] **The Race Question In Modern Science, The Race Concept Results of an İnquiry**, UNESCO, Paris, 1952, s.82-83

son yıllarda birçok Avrupa ülkesinde Neo-Naziler ve çoğunluğunu gençlerin oluşturduğu diğer gruplar tarafından sığınmacıları hedef alan ırkçı saldırılarda artış görülmüştür.[57]

Irk verisi ile ilgili açıklamalarımıza son verirken bir konuya daha değinmekte fayda görüyoruz ki bu da kişinin ten rengini belli edecek şekilde fotoğrafının çekilmesinin, ırk verisinin işlenmesi anlamına gelip gelmeyeceği hususudur. Bu kapsamda konuyla ilgili İngiltere'de görülen bir dava dikkat çekici bir emsal olmuştur. Naomi Campbell isimli bir mankenin uyuşturucu bağımlılarının katıldıkları toplantıdan çıkarken çekilen fotoğrafının gazetede yayınlanmasının ardından açılan davada Mahkeme, kişinin fiziksel özelliklerinden veyahut elbisesinden ırkının veya etnik kökeninin anlaşılabildiği fotoğrafları hassas veri saymıştır.[58] Kararın aksine Veri Çalışma Grubu[59]'nun bir raporunda ise bazı üye devletlerde fotoğrafın kişinin ırk/etnik kökenini ayırmak için kullanılabilecek olması nedeniyle hassas veri olarak kabul edildiği ancak genellikle internetteki fotoğrafların, kendisine ait olduğu kişiye ilişkin özel nitelikli veriyi ifşa etme amacıyla kullanılmadığı sürece hassas veri olmayacağı belirtilmiştir.[60]

2.2. Etnik Köken

Etnik köken terimi ilk olarak antik Yunan'da *"ethnos"* kelimesi ile ortaya çıkmış ve bu sözcük, yabancılar veyahut site devleti dışında yaşayan topluluklar için kullanılmıştır.[61]

Etnik köken kavramının tanımlanması için ortak miras, sosyal yönden arasında ilişki bulunan kültürel veya fiziksel nitelikler ve birtakım davranış ve yaklaşımların bir arada bulunması zorunluluk arz etmektedir. Bu bağlamda, ortak miras gerçek olabileceği gibi farazi de olabilecektir ve ortak bir ırkın mevcut olması da gerekmemektedir. Farklı inançlar, dinler, diller,

---

[57] United Nations, **Chapter 13 The Right To Equality And Non-Discrimination In The Administration Of Justice, Human Rights in the Administration of Justice: A Manual on Human Rights for Judges, Prosecutors and Lawyers**, s.613; Irka dayalı ayrımcılık, kişilere veya gruplara, taşıdıkları ırk özelliğine bağlı olarak farklı (eşit olmayacak şekilde) davranılması şeklinde tanımlanmaktadır.Bkz. Pager, Devah, and Hana Shepherd. 2008. **"The Sociology of Discrimination: Racial Discrimination in Employment, Housing, Credit, and Consumer Markets"**. Annual Review of Sociolgy, Harvard University, 34:181-209.; Irkçılığın, meydana geldiği her türü ile birlikte günümüzün henüz kabul edilmemiş bir insan hakları problemi olup dünya genelinde milyonlarca insanın hayatını ve haklarını tehdit ettiği ifade edilmektedir. Bkz. Anna Spain Bradley, **Human Rights Racism**, Harvard Human Rights journal / Vol. 32, 2019, s.2

[58] Campbell v. Mirror Group England and Wales High Court 27.3.2002

[59] GDPR'dan önce yürürlükte bulunan 95/46/AT sayılı Yönerge ile kurulmuş olan madde 29 Veri Koruma Çalışma Grubu, danışma organı vasfını taşımasının yanı sıra verilerin korunması ile ilgili birçok konuda öneri ve görüş sunarak bu alana önemli katkılar sunmuştur. Söz konusu grubun yerini GDPR'ın yürürlüğe girmesiyle beraber Avrupa Veri Koruma Kurulu almıştır. Bkz. Canan İmançlı, **Kişisel Sağlık Verilerinin Korunamamasından Doğan Özel Hukuk Sorumluluğu**, Yüksek Lisans Tezi, İstanbul -2019 s.21

[60] Article 29 Data Protection Working Party Opinion 5/2009 on online social networking, Adopted on 12 June 2009, s.8

[61] Mathias Bös, **International Encyclopedia of the Social & Behavioral Sciences** (Second Edition) 2015, Pages 136-141, s.136

kurumlar ve uygulamalar gibi kültürel özellikler bu kimliğin (etnik kökenin) temelini oluşturmaktadır. Ayrıca bazı durumlarda bu temel, kendini vücut şekli veya ten rengi gibi fiziksel özelliklerde somutlaştırabilmektedir. Böyle bir ortak kimliğin etnik grubun üyeleri arasında yerleşebilmesi için söz konusu grubun üyeleri, fikilerini, davranış biçimlerini, duygularını ve bir amacı paylaşmalıdırlar. Neticeten bu bireyler, kendilerini diğer topluluklardan ayırıp aynı kaderi paylaştıkları yönünde bir düşünceyi benimsemelidirler.[62]-[63]

2.3. Siyasi Düşünce

Çağdaş demokrasilerin temel yapı taşı niteliğindeki siyasi partiler, vatandaşların ülke yönetimine katılmasına aracılık eden önemli kurumlardır. Ancak kişilerin savunduğu siyasi düşüncelerden veyahut desteklemekte olduğu siyasi partilerden ötürü ayrımcılığa maruz kalmaması ve toplumda meydana gelebilecek olası çatışmaların önüne geçilmesi açısından siyasi verilerin işlenilmesinde büyük bir hassasiyet gösterilmelidir. Aynı yönde belirtmek gerekirse AHİM'in kararına konu bir olayda kişinin katıldığı bazı siyasi içerikli gösteriler ile ilgili olarak söz konusu kişinin bahsi geçen o gösterilere katıldığı yönündeki bilgilerin polis tarafından kayıt altına alınması durumunda siyasi görüşü belirten bu verilerin yüksek korumaya ihtiyaç duyduğu ifade edilmiştir.[64] Nitekim bu doğrultuda da 6698 sayılı Yasa uyarınca bahsi geçen türden veriler hassas veri kategorisi içerisine alınmıştır. Öte yandan GDPR ve Birleşik Krallık uygulaması da konuyla ilgili yol gösterici niteliktedir. GDPR'a göre seçim faaliyetlerinde olmakla birlikte şayet üye devletlerin demokratik sistemleri siyasi partilerin, kişilerin siyasi görüşlerini toplamasını gerektirirse bu veri işleme faaliyeti yeterli güvenlik

---

[62] Rishikeshav Regmi, **Ethnicity And Identity**, Occasional Papers in Sociology and Anthropology Vol.8 2003 p.1-11, s.2-3; Webert, Horowitz ve Schermerhorn gibi sosyal teorisyenler fenotipsel farklılıkla yansıtılan biyolojik etmenleri etnik kökenin ana noktası olarak yorumlamışlar ve ardından uyruğu merkez kavram olarak kabul etmişlerdir. Bkz. Peter Ratcliffe University of Warwick, **"Ethnic group", Sociopedia.isa** 2014, s.5

[63] Etnik kimliğin iç ve dış görünüşü olduğu belirtilmekle beraber dış görünüşünün kültürel ve sosyal olan ve ayrıca gözlemlenebilir bazı davanışlara dayandığı belirtilmektedir. Bu davranışlar: 1) Etnik dili konuşma ve etnik adetleri uygulama, 2) Etnik kökene dayalı kişisel ilişkiler kurma (örneğin aile veya arkadaşlık ilişkisi), 3) Etnik kökene dayalı kuruluşlara (örneğin kilise, okul) katılma, 4) Çeşitli klüp ve organizasyonlar gibi etnik kökene dayalı gönüllü topluluklara katılma, 5) Etnik köken odaklı organizasyonların faaliyetlerine katılma (örneğin piknik, konferans, konser). Etnik kökenin iç görünümü ise fikirleri ve duyguları kastetmektedir. Bu iç görünüm ise 1) Zihinsel 2) Ahlaki 3) Duygusal olarak üç şekilde ortaya çıkmaktadır. Bkz. **Definition And Dimensions Of Ethnicity: A Theoretical Framework In Challenges of Measuring an Ethnic World: Science, politics and reality: Proceedings of the Joint Canada-United States Conference on the Measurement of Ethnicity** April 1-3, 1992, pages 407-27, s.8; Anthony D. Smith ise etnik grubu, atalarından kalan mitleri, tarihi ve kültürleri belirli bir bölge ile ilişkili şekilde birlik ruhu içinde paylaşan insanlar olarak tanımlamaktadır. Bkz. Anthony D. Smith, **Ethnic Origins of Nations**, Blackwell Publishing, 1986, s.32

[64] AİHM, Case Of Catt V. The United Kingdom, Application no. 43514/15 24.1.2019 Para.123; Nitekim son verilere göre Türkiye'de 102 tane siyasi partinin faaliyet gösterdiği düşünüldüğünde bu partilere üye kişi sayısının çok fazla olduğu ve bundan dolayı siyasi düşünce verisinin ne kadar çok işlendiği sonucu ortaya çıkmaktadır. Bkz. https://www.siviltoplum.gov.tr/siyasi-partilere-iliskin-istatistikler (22.11.2020 tarihinde erişildi.)

önlemlerinin alınması şartıyla ve kamu yararı amacıyla yapılabilecektir.[65] Birleşik Krallık Veri Koruma Yasası'nda ise kişinin siyasi düşüncesini belli eden verilerin işlenebilmesi, ancak siyasi partinin amacı için gerekli olması, verisi işlenen kişiye zarar vermemesi ve ilgili kişinin kendi verilerinin işlenmemesi gerekliliğini yazılı olarak bildirmemesi gibi şartlara bağlı tutmuştur.[66]

2.4. Felsefi İnanç

AİHM'e göre dini ve felsefi inançlar, -dinlerin kozmolojik, felsefik veya ahlaki her türlü soruya cevabı olan veya olabilecek geniş bir dogmatik ve ahlaki bir varlık oluşturduğu göz önüne alındığında- öznel anlayışların dahi önemli olabildiği din konusuna karşı kişilerin takındıkları tavrı/tutumu ilgilendirmektedir.[67] Ayrıca AİHM, felsefenin birçok anlam taşıdığını, kavramın tam tekmil bir düşünce sistemini çağrıştırabildiği gibi önemsiz konulardaki görüşleri belirtmek için de kullanıldığını ifade etmiştir.[68] Ayrıca Mahkeme tarafından hazırlanan AİHS m.9(düşünce, vicdan ve din ve özgürlüğü) ile ilgili rehberde bazı felsefi inançlar olarak barışçıllık, askerlik hizmeti karşıtlığı, veganlık, kürtaj karşıtlığı, alternatif tıp hakkında ve tıp felsefesi hakkında ortaya konulan düşünceler içeren doktor görüşü, evliliğin bir erkek ve bir kadın arasında hayat boyu süren bir birliktelik olduğu ve homoseksüel birlikteliğin reddedilmesi gibi düşünce formları da zikredilmiştir.[69]

2.5. Din, mezhep, diğer inanç

İslam Ansiklopedisi'nde din kavramına ilişkin olarak her dinî kültürün din kavramını ifade etmek üzere seçtiği kelimelere ait anlamların ortak noktasının "yol, inanç, âdet, bağ, kulluk" olduğunun ifade edilebileceği ve ayrıca bütün bu kelimelerin, kökleri insanın iç hayatında bulunan ve semereleri çeşitli davranışlarla tezahür eden köklü ve evrensel bir fenomeni ifade etmeyi amaçladığı belirtilmiştir.[70]

Din ile ilgili veriler karşımıza en çok eski tip nüfus cüzdanlarında çıkmaktadır. Zira bu kimliklerin arka yüzünde din hanesi şeklinde bir bölüm bulunmaktadır. Şayet eski tür kimlik kartlarının arka yüzünün fotokopisinin çekilmesi gibi bir işlem yapılırsa özel nitelikli veri

---

[65] GDPR Recital 56

[66] Data Protection Act 2018, Schedule 1 para. 22; **Guidance on political campaigning, Draft framework code for consultation**, Information Commissioner's Office (ICO) s.45

[67] Case of İzzettin Doğan And Others V. Turkey (Application no. 62649/10) para. 107; Case of Mansur Yalçın and Others

[68] Case of Campbell And Cosans V. The United Kingdom (Application no. 7511/76; 7743/76), para. 36

[69] European Court of Justice, **Guide on Article 9 of the European Convention on Human Rights**, Updated on 31 August 2020, s.9

[70] Günay Tümer, **TDV İslam Ansiklopedisi**, TDV İslâm Araştırmaları Merkezi, 1992 s.312,320

işlenmesi meydana gelecektir.[71] Diğer bir örnek ise uçak bileti alırken kişilerin dinleriyle ilgili taşıdıkları hassasiyetten dolayı yemek seçimlerinde hangi dine mensup olduklarını belirtmesi durumudur. Bu halde de uçuş şirketi tarafından hassas veri işlenmiş olacaktır.[72]

Mezhep kavramı ise dinin aslî veya fer'î hükümlerinin dayandığı delilleri bulmakta ve bunlardan hüküm çıkarıp yorumlamakta otorite sayılan âlimlerin ortaya koyduğu görüşlerin tamamı veya belirledikleri sistem şeklinde tanımlanmaktadır.[73] Mezhep verisi işlenirken son derece dikkatli olunmalı ve gereken tedbirler alınmış olmalıdır. Zira mezhep farklılığına dayanan çatışma ve ayrımcılıklar son derece yıkıcı sonuçlara yol açabilmektedir. Nitekim Anayasa Mahkemesinin verdiği bir kararın karşı oy gerekçesinde mezheplerin, ülkemizin gerçeklerinden olup varlığı inkar edilemeyeceği bunun yanında mezhep farklılıklarının körüklenmesinin birçok zarara yol açtığının tecrübe edildiği belirtilerek bireylerin mezhep bilgilerinin aleniştirilmesinden kaçınılması gerektiği ifade edilmiştir.[74]

2.6. Kılık ve kıyafet

Kılık kıyafet kategorisi ülkemize özgü olarak özel nitelikli veriler arasında kabul edilmiştir. Ancak bu noktada kılık kıyafetle ilgili her verinin hassas veri olarak kabul edilmesi, giyim sektöründeki şirketlerin işlemekte olduğu -örneğin kendi müşterilerine ilişkin- çoğu verinin hassas veri sayılmasına yol açacaktır. Özel nitelikli kişisel verilerin düzenlenme biçimi göz önüne alındığında bu türden bir yaklaşımın bahse konu veri kategorisinin sınırlarını kanunun amacına aykırı olarak genişleteceği açıktır. Bu durumda, madde gerekçesinde belirtilen ayrımcılık vurgusu dikkate alınarak bir yorum yapılması gerekmektedir. Böylece ancak ayrımcılığa yol açacak şekilde işlenen kılık kıyafet verisi (örneğin kişinin açık giyindiği, başının örtülü olduğu gibi) hassas veri kategorisine dahil edilmek suretiyle kanunun amacına uygun bir yorum tercih edilmiş olacaktır.[75]

---

[71] Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin Korunması Kanunu ve Getirdikleri**, KVKK Yayınları no: 26, s.13

[72] Handbook on European data protection law 2018 Edition, Publications Office of the European Union, s.91

[73] İlyas Üzüm, **TDV İslam Ansiklopedisi**, 2004, YDV İslam Araştırmaları Merkezi, s.526-532; Anayasa Mahkememiz ise bir kararında mezhep kavramını bir dinin görüş, yorum ve anlayış farklılıkları sebebiyle ortaya çıkan kollarından her biri olarak tanımlamıştır.

[74] AYM, E. 2016/125 K. 2017/143 T. 28/9/2017 Osman Alifeyyaz PAKSÜT karşı oy yazısı

[75] Dülger, Kişisel Verilerin Korunması Hukuku, s.180; AYM ise kılık kıyafet ibaresini *"kişilerin... dinî inancıyla bağlantılı kılık ve kıyafetine ilişkin verilerin özel nitelikli kişisel veriler olduğu kuşkusuzdur."* şeklinde yorumlamıştır. Bkz. AYM, E. 2016/125 K. 2017/143 T. 28/9/2017

2.7. Dernek, vakıf, sendika üyeliği

Ülkemizde özellikle vakıf kültürünün Osmanlı Devleti'nden bu yana yaygın olması sivil toplum açısından örgütlenmenin etki alanını genişletmektedir. Son istatistiklere göre Türkiye'de faal dernek sayısı 121.501 olup 2010 yılından bu yana her yıl 100'ün üzerinde de vakıf açılmaktadır.[76] Bunun yanında sadece İstanbul'da faaliyet gösteren sendika sayısı ise 149'dur.[77] Dernek, vakıf ve sendika gibi kuruluşlar özellikle ilk üyelik kaydı sürecinde üye olmak isteyen kişilerden birçok bilgi talep etmekte ve bu verileri üyelik süreci içerisinde farklı amaçlar (örneğin toplantı saati ve yerini bildirmek için SMS gönderme) dahilinde işlemektedir. Söz konusu kuruluşların ülkemizdeki sayıları ve üye potansiyeli düşünüldüğünde çok fazla kişisel verinin işleme faaliyetine konu olduğu görülecektir. Bu nedenle yukarıda değindiğimiz kuruluşların özellikle üyelerine ilişkin kişisel verileri işlerken gereken tedbirleri alması gerektiğini belirtmek gerekir.

2.8. Sağlık Verisi

Sağlık verisi, kişinin fiziksel ve ruhsal durumu yanında kişiye sunulan sağlık hizmetleriyle de ilgili bilgilerdir. Yapılan test sonuçları, kullanılan ilaçlar gibi bilgiler bu kategori kapsamında değerlendirilmektedir.[78] Ayrıca sağlık verisi, kişinin sadece şu anki durumunu değil; geçmiş durumunu da ilgilendirmektedir.[79]

Diğer alanlarda olduğu gibi sağlık sektöründe de kişisel verilerin işlenmesi giderek artmaktadır. İlk olarak kan örnekleri, röntgenler, geçmişte yaşanılan hastalıklar ve tedavileri, hastanın kullandığı ilaçlar gibi birçok sağlık verisinin eczanelerden hastanelere kadar birçok kurum arasında dolaşıma sokulduğunu belirtmek gerekir. İşlem hayatının gelişen hızının getirilerinden biri olan ve daha iyi sağlık hizmeti sunulması amacıyla ortaya çıkan bu durum, sağlık alanında kişisel verilerin korunması konusunda birçok endişeyi beraberinde getirmiştir. Uygulamada ortaya çıkan bazı sorunlar bireylerin bu konudaki endişelerinde haklı olduklarını ortaya koymaktadır. Sağlık verilerinin bilimsel araştırma amacıyla anonimleştirilmeden ya da

---

[76] Yıllara göre değişimi gösteren grafik için bkz. https://cdn.vgm.gov.tr/genelicerik/genelicerik_945_290519/06-yil-icinde-kurulan-yeni-vakif-sayilari-2001-050.pdf (22.11.2020 tarihinde erişildi.); Dernek sayıları için bkz. https://www.siviltoplum.gov.tr/dernek-sayilari (22.11.2020 tarihinde erişildi.)

[77] Sorgulama sayfası için bkz. https://www.siviltoplum.gov.tr/sendikalara-iliskin-istatistikler (22.11.2020 tarihinde erişildi.)

[78] **100 Soruda Kişisel Verilerin Korunması Kanunu**, KVKK Yayınları, Nisan 2018, Ankara, s.21; Danıştay bir kararında sağlık verisini, bireyin fiziksel/biyolojik özelliklerine ilişkin bilgiler olarak tanımlamıştır. Bkz. Danıştay 15. Dairesi E.2014/150 T. 8.7.2014.

[79] Alaattin Bük, **Bilişim Alanında Kişisel Verilerin Korunması**, Seçkin Yayınları, Ankara 2018, s.40

hastaların rızalarının alınmadan kullanılması ve paylaşılması[80], muayene olduktan sonra hastaya ilgili hastalıkla bağlantılı reklam sms'lerinin iletilmesi, hasta verilerinin yedeklendiği DVD'lerin fiziksel güvenliklerinin sağlanmadan saklanması sözünü ettiğimiz sorunlara örnek gösterilebilir.[81] Bu konuda, başta hastaneler olmak üzere hastaların kişisel verilerini işleyen bütün kurumlar ve sağlık çalışanları gerekli altyapıya sahip olmalıdır. Ayrıca etkin korumayı sağlayacak düzenlemelerin yapılması ve bu kapsamda da meşru amaç için toplanma, belirli bir süre için tutulma, veri güvenliğinin sağlanması, asgari miktarda (gerekenden fazla olmayacak şekilde) bilgi toplanması hususlarına dikkat edilmelidir.[82] Ancak bu noktada, diğer sektörleri de yakından ilgilendiren şu hususa dikkat çekmek gerekir: Kişisel verilerin korunmasına yönelik yasal düzenlemelerin önemi yadsınmamakla birlikte söz konusu düzenlemeler yeterli değildir. Bireylerin sahip oldukları haklar konusunda yeterince aydınlatılması ve mahremiyet hakkına yönelik farkındalıklarının artırılması, yasal düzenlemelerin daha etkin bir şekilde hayata geçirilebilmesine olanak sağlayacaktır. Ayrıca eklemek gerekirse kişisel verilerin mahremiyetini örselemeden bu bilgilerin kullanılabilmesinin temel yolu, kavramın tanımında yer alan "kişi"nin belirlenebilirliğinin kaldırılması yani bilgilerin anonimleştirilmesi olacaktır. Böylece bilgilerin kişisellik niteliği ortadan kalkarak sadece veri özelliği söz konusu olacaktır.[83]

Teknolojik imkanların gelişmesiyle birlikte ülkemizde de sağlık verilerinin işlendiği programların kullanımı artmıştır. Elektronik ortamda bireylerin kişisel verilerinin dolaşımını sağlayan son örneklerden biri e- nabız uygulamasıdır. E-nabız, sağlık hizmeti veren kurumlardan toplanan sağlık verilerine vatandaşların ve sağlık çalışanlarının internet ve mobil cihazlar üzerinden erişebildiği bir uygulama olmakla birlikte söz konusu sistem sayesinde hastaların tıbbi özgeçmişi (hastalıklar, yapılmış olan testler ve konulan tanılar) de görülebilmektedir.[84]

---

[80] Dünya Sağlık Örgütü'nün muayenelerde ve bilimsel araştırmalarda kişisel verilerin kullanımının artmasından ötürü 2000'de yayınladığı bildirgede de yer aldığı üzere bilimsel araştırma gibi amaçlarla elde edilecek kişisel verilerin hastaların rızalarının raporda da belirtilen Helsinki deklerasyonundaki standartlara göre alınması gerektiği ve hastaların kendi kişisel verilerinin saygı duyulacağını bilmesinin bu verileri paylaşma konusunda onlara güven vereceği belirtilmiştir. Bkz. World Medical Association, **Declaration Of Taipei On Ethical Considerations Regarding Health Databases And Biobanks**, October 2002 Ayrıca bkz. Bonnie Kaplan, **How Should Health Data Be Used? Privacy, Secondary Use And Big Data Sales**, Yale Isps-Bioethics Working Paper, October 2014, s.7

[81] Enis Karaarslan/Ali Murat Ergin/Nalin Turğut/Özgür Kılıç, **Elektronik Sağlık Kayıtlarının Gizlilik ve Mahremiyeti**, Conference Paper, December 2015, s.8

[82] Elif Küzeci, **Türkiye'de Sağlık Verilerinin Korunması: Hukuksal Çerçeve**, Kişisel Sağlık Verileri Ulusal Kongresi, Nisan 2016, İstanbul Türk Tabipleri Birliği Yayınları, s.20

[83] M.Cumhur İzgi, **Mahremiyet Kavramı Bağlamında Kişisel Sağlık Verileri**, Türkiye Biyoetik Dergisi, 2014 Vol. 1, No. 1, s.35-36

[84] Bkz. Sağlık Bakanlığı, **e-nabız Kullanım Kılavuzu** 2018, s.3

Bunun yanında 2020 yılında tüm dünyayı sarsan Covid-19 virüsü ile mücadele sürecinde hayatımıza giren birçok tedbirin uygulanmasında kişilerin sağlık verilerinin olağanüstü seviyede işlendiği görülmektedir. Söz konusu önlemler düşünüldüğünde akla ilk gelenlerden birisi ise HES (Hayat Eve Sığar) kodu uygulaması olmaktadır. HES kodu, Covid-19 hastalığı yönünden bu kodun sahibi olan kişinin hasta olup olmadığı veya hastalığı taşıyan kişilerle temasının bulunup bulunmadığını göstermektedir. Bu kod, özellikle sayahat yapacak kişiler açısından zorunlu tutulmakla birlikte bazı yerlere (örneğin AVM, Adliye) giriş yaparken ilgili kurumlar tarafından aranmaktadır. İçerdiği bilgiler ve bu bilgilerin tabi tutulduğu işlemler dikkate alındığında HES kodu aracılığıyla vatandaşların kişisel sağlık verilerinin işlendiğini söylemek yanlış olmayacaktır.[85] Pandemi ile ilgili diğer bir örnek ise hastalığın tespiti sürecinde yapılan test sonuçlardır. Antijen, antikor ve PCR testleri sonucunda elde edilen veriler sağlık verisi kategorisinde olup hassas veri niteliğini haizdir. Bu kapsamda özel nitelikli verilere ilişkin hükümler bahsi geçen test sonuçlarındaki verilere de uygulanacaktır.[86]

2.9. Cinsel hayat

Biyolojik olarak cinsellik, temel bir iç güdü olmasının yanı sıra birçok organ ve hormonun birlikte katıldığı ve tüm metabolizmanın aktif olduğu bir süreçtir.[87] Cinsel hayat, kapsamı oldukça geniş olan bir kavram olup çeşitli unsurları içinde barındırmaktadır. Bu unsurlardan ilki ve en önemlisi ise cinsiyettir. Cinsiyet, kişinin biyolojik durumunu ifade eden ve erkek, kadın ve intersex[88] şeklinde alt kategorileri olduğu kabul edilen bir kavramdır.[89]

Cinsel yaşamın diğer önemli bir kavramı olan cinsel eğilim ise kişinin cinsel veya duygusal olarak etkilendiği cinsiyeti belirtmektedir.[90] Ayrıca bu terim kimlik, davranış ve diğer kişilerle

---

[85] Sinan Sami Akkurt, **Kişisel Sağlık Verilerinin İşlenmesine Ve Covıd19 Pandemisi Sürecinde Mobil Uygulamalarla Paylaşılmasına Hukukî Bir Bakış**, İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi Covid-19 Hukuk Özel Sayısı Yıl:19 Sayı:38 Yaz 2020/2 (Covid-19 Özel Ek), s.153; Ayrıca bkz. https://hayatevesigar.saglik.gov.tr/hes.html

[86] Akkurt, s.148; HES kodunun kişisel veri olduğu ancak başlı başına özel nitelikli veri niteliği taşımadığı ve söz konusu kodun okutulması neticesinde kişinin risk taşıyıp taşımadığını belirten bilgilerin ise hassas veri kategorisinde değerlendirileceği ifade edilmiştir. Bkz. Umut Zorer, **COVID-19 Pandemisinde Temas Takip Uygulamaları Ve Gözetim Toplumu, Covıd-19 Pandemisinde Dijital Dönüşüm ve Hukuk**, İstanbul Barosu - 2021, s.20

[87] Cinsel Eğitim Tedavi ve Araştırma Derneği (CETAD), **Bilgilendirme Dosyası – 1 Cinsel Yaşam ve Sorunları**, s.8

[88] Intersex terimi, ne erkek ne de kadın vücudunun tipik niteliklerine uyan özellikler gösteren cinsiyet karakteriyle doğan kişileri ifade etmektedir. Bkz. **Factsheet Intersex**, United Nations Human Rights

[89] American Psychological Association. (2012). **Guidelines for Psychological Practice with Lesbian, Gay, and Bisexual Clients**, American Psychologist, 67(1), 10–42.

[90] American Psychological Association & National Association of School Psychologists. (2015). **Resolution on gender and sexual orientation diversity in children and adolescents in schools**

olan ilişkileri de ifade etmektedir.[91] Bu kapsamda gay, lezbiyen, biseksüel terimleri de cinsel eğilim içerisinde kullanılmaktadır.[92] Transbirey terimi ise doğumla sahip olunan cinsiyetten farklı bir cinsel kimlik taşıyan kişiyi tanımlamaktadır.[93]

Avrupa İnsan Hakları Mahkemesi, cinsel yaşam ve cinsel eğilim kavramlarını, özel ve aile hayatına saygı hakkı (AİHS m.8) kapsamında koruma altına alınmış olan kişisel alanın önemli unsurları olarak değerlendirmektedir.[94] Mahkeme, özel hayatın kapsamının geniş olduğunu vurgulamakla birlikte kişinin bu hayat alanının kendi kimliğinin birçok yönünü -cinsel kimlik ve cinsel yönelim gibi- kapsamakta olduğunu belirtmektedir. Ayrıca AİHM, cinsel yönelimin, kişinin kimliğinin temel parçalarından biri olduğunu ve cinsel yönelim ile cinsiyetin iki ayrı ve dahi sıkı ilişkili özellikler olduğunu kabul etmektedir.[95]

2.10. Ceza mahkumiyeti ve güvenlik tedbiri

Kişilerin adli siciline ilişkin bilgilerin hangi tür işlemlere tabi tutulacağı başta Adli Sicil Kanunu olmak üzere mevzuatımızda çeşitli yerlerde düzenlenmiştir. Adli Sicil Kanunu'nun birinci maddesinde söz konusu kanunun kesinleşmiş ceza ve güvenlik tedbirlerine mahkûmiyete ilişkin bilgilerin otomatik işleme tâbi bir sistem kullanılarak toplanmasına, sınıflandırılmasına, değerlendirilmesine, muhafaza edilmesine ve gerektiğinde en seri ve sağlıklı biçimde ilgililere bildirilmesine dair usul ve esasları belirlediği hüküm altına alınarak kişilerin adli sicil bilgilerine ilişkin olarak nasıl bir yol izleneceğinin genel çerçevesi çizilmiştir.

Bireylerin toplum içerisindeki itibarının korunması açısından adli sicil bilgileri büyük öneme sahiptir. Nitekim kişilerin lekelenmeme hakkıyla yakından bağlantılı olan arşiv kayıtlarının ne kadar süre ile saklanacağı konusu birçok tartışmaya konu olmuştur. Zira hakkında verilen bir mahkumiyet kararını, kişinin ömrü boyunca yanında taşıması birçok hak ihlalini beraberinde getirecektir. Nitekim GDPR'ın gerekçe bölümünde de bu türden bilgiler üzerinde kişinin kontrolünün önlenmesinin kendisi açısından fiziksel ve ruhsal zararlara yol açabileceğine değinilmiştir.[96] Anayasa Mahkememiz ve AİHM de birçok kararında bahsi geçen bilgilerin uzun süre saklanmasının veya ölçüsüz şekilde işlemlere tabi tutulmasının hak ihlallerine sebep

[91] European Union Agency for Fundamental Rights, **EU LGBT survey European Union lesbian, gay, bisexual and transgender survey Results at a glance**,2013, s.8

[92] American Psychological Association. (2015). **APA dictionary of psychology** (2nd ed.)

[93]American Psychological Association. (2015). **Guidelines for Psychological Practice with Transgender and Gender Nonconforming People**, American Psychologist, 70(9), 832-864.

[94] **Guide on Article 8 of the European Convention on Human Rights**, European Court of Human Rights, August 2020, s.38

[95] Case of Sousa Goucha v. Portugal para.23-27; Case Of Beizaras And Levickas v. Lithuania, para.109

[96] Bkz. GDPR, Recital 75

olacağını ifade etmiştir. Konuyla ilgili önemli bir kararında Anayasa Mahkemesi, Adli Sicil Kanunu'nun arşiv bilgilerinin silinmesinde öngördüğü 80 yıl üst sınırı ile ilgili olarak kişinin belli bir tarihte aldığı herhangi bir mahkumiyet kararına ilişkin kaydın bireyin ölümüne kadar ya da seksen yıl süreyle muhafaza edilmesinin, Anayasa'nın 5. ve 17. maddelerinde belirtilen kişinin maddi ve manevi varlığının geliştirilmesi ilkesi ve cezaların ıslah edici olma amacı ile bağdaşmadığını ifade etmiş ve Adli Sicil Kanunu'nun 12. maddesinin birinci fıkrasının iptaline karar vermiştir.[97]

108 Sayılı Sözleşme'ye bakıldığında ise sözleşmenin 6. maddesinde hassas verilere yer verilmiş ve devletlerin iç hukukunda bu türden veriler için uygun güvencelerin sağlanması gerektiği ve aynı durumun ceza mahkumiyeti ile ilgili veriler için de geçerli olduğu belirtilmiştir.[98] GPDR'da ise mahkumiyete veya güvenlik tedbirlerine ilişkin bilgiler özel veri kategorisinde sayılmamış ancak ayrıca düzenlenen bir madde ile koruma kalkanı oluşturulmuştur.[99]

2.11. Biyometrik veri

Biyometrik veri, kişinin bizzat kendisinin taşıması nedeniyle değiştirilmesi veya unutulması mümkün olmayan verilerdir. Biyometrik veriler fizyolojik veyahut davranışsal olabilir. Fizyolojik biyometrik veriler, insan vücuduna ilişkin benzeri olmayan özellikleri barındırmaktadır. Örneğin, iris, retina, parmak izi, avuç içi, yüz, damarlar fizyolojik biyometrik veri olarak sayılmaktadır. Öte yandan davranışsal biyometrik veri ise dinamik bir yapıda olup zaman, ruh hali, yaş gibi etkenlere göre değişkenlik gösterebilmektedir. Örnek olarak yürüyüş şekli, akıllı cihazlar kullanırken kişinin ekrana uyguladığı basınç, araba sürüş biçimi bu kapsamdadır.[100] Biyometrik verilerle kişinin kendine has özelliklerinin yanında kimliği de tespit edilebilmektedir.[101]

---

[97] AYM, E. 2008/44 K.2011/21 T. 201.1.2011

[98] 108 Sayılı Sözleşme m.6'ya göre iç hukukta uygun güvenceler sağlanmadıkça, ırksal kökeni, siyasi düşünceleri, dini veya diğer inançları ortaya koyan kişisel veriler ile sağlık veya cinsel hayatla ilgili kişisel veriler otomatik işleme tabi tutulmayacak ve aynı durum ceza mahkumiyetiyle ilgili kişisel veriler için de geçerli olacaktır.

[99] Bkz. GDPR m.10

[100] Biyometrik imza verisinin kullanılmasına ilişkin görüş talebi" ile ilgili olarak Kişisel Verileri Koruma Kurulunun 27.08.2020 Tarihli ve 2020/649 Sayılı Karar Özeti. Ayrıca kararda biyometrik imza da biyometrik veri olarak kabul edilmiştir.

[101] Danıştay 15. Dairesi E. 2014/4562 T. 11.9.2014; Ayrıca Danıştay 15. Dairesi 5510 sayılı Sosyal Sigortalar ve Sağlık Sigortası Kanunu'nun 67. maddesinin 3. fıkrasına eklenen ve biyometrik yöntemlerle kimlik doğrulamasının yapılmasının önünü açan hükmün iptali için de Anayasa Mahkemesine başvurmuş ancak söz konusu kuralın anayasaya uygun olduğu yönünde karar verilerek iptal istemi reddedilmiştir. Bkz. AYM E.2014/180 K. 2015/30 T.19.3.2015. Diğer bir kararında ise AYM. Aynı yasanın farklı bir hükmü ile ilgili olarak Danıştay 15. Dairesinin yaptığı başvuruyu kabul etmiştir. Bkz. E. 2014/74 K. 2014/201 T. 25.12.2014

Biyometrik verilerle ilgili olarak bu hassas verilerin işlenmesine olanak sağlayan bazı hükümler mevzuatımızda düzenlenmiştir. Örneğin kişinin ceza infaz kurumuna yerleştirilme işlemlerine ilişkin olarak 5275 sayılı Ceza ve Güvenlik Tedbirlerinin İnfazı Hakkında Kanun'un 21'inci maddesinin 3'üncü fıkrasında tanıya yönelik olmak suretiyle hükümlülerin parmak ve avuç içi izleri alınacağı ve fotoğraflarının çekileceği, kan grupları, vücutlarının dış özellikleri ve ölçülerinin belirlenmesinin akabinde kayıt altına alınan söz konusu bilgilerin hükümlünün kişisel dosyasında veya elektronik ortamda saklanacağı belirtilmiştir. Ayrıca söz konusu bilgilerin kanunun zorunlu kıldığı hâller dışında hiçbir kurum ve kişiye verilemeyeceği hüküm altına alınmıştır. Söz konusu hüküm incelendiğinde görülmektedir ki parmak ve avuç içi izleri gibi biyometrik veriler, kişi kuruma kabul edilirken yetkili makamlarca işlenebilecektir.

Biyometrik veri başlığı altında önemli bir tartışma konusuna değinmekte fayda görüyoruz. Son zamanlarda Covid-19 pandemisinin de etkisiyle uygulama alanı genişleyen uzaktan eğitim sistemlerinde görüntü ve ses kaydı yapılmasıyla ilgili olarak Kişisel Verileri Koruma Kurulunun yayınladığı 7.4.2020 tarihli kamuoyu duyurusunda uzaktan eğitim platformlarında, öğrencilerin ad ve soyadları gibi kişisel verileri ile ses ve görüntü gibi biyometrik veri kapsamında değerlendirilebilecek bazı özel nitelikli kişisel verilerinin işlendiğinin görüldüğü ifade edilmiştir.[102] Söz konusu duyurudan sonra ses ve görüntü verisinin biyometrik veri grubunda değerlendirilip değerlendirilemeyeceği tartışmaları gündeme gelmiştir. Ancak belirtelim ki her türlü görüntü ve ses verisinin özel nitelikli veriler arasında sayılan biyometrik veri kategorisinde değerlendirilmesi mümkün gözükmemektedir. Zira bir görüntü veya sesin biyometrik veri kapsamında sayılabilmesi için o verinin işlendiği sistemin, veri sahibini diğer kişilerden ayırt edebilecek niteliklere sahip olması gerekmektedir. Örneğin görüntülü görüşme esnasında görüşmenin yapıldığı uygulama yüz tanıma özelliği aracılığıyla toplantıya katılan kişinin kim olduğunu tespit edebiliyorsa artık biyometrik verinin işlendiğinden bahsedilebilecektir. Bu kapsamda değerlendirme yapıldığında ise neticeten her türlü ses veya görüntünün biyometrik veri kapsamına alınamayacağı ve biyometrik veriden söz edilebilmesi için verinin işlendiği sistemin yukarıda değinilen niteliklere sahip olması gerektiği sonucuna varılacaktır.[103]

---

[102] Kişisel Verileri Koruma Kurulunun 7.4.2020 tarihli Uzaktan Eğitim Platformları Hakkında Kamuoyu Duyurusu

[103] Dülger, *Kişisel Verilerin Korunması Hukuku*, s.180-182; Kişisel Verileri Koruma Kurulu, 25/03/2019 tarih ve 2019/81 sayılı kararı ve 31/05/2019 tarih ve 2019/165 sayılı karar özeti; GDPR'a göre fotoğraf, ancak kişinin kimliğinin benzersiz ve tek olarak tespit edilmesini veya doğrulanmasını sağlayan teknik araçlar vasıtasıyla işlendiğinde biyometrik veri olarak kabul görecektir. Bkz. GDPR, Recital 51; İngiltere'de görülen ve Naomi Campbell isimli mankenin fotoğrafının uyuşturucu bağımlılarının katıldıkları toplantıdan çıkarken çekilip gazetede yayınlanması ile ilgili davada mahkeme, fotoğraf verisi ile ilgili bazı tespitlerde bulunmuştur. Buna göre kişilerin fotoğrafları, yazılı açıklama/betimlemelerden daha fazla bilgi içermektedir ve bu yüzden fotoğraflar daha canlıdır ve

Son olarak günümüzde birçok alanda yaygınlaşmaya başlayan ve biyometrik verinin ana işleme merkezlerinden olan yüz tanıma sistemlerine değinmekte fayda vardır. Kimlik tanımada yüzün bu kadar ön planda olmasının nedeni insanı diğer kişilerden ayırıcı bir özellik taşıması ve aleni olarak gözlemlenebiliyor olması şeklinde belirtilmiştir. Buna ek olarak sakal gibi unsurlar tanınmamak için rahatlıkla değiştirilebilirken yüzün değiştirilmesi ise oldukça zordur.[104] Uygulama alanı gittikçe artan bu sistemler başta teknoloji şirketleri olmak üzere resmi kurumlar[105] tarafından da birçok alanda kullanılmaktadır. Ancak bu noktada unutmamak gerekir ki biyometrik veriler, hassas veri kategorisinde yer almasının bir sonucu olarak ilgili kişiye ilişkin mahrem bilgi niteliğinde olmaları nedeniyle bu veriler kamu makamlarınca işlenecek ise kamu hizmeti amacının bulunması, veri işleme açısından başka bir çözümün bulunamamış olması ve gereken güvenlik önlemlerinin de tesis edilmiş olması aranmalıdır.[106]

2.12. Genetik veri

Genetik veri, gerçek kişiden alınan biyolojik örneklerin incelenmesiyle (örneğin DNA, RNA, kromozom incelenmesi ya da buna eşdeğer bir bilgiyi sağlayan unsurun tetkiki ile) ulaşılan, ırsi olarak aktarılan ya da elde edilen ve -bireyin- genetik karakterlerini ilgilendiren kişisel veriler şeklinde tanımlanmaktadır.[107] Diğer bir tanımlamada ise genetik veri, bireyin veya birbirleriyle ilişkili kişilerin kalıtsal/ırsi özelliklerini ilgilendiren bilgiler şeklinde anlamlandırılmıştır.[108]

Söz konusu verilerin sağlık verisine nazaran kendilerini eşsiz yapan bazı özelliklere sahip oldukları görülmektedir. Ayrıca genetik veriler şu an -veya muhtemelen gelecekte- kişinin tüm hayatını ilgilendiren bilimsel, tıbbi ve kişisel bilgiler içermektedir. Kendine özgü bu özelliklerinden dolayı da genetik veri özel bir yasal korumayı beraberinde gerektirmektedir.[109]

---

binlerce kelimeye eşdeğerdir. Bkz. House of Lords Opinions of The Lords of Appeal For Judgment in the Cause Campbell (Appellant) v. MGN Limited (Respondents) [2004] UKHL 22 para31

[104] Yanna Welinder, Harvard Journal of Law & Technology Volume 26, Number 1 Fall 2012, **A Face Tells More Than A Thousand Posts: Developing Face Recoinition Privacy In Social Networks**, s.167

[105] Bu noktada Çin'in 2020'de uygulamasına başladığı "Vatandaşa Not" sistemi dikkat çekicidir. Çin hükümetinin projesine göre 2020 yılından sonra akıllı telefonlar aracılığıyla vatandaşların kişisel verilerinin toplanması ve vatandaşlara not verilmesi planlanmaktadır. Örneğin kredi borcunu ödeyemeyen vatandaşa düşük not verilip bir daha kredi alamama veya bir yere seyahat edememe cezası verilecek ve veri toplama konusunda ise bankalar, sohbet uygulamaları ve online satış siteleri de hükümete bu doğrultuda yardımcı olacaktır. Ayrıca şu an vatandaşların izlenmesinde kullanılan 170 milyonun üzerinde kamera ve yüz tanıma sistemlerinin de veri toplama konusunda yardımcı olması hedeflenmektedir. Bkz. https://www.dw.com/tr/%C3%A7in-vatanda%C5%9Fa-not-sistemine-ge%C3%A7iyor/av-43809155 (10.10.2020 tarihinde erişildi.)

[106] Aydın Akgül, **Kişisel Verilerin Korunması Bağlamında Biyometrik Yöntemlerin Kullanımı ve Danıştay Yaklaşımı**, TBB Dergisi 2015 (118), s.212

[107] GDPR, Recital para.34

[108] Article 2 of Law of 2 August 2002 on the Protection of Persons with regard to the Processing of Personal Data

[109] Article 29 Data Protection Working Party, **Working Document on Genetic Data**, Adopted on 17 March 2004 s.4

Genetik verilerden günümüzde karşımıza sıkça çıkanlar özellikle DNA ve hücre örnekleridir. Kanada Yüksek Mahkemesi'nin bir kararında kişinin DNA bilgisinden, insana ait en üst düzey kişisel ve özel bilgiyi içerdiği noktasında şüphe olmayan bir veri çeşidi şeklinde bahsedilmiştir.[110] AİHM ise hücre örneklerinin, kişinin sağlığıyla da ilgisi olan hassas bilgi içermesinin yanı sıra bireyin kendisine ve yakınlarına ait münhasır genetik kodlar barındırdığını ifade etmiştir.[111]

Genetik veriler, kişiye özgü çok hassas bilgiler içerdiğinden kişinin hangi ırktan geldiğinin tespiti gibi farklı bilimsel çalışmalara da konu olmaktadır.[112] Ancak ırkla olan bu ilişkisi soncunda genetik verilere bazı insanlar tarafından çekinceyle yaklaşılmaktadır. Örneğin Amerika Birleşik Devletleri'nde -kendi sağlığı açısından zorunlu olmasına rağmen- elde edilecek sonuçların işverenleri yahut sigorta şirketleri tarafından bilinmesinden korkan ve genetik teste girmeyen insanlara ilişkin birçok hadise vuku bulmuştur.[113]

3. Kişisel Verilerin İşlenmesi

6698 sayılı Kişisel Verilerin Korunması Yasası'nın Tanımlar başlıklı 3. maddesinde kişisel verilerin işlenmesi kavramı *"Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem"* olarak tanımlanmıştır. Görülmektedir ki bu tanımlama, işleme kavramıyla ilgili olarak oldukça geniş bir yorumlamayı beraberinde getirecektir. Söz konusu durum madde gerekçesinde *"Kişisel verilerin işlenmesi kavramı geniş bir alanı kapsamaktadır. Buna göre kişisel verilerin işlenmesi, verilerin ilk defa elde edilmesinden başlayarak veriler üzerinde gerçekleştirilen tüm işlem türlerini ifade etmektedir."* şeklinde ifade edilmiştir. Kişisel Verileri Koruma Kurumunca yapılan tanımlamada ise kişisel verilerin işlenmesi kavramı, verilerin toplanmasından

[110] Canada Supreme Court, R. V.S.A.B, 2003 SCC 60, 31.10.2003

[111] Case of S. And Marper V. The United Kıngdom, (Applications no. 30562/04 and 30566/04) para.72. Ayrıca Mahkeme bu davada hücre ve DNA örneklerini parmak iziyle karşılaştırması sonucu hücre ve DNA örneklerinin içerdiği bilgilerden ötürü parmak izine nazaran saklanmasında daha büyük bir etki görüleceği sonucuna varmıştır.

[112] Sandra Soo-Jin Lee, Joanna Mountain, Barbara A. Koenig, Volume 1 Issue 1 Yale Journal of Health Policy, Law, and Ethics Article 3 2001, **The Meanings of "Race" in the New Genomics: Implications for Health Disparities Research**

[113] Article 29 Data Protection Working Party, **Working Document on Genetic Data**, Adopted on 17 March 2004 s.2

silinmeleri, yok edilmeleri veya anonim hale getirilmelerine kadarki süreçte muhatap oldukları her türlü faaliyet şeklinde tarif edilmiştir.[114]

Kanundaki işleme eyleminin düzenlenme şekli dikkate alındığında kişisel verileri ilgilendiren her işlemin kişisel verilerin işlenmesi olarak kabul edilerek KVKK kapsamında kabul edileceği söylenebilecektir. Zira maddede sayılan işlemler tahdidi değil; tadadi bir biçimde sayılarak yasada yerini almıştır. [115]

Kişisel verilerin işlenmesi ile ilgili olarak karşımıza çıkan fiillerin işleme kapsamında olup olmadığını belirlemek için öncelikle bu işlemin otomatik olarak icra edilip edilmediğine bakılmalıdır. Nitekim yasa otomatik yollarla işlemeyi otomatik olmayan yollarla işlemeden ayırmıştır.

Öncelikle otomatik yollarla yapılan veri işleme faaliyetlerinin hepsinin kişisel verilerin işlenmesi olarak kabul edileceği ve 6698 sayılı Yasa'nın uygulama alanında olacağını belirtmemiz gerekir. Bununla birlikte otomatiklik kavramı yasada tanımlanmamıştır. Aslında bu kavram ile anlatılmak istenen teknik destek aracılığıyla verilerin işleme faaliyetine konu olmasıdır.[116] Kişisel Verileri Koruma Kurumu ise otomatiklik kavramını OECD'nin *"İnsan müdahalesi ya da yardımı konusundaki ihtiyacı asgari seviyeye indiren, kendi aralarında bağlantılı ve etkileşimli elektrikli veya elektronik bir sistem tarafından gerçekleştirilen veri işleme faaliyeti"* şeklinde yaptığı tanımlamaya atıfta bulunarak bilgisayar ve telefon gibi işlemcisi olan cihazların yazılım veya donanım özellikleri vasıtasıyla önceden hazırlanan algoritmalar da kullanılarak insan müdahalesi olmadan ve yine bu cihazlarla yapılan işleme faaliyeti olarak tanımlamıştır.[117]

Otomatik olmayan yöntemlerle yapılan işleme faaliyeti açısından ise bu faaliyetin kanun kapsamında değerlendirilebilmesi için söz konusu verilerin, veri kayıt sisteminin bir parçası olması şartı öngörülmüştür. Buna göre veri kayıt sistemi, kişisel verilerin belirli kriterlerle yapılandırılmak suretiyle işlendiği sistemi ifade etmekle birlikte bu sistem elektronik ya da fiziki (örneğin kağıt üzerinde yer alma gibi[118]) ortamda oluşturulabilecektir. Örneğin kişisel veriler ad, soyad, kimlik numarası gibi kriterlerle sınıflandırılabileceği gibi kredi borcunu ödememiş kişiler şeklindeki bir sınıflandırma sonucunda da veri kayıt sisteminden söz

[114] Kişisel Verileri Koruma Kurumu, **6698 Sayılı Kanun'da Yer Alan Temel Kavramlar**, s.11
[115] Elif Küzeci, **Kişisel Verilerin Korunması**, 3. Bası, Ankara 2019, s.323
[116] Küzeci, *Kişisel Verilerin Korunması*, s.323
[117] Kişisel Verileri Koruma Kurumu, **6698 Sayılı Kanun'da Yer Alan Temel Kavramlar**, s.13-14
[118] **Handbook on European data protection law,** 2018 Edition, Publications Office of the European Union, s.47-48

edilebilecektir.[119] Aynı şekilde kişilerin isim ve soyisimleri de belirli kriterlere göre bir kağıda yazılırsa bu durumda da KVKK kapsamında değerlendirilen bir kayıt faaliyeti meydana gelecektir.[120] İşte böyle bir sistemin söz konusu olduğu durumda yapılan otomatik olmayan yöntemlerle işleme faaliyeti de KVKK kapsamında kişisel veri işlenmesi olarak sayılacaktır.

Çalışmamızın konusu açısından şu noktaya değinmekte fayda görüyoruz: Kişisel verilerin işlenmesi tanımının kapsamında değerlendirilmeyen yani otomatik yolların bulunmadığı ve bir veri kayıt sistemi ile de bağı bulunmayan verilerin işleme tabi tutulması durumunda işleme konu olan veriler, kişisel veri niteliğini taşımakta ise TCK'de yer alan ve kişisel verileri konu edinen suç tipleri bağlamında cezai sorumluluk veyahut özel hukuk bağlamında tazminat sorumluluğu doğabilecektir. Ayrıca belirtilmelidir ki yine bu veriler, eğer ileride bir veri kayıt sistemine dahil edilirler ise KVKK kapsamına girmiş olacaklardır.[121]

Kişisel verilerin işlenmesi fiilinin daha iyi anlaşılabilmesi ve kavramın daha somut hale gelmesi için çeşitli örneklere değinmek yararlı olacaktır. Bu anlamda, işverenin, çalışanına dair maaş bilgilerini de içeren bilgileri tutması ve bunu yetkili resmi kurumlara iletmesi[122], kişisel verilerin silinmesi veya imha edilmesi[123], CD veya hard diske kaydedilmesi[124], reklam sms'i gönderimi, kişinin fotoğrafının websitesine konması, e-mail gönderimi, IP ve MAC adreslerinin depolanması, CCTV kayıtlarının tutulması[125], önlü arkalı kimlik fotokopisinin hizmet sunan şirket tarafından alınması[126], güvenlik kameralarının görüntü kaydetmesi[127], internet sitelerinin çerezleri(cookie) işlemesi[128], GPS yoluyla kişinin izlenmesi[129], sosyal medya kullanıcılarının reklam amacıyla kişisel yönlerinin değerlendirilmesi ve onlar hakkında tahminler yapılmasını içeren profil çıkarma işlemi[130], kişilerin vergilendirilebilir gelirlerinin gazetede yayınlanması[131], kişinin siyasi görüşüne ulaşılmasını sağlayan ve bir etkinliğe, greve vb., katıldığını gösteren

[119] Kişisel Verileri Koruma Kurumu, **6698 Sayılı Kanun'da Yer Alan Temel Kavramlar**, s.15
[120] **100 Soruda Kişisel Verilerin Korunması Kanunu**, KVKK Yayınları, Nisan 2018, Ankara, s.25
[121] Dülger, *Kişisel Verilerin Korunması Hukuku*, s.175-176
[122] Handbook on European data protection law 2018 Edition, Publications Office of the European Union, s.48-49
[123] 108 Sayılı Sözleşme m.2
[124] **100 Soruda Kişisel Verilerin Korunması Kanunu**, KVKK Yayınları, Nisan 2018, Ankara, s.22
[125] https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-constitutes-data-processing_en
[126] Kişisel Verileri Koruma Kurulu, 01.10.2019 tarih ve 2019/294 sayılı karar özeti
[127] AİHM, C-212/13, Rynes V. Úřad Pro Ochranu Osobnıch Údajů, 11.12.2014("RYNES")
[128] Case 15/57/C, Belgian Commission for the Protection of Privacy v. Facebook Inc., Facebook Belgium SPRL and Facebook Ireland Limited
[129] AİHM, Case of Uzun V. Germany, (Application no. 35623/05), 2 September 2010
[130] European Data Protection Board, **Guidelines 8/2020 on the targeting of social media users,** Version 1.0 Adopted on 2 September 2020, para. 77
[131] AİHM, Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland, para.138

görüntülerin kaydı, havalimanlarında yolcular için öngörülen yüz tanıma sistemlerinin kullanılması[132] gibi durumlar kişisel verilerin işlendiği sayısız durumdan sadece birkaçıdır.

4. Kişisel Verilerin Korunması Hakkı

Kişisel verilerin korunması hakkı, son yıllarda sıklıkla gündeme gelmekte ve teknolojinin gelişmesi ile birlikte kişisel verilerin kullanımının artması sonucu yaşanılan hak ihlallerine karşı koruyucu bir kalkan olarak kabul görmektedir. Artık literatürde ve yargı kararlarında kendisine açıkça yer bulan bu hak, bireyin kendisini güvende hissetmesini sağlamakla birlikte ayrıca kişiliğini geliştirmesinde ona yardımcı olmaktadır. Zira sahip olduğu verileri başkası tarafından saklanan, aktarılan veya işlenen kişi, her an izlendiği kanısına varacak ve bundan dolayı davranışlarını özgürce sergileyebilmesinin önüne bir set çekilmiş olacaktır. İşte kişisel verilerin korunması hakkı tam bu noktada devreye girerek özel hayat açısından bir kaygı duyulmasının önüne geçecektir.

Kişisel verilerin korunması hakkı ile ilgili olarak hukuki nitelendirme açısından farklı görüşler dile getirilmektedir. Meydana gelen söz konusu yorum farklılıkları sonucunda temelde iki ana yaklaşım dikkat çekmektedir. Bunlardan birincisi kişisel verilerin korunması hakkını ekonomik hak olarak görürken diğeri ise bahse konu hakkı, doğuştan gelen bir hak olarak kabul etmektedir. İlk yoruma göre veriler, üzerinde çeşitli işlemler yapılabilen bir mal olarak kabul edilirken diğer bakış açısına göre kişisel veriler, doğuştan bahşedilmiş bir hakkın konusu olarak ele alınmaktadır. Amerika Birleşik Devletleri'nde ilk görüş ağırlıklı olarak kabul edilirken diğer yaklaşım Kıta Avrupası'nda benimsenmektedir.[133]

4.1. Ekonomik Hak Görüşü

Ekonomik hak görüşüne göre kişisel verilerden sahibi olan kişi ekonomik olarak yararlanabilmelidir. Aslında bu türden bir yaklaşım kişisel verilerin korunması hakkının insan hakları bağlamından ayrılmasına neden olmaktadır. Bu görüş daha çok Amerika Birleşik Devletleri gibi veri güvenliğinin çok yüksek olmadığı ülkelerde kabul edilmektedir. Ekonomik hakkın bir alt başlığı ise mülkiyet hakkı ve fikri mülkiyet hakkı olarak ikiye ayrılmaktadır.[134]

---

[132] EDPB, **Guidelines 3/2019 on processing of personal data through video devices**, Version 2.0Adopted on 29 January 2020, s.17-18

[133] Küzeci, *Kişisel Verilerin Korunması*, s.59

[134] Sinem Göçmen Uyarer, **Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması**, Seçkin Yayınları, Ankara 2019, s.23; Amerika Birleşik Devletleri'nde bilgi gizliliği ile ilgili olarak sektörel yaklaşım tercih edilmektedir. Bu anlayışa göre veri toplama faaliyetleri olabildiğince iş hayatıyla uyumlu olarak yürütülmek istenmekte, gizliliğe ilişkin regülasyonların belirli durumlarla sınırlı kalmak kaydıyla

4.1.1. Mülkiyet Hakkı Görüşü

Kişisel veri, modern ekonomi düzeninde çatışma içerisindeki menfaatlere konu olmaktadır. Bu anlamda kişisel veri, bilgi endüstrisi için soyut bir ürün çeşidi iken bireyler için de kişisel bir malvarlığı değeri olarak nitelendirilmektedir. Ayrıca belirtmek gerekirse kişisel veri sadece insanın kişiliğine ait bir değer olarak görülmemekte ve bununla birlikte veri odaklı ekonominin önemli bir unsuru olmasının yanı sıra tüketici gücünün pazarda yer alan önemli bir aracı olarak kabul görmektedir.[135] Özellikle kişisel veri işleyen şirketler, bu verileri malvarlığı değeri gibi görmekle birlikte müşterilerinden topladıkları bu bilgileri bir araya getirip başka şirketlere satmaktadırlar.[136] Nitekim Amerikan mahkemelerinin uygulamasında da verinin malvarlığına ilişkin olduğuna dair kararlara rastlanılmaktadır. Örneğin müşteri tarafından havayolu şirketine verilen bilginin şirket tarafından depolanıp diğer bilgilerle ilişkilendirilmesine konu bir kararda söz konusu müşteri bilgilerinin artık şirketin malvarlığına dahil olduğu ifade edilmiştir.[137]

Mülkiyet hakkı yaklaşımına göre kişisel bilgi, değer biçilebilen ve serbest pazarda değiş tokuşa konu olabilen bir mal/ürün olarak kabul görmektedir. Kişisel bilgi bir kez üretildi mi artık fiyatının belirlenmesi ve tüketimi arz-talep kurallarına göre belirlenmelidir. Bu noktada artık mahremiyeti ilgilendiren genel geçer ve zor sorunlarla ilgili sorumluluk, kişiler tarafından verilen bireysel kararlara yüklenmiş olmaktadır. Böylece bireyler, siber alemde işlem yaptıkları karşılarındaki muhatapları ile kişisel bilgilerin nasıl işleneceği noktasında devletin önemli bir müdahalesi olmadan anlaşabileceklerdir.[138] Burada ana dayanak noktasını kişinin, kendisi hakkındaki bilgiye mal sahibi gibi sahip olabilmesi ve bu bilgiyle ne yapılacağı konusunda yetkili kılınması oluşturmaktadır.[139] Kişinin mevcut bilgi üzerinde belirttiğimiz şekildeki kontrol yetkisi onun söz konusu veri üzerinde sahip olduğu bir çeşit mülkiyet hakkı olarak yorumlanmaktadır. Zira bir şeyin üzerinde kontrol yetkisine sahip olmak birtakım yasal hakları (örneğin zilyetlik, devir ve ferağ yetkisi, ticari anlamda yararlanma, başkalarının müdahalesini

---

yapılması öngörülerek idarenin müdahalesini minimuma indrimek ve bu suretle şirketlerin üzerindeki yükün azaltılması hedeflenmektedir. Bkz. Burk, Dan L., **Privacy and Property in the Global Datasphere** (April 28, 2005). Minnesota Legal Studies Research Paper No. 05-17, s.4-5

[135] Malgieri, Gianclaudio, **Property and (Intellectual) Ownership of Consumers' Information: A New Taxonomy for Personal Data** (April 20, 2016). Privacy in Germany - PinG, n. 4, 2016, 133 ff., s.2

[136] Jacob M. Vİctor, The Yale Law Journal, **The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy**, 123:513 2013, s.517

[137] In Re Northwest Airlines Privacy Litigation, United States District Court D.Minnesota, 6 June 2004, 2004 WL 1278459

[138] Jerry Kang, **Information Privacy in Cyberspace Transactions**, Stanford Law Review [Vol. 50:1193, s.1246-1248

[139] Jessica Litman, Information Privacy/Information Property, Stanford Law Review [Vol. 52:1283, s.1287

engelleme gibi) da beraberinde getirmektedir.[140] Bunun sonucunda ise mülkiyet hakkını temel alan bir yaklaşımın ilgili kişiye daha çok denetim yapabilme imkanı sağlayacağı ve malike tanınan geniş yasal korumalardan yararlanabileceği öngörülmektedir. Ayrıca bu görüşe göre şirketlerin kişisel verilerin toplanması ve işlenmesi sürecinde meydana gelen maliyetleri dikkate alacak olması da kişisel verilerin korunması noktasında olumlu bir yön olarak kabul edilmektedir.[141] Bununla birlikte verinin el değiştiren mal haline getirilmesi, veri ticaretinin artmasını sağlayarak mahremiyete yönelik tehditleri de beraberinde getirebilecektir.[142]

4.1.2. Fikri Mülkiyet Hakkı Görüşü

Fikri mülkiyet, genellikle zihinsel bir sürecin ürünü olan ve sahip olduğu değer bazı fikir ya da fikirlere dayanan soyut bir malvarlığı unsuru olarak nitelendirilmektedir.[143] Söz konusu hak, Anglo-Amerikan sistemlerinde eser sahibinin doğal hakkı olarak görülmeyip faydacılık/yararcılık anlayışında temellendirilmiştir.[144]

Fikri mülkiyet hakkı görüşüne göre bu hak ile kişisel verilerin korunması hakkı arasında benzerlik kurulmakta ve söz konusu kişisel veriler telif hakkına benzer bir anlayışla korunmaktadır.[145] Bu görüşün dayanak noktası ise eser sahibi olma durumunda görüldüğü gibi hakkın konusunun -mevcut durumda kişisel verilerin- sözleşmeyle kullanım haklarının devredilmesi düşüncesidir.[146] Ayrıca yine bu görüşe göre eser sahibi, düşünce ürünü, kitap, resim gibi ortaya koyduğu eserler üzerinde fikri mülkiyet hakkı kapsamında manevi haklara sahip olduğu gibi ilgili kişi de verileri üzerinde bu türden bir hakka sahiptir.[147]

Kişisel verilerin korunmasının fikri mülkiyet ile bağdaştırılması noktasında hem olumlu hem de olumsuz görüşler dile getirilmiştir. Bu bağlamda fikri mülkiyet hakkı veri sahibine tanınacak olursa örneğin, kişisel verileri başkaları tarafından işlenen/ yanlış işlenen kişinin kendi verilerini kontrol etmesi kabul edilecek ve o kişinin saygınlığı korunmuş olacaktır. Buna ek olarak belirtmek gerekir ki, kişisel veri maddi bir değere sahip olduğundan (özellikle veri depolayanlar, veri ticareti yapanlar için) veriyi elinde bulunduran kişinin, veri öznesi olmadan

---

[140] Daniel J. Solove, **Privacy and Power: Computer Databases and Metaphors for Information Privacy**, Stanford Law Review [Vol. 53:1393, s.1446

[141] Küzeci, *Kişisel Verilerin Korunması*, s.60

[142] Paul M. Schwartz, **Property, Privacy, And Personal Data**, Harvard Law Review [Vol. 117:2055, s.2072

[143]Adam D. Moore, **Intellectual Property and Information Control: Philosophic Foundations and Contemporary Issues**, April 2004, s.32

[144] Adam D. Moore, **Privacy, Intellectual Property, and Hacking: Evaluating Free Access Arguments**, s.8

[145] Küzeci, *Kişisel Verilerin Korunması*, s.62

[146] Uyarer, *Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması*, s.27-28

[147] Dülger, *Kişisel Verilerin Korunması Hukuku*, s.79

haksız bir şekilde bu verilerden maddi menfaat sağlaması adaletsiz bir sonuç olacaktır. Öte yandan fikri mülkiyet hakkının tanınmaması gerektiğini savunanlara göre ise, kişisel verilerin fikri mülkiyet hakkı kapsamında korunması, bireyin kişiliğinin metalaştırılması anlamına gelecek olup bu sonuç insafsız bir yaklaşım anlamına gelecektir. İnsan hakları savunucularına göre bu şekildeki bir yaklaşım insana sadece bir malvarlığı değeri ya da malvarlığı değerini üreten bir yapı olarak bakılmasına yol açacaktır. Ayrıca bilgiyi (kişisel veriler de bu kapsamda olmak üzere) depolama ve iletme haklarını da içeren ifade özgürlüğü, kişisel verinin fikri mülkiyete dahil bir değer olarak tanınmasıyla kısıtlanabilecektir. Son olarak bu fikri savunanlara göre fikri mülkiyetin kabulü toplumu, önemli bilgileri özellikle siyasi veya ekonomik açıdan güçlü insanlara dair kişisel bilgileri dile getirmekten alıkoyacaktır.[148]

4.2. Özel Hayatın Gizliliği Görüşü

Kişisel verilerin korunması hakkı en başta özel hayatın gizliliği başlığı altında incelenen temel hak ve hürriyetlerdendir.[149] Zira kişisel verilerin korunmasının temelinde kişiliğin korunması vardır. Bu kapsamda kişisel verilerin korunması hakkı, özel hayatın gizliliği kavramının değişik bir formu olarak karşımıza çıkmaktadır.[150] Kavramın oldukça geniş bir alana yayılması nedeniyle özel hayatın gizliliği ile ilgili sadece çalışmamızı ilgilendiren noktalara değinmeyi yararlı görüyoruz.

Kişinin farklı hayat alanları olmakla birlikte bu alanlar kamuya açık alan, özel alan ve gizlilik alanı olarak üçe ayrılmaktadır. Kamuya açık alan, bireyin kendisinin haricinde diğer kişiler tarafından da bilinen konulardan oluşmakta iken, özel alan, kişinin belirli kişilere açtığı, sınırlı sayıda kişi tarafından bilinmesini istediği alandır. Son olarak gizli alan ise üçüncü kişilerin giremediği ve kişinin kendisine has mahrem alanıdır. Belirtilen üç hayat alanından özel ve gizli alan kişilik hakkı kapsamında korunmakla birlikte bu iki alana yapılacak müdahaleler kişilik hakkına halel getirecektir.[151] Bununla birlikte hayat alanının en dış çemberini oluşturan genel

[148] Dorrothy J. Glancy, **Personal Information as Intellectual Property**, s.2

[149] Bu konuda görüş birliği yoktur. Avrupa merkezli yaklaşım kişisel verilerin korunması hakkını insan hakları bağlamında incelerken ABD'de söz konusu hakka, ekonomik bir hak olarak yaklaşılmaktadır.; Ayrıca bkz. Hüseyin Murat Develioğlu, **6698 Sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku**, s.13. Avrupa Hukuku'nda kişisel verilerin korunması hakkının, genel olarak bir insan hakkı olan özel yaşamın gizliliği kapsamında ele alındığı ifade edilmelidir.

[150] **100 Soruda Kişisel Verilerin Korunması Kanunu**, KVKK Yayınları, Nisan 2018, Ankara

[151] Dural/Öğüz, s.135-138

hayat alanı kısmında da kişisel veriler hukuki korumadan yoksun değildir. Kişisel verilerin korunmasında uyulması gereken temel ilkeler bu alanda da geçerliliğini sürdürmektedir.[152]

Kişisel verilerin korunması hakkı, bireyin demokratik hukuk devletinde özgür iradesini kullanıp kendi yaşamını bizzat düzenleyebilmesinin bir gereği olarak karşımıza çıkmaktadır. Bunun sonucunda birey, yaşamını özgür ve onurlu bir şekilde kendisini baskı altında hissetmeden sürdürebilecektir.[153] Zira sürekli izlenerek yaşamına ilişkin bilgileri kaydedilen ve bütün bunların sonucunda adeta şeffaflaşan bireyin kişiliğini geliştirebilmesi pek mümkün gözükmemektedir.[154] Bundan dolayıdır ki kişisel verilerin korunması hakkı bireyin hızla gelişen teknoloji karşısında korumasız kalmasını önleyerek onun rahat bir şekilde yaşam sürdürmesine yardımcı olur.

Yukarıda belirttiğimiz gibi kişisel verilerin korunması hakkı, günümüzde halen özel hayatın gizliliği başlığı altında değerlendirilmektedir. Ancak teknolojide meydana gelen gelişmeler doğrultusunda bu hakkın artık özel hayatın gizliliği kavramından ayrı olarak ele alınmaya başlandığını belirtmekte fayda vardır. Nitekim bugün Avrupa ülkeleri başta olmak üzere ülkemizde de kişisel verilerin korunması hakkı bu hakka özgü olarak çıkarılan kanunlarla korunmaya çalışılmaktadır. Mevcut yaklaşımlar da göstermektedir ki kişisel verilerin korunması hakkı artık münhasıran bir hak olarak kabul edilmeye başlanmıştır. [155]

Son olarak eklemek gerekirse insanın bir meta şeklinde görülmesini engellemek ve ona hak ettiği saygınlığın gösterilmesini sağlamak amacıyla kişisel verilerin korunması hakkının, yasalar başta olmak üzere çeşitli düzenlemeler hayata geçirilerek korunması gerekmektedir. Zira bilişim sistemlerinde meydana gelen gelişmeler her geçen gün kişisel veri dolaşımını artırmaktadır. Özellikle istihbari bilgi temini, ulusal güvenlik kaygısı gibi nedenlerle devletlerin vatandaşı olan veya olmayan insanların (9/11 saldırılarından sonra giderek artacak şekilde) kişisel verilerini toplamaya çalışması insan hakları bakımından son derece kaygı vericidir.[156] Ayrıca elde edilen verilerin amaçlarına uygun kullanılıp kullanılmadığı da ayrı bir tartışma konusudur. Bu noktada

---

[152] Küzeci, *Kişisel Verilerin Korunması*, s.70

[153] Aydın Akgül, **Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması**, Beta Yayınları, İstanbul 2014, s.45

[154] Küzeci, *Kişisel Verilerin Korunması*, s.67

[155] Uyarer, *Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması*, s.32; Kişisel verilerin korunması hakkının bağımsız bir hak olarak kabul edilmesinin isabetli olmadığı zira anılan hakkın kimi zaman kişilik hakkı kapsamında bir değere dönüşürken kimi zaman da ekonomik değere sahip bir kavrama dönüşeceği hakkında bkz. Sinan Sami Akkurt **Kişisel Veri Kavramının Hukuki Niteliğine İlişkin Yaklaşımlara Mukayeseli Bir Bakış**, Kişisel Verileri Koruma Dergisi, Cilt: 2, Sayı: 1, s.29

[156] Sosyal medya sitelerinin de istihbarat örgütleriyle kişisel veri toplama konusunda ilişkileri olduğu son zamanlarda sıkça tartışılmaktadır. Bkz. https://www.cbsnews.com/news/social-media-is-a-tool-of-the-cia-seriously/ (31.12.2020 tarihinde erişildi.); Çin'in 2020'de uygulamasına başladığı "Vatandaşa Not" sistemi ile ilgili bkz. dn.105

Benjamin Franklin'in bir sözüne atıfta bulunarak kişisel verilerin korunması hakkı ile ilgili açıklamalarımıza son vermek istiyoruz: *"Temel bir özgürlüğü, geçici güvenlik için terk edenler, ne özgürlük ne de güvenliği kazanacaklardır."*

5. Türk Hukukunda Kişisel Veriler

5.1. Anayasa

Teknolojinin getirdiği imkanların çeşitliliği, temel hak ve hürriyetlere yapılabilecek müdahaleleri kolaylaştırmış ve bunun sonucunda da yasa koyucular meydana gelen hukuki sorunların çözüme kavuşturulması için çeşitli düzenlemeler yapmak zorunda kalmıştır. Ülkemizde kişisel verilerle ilgili olarak ilk defa 1989 yılında özel bir kanun ihdası amacıyla komisyon kurulmuş ancak komisyon çalışmalarını tamamlayamadan dağılmıştır. Ardından çeşitli tarihlerde başlatılan yeni kanun çıkarma girişimleri de sonuçsuz kalmış ve nihayet 2010 yılında Anayasamızda değişiklik yapılmıştır. 1982 Anayasası'nın "Özel hayatın gizliliği" başlıklı yirminci maddesine 2010'da eklenen üçüncü fıkrada herkesin kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahip olduğu ve bu hakkın kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsayacağı belirtilmiştir. Ayrıca kişisel verilerin ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebileceği ve kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği hüküm altına alınmıştır. Söz konusu hükme göre bireyler kişisel verilerinin üçüncü kişilerin eline geçmemesi için gerekli tedbirlerin alınmasını isteyebilecek, kişisel verilerinin amacına uygun olarak işlenip işlenmediğini öğrenebilecek ve ilgili kişisel verilerinde bir yanlışlık olması durumunda düzeltme veya silinme talebinde bulunabilecektir.[157] Böylece kişisel verilerin korunması hakkı açıkça anayasal bir temele oturtularak[158] temel hak ve

[157] Kişisel Verileri Koruma Kurumu, **Anayasal Bir Hak Olarak Kişisel Verilerin Korunmasını İsteme Hakkı**, s.4-6; Değişiklik gerekçesinde, Anayasada kişisel verilerin korunmasına yönelik dolaylı hükümlerin bulunduğu ancak bu hükümlerin yeterli olmadığı mukayeseli hukukta ve tarafı olduğumuz uluslararası belgelerde de kişisel verilerin korunmasının önemle vurgulandığı, söz konusu maddeyle, herkesin, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkının anayasal bir hak olarak teminat altına alındığı belirtilmiştir. Bkz. **11/1982 Tarihli ve 2709 Sayılı Türkiye Cumhuriyeti Anayasasının Bazı Maddelerinde Değişiklik Yapılması Hakkında Kanun Teklifi ve Anayasa Komisyonu Raporu (2/656)**

[158] Yeşim ÇELİK, **Özel Hayatın Gizliliğinin Yansıması Olarak Kişisel Verilerin Korunması ve Bu Bağlamda Unutulma Hakkı**, TAAD, Yıl:8, Sayı:32 (Ekim 2017), s.407

hürriyetler arasında kendisine yer bulmuş ve içinde bulunduğumuz bilgi çağı açısından önemli bir adım atılmıştır.[159]

Söz konusu hükümde hakkın kapsamı, kişisel verilerin işlenebilme şartları belirtilmiş ve bu alandaki ayrıntılı düzenlemenin yasayla yapılacağı ifade edilmiştir. Böylece teknolojinin hızla gelişmesi ve hayatımızın her alanına egemen olmasına kanun koyucu kayıtsız kalmamış ve normlar hiyerarşisinin en tepesinde yer alan anayasada değişiklik yapmak suretiyle kişisel verilerin korunması hakkını anayasal bir dayanağa kavuşturmuştur.

Unutmamak gerekir ki Anayasamızın bireyin maddi ve manevi varlığını serbestçe geliştirme hakkı (m.17), hukuk devleti ilkesi (m.2), dini ve vicdani kanaatleri açıklamaya zorlanamama (m.24), konut dokunulmazlığı (m.21),özel hayatın gizliliği hakkı (m.20), düşünce ve kanaatleri açıklamaya zorlanamama (m.25), haberleşmenin gizliliği (m.22) başlıklı maddeleri, kişisel verilerin korunması hakkının yukarıda değindiğimiz 2010 değişikliğinden önceki anayasal dayanağını oluşturan maddeleri arasında yer almıştır.[160]

5.2. Türk Borçlar ve Türk Medeni Kanunu

6698 sayılı Kişisel Verilerin Korunması Yasası'nda kişisel verinin ilgili kişisinin hakkını arama yöntemlerine değinilmiş ve son olarak ise "Kurula Şikayet" başlıklı 14. maddenin son fıkrasında *"Kişilik hakları ihlal edilenlerin, genel hükümlere göre tazminat hakkı saklıdır."* hükmü düzenlenmiştir. Maddenin gerekçesinde de bu husus *"Veri sorumlusunun hukuki statüsüne göre ilgililer adli ya da idari yargıda dava açabileceklerdir."* şeklinde ifade edilmiştir.

Yukarıda değindiğimiz 14. maddedeki genel hükümler ile ifade edilen Türk Medeni Kanunu'nun kişilik haklarına saldırı ile ilgili hükümlerinin yanı sıra Türk Borçlar Kanunu'nun haksız fiil ile ilgili tazminat hükümleridir. Söz konusu kurallar uyarınca veri öznesi olan kişi maddi zararının yanı sıra manevi zararının giderilmesini de isteyebilecektir. Bu noktada KVKK'de sorumluluk ile ilgili ayrıca özel bir düzenleme bulunmamasının bir sonucu olarak kusur sorumluluğu ilkesi ile yetinilmesi gerektiğini belirtelim.[161]

---

[159] Doğan Kılınç, **Anayasal Bir Hak Olarak Kişisel Verilerin Korunması**, AÜHFD, 61 (3) 2012:1089-1169, s.1161

[160] Kılınç, s.1131

[161] Damla GÜRPINAR, **Kişisel Verilerin Korunamamasından Doğan Hukuki Sorumluluk**, D.E.Ü. Hukuk Fakültesi Dergisi, Prof. Dr. Şeref ERTAŞ'a Armağan, C. 19, Özel Sayı-2017, s. 679-694, s.689-690.Somut olaya göre tehlike sorumluluğunun uygulanıp uygulanamayacağı hakkında bkz. Aynı eser; Maddede yer alan "genel hükümler" den TMK m.23 vd.'nın anlaşılması gerektiği hakkında bkz. Mehmet Oğuz Vuraloğlu, **Kişisel Verilerin İşlenmesi Suretiyle Kişilik Hakkı İhlâlinde Kazancın Devri Talebi**, YÜHFD Cilt: XV Sayı:1 (2018), s.186; Aynı yönde bkz. Yasemin Avcı, **Kişisel Verilerin Korunması** (Yüksek Lisans Tezi- Konya 2019) , s.96-111; Medeni

Kişisel verilerin işlenmesi ile ilgili TMK ve TBK'de sayılan hukuki korumalardan yararlanılabilmesi için hukuka aykırı bir fiil olması gerekmektedir. Örneğin açık rıza alınması gereken hallerde açık rıza alınmaması, aydınlatmanın yapılmaması veya açık rızanın sınırlarının aşılması gibi durumlarda sorumluluk doğmuş olacaktır. İlgili kişi böylesi hallerde TMK'nin 25. maddesinde sayılan önleme veya saldırıya son verme davasının yanı sıra tespit davası, vekâletsiz iş görmeye dayanan dava veya tazminat davaları açabileceği gibi Borçlar Kanunu'nunda öngörülen tazminat hükümlerine de başvurabilecektir.[162] Son olarak belirtelim ki Kişisel Verileri Koruma Kurumu, genel hükümlere göre tazminatın Kişisel Verileri Koruma Kurulundan değil veri sorumlularından talep edilebileceğini kabul etmektedir.[163]

5.3. İş Kanunu

İşçi-işveren ilişkisinde kişisel verilerin işlenmesine yönelik başlıca düzenlemeler Türk Borçlar Kanunu m.419 ve 4857 sayılı İş Kanunu'nun 75. maddesinde yer almaktadır.[164] İş Kanunu'ndaki düzenlemeye göre işveren her işçi için özlük dosyası düzenlemek ve saklamak yükümlülüğü altındadır. Özlük dosyası ise işçinin mesleki durumunu ilgilendiren ve işe başlama, çalışma, yükselme ve işveren-işçi ilişkisinin bitimine ilişkin olup iş ilişkisinin gerektirdiği belgelerin de yer aldığı dosya olarak tanımlanmaktadır.[165] Niteliği itibarıyla işçiye ait birçok kişisel veriyi barındıran özlük dosyaları, mahremiyet açısından önemli bir yere sahiptir. Bu nedenledir ki işverenlerin bu verilerin işlenmesi süreçlerinde son derece dikkatli olması gerekmektedir. Nitekim iş ilişkisi kapsamında işçiye ait kişisel verileri elinde bulunduran işverenin söz konusu verileri kullanabilme sınırı da Borçlar Kanunu'nun 419'uncu maddesinde

---

Kanun m.24-25 açısından sorumluluğun doğup doğmadığının tespitinde hukuka aykırılığı ortadan kaldıran nedenlere dikkat edilmelidir. Özellikle KVKK'de sayılan hukuka uygunluk sebepleri somut olayda hukuki sorumluluğun doğmasını önleyecektir. Bkz. Avcı, s.102 vd.

[162] Avcı, *Kişisel Verilerin Korunması*, s.104-126; Kişisel verilerinin hukuka aykırı olarak işlenmesinden ötürü mağdur olan kişinin kazancın devrini de talep edebileceği yönünde bkz. Vuraloğlu, *Kişisel Verilerin İşlenmesi Suretiyle Kişilik Hakkı İhlâlinde Kazancın Devri Talebi*, s.191

[163] **6698 Sayılı Kişisel Verilerin Korunması Kanunu Hakkında Doğru Bilinen Yanlışlar**, KVKK Yayınları No: 31 Nisan 2020, Ankara, s.52-53

[164] İş Kanunu'nun 75'inci maddesine göre işveren çalıştırdığı her işçi için bir özlük dosyası düzenlemek ve bu dosyada, işçinin kimlik bilgilerinin yanında, bu Kanun ve diğer kanunlar uyarınca düzenlemek zorunda olduğu her türlü belge ve kayıtları saklamak ve bunları istendiği zaman yetkili memur ve mercilere göstermek zorundadır.
Borçlar Kanunu'nun 419'uncu maddesine göre işveren, işçiye ait kişisel verileri, ancak işçinin işe yatkınlığıyla ilgili veya hizmet sözleşmesinin ifası için zorunlu olduğu ölçüde kullanabilecektir.

[165] Eser Şık, **İşverenin Özlük Dosyası Düzenleme Borcu**, Yüksek Lisans Tezi, İZMİR – 2012, s.16; Yeliz Polat, **4857 Sayılı İş Kanunu'na Göre İşçi Özlük Dosyası**, Yüksek Lisans Tezi, İstanbul, 2011, s.4; Doktrinde iş hukuku özelinde kişisel veri kavramının, bilgisayar ortamında veya özlük dosyalarında saklanan, işçinin özel ve mesleki yaşamını kapsayan, işçiyi doğrudan veya dolaylı ilgilendiren tüm bilgiler, işaretler veya notlardan oluştuğu ifade edilmiştir. Bkz. A. Eda Manav, **İş İlişkisinde İşçinin Kişisel Verilerinin Korunması**, Gazi Üniversitesi Hukuk Fakültesi Dergisi C. XIX, Y. 2015, Sayı: 2, s.99 dn.19

çizilmiştir. Söz konusu hükme göre elde edilen veriler işçinin işe yatkınlığıyla ilgili veya hizmet sözleşmesinin ifası için zorunlu olduğu ölçüde kullanabilecektir.

İş Hukuku ile kişisel verilerin korunması aslında yakından bağlantılı olan iki önemli alanı oluşturmaktadır. Bu sıkı ilişkinin yoğunluğu ise teknolojinin gelişimiyle birlikte sürekli olarak artış göstermektedir. Nitekim işverenlerin, iş yerinin nizamının sağlanması veya verilen işin sağlıklı bir şekilde yürütülmesi gibi gerekçelerle uygulamaya soktuğu yöntemlerin çoğu git gide kişisel verilerin işlenmesini konu alır hale gelmektedir.[166] Özellikle işçinin maillerinin denetlenmesi, giriş çıkışlarda parmak izi/göz izi okutulması ve yüz tanıma sistemleri gibi uygulamalar iş hukukundaki kişisel veri işleme alanlarının yelpazesini genişletmiştir. Taşıdığı önemden ötürü yüz tanıma teknolojisine bu noktada ayrı bir parantez açmakta fayda vardır. Şöyle ki yüz tanıma teknolojisi kişilerin kimliklerinin tespiti amacıyla kullanılan parmak izi, avuç içi damar tanıma sistemi, DNA dizilimi analizi ve göz tanıma sistemi gibi kimlik belirleme yöntemlerinden biridir.[167] Diğer sistemlerin aksine yüz tanıma teknolojisinin kişinin yaşı, ırkı, cinsiyeti, sosyal statüsü, dini gibi kişisel verilerini de içerebileceğine dikkat çekilmektedir.[168] Bunun sonucunda ise son derece hassas verilere ulaşmak kolaylaşmaktadır. İşyerlerinde kullanımı artmakta olan bu sistemlere ilişkin olarak veri güvenliği açısından gerekli önlemlerin alınması işçilerin özel hayatının, mahremiyetinin ve özellikle kişisel verilerinin korunması için son derece önemlidir.

Gelişen teknolojinin sağladığı imkanların artması işçilerin kişisel verilerinin hukuki korumadan yoksun kalma ihtimalini artırmakta ve tam bu noktada işverene önemli görevler düşmektedir. Çünkü işçilerin kişisel verileri, kişilik hakkı kapsamındadır ve bu veriler özel hayatın gizliliği içerisinde değerlendirilecektir. Aynı şekilde işçilerin, kendi verileri üzerinde korunma hakkı da bulunmaktadır.[169] Bu doğrultuda unutulmamalıdır ki işverence elde edilen işçilerin kişisel verileri ifşa edilmemeli ve işveren, söz konusu bilgilerin yetkisi olmayan 3. şahısların eline- kazayla dahi olsa- geçmesini önleme noktasında üzerine düşen sorumluluğu yerine getirmelidir. Son olarak işveren, kişisel verileri işlemekle görevli olan personelin gerekli eğitimi almasını, Veri Koruma Hukukunun kurallarından haberdar olmasını sağlamakla da yükümlüdür.[170]

Tüm bunlara ek olarak belirtmek gerekir ki işçi, iş ilişkisi kapsamındaki konumu itibarıyla işverene bağlıdır ve bu durum işverenlerin, kendi himayesinde çalışanların kişisel verilerini

[166] K. Ahmet Sevimli, **İşçinin Özel Yaşamına Müdahalenin Sınırları**, Doktora Tezi, s.140-141
[167] Sharon Nakar & Dov Greenbaum, **Now You See Me. Now You Still Do: Facial Recognition Technology And The Growing Lack Of Privacy**, Boston University Journal Of Science & Technology Law, s.94
[168] Nakar & Greenbaum, s.120
[169] Nuri Çelik/Nurşen Caniklioğlu/Talat Canbolat, **İş Hukuku Dersleri**, Beta Yayınları, Ekim 2017, s.333
[170] Sevimli, s.171

işleyebilmesi sonucunu doğurur. Nitekim işverenler, kendileri için öngörülen yasal sorumlulukları yerine getirmek, işe alımda yahut işçinin eğitiminde veya terfi almasında kullanmak, iş sağlığı ve güvenliğininin tesisi, iş yeri güvenliğinin sağlanması ve müşteri ilişkilerinin kontrol dilmesi gibi amaçlarla iş başvurusunda bulunan işçi adaylarının ya da hali hazırdaki çalışanlarına ait bilgileri işlemekte, diğer birtakım hallerde ise söz konusu verileri üçüncü kişilerle paylaşmaktadırlar.[171] Diğer taraftan iş ilişkisi kapsamında yönetim hakkının bir sonucu olarak da tanımlanabilecek "denetim ve gözetim" kavramları, sadece işverene tanınan bir hak olarak değil, aynı zamanda bir ödev olarak karşımıza çıkmaktadır.[172] Ancak işveren bu ödevi yerine getirirken işçinin kişisel verilerinin korunması hakkını ihlal etmemeli ve kişisel verilerinin işlenmesi konusunda işçinin açık rızasını almalıdır. Çünkü işçinin kişilik hakları, bu bağlılık ilişkisi içerisinde işverene verilmiş yönetim hakkının sınırını oluşturmaktadır.[173]

Son olarak eklemek gerekirse işçinin kişisel verilerinin işe alım süreci, iş sözleşmesi süresi ve işten ayrılmadan sonraki evrede işlenmesi nedeniyle işçi bu dönemlere ilişkin olarak kendi verilerinin korunması konusunda KVKK'nin tanıdığı haklardan yararlanabilecektir.

5.4. Türk Ceza Kanunu

5237 sayılı Türk Ceza Kanunu'nun Kişilere Karşı Suçlar başlıklı ikinci kısmının Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar başlıklı dokuzuncu bölümünde 135. maddede Kişisel verilerin kaydedilmesi, 136. maddede Verileri hukuka aykırı olarak verme veya ele geçirme ve 138. maddede Verileri yok etmeme suçlarına yer verilmiştir. Sayılan suçlar kişisel verileri doğrudan konu alırken diğer bazı suçlar ise kişisel verilerin korunmasını dolaylı yoldan sağlamaktadır. Dolaylı koruma sağlayan suç tiplerine örnek olarak ise 134. maddede yer alan Özel hayatın gizliliğini ihlal, 133. maddede yer alan Kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması ve 244. maddede yer alan Sistemi engelleme, bozma, verileri yok etme veya değiştirme suçları gösterilebilecektir.

765 sayılı eski TCK'deki hükümler incelendiğinde yukarıda zikrettiğimiz yeni TCK'de yer alan ve kişisel verileri doğrudan koruyan suç tiplerinin yer almadığı görülmektedir. Bu farklılık göz önüne alındığında kişisel verilerin korunması ve teknoloji ilişkisiyle ilgili olarak Ceza Hukuku bağlamında şu tespitler yapılabilecektir: Dijitalleşmenin sosyolojik, ekonomik sonuçları olduğu

[171] Manav, s.131

172 C. Gökhan Erbaş, **6698 sayılı Kişisel Verilerin Korunması Kanunu Kapsamında İşçinin Elektronik Ortamda Gözetlenmesi**, Hacettepe HFD, 7(1) 2017, 97-108, s.105

[173] Ayşe Merve BELGE, **Özellikle Kişisel Verilerin Korunması Kanunu Çerçevesinde İşçilerin Kişisel Verilerinin İhlâli ve Korunması Yolları**, D.E.Ü. Hukuk Fakültesi Dergisi, Prof. Dr. Şeref ERTAŞ'a Armağan, C. 19, Özel Sayı-2017, s.1039

gibi hukuki sonuçları da vardır. Söz konusu hukuki sonuçlar, günümüzde özellikle Veri Koruma Hukuku sahasında daha fazla belirginleşmektedir. Bu minvalde toplumu etkileyen teknolojik değişimler nedeniyle daha önce karşılaşılmamış ancak cezai sorumluluğu gerektiren zarar verici eylemlerin ortaya çıkması kaçınılmazdır. Devletin sözü edilen bu cümleden eylemlere karşı gösterdiği reaksiyon, Ceza Hukuku'nda yeni suç tipleri ihdas etmek şeklinde olmuştur. Böylece Türk Ceza Kanunu'nda kişinin bireysel özerkliğine, özel hayatına (özellikle kişisel verilerine) ve insan onuruna yönelik zarar verici eylemlerin cezalandırılması yoluna gidilmiştir.[174] Devletin cezalandırma tekeli sınırlarının, teknolojinin gelişimi gözetilerek yeni suç tipleri öngörülmesi suretiyle genişletilmesi kişisel verilerin korunması hakkının ihlalinde caydırıcılığın artırılması açısından son derece dikkate değer bir gelişmedir.

5.5. 6698 Sayılı Kişisel Verilerin Korunması Kanunu

Mevzuatımızda kişisel verilerle ilgili farklı kanunlarda çeşitli hükümler yer almakla birlikte Türk kanun koyucusu bu alana ilişkin olarak ve teknolojinin geldiği safhayı da gözetmek suretiyle özel bir düzenleme yapılması gerektiğini 6698 sayılı Kanun'un gerekçesinde şu şekilde belirtmiştir: *"Kişisel verilerin işlenebilmesi hususunda özel bir kanun ve etkin bir denetim mekanizmasının bulunmaması toplumumuzda olumsuz bir algının oluşmasına sebebiyet vermektedir. Oluşan bu algının ortadan kaldırılması için kişisel verilerin belli şartlar dahilinde işlenmesine, muhafaza edilmesine ve kontrolüne ilişkin esasların belirlenmesi gerekmektedir."* Gerekçede de belirtildiği üzere, kişisel verilerin korunması konusunda özel bir düzenleme olmamasına getirilen eleştirilerle birlikte toplumun beklentileri kanunun ihdası aşamasında dikkate alınmıştır.

6698 sayılı Yasa'nın düzenlenmesinde ülkemizin içinde bulunduğu uluslararası düzlem de etkili olmuştur. Bu kapsamda uzun zamandır süregelen AB'ye üyelik müzakereleri ile birlikte uluslararası iş birliği ve ticaretin artırılması konuları büyük öneme sahiptir. Ayrıca EUROPOL ve EUROJUST ile yetkili makamlarımız arasında veri akışının sağlanmasında karşılaşılan zorlukların yanı sıra yabancı sermayenin ülkemize çekilmesi gibi faktörler söz konusu kanuna duyulan ihtiyacı bir hayli artırmıştır.[175] Kişisel veriler ile ilgili olarak özel bir düzenleme yapılmasının diğer bir nedeni ise mevzuatımızda bulunan hali hazırdaki kişisel verilere ilişkin birtakım düzenlemelerin söz konusu verilerin işlenmesinden sonraki süreçlere ilişkin olmasıdır. Ancak unutulmamalıdır ki kişisel verilerin ne şekilde işlenebileceği önceden hüküm altına

[174] İbrahim Korkmaz, **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, Seçkin Yayınları, Nisan 2017, s.315

[175] Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin Korunması Kanununa Duyulan İhtiyaç**, s.4-6

alınmadığı takdirde veri ihlalleri söz konusu olabilecektir. Bunun sonucunda ise kişilerin özel hayatı ancak bir ihlal ortaya çıktıktan sonra korunmaya çalışılacaktır. Kişisel Verilerin Korunması Kanunu'nun ihdası ile kişisel verilerin işlenmesi sürecinden önceki aşamalara yönelik kurallar düzenlenmiş olup kişilerin özel hayatına müdahale sonucunu doğuracak işlemlerin nasıl yapılması gerektiği açıklığa kavuşturulmuştur. Böylece hukuk devletinin güvencelerinden olan ve bireylerin temel hak ve özgürlüklerinin ihlal edildikten sonra olduğu kadar ihlale uğramadan önce de korunması gerekliliği gözetilmiş olacaktır.

Bir sonraki başlığımızda 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun öncelikle tarihçesine değinilecek ve sonrasında kanunun sistematiği dikkate alınarak kişisel verilere ilişkin temel kavramlar açıklanacaktır.

6. Özel Bir Kanun Olarak 6698 Sayılı Kişisel Verilerin Korunması Yasası

6.1. Genel Olarak

108 sayılı Avrupa Konseyi Sözleşmesi'nin[176] imzalandığı günden itibaren ülkemizde çeşitli kanun ihdası girişimlerinde bulunulmuş ancak ya toplanan komisyonlar çalışmalarını tamamlayamamış ya da tamamlanan tasarılar kanunlaşamamıştır. Bu şekilde devam eden süreç Kişisel Verilerin Korunması Yasası'nın Türkiye Büyük Millet Meclisince 24 Mart 2016 tarihinde kabul edilerek yürürlüğe girmesiyle son bulmuştur. Teknolojinin hayatımızın her alanını hızla ele geçirmekte olduğu göz önüne alındığında kişisel verilerin korunması konusunda özel bir düzenlemenin Nisan 2016 gibi geç bir tarihte mevzuatımıza girmesi temel hak ve hürriyetlerin korunması açısından üzücü bir sonuçtur. Zira kişisel veriler, içinde bulunduğumuz zamanda günlük yaşamımızdaki birçok işlemde kullanılmaktadır ve bireylerin özel hayatının gizliliği bu noktada tehdit altında kalmıştır. Ancak unutulmamalıdır ki mevcut kanun her ne kadar geç bir tarihte yürürlüğe girse de hukuk uygulayıcılarının gayretleri neticesinde Bilgi ve Teknoloji Çağı'nın hızı yakalanabilecektir. Bu takdirde biz hukukçuların üzerine önemli görevler düşmektedir.

Yukarıda değinmiş olduğumuz hususlara ek olarak kanunun muhtevası incelendiğinde şu tespitler ortaya konulabilecektir: Kanunda ilk olarak bazı terimlerin tanımlamaları yapıldıktan sonra kişisel verilerin işlenme şartları, kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesi, kişisel verilerin aktarılmasına ilişkin hükümlere yer verilmiştir. Sonrasında veri sorumlusunun yükümlülüklerine, ilgili kişinin haklarına değinilip veri sorumlusuna başvuru ve

[176] 108 Sayılı Sözleşme 1981 yılında ülkemizce imzalanmış ancak Mart 2016'da 29656 sayılı Resmi Gazete ile iç hukukumuza dahil edilmiştir.

veri sorumluları siciline ilişkin kurallar düzenlenmiştir. Yasanın son kısmında ise suçlar ve kabahatlerle birlikte Kişisel Verileri Koruma Kurumu'nun yapısına ilişkin düzenlemeler yer almıştır.

6.2. Amaç

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun birinci maddesinde söz konusu kanunun amacı kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerinin korunması, kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasların belirlenmesi olarak belirtilmiştir.

Veri koruma kanunları incelendiğinde farklı amaçların yer aldığı görülmekle beraber 6698 sayılı KVKK'de başlıca benimsenen amaç hak ve özgürlüklerin koruma altına alınmasıdır. Bu yönüyle kanunun geri kalan hükümleri tetkik edilirken birinci maddede belirtilen temel hak ve özgürlükleri koruma amacı unutulmamalıdır. Ayrıca bu noktada, kişisel verilerin korunması hakkından kanunun ne amaç maddesinde ne de diğer hükümlerinde söz edilmediğini ve bu durumun çeşitli eleştirilere konu olduğunu belirtmemiz gerekir. [177]

6.3. Kapsam

6698 sayılı KVKK'nin 2. maddesinde söz konusu yasanın uygulanacağı kişiler, kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler olarak belirlenmiştir.

Kişisel Verileri Koruma Kanunu'nun kapsamının sınırları çizilirken kişisel verileri işlenen kişiler ile söz konusu verileri işleyen kişiler yönünden ikili bir ayrım öngörülmüştür. Verisi işlenen kişiler açısından bu ayrıma bakıldığında söz konusu kanunun işlemeye konu verilerin sadece gerçek kişiye ait olması durumunda uygulanacağını ve dahi tüzel kişilerin kapsama dahil edilmediğini vurgulamak gerekir. Ancak şu husus unutulmamalıdır ki tüzel kişiye ait verilerin gerçek bir kişi ile ilişkilendirilerek o kişinin kimliğinin belirlenebildiği haller de kanunun kapsamında sayılmalıdır.[178]

[177] Küzeci, *Kişisel Verilerin Korunması*, s.311-312
[178] Dülger, *Kişisel Verilerin Korunması Hukuku*, s.346-347

Yukarıda belirttiğimiz ayrımın kişisel verileri işleyen kişileri baz alan ikinci alt başlığı bakımından KVKK'nin kapsamı irdelendiğinde ise bu kişilerin gerçek veya tüzel kişi olmasının kanunun kapsamına girip girmemesi açısından bir farklılık arz etmeyeceği ifade edilmelidir.[179]

6698 sayılı yasanın kapsamının belirlenmesindeki diğer bir ölçüt ise işlemeye konu kişisel verilerin işlenme şeklidir.[180] Bu bağlamda dikkat çekilmelidir ki kısmen veya tamamen otomatik olan yollarla işleme eylemleri kanunun kapsamına girmektedir. Otomatiklik kavramı ile anlatılmak istenenin bilgisayar ve telefon gibi işlemcisi olan cihazlar tarafından yazılım veya donanım özellikleri vasıtasıyla öncesinde hazırlanan algoritmalar da kullanılarak insan müdahalesi olmadan yapılan işleme faaliyeti olduğuna yukarıda değinilmişti.[181]

İkinci olarak kanunun uygulanabileceği veri işleme yöntemi ise bir veri kayıt sisteminin parçası olan kişisel verilerin otomatik olmayan yollarla işlenmesidir. KVKK otomatik olmayan yöntemleri tamamen kapsam dışı bırakmamakla birlikte bu gibi yöntemlerle işlenen verilerin bir veri kayıt sisteminin parçası olmasını şart koşmuştur. Örneğin kişilerin ad ve soyadlarının herhangi bir kritere bağlı olmadan gelişigüzel bir şekilde kağıda yazılması kanunun kapsamına girmez iken bahse konu isim ve soyisimlerin sistematik olarak bir deftere kaydedilmesi eylemi kanunun uygulama alanına dahil edilecektir.[182] Bu noktada şu hususun altını çizmekte fayda vardır: Bir veri kayıt sistemine dahil olmayıp otomatik olmayan yollarla işlenen veriler de hali hazırda kişisel veri olma özelliklerini sürdürmekle birlikte Kişisel Verilerin Korunması Kanunu kapsamına dahil olmamaktadır. Ancak unutulmamalıdır ki söz konusu veriler açısından Türk Ceza Kanunu anlamında sorumluluk devam etmektedir. Zira TCK açısından KVKK'de öngörülenin aksine otomatik olmayan yollarla veri işleme halinde doğacak sorumluluk bakımından veri kayıt sistemi kriteri benimsenmemiştir.[183]

6698 sayılı yasanın kapsamı açısından bu kanunun 28. maddesi ayrıca incelenmelidir. Söz konusu maddenin birinci fıkrasında başkaca bir şart öngörülmeden kanunun kapsamı dışında kalan haller düzenlenirken maddenin ikinci fıkrasında kısmen kanun kapsamına alınmayan durumlar sayılmıştır. KVKK'nin tamamen kapsamı dışında sayılan haller a)Kişisel verilerin, üçüncü kişilere verilmemek ve veri güvenliğine ilişkin yükümlülüklere uyulmak kaydıyla

[179] Dülger, *Kişisel Verilerin Korunması Hukuku,* s.347; Kişisel Verileri Koruma Kurumu, 6698 Sayılı Kişisel Verilerin Korunması Kanunu'nun Amacı ve Kapsamı, s.4
[180] Dülger, *Kişisel Verilerin Korunması Hukuku*, s.346-348
[181] Bkz. 118 sayılı dipnot
[182] Kişisel Verileri Koruma Kurumu, **6698 Sayılı Kişisel Verilerin Korunması Kanun'unun Amacı ve Kapsamı**, s.6
[183] Dülger, *Kişisel Verilerin Korunması Hukuku*, s.346-348

gerçek kişiler tarafından tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında işlenmesi, b) Kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi c) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi, ç) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi, d) Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi şeklinde düzenlenmiştir.

28. maddenin 2. fıkrasında ise a) Kişisel veri işlemenin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması b) İlgili kişinin kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi c) Kişisel veri işlemenin kanunun verdiği yetkiye 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 ç) Kişisel veri işlemenin bütçe, vergi ve mali konulara ilişkin olarak devletin ekonomik ve mali çıkarlarının korunması için gerekli olması durumlarında KVKK'nin amacına ve temel ilkelerine uygun ve orantılı olmak kaydıyla kanunun, veri sorumlusunun aydınlatma yükümlülüğünü düzenleyen 10' uncu, zararın giderilmesini talep etme hakkı hariç, ilgili kişinin haklarını düzenleyen 11' inci ve Veri Sorumluları Siciline kayıt yükümlülüğünü düzenleyen 16'ncı maddelerinin uygulanmayacağı hükme bağlanmıştır. Madde lafzından da açıkça anlaşılacağı gibi kanunun uygulanması açısından maddenin birinci fıkrasında öngörülenin aksine tüm maddeleri kapsamayan ve sadece hükümde belirtilen kanun maddelerini içeren bir istisna getirilmiştir.

6.4 Tanımlar

Bu başlık altında çalışmamız açısından önem arz eden ve kişisel veri kavramı ile yakından ilişkili olan kavramlara değinilecektir. Söz konusu kavramların türediği ana kavram olan kişisel veri kavramı ilk kısımda ayrıntılı olarak incelendiği için burada yalnızca ilgili bölüme atıf yapmakla yetiniyoruz.

6.4.1. Açık Rıza ve İstisnaları

Açık rıza kavramı Kişisel Verilerin Korunması Kanunu'nun Tanımlar başlıklı 3. maddesinde belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza olarak tanımlanmıştır. Açık rıza, ilgili kişinin kendi isteği ile veya karşısındaki kişinin talebi üzerine kendi verilerinin işlenmesini onaylaması şeklinde anlaşılmalıdır. Anayasamızın Özel Hayatın Gizliliği başlıklı 20. maddesinin 3'üncü fıkrasında da yer verilen açık rıza, özel nitelikli verilerle birlikte diğer kişisel veriler açısından da bir hukuka uygunluk sebebi oluşturmaktadır. Ancak rızanın kişisel verilerin işlenmesini hukuka uygun hale getirmesi bazı şartları taşımasına bağlıdır. Öncelikle açık rıza, belirli bir konuya ilişkin olmalı ve sadece o konuyla sınırlanmalıdır. Bu bağlamda açık rızanın hangi konuya ilişkin olarak istenildiği açıkça ifade edilmelidir. Açık rızanın taşıması gereken ikinci özellik, bilgilendirilmeye dayalı olarak verilmesidir. Verisi işlenecek kişi, işleme faaliyetinden önce, kendisinin de anlayabileceği bir dille hangi amaçlar için verisinin kullanılacağı hakkında bilgilendirilmelidir. Zira ilgili kişinin ne için rıza verdiğini rıza beyanını ortaya koymadan önce bilmesi gerekir. Üçüncü ve son olarak açık rıza özgür iradeye dayalı olmalıdır. Günümüzde sıkça karşılaştığımız ve birçok şirketin uyguladığı yöntemlerin aksine rıza, yararlanılmak istenen ürün veya hizmetten istifade edebilmenin ön şartı olarak aranmamalıdır.[184] Nitekim bu durumda hizmeti almak isteyen ilgili kişinin rıza beyanı özgür iradesine değil; tam aksine baskı altında bir zorunluluk hissetmesine dayanmaktadır.

6.4.2. Kişisel Verilerin İşlenmesi

Kişisel verilerin işlenmesi kavramı çalışmamızın başında ayrıntılı bir şekilde incelendiğinden bu başlık altında yalnızca konumuz açısından önemli birkaç noktaya değinmekte fayda görüyoruz.

Kişisel verilerin işlenmesi Kişisel Verilerin Korunması Kanunumuzda *"Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem"* olarak tanımlanmıştır. Tanımdan da anlaşılacağı üzere

[184] Kişisel Verileri Koruma Kurumu, **Açık Rıza**, 1-6; *"…bu çerçevede açık rızanın özgür iradeyle açıklanması gerektiğinden, herhangi bir ürün ve/veya hizmetin sunumunun da (ya da herhangi bir üründen ve/veya hizmetten yararlandırılması) ilgili kişi tarafından açık rıza verilmesi şartına bağlanmaması… gerektiği"* Kişisel Verileri Koruma Kurulu, 20/04/2021 tarih ve 2021/389 sayılı karar özeti

işleme kavramının sınırları son derece geniştir. Maddede veri işleme türü olarak sayılan işlemler ise sınırlayıcı olmayıp yalnızca örnek olarak belirtilmiştir.

Kişisel verilerin işlenmesi süreci verilerin toplanmasından itibaren silinmeleri, yok edilmeleri veya anonim hale getirilmelerine kadarki süreçte muhatap oldukları her türlü faaliyeti kapsamaktadır. Kişisel verilerin silinmesi ile kişisel verilerin, ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemi kastedilirken; kişisel verilerin yok edilmesi ile kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi ifade edilmektedir. Anonim hale getirilme ise kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi olarak anaşılmalıdır.[185]

Çalışmamız açısından önemli olan noktalardan birini KVKK'deki işleme kavramı ile Türk Ceza Kanunu'nun 136. maddesindeki suç tipi için öngörülen fiiller arasındaki ayırımın ortaya konulması oluşturmaktadır.

Öncelikle belirtelim ki TCK'nin 136. maddesinde öngörülen verme, yayma ve ele geçirme fiilleri, KVKK'de yer alan kişisel verilerin işlenmesi kavramına dahil olan eylem çeşitleridir. Ancak bu noktada KVKK'de öngörülen işleme kavramının kapsamına girmeyen ve fakat TCK açısından cezai sorumluluk oluşturacak ihtimaller de unutulmamalıdır. Zira Kişisel Verilerin Korunması Kanunu'nda veri işlenmesi kavramı için tamamen veya kısmen otomatik yolla işleme ya da otomatik olmayan yolla herhangi bir veri kayıt sisteminin parçası olmak kaydıyla işleme şeklinde bazı hareket formları öngörülmüştür. Ancak söz konusu şartları sağlamayan fiiller, 6698 sayılı Kanun kapsamında kişisel verilerin işlenmesi olarak kabul edilmemekle birlikte Ceza Kanunumuzda bu yönden bir ayrım yapılmadığından suça vücut verebilecektir. Örneğin herhangi bir veri kayıt sisteminin parçası olmayan kişisel verilerin otomatik olmayan yollar aracılığıyla 136. maddede sayılan fiillere konu olması ve diğer şartların da sağlanması halinde Türk Ceza Kanunu açısından sorumluluk doğacaktır.

6.4.4. İlgili Kişi ve Hakları

İlgili kişi, Kişisel Verilerin Korunması Kanunumuzda kişisel verisi işlenen gerçek kişi olarak tanımlanmıştır. Tanımda ilk dikkat çeken husus ilgili kişinin ancak gerçek kişi olabileceğinin öngörülmüş olmasıdır. Kanun, açıkça tüzel kişileri tanımlamaya dahil etmemiştir. Bununla birlikte 2008 tarihli Kişisel Verilerin Korunması Kanunu tasarısında kanunun kapsamına kişisel

[185] Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik, m. 8-10

verileri işlenen gerçek kişiler yanında tüzel kişilerin de dahil edildiğini belirtmek gerekir.[186] İlgili kişi kavamının kapsamına tüzel kişilerin dahil edilip edilemeyeceği hususu çeşitli tartışmalara konu olmakla birlikte Anayasa Mahkememizin 2013/84 esas ve 2014/183 karar sayılı kararına bu noktada değinmekte fayda görüyoruz. Bahsi geçen kararın verildiği iptal davasında 6475 sayılı Posta Hizmetleri Kanunu'nun çeşitli maddelerinin Anayasa'ya aykırılığı iddiası ileri sürülmüştür. İpali istenen yasa maddelerinden birinde -yasanın 3. maddesinde- adres bilgi kayıt sistemi isimli veri tabanının, gerçek ve tüzel kişiler ile kamu kurum ve kuruluşlarına ait fiziki ve elektronik adreslerin reklam ve tanıtım amacıyla PTT hizmetlerinden yararlananlara ücret karşılığı kullandırılmasına yönelik olarak oluşturulduğu yer almaktadır. Ancak düzenlemede dikkat çeken nokta, bu sistemin oluşturulması sırasında gerçek kişilerin rızasının alınmasına rağmen tüzel kişilere ilişkin böyle bir şartın öngörülmemesi olmuştur. Anayasa Mahkemesi ise iptal istemine ilişkin kararında Anayasa'nın Özel Hayatın Gizliliği başlıklı 20. maddesinde *"Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir."* şeklinde düzenlenen hükümde yer alan "herkes" ibaresinin tüzel kişileri de kapsadığını ve dünyadaki gelişmelerin, kişisel verilerin korunmasının kapsamına tüzel kişilerin de dahil edilmesi gerekliliğini ortaya koyduğunu ifade etmiştir. Söz konusu gerekçelerle ilgili maddedeki "gerçek" ibaresi iptal edilmiştir.[187] Çalışmamızın ilk başlıklarında da değindiğimiz üzere başta KVKK olmak üzere GDPR ve diğer düzenlemelerin konuya yaklaşımı oldukça nettir ve tüzel kişiler ilgili kişi olarak kabul görmemektedir. Ayrıca Kişisel Verileri Koruma Kurumu da tüzel kişilere ait verilerin korunması konusunun hiçbir şekilde Kanun'un kapsamında olmadığını belirtmiştir.[188]

İlgili kişi kavramının kapsamını belirledikten sonra bu kişinin haklarından bahsetmek gerekmektedir. 6698 sayılı Kanun'da ilgili kişinin hakları 11. maddede sayılmıştır. Söz konusu haklar, kişisel veri işlenip işlenmediğini öğrenme, kişisel verileri işlenmişse buna ilişkin bilgi talep etme, kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme, yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme, kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme, 7'nci maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok

[186] Başbakanlık Kanunlar ve Kararlar Genel Müdürlüğü, **Kişisel Verilerin Korunması Kanunu Tasarısı (2008) 1-576**, 22.4.2008

[187] Anayasa Mahkemesi E.2013/84 K.2014/183 T.4.12.2014 Bkz. **Anayasa Mahkemesi Kararları Dergisi** sayı 52/3cilt, Anayasa Mahkemesi Yayınları, Mayıs, 2017, s.1759-1847. Kararın karşıoylarının bir kısmında mahremiyet hakkı kapsamında değerlendirilme yapıldığı görülmektedir. Hasan Tahsin Gökcan ise karşıoy yazsısında Anayasa'daki düzenlemenin tüzel kişileri de kapsadığını ancak hangi bilgilerin kişisel veri sayılacağı konusunda tüzel kişiler ve gerçek kişiler arasında farklılıklar olduğunu belirtmiştir.

[188] Bkz. Dn.15

edilmesini isteme, (d) ve (e) bentleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme, işlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme, kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme olarak sayılmıştır. Ayrıca aynı maddede sayılan bu hakların veri sorumlusuna başvurarak kullanılacağı düzenlenmiştir.[189]

6.4.5. Veri Sorumlusu ve Yükümlülükleri

Kişisel Verilerin Korunması Kanunu'nda veri sorumlusu, kişisel verilerin işlenme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi olarak tanımlanmıştır.

Veri sorumlusu, KVKK'nin merkezinde yer alan bir kavram olup söz konusu kavramın tanımlanması kanunun uygulanacağı kişilerin kapsamını belirleyecektir. Veri sorumlusu kavramının sınırları çizilirken veri işleme faaliyetinden yola çıkarak bu faaliyetin yerine getirildiği araçlarla birlikte işleme ile güdülen amaç da göz önünde tutulmalıdır. Zira bir kişiye verilen veri işleme araçları ve amaçlarını belirleme yetkisinin genişliği ile o kişinin veri sorumlusu olma ihtimali doğru orantılıdır. Diğer bir deyişle kişisel verilerin işlenmesinden elde edilen menfaat ölçüsünde işleme faaliyetinden doğan sorumluluğun üstlenilmesi gerekmektedir.[190]

İşleme faaliyetinin araçlarını ve amaçlarını belirlemek aslında işlemenin neden ve nasıl yapılacağını belirlemeye eşdeğer anlamdadır. Bu bağlamda işlemenin neden ve nasıl yapılacağı konusunda sahip olunan hangi yoğunluktaki bir etkinin veri sorumlusu olma sonucunu doğurduğunun belirlenmesi gerekir. Bununla birlikte veri işlemenin amacına veya araçlarına atfedilen önem, işlemenin meydana geldiği bağlama göre de değişiklik gösterebilecektir.[191]

Veri sorumlusunun tüzel kişi olması durumunda sorumluluk rejiminin nasıl belirleneceği de önemli bir konudur. Tüzel kişiler, kişisel verilerin işlenmesi ile ilgili yürüttükleri faaliyetler bağlamında kendileri bizzat veri sorumlusu olmaktadır. Veri işleme faaliyetlerinden doğan hukuki sorumluluk da tüzel kişiliğin şahsına ait olacaktır. Bu anlamda kamu hukuku ve özel hukuk tüzel kişileri arasında herhangi bir farklılık yoktur. Ayrıca belirtmek gerekir ki bir şirket

[189] Kişisel Verileri Koruma Kurumu, **Kanun Kapsamındaki Hak ve Yükümlülükler**, s.10

[190] Mesut Serdar Çekin, **Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku**, 3. Baskı, İstanbul-Temmuz 2020 On İki Levha yayıncılık, s.51-55

[191] Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", February 2010, s.13.

organizasyonu içerisindeki birimler tüzel kişiliğe sahip olmadığından veri sorumlusu olması mümkün olmamakla birlikte şirketler topluluğundaki her bir şirketin ayrı tüzel kişiliği olması nedeniyle hepsinin ayrı ayrı veri sorumlusu olacağını ifade edelim.[192]

Veri sorumlusu, kişisel verilerin işlenmesi ile ilgili kararları alma yetkisine sahip olup verilerin işlenme amacı ve yöntemini belirlemektedir. Diğer bir ifadeyle kişisel verilerin neden ve nasıl işleneceği hakkında karar vermektedir. Bu doğrultuda veri sorumlusu, sahip olduğu söz konusu yetkilerin yanında ayrıca birtakım yükümlülükler de taşımaktadır ki bu noktada veri sorumlusu kavramı, Kişisel Verilerin Korunması Kanunu'nun çeşitli hukuki yükümlülükleri ortaya koymak amacıyla referans aldığı bir statü olarak karşımıza çıkmaktadır.[193]

6698 sayılı Kanun'da veri sorumlusu için öngörülen yükümlülükler aydınlatma yükümlülüğü, veri güvenliğinin sağlanması, Kişisel Verileri Koruma Kuruluna bildirim yükümlülüğü, Veri Sorumluları Sicili'ne (VERBİS) kayıt yükümlülüğü ve diğer yükümlülükler şeklinde düzenlenmiştir.[194] İlk yükümlülük olan aydınlatma yükümlülüğünde, veri sorumlusuna veya yetkilendirdiği kişiye kişisel verilerin elde edilmesi sırasında ilgili kişiye veri sorumlusunun ve varsa temsilcisinin kimliği, kişisel verilerin hangi amaçla işleneceği, işlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceği, kişisel veri toplamanın yöntemi ve hukuki sebebi ve son olarak kanunun 11'inci maddesinde sayılan ilgili kişinin hakları hakkında bilgi verme mükellefiyeti yüklenmiştir.

6698 sayılı Kanun'un 12. maddesinde yer verilen veri sorumlusu açısından diğer bir yükümlülük ise veri güvenliğinin sağlanmasıdır. Bu yükümlülük kapsamında veri sorumlusu, kişisel verilerin hukuka aykırı olarak işlenmesini ve kişisel verilere hukuka aykırı olarak erişilmesini önlemek, kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbiri almak zorundadır. Yine aynı doğrultuda veri sorumlusunca işlenen verilerin hangi verilerden oluştuğunun yanı sıra söz konusu verilerin korunmasında karşılaşabilecek risklerin ve bu risklerin gerçekleşmesi durumunda yol açılabilecek tehditlerin tespiti gerekmektedir. Ayrıca veri sorumlusunun

[192] Kişisel Verileri Koruma Kurumu, **Veri Sorumlusu ve Veri İşleyen**, s.1

[193] Kişisel Verileri Koruma Kurumu, **Veri Sorumlusu ve Veri İşleyen**, s.1-4; Bu suretle veri sorumlusu kavramı, verisi işlenen ilgili kişilerin veri işleme faaliyetleri hakkında bilgilendirilmesi, haklarını savunabilmeleri ve karşılarında sorumlu bir muhatap bulabilmeleri açısından son derece önemlidir. Bkz. Sinem Göçmen Uyarer, **6698 Kişisel Verilerin Korunması Kanunu ve 5237 Sayılı Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması**, İstanbul-2019, s.95; Veri sorumlusunun tespit edilmesinin kişisel verilerle ilgili olan yükümlülüklere uyulup uyulmadığının belirlenmesi ve bu yükümlülükleri ihlal etme durumunda sorumluya uygulanacak yaptırımlar bakımından önemlidir. Bkz. Yasemin Avcı, **Kişisel Verilerin Korunması**, Yüksek Lisans Tezi, Konya-2019, s.18

[194] Mesut Halıcıoğlu, **Türk Hukukunda Veri Sorumlusu Kavramı**, Yüksek Lisans Tezi Ankara 2019, s.81

çalışanlarına gerekli eğitimler verilmeli ve veri güvenliğine ilişkin olarak politikalar hazırlanmalıdır.[195]

Veri sorumlusunun Kurula bildirim yükümlülüğünde ise veri sorumlusuna, işlediği kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde bu durumu en kısa sürede ilgilisine ve Kurula bildirmek mükellefiyeti yüklenmiştir. Kişisel Verileri Koruma Kurulu, veri sorumlusuna bu şekilde bir sorumluluk yüklenmesi ile hedeflenen amacın meydana gelen veri ihlalinden etkilenen kişileri ilgilendiren olumsuz sonuçların önlenmesi veya asgari seviyeye indirilmesi olduğunu ifade etmiştir.[196]

Sayılan bu yükümlülüklerin yanında veri sorumluları Veri Sorumluları Sicili'ne (VERBİS) kaydolmak zorundadır. VERBİS, kamuya açık şekilde tutulması gereken bir sicildir. Kamuya açıklıkla birlikte veri sorumlularının kamu tarafınca bilinmesi suretiyle hak ihlallerine karşı etkin bir mücadele sağlanmış olacaktır.[197]

Veri sorumlusu-veri işleyen kavramları arasındaki farklara bir sonraki veri işleyen başlığında değinilecektir.

6.4.6. Veri İşleyen

Kişisel Verilerin Korunması Kanunu'nda veri işleyen kavramı, veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi şeklinde ifade edilmiştir.

Veri işleyen, veri sorumlusunun organizasyonu dışında ve veri sorumlusundan aldığı talimatlara göre kişisel veri işleme faaliyeti gösteren kişidir. Verilerin işlenmesi ile ilgili kararlar veri sorumlusu tarafından alınırıken veri işleyen, işleme faaliyetinin daha çok teknik yönü ile ilgilenir. Ayrıca belirtmek gerekir ki veri sorumlusu ve veri işleyen sıfatları aynı kişide birleşebilir.[198] Şöyle ki aynı kişi, bazı veri işleme faaliyetleri açısından veri sorumlusu olabileceği gibi diğer bazı faaliyetler özelinde veri işleyen sıfatını taşıyabilecektir. Somut

---

[195] Kişisel Verileri Koruma Kurumu, **Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)**, KVKK Yayınları, Ocak 2018, Ankara, s. 8-12

[196] Kişisel Verileri Koruma Kurulu, Kişisel Veri İhlali Bildirim Usul ve Esaslarına İlişkin Kişisel Verileri Koruma Kurulunun 24.01.2019 Tarih ve 2019/10 Sayılı Kararına İlişkin Duyuru

[197] Kişisel Verileri Koruma Kurumu, **Veri Sorumluları Sicili**, s.1

[198] Kişisel Verileri Koruma Kurumu, **Veri Sorumlusu ve Veri İşleyen**, s.1-5; Ancak şu husus unutulmamalıdır: Veri sorumlusu, kendisi için bir veri işleyen görevlendirse dahi veri koruma hukuku açısından yükümlülükleri devam etmektedir. Bkz. Sinem Göçmen Uyarer, **6698 Kişisel Verilerin Korunması Kanunu ve 5237 Sayılı Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması**, İstanbul – 2019, s.98

olayda veri sorumlusu mu yoksa veri işleyen olarak mı hareket edildiği spesifik olarak o veri grubu veya işleme faaliyetleri göz önünde bulundurularak tespit edilmelidir.[199]

Veri sorumlusu ve veri işleyen farkının anlaşılması için şu örneklere dikkat çekmekte yarar görüyoruz: İlk örnekte bir kamu kuruluşunun topladığı verilerin saklanması için bulut hizmeti sağlayıcısı ile sözleşme akdettiği bir durumda bulut hizmetini sunan taraf veri işleyen sıfatını haiz olacaktır. Zira kendisinin tek faaliyeti söz konusu kuruluşun talimatları doğrultusunda ondan aldığı verileri saklamaktır.[200] Farklı bir örnekte ise bina maliki tarafından güvenlik şirketi ile imzalanan sözleşme uyarınca binaya kamera sistemi kurulmuştur. Video ile gözetleme amacının ve görüntülerin toplanıp depo edilme yönteminin özellikle malik tarafından belirlenmesi nedeniyle bina maliki veri sorumlusu olarak kabul edilecektir.[201] Diğer bir örnek ise çağrı merkezi hizmeti veren şirketin, bu hizmeti alan veri sorumlusu tarafından kendisine verilen yetkiye dayanarak veri işleme faaliyetini gerçekleştirmesidir. Bu örnekte de çağrı merkezi hizmeti veren şirket veri işleyen statüsündedir.[202] Son olarak bir muhasebe şirketi kendi çalışanlarını ilgilendiren ve kendisinin tuttuğu kişisel verilere ilişkin olarak veri sorumlusu kabul edilmektedir. Ancak yine aynı muhasebe şirketi, kendisinin hizmet verdiği ve müşterisi olan şirketlere ilişkin tuttuğu veriler bakımından ise veri işleyen olarak kabul edilecektir.[203]

6.5. Kişisel Verilerin İşlenmesinde Uyulması Gereken Genel İlkeler

Kişisel Verilerin Korunması Kanunu'nda kişisel verilerin işlenmesi sürecinde uyulması zorunluluk arz eden birtakım ilkeler düzenlenmiştir. Bu ilkeler sırasıyla hukuka ve dürüstlük kurallarına uygun olma, doğru ve gerektiğinde güncel olma, belirli, açık ve meşru amaçlar için işlenme, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ve son olarak ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme şeklinde belirtilmiştir.

İlk olarak değinmek gerekirse hukuka ve dürüstlük kurallarına uygun olma ilkesi ikiye ayrılarak incelenmelidir. Birinci ayrımda hukuka uygunluk söz konusudur. Kişisel verilerin işlenmesinde hukuka uygun olma ilkesi aslında hukuk devleti ilkesinin bir gereği olarak karşımıza

---

[199] Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", February 2010, s.25.

[200] Kişisel Verileri Koruma Kurumu, Veri Sorumlusu ve Veri İşleyen, s.10

[201] Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", February 2010, s.18

[202] **100 Soruda Kişisel Verilerin Korunması Kanunu**, KVKK Yayınları, Nisan 2018, Ankara, s.31

[203] TBMM, **Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu**, Madde Gerekçeleri, s.7

çıkmaktadır.[204] Hukuka uygunluk ilkesinden kasıt, kişisel verilerin işlenmesi sırasında kanunlar ve diğer hukuki düzenlemelerle belirlenen ikelere uygun hareket edilmesi olarak kabul edilmektedir. Unutulmaması gereken diğer bir husus ise işleme faaliyetinin başından sonuna kadar hukuka uygunluğunun korunmasının bu ilkenin bir sonucu olduğudur.[205]

İnceleme konusu olan ilkenin ikinci ayrmını ise dürüstlük kurallarına uygunluk oluşturmaktadır. Dürüstlük kurallarına uygunluk, veri sorumlusu veya veri sorumlusu adına veri işleyen kişinin kendilerine tanınan hakları kötüye kullanmalarının önüne geçilmesini hedeflemektedir.[206] Nitekim doktrinde bu ilke ile verisi işlenen ilgili kişinin özel hayatının gizliliği, maddi ve manevi bütünlüğü ile özerkiliğinin veri sorumlusunca makul olmayan sebeplerle ihlal edilmemesi için sorumluyu zorladığı ifade edilmiştir.[207] Dürüstlük ilkesi, ilgili kişinin bir veri işleme faaliyetinin olup olmadığı şayet var ise işlemenin amacı hakkında bilgilendirilmesini beraberinde getirmektedir. Buna göre veri sorumlusu, somut olayın özelliklerinin gerektirdiği derecede bilgiyi ilgili veri öznesi ile paylaşacaktır.[208]

Doğru ve gerektiğinde güncel olma ilkesi, işlemeye konu verilerin "doğru" olarak işlenmesinin yanı sıra eksik veya yanlış veri işlemenin söz konusu olduğu durumlarda veri öznesince kullanılan düzeltme talebi hakkıyla bağlantılı olarak ilgili kişiye ilişkin bilgilerin güncellenmesini kapsamaktadır.[209] İşlemeye konu olan verilerin doğru ve güncel olacak şekilde tutulması ilgili kişinin temel hak ve özgürlüklerinin muhafazası açısından önemlidir. Örnek vermek gerekirse adres bilgisi doğru kaydedilmeyen kişiye gönderilecek tebligat muhatabına iletilemezse maddi ve manevi zararlar ortaya çıkabilecektir.[210] Ayrıca bahse konu ilke incelendiğinde kişisel verinin doğruluğunun mutlak surette sağlanmasının zorunluluk arz etmesine karşılık güncellik şartının, yalnızca gereken durumlarda yerine getirilmesi gerektiği anlaşılmaktadır.

Diğer bir ilke olan belirli, açık ve meşru amaçlar için işlenme ilkesi uyarınca işlemeye konu olan verilerin hangi amaçlar hedeflenerek ne kadar süreyle ve hangi sınırlar dahilinde işleneceği hakkında ilgili kişi bilgilendirilmelidir. Bu kapsamda, veri öznesi olan birey, işleme faaliyetini açıkça anlayabilmeli, bu faaliyeti meşru kılan hukuki şartları idrak edebilmeli ve son olarak veri

---

[204] Çekin, s.69
[205] Küzeci, *Kişisel Verilerin Korunması*, s.201
[206] Çekin, s.70
[207] Küzeci, *Kişisel Verilerin Korunması*, s.201
[208] GDPR, Recital para. 60
[209] Uyarer, *6698 Kişisel Verilerin Korunması Kanunu ve 5237 Sayılı Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması*, s.105-106
[210] Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler**, s.5-6

işlemenin amacı belirlenebilir bir şekilde ortaya konulmuş olmalıdır. Aynı yönde belirtilmelidir ki meşru amaç, veri sorumlusunun kişisel verileri, sunduğu hizmet veya işle bağlantılı ve ancak gereklilik arz etmesi halinde işlemesini ifade etmektedir. Açıklılık ve belirlilik açısından ise önemli olan husus, kişisel verilerin işlenme amaçlarının açıklanmasında ilgili kişinin anlamayacağı şekilde teknik-hukuki ifadelerden uzak durulmasıdır. Nitekim bu ilke göz ardı edilecek olursa veri sorumlusunun işleme faaliyeti açısından sınırsız bir takdir yetkisi doğması ve kişilerin de kendi verileri üzerinde sahip oldukları denetim imkanının azalması tehlikesi ile karşılaşılacaktır.[211]

Kişisel verilerin işlendikleri amaçla sınırlı, bağlantılı ve ölçülü olması ilkesi açısından şu tespitler yapılabilecekir: Veri işlemenin amacına ulaşılması için gerekli olan kişisel verilerin işlemeye konu olmasının yanı sıra söz konusu amaç açısından zorunluluk arz etmeyen verilerin işlenmesinden kaçınılması gerekmektedir. Bu bağlamda henüz mevcudiyet kazanmamış ancak ileride gerçekleşmesi tahmin edilen amaçlar doğrultusunda veri toplanmamalıdır. Ölçülülük ilkesi ise işleme faaliyeti ile bu faaliyetle hedeflenen amaç arasında makul bir denge kurulmasını öngörmektedir. Bu kapsamda veri işleme, amacı gerçekleştirebilecek ölçüde olmalıdır.[212] Nitekim ulaşılması hedeflenen amacın gerektirdiğinden fazla veya söz konusu amacı aşan işleme faaliyeti hukuka aykırı olacaktır.[213] Örneğin, Danıştay tarafından KVKK'nin yürürlükte olmadığı dönemde verilen bir kararda[214], personelin mesai devamlılığının ölçülmesi amacıyla parmak izi sisteminin kullanılması şeklindeki bir uygulamadan kaynaklanan uyuşmazlıkla ilgili olarak bu şekilde öngörülen bir mesai kontrol sistemi ile uygulamayı benimseyen kurumun amaçladığı kamu yararı arasında orantılılık bulunmadığı sonucuna varılmış ve söz konusu uygulamanın Anayasada yer alan ölçülülük ilkesine aykırı olduğu sonucuna varılmıştır.[215]

İşlemeye konu verilerle ilgili olarak mevzuatta bir süre belirtilmişse o süreyi aşmayacak şekilde söz konusu veriler tutulmalıdır. Bunun yanında şayet işlenen veriler için ilgili düzenlemelerde

---

[211] Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler**, s.7-8; Uyarer, *Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması*, s.123

[212] Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler**, s.9; TBMM, **Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu**, Madde Gerekçeleri, s.8-10; Neticeten kişisel verilerin herhangi bir amaç olmadan ileride gereklilik doğması ihtimali göze alınarak tutulması sonucunda kişinin kendisini ifade etmesi ve kişiliğini geliştirme imkanı zarar görecektir. Bkz. Küzeci, *Kişisel Verilerin Korunması*, s.203

[213] Göksu Hazar Erdinç, **Kişisel Verileri Koruma Dergisi, Cilt: 2, Sayı: 1, 2020, Ölçülülük İlkesi ve Açık Rıza Kapsamında Biyometrik Verilerin İşlenmesi**, s.11

[214] Danıştay İdari Dava Daireleri Kurulu Esas No: 2010/1285 Karar No: 2013/3325, Danıştay Dergisi Yıl: 2014 Sayı: 135, s.29-33

herhangi bir süre öngörülmemişse işleme amacı dikkate alınarak gereken süre belirlenecek ve bu süreyi aşmayacak şekilde kişisel veriler işlenecektir.

Kişisel verilerin herhangi bir süre sınırlaması olmaksızın tutulması bireylerin kendi verileri üzerindeki haklarının etkisiz hale gelmesine yol açacağı gibi kişilerin sınırsız bir süre boyunca kayıt altına alınmasına neden olunacaktır. Veri sorumlusunun her ihtimale karşı tedbir alma anlayışıyla veri depolaması noktasında herhangi bir takdir yetkisinin bulunmadığı gözetildiğinde gereken sürenin geçmesiyle birlikte işleme faaliyetine konu veriler silinecek, yok edilecek veyahut anonim hale getirilecektir. Aksi halde Türk Ceza Kanunu'nun 138. maddesinde düzenlenen verileri yok etmeme suçu gündeme gelebilecektir.[216]

Çalışmamızın bu kısmında kişisel verileri işlenen bireylerin, söz konusu bilgilerin sınırsızca kullanılması ve depolanmasına karşı korunmasını sağlayan unutulma hakkına değinmekte yarar görüyoruz. Unutulma hakkı, son yıllarda özellikle bazı olaylarla adı anılan kişilerin bu olayın üzerinden uzun süre geçmesine rağmen halen isimlerinin internetteki arama sonuçlarında çıkmasından duyduğu rahatsızlıktan dolayı sıkça gündeme gelmektedir. Söz konusu hak ile ilgili olarak Avrupa Birliği Adalet Divanı'nın verdiği C-131/12 sayılı karar önemli bir yer tutmaktadır. Karara konu olayda Mario Costeja González isimli kişi, Google arama motoruna isminin yazılması durumunda arama sonuçlarında 1998 tarihli ve kendi sosyal güvenlik borçlarını ödeyememesi nedeniyle bazı taşınmaz mallarının satılmasına ilişkin haberin çıktığını ancak borçları ile ilgili sürecin çoktan tamamlanmış olması nedeniyle artık haberin kendisiyle ilgisinin bulunmadığını ve bu nedenle kendisi ile ilgili verilerin kaldırılmasını istemiştir.[217] ABAD ise 95/46 EC sayılı Direktif kapsamında bir inceleme yapmış ve işlenen kişisel verilerin tarihi, istatiksel veya bilimsel amaçlar bakımından da bir gereklilik olmadığı durumlarda daha önceden belirlenen süreleri aşacak şekilde depolanması ile ilgili olarak kamu yararı şeklinde özel bir hal de olmadığında söz konusu bilgilerin silinmesi gerektiğine ve kişinin bunu talep etme hakkı olduğuna kanaat getirmiştir.[218]

Unutulma hakkı, internetin gelişmesine paralel olarak önemini giderek artırmış ve artık yargı kararlarında da kendisine yer bulmaya başlamıştır. Bu minvalde Yargıtay Hukuk Genel Kurulu, unutulma hakkını üstün bir kamu yararı olmadığı sürece, dijital hafızada yer alan geçmişte yaşanılan olumsuz olayların bir süre sonra unutulmasını, başkalarının bilmesini istemediği

[216] Uyarer, *Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması*, s.124-125

[217] ABAD, Judgment of the Court (Grand Chamber), 13 May 2014.Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González. Para.14-15

[218] Seray Nalbantoğlu, **Bir Temel Hak Olarak Unutulma hakkı**, TAAD, Yıl:9, Sayı:35 (Temmuz 2018), s.591

kişisel verilerin silinmesini ve yayılmasının önlemesini isteme hakkı olarak tanımlamaktadır.[219] Bu hak sayesinde kişi, kendisini ilgilendiren ancak edinildiği takdirde üçüncü kişiler nezdinde şahsına yönelik olumsuz algı oluşturacak bilgilerin silinmesini talep edebilecektir. Böylece birey, önyargılardan kurtularak manevi gelişimini sürdürebilecektir.[220] Özellikle arama motorlarında çıkan sonuçlardan kişinin kendisinin çıkarılmasını isteme hakkını veren bu hak, diğer yandan bireye ilişkin kişisel verilerin yayılmasının önlenmesi talebini de kapsamaktadır.[221] Sonuç olarak kişi, kendisine ait ancak hatırlanmasını istemediği verilerin silinmesini istemek suretiyle kendi verileri üzerinde bir kontrol yetkisine sahip olmaktadır.[222]

6.6. Verilerin İşlenme Şartları

6698 sayılı Kanun'un 5. ve 6. maddelerinde kişisel veriler ile özel nitelikli kişisel verilerin işlenebilme şartları düzenlenmiştir. Böylece günümüzde kullanım alanları gittikçe genişleyen kişisel verilerin hangi hallerde hukuka uygun bir şekilde işleneceği belirlenmiş olup veri sorumuluları ile veri işleyenler açısından dikkate alınması gereken koşullar ortaya konulmuştur.

---

[219] YARGITAY HUKUK GENEL KURULU E. 2014/4-56 K. 2015/1679 T. 17.6.2015 Ayrıca kararda bireyin isminin kişisel veri olduğu da vurgulanmak suretiyle 4 yıl önce gerçekleşen cinsel saldırı suçunun mağduru olan kişinin isminin rumuzlanmadan kitapta yayınlanması fiilinin unutulma hakkından yola çıkılarak özel hayatın gizliliğini ihlal ettiği sonucuna varılmıştır. Kararda ayrıca görüşmeler sırasında azınlıkta kalan bazı üyelerin mahkeme kararlarındaki isimlerin rumuzlanmasına gerek olmadığı, yargılamanın istisnai haller dışında açık bir şekilde yapıldığını savunmuş oldukları ancak burada sorunun mahkeme kararında isimlerin rumuzlanması değil; kararın kitaba alınırken isimlerin rumuzlanması gerekip gerekmediği olduğundan bu görüşün çoğunluk tarafından kabul edilmediği belirtilmiştir. Diğer kararlar için bkz. YARGITAY 19. CEZA DAİRESİ E. 2018/8285 K. 2019/5447 T. 11.3.2019; YARGITAY 19. CEZA DAİRESİ E. 2019/23945 K. 2019/7563 T. 29.4.2019; AYM NBB Bireysel Başvuru Kararı, pg 45, R.G. Tarih ve Sayı: 24/8/2016-2981

Diğer tanımlamalar için bkz. Serdar Gülener, **Dijital Hafızadan Silinmeyi İstemek: Temel Bir İnsan Hakkı Olarak "Unutulma Hakkı"**, TBB Dergisi 2012 (102), s.226; Kişisel Verileri Koruma Kurumu, **Unutulma Hakkı (Unutulma Hakkının Arama Motorları Özelinde Değerlendirilmesi)**, s.9; Unutulma hakkının özel hayatın gizliliği ile ilişkisi hakkında bkz. Kübra Kaya, **Özel Hayatın Gizliliği Hakkı ile Kişisel Verilerin Korunması Hakkı Bağlamında Ortaya Çıkan Bir Hak Olarak Unutulma Hakkının Değerlendirilmesi,** TİHEK Akademi Dergisi, Yıl:5 Sayı:8 -2022, s.177-196

[220]YARGITAY 19. CEZA DAİRESİ E. 2016/15510 K. 2017/5325 T. 5.6.2017

[221] Tevfik Sönmez Küçük, **Bir Anayasal Hak Olarak Unutulma Hakkı**, Avrupa Ve Türk Hukukunda Kişisel Verilerin Korunmasına İlişkin Güncel Sorunlar Uluslararası Sempozyum (Bildiri Özetleri), s.22; Halise Şerefoğlu Henkoğlu, **Unutulma Hakkı: Dijitalleşme Sürecinde Bilgiye ErişimÖzgürlüğünü Tehdit Eder mi?**, Bilgi Sistemleri Ve Bilişim Yönetimi Beklentiler ve Yeni Yaklaşımlar s.191

[222] Aydın Akgül, **Kişisel Verilerin Korunmasında Yeni Bir Hak: "Unutulma Hakkı" Ve AB Adalet Divanı'nın "Google Kararı"** (Hakemli Makale) TBB Dergisi 2016 (116), s.11; Ayşe Nur Akıncı, **Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi**, İktisadi Sektörler ve Koordinasyon Genel Müdürlüğü Bilgi Toplumu Dairesi Başkanlığı, Haziran 2017, s.34

6.6.1. Kişisel Verilerin İşlenme Şartları

KVKK'nin beşinci maddesinde özel nitelik taşımayan kişisel verilerin işlenebileceği haller sayılmıştır. Maddenin ilk fıkrasında açık rıza şartı düzenlenmişken 2. fıkrada açık rıza olmadan söz konusu verilerin işlenebileceği yedi hal yer almıştır.

KVKK'de sayılan veri işleme şartlarına geçmeden önce kişisel verilerin işlenmesi ilkeleri ile veri işleme şartları arasındaki ilişkiye değinmekte fayda görüyoruz. Kişisel verilerin işlenmesinden söz edildiği bir yerde öncelikli olarak somut olayda dikkat edilmesi gereken nokta yukarıda değindiğimiz veri işleme ilkelerinin mevcut olup olmadığının saptanmasıdır. Zira hukuka uygun bir işleme faaliyetinden söz edilebilmesi için ilk olarak genel ilkelere uygun bir işlemenin yürütülüyor olması gerekmektedir ve bu doğrultuda ancak genel ilkelere aykırı bir faaliyetin olmadığı tespit edildikten sonra kanunda sayılan kişisel verilerin işlenme şartları somut olay bazında incelenecektir. Nitekim örneğin ölçülülük ilkesine aykırı bir işleme faaliyeti açık rıza alınarak hukuka uygun hale getirilemeyecektir. Çünkü genel ilkelerden sayılan ölçülülük ilkesi ihlal edildiği için o veriler hiçbir şekilde işlemeye konu olmamalıdır.[223]

6.6.1.1. Açık Rıza

Açık rıza, yukarıda da belirtmiş olduğumuz üzere önceden yapılmış bir bilgilendirmeye ve özgür iradeye dayalı, spesifik bir konuya özgü ve o konuyla sınırlandırılmış şekilde verilmiş olmalıdır. Ancak bu şartları ihtiva eden açık rıza hukuka uygunluk sebebi olarak kabul edilebilecektir.

İlgili kişinin kendi isteği ile veya karşısındaki kişinin talebi üzerine kendi verilerinin işlenmesini onaylaması şeklinde tanımlanan açık rıza, mevzuatımız kapsamında kişisel verilerin işlenmesi açısından aranan temel bir şart olarak kabul edilmiştir.[224] Açık rıza ile veri öznesi veri sorumlusuna, sahibi olduğu ve hukuk düzenince korunan hukuki değere ilişkin olarak verdiği kararı bildirmiş olup işlenecek verilerin sınırları da belirlenmiş olmaktadır. Bununla birlikte açık rıza beyanının mutlaka yazılı bir şekilde bildirilmesi gerekmeyip söz konusu beyanın, ilgili kişinin olumlu irade beyanı niteliğinde olması gerekmektedir. Ayrıca açık rızanın verilmesi hususundan doğan ispat yükümlülüğü de veri sorumlusuna aittir.[225]

---

[223] Erdinç, s.12

[224] Erdinç, s. 1-19.

[225] Kişisel Verileri Koruma Kurumu, **Açık Rıza**, 1-3; Bundan dolayı açık rızanın yazılı olarak alınmasının veri sorumlusu açısından daha yararlı olacağı hakkında bkz. Sevgi Türkmen **Özel Nitelikli Kişisel Verilerin İşlenmesinde Açık Rızanın Aranmadığı Haller**, Yüksek Lisans Tezi, İSTANBUL – 2019, s.113

Açık rızanın taşıması gereken niteliklerden ilki rıza beyanının belirli bir konuya ilişkin olarak ve ucu açık olmayacak şekilde verilmiş olmasıdır. Rızanın hangi konuyla ilgili verildiği bilinmeli ve ilgili kişinin tüm kişisel verilerinin işlenmesine yol açacak genel beyanlardan kaçınılmalıdır.[226]

Açık rıza beyanı açısından gerekli ikinci unsur ise verilecek rıza öncesinde ilgili kişiye bir bilgilendirme yapılmış olmasıdır. Rıza verecek kişinin, hangi işlemlere rıza gösterdiği ve bu rızasının sonuçları hakkında bilgi sahibi olması sağlanmalıdır. Bu kapsamda verilerin işlenme amaçları, kimlere hangi sebeplerle aktarılacağı ve toplanma yöntemlerinin yanı sıra işleme faaliyetinin hukuki sebebi ile ilgili olarak veri öznesine bilgi verilecektir. Aslında bu unsur kanunda veri sorumlusunun aydınlatma yükümlülüğü olarak karşımıza çıkmaktadır. Ayrıca bilgilendirme, kişinin anlayabileceği bir şekilde olmalı ve bu meyanda kafa karıştırıcı terimler kullanılmamalı ve bilgilendirme metninin şekli -okunması zor punto kullanılması gibi- de anlaşılabilirliğe zarar vermemelidir. Unutulmaması gereken bir diğer nokta ise açık rızanın özgür iradeye dayalı olarak verilmesi gerekliliğidir. Bu bağlamda, öncelikle veri işleme faaliyetinin tarafları arasındaki ilişki dikkate alınmalıdır. Örneğin kişinin kendini baskı altında hissedebileceği –işçi ve işveren ilişkisi gibi- durumlarda dikkatli bir şekilde değerlendirme yapılmalıdır. Son olarak rızanın bir ürün veya hizmetin sunulmasının ön şartı olarak ileri sürülmemesine de hassasiyet gösterilmelidir. Böylesi durumlarda rıza beyanı özgür bir irade temelinde verilmemiş olacağından KVKK anlamında geçerli bir açık rızadan söz edilemeyecektir.[227]

Açık rıza kavramı ile ilgili açıklamalarımızın sonuna gelirken pratikte karşılaşılan iki önemli konuya değinmek istiyoruz. Bunlardan ilki ilgili kişinin verdiği rıza beyanını geri alıp alamayacağı ve şayet geri alırsa veri sorumlusunun nasıl davranması gerektiğidir. Kişisel Verileri Koruma Kurumu, konuyla ilgili olarak yaptığı açıklamada, açık rıza vermenin kişiye sıkı sıkıya bağlı bir hak olduğunu ve kişinin istediği zaman bu rızayı geri alabilme hakkına sahip olduğunu belirtmiştir. Ayrıca Kurum, geri alma beyanının veri sorumlusuna ulaştığı andan itibaren sonuç doğuracağını ve açık rızaya dayalı olarak gerçekleştirilen tüm faaliyetlerin bu andan itibaren veri sorumlusunca sonlandırılması gerektiğini ifade etmiştir.[228]

---

[226] Rızanın belirli bir konuya ilişkin olması aslında genel ilkeler arasında sayılan amaca bağlılık ilkesi ile sıkı bağlantı içerisindedir. Bkz. Türkmen, s.112; Ayrıca belirtelim ki Kişisel Verileri Koruma Kurumu bu türden genel rıza beyanları için battaniye rıza terimini kullanmaktadır. Bkz. KİŞİSEL VERİLERİ KORUMA KURUMU | KVKK | Açık Rıza Alırken Dikkat Edilecek Hususlar (Erişim Tarihi: 11.12.2021)

[227] Kişisel Verileri Koruma Kurumu, **Açık Rıza**, s.4-6

[228] **100 Soruda Kişisel Verilerin Korunması Kanunu**, KVKK Yayınları, Nisan 2018, Ankara, s.29

Değinmekte yarar gördüğümüz diğer önemli husus ise birden fazla veri işleme amacının bulunduğu bir durumda veri sorumlusunca açık rızanın nasıl elde edilmesi gerektiğidir. Zira yukarıda da belirttiğimiz üzere battaniye rıza olarak adlandırılan ve veri sorumlusunun her türlü işleme faaliyeti için tek rıza alması anlamına gelen rıza alma yöntemleri kanuna aykırı olacaktır. Konuyla ilgili olarak yakın zamanda gündeme gelen Watsapp uygulamasının veri işleme politikasına ilişkin yaptığı kamuoyu duyurusunda Kişisel Verileri Koruma Kurumu, açık rıza alınırken her bir işleme faaliyeti açısından seçenek sunulmak suretiyle ilgili kişilerden ayrı ayrı rıza alınması gerektiğini bildirmiştir.[229] Böylece veri sorumlusu, torba rıza alınması yöntemine başvurmayarak şeffaf bir şekilde ve veri öznesinin bilgilendirilmesini sağladıktan sonra her bir veri işleme faaliyeti için ayrı ayrı rıza alma yoluna gidecektir.

6.6.1.2. Kanunlarda Açıkça Öngörülme

Kişisel Verilerin Korunması Kanunu'nun beşinci maddesinde, kişisel verilerin işlenme şartları düzenlenirken öncelikle açık rıza şartına yer verilmiş daha sonra maddenin ikinci fıkrasında ise açık rıza aranmayan haller öngörülmüştür. Bu durumlardan ilki kişisel verilerin işlenebileceğinin kanunlarda açıkça öngörülmüş olmasıdır. Mevzuatımızın birçok yerinde teknolojinin de gelişim hızına bağlı olarak kişisel verilerle ilgili çeşitli düzenlemeler yapılmış ve kişisel verilerin işlenmesine hukuki zemin sağlayan maddeler yürürlüğe konulmuştur. Bahsi geçen hükümlerin azımsanamayacak sayıda olmasından ötürü çalışmamızın kapsamının fazla genişlememesi açısından burada önemli gördüğümüz ve uygulamada karşımıza sıklıkla çıkan hükümlere değinilecektir.

Öncelikle belirtmek gerekir ki 5271 sayılı Ceza Muhakemesi Yasası'nın 75. maddesi ve devamında şüpheli, sanık ve diğer kişilerin beden muayenesi ve vücutlarından örnek alınması hükümleri düzenlenmiştir. Söz konusu hükümlere göre gerekli diğer şartların da yerine getirilmesi ile kişilerden kan veya benzeri biyolojik örnekleri ile saç, tükürük ve tırnak gibi örnekler alınabilecektir. Aynı doğrultuda 80. maddede 75, 76 ve 78'inci maddeler kapsamında alınan örnekler üzerinde yapılan inceleme sonuçlarının kişisel veri niteliği taşıdığı belirtilmiştir. Aynı yasanın 81. maddesinde ise üst sınırı 2 yıl veya daha fazla hapis gerektiren suç söz konusu olduğunda şüpheli veya sanıktan diğer şartların da sağlanması durumunda fotoğrafı, beden ölçüleri, parmak ve avuç içi izi, bedeninde yer almış olup teşhisini kolaylaştıracak diğer özellikleri ile sesi ve görüntüleri kaydının alınabileceği düzenlenmiştir. Kimlik teşhisi için alınan bu örneklerin de kişisel veri niteliğinde olduğu aşikardır.

[229] https://www.kvkk.gov.tr/Icerik/6856/WHATSAPP-UYGULAMASI-HAKKINDA-KAMUOYU-DUYURUSU

Adli Sicil Kanunu'nun bazı maddelerinde kişilere ait verilerin işlenebileceği haller düzenlenmiştir.[230] Öncelikle belirtelim ki kişilerin ceza mahkumiyeti ve güvenlik tedbirleriyle ilgili veriler KVKK'nin 6. maddesi uyarınca özel nitelikli kişisel veri kategorisinde değerlendirilmektedir.

5352 sayılı Adli Sicil Kanunu'nun 4. maddesinde adli sicile kaydedilecek bilgiler sayılmış ve adli sicil bilgilerinin Adalet Bakanlığı Adlî Sicil ve İstatistik Genel Müdürlüğündeki Merkezî Adlî Sicilde tutulacağı öngörülmüştür. Bu bağlamda söz konusu kanun kapsamında belirtilen bilgileri kaydetmekle görevli kişi tarafından yukarıda değindiğimiz kişisel verilerin sisteme girilerek kaydedilmesi hukuka uygun bir işleme faaliyeti olacaktır.[231] Bunun yanında Adli Sicil Kanunu'nda düzenlen adli sicil bilgilerinin verilebileceği ve silineceği hallerde de KVKK'de sayılan kanunlarda açıkça öngörülme şartı gerçekleşmiş olacak ve veri işleme faaliyeti hukuka uygun olarak gerçekleşecektir.

Kişisel verilerin işlenmesine olanak sağlayan diğer önemli bir düzenleme ise Nüfus Hizmetleri Kanunu'nda yer almaktadır. Söz konusu kanunda nüfus kütüklerinin ne şekilde ve kimler tarafından tutulacağı düzenlenmiştir. Buna göre kişilerin kimlik numarası, adı, soyadı, cinsiyeti, doğum yeri ve tarihi, dini, medeni hali, yerleşim yeri, biyometrik verisi ve fotoğrafı gibi birtakım bilgiler yetkili kişi ve kurumlarca kaydedilecektir.[232] Aynı kanunda düzenlenen MERNİS ve Kimlik Paylaşım Sistemi gibi sistemler aracılığıyla da birçok kişisel veri işlenmektedir.

Kişisel verilerin işlenmesini hukuka uygun hale getiren kanunlar özelinde son olarak Sivil Havacılık Kanunu'na değinmek istiyoruz. 2920 sayılı Sivil Havacılık Kanunumuzun 40. maddesinde yer alan düzenlemeye göre seyahat edecek kişilerin bilgileri seyahatlerini kolaylaştırmak veyahut güvenlik ve risk değerlendirmesi yapılması amacıyla KVKK kapsamında toplanabilecek, işlenebilecek, paylaşılabilecek ya da kaydedilebilecektir. Ayrıca belirtilmelidir ki özellikle son yıllara damgasını vuran Covid-19 salgını nedeniyle oldukça büyük zarar gören havacılık sektöründe, havayolu taşımacılığını canlı tutabilmek adına alternatif yöntemler geliştirilmekte ve bu kapsamda daha fazla kişisel veri işleme faaliyeti gerçekleştirilmektedir. Örneğin virüsün bulaşmasını en aza indirecek şekilde kişilerin temasını asgari düzeye indirmek amacıyla yolcuların göz ve yüz tanıma sistemlerinden geçerek seyahat

---

[230] Örneğin Adlî sicil bilgilerinin verilebileceği kişiler yedinci maddede şu şekilde düzenlenmiştir: *"(1) Adlî sicil bilgileri, kullanılış amacı belirtilmek suretiyle; a) İlgili kişiye veya vekâletnamede açıkça belirtilmek koşuluyla vekiline, b) Kamu kurum ve kuruluşlarına, kamu kurumu niteliğindeki meslek kuruluşlarına…verilebilir."*

[231] İbrahim Korkmaz**, Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, Seçkin Yayınları, 2019-Ankara, s.415-416

[232] Korkmaz, *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması*, s.417

etmeleri ya da seyahat edecek kişilerden çeşitli sağlık verilerinin istenmesi kişisel verilerin işlendiği durumlar arasında yer almaktadır.

4857 sayılı İş Kanunu kapsamında işverenin, işçiye ait özlük dosyası tutması yükümlülüğü uyarınca, işçiye ait dosyada birtakım kişisel verileri açık rıza almadan işleyebileceğine yukarıda değinmiştik.[233]

6.6.1.3. Hayat veya Beden Bütünlüğünün Korunması

KVKK'nin 5. maddesinin 2.fıkrasında yer alan şartlardan ikincisi olan fiili imkansızlık durumunda rıza olmadan veri işlenebilmesi için iki koşulun bir arada mevcut bulunması gerekmektedir. Bunlardan ilki, kişinin kendisinin yahut bir diğer kişinin hayatı ya da beden bütünlüğünü korumak için kişisel veri işlenmesinde zorunluluk olması ikincisi ise fiili imkansızlıktan dolayı kişinin rızasını açıklayamayacak durumda olması veya rızasına geçerlilik tanınmayan bir kimsenin bulunması halidir.

Madde gerekçesinde kişinin rızasını açıklayamaması veyahut açıkladığı rızaya geçerlilik tanınmaması durumunda kişisel verilerin hukuka uygun bir şekilde nasıl işleneceği belirtilmiştir. Buna göre örneğin verisi işlenecek kişinin şuurunun yerinde olmaması ya da akıl hastası olması nedeniyle rızasına geçerlilik tanınmadığı bir durumda tıbbi müdahale yapılırken sağlığının korunması amacıyla kan grubu, kullanılan ilaçlar veya önceki ameliyatlar gibi kişisel verileri işlenebilecektir.[234] Aynı şekilde kişinin hürriyetinden yoksun bırakılması durumunda o kişiyi kurtarabilmek amacıyla kendisinin veya şüphelinin telefonu/bilgisayarı gibi araçlar üzerinden yer tespiti için kişisel veriler işlenebilecektir.[235]

6.6.1.4. Sözleşmenin Kurulması veya İfası

Günümüzde özellikle online alışveriş pazarının bir hayli genişlemesiyle birlikte kişiler arası sözleşmelerin çeşidi ve sayısında artış meydana gelmiştir. Bunun bir sonucu olarak ise söz konusu sözleşmelerin gerek kurulumu gerekse ifası aşamalarında sözleşmenin taraflarına ait kişisel veriler fazlaca işlenmektedir.

---

[233] Türkmen, s.178

[234] Ancak madde gerekçesinde verilen bu örnekler özel nitelikli kişisel veri kategorisine ait olduğundan yanıltıcıdır. Buna binaen özel nitelikli veri vasfına sahip sağlık verileri fiili imkansızlık durumu gerekçe gösterilerek işlenemeyecektir. Bkz. Dülger, *Kişisel Verilerin Korunması Hukuku*, s.395

[235] Türkiye Büyük Millet Meclisi, Sıra Sayısı: 117, **Kişisel Verilerin Korunması Kanunu Tasarısı, (1/541) ve Adalet Komisyonu Raporu**, s.8; Bu şekilde aslında varsayılan rızaya geçerlilik tanındığı yönünde bkz. Melike Köse Aysun, **Kişisel Verilerin Kaydedilmesi Suçu**, Seçkin Yayınları, Kasım 2018, s.166

Sözleşme taraflarının kişisel verilerinin işlendiği durumlar arasında en sık karşılaşılanlardan biri ise internet üzerinden yapılan satış sözleşmeleridir. İlgili sözleşmenin taraflarca onaylanması ile birlikte işlenmesi gerekli olan kişisel veriler açısından gerçekleştirilecek işleme faaliyeti için ayrıca bir rıza alınması gerekmediği gibi sözleşmeye verilen onay beyanı, veri işlenmesini de kabul etme anlamını taşıyacaktır. Örneğin, satış sözleşmesinde ürünü satın alan kişiye satım konusu eşyanın alıcıya ulaştırılması için alıcının adres verisinin işlenmesi açısından tekrardan rıza alınması gerekmeyecektir.[236] Ayrıca düzenlenen sözleşme uyarınca yapılacak ödeme için hesap numarası alınması ya da bankaların akdettiği kredi sözleşmeleri açısından kredi alan kişinin maaş bordrosu gibi kişisel verilerini içeren belgeleri istemesi de sözleşme ile ilgili veri işlemeye örnek olarak gösterilebilecektir.[237]

6.6.1.5. Hukuki Yükümlülüğün Yerine Getirilmesi

Veri sorumlusunun kendisine yüklenen hukuki yükümlülükleri yerine getirmesi sırasında veri işleme açısından bir zorunluluk doğar ise ilgili kişinin rızasına ihtiyaç duyulmadan kişisel veriler işlenebilecektir. Madde gerekçesinde ise ç bendinde sayılan kişisel veri işleme şartı için örnek olarak firmanın kendi çalışanına maaş ödemesi yapabilmesi amacıyla hesap numarası verisinin işlenmesi hali gösterilmiştir.[238] Ayrıca bu örnekte dikkatten kaçırılmaması gereken bir nokta da işveren ve işçinin arasında kurulan sözleşme ilişkisine dayanılarak işçinin kişisel verisinin işlenmekte olduğudur. Burada aslında iki ayrı veri işleme şartının iç içe geçtiği görülmektedir. Veri sorumlusunca hukuki yükümlülük kapsamında kişisel veri işlenmesinin sıkça karşımıza çıktığı yerlerden birisi de mahkemeler gibi resmi merciler tarafından veri sorumlusundan birtakım kişisel verilerin istenmesi durumudur.[239] Özellikle savcılık makamlarınca dolandırıcılık suçlarında banka hesap bilgilerinin ilgili bankalardan sorulması, sahte telefon hattı çıkarma vakalarında cep telefonu operatorü şirketlerinden abone bilgilerinin talep edilmesi yahut sahtecilik suçlarında kişinin farklı kurumlar nezdinde bulunan ve mukayeseye elverişli yazı ve imza örneği içeren evrakın istenmesi sıkça karşılaşılan örneklerdir.

[236] Küzeci, *Kişisel Verilerin Korunması,* s.344

[237] Türkiye Büyük Millet Meclisi, Sıra Sayısı: 117, **Kişisel Verilerin Korunması Kanunu Tasarısı, (1/541) ve Adalet Komisyonu Raporu**, s.9

[238] Türkiye Büyük Millet Meclisi, Sıra Sayısı: 117, Kişisel Verilerin Korunması Kanunu Tasarısı, (1/541) ve Adalet Komisyonu Raporu, s.9

[239] Dülger, *Kişisel Verilerin Korunması Hukuku*, s.402-403

6.6.1.6. Verinin Alenileştirilmiş Olması

Kişisel verilerin işlenme şartlarından bir diğeri verinin, veri öznesi tarafından alenileştirilmiş olması yani herhangi bir şekilde kamuoyuyla paylaşılması durumudur. Artık diğer kişiler tarafından öğrenilebilecek bir forma giren verinin bu şekliyle işlenmesi halinde korunması ile beklenen hukuki değerin artık mevcut olmayacağı kabul edilmektedir.[240]

Kişinin kendisi tarafından aleni hale getirilmiş bir kişisel verinin kullanımında son derece dikkatli olunmalıdır. Zira verinin alenileştirilmiş olması onun her türlü kullanıma açıldığını veya veri öznesince diğer kişiler tarafından yapılacak bütün veri işleme faaliyetlerine rıza gösterildiği anlamına gelmemektedir.

Aleni hale getirilen kişisel verinin işlenmesinde öncelikli olarak dikkat edilmesi gereken husus bu verinin ilgili kişi tarafından mı yoksa farklı üçüncü kişilerce mi alenileştirildiğinin tespit edilmesidir. Nitekim diğer kişilerce yapılan alenileştirme, verinin açık rıza olmaksızın işlenmesini hukuka uygun hale getirmeyecektir. Burada unutulmaması gereken ise ilgili kişinin kendi verisini alenileştirmesinde güttüğü amaçtır. Söz konusu amacın belirlenmesi, aleni hale gelmiş o verinin diğer kişiler tarafından işlenmesinin sınırlarını oluşturmaktadır. Çünkü bahsi geçen bu amaç dışındaki kullanımlar hukuka aykırı olarak kabul edilecektir.[241] Bu kapsamda alenileştirme amacı ve alenileştirmenin hangi bağlamda meydana geldiği her somut olaya göre ayrı ayrı değerlendirilmelidir.[242]

Alenileştirme konusuyla ilgili olarak bu noktada Yargıtay Ceza Genel Kurulunun 17.06.2014 tarihli kararına değinmekte fayda görüyoruz. Söz konusu karara konu olayda, yerel bir gazetenin köşe yazarı olan kişinin gazetede yer alan fotoğrafı kendi rızası olmadan bir arkadaşlık sitesine konarak erkek arkadaş aradığı şeklinde bilgilerle birlikte yayınlanmıştır. Ceza Genel Kurulu, olayda herhangi bir hukuka uygunluk nedeninin bulunmadığını ve bu şekliyle köşe yazarının fotoğrafının yayınlanması eyleminin hem alenen hakaret suçunu hem de kişisel verileri hukuka aykırı olarak yayma suçunu oluşturduğu kanaatine varmıştır. Ancak karşı oy yazısında öncelikle katılanın, kendi fotoğrafının arkadaşlık sitesinde yayınlanmasından haberdar olmasından sonra ilgili fotoğrafı o siteye koyan sanıklarla konuşması üzerine fotoğrafının 48 saat içerisinde websitesinden kaldırılmasının su üzerine yazı yazmak gibi bir şey

[240] Türkiye Büyük Millet Meclisi, Sıra Sayısı: 117, Kişisel Verilerin Korunması Kanunu Tasarısı, (1/541) ve Adalet Komisyonu Raporu, s.9

[241] Dülger, *Kişisel Verilerin Korunması Hukuku*, s.405-406. Yazar ayrıca amacın belirlenmesinde ilgili kişinin beyanının dikkate alınmasını şayet beyanı yoksa dürüstlük kuralına göre bir belirleme yapılması gerektiğini belirtmektedir.

[242] Habip Bozkurt, **Kişisel Verilerin İşlenmesinin Hukuki Boyutu**, Yüksek Lisans Tezi İstanbul, Mayıs, 2019, s.105

olduğu, katılanın görev yaptığı gazetede kendi fotoğrafını köşe yazısına koyuyor oluşunun fotoğrafın alenileştirilmesi anlamına geldiği, bu durumla bağlantılı olarak halen kanunlaşmayı bekleyen Kişisel Verileri Koruma Kanunu tasarısında ilgili kişi tarafından aleni hale getirilen verinin açık rıza olmadan işlenebileceğinin belirtildiği ve son olarak ilgili kişinin her türlü yazılı, görsel, işitsel ve elektronik kitle ileşitim (TCK'nın 6/1-9) okyanusuna bıraktığı bir kişisel verisinin hangi okyanus, deniz, göl, gölet ve bataklığa gireceğine artık engel olamayacağı ve artık bu aşamada ortaya çıkan başka suçların araştırılması gerektiği ifade edilmiştir.[243]

6.6.1.7. Hakkın Tesisi, Kullanılması veya Korunması

İlgili kişinin açık rızası olmadan kişisel verilerinin işlenebileceği diğer bir hal ise bir hakkın tesisi, kullanımı veyahut korunmasında işleme faaliyetinin zorunluluk arz etmesi durumudur. Buradaki hakkın kime ait olduğu noktasında maddenin metninde ya da gerekçesinde bir açıklık getirilmemiştir. Söz konusu hakkın ilgili kişiye mi ait olduğu yoksa veri sorumlusunun hakkı mı olduğu açıklanmamıştır.[244] KVKK'nin 5/2-e bendinde sayılan işleme şartına örnek olarak -madde gerekçesinde- bir şirkete kendi çalışanının açtığı davada şirketin, çalışanının verilerini ispatlama faaliyeti için kullanması veya kısıtlı bir kişinin menfaatlerinin korunması için vasisinin kısıtlının mali bilgilerini kullanması verilmiştir.[245] Diğer bir örnek olarak ise ticari ilişkiden doğan bir alacağın takibi amacıyla borçlunun bazı bilgilerinin kullanılması suretiyle icra takibi başlatılması durumu gösterilebilecektir.[246]

6.6.1.8. Veri Sorumlusunun Meşru Menfaati

İlgili kişinin açık rızası olmadan kişisel verilerinin işlenebileceği son hal ise veri sorumlusunun meşru menfaatleri açısından veri işlenmesinde zorunluluk bulunması durumudur. Ayrıca böylesi durumlarda verisi işlenen ilgili kişinin temel hak ve özgürlüklerine zarar verilmemesi gerekmektedir. Örneğin, bir şirketin, kendi çalışanlarının verilerini, maaş zamları, terfi etme durumları veya işletmenin yeniden yapılandırılması ile ilgili olarak işlemesi veri sorumlusunun meşru menfaatinin söz konusu olduğu durumlardandır.[247] Ayrıca şirket içi rekabetin artırılması amacıyla ayın elemanı seçimi gibi uygulamalarda da kişisel verilerin işlenmesi, meşru menfaatin bulunduğu hallerden sayılmaktadır. Son olarak belirtmek gerekir ki veri

[243] Yargıtay E. 2012/12-1510, K. 2014/33,1 T.17.06.2014
[244] Bozkurt, s.105
[245] Türkiye Büyük Millet Meclisi, Sıra Sayısı: 117, Kişisel Verilerin Korunması Kanunu Tasarısı, (1/541) ve Adalet Komisyonu Raporu, s.9
[246] Nevzat Ali Anı, **Kişisel Verilerin İşlenmesi ve Açık Rıza**, Yüksek Lisans Tezi, İstanbul, 2018, s.114
[247] Türkiye Büyük Millet Meclisi, Sıra Sayısı: 117, Kişisel Verilerin Korunması Kanunu Tasarısı, (1/541) ve Adalet Komisyonu Raporu, s.9

sorumlusunun meşru menfaatinin mevcut olduğu tüm durumlarda kişisel verilerin işlenebileceği gibi bir sonuca ulaşılması isabetli olmayacaktır. Veri işleme faaliyetinin gerçekleştirilebilmesi için veri sorumlusunun meşru menfaati bakımından bir zorunluluk da bulunmalı ve temel hak ve özgürlükleri daha az ihlal eden bir seçenek var ise bu yol tercih edilmelidir.[248]

6.6.2. Özel Nitelikli Kişisel Verilerin İşlenme Şartları

Kişisel Verilerin Korunması Yasası'nın 6. maddesinde özel nitelikli kişisel verilerin işlenme şartları düzenlenmiştir. Özel nitelikli kişisel verilerin işlenmesi açısından Kanunumuzun öngördüğü ana kural açık rıza olmadan söz konusu verilerin işlenemeyeceğidir. Buna ek olarak ise maddede açık rızanın olmadığı hangi hallerde hassas verilerin işlenebileceğini vaz eden koşullar yer almıştır. Özel kategoride yer alan veriler için öngörülen ana kuralı oluşturan açık rıza şartına önceki başlıklarda ayrıntılı olarak değinildiği için bu başlık altında tekrardan yer verilmeyecek ve açık rıza bulunmaksızın gerçekleştirilebilecek işleme faaliyetleri irdelenecektir.

KVKK'nin özel nitelikli kişisel verilerin işlenme şartları başlıklı altıncı maddesinde açık rıza olsun veya olmasın hassas verilerin işlenmesinde genel bir şart olarak Kişisel Verileri Koruma Kurulunca belirlenen önlemlerin sorumlu kişilerce alınması durumu belirtilmiştir.

Özel kategorideki verilerin taşıdığı önem göz önüne alındığında bu verilerin işlenmesi neticesinde meydana gelecek zararın ciddi nitelik taşıyacak olmasından ötürü hassas veriler için farklı tedbirlerin alınması gerekliliği ortaya çıkmaktadır. Bu kapsamda veri sorumlusunca veri güvenliğine ilişkin olarak yerine getirilmesi gereken başlıca yükümlülükler 12. maddede yer alan; kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak ile son olarak veri sorumlusunun kendi kurum veya kuruluşunda bu Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak olarak belirtilebilir.[249]

Kişisel Verileri Koruma Kurulunun özel nitelikli veriler ile ilgili olarak veri sorumlularınca alınması gereken yeterli önlemleri belirlediği kararı 7 Mart 2018 Tarihli ve 30353 Sayılı Resmî Gazete'de yayınlanmıştır. Bu karar uyarınca veri sorumluları öncelikle hassas verilerin güvenliğine yönelik ayrı bir politika ve prosedür belirlemeli, bahse konu verilerin işlenmesi aşamasında görev alan çalışanlara düzenli bir şekilde eğitimler verilmeli, bu çalışanlarla gizlilik

[248] Avcı, s.71

[249] Türkmen, s.121-122

sözleşmeleri yapılmalı, verilere erişebilme yetkisi olan kişilerin bu yetkilerinin kapsam ve süreleri belirlenmeli, görevi değişen veya işten ayrılan çalışanların söz konusu yetkileri hemen kaldırılmalı ve kendisine daha önceden verilen veri envanteri geri alınmalı ve son olarak düzenli aralıklarla yetki kontrolleri yapılmalıdır. Kararın devamında ise özel nitelikli verilerin işlendiği, erişildiği ve/veya muhafaza edildiği ortamların fiziksel yahut elektronik olmasına göre bir ayrıma gidilerek alınacak önlemler belirtilmiş ve bu verilerin aktarılmasında uyulacak tedbirler açıklanmıştır. Kararda son olarak Kurumun internet sitesinde yayınlanan Kişsiel Veri Güvenliği Rehberinde düzenlenen teknik ve idari tedbirlerin de dikkate alınması gerektiği yer almıştır.[250]

Özel nitelikli verilerin işlenmesi açısından öngörülen genel şart olan Kişisel Verileri Koruma Kurulunca belirlenen önlemlerin alınması koşuluna değindikten sonra açık rıza olmadan hassas verilerin hangi durumlarda işlenebileceği konusuna dikkat çekmek istiyoruz. Bu noktada KVKK'de ikili bir ayrıma gidilmiştir. Şöyle ki sağlık ve cinsel hayat ile ilgili veriler farklı bir rejime tabi tutulurken diğer özel nitelikli veriler olan ırk, etnik köken, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançlar, kılık ve kıyafet, dernek, vakıf ya da sendika üyeliği, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili veriler ile biyometrik ve genetik veriler için başkaca bir usul öngörülmüştür.

Öncelikle sağlık ve cinsel hayatla ilgili veriler dışındaki hassas verilerin açık rıza aranmadan ancak kanunlarda belirtilen durumlarda işlenebileceğini belirtmemiz gerekir.[251] Yasalarımızda bu türden verilerin işlenmesine cevaz verilen birçok hüküm bulunmakla birlikte burada sıkça karşımıza çıkan bazı örneklere değinilecektir. Bu kapsamda öncelikle 2559 sayılı Polis Vazife ve Salahiyet Kanunu'nun 5. maddesine ihtimam gösterilmesi gerekir. Zira maddede polise parmak izi alma yetkisi tanınmıştır. Bunun yanında Adli Sicil Kanunun'da da kişilerin ceza mahkumiyetlerine ilişkin verilerin rıza gerekmeden işlenebileceği durumlar düzenlenmiştir. Aynı şekilde CMK'nin 81. maddesinde yer alan fiziki kimliğin tespiti ile ilgili hükümler de birtakım özel nitelikli verilerin işlenebileceğini öngörmektedir. [252]

Kişisel Verilerin Korunması Kanunu'nda özel nitelikli verilerin açık rıza olmadan işlenmesi için öngörülen ayrımın ikinci alt başlığı sağlık ve cinsel hayata ilişkin verileri konu almaktadır.

---

[250] Kişisel Verileri Koruma Kurulunun 31.01.2018 tarihli ve 2018/10 sayılı kararı

[251] Doktrinde genel nitelikli kişisel veriler açısından açık rıza olmadan işlenebilme şartı olarak "kanunlarda açıkça öngörülme" hali sayılmışken özel kategorideki veriler açısından sadece "öngörülmüş olma" şeklinde bir belirleme yapılmasının özel nitelikli verilerin korunması ilkesine aykırılık oluşturacağı ve madde gerekçesi dikkate alınarak kanunun lafzının kanunlarda açıkça öngörülme şeklinde anlaşılması gerektiği ifade edilmiştir. Buna ek olarak yasalarda açıkça öngörülmesi gereken hususun yalnızca hassas verinin işlenebileceğinin değil; bu verilerin açık rıza alınmadan işlenebileceği olduğu belirtilmektedir. Bkz. Türkmen, s.172-173

[252] Türkmen, s.174-175

Şöyle ki sağlık ve cinsel hayata ilişkin bilgilerin açık rıza olmaksızın işlenebilmesi için birden fazla şart bir arada sağlanmış olmalıdır. Bunlar; sağlık veya cinsel hayata ilişkin bir verinin bulunması, kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacının bulunması ve son olarak sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından bir işleme faaliyeti olmasıdır.

7. Kişisel Verilere İlişkin Uluslararası Düzenlemeler

7.1. Genel Olarak

Globalleşen dünyada teknolojinin süratli değişimi ve gelişimi neticesinde ülkelerin birbirleriyle olan ilişkileri (özellikle ekonomi alanında) daha da sıkılaşmıştır. Artık alışılagelmiş ticaret anlayışı değişmekte ve elektronik ortamla birlikte internetin etkisi de günden güne ülkeler arası işlemlerde artmaktadır. Ayrıca, İnstagram, Twitter, Facebook gibi sosyal medya siteleri de bireylerin gündelik hayatında vazgeçilmezler arasında yer almaktadır.[253] Nitekim son yıllarda kullanıcı sayıları milyarları bulan söz konusu platformlar siyasetten ekonomiye birçok alan üzerinde ciddi etkiler uyandıracak bir hal almıştır. Ancak gerek ülkeler arası ilişkiler olsun gerekse sosyal medya siteleri olsun bahsettiğimiz faaliyetlerin sürdürülmesi esnasında sayısız kişisel veriye ihtiyaç duyulmaktadır. Nitekim aynı doğrultuda kişilerin veri güvenliğine ilişkin endişeleri de giderek artmaktadır.[254] Zira özellikle sosyal medya, kişisel bilgilerin toplanmasını, kişilerin bu platformlardaki hareketlerinin izlenmesini, kişilerin konumları ve aktiviteleri gibi bilgilerinin toplanmasını kolaylaştırmıştır.[255] Meydana gelen tüm bu gelişmelerin ve beraberinde gelen veri güvenliği ve mahremiyete ilişkin endişelerin sonucu olarak uluslararası alanda birtakım düzenlemeler yapılmıştır.

---

[253] Hootsuite and We Are Social tarafından Ocak 2018'de yayınlanan rapora göre dünya genelinde yaklaşık 4 milyar internet kullanıcısı var iken sosyal medya kullanıcı sayısı 3.2 milyar kişidir. Bkz. **We Are Social and Hootsuite Report**, Digital In 2018, s.7; Hızla değişen teknoloji, giderek artan istek ve ihtiyaçlar, birtakım iletişim araçlarının gelişmesini sağlamıştır. Bu iletişim araçları artık günümüzde iyice popüler olan internet ve internet üzerinden sosyal paylaşım ağlarıdır. Bkz. Başak Solmaz/Gökhan Tekin/ Züleyha Herzem/Muhammed Demir, **İnternet ve Sosyal Medya Kullanımı Üzerine Bir Uygulama**, Selçuk Üniversitesi İletişim Fakültesi Akademik Dergisi, Cilt 7, Sayı 4 (2013), s.23

[254] Uyarer, *Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması*, s.42-43; Facebook, politika alanında danışmanlık hizmeti veren ve 2016 Amerika başkanlık seçimlerinde Başkan Donald J. Trump için çalışan Cambridge Analytica ile 87 milyon kullanıcının bilgilerini paylaşmıştır. Skandalın ortaya çıkmasının ardından Facebook CEO'su Mark Zuckerberg Amerikan Senatosu ve Avrupa Parlamentosu'nda ifade vermiş ve Facebook'un hisseleri büyük düşüş yaşamıştır. Bkz.https://www.bbc.com/news/technology-43649018 (14.09.2018 tarihinde erişildi.)

[255] U.S. Gov't Accountability Office, Information Resellers: **Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace** (2013) s.1

7.2. OECD

Kişisel verilerin korunması hakkının ayrıca spesifik bir şekilde ele alınarak birtakım uluslararası ölçütlerin ortaya konulmasına dair ilk çalışma Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD) tarafından yayınlanan 1980 Gizliliğin Korunması ve Sınır Ötesi Kişisel Veri Akışları Hakkında Rehber İlkelerdir.[256] Söz konusu Rehber İlkeler OECD üyesi olan ülkelerin yanında üye olmayan devletlerdeki düzenlemeleri de etkilemiştir. Rehber ilkelerin hazırlanmasında ise OECD üyesi ülkelerin mahremiyetin korunması ile ilgili düzenlemelerinde görülen farklılıklar etkili olmuştur. Zira söz konusu düzenlemelerdeki birbirinden farklı anlayışlar ülkeler arası veri aktarımında çeşitli engellere sebebiyet vermiştir. Ayrıca belirtilmelidir ki bu türden veri akışları son yıllarda bilgisayar ve iletişim teknolojisindeki gelişmelere bağlı olarak büyük bir artış göstermiştir. OECD de ulusal regülasyonlar arasındaki bu farklılıkları gidermek ve ülkeler arası veri dolaşımı ile kişisel verilerin korunması noktasında bu türden düzenlemeler arasında uyumun sağlanması amacıyla bahsi geçen ilkeleri ortaya koymuştur.[257]

Rehber İlkeler, öncelikle asgari ölçütleri belirledikten sonra ulusal düzeyde kişilerin özel hayatının ve veri güvenliğinin korunması ile kişilerin özgürlüklerinin korunmasını ilgilendiren ana kuralları düzenlemiş ardından üye ülkeler arası ilişkileri ilgilendiren prensiplere yer vermiştir. İlkelerin devamında söz konusu kuralların eşit şekilde uygulanmasının yanı sıra üye ülkeler arası özellikle veri paylaşımı yoluyla yardımlaşma ve kişisel verilerin korunmasıyla bağdaşmayan ulusal düzenlemelerden kaçınmaya ilişkin prensipler düzenlenmiştir.[258]

7.3. BM

Birleşmiş Milletler nezdinde 14 Aralık 1990'da Bilgisayarla İşlenen Kişisel Veri Dosyalarına İlişkin Rehber İlkeler yayınlanmıştır. Söz konusu çalışmada, bilgisayarlaşmanın insanın özel hayatının yanında diğer özgürlüklerini de etkilediği ve kişinin, mahremiyetinin haricinde günlük hayatında kendisinin de tehdit altında olabileceği belirtilmiştir.[259] Rehber İlkelerde, kişisel verilerin hukuka uygun olarak toplanması ve işlenmesi, toplanan verilerin güncellik durumunun düzenli olarak kontrol edilmesi, verilerin işlenme amaçlarının belirli olması, ilgili kişinin kendisiyle ilgili bilgilerin işlenip işlenmediğini öğrenme hakkı, bazı hassas verilerden ötürü

[256] Bük, s.65-66

[257] The OECD Privacy Framework, **Chapter 3. Original Explanatory Memorandum To The OECD Privacy Guidelines**, 2013, s.19,39

[258] The OECD Privacy Framework, **Chapter 3. Original Explanatory Memorandum To The OECD Privacy Guidelines** (1980), 2013, s.47

[259] UN Economic and Social Council, **Commentary on Proposed Amendments**, E/CN.4/Sub.2/1988/22 s. 4

ayrımcılık yapılmaması kuralı, verilerin korunması hususunda gerekli tedbirlerin alınması ve yurt dışına veri aktarımı ile ilgili kurallar yer almıştır.[260]

7.4. 108 Sayılı Sözleşme

Tam ismi 108 no'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Gerçek Kişilerin Korunmasına Dair Sözleşme olan bu düzenleme 1981 yılında ülkemizce de imzalanmış ve Mart 2016'da 29656 sayılı Resmi Gazete ile iç hukukumuza dahil edilmiştir. Söz konusu sözleşme hem kamusal hem de özel sektörü kapsamına almakla birlikte yalnızca otomatik yollarla işlenen verileri koruma altına almaktadır. Bununla birlikte taraf devletler Sözleşme'nin 3. maddesi uyarınca işbu sözleşme hükümlerini otomatik olmayan veri işleme işlemlerine de uygulayabilecektir.[261]

108 Sayılı Sözleşme, Avrupa Konseyi tarafından 28 Ocak 1981 tarihinde kabul edilmiştir ve kişisel verilerin koruma altına alınması noktasında bağlayıcı nitelikte olan ilk uluslararası düzenleme olarak kabul görmektedir. Söz konusu Sözleşme Avrupa Konseyi tarafından kabul edilmiş olmakla birlikte ihtiva ettiği 23. madde ile Avrupa Konseyi'ne üye olmayan devletlerin de belirli şartlar dahilinde Sözleşme'ye taraf olabileceklerini hüküm altına almıştır.[262]

108 sayılı Sözleşme'nin amacı kişilerin özel hayata saygı hakkının kişisel verilerin otomatik işleme tabi tutulmasına karşısında korunması şeklinde belirtilmiştir. Sözleşme'de ayrıca taraf devletlere bu sözleşme ile kişisel verilerin korunmasına yönelik olarak belirlenen temel ilkeleri işler hale getirmek için gerekli tedbirleri alma yükümlülüğü de yüklenmiştir. Bunun yanı sıra söz konusu düzenleme ile veri güvenliğine ilişkin alınması gereken önlemler, ilgili kişinin hakları, ülkeler arası veri akışı, taraf devletler arasında iş birliği gibi konulara ilişkin çeşitli hükümler getirilmiştir.[263]

Söz konusu Sözleşme'yi imzalayan ilk ülkeler arasında yer almasına karşın Türkiye, düzenlemeyi kendi iç hukukuna dahil ederek yürürlüğe koyan son ülke olmuştur. Nitekim 6698 sayılı Kanun'un yasalaşması aşamasında bu konuyla ilgili olarak çeşitli eleştiriler de dile getirilmiştir. Ulusal hukukumuza geç bir tarihte dahil edilmesine karşın Sözleşme, özel veri koruma yasamız olan KVKK açısından yön gösterici bir niteliğe sahip olmuştur. Nitekim 108

[260] UN Economic and Social Council, **Guidelines Concerning Computerized Personal Data Files** E/CN.4/Sub.2/1988/22 21 July 1988

[261] Çiğdem Ayözger Öngün, **Kişisel Verilerin Korunması Hukuku**, 2. Baskı, İstanbul-2019, s.73-74

[262] Sedat Erdem Aydın, **AİHM İçtihatları Bağlamında Kişisel Verilerin Kaydedilmesi Suçu**, 12 Levha Yayıncılık, Aralık 2015, s.39-40

[263] 108 no'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Gerçek Kişilerin Korunmasına Dair Sözleşme, 17 Mart 2016 Tarihli ve 29656 Sayılı Resmî Gazete

Sayılı Sözleşme'nin iç hukukumuz açısından öneminin ve etkilerinin anlaşılması bakımından KVKK'nin gerekçesi bize bu noktada yardımcı olacaktır. Bu bağlamda belirtmek gerekir ki özellikle Kanun'un 19. ve 21. maddelerinin gerekçelerinde ilgili Sözleşme'ye atıfta bulunularak 108 Sayılı Sözleşme'nin hükümleri doğrultusunda bağımsız veri koruma otoritelerinin kurulduğu belirtilmektedir. Bunun sonucunda ise görevi ile ilgili konularda hiçbir makamdan emir ve talimat almayacak bir kuruluşun düzenlendiği ifade edilmiştir.[264]

7.5. Avrupa İnsan Hakları Sözleşmesi (AİHS)

Avrupa Konseyi tarafından 4 Kasım 1950 tarihinde kabul edilen Avrupa İnsan Hakları Sözleşmesi, insan haklarının korunmasına ilişkin olarak öngördüğü Avrupa İnsan Hakları Mahkemesi (AİHM) kurumu ile birlikte düşünüldüğünde temel hakların korunması noktasında son derece etkili bir konumda bulunmaktadır. Söz konusu Sözleşme'de kişisel verilere ilişkin herhangi bir spesifik düzenleme bulunmamakla birlikte Özel ve Aile Hayatına Saygı başlığını taşıyan sekizinci madde kişisel verilerin korunması açısından önemlidir. Zira AİHM, 8'inci maddenin kapsamını kişisel verileri de içine alacak şekilde geniş bir yoruma tabi tutmaktadır. Nitekim S. ve Marper v. Birleşik Krallık Davası kararında Mahkeme, kişinin özel hayatına dair verilerinin saklanmasını Sözleşme'nin 8. maddesi bağlamında bir müdahale olarak yorumlamıştır. Ayrıca aynı kararda özel hayata ve aile hayatına saygı hakkının kullanılması noktasında kişisel verilerin korunmasının büyük bir önemi haiz olduğu ve iç hukukun kişisel verilerin korunması açısından yeterli güvenceleri temin etmesi gerekliliği vurgulanmıştır.[265]

AİHM, kişisel verilerin korunmasını Sözleşme'nin 8'inci maddesi kapsamında değerlendirmekle birlikte bazı diğer kararlarında ifade özgürlüğü ile birlikte değerlendirmeye tabi tutmaktadır.

AİHS'in 10'uncu maddesinde düzenlenen ifade özgürlüğü bağlamında kişilerin herhangi bir müdahale ve sınırlamaya tabi tutulmadan düşüncelerini açıklayabilmesi hakkı düzenlenmiştir. Ancak her temel hak ve özgürlükte olduğu gibi düşünce ve ifade hürriyetinin de bazı sınırları vardır. Bu noktada değinmek gerekir ki kişisel verilerin korunması ile ifade özgürlüğünün karşı karşıya geldiği yegane çatışma noktaları basının haber verme özgürlüğü kapsamında yaptığı yayınlar ve özellikle unutulma hakkının ihlali niteliğinde sayılabilecek haberlerdir. Unutulma hakkının kişisel verilerin korunması konusu açısından değerlendirilmesi çalışmamızın daha

[264] Dülger, *Kişisel Verilerin Korunması Hukuku*, s.91; Türkiye Büyük Millet Meclisi, **Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu**, Madde Gerekçeleri, s.14-15

[265] Dülger, *Kişisel Verilerin Korunması Hukuku*, s.93; Adalet Bakanlığı Tematik Bilgi Notu, Kişisel Verilerin Korunması, 2015, s.1,12; AİHM, S. ve Marper v. Birleşik Krallık Davası Kararı (Başvuru no.30562/04 ve 30566/04)

önceki bölümlerinde ABAD'ın vermiş olduğu Google kararı bağlamında yapıldığından bu kısımda sadece AİHM'in M.L. ve W.W.v. Germany kararına değinilecektir.[266] Söz konusu karar, daha önceden işledikleri suç nedeniyle mahkum edilen başvuruculaların ceza mahkumiyetlerine ilişkin bilgilerin çeşitli medya kuruluşlarının internet sitelerinden kaldırılması taleplerine ilişkinidir. AİHM, uyuşmazlığa ilişkin olarak kişisel verilerin AİHS m.8 uyarınca koruma altına alındığını belirtmekle birlikte basının kamuoyunu bilgilendirme fonksiyonu dışında daha önceden yapılmış haberlerin arşivlenmesi gibi önemli bir görevi de olduğunu belirtmiştir. Bu kapsamda arşivlerin bilgiye erişim noktasında hatırı sayılır bir katkısının olduğu ve araştırma faaliyetleri açısından önemli bir kaynak görevi gördüğü ifade edilmiştir. Tüm bu tespitlerin sonucu olarak Mahkeme, ifade özgürlüğü bağlamında bir değerlendirme yaparak yapılan haberin basının ifade özgürlüğü kapsamında olduğunu ve kamunun başvuruya konu habere erişiminin başvuruculaların unutulma hakkına üstün tutulması gerektiği kanaatine varmıştır.[267] Bahsi geçen karar ifade özgürlüğü ile kişisel verilerin korunması hakkının dengelenmesi açısından son derece önemlidir. Zira bu iki hak, kişiler açısından son derece hassas nitelikte olmakla birlikte her vakıa kendi özelinde dikkatlice bir değerlendirmeye tabi tutulmalıdır.[268]

7.6. Avrupa Genel Veri Koruma Tüzüğü (GDPR)

Avrupa veri koruma hukuku tarihi genel bir direktif uygulamasıyla değil her ülkenin kendi ulusal düzenlemelerini hayata geçirmesiyle başlamıştır. Ülke bazında düzenleme anlayışı bir süre devam etmiş ardından özellikle Amerika Birleşik Devletleri'nin etkisinin büyük olduğu bilgi mahremiyetine ilişkin genel düzenlemeler yapma fikri etkinliğini artırmıştır.[269] Bununla birlikte aynı anlayış doğrultusunda Avrupa Birliği (AB) içerisinde kişisel verilerin kullanımı çeşitli direktiflerle düzenlemiştir. Ancak bunlardan en kapsamlı olanı, bireyin mahremiyetini ve kişisel verilerin kullanımını koruyan "AB Veri Koruma Direktifi (95/46/EC)" olmuştur. [270] Böylece Avrupa Birliği üyesi ülkeler için bilgi güvenliği ile ilgili ortak uygulanabilir kurallar ortaya konulmuştur.

---

[266] Bkz. s.57

[267] Mehmet Bedii Kaya, Unutulma Hakkı: AİHM'in Unutulma Hakkına Yaklaşımı, s.1-16; M.L. ve W.W. / Almanya (başvuru no.: 60798/10) (28.6.2018)

[268] Sinem Göçmen Uyarer, **Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması**, Seçkin Yayınları, Ankara 2019, s.23

[269] Paul M. Schwartz, **The Eu-U.S. Privacy Collision: A Turn To Institutions And Procedures**, Harvard Law Review [Vol. 126:1966, s.1969]

[270] Bkz. Nurullah Tekin, **Kişisel Verilerin Korunması ile İlgili Türkiye'deki Kanun Tasarısının Avrupa Birliği Veri Koruma Direktifi Işığında Değerlendirilmesi**, Ulusal Hakemli Uyuşmazlık Mahkemesi Dergisi, Aralık 2011, 4. Sayı, s.223

1995 tarihli Veri Koruma Direktifi, Avrupa Birliği'nde kişisel verilerin korunması anlamında bir dönüm noktası olmuştur. Ancak direktifin yayınlanmasından bu yana teknolojideki hızlı değişim ve globalleşme hayatımızı ciddi bir şekilde değiştirmiştir. Örneğin, kişilerin bilgilerinin rahatlıkla ve sayısız kullanıcıyla paylaşılmasının önü açılmış özellikle sosyal paylaşım siteleri bunun en açık örneği olmuştur. Ayrıca veri depolama yöntemleri de çeşitlenerek özel şirketlerin yanı sıra devlet makamlarının da kişisel verileri, farklı amaçlar dahilinde kullanması tetiklenmiştir.[271] Bunun sonucunda teknolojinin getirdiği tüm bu yeni gelişmelere cevap verebilmek ve kişilerin temel hak ve özgürlüklerinin korunabilmesi adına bir revizyon yapılması elzem hale gelmiştir.[272]

Avrupa Birliği'nin veri koruma kuralları birçok ülkeye referans olmuş ve bu ayrıcalıklı konumundan ötürü söz konusu kuralların dijital çağ açısından yeterli korumayı sağlaması için değişiklikler yapılması zorunluluğu doğmuştur. Bu doğrultuda 2016 yılının Mayıs ayında Avrupa Genel Veri Koruma Tüzüğü (GDPR), Avrupa Birliği Resmi Gazetesi'nde yayınlanmış ve akabinde 25 Mayıs 2018'de söz konusu tüzük yürürlüğe girmiştir.[273]

GDPR'de öncelikle tanımlar maddesi düzenlenmiş ardından kişisel verilerin işlenme şartları, açık rıza koşulları, hassas verilerin işlenme şartları, ilgili kişilerin hakları, unutulma hakkına ilişkin hükümler yer almıştır. Tüzük'ün devamında ise veri sorumlusunun yükümlülükleri, kişisel verilerin güvenliği, veri transferine ilişkin kurallar ve bağımsız veri koruma otoritelerine ilişkin hükümler bulunmaktadır.

Avrupa Genel Veri Koruma Tüzüğü, hali hazırda ulusal hukuk sistemlerinde ve 108 sayılı Sözleşme'de düzenlenmiş veri koruma kurallarını yansıtmakla birlikte bunları aynı zamanda genişletmektedir. Burada dikkate değer diğer bir husus ise GDPR'ın uygulanabilirliği meselesidir. Söz konusu Tüzük'ten önce yürürlükte bulunan 1995 tarihli Veri Koruma Direktifi, Avrupa Birliği açısından detaylı ve bir hayli geniş veri koruma sistemi öngörmüştü ancak

---

[271] Communication From The Commission to The European Parliament, The Council, The Economic And Social Committee And The Committee Of The Regions, **A comprehensive approach on personal data protection in the European Union**, Brussels, 4.11.2010 COM (2010) 609 final, s.2; Commission Staff Working Paper **Executive Summary of the Impact Assessment, Brussels**, 25.1.2012 SEC (2012) 73 final, s.2

[272] Christopher Kuner, **The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law**, Copyright 2012 By The Bureau Of National Affairs, Inc. Pvlr Issn 1538-3423, s.2; Communication From The Commission To The European Parliament, The Council, The Economic And Social Committee And The Committee Of The Regions, A comprehensive approach on personal data protection in the European Union, Brussels, 4.11.2010 COM (2010) 609 final, s.3

[273] European Data Protection Supervisor, **Annual Report 2017**, s.13; GDPR, Article 99/2; GDPR için Avrupa Veri Koruma Hukuku açısından Kopernik Devrimi benzetmesi dahi yapılmaktadır. Zira söz konusu düzenleme daha etkili bir hukuki çerçeve sunmasının yanında temel hak ve özgürlüklerin korunmasını artırmakla birlikte hukuki güvenlik de sunmaktadır.Bkz. Christopher Kuner, The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law, Privacy and Security Law Report Bloomberg BNA, s.14

Direktif, AB hukuku açısından direkt uygulanamamakta ve üye ülkelerin söz konusu direktifi uygulayabilmesi için kendi ulusal hukuk sistemlerine aktarmaları gerekmekteydi. Bunun sonucunda ise üye ülkelerin Direktifi kendi sistemlerine farklı yorumlarla adapte etmesi nedeniyle uygulamada birlik sağlanamamıştı. İşte tam bu noktada AB'deki ülkelerde direkt olarak uygulanabilir özelliğe sahip olan GDPR yürürlüğe sokularak veri koruma kuralları açısından Birlik kapsamında yeknesaklık sağlanmıştır.[274]

Tüzük, Avrupa Veri Koruma Hukukunu daha modern hale getirmiş ve dijital çağın getirdiği ekonomik ve sosyal zorluklar bağlamında bireyerin temel haklarının korunması açısından daha uyumlu bir forma sokmuştur. Buna ek olarak söz konusu regülasyon, Avrupa Birliğinde bulunmamakla birlikte AB'de bulunan veri öznelerine ürün veya hizmet sunan veri işleyenlere/sorumlularına da uygulanacaktır. Avrupa pazarında önemli paya sahip olan ve AB kapsamında milyonlarca müşterisi bulunan teknoloji şirketleri düşünüldüğünde bahsi geçen kuruluşların bu kurallara tabi tutulması kişilerin korunması açısından son derece önemlidir.[275]

GDPR, getirdiği yeni yükümlülükler ve koruma araçlarıyla özel hayatın gizliliğinin korunması için yeni bir çerçeve çizmiştir. Ayrıca kurumsal veri işleme açısından daha yüksek standartlar belirlediği için özel kategorideki verilerin işlenmesinde bireylere daha çok yetki ve "kıymet" vermektedir.[276] Zira hassas veriler, doğaları gereği, işlendiklerinde ilgili kişi açısından risk oluşturabilmekte ve genişletilmiş korumaya ihtiyaç duyulabilmektedir. Bu doğrultuda söz konusu verileri işlemek genel olarak yasaklanmıştır ve sınırlı sayıdaki durumlarda işlenilmeleri hukuka uygun olacaktır.[277]

---

[274] Handbook on European data protection law 2018 edition, s.29-30; GDPR incelendiğinde Avrupa genelindeki veri koruma yasaları açısından 95/46/EC sayılı Direktif'e nazaran daha geniş bir kapsamda uyumlaşma hedeflendiği görülmektedir. Bkz. Lothar Determann, **Kişisel Verilerin Korunması Uygulama Kılavuzu**, 1. Baskı, İstanbul, Ocak- 2020, s.24

[275] Handbook on European data protection law 2018 edition, s.30-31; GDPR, önemli değişiklikler ortaya koymakla birlikte şirketleri, kişisel verilerle ilgili işlemlerinde daha dikkatli davranmaya sevk etmekte ve onları mahremiyet meselesini daha ciddi ele almaya zorlamaktadır. Bkz. Hoofnagle, C. J., van der Sloot, B., & Zuiderveen Borgesius, F. (2019). **The European Union General Data Protection Regulation: What It Is And What It Means**, Information & Communications Technology Law, 28(1), 65-98, University of Amsterdam, s.98; İlk olarak kişisel verileri koruyan diğer düzenlemelerde olduğu gibi GDPR'ın da teknolojinin hızlı gelişmesinin bir sonucu olduğu belirtilmelidir. GDPR'ın amacı Avrupa'yı dijital çağa uygun hale getirmektir. Bkz. https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en (10.09.2018tarihinde erişildi.)

[276] Paolino Fierro, **The General Data Protection Regulation (GDPR): From static to dynamic compliance**, Law And Economics Yearly Review, Volume 6 – Part 2 – 2017

[277] Handbook on European data protection law 2018 edition, s.96

2. BÖLÜM: VERİLERİ HUKUKA AYKIRI OLARAK VERME VEYA ELE GEÇİRME SUÇU

1. Genel Olarak

Bilgi, var olduğu ilk günden bu yana bir güç kaynağı olarak görülmüş ve kendisine sahip olunması noktasında birçok rekabete şahit olmuştur. Özellikle 21. yüzyılın başlarında teknolojide meydana gelen gelişmelerle ve bilişim sistemlerinin hayatımızın hemen hemen her alanında hakimiyet kurmasıyla bu kavramın önemi daha da artmıştır. Yapay zekanın da katkısıyla insana duyulan ihtiyaç her geçen gün azalmış ancak mevcut sistemin yol kat edebilmesi için bilgiye büyük oranda muhtaç olunduğu gün yüzüne çıkmıştır. Zira bilgi kavramı yeni çağın petrolü olarak kabul edilmiştir. Nitekim başta devletler, istihbarat teşkilatları aracılığıyla; şirketler ise elindeki imkanları kullanarak bireyler hakkında birçok bilgi toplamaktadır. Günümüzde teknolojide görülen çeşitlilik bilgi kavramının da çeşitlenmesine ve değişik formlara bürünmesine yol açmıştır. İşte tam bu noktada çalışmamızın etrafında şekillendiği kişisel veri terimi karşımıza çıkmaktadır. Çünkü kişisel veri de yukarıda belirttiğimiz üzere kanun tarafından belirlenmiş birtakım niteliklere sahip bir bilgi çeşididir.

Başta bilişim sistemleri olmak üzere işlem hayatının devamı açısından temel yapıtaşı niteliğinde olan kişisel veri, birçok farklı çeşitte işleme konu olmaktadır. Bahsi geçen işlem çeşitliliği teknolojinin hızlı gelişmine paralel olarak her geçen gün artmaktadır. Örneğin devlet mekanizması içerisinde ilk önce kişisel veri işleme faaliyeti gösteren kurumlar olarak vergi[278] ve icra daireleri[279] ve tapu müdürlükleri karşımıza çıkmaktadır. Özel kuruluşlar açısından ise banka, hastane ve sosyal medya devlerinin de dahil olduğu teknoloji şirketleri ön sıralarda yer almaktadır. Ancak kişisel verileri işleme tabi tutan oluşumlar yalnızca değindiğimiz bu kuruluşlarla sınırlı değildir. Teknolojinin imkanları sayesinde herhangi bir organizasyona sahip olunmadan da bireyler tarafından birçok kişisel veri dolaşıma sokulabilmektedir.

Bu aşamaya kadar kadar kişisel verinin neden ve nasıl işleme faaliyetine konu olduğunu izah etmeye çalıştık. Veri işleme ile ilgili olarak bu safhada gözden kaçmaması gereken diğer bir soru ise veri işlemenin nasıl olması gerektiğidir. Nitekim çalışmamızın konusunu da işleme faaliyetinin sadece birkaç formunu oluşturan verme, yayma ve ele geçirme fiillerinin hukuka aykırı olarak meydana gelmesi oluşturmaktadır. Kişisel veriler, çeşitli amaçlar doğrultusunda hukuka aykırı olarak birçok işleme konu olmaktadır. Kimi zaman kar gütme saikiyle şirketler tarafından veri işlenebileceği gibi kimi zaman da dolandırıcılık, şantaj ve tehdit amacıyla söz konusu veriler kullanılmaktadır. Örneğin son zamanlarda kimlik hırsızlığı olarak da bilinen suç

[278] *Bu veriler vergi idaresi tarafından, işlevi gereği, sürekli toplanmakta, bunların korunması da özel hayatın gizliliği hakkının vergilendirme alanındaki görünümü olan vergi mahremiyeti hakkıyla sağlanmaktadır."* Ayrıntılı bilgi için bkz. İnci Solak Akman, **Vergi Mahremiyetini İhlal** (Doktora Tezi), Ankara 2012 s.39 vd.

[279] İstanbul BAM 23. HD T.31.03.2017 ve E.2017/596 K. 2017/527

tipi sıklıkla karşımıza çıkmaktadır. Kimlik hırsızlığında fail, farklı bir kişinin kimlik bilgilerini hukuka aykırı yollardan elde ederek elde ettiği bu kişisel verilerle banka hesabı açmakta, kredi çekmekte yahut farklı diğer birtakım suçlar işlemektedir. İnternette yer alan kişilere ait bilgilerin ele geçirilmesi şeklinde tanımlanan kimlik hırsızlığı[280] eylemi çeşitli şekillerde ortaya çıkabilmektedir. Somutlaştırmak gerekirse "oltalama" ("phishing") olarak adlandırılan işlemde dolandırıcılar rastgele kullanıcıların hesaplarına gönderdikleri e-posta ve SMS'lerle kullanıcının özel bilgilerini (şifre, parola, müşteri numarası, kredi, kartı numarası gibi) ele geçirmeyi hedeflemektedirler.[281] Özellikle bilişim sistemlerine sızan hackerlar tarafından bu yöntem çokça tercih edilmektedir. Ne yazık ki teknolojinin gelişmesinin de kötüniyetli kişilerin bu şekilde kişisel verileri elde edip kullanmasında rolü büyüktür.[282] Kimlik hırsızlığı ile ilgili son olarak belirtelim ki bu konu çeşitli yargı kararlarında da yerini almaya başlamıştır. Örnek olarak Yargıtay bir kararında, yakalanan sanıkların üzerinden çıkan materallerin incelenmesi neticesinde ATM'de işlem yapan müşterilerin görüntüleri ile kart bilgilerine ulaşıldığını ve henüz bu bilgiler ile kart üretildiğine ilişkin herahangi bir delilin olmaması nedeniyle somut olayda Türk Ceza Kanunu'nun 136. maddelerinde düzenlenen kişisel verileri hukuka aykırı olarak ele geçirmek suçunun oluştuğu kanaatine varmıştır.[283_284] Teknolojinin gelişim hızı

---

[280] Ali Karagülmez, **Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri**, Seçkin Yayınları, Ankara 2009, s.461; Kimlik hırsızlığı, kişilerin kimlik bilgilerinin onların rızası olmadan başkası tarafından kullanılmasıdır. Bu işlem genellikle dolandırıcılık amacıyla kullanılmakta olup internetteki kişisel verilerin kullanımının artmasıyla bu konudaki kaygılar oldukça artmıştır. Kimlik hırsızlığındaki "kimlik" ifadesi belirli bir kişiye özgü bilgi anlamında kullanılmaktadır. Buna örnek olarak ise kişinin telefon numarası, adresi, kredi kartı numarası verilebilir. Bkz. Tara J. Radin, **Identity Theft (www.britannica.com)**; Kimlik hırsızlığı, Amerika Birleşik Devletleri Federal Ticaret Komisyonu tarafından kişisel bilgilerin çalınması ve sahibinin izni olmadan kullanılması şeklinde tanımlamaktadır. Bkz**. Identity Theft What to Know What to Do**, Federal Trade Commission

Kimlik hırsızlığının 2017'de rekor kırdığı, dolandırıcıların artık daha bilgili olduğu ve kişilerin daha önemli finansal bilgilerini ele geçirmek için özellikle güvenliği zayıf olan hesapları kullandığı belirtilmektedir. Kathy Kristof, **Identity Theft Has Never Been More Rampant (www.cbsnews.com)**; Javelin Strateji ve Araştırma Şirketi'nin 2018 raporuna göre Amerika'da 2017'de 1 milyon çocuk kimlik hırsızlığından mağdur olmuş ve toplam 2.6 milyar dolar kayıp yaşanmıştır. Mağdurların üçte ikisinin yaşının sekizin altında olduğu belirtilmektedir. Bkz. **2018 Child Identity Fraud Study**, Javelin Strategy&Research; Herb Weisbaum, **More Than 1 Million Children Were Victims of ID Theft Last Year (www.nbcnews.com)**; Ayrıca 2019 yılı raporuna göre 2018 yılında toplamda 14.4 milyon kişi mağduriyet yaşamıştır. Bkz. **2019 Identity Fraud Study: Fraudsters Seek New Targets and Victims Bear the Brunt**, Javelin Strategy&Research; Amerika ve Kanada'da kimlik hırsızlığı her yıl toplam nüfusun %4'ünü etkilediği ve kimlik hırsızlığı yöntemlerinin arttığı yönünde ve kimlik hırsızlığı hakkında ayrıntılı bir inceleme için bkz. Norm Archer/ Susan Sproule/ Yufei Yuan/ Ken Guo/ Junlian Xiang, **Identity Theft and Fraud Evaluating and Managing Risk**, University of Ottawa Press (2012), s.2

[281] Türkiye Bankalar Birliği, **Dolandırcılık Eylemleri ve Korunma Yöntemleri**, Aralık 2015, s. 49

[282] Dülger'e göre ABD ve İngiltere gibi ülkelerin yaptırıma bağladığı kimlik hırsızlığı 136. madde aracılığıyla Türkiye'de de yaptırımsız kalmamış olacaktır. Bkz. Dülger, *Kişisel Verilerin Korunması Hukuku*, s.617

[283] YARGITAY 8. CEZA DAİRESİ E. 2018/8124 K. 2018/14646 T. 19.12.2018; Diğer bir kararında mahkeme şu şekilde hükme varmıştır: *"Mağdurlara ait kart bilgileri kopyalanarak bir kart oluşturulmaması halinde ise ele geçirilen kopyalama cihazında bilgi bulunması halinde eyleminin mağdur sayısınca TCK.nun 136. maddesinde düzenlenen kişisel verileri hukuka aykırı olarak ele geçirme, bulunmaması halinde ise kişisel verileri hukuka aykırı*

göstermektedir ki kimlik hırsızlığı ileride birçok farklı forma dönüşecek ve içtihatlara konu olacaktır.

Hayatımızın her alanında karşımıza çıkan teknolojik gelişmeler hukuk sistemlerini de etkileyerek dinamik bir sosyal bilim dalı olan hukukun çeşitli alanlarında birçok değişikliğe sebep olmuştur. Zira değişen ve gelişen sosyal hayatımızın bir düzen içerisinde devam etmesi için hukuk kurallarının yeniden düzenlenmesi elzem hale gelmektedir. Aynı neticelerle ceza hukuku alanında da karşılaşılmaktadır. Nitekim 5237 sayılı Türk Ceza Kanunun genel gerekçesinde hayat düzeninin geçirdiği değişiklikler sonucunda hayatımıza giren yeni sosyal değerlerin korunması için kanunlarda değişiklik yapılması ihtiyacının ortaya çıkacağı ve bu minvalde, değişen değerlerin en kısa sürede ceza mevzuatına yansıtılmasının zaruret arz ettiği ifade edilmiştir.[285] Nitekim Türk kanun koyucusu meydana gelen teknolojik gelişmeleri ve bu bağlamda verilerin işlem hayatına yavaş yavaş egemen olmasını göz önünde tutarak kişisel verilere ilişkin bazı düzenlemeler getirmiştir. İşte çalışmamızın konusunu oluşturan verileri hukuka aykırı olarak verme veya ele geçirme suçunun ihdası da meydana gelen en önemli değişikliklerdendir.

Madde metninin ayrıntılı olarak incelenmesine geçmeden önce 136. madde ile ilgili Anayasa Mahkemesi'ne yapılan iptal başvurusuna değinmek istiyoruz. Söz konusu başvuru Batman 2. Asliye Ceza Mahkemesince yapılmış olup Anayasa Mahkemesi tarafından 12.11.2015 tarihli karar ile reddedilmiştir. Şöyle ki Yerel Mahkeme başvuru gerekçesinde iptal başvurusuna konu 136. madde ile ilgili olarak ceza kanununda kişisel veriye ilişkin herhangi bir tanım ve sınırlandırma yer almaması nedeniyle suçta ve cezada kanunilik ilkesinin ihlal edildiğini belirtmiştir. Ayrıca başvuruda, yürürlükteki mevzuatta kişisel veri tanımının yapılmadığı belirtildikten sonra kişisel verilerin başlıcaları sayılmış ve sayılan bu kadar bilgilerden hangilerinin veri olarak kabul edilerek bu suçları işleyenlerin cezalandırılacağının belirsiz olduğu vurgulanmıştır. Anayasa Mahkemesi ise söz konusu iptal başvurusunu, kişisel veri

---

olarak ele geçirmeye teşebbüs suçunu oluşturacağı gözetilmeden eksik araştırma ile yazılı şekilde hüküm kurulması" YARGITAY 8. CEZA DAİRESİ E. 2018/6171 K. 2018/10436 T. 8.10.2018

[284] YARGITAY 15. CEZA DAİRESİ E. 2019/2249 K. 2019/7187 T. 25.6.2019; Aynı yönde bkz. İbrahim Korkmaz, Kişisel Verilerin Ceza Hukuku Kapsamında Korunması, s.443 dn.450'deki karar (YARGITAY 8. CEZA DAİRESİ E. 2012/32153 K. 2013/25660 T. 28.10.2013); Aynı yönde diğer bir karşı oy için bkz. YARGITAY 15. CEZA DAİRESİ E. 2019/1914 K. 2019/6983 T. 20.6.2019; Diğer bir karar YARGITAY 15. CEZA DAİRESİ E. 2017/27594 K. 2019/6612 T. 30.5.2019; Yargıtay Ceza Genel Kurulu ise kimlik hırsızlığı terimine kişisel veriler kategorizasyonunda ekonomik ve finansal kişisel veriler başlığı altında yer vermektedir. *"Ekonomik ve finansal kişisel veriler: Suçlular tarafından suistimale ve kimlik hırsızlığına hedef olmamak için kişinin mali varlığı, sahip olduğu hisse ve hesaplar, borçları, yaptığı alış verişler, kredi kartlarına ilişkin veriler."* YARGITAY CEZA GENEL KURULU E. 2012/12-1510 K. 2014/331 T. 17.6.2014

[285] Türkiye Büyük Millet Meclisi, Mayıs 2003, **5237 sayılı Türk Ceza Kanunu Genel Gerekçesi**, s.3-4

kavramının teknolojide meydana gelecek gelişmelere bağlı olarak değişik formlarda ortaya çıkabileceğini ve bundan dolayı tüm veri çeşitlerinin önceden kanunda sayılmasının mümkün olmadığını gerekçe göstererek reddetmiştir. Buna ek olarak AYM, kişisel veri kavramının kapsamının uygulamada netleştirileceğini de vurgulamıştır.[286]

2. Madde Metni, Gerekçesi ve Yapılan Değişiklikler

Verileri hukuka aykırı olarak verme veya ele geçirme suçu, 5237 sayılı Türk Ceza Kanunu'nun ikinci kitabının Kişilere Karşı Suçlar başlıklı ikinci kısmının Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar başlıklı dokuzuncu bölümünde düzenlenmiştir. Söz konusu madde *"(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."* hükmünü havidir. İki fıkradan oluşan maddenin birinci fıkrasında kişisel verileri hukuka aykırı olarak bir başkasına verme, yayma veya ele geçirme fiillerinin müeyyidesi düzenlenmiş iken 2019 yılında yapılan değişiklikle eklenen ikinci fıkrada suçun konusuna bağlı olarak meydana gelen nitelikli hal hükmü yer almıştır. Hükmün gerekçesine geçmeden önce söz konusu 136. maddenin bugüne dek geçirdiği değişikliklere değinmekte yarar görüyoruz.

Öncelikle ifade etmek gerekirse 136. madde bir kez ceza miktarı değişikliği ve bir kez de yeni fıkra eklenmesi olmak üzere toplamda iki değişikliğe uğramıştır. 2014 yılında yapılan ilk değişiklikle birinci fıkradaki fiillerin cezasının alt sınırı bir yıldan iki yıla çıkarılmıştır. 6526 sayılı Terörle Mücadele Kanunu ve Ceza Muhakemesi Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Yasa'nın 4. maddesiyle getirilen söz konusu değişikliğin gerekçesinde bu düzenleme ile birlikte kişisel verilerin yanı sıra özel hayat açısından daha etkili bir korumanın sağlandığı belirtilmiştir. Ayrıca 6526 sayılı Kanun'un genel gerekçe bölümünde ise Anayasa'nın 20. maddesinde düzenlenen kişisel verilerin korunmasını isteme hakkına vurgu yapılmıştır.[287]

Madde metninde kanun koyucu tarafından yapılan ikinci değişiklik ise 2019 yılında 7188 sayılı Kanun ile eklenen ikinci fıkradır. Söz konusu hükümde, verileri hukuka aykırı olarak verme veya ele geçirme suçunun konusunun Ceza Muhakemesi Kanunu'nun Mağdur ile Şikâyetçinin Dinlenmesi başlıklı 236. maddesinin beşinci ve altıncı fıkraları uyarınca kaydedilen beyan ve

[286] AYM, Esas Sayısı: 2015/32 Karar Sayısı: 2015/102 Karar Tarihi: 12.11.2015

[287] 6526 sayılı Terörle Mücadele Kanunu Ve Ceza Muhakemesi Kanunu İle Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun'un Teklif Metni, TBMM Yasama Dönemi:24 Yasama Yılı: 4 Sıra Sayısı: 560 s.7-8

görüntü olması durumunda birinci fıkraya göre verilecek cezanın bir kat artırılması öngörülmektedir. Bahse konu değişikliğin gerekçesinde ise verilecek cezada artırıma gidilmesinin nedeni olarak cinsel istismar ve cinsel saldırı suçlarının mağdurlarının örselenmesinin önlenmesi olduğu ifade edilmiştir.[288]

İnceleme konumuz olan verileri hukuka aykırı olarak verme veya ele geçirme suçunun gerekçesinde suça konu verilerin -136. maddede sayılan fiiller işlenmeden önce- hukuka uygun olarak kaydedilmiş olup olmaması hususunun suçun sübutuna etki etmeyeceği belirtilmiştir.

Madde metni ile ilgili açıklamalarımıza son vermeden önce 136. maddenin düzenleniş şekliyle ilgili birkaç noktaya değinmemiz gerekmektedir. Öncelikle madde başlığına bakıldığında kişisel veri kavramı yerine sadece veri kavramının kullanılmış olduğu görülmektedir. Madde metninde kişisel veri ibaresinin tercih edilmiş olmasına rağmen maddenin başlığında sadece veri kelimesinin yer alması, birbiriyle örtüşmeyen iki farklı terimin aynı madde için kullanılmasına neden olmuştur. Söz konusu iki terim birbiriyle uyuşmamaktadır. Zira kişisel veri, gerçek kişileri ilgilendirirken veri kavramı kişisel verileri de kapsayan ve gerçek kişilere ilişkin olmayan bilgileri de içeren bir özelliğe sahiptir. Bahsedilen bu uyumsuzluğa rağmen 136. maddenin kanunda düzenlendiği yer ve madde metninin düzenlenme şekli itibarıyla bu madde ile kastedilen veri çeşidinin kişisel veriler olduğunu belirtmemiz gerekir.[289] Ayrıca madde başlığında yayma ifadesine yer verilmemiştir. Nihayet bazı yazarlar başlığın düzenleniş şeklinin isabetli olmadığını ifade etmektedirler.[290]

Son olarak değinmek gerekirse doktrinde 136. maddenin 765 sayılı eski TCK'de karşılığının bulunmadığını belirten yazarlar olduğu gibi kimi müellifler ise söz konusu suçun karşılığını 765 sayılı TCK'nin 525/a.1. maddesinin oluşturduğunu ifade etmektedir.[291]

---

[288] 7188 Sayılı Ceza Muhakemesi Kanunu Ve Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun'un Teklif Metni, TBMM, Yasama Dönemi:27 Yasama Yılı: 3, s.12

[289] Karagülmez, s.401

[290] Zeki Hafızoğulları/ Muharrem Özen, **Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar**, Ankara Barosu Dergisi, Yıl:67, Sayı: 4, Güz 2009, s.21; Korkmaz, *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması* (Nisan 2019), s.442

[291] Sinem Göçmen Uyarer, **Kişisel Verilerin Korunması**, Ağustos 2019, Seçkin Yayıncılık, s.210, 452 ve 454. Dipnotlar. ETCK m.525/a.1. maddesi şu şekilde düzenlenmişti: *"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."*

3. Korunan Hukuki Değer

Kaynağını kanundan alan ceza hukukunda kanunsuz suç ve ceza olmaz ilkesi kabul edilmiştir. Bu kabulün sonucunda ise suç olarak adlandırılan insan davranışının ceza kanununu ihlal eden bir nitelik taşıdığı belirtilmektedir. Kısaca vurgulamak gerekirse bir fiile suç vasfının verilmesi bahse konu ihlal edicilik özelliğine bakılarak yapılacaktır. Somut olayda karşımıza çıkan beşeri davranışın ihlal içeren bir davranış olduğu tespit edildiğinde ise ikinci olarak hangi insani değeri/menfaati hedef aldığı incelenmelidir. İşte bu noktada tespit edilecek hukuki değer, suçun hukuki konusunu oluşturacak ve ihdas edilen o suç ile kanun koyucu tarafından hangi değerlerin koruma altına alınmaya çalışıldığı görülecektir.[292] Suçlar ile korunan hukuki değerler zamana bağlı olarak değişkenlik gösterebilir. Örneğin günümüzde henüz önemli görülmeyen bazı değerler gelecekte koruma altına alınabilecek veya şu anda önemli addedilen bazı değerler ise gelecekte önemini yitirebilecektir. Ayrıca hukuki değerler, kendi içerisinde bir hiyerarşiye sahiptir. Şöyle ki toplum içinde bazı menfaatler zamanla daha önemli hale gelebilecek ve hukuk kurallarının da bu hiyerarşik önem derecesine göre düzenlenmesi gerekecektir. Nihayet *"bütün hukuksal değerlerin pozitif öncesi, ideal, soyut bir karakteri vardır."*[293]

Suçun hukuki konusu aslında ceza tehdidi kullanılarak ceza normu ile korunmak istenen şeydir.[294] Nesnel bir nitelik taşımamakla birlikte manevi-metafizik bir anlama sahip olan hukuki değere saldırılması, o davranışı sergileyen kişinin söz konusu değeri tanımaması olarak anlaşılır.[295]

TCK'nin 136. maddesinde düzenlenen verileri hukuka aykırı olarak verme veya ele geçirme suçuyla korunmak istenen hukuki değerin niteliği hakkında çeşitli görüşler vardır. Doktrindeki bir görüş, kişisel verilerin korunmasının özel hayatla yakın bağlantılı olduğunu belirterek 136. madde ile kişilerin özel hayatının gizliliğinin korunduğunu belirtmektedir.[296] Bir diğer görüşe göre bu suçla koruma altına alınan değerler, genelde özel hayat ve özel olarak kişisel verilerdir.[297] Diğer bir görüşe göre 136. madde ile kişisel verilere saygı hakkı korunmakta ve geniş kapsamda ise özel hayat muhafaza altına alınmaktadır.[298] Farklı bir görüşe göre söz konusu suç ile özel hayatın gizliliği ve korunması hakkını hedef alan ihlallerin önlenmesi

[292] Zeki Hafızoğulları/ Devrim Güngör, **Türk Ceza Hukukunda Suçların Tasnifi** (Hakemli Makale), TBB Dergisi, 2007 Sayı 69, s.22-23
[293] Yener Ünver, **Hukuk Felsefesi ve Sosyolojisi Arkivi**, 8. Kitap, İstanbul Barosu, İstanbul 2003, s.115-116
[294] Hafızoğulları/ Özen, *Türk Ceza Hukuku Genel Hükümler*, s.199
[295] İzzet Özgenç, **Türk Ceza Hukuku Genel Hükümler**, Eylül 2019, Seçkin Yayıncılık, s.175
[296] İbrahim Şahbaz, **Açıklamalı ve İçtihatlı Türk Ceza Kanunu**, 1. Cilt, Ankara 2016, s.1598
[297] Doğan Soyaslan, **Ceza Hukuku Özel Hükümler**, 13. Baskı, Ankara 2020, s.364
[298] Handan Yokuş Sevük, **Türk Ceza Hukuku Özel Hükümler**, Adalet Yayınevi, Ankara 2020, s.495

amaçlanmaktadır.[299] Öğretide yer alan diğer bir görüş ise bu suç ile kişilerin kişisel verilerinin koruma altına alındığını ifade etmektedir.[300] Başka bir görüş, bahse konu suç ile kişisel verilerin korunması hakkının korunduğunu belirtmektedir.[301] Öğretide yer alan diğer farklı bir görüş ise 136. madde ile getirilen suç tipi ile Anayasa'da yer alan özel hayatın gizliliğinin içerisinde değerlendirilen ancak ayrı bir hak olarak kabul gören kişisel verilerin korunması hakkının korunduğunu savunmaktadır.[302] Son olarak bu suç tipi ile Anayasa'da ayrıca bir hak olarak tanınan kişisel verilerin korunması hakkının korunmasının yanı sıra kişinin mahremiyetinin de himaye edildiği ve bu suretle bireyin toplumdaki varlığını huzurlu bir şekilde sürdürmesinin amaçlandığını bildiren bir görüş de mevcuttur.[303]

Yargıtay Ceza Genel Kurulu 136. madde ile korunan hukuki değeri genel olarak kişilerin özel hayatı ve hayatın gizli alanı, özelde ise kişisel veriler olduğunu belirtmiştir. Ayrıca aynı kararında CGK, söz konusu düzenlemeler ile tüm kişisel verilerin koruma altına alındığını, ve bu verilerin mutlaka gizli olmasının gerekmediğini nitekim gizli olmayan ve herkes tarafından bilinen kişisel verilerin de hukuka aykırı eylemlere karşı korunması gerektiğini ifade etmiştir. Son olarak kararda kişisel verilerin korunmasına ilişkin suçlarda korunan hukuki değerin "sır" olmayıp, verinin ilgilisi olan kişinin kişilik hakları olduğuna kanaat getirilmiştir.[304]

4. Suçun Unsurları

5237 sayılı Türk Ceza Kanunu'nda suç kavramının tanımı yapılmamış olup her suç tipi kendi özelinde ve de kanunilik ilkesinin bir sonucu olarak ayrı ayrı tanımlanmıştır.[305] Çağdaş ceza hukukunun yapıtaşlarından biri olan suç kavramı için, birçok müellif tarafından çeşitli tanımlamalar yapılmıştır. Hukuk düzenince ceza veya güvenlik tedbiri yaptırımına bağlanan "*suç, ceza normunun yasaklamış olduğu, tipe uygun, kasten veya taksirle gerçekleştirilen*

[299] Ali Parlar/ Mustafa Öztürk, **Doğrudan ve Dolaylı Bilişim Suçları ve Bilişim Sistemleri Aracılığıyla İşlenen Suçlar**, Aristo Yayınevi, Mart 2020 İstanbul, s.543

[300] Dülger, *Kişisel Verilerin Korunması Hukuku*, s.731

[301] Korkmaz, *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması* (2019), s.446; Aynı yönde bkz. Şeyma Sert, **Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması**, Seçkin Yayınları, Şubat 2019 Ankara, s.136

[302] Mahmut Koca/İlhan Üzülmez, **Kişisel Verilerin Kaydedilmesi Suçu** (Hakemli Makale), D.E.Ü. Hukuk Fakültesi Dergisi, Prof. Dr. Durmuş TEZCAN'a Armağan, C.21, Özel S., 2019, s. 69-93, s.75

[303] Hasan Sınar, **Kişisel Verileri Hukuka Aykırı Olarak Verme, Yayma veya Ele Geçirme Suçu (TCK Md. 136)**, Kişisel Verileri Koruma Dergisi, Cilt: 2, Sayı: 1 s.36

[304] YARGITAY CEZA GENEL KURULU E. 2012/12-1510 K. 2014/331 T. 17.6.2014; YARGITAY CEZA GENEL KURULU E. 2015/12-708 K. 2019/414 T. 9.5.2019; YARGITAY CEZA GENEL KURULU E. 2017/12-829 K. 2017/363 T. 4.7.2017

[305] Veli Özer Özbek/ Koray Doğan/ Pınar Bacaksız/ İlker Tepe, **Türk Ceza Hukuku Genel Hükümler**, Seçkin Yayınları, Eylül 2018-Ankara, s. 205

hukuka aykırı haksız bir fiildir."[306] Suç, ceza hukukundan doğan ve deneme yanılmaya dayalı olmayıp insan davranışının karşılığı olarak önceden öngörülen bir değer yargısı olarak karşımıza çıkmaktadır. Bu nedenledir ki bir suçtan söz edilebilmesi için onu meydana getiren bir kanun hükmü bulunmak zorundadır. Kanun hükmünün olmadığı bir yerde suçtan da bahsedilemeyecektir.[307] Böylelikle suç, kanunda belirtilen soyut suç tanımını karşılayan bir fiil olarak tanımlanabilecektir.[308]

Ceza tehdidi ile yasaklanan bir fiil olan suç[309], yapısı itibarıyla birçok unsuru içinde barındırmaktadır. Ceza hukukçularının çalışmalarının çoğunu ceza hukukunun genel kısmında yürütmesinin sonucunda bu alanda önemli gelişmeler yaşanmış ve suçun unsurları ortaya konmuştur.[310] Söz konusu unsurları tespit etmek ve suçun anatomisini suçu parçalarına ayırarak analitik bir incelemeyle sergilemek ise suç teorisinin görevidir. Suç teorisinin buradaki amacını suç ile suç olmayan fiillerin ayırt edilmesi oluşturmaktadır. Böylece hukuki açıdan suçun ne olduğu açıklığa kavuşturulur.[311] Söz konusu faaliyet sürdürülürken ise suç teorisinin birçok faydası ortaya çıkar. Şöyle ki pratikte karşılaşılan ve ceza hukukunu ilgilendiren birçok problem suç teorisinden yararlanılarak çözüme kavuşturulacaktır. Bu nedenledir ki karşılaşılan somut vakıada doğruya ulaşmak yalnızca genel teoriye başvurulduğu ölçüde mümkündür.[312] Suç teorisi ile birlikte ilk önce suçun ne olduğu ve onu diğer hukuka aykırı fiillerden ayıran etkenlerin neler olduğu incelendikten sonra suçu etkileyen nedenler, suçun ne zaman doğduğu gibi hususlar irdelenir. Sonrasında ise suçların hangi değerleri koruduklarından yola çıkarak suç tipleri gruplandırılır.[313]

Suç teorisinin konusunu oluşturan ve suça vücut veren suçun unsurların tespit edilmesinde birçok görüş ortaya atılmıştır.[314] Çalışmamızın kapsamını ve amacını aşmaması açısından söz konusu görüşlere değinmeyip burada sadece eserimizde suçun unsurları incelenirken izlenecek yönteme yer vereceğiz. Biz bu çalışmamızda daha isabetli olduğunu düşündüğümüz ve suçun tipiklik, maddi unsurlar, manevi unsurlar ve hukuka aykırılık unsuru olmak üzere dört unsuru

---

[306] Kayıhan İçel, **Ceza Hukuku Genel Hükümler**, 2018 Beta Yayınları, s.223; Artuk/Gökcen/Yenidünya, **Ceza Hukuku Genel Hükümler**, Ekim 2016, s.198

[307] Zeki Hafızoğulları/Muharrem Özen, **Türk Ceza Hukuku Genel Hükümler**, 12. Baskı, Ankara Ekim 2019, s.151

[308] Haluk Toroslu/Nevzat Toroslu, **Ceza Hukuku Genel Kısım**, Savaş Kitapevi, Ankara 2018, s.100

[309] Haluk Toroslu/Nevzat Toroslu, s.99

[310] Sulhi Dönmezer/Sahir Erman, **Nazari ve Tatbiki Ceza Hukuku Genel Kısım**, Cilt 1, İstanbul 1973, s.323; Faruk Erem/Nevzat Toroslu, **Türk Ceza Hukuku Özel Hükümler**, Ankara 1973, s.5

[311] İçel, s.225; Mahmut Koca/İlhan Üzülmez, **Türk Ceza Hukuku Genel Hükümler**, Seçkin Yayıncılık, Eylül 2017 Ankara, s.83

[312] İçel, s.225

[313] Dönmezer/ Erman, *Nazari ve Tatbiki Ceza Hukuku Genel Kısım*, s.321

[314] Dönmezer/ Erman, *Nazari ve Tatbiki Ceza Hukuku Genel Kısım*, s.324; Söz konusu görüşlere ilişkin olarak bkz. İçel, s.225-227

olduğunu kabul eden görüşün[315] aşağıdaki sistematiği doğrultusunda kişisel verilerin verilmesi, yayılması veya ele geçirilmesi suçunu izah etmeye çalışacağız: 1) Tipiklik, 2) Maddi Unsurlar: Fiil, Netice, Fail, Konu, Nitelikli Unsurlar, 3) Manevi Unsurlar: Kast, Taksir, Saik, Neticesi Sebebiyle Ağırlaşmış Suç, 4) Hukuka Aykırılık

4.1. Maddi Unsurlar

4.1.1. Fiil

Ceza normunun konusu dış dünyaya hareket veya ihmal şeklinde akseden beşeri davranışlardır. Nitekim fiil unsuru, suçun ilk kurucu unsuru olmakla birlikte modern ceza hukukunun hareket noktasıdır.[316] Bu davranış çeşidi yani eylem, insanın neden olduğu olay anlamına gelmekle birlikte dış dünyada değişiklik meydana getiren bir bütündür.[317] Söz konusu noktada insan bedeni, hali hazırda mevcut bulunan koşulları değiştirerek bir hukuki menfaati ihlal etmektedir.[318] Ceza hukuku bağlamında fiil, yasadaki suç tanımlamasını karşılayan veya o tanımdaki neticeyi gerçekleştirme amacını taşımasının yanı sıra aynı zamanda iradi olan insan davranışıdır.[319]

Verileri hukuka aykırı olarak verme veya ele geçirme suçunun fiil unsuru, kişisel verilerin hukuka aykırı olarak bir başkasına verilmesi, yayılması veya ele geçirilmesidir.

136. maddedeki suçun fiil unsuruna ilişkin olarak vurgulanması gereken hususlardan ilki, hükümde gösterilen hareketlerden birinin gerçekleştirilmesiyle suçun meydana geleceği yani suçun oluşması için hareketin yanında ayrıca bir zarar oluşup oluşmadığının önem arz etmemesidir. Bu yönüyle suç, tehlike suçudur. Tehike suçlarında icra edilen hareket sonucunda suçun konusu üzerinde bir zarar oluşması aranmamakta ve bununla birlikte o suç konusunun zarara uğrama tehlikesi dahi suçun oluşumu için yeterli görülmektedir.[320] Ayrıca fiil ile sonuç arasında bir illiyet bağının araştırılması hakkında maddede bir ifade yer almadığından bahse konu suç tipinin soyut tehlike suçu olduğunu belirtmek gerekir.[321] Soyut tehlike suçlarında hakim, önüne gelen olayda failin hareketinin suçun konusu üzerinde bir tehlike oluşturup oluşturmadığını araştırmamaktadır. Zira suça konu hareketin yapılması ile tehlike oluşmuş

[315] Artuk/Gökcen/Yenidünya, Ceza Hukuku Genel Hükümler, 10. Baskı, Ekim 2016
[316] Selahattin Keyman, **Cürmi Fiilin Yapısal Unsuru Olarak Hareket**, AHFD XL 1-4(1988), s.122
[317] İçel/ Özgenç/ Sözüer/ Mahmutoğlu/ Ünver, **Suç Teorisi**, İstanbul 1999, s.54
[318] Keyman, s.154
[319] Nur Centel, Hamide Zafer, Özlem Çakmut, **Türk Ceza Hukukuna Giriş**, Üçüncü Bası, Beta Yayınları, s.234
[320] İçel, s.278
[321] Veli Özer Özbek/ Koray Doğan/ Pınar Bacaksız, **Türk Ceza Hukuku Özel Hükümler**, 14. Baskı, Ankara 2019, Seçkin Yayıncılık, s.598; Uyarer, *Kişisel Verilerin Korunması*, s.215

varsayılır. Bu bağlamda, Türk Ceza Kanunu'nda düzenlenen hakaret ve müstehcenlik suçları soyut tehlike suçlarına örnek olarak verilebilecektir. [322]

Verileri yayma ve ele geçirme suçu, maddede belirtilen hareketlerin meydana gelmesiyle oluşmakla birlikte suçun sübuta ermesi için ayrıca bir netice aranmamakta ve bu haliyle söz konusu suç, sırf hareket suçu olarak düzenlenmiş bulunmaktadır. Sırf hareket suçlarında kanun, suça vücut verecek harekete ek olarak ayrıca bir netice göstermemekte ve yalnızca düzenlediği hareket çeşitlerinin yapılmasıyla suçun oluşacağını kabul etmektedir. Burada hareketin icrası ile birlikte suç tamamlanmış kabul edilmekte ve neticenin de ortaya çıktığı öngörülmektedir.[323] Ayrıca belirtmek gerekir ki bu suçun oluşmasında kesintisizlik önem taşımamaktadır ve bu yönüyle 136. maddede düzenlenen suç, ani hareketli suç tiplerinden sayılacaktır.[324] Ani suçlarda fiilin neden olduğu netice devamlılık göstermemekte ve hemen sona ermektedir. Suçun işlenmesi ile meydana gelen netice belirli bir zaman diliminde devam etmemektedir. Bu suçlara örnek olarak ise kasten öldürme ve kasten yaralama suçları gösterilebilecektir.[325]

İnceleme konumuzu oluşturan suç tipi seçimlik hareketli bir suç olarak düzenlenmiştir. 136. maddede yer alan hareketlerden birinin veyahut birkaçının aynı anda meydana gelmesi durumunda da tek bir suç işlenmiş olacaktır. Ancak birden fazla seçimlik hareketin söz konusu olduğu vakılarada bu durum dikkate alınacak ve temel ceza alt sınırdan uzaklaşılarak verilebilecektir.[326] Seçimlik hareketli suçlarda kanun, birbirine alternatif olabilecek farklı hareketleri aynı suç olarak kabul etmekte ve bu hareketlerden birisinin oluşması durumunda suçun sübut bulduğunu kabul etmektedir. Söz konusu suçun oluşması için seçimlik olarak gösterilen hareketlerin hepsinin bir anda yapılması gerekli değildir ve dahi yasada düzenlenen hareketlerden sadece biri yapılsa da o suç oluşacaktır. Örnek vermek gerekirse Türk Ceza Kanunu'nda düzenlenen hakaret, mala zarar verme, insan ticareti seçimlik hareketli suçlardan bazılarıdır.[327] Ancak dikkatten kaçırılmaması gereken diğer bir husus da seçimlik hareketlerin işlenmeleri arasında ayrı bir suç oluşmasına yol açacak derecede zaman farkı olması durumunda

[322] Özbek/ Doğan/ Bacaksız/ Tepe, *Türk Ceza Hukuku Genel Hükümler*, s. 228

[323] Timur Demirbaş, **Ceza Hukuku Genel Hükümler**, Seçkin Yayınları, 14. Baskı, Ankara 2019, s.242

[324] Özbek/ Doğan/ Bacaksız, *Türk Ceza Hukuku Özel Hükümler*, s.598

[325] Özbek/ Doğan/ Bacaksız/ Tepe, *Türk Ceza Hukuku Genel Hükümler*, s. 228

[326] Dülger, *Kişisel Verilerin Korunması Hukuku*, Hukuk Akademisi, 3. Baskı, İstanbul 2020, s.731; Korkmaz, *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması* (2019), s.448; Soyaslan, s.366; Hasan Gerçeker, **Yorumlu Uygulamalı Türk Ceza Kanunu** Cilt 1, 5. Baskı, Seçkin Yayınları, Ankara 2020, s.1358; *"Seçimlik hareketlerden hepsinin birden yapılması suçun birden fazla olduğuna işaret etmez. Ortada yine de tek bir suç vardır. Ancak bu durumu hakim cezayı belirlerken dikkate alır."* Artuk/Gökcen/Yenidünya, *Ceza Hukuku Özel Hükümler*, s.20; Hakan Hakeri, **Ceza Hukuku Genel Hükümler**, Adalet Yayınevi, Ankara 2013, s.139

[327] Mahmut Koca/İlhan Üzülmez, **Türk Ceza Hukuku Genel Hükümler**, Seçkin Yayıncılık, Eylül 2017 Ankara, s.122

ayrı ayrı cezalandırma yapılması gerekeceğidir. Yargıtay da ele geçirme ve yayma fiillerinin arasında iki gün olan bir olayda bağımsız iki eylem olduğunu belirterek iki ayrı mahkumiyet hükmü kurulması gerektiğine karar vermiştir.[328]

Kişisel verilerin, hukuka aykırı olarak bir başkasına verilmesi, yayılması veya ele geçirilmesinde bu hareketlerin nasıl icra edileceği ile ilgili kanun koyucu bir özelleştirme yapmadığı için 136. maddedeki suçun serbest hareketli bir suç olduğunu belirtmemiz gerekir. Serbest hareketli suçlarda kanun, suçun fiil unsurunun nasıl gerçekleştirileceği yönünde spesifik bir düzenleme yapmamakta ve o suçun hangi hareketlerle icra edilebileceğini belirtmemektedir.[329] İnceleme konumuz olan suç tipinin nasıl işleneceği hususunun KVKK ile olan bağlantısına burada değinmekte fayda görüyoruz. Şöyle ki çalışmamızın ilk bölümünde yer alan Kişisel Verilerin İşlenmesi başlığı altında da değindiğimiz üzere 136. maddede yer alan seçimlik hareketlerin hepsi 6698 sayılı Kişisel Verilerin Korunmaası Kanunu'nda tanımlanan kişisel verilerin işlenmesi kavramı kapsamına girmektedir. Ancak yine belirttiğimiz üzere söz konusu suçun, veri işleme faaliyetinin tanımında yer alan otomatik veya otomatik olmayan yolların her ikisinin de araç olarak kullanılması suretiyle işlenebilmesi mümkündür.[330] Böylece suça konu verilerin otomatik olmayan yollarla ve herhangi bir veri kayıt sisteminin de parçası olmayacak şekilde verilmesi, yayılması veya ele geçirilmesi sonucunda da 136. maddedeki suç meydana gelecek ancak KVKK bağlamında bir veri işleme faaliyetinden bahsedilemeyecektir.

Maddede sayılan fiillere bakıldığında verme, yayma ve ele geçirme şeklinde düzenledikleri ve bu hareketlerin kanun koyucu tarafından yapılmaması gereken fiiller olarak kabul edildiği görülecektir. İcrai suç, işte bu şekilde kanun koyucunun yapılmamasını istediği hareketin aktif bir şekilde gerçekleştirilmesi sonucu oluşan suç tipi olarak kabul edilmektedir. Şöyle ki bu türden suçlarda yapılması yasaklanan fiile ilişkin ihlal, olumlu bir davranışla ortaya konulmuş olur. Türk Ceza Kanunu m.81'de düzenlenen kasten öldürme suçu icrai suça örnek olarak verilebilecektir.[331] Bu doğrultuda değinmek gerekirse 136. maddede düzenlenen suç, icrai suçlar arasında yer almaktadır. Ayrıca hareket sayısı bakımından da bu suç tek hareketli suçlardandır. Tek hareketli suçlarda suçun sübutu için tek bir hareketin yapılması yeterli olmakta ve kanunda birden fazla hareket suçun oluşması için aranmamaktadır.[332]

---

[328] YARGITAY 12. CEZA DAİRESİ E. 2017/3570 K. 2018/808 T. 24.1.2018

[329] Demirbaş, s.228

[330] Kader Sarıusta, **Kişisel Verilerin Ceza Hukuku Yoluyla Korunması**, Yüksek Lisans Tezi, Gaziantep Temmuz 2018, s.153

[331] İçel, s.278

[332] Demirbaş, s.229

Verileri hukuka aykırı olarak verme, yayma veya ele geçirme suçunu ihdas eden kanun koyucu ileride ayrıntısıyla inceleyeceğimiz hareket çeşitlerini düzenlerken verme ve yayma fiilini kişisel veriyi elinde bulunduran kişi açısından ele almışken ele geçirme hareketini ise verinin elinde bulunmadığı ancak buna sahip olmak isteyen kişi açısından değerlendirmiştir.[333] Bununla birlikte suça konu verilerin önceden hukuka uygun olarak kaydedilmiş olup olmamasının da 136. madde açısından önem arz etmediği maddenin gerekçesinde belirtilmiştir.[334] Son olarak değinelim ki maddede sayılan üç farklı fiilin de hukuka aykırı olarak gerçekleştirilmesi gerekir. Hukuka aykırılık unsuru başlığı altında bu konu ayrıntısıyla izah edilecektir.

4.1.1.1. Verme

"Vermek" fiili sözlükte *"Düşünce veya bilgi anlatan şeyleri başkalarına iletmek, bildirmek"* olarak tanımlanmaktadır.[335] Verme ve yayma fiilleri birbirine oldukça benzemekle birlikte kanun koyucunun burada birbirinden farklı iki hareketi cezalandırmak istediği anlaşılmaktadır. Şöyle ki vermek, yaymaktan daha dar kapsamlı bir eylemdir. Verme durumunda kişisel verilerin mağdur dışındaki bir üçüncü kişiye verilmesi söz konusuyken yayma halinde birden fazla kişiye kişisel verilerin iletilmesi gündeme gelir.[336] Aslında verme ve yayma fiilleri aynı amacı gerçekleştirmektedir. Zira iki fiilde de bir diğer kişi/kişilere suça konu verinin aktarımı söz konusudur. Ancak kişisel verilerin hukuka aykırı olarak verilmesinde iki kişinin arasında meydana gelen bir fiilden söz edilmekteyken verilerin yayılması durumunda tek kişi ile sınırlı kalınmayıp birden fazla kişiye veri aktarımı olmaktadır.[337] Bu noktada 136. maddenin lafzı, verme ve yayma fiillerinin ayrımında yol gösterici olacaktır. Nitekim verme hareketi düzenlenirken *"bir başkasına verme"* tabiriyle kişisel verilerin bir üçüncü kişiye verilmesi ve birden fazla kişiye verilmesi arasındaki sınır çizilmiştir.[338] Söz konusu iki fiilin farklılığını somutlaştırmak açısından örnek vermek gerekirse kişinin fotoğraflarının başka bir kişiye Watsapp uygulaması üzerinden gönderilmesi verme eylemini oluşturacakken fotoğrafların Twitter, Facebook gibi sosyal medya platformlarında herkesin görebileceği şekilde yayınlanmasıyla yayma fiilinin icra edilmiş sayılacağını belitmemiz gerekir.

---

[333] Mustafa Artuç, **Kişilere Karşı Suçlar**, Adalet Yayınevi, 2. Baskı, Ankara 2018, s.1647

[334] *"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."* Bkz. 136. madde gerekçesi.

[335] TDK, **Güncel Türkçe Sözlük**

[336] Mustafa Artuç, **Pratik Türk Ceza Kanunu**, 5.Baskı, Ankara 2019, Adalet Yayınevi, s.767

[337] Özbek/ Doğan/ Bacaksız, *Türk Ceza Hukuku Özel Hükümler*, s.597; Artuç, *Kişilere Karşı Suçlar*, s.1647

[338] Veysel Gültaş, **Özel Hayata Karşı Suçlar**, Bilge Yayınevi, Ankara 2016, s.222

Maddede belirtilen başkası ibaresi ile gerçek kişiler yanında tüzel kişiler de kast edilmekle birlikte kişisel veriler şirket, dernek gibi tüzel kişilere verilecek olursa da bu suç oluşacaktır.[339] Bunun sonucunda günümüzde sıkça karşılaşılan çeşitli şirketlere (örneğin bankalara, sigorta şirketlerine) veri aktarımını konu alan eylemler de yaptırıma bağlanmış olmaktadır.

Verileri hukuka aykırı olarak verme veya ele geçirme suçunun gerekçesinde de belirtildiği üzere bu suçun oluşumu açısından suça konu verilerin hukuka uygun veya aykırı olarak kaydedilmiş olmasının herhangi bir önemi yoktur. Suç, maddede belirtilen seçimlik hareketlerden birinin veya birkaçının yapılmasıyla vücut bulacaktır. Bu hususa ek olarak cevaplanması gereken diğer bir soru ise 136. maddede yer verilen suçun sübutu açısından verilerin kaydedilmesinin zorunluluk arz edip etmediği meselesidir. Şöyle ki Türk Ceza Kanunu'nun 135. maddesinde düzenlenen kişisel verilerin kaydedilmesi suçu, 136. maddede ihdas edilen suçun oluşumu açısından mecburi bir şart olarak aranmamaktadır. Ayrıca yine bu madde –TCK m.136- kendi içinde de kaydetme unsuruna yer vermemektedir.[340]

Madde de verme eyleminin nasıl icra edileceği ile ilgili herhangi bir özelleştirme yapılmamıştır. Bunun sonucu olarak veriler bizzat elden (evrak, CD, USB bellek, hafıza kartı vb.) teslim edilebileceği gibi elektronik ortamda da (e-mail, watsapp, twitter, facebook, sms) iletilebilecektir. Yargıtay Ceza Genel Kurulu'na göre de *"...veriler ... elden, posta ya da internet üzerinden elektronik posta ile vb. şekillerde verilebilecektir."*[341] Son olarak değinelim ki, kamu kurumları veya özel kuruluşlar tarafından hukuka uygun olarak tutulan verilerin hukuka aykırı olarak başkasına verilmesinde de 136. maddedeki suç oluşacaktır.[342]

4.1.1.2. Yayma

"Yaymak" fiili TDK'de *"Birçok kimseye duyurmak"* olarak tanımlanmıştır.[343] Verme fiilinin yaymaya nazaran daha dar kapsamlı olduğu ve yayma düzeyine ulaşmayan bir hareket olduğunu yukarıda belirtmiştik. Kişisel verilerin hukuka aykırı olarak yayılmasında birden fazla kişiye bu verilerin iletilmesi söz konusudur. Verilerin yayılması ile birlikte mağdura ait veriler artık diğer kişilerin bilgisine sunulmaktadır.[344] 5237 Sayılı TCK'nin Hükümet Tasarısı'nın 198. maddesinde yayma fiili, "*Kişisel verileri, yetkisiz kişilere veren, ifşa eden ... hapis cezası*

[339] Karagülmez, s.402

[340] Dülger, *Kişisel Verilerin Korunması Hukuku*, s.733-736. Yazar, konuyla ilgili olarak verilerin ele geçirilmeden de teknolojik imkanlar vasıtasıyla artık yayılmasının mümkün olduğunu ve bilgilerin herhangi bir kaydetme faaliyetine konu olmadan verme ya da yayma fiillerine konu olabileceğini belirtmektedir.

[341] YARGITAY CEZA GENEL KURULU E. 2012/12-1510 K. 2014/331 T. 17.06.2014

[342] Metin Çokmutlu, **Türk Ceza Hukukunda Kişisel Verilerin Korunması**, Doktora Tezi, Kocaeli 2014, s.219

[343] TDK **Güncel Türkçe Sözlük**

[344] YARGITAY 12. CEZA DAİRESİ E. 2013/30406 K. 2014/2980 T. 10.2.2014

verilir."[345] şeklinde düzenlenmişti. Ancak bu ifşa kelimesi Adalet Komsyonu'nda "yayma" olarak değiştirilmiştir. Zira Adalet Komisyonu görüşmelerinde yayma kelimesinin özellikle görüntünün ifşasını belirttiği vurgulanmıştır.[346] 136. madde ile ilgili olarak Hükümet Tasarısı'nda yer alan "ifşa" kelimesinden de görüleceği üzere burada kişisel verilerin birden fazla kişiye yayılmasının ve bu şekilde verme eyleminden farklı bir eylemin cezalandırılması amacı güdüldüğü anlaşılmaktadır.

Yayma fiilinin nasıl icra edileceği maddede özel olarak belirtilmemiştir. Bu suretle yayma elden teslim[347](örneğin evrak, CD, harici disk, hafıza kartı, USB bellek) veya sms, mail iletisi[348] şeklinde olabileceği gibi verilerin, herkesin erişebileceği şekilde bir web sayfasında[349], radyo, televizyon ve gazetede, sosyal medya sitelerinde paylaşılması şeklinde de olabilir.[350] Özellikle sosyal medyada başka kişilerin kişisel verilerinin kullanılması suretiyle sahte hesap açılması son yıllarda çokça karşımıza çıkmaktadır. Örneğin Yargıtay kararına[351] konu bir olayda sanığın başkasının fotoğrafını kullanarak Facebook hesabı açması şeklindeki hareketi, kişinin resminin kişisel veri niteliği taşımasından bahisle 136. madde kapsamında değerlendirilmiştir.

Kişisel veri sahibinin, 3. kişilerin öğrenmesini arzu etmeyeceği bilgilerini kendi rızası olmadan öğrenen kişi sayısının verme fiilindekine nazaran artmış olması hareketin ağırlığını -yani özel hayatı ihlal boyutunu- daha da artırmaktadır. Günümüzde teknolojinin geldiği nokta göz önüne alındığında başkasına ait kişisel veriler tek tuşla milyonlarca hatta milyarlarca kişinin erişimine açılabilmektedir. Bundan dolayı yayma fiilinde kişisel verilerin korunması hakkı özelinde özel

---

[345] Türk Ceza Kanunu Tasarısı, s.53

[346] Karagülmez, s.402

[347] *"Katılanın diz kapağı ile başı arasındaki kısmının görüntülendiği fotoğrafların üzerine, adı ve kızlık soyadı ile evlendikten sonra edindiği soyadı ve telefon numarasını yazarak katılanın iç çamaşırlarına ve geceliğine zımbalayıp katılanın oturduğu bina ile Adapazarı ve Hendek ilçelerindeki bir kısım binalara ve sokaklara bıraktığı olayda katılanın kişisel veri niteliğindeki ad, soyad ve cep telefonu numarasını hukuka aykırı şekilde yaymasının TCK'nın 136. maddesindeki verileri hukuka aykırı olarak verme veya ele geçirme suçunu oluşturduğu"* YARGITAY CEZA GENEL KURULU E. 2015/12-708 K. 2019/414 T. 9.5.2019

[348] YARGITAY 12. CEZA DAİRESİ E. 2012/25427 K. 2013/15774 T. 10.6.2013

[349] Mağdurun rızası dışında telefon numarası kullanılarak arkadaşlık sitesinde profil oluşturulması ve bunun üzerine websitesine giren kişilerce mağdura mesajlar gönderilmesi olayında Yargıtay 136. maddedeki suçun oluştuğuna kanaat getirmiştir. Bkz. YARGITAY CEZA GENEL KURULU E. 2017/12-829 K. 2017/363 T. 4.7.2017

[350] Ceza Genel Kurulu bir kararında yayma hareketi ile ilgili olarak bu hareketin farklı biçimlerde işlenebileceğini websitesinde kişisel veri yayınlama, verileri birden çok kişiye e-posta veya telefon aracılığıyla kısa mesajla gönderme veyahut kişisel verileri yazılı ya da görsel medyada yayınlamanın bu meyanda olduğunu belirtmiştir. Bkz. YARGITAY CEZA GENEL KURULU E. 2015/12-708 K. 2019/414 T. 9.5.2019

[351] *"Mağdurun kişisel veri niteliğindeki resmini, hukuka uygunluk nedenlerinin bulunmaması sebebiyle hukuka aykırı olduğunda tereddüt bulunmayan bir yöntemle "Nesrin Hülya E." adlı facebook hesabı üzerinden başkalarının görgüsüne sunan sanık hakkında, genel kastla işlenen verileri hukuka aykırı olarak verme veya ele geçirme suçundan dolayı mahkumiyet kararı verilmesine dair yerel mahkemenin kabulünde bir isabetsizlik görülmemiştir."* YARGITAY 12. CEZA DAİRESİ E. 2015/13248 K. 2017/3108 T. 12.4.2017

hayatın gizliliği ve korunmasının, verme hareketine oranla daha büyük bir ihlalle karşı karşıya kaldığını söylemek yanlış olmayacaktır.

Günümüzde evli, yakın arkadaş veya iş ortağı olan kişilerin birlikte aynı e-mail veya sosyal medya hesabını kullanmasına sıkça rastlanmaktadır. Bu kişilerin, söz konusu hesapları ortak kullanmalarına neden olan ilişkileri bittikten sonra (örneğin boşanma durumunda) birbirlerine ait bilgileri yine ortak kullanımlarındaki hesaplardan yayınlaması da 136. maddedeki yayma hareketini meydana getirecektir.

136. maddedeki seçimlik hareketlerden olan yayma fiilinin en çok karşımıza çıktığı diğer durumlardan birisi ise kişinin fotoğraflarının çeşitli internet sitelerinde yayınlanmasıdır. Özellikle bireylerin boşandıktan sonra evli oldukları süreçteki ya da arkadaşlık ilişkisi biten kişilerin, ilişkileri devam ederken çekildikleri fotoğrafların sosyal medyada servis edilmesine son zamanlarda birçok kez tanık olunmuştur. Bu ve benzeri olaylarda Yargıtay, yayınlanan fotoğrafın niteliğine bakmakta ve elde edilen sonuca göre söz konusu eylemi 134. veya 136. madde kapsamında değerlendirmektedir.[352] Yargıtay'ın istikrar kazanan uygulamasında özel hayata ilişkin görüntü ve sesin kişisel veri niteliği taşıdığında kuşku bulunmadığı ancak bu bilgilerin yayılması fiilinin 134. maddede düzenlenmesi nedeniyle suça konu verilerin 136. madde anlamında kişisel veri olmadığı tespitinde bulunulmakta ve özel hayatın gizliliğini ihlal (m.134) suçundan hüküm kurulması gerektiği vurgulanmaktadır.[353] Bazı kararlarda ise suça konu görüntüler özel hayat kapsamında görülmeyip 136. maddenin uygulanması gerekliliği dile getirilmiştir.[354]

[352] YARGITAY 12. CEZA DAİRESİ E. 2018/8360 K. 2019/9056 T. 18.9.2019; Aynı yönde bkz. YARGITAY 12. CEZA DAİRESİ E. 2019/536 K. 2019/10825 T. 13.11.2019

[353] Bkz. YARGITAY 12. CEZA DAİRESİ E. 2017/3928 K. 2018/3190 T. 21.3.2018; YARGITAY 12. CEZA DAİRESİ E. 2012/20543 K. 2012/20422 T. 2.10.2012; YARGITAY 12. CEZA DAİRESİ E. 2018/8360 K. 2019/9056 T. 18.9.2019; YARGITAY CEZA GENEL KURULU E. 2015/12-708 K. 2019/414 T. 9.5.2019 Ceza Genel Kurulu bu kararında sanığın, katılanın baş ve diz kapağı arasındaki kısmının görüntülendiği fotoğrafların üzerine katılanın ad, soyad ve telefon numarasını yazarak çeşitli yerlere bırakıp ifşa ettiği olaya ilişkin olarak, fotoğrafları ve fotoğrafların üzerine yazılı bilgileri ikiye ayırarak incelemiş ve görüntülerin yayılmasının 134. madde kapsamında; ad, soyad ve telefon numarası gibi bilgilerin yayılmasının ise 136. madde kapsamında olduğuna hükmetmiştir. Benzer nitelikte bir karar için bkz. YARGITAY 12. CEZA DAİRESİ E. 2018/8327 K. 2019/8315 T. 10.7.2019; Ayrıntılı açıklamalar için bkz. İçtima başlığı

[354] YARGITAY 12. CEZA DAİRESİ E. 2018/8198 K. 2019/6187 T. 15.5.2019; YARGITAY 12. CEZA DAİRESİ E. 2018/4902 K. 2018/11057 T. 21.11.2018; YARGITAY
12. CEZA DAİRESİ E. 2017/7527 K. 2018/3987 T. 4.4.2018; YARGITAY 12. CEZA DAİRESİ E. 2015/11703 K. 2017/870 T. 8.2.2017; YARGITAY 12. CEZA DAİRESİ E. 2015/11112 K. 2017/637 T. 1.2.2017; YARGITAY 12. CEZA DAİRESİ E. 2017/2960 K. 2018/1541 T. 14.2.2018; YARGITAY 12. CEZA DAİRESİ E. 2016/6247 K. 2017/6230 T. 13.9.2017; YARGITAY 12. CEZA DAİRESİ E. 2015/14419 K. 2017/3118 T. 12.4.2017; YARGITAY 12. CEZA DAİRESİ E. 2018/8198 K. 2019/6187 T. 15.5.2019

İnceleme konumuz olan fiil basın ve yayın araçlarıyla etkin olarak işlenebilir. *"Zira ifade ve basın özgürlüğü kapsamında internet ortamına yüklenen haber ve fikirler çoğu kez kişisel verilerin de kullanılmasını ve işlenmesini beraberinde getirir."*[355] Bu bağlamda, Yargıtay'ın da kararına konu bir olayda, mağdurun cep telefonu numarasının kendi rızası olmaksızın filmde yayınlanması fiili 136. madde kapsamında kabul edilmiştir.[356]

Yayma eyleminde yayılan kişisel verilerin ulaşılabilir olması gerekir. Yayma açısından kişisel verilerin üçüncü kişiler tarafından öğrenilebilir hale getirilmesi yeterlidir ve ayrıca suça konu verilerin öğrenilmiş olması veya algılanmış olması aranmamaktadır.[357]

Ölen kişinin kişisel verilerinin de öldükten sonra açıklanmaması gerekliliğinin kanunun amacına uygun olduğu belirtilmektedir.[358] Ölen kişinin verileri ile ilgili olarak Alman Ceza Kanunu'nda yer alan düzenlemeye çalışmamızın ilk bölümünde değinilmişti.[359]

Son olarak yayma fiiline verilebilecek diğer bir örnek ise toplu e-mail gönderme işlemidir. Bu tarz maillerde cc kısmında birbiriyle alakası olmayan birçok kişi yer alabilmektedir. Böylelikle kişisel veri niteliğindeki e-mail adresleri, adres sahibinin tanımadığı birçok kullanıcının eline geçmektedir. Bu nedenle toplu mail atımlarında dikkatli olunmalı ve Bcc kısmının kullanılarak e-mail adreslerinin birbirini tanımayan kişiler arası dolaşımı engellenmelidir.

4.1.1.3. Ele Geçirme

Ele geçirme eylemi *"sahibi olmak"* ve *"gizlenmek istenen bir şeyi elde etmek"* anlamlarına gelmektedir.[360] Ele geçirme hareketi ile fail, hukuka aykırı yolları kullanarak başka bir kişiye ait kişisel verilere sahip olmakta ve böylece ele geçirilen veriler üzerinde yasal olmayan tasarruf yetkisine sahip olmaktadır.[361]

Kişisel verilerin ele geçirilmesi farklı şekillerde meydana gelebilir. Bu noktada esas olan ele geçirmede kullanılan yolun hukuka aykırı olmasıdır.[362] Ele geçirme fiili kaydetme şeklinde de icra edilebilir. Ancak bu durumda kaydetme fiilinin 135. maddede başkaca bir suç tipi olarak

---

[355] AYM, N.B.B. Başvurusu R.G. Tarih ve Sayı : 24/8/2016-29811

[356] YARGITAY 12. CEZA DAİRESİ E. 2018/8182 K. 2019/5890 T. 8.5.2019; YARGITAY 12. CEZA DAİRESİ E. 2018/4902 K. 2018/11057 T. 21.11.2018

[357] Aysun, s.108, dn.350 ve s.109, dn.354

[358] Sabire Sanem Yılmaz, **Tıp Alanında Kişisel Verilerin Açıklanması Suçu**, Nisan 2019 Ankara, s.121

[359] Bkz. dn. 25

[360] TDK Güncel Türkçe Sözlük

[361] Şahbaz, s.1599; Handan Yokuş Sevük, **Türk Ceza Hukuku Özel Hükümler**, Adalet Yayınevi, Ankara 2020, s.498; *"Kişisel verileri ele geçirmek, o verileri yakalamak, onların sahibi olmaktır."* Hafızoğulları/ Özen, *Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar*, s.21

[362] Gültaş, s.222

düzenlenmesi nedeniyle 136. maddedeki ele geçirme hareketinin kaydetme şeklinde olmayan icra şekillerini kapsadığını vurgulamamız gerekmektedir.[363] Bazı yazarlar ise örneğin sistemdeki verilerin USB, CD-rom, hafıza kartı gibi depolama aygıtlarına kaydedilip bunların alınmasıyla da ele geçirmenin meydana gelebileceğini savunmaktadır.[364]

Yargıtay'ın bu noktadaki görüşü, kişisel verinin kaydedilmiş haliyle başka bir nesne üzerine taşınarak sabitlenmesi ve istenildiğinde tekrar kullanılabilmesini sağlayan her türlü faaliyetin ele geçirmeye vücut vereceği yönündedir. Taşımanın ise yazının başka bir kağıt, defter vb. nesne üzerine geçirilmesi, taşınabilir belleğe veya CD'ye aktarılması gibi işlemler olduğu birçok kararda belirtilmiştir.[365] Örneğin Yüksek Mahkeme kararına konu olayda sanık, kendisine tamir için bırakılan dizüstü bilgisayardaki fotoğraflar ile elektronik posta adres ve şifreleri ele geçirip flash diske aktarmıştır. Mahkeme burada 135. maddedeki kişisel verileri kaydetme suçunun değil; 136. maddedeki verileri verme, yayma, ele geçirme suçunun oluştuğuna hükmetmiştir.[366] Diğer bir karara konu olayda ise kredi kartı bilgilerinin kopyalama yöntemiyle cihaza aktarımı durumunda mağdur sayısınca kişisel verileri hukuka aykırı olarak ele geçirme suçunun oluşacağı belirtilmiştir.[367]

Suçun oluşması açısından ele geçirilen kişisel verilerin saklanması veya söz konusu veriler ele geçirildikten sonra belirli bir sürenin geçmesi aranmamaktadır.[368]

Ele geçirme hareketi ile ilgili olarak üzerinde durulması gereken diğer bir husus ise söz konusu seçimlik hareketin kişisel verilerin kaydedilmesi ile olan ilişkisidir. Şöyle ki *Koca/Üzülmez'e* göre kişisel verilerin ele geçirilmesi bu verilerin kaydedilmesi açısından gereklidir. Bu durumda kaydetmeden önce hukuka uygun bir şekilde sahip olunan verilerin sonradan kaydedilmesi suç oluşturmayacaktır. Ancak kaydetmeye konu veriler daha öncesinde hukuka aykırı olarak ele geçirilmiş ise hem kişisel verilerin kaydedilmesi suçu oluşacak hem de verileri hukuka aykırı

---

[363] Özbek/ Doğan/ Bacaksız, *Türk Ceza Hukuku Özel Hükümler*, s.598; Kişisel verilerin kaydedilmesi suçu ile ele geçirme fiili arasındaki ilişkiye ilişkin değerlendirmeler için bkz. Kerim Çakır, **Kişisel Verilerin Kaydedilmesi Suçu**, Antalya Bilim Üniversitesi Hukuk Fakültesi Dergisi, Cilt 8, Sayı:16, Aralık 2020, s.575

[364] Sarıusta, s.155-156, dn.611

[365] *"Kişisel verilerin, üzerinde yazılı olduğu belgenin bulunduğu yerden alınması ya da kaydedilmiş haliyle başka bir nesne üzerine taşınarak (örneğin; yazının başka bir kağıt, defter vb. nesne üzerine geçirilmesi, taşınabilir belleğe veya CD'ye aktarılması gibi işlemlerle) sabitlenmesi, böylece istenildiğinde tekrar kullanılabilmesi olanağını sağlayan her türlü faaliyet, kişisel verileri "ele geçirme" kapsamında değerlendirilebilir ise de…"* YARGITAY 12. CEZA DAİRESİ E. 2016/2168 K. 2016/5860 T. 6.4.2016; Aynı yönde bkz. YARGITAY 12. CEZA DAİRESİ E. 2018/8152 K. 2019/4886 T. 10.4.2019; YARGITAY 12. CEZA DAİRESİ E. 2017/3928 K. 2018/3190 T. 21.3.2018; YARGITAY 12. CEZA DAİRESİ E. 2017/12083 K. 2018/2539 T. 7.3.2018; YARGITAY 17. CEZA DAİRESİ E. 2015/25941 K. 2018/126 T. 8.1.2018; YARGITAY 12. CEZA DAİRESİ E. 2014/9139 K. 2014/20323 T. 20.10.2014

[366] YARGITAY 12. CEZA DAİRESİ E. 2013/15899 K. 2014/8411 T. 7.4.2014

[367] YARGITAY 8. CEZA DAİRESİ E. 2018/10126 K. 2019/1793 T. 11.2.2019

[368] Bük, s.151, dn.490

olarak verme veya ele geçirme suçu meydana gelecektir fakat yazarlar ortaya çıkan bu sonuca bir eleştiri getirmektedir. Zira ele geçirmenin ardından bu veriler ayrıca kaydedilirse fail iki ayrı suçtan ceza alacak ve işlediği fiilin haksızlık derecesine nazaran daha ağır bir yaptırımla karşılaşacaktır. Nitekim kaydetme fiili, ele geçirmede meydana gelen haksızlığın ağırlığını da taşımaktadır ve verilerin ele geçirilmesi durumundaki haksızlık, kaydetme fiilindekine oranla daha azdır. Ayrıca ele geçirmeye konu olan bilgiler kaydedilmez, başkasına verilmez veyahut yayılmaz ise ele geçirme fiili hazırlık hareketi niteliğindedir ve cezalandırılmaması gerekir. Bununla birlikte ele geçirme hareketi, diğer fiiller olan verme, yayma ya da kaydetme ile anlaşılabilecek niteliktedir. Bu bağlamda yine müelliflere göre ele geçirme seçimlik hareketi 136. maddeden çıkarılmalıdır. Son olarak olarak yazarlar, 136. maddede sayılan üç seçimlik hareketin haksızlık içeriği bakımından yakın derecede olması gerektiğini ancak ele geçirme fiilinin bu açıdan diğer iki fiille bir denklik içerisinde olmadığını belirtmektedirler.[369]

136. maddedeki suç serbest hareketli suç özelliği gösterdiğinden verme ve yayma eylemlerinde de bahsedildiği üzere ele geçirme fiilinin de gerçekleştiriliş şekli noktasında yasada bir özelleştirme yoluna gidilmemiştir.[370] Bunun sonucunda ele geçirme eylemi farklı şekillerde gerçekleştirilebilir. Örneğin verilerin muhafaza edildiği belgelerin bulunduğu yerden alınması veya söz konusu kişisel bilgilerin tutulduğu bilişim sistemine girilerek bu bilgilerin veri taşıma araçlarına (örneğin CD, disket, USB bellek, harici disk) aktarılması sonucu suç oluşacaktır.[371] Yargıtay da bir kararında[372] *"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 işlemler) sabitlenmesi, böylece istenildiğinde tekrar kullanılabilmesi olanağını sağlayan her türlü faaliyet, kişisel verileri "ele geçirme" kapsamında değerlendirilebilir…"* şeklinde bir değerlendirme yapmıştır. Bu aşamada ele geçirme fiilinin somutlaşması açısından güncel örneklere değinmekte fayda görmekteyiz. Günümüzde teknolojinin geldiği safha düşünüldüğünde kişisel verilerin ele geçirilmesi birçok farklı ve tehlikeli yöntemle icra edilebilmektedir. Örneğin sanal ağlar aracılığıyla truva atı gibi yazılımlar kullanılarak mağdurların kullanmakta oldukları bilişim sistemlerine kapalı olsa dahi erişim sağlanmak

---

[369] Koca/ Üzülmez, *Kişisel Verilerin Kaydedilmesi Suçu* s. 69-93, s.80; Kerim Çakır, **Kişisel Verilerin Kaydedilmesi Suçu**, Antalya Bilim Üniversitesi Hukuk Fakültesi Dergisi, Cilt 8, Sayı:16, Aralık 2020, s.592

[370] Ceza Genel Kurulu'nun bir kararında *"Kişisel verilerin ele geçirilmesi" seçimlik hareketi ise; kişisel verilerin kayıtlı olduğu belgelerin alınması ya da kayıtlı olduğu bilişim sisteminden ele geçirilmesi vb... şekillerde gerçekleştirilebilecektir. Ele geçirme fiili, başkasının hakimiyeti altında bulunan bir kişisel verinin, failin hakimiyeti altına girmesi ile gerçekleşmiş olacaktır."* şeklinde ifadelere yer verilmiştir. E. 2017/829, K. 2017/363, T. 4.7.2017

[371] Şaban Cankat Taşkın, **Bilişim Suçları**, Bursa 2008, Beta Yayınları, s.107

[372] YARGITAY 12. CEZA DAİRESİ E. 2017/12083 K. 2018/2539 T. 7.3.2018

suretiyle kişisel veriler ele geçirilebilmektedir. Aynı zamanda hafıza kartları, USB bellek gibi veri depolayıcıların fiziken içinden veri çekilecek olan aygıtlara takılarak veri aktarımı yapılması da suça vücut verecektir.[373] Son olarak belirtelim ki failin bir şirketin sistemine girerek şirket müşterilerinin bilgilerini kopyalaması[374], bilgisayarların hafızası sayılan donanımların sökülmesi ve kişisel veri içeren liste kağıtlarının bulunduğu yerden alınması gibi haller de ele geçirme fiiline örnek olabilecektir.

Ele geçirme fiili ile ilgili önem arz eden diğer bir konu ise suça konu verilerin duyu organları aracılığıyla öğrenilmesi ve/veya bu şekilde öğrenilen bilgilerin başka kişilere aktarılması durumunda hangi suçların oluşacağı hususudur. Söz konusu hukuki problem Yargıtay'ın çeşitli kararlarında farklı şekilde ortaya konmuştur. Yüksek Mahkeme kimi kararlarında kişisel verilerin kaydedilmeden önceden öğrenilmesi veya hafızada tutulan verilerin başkasına açıklanması yahut bu verilerin salt duyu organlarıyla elde edilmesini özel hayatın gizliliği ihlal suçu kapsamında değerlendirmiştir.[375] Buna karşılık diğer bazı kararlarda ise sadece duyu organlarıyla suça konu verilere vakıf olunması 136. madde kapsamında değerlendirilmiştir.[376] Aynı şekilde mağdura ait verilerin duyu organlarıyla öğrenilerek diğer kişilere ifşa etme eylemi de inceleme konumuz suç kapsamında değerlendirilmektedir.[377]

Teknolojinin hızlı gelişmesi devlet kurumlarının kullandığı birçok sistemin elektronik ortama aktarılması sonucunu doğurmuştur. Ancak söz konusu sistemler, kendi içlerinde vatandaşlara ait

---

[373] Dülger, *Kişisel Verilerin Korunması Hukuku*, s.740; Sarıusta, s.156

[374] Gültaş, s.222;

[375] YARGITAY 12. CEZA DAİRESİ E. 2017/3928 K. 2018/3190 T. 21.3.2018; Aynı yönde bkz. YARGITAY 12. CEZA DAİRESİ E. 2017/2960 K. 2018/1541 T. 14.2.2018; YARGITAY 17. CEZA DAİRESİ E. 2015/25941 K. 2018/126 T. 8.1.2018

[376] YARGITAY 12. CEZA DAİRESİ E. 2018/8152 K. 2019/4886 T. 10.4.2019*"Bu noktada belirtmek gerekir ki, kişisel verilerin, üzerinde yazılı olduğu belgenin bulunduğu yerden alınması ya da kaydedilmiş haliyle başka bir nesne üzerine taşınarak (örneğin; yazının başka bir kağıt, defter vb. nesne üzerine geçirilmesi, taşınabilir belleğe veya CD'ye aktarılması gibi işlemlerle) sabitlenmesi, böylece istenildiğinde tekrar kullanılabilmesi olanağını sağlayan her türlü faaliyet, kişisel verileri "ele geçirme" kapsamında değerlendirilebileceği gibi, kişisel verilerin kaydedilmeden önce öğrenilmesi, kişisel verilere salt duyu organları aracılığıyla vakıf olunması da aynı kapsamda değerlendirilmelidir."*; Katılana ait verilerin okunmasının 136. maddedeki verileri hukuka aykırı olarak verme veya ele geçirme suçunu oluşturduğu yönünde bkz. YARGITAY 12. CEZA DAİRESİ E. 2019/578 K. 2020/5427 T. 21.10.2020; YARGITAY 12. CEZA DAİRESİ E. 2015/3691 K. 2015/7773 T. 11.05.2015; YARGITAY 12. CEZA DAİRESİ E. 2014/9139 K. 2014/20323 T. 20.10.2014 "*kaydedilmiş kişisel verilerin görme, okuma vb. eylemlerle içeriğinin öğrenilmesinin, kişisel verilerin ele geçirildiğinin kabul edilebilmesi için yeterli olduğu"*; Yalnızca öğrenmenin ele geçirme fiilini karşılamayacağı yönünde bkz. Murat Volkan Dülger, **Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması**, İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi 3 (2), Güz 2016; 101-167, s.132

[377] YARGITAY 12. CEZA DAİRESİ E. 2012/13104 K. 2012/14146 T. 5.6.2012 Bu kararında Yargıtay, sanığın özel bir Tıp Merkezinin bilgi sistemine girerek, psikiyatri anabilim dalında tedavi gören mağdure hemşirenin muayene bilgilerini okuduktan sonra hastane çalışanlarına ifşa etmesi eylemine ilişkin olarak söz konusu fiilin 136/1. maddedeki suçu oluşturacağı kanaatine varmıştır.

sayısız bilgiyi barındırdığından bu verilere sahip olmak isteyen kişilerce hedef alınabilmektedir. Örnek olarak değinmek gerekirse kişiye ait özel nitelikli veriler de dahil olmak üzere birçok bilginin yer aldığı e-devlet, e-nabız uygulamaları, UYAP, MERNİS gibi sistemler kişisel veriler açısından son derece önemlidir. Yargıtay'ın kararına[378] konu bir olayda da katip olarak görev yapan fail, şikayetçinin malvarlığına dair bilgilere erişebilmek için UYAP sistemini kullanıp şikayetçiyi dosyaya taraf olarak ekleyerek malvarlığını sorgulamış ve raporunu almıştır. Bunun üzerine Yüksek Mahkeme, verilen kovuşturmaya yer olmadığına dair karara yapılan itirazın reddine ilişkin olarak şüpheli hakkında kamu davası açılması gerektiğini belirterek kanun yararına bozma hükmü vermiştir.

Ele geçirmenin karşımıza çıktığı diğer bir durum ise sürmekte olan davada delil olarak sunma amacıyla davanın karşı tarafına ait kişisel verilerin çeşitli kuruluşlardan (banka, hastane vb.) temin edilerek mahkemeye getirilmesi halidir. Yargıtay çeşitli kararlarında delillendirme amaçlı yapılan bu eylemlerin suça vücut vermeyeceğini belirtmiş ayrıca mahkemelerin bu verilere gerektiğinde ulaşabilme imkanına sahip olduğuna da dikkat çekmiştir. Örneğin bir kararında[379] Yüksek Mahkeme, boşanma davasında delil olarak sunma amacıyla hastaneden elde edilen muayene raporuna ilişkin olarak davayı gören mahkemenin gerektiğinde söz konusu belgelerin aslını alabileceğini, sanığın mahkeme dışında üçüncü kişilere bahsi geçen belgeleri verdiğine dair herhangi bir iddia yer almadığını ve sanığın bu eyleminin mevcut davada delillendirme amacı güdülerek işlendiği gerekçesiyle beraat kararı verilmesinde bir isabetsizlik görmemiştir. Yüksek Mahkemenin genel uygulaması bu yönde olmakla birlikte farklı kararları da mevcuttur. Nitekim Yargıtay Ceza Genel Kurulunun verdiği bir kararda idareye verilecek şikayet dilekçesinin ekinde kullanılmak üzere doğum belgesinin hastaneden alınması ve dilekçede kullanılması 136. madde kapsamında görülmüştür.[380] 12. Ceza Dairesi'nin bir kararında ise kişinin rızası alınmaksızın banka hesap hareketlerinin, hakkında verilen suç duyurusuna ek

[378] YARGITAY 12. CEZA DAİRESİ E. 2017/12083 K. 2018/2539 T. 7.3.2018

[379] YARGITAY 12. CEZA DAİRESİ E. 2015/731 K. 2015/12033 T. 29.6.2015 Aynı yönde bkz. YARGITAY 12. CEZA DAİRESİ E. 2013/30307 K. 2014/16617 T. 7.7.2014: Hasta ile ilgili sağlık verilerinin (hasta bilgi formu ve röntgen filmi) kasten yaralama ve tehdit suçlarından açılan davada karşı kanıt olarak ileri sürülmesi amacıyla temin edilmesi ve mahkemeye sunulmasının ispatlama amacıyla hukuka aykırılık bilinci taşınmadan yapıldığına ilişkin olarak bkz. YARGITAY 12. CEZA DAİRESİ E. 2017/3928 K. 2018/3190 T. 21.3.2018; Bazı kararlarda ise aile birliğini koruma amaçlı yapılan eylemlerin suç oluşturmayacağı kabul edilmiştir. Bkz. YARGITAY 12. CEZA DAİRESİ E. 2018/8313 K. 2019/8077 T. 3.7.2019; YARGITAY 12. CEZA DAİRESİ E. 2015/10438 K. 2016/12933 T. 23.11.2016

[380] YARGITAY CEZA GENEL KURULU E. 2012/12-1514 K. 2014/312 T. 10.6.2014; Aynı yönde diğer bir kararda ise hakkındaki idari soruşturmada kullanılmak üzere sanığın katılana ait doğum raporunu hukuka aykırı olarak ele geçirip adı geçen soruşturmada kullanması üzerine 136. maddedeki suçun unsurlarının oluştuğu ifade edilmiştir. Bkz. YARGITAY 12. CEZA DAİRESİ E. 2011/15747 K. 2012/12099 T. 15.5.2012

olarak konulması eyleminin suç oluşturacağı sonucuna varılmıştır.[381] Kişisel verilerin farklı amaçlarla kullanılması yargılama safhalarında karşımıza çıkabildiği gibi yargılamadan sonra da görülebilmektedir. Buna ilişkin olarak Yargıtay'ın kararına konu bir olayda mahalli idareler seçiminde muhtar adayı olan sanık, diğer aday olan katılanın zimmet suçuna ilişkin temyiz aşamasında olan hakkındaki mahkumiyet kararını köy kahvesindeki panoya asmış ve bir saat sonra kaldırmıştır. Yüksek Mahkeme, sanığın o davada taraf olması hasebiyle kararın bir örneğine sahip olduğu ve bahse konu kararı hukuka aykırı olarak ele geçirmediği yönünde kanaat bildirmiştir.[382]

Ele geçirme, kişilerin kandırılıp kişisel verilerin verilmesinde araç olarak kullanılmasıyla da gerçekleştirilebilir. Örneğin kendisini, kendisiyle aynı adı taşıyan müdür yardımcısıymış gibi tanıtıp bir öğrencinin güvenini kazandıktan sonra o öğrenciden okuldaki diğer öğrencilerin bilgilerini temin eden sanığın eylemi de 136. madde kapsamında değerlendirilmiştir.[383]

4.1.2. Fail

Kişisel verileri hukuka aykırı olarak verme, yayma veya ele geçirme suçunun faili, kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan ya da bu verileri ele geçiren kişidir. Madde metninde de görüleceği üzere 136. maddedeki suçun faili herkes olabilecektir. Suç tipi açısından fail olmak için ayrıca herhangi bir kriter aranmadığından bu suç özgü suçlardan değildir.[384] Bahis konumuz olan suçun kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle veya belli bir meslek ve sanatın sağladığı kolaylıktan yararlanılarak işlenmesi hali 137. maddede daha ağır cezayı gerektiren nitelikli hal olarak öngörülmüştür. Bu kapsamda belirtmek gerekirse örneğin kişiye ait sağlık verilerinin bir doktor tarafından başkasına hukuka aykırı olarak verilmesi veya söz konusu bilgilerin ele geçirilmesi halinde 137. maddedeki nitelikli hal uygulanacaktır.[385] Suçun faili ile ilgili olarak düzenlenen nitelikli haller aşağıda ayrıntısıyla incelenecektir.

Tüzel kişiler ise bu suçun faili olamayacak ancak TCK m.140'taki koşullar oluştuğunda tüzel kişi hakkında güvenlik tedbiri uygulanacaktır.[386]

---

[381] YARGITAY 12. CEZA DAİRESİ E. 2016/9332 K. 2016/13355 T. 14.12.2016
[382] YARGITAY 12. CEZA DAİRESİ E. 2016/9332 K. 2016/13355 T. 14.12.2016
[383] YARGITAY 12. CEZA DAİRESİ E. 2015/9893 K. 2016/12504 T. 9.11.2016
[384] Gerçeker, s.1357; Artuç, *Kişilere Karşı Suçlar*, s.1645; Parlar/ Öztürk, s.545
[385] Sevük, s.495
[386] Hafızoğulları/ Özen, *Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar*, s.21

4.1.3. Mağdur

Çalışmamızın konusu olan verileri hukuka aykırı olarak verme veya ele geçirme suçu, mağdur unsuru açısından herhangi bir özellik arz etmemektedir ve bu suçun mağduru herkes olabilecektir.[387] 136. maddesinin 2. fıkrasında öngörülen nitelikli hal meydana geldiğinde ise suçun mağduru cinsel istismar ve cinsel saldırı suçlarının kendisine karşı işlendiği ve 5271 sayılı Ceza Muhakemesi Kanunu m. 236/5 ve 236/6'ya göre beyan ve görüntüleri kayda alınan kişiler olacaktır.[388]

Söz konusu suçun mağduru olabilmek açısından suça konu verilerin maliki veya zilyedi olmak aranmamakla birlikte burada aranan kriter 136. maddedeki hareketlere konu olan verilerin mağdurla ilgili olmasıdır.[389] Bunun yanı sıra mağdurluk açısından diğer bir önemli sorun ise tüzel kişilerin bahse konu suçun mağduru olup olamayacağı noktasında ortaya çıkmaktadır. Doktrinde bu konuyla ilgili farklı görüşler vardır. Kimi yazarlar[390] 136. maddedeki suçun mağdurunun yalnızca gerçek kişiler olabileceğini belirtirken kimi yazarlar[391] ise tüzel kişilerin de mağdur olabileceğini ifade etmektedir. Kanaatimizce KVKK m.3'te tanımı yapılan kişisel veri kavramı dikkate alındığında kişisel verinin ancak gerçek kişiyi ilgilendiren bilgilerden ibaret olduğunun açıkça ortaya konulduğu anlaşılmaktadır. Bu doğrultuda 136. maddedeki suçun mağdurunun yalnızca gerçek kişi olacağı ve tüzel kişilerin sadece suçtan zarar gören sıfatına sahip olabileceği belirtilmelidir.[392]

Söz konusu suçun işlenmesi ile mağdur olan kimse bu vakıa üzerine vakit kaybetmeden ilgili makamları haberdar etmeli ve kendisine karşı işlenen suça tepki olarak aynı davranışı faile karşı işlememelidir. Aksi halde kendisi de yeni bir verileri hukuka aykırı olarak verme veya ele geçirme suçunu işlemiş olacaktır. Örneğin Yargıtay kararına konu bir olayda mağdurun telefon numarası başka bir kişiye ait fotoğrafın altında sosyal medyada paylaşılmıştır. Akabinde verileri paylaşılan mağdur, kendisini cinsel içerikli arayan kişilere, artık telefon numarasını

---

[387] Gerçeker, s.1358

[388] Sevük, s.496

[389] Dülger, *Kişisel Verilerin Korunması Hukuku*, s.732; Aynı yönde bkz. Elif Mendos Kuşkonmaz, **Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması**, Yüksek Lisans Tezi, İstanbul 2013, s.154

[390] Hafızoğulları/ Özen, *Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar* s.21; Koca/Üzülmez'e göre 135-138. maddeler arasındaki suçların faili ve mağduru ancak gerçek olabilir. Bkz. Mahmut Koca/İlhan Üzülmez, *Kişisel Verilerin Kaydedilmesi Suçu*, s.73

[391] *"Tüzel kişilere ait verilerin de TCK'nin 135 ile 136. maddeleri kapsamında korunabileceğini belirtmek yanlış olmayacaktır."* Bkz. Bük, s.205; Soyaslan, s.364

[392] Aysun, s.107; Dülger, *Kişisel Verilerin Korunması Hukuku*, s.732; Yargıtay da bir kararında kişisel verilerin gerçek kişiye ait bilgiler olduğunu ve bu durumda katılana ait kredi kartı bilgileri hariç, şirkete ait mali bilgilerin ve programların "kişisel veri" olarak kabul edilemeyeceği şeklinde hüküm kurmuştur. Bkz. YARGITAY 12. CEZA DAİRESİ E. 2013/10672 K. 2013/15772 T. 10.6.2013; Bu suçun mağdurunun hem gerçek kişiler hem de tüzel kişiler olabileceği hakkında bkz. Soyaslan, s.353

değiştirdiğini söyleyerek kendi numarasını yayan ilk sanığın telefonunu vermiştir. Yargıtay ise burada m.136'daki suçun oluşacağını belirtmiştir.[393]

4.1.4. Konu

Kişisel verileri verme, yayma veya ele geçirme suçunun konusunu kişisel veriler oluşturmaktadır. Kişisel veri kavramının tanımlandığı 6698 sayılı Kişisel Verilerin Korunması Yasası'na göre kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi bu kapsamda 136. maddedeki suça konu olabilecektir. Söz konusu suç tipinin konusunu hangi türden bilgilerin oluşturabileceğini tek tek saymak mümkün olmamakla birlikte uygulamada sıkça karşılaşılan birtakım kişisel veri çeşitlerine değinmekte fayda görmekteyiz. Bu kapsamda kişinin adı ve soyadı, doğum tarihi, doğum yeri, mesleği, banka hesabı bilgileri, kimlik numarası, yargılandığı suçlar ve ceza mahkumiyeti bilgileri, girmiş olduğu internet sitesi çerezleri, parmak izi, posta kodu, fotoğrafı, IP adresi, medeni durumu, e-posta adresi, ikametgah bilgisi, kan grubu, görüntü ve ses kaydı, sağlık durumuna ilişkin bilgiler, üye olduğu sivil toplum kuruluşları, mali durumuna ilişkin bilgileri, telefon numarası, GPS bilgisi, HTS kaydı, banka kartı bilgileri gibi veriler bu suça konu olabilecektir. Suçun konusu açısından önem arz eden Yargıtay Ceza Genel Kurulunun E.2012/12-1510 K.2014/331 sayılı kararında da çeşitli açıklamalar yapılmış olmakla birlikte yine bu kararda bazı veriler örnekseme yoluyla sayılmıştır. Yukarıda belirttiğimiz bilgilerden farklı olarak bahsi geçen karara göre kişinin anne ve babasının ismi, nüfusa kayıtlı olunan cilt ve aile sıra numarası, boşanma ve evlenme tarihi, evlatlık ilişkisine ilişkin bilgiler, din bilgisi, mezun olunan okullar, hastalık ve tahlil bilgileri, günlük ve anı defterindeki bilgiler, e-posta şifresi, boyu ve kilosuna ilişkin bilgiler, kurum sicil numarası, ten ve saç rengi gibi bilgiler de 136. madde kapsamında kişisel veri sayılabilecektir. Suçun konusunun 136. maddenin ikinci fıkrasında belirtildiği üzere Ceza Muhakemesi Kanunu'nun 236. maddesinin 5 ve 6'ıncı fıkralarına göre kayda alınan beyan ve görüntülerden olması halinde ise ceza bir kat artırılacaktır. Suçun konusunu oluşturan kişisel veri kavramına çalışmamızın birinci bölümünde ayrıntılı bir şekilde yer verildiği için bu kısımda birinci bölümdeki açıklamalarımıza atıf yapmakla yetiniyoruz.

[393] YARGITAY 12. CEZA DAİRESi E. 2012/22005 K. 2013/24489 T. 4.11.2013

4.1.5. Nitelikli Haller

Kişisel verileri hukuka aykırı olarak verme, yayma veya ele geçirme suçu için Türk Ceza Kanunu'nda toplamda üç farklı nitelikli hal öngörülmüştür. Söz konusu nitelikli hallerin tamamı failin daha ağır ceza almasına neden olacak vasıftadır. 136. maddenin ikinci fıkrasında suçun konusu ile ilgili ağırlaştırıcı hal öngörülmüş iken 137. maddede yer alan iki nitelikli halde ise failin sıfatı dikkate alınmıştır. Aşağıda tüm nitelikli haller ayrı ayrı başlıklar altında incelenecektir.

4.1.5.1. Suçun konusunun CMK Uyarınca Kayda Alınan Beyan ve Görüntüler Olması

Ceza Muhakemesi Kanunumuzda 2019 yılında 7188 sayılı Kanun ile birlikte birçok değişiklik yapılmış ve bu değişikliklerden bazıları da birtakım suçların soruşturma ve kovuşturma evrelerini değişitirecek nitelikte olmuştur. Bu bağlamda Türk Ceza Kanunu'nun 102. maddesinin 2'nci fıkrasında düzenlenen cinsel saldırı suçunun vücuda organ veya sair bir cisim sokulması suretiyle gerçekleştirilmesi hali ile 103. maddede yer alan cinsel istismarın vücuda organ veya sair bir cisim sokulması suretiyle gerçekleştirilmesi haline ilişkin olarak bu suçlardan mağdur olan kişilerin beyan ve görüntülerinin kayda alınması imkanı getirilmiştir. Söz konusu değişikliği getiren 7188 sayılı Kanun'un gerekçesinde, adı geçen suçlardaki mağdurların beyan ve görüntülerinin kayda alınması suretiyle cinsel suç mağdurlarının tekrar tekrar beyanının alınmasının önüne geçilerek bu kişilerin örselenmesinin önlenmesinin amaçlandığı belirtilmiştir. Ayrıca mağdurlara soru sorulma sürecinde uzmanların eşlik etmesinin olası travmatik sonuçları azaltacağı da ifade edilmektedir. Zira bu madde hükmü ile soruşturma aşamasında cumhuriyet savcısı veya kovuşturma evresinde görevli hakim tarafından sorulacak sorular uzmanlar aracılığıyla mağdura yöneltilerek mağdurun yargılama sürecinden daha az etkilenmesi hedeflenmektedir.[394]

Ayrıca 7188 sayılı Yasa ile Çocuk İzlem Merkezleri'nin cinsel istismar suçunun nitelikli haliyle sınırlı olmak kaydıyla kovuşturma aşamasında da kullanılmasına imkan sağlanmıştır. CMK'nin 236. maddesinin 6. fıkrasında ise çocuklara yönelik olarak getirilen düzenlemeden farklı olarak mağdurun beyanlarının kayıt altına alınması, o mağdurun rızasına bağlı tutulmuştur. Zira çocuklarla ilgili durumlarda beyanın kayda alınması zorunludur. Bu noktada belirtmek gerekir

[394] TBMM, Yasama Dönemi: 27 Yasama Yılı :3 Sıra Sayısı: 105, 7188 Sayılı Kanun'un 22. Maddesinin Gerekçesi, s.15-16

ki söz konusu düzenleme ile çocuğun menfaatleri ön planda tutularak çocuk mağdurun bir kez dinlenmek suretiyle işlemin tamamlanması hedeflenmiştir.[395]

Yukarıda bahsettiğimiz hükümlere ek olarak 236. maddenin son iki fıkrasında mağdurun mahremiyetinin korunması açısından da bazı hükümler getirilmiştir. Şöyle ki değindiğimiz usule dayanılarak alınan beyan ve görüntülerin dava dosyasında muhafaza edilmekle birlikte kimseyle paylaşılmayacağı ve bu verilerin gizliliği açısından gereken önlemlerin alınacağı emredici şekilde ifade edilmiştir. Maddenin son fıkrasında ise alınan beyan ve görüntü kayıtlarının yazılı tutanağa geçirileceği ve bu tutanağın talepte bulunan şüpheli, sanık, müdafii, mağdur, vekil veya kanuni temsilciye verileceği hüküm altına alınmıştır. Son olarak ise beyan ve görüntü kayıtlarının bu kişilere soruşturma ve kovuşturma makamlarının gözetiminde gizliliği korunmak suretiyle izletilebileceği de belirtilmiştir. Böylece 5271 sayılı CMK'de yapılan değişikliklerle mağdurun mahremiyeti bir kez daha koruma altına alınmış ve kaydedilen verilerin aleni hale getirilmesi engellenmek istenmiştir.[396] Önemle belirtmek gerekir ki söz konusu kayıtlara bahse konu yargılamanın sujeleri erişebilecek ve bu bağlamda mağdur ve sanık, iddia ve savunma hakkına dayanarak kayıtları alabilecektir. Ancak belirttiğimiz kişilerin elde ettikleri kayıtları hukuka aykırı olacak şekilde başkasına vermesi veya yayması durumunda 136. maddedeki suç meydana gelecektir. Aynı şekilde saydığımız kişiler dışında hukuken kayıtlara erişim hakkı olmayan diğer kişilerin de bu verileri ele geçirmesi veya yayması durumunda yine inceleme konumuz olan suç sübuta erecektir.[397]

Ceza Muhakemesi Yasası'na getirilen söz konusu değişikle birlikte kırılgan mağdur olarak kabul edilen kişilerin artık özel ortamlarda beyanlarına başvurularak daha az yıpratıcı bir yöntem benimsenmiş olmaktadır. Bu kapsamda çocukların cinsel istismarı suçunun mağduru olan çocuğun ifadesi Çocuk İzlem Merkezi[398] (ÇİM)'nde alınacak ve burada mağdur, uzman kişi tarafından dinlenecektir. Cumhuriyet savcısı ve çocuk mağdurun avukatı ise söz konusu görüşmeyi izleyecek ve bu görüşme kayda alınacaktır.[399] Kayıt esnasında çocuğa yardımcı olacak uzmanın etkin katılımı sağlanacak ve mağdur çocuğun örselenmesine yol açmayacak şekilde ifade alma işlemi yürütülecektir. Kayıt işleminde ise kaydın konusu mağdurun

[395] Fahri Gökçen Taner, **Kırılgan Mağdurun Beyanının CMK'nın 236. Maddesi Uyarınca Alınması ve Uygulanan Özel Usuller Karşısında Savunma Hakkının Dengelenmesi**, TBB Dergisi 2021 (153), s.27-30

[396] Taner, s.32

[397] TBMM: 27 Yasama Yılı :3 Sıra Sayısı: 105, 7188 Sayılı Kanun'un 22. Maddesinin Gerekçesi, s.16

[398] Çocuk İzlem Merkezleri 4.10.2012 tarih ve 28431 sayılı Resmi Gazete'de yayımlanan 2012/20 numaralı Başbakanlık Genelgesi ile kurulmuştur.

[399] Taner, s.27-30

görüntüsü ve sesi olacaktır. Burada dikkat edilmesi gereken önemli bir diğer husus da alınan beyanın delil kalitesinin bozulmamasına özen gösterilmesidir.[400]-[401]

İşte kanun koyucu açıkladığımız usule göre alınan beyan ve görüntüleri kişisel veri olarak kabul ederek bu verilerin verilmesi, yayılması veya ele geçirilmesi durumunda verilecek cezanın bir kat artırılacağını 136. maddenin ikinci fıkrası ile hüküm altına almıştır. Böylelikle cinsel suç mağduru kişilerin durumu göz önüne alınarak söz konusu verilerin güvenliğinin sağlanması amaçlanmıştır.[402]

4.1.5.2. Suçun, Yetkisini Kötüye Kullanan Kamu Görevlisi Tarafından İşlenmesi

Türk Ceza Kanunu'nun 137. maddesinde verileri hukuka aykırı olarak verme veya ele geçirme suçu açısından iki farklı ağırlaştırıcı hal öngörülmüştür. Bu hallerden ilki suçu, kamu görevlisinin görevinin verdiği yetkiyi kötüye kullanarak işlemesidir. Böyle bir durumda faile verilecek ceza yarı oranında artırılacaktır.

Kamu görevlisi teriminin sabit bir tanımı olmamakla birlikte doktrinde çeşitli anlamlandırmalar yapılmıştır.[403] Konumuz açısından önemli olan TCK kapsamındaki kamu görevlisi deyimi olup bu kavram, Ceza Kanunumuzun 6. maddesinde tanımlandığı üzere *"Kamu görevlisi deyiminden; kamusal faaliyetin yürütülmesine atama veya seçilme yoluyla ya da herhangi bir surette sürekli, süreli veya geçici olarak katılan kişi"*yi ifade etmektedir. 137. maddedeki ilk nitelikli halin oluşması açısından failin kamu görevlisi olması aranmıştır. Ancak failin sadece kamu görevlisi sıfatını taşıması söz konusu nitelikli halin oluşması için yeterli değildir. Bunun yanında kamu görevlisi olan fail, suça konu fiili işlerken görevinden aldığı yetkiyi kötüye kullanmalıdır. Diğer bir ifadeyle somut olayda failin suçu işlemesine neden olan ve işlediği suçu ilgilendiren yetki ve görevi olmalıdır.[404] Nitekim Yargıtay da failin fiilinin kendi yürüttüğü

---

[400] Murat Aydın, **AGO Uygulaması İçin Temel Hukuk Bilgisi Kitabı**, s.50; 01.04.2021 tarih ve 176 numaralı Adalet Bakanlığı Genelgesi ile Adli Görüşme Odaları'na ilişkin özen gösterilmesi gereken hususlar belirlenmiştir. Ayrıca Genelgede Adli Görüşme Odaları (AGO) ve Çocuk İzlem Merkezlerinin (ÇİM) temel amaçlarının mağdur ve failin karşılaşmasının önüne geçilmesi suretiyle ikinci kez örselenmesinin engellenmesi ve mağdurun beyanının uzman kişi eşliğinde alınarak sağlıklı koşullarda delil elde edilmesi olduğu belirtilmiştir. Son olarak Genelge ÇİM ve AGO uygulamalarının birbirlerini tamamlayıcı nitelikte olduğunu da vurgulamıştır.

[401] Çocuk İzlem Merkezlerine ilişkin olarak çeşitli problem ve çözüm önerileri için bkz. Gülçin Orhan/ Betül Ulukol/ Hayri Canbaz, **Çocuk İzlem Merkezi Modeli Ve Bu Modelde Gözlenen Sorunlar**, Kriz Dergisi 27 (3): 178-186; Dr. Eda Ermağan Çağlar - Dr. Tuğba Türk, **İstismara Maruz Kalan Çocuklarla Adli Görüşme: NICHD Protokolü Önerisi**, TAAD, Yıl: 11, Sayı: 38 (Nisan 2019)

[402] Sevük, s.503; Sınar, s.49

[403] Yıldırım/Yasin/Kaman/Özdemir/Üstün/Okay Tekinsoy, **İdare Hukuku**, Ekim 2016 s.209 vd.

[404] Gerçeker, s.1362. Böylece görevi kötüye kullanmanın özel bir şekli düzenlenmiş olmaktadır.; Gültaş, s.214; Örneğin Adli Tıp Kurumunda görev yapan bir memurun Kurumun sistemindeki verileri ifşa etmesi kamu görevlisinin görevinden kaynaklı yetkiyi kötüye kullanması anlamına gelecektir. Bkz. Sert, s.143

görevi ile ilgili olmaması durumunda nitelikli halin uygulanamayacağına karar vermektedir.[405] Örnek vermek gerekirse CMK m.135 uyarınca bir kişi hakkında iletişimin denetlenmesi kararı verilmesine müteakip mahkeme kararını yerine getiren görevli memurun ses kayıtlarını yayması sonucunda söz konusu nitelikli hal oluşacaktır. Nitekim kayıt işlemini yapan kamu görevlisi bu alanda yetkilidir ve görevinden kaynaklı bir yetkiyi kötüye kullanmıştır. Aynı şekilde iletişimin denetlenmesinde görevi olmayan kamu görevlisinin ses kayıtlarını ifşa etmesi durumunda – kamu görevlisi sıfatını taşısa dahi- görevinden kaynaklı yetki somut olayda mevcut olmadığı için nitelikli halden söz edilemeyecektir.[406] Son olarak belirtmek gerekir ki kamu görevlisinin yürüttüğü kamu görevi nedeniyle söz konusu suça konu fiileri işlemesi halinde fail hakkında 4483 sayılı Yasa uyarınca yetkili merciden soruşturma izni alınması gerekmektedir.[407]

Bahse konu nitelikli hal açısından değinmemiz gereken son husus ise görevi kötüye kullanma suçunun bu tür durumlarda meydana gelip gelmeyeceğidir. Şöyle ki 137. maddedeki nitelikli halin mevcut olduğu somut olayda 257. maddede düzenlenen ve genel norm niteliğindeki görevi kötüye kullanma suçundan hüküm kurulmayacaktır. Zira 137. madde daha özel bir düzenlemedir ve öncelikle başvurulması gerekmektedir.[408]

4.1.5.3. Suçun Bir Meslek ve Sanatın Sağladığı Kolaylıktan Yararlanılarak İşlenmesi

İnceleme konumuz olan suç tipi açısından TCK m.137'de öngörülen ikinci nitelikli hal, failin mesleğinin ve sanatının sağladığı kolaylıktan faydalanarak bu suçu işlemesidir. Kanun koyucu söz konusu nitelikli hal açısından da önceki bentteki nitelikli halde olduğu gibi verilecek cezanın yarı oranında artırılmasını vaz etmiştir.

Failin bahsi geçen durumdan dolayı daha ağır ceza ile cezalandırılabilmesi için bir meslek ve sanatla ilişkisinin olması, uğraştığı bu meslek ve sanatın kişisel verileri verme, yayma veya ele

---

[405] YARGITAY 12. CEZA DAİRESİ E. 2018/2226 K. 2018/8746 T. 26.9.2018; YARGITAY 12. CEZA DAİRESİ E. 2018/636 K. 2018/6140 T. 30.5.2018; Sanığın işlediği fiilin görevi kapsamında olup olmadığının araştırılmamasının bozma nedeni olarak kabul edildiği kararlar için bkz. YARGITAY 12. CEZA DAİRESİ E. 2013/9734 K. 2014/2288 T. 3.2.2014; YARGITAY 12. CEZA DAİRESİ E. 2013/8389 K. 2014/62 T. 13.1.2014

[406] Karagülmez, s.409; YARGITAY 12. CEZA DAİRESİ E. 2018/636 K. 2018/6140 T. 30.5.2018 Bu kararında Yargıtay, sanığın kendisini trafikte sıkıştırdığını iddia ettiği mağdurun plakasını polis memuru olan tanığı arayarak sorgulatıp mağdurun kimlik bilgilerine ulaşması eyleminde sanığa bilgileri veren polis memurunun eyleminin görevinin sağladığı yetkiyi kötüye kullanması kapsamında olmadığı kanaatine varmıştır.

[407] Artuç, *Pratik Türk Ceza Kanunu*, s.767

[408] İZMİR BÖLGE ADLİYE MAHKEMESİ 10. CEZA DAİRESİ E. 2017/1122 K. 2017/1114 T. 5.7.2017 *"Verileri hukuka aykırı olarak verme veya ele geçirme" suçunun, eylemlerin kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle işlenmekle TCK'nın 137/1-a maddesinde düzenlenen nitelikli halini oluşturduğu, özel suç tanımı bulunması halinde genel nitelikteki TCK'nın 257. maddesinin uygulanma olanağının bulunmadığı da göz önüne alındığında"*

geçirme fiilleri açısından kendisine bir kolaylık sağlaması ve son olarak failin bu kolaylıktan yararlanarak suça konu fiilleri işlemesi gerekmektedir.[409]

İncelemekte olduğumuz nitelikli hal açısından dikkate değer diğer bir husus ise madde metninin düzenleniş biçimidir. Zira madde metnine bakıldığında meslek ve sanatın sağladığı kolaylıktan bir arada bahsedildiği görülmekte ve bu kapsamda nitelikli halin oluşması için -ve bağlacı kanalıyla- failin hem mesleğinin hem de sanatının sağladığı kolaylıktan yararlanması gerektiği şeklinde bir anlam ortaya çıkmaktadır. Ancak belirtilmelidir ki iki durumun bir arada bulunması çok zor olduğundan maddede yer alan "ve" bağlacını "veya" olarak yorumlamak maddenin düzenleniş amacına daha uygun düşecektir. Dikkatten kaçırılmaması gereken diğer bir nokta da icra edilen sanat veya mesleğin suçu işlemeye imkan vermesi ve işlenen suç ile bu meslek veya sanat arasında bir illiyet bağı kurulması gerekliliğidir.[410]

Sanat ve meslek kavramlarının somutlaşması açısından bu kelimelerin ıstılahi anlamlarına ve bazı olay örneklerine değinmenin faydalı olacağını düşünüyoruz. Öncelikle meslek, TDK'de 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 tanımlanmaktayken sanat kavramı bir şey yapmada gösterilen ustalık olarak ifade edilmiştir. Bu bağlamda örneğin bir banka çalışanının müşterilerin bilgilerine ulaşması[411], serbest çalışan doktorun hastalarına ilişkin bilgilere erişmesi[412], şirket çalışanının çalıştığı şirketin müşterilerinin kişisel verilerini başkasına satması[413], yemek teslimatı yapan kuryenin işinden dolayı numarasını öğrendiği kişilerin telefon numaralarını kullanması[414] 137. maddenin b bendindeki ağırlaştırıcı hale vücut verecektir. Son tahlilde 137. maddede yer alan iki nitelikli halin karşı karşıya gelmesi durumuna da değinmek gerekmektedir. Yargıtay bu sorunla ilgili olarak kamu görevlisinin görevi dışında bir meslek veya sanata sahip olamayacağı ve bu nedenle kamu görevlileri hakkındaTCK m.137/1-b uyarınca cezalandırma yapılamayacağı kanaatindedir.[415]

---

[409] Gerçeker, s.1362

[410] İbrahim Korkmaz, **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, Doktora Tezi, Ankara 2017, s.441-442

[411] Sedat Erdem Aydın, **AİHM İçtihatları Bağlamında Kişisel Verilerin Kaydedilmesi Suçu**, 12 Levha Yayıncılık, Aralık 2015, s.160

[412] Yaşar/ Gökcan,/Artuç, s.4122

[413] YARGITAY 12. CEZA DAİRESİ E. 2017/1636 K. 2018/3978 T. 4.4.2018

[414] Sınar, s.52

[415] YARGITAY 12. CEZA DAİRESİ E. 2018/2226 K. 2018/8746 T. 26.9.2018; YARGITAY 12. CEZA DAİRESİ E. 2013/8447 K. 2014/2291 T. 3.2.2014

4.2. Manevi Unsur

Kişisel verileri hukuka aykırı olarak verme, yayma veya ele geçirme suçunun manevi unsuru kasttır.[416] Bu bağlamda fail suça konu fiilleri işlerken başkasına ait bir veriyi verdiğini, yaydığını veya ele geçirdiğini bilmeli ve istemelidir.[417] 136. maddede açıkça öngörülmemiş olduğundan bu suç taksirle işlenemeyecektir.[418] Ayrıca yine maddede yer almadığı içindir ki bu suçun oluşmasında özel kast aranmamakta ve genel kast yeterli görülmektedir.[419] Suçun işlenmesinde failin herhangi bir saik taşımasının önemi bulunmamaktadır.[420]

Manevi unsur açısından önemle vurgulanması gereken diğer bir husus ise hukuka aykırılığa 135. maddedeki kişisel verilerin kaydedilmesi suçunda olduğu gibi kanun koyucu tarafından özellikle suç tipinde yer verilmiş olmasıdır. Bu gibi durumlarda hukuka özel aykırılık kavramı karşımıza çıkmaktadır. Hukuka özel aykırılık durumunda, kanun koyucu *"hukuka aykırı olarak"*[421], *"hukuka aykırı başka bir davranışla"*[422], *"hukuka aykırı yollarla"*[423] şeklindeki ifadelerle hukuka aykırılığa özellikle dikkat çekmektedir. Şüphesiz ki hukuka aykırılığın bu şekilde ayrıca vurgulanmasının mutlaka bir nedeni vardır.[424]

Hukuka aykırılığın ayrıca vurgulandığı hallerde hukuka aykırılık, tipikliğe ait bir unsur halini alır.[425] Bu doğrultuda failin işlediği fiilin hukuka aykırı olduğunu bilmesi ve bunun bilincinde olması aranmaktadır. Böylece söz konusu fiilin işlenebilmesi açısından doğrudan kastın varlığı gereklidir[426] ve failin kastı hukuka aykırılığı da kapsamına almalıdır. Aksi halde suçun işlenmediği sonucuna varılacaktır.[427] Ayrıca failin cezalandırılabilmesi için işlediği fiilin hukuka aykırı olduğunu bilmesi ispatlanmış olmalıdır. Yargılama sırasında ise hakim, hukuka

---

[416] Soyaslan, s.366

[417] Hafızoğulları/ Özen, *Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar*, s.21

[418] Volkan Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku**, Seçkin Yayınevi, Ankara, 2014, 4. Bası, s.621; Rezzan İtişgen, **Türk Ceza Hukukunda Kişisel Verileri Hukuka Aykırı Olarak Verme Veya Ele Geçirme Suçu**, TAAD, Yıl:6, Sayı:23 (Ekim 2015), s.190

[419] Şahbaz, s.1599

[420] Ali Parlar, **Türk Ceza Kanunu Şerhi**, Cilt 2, Bilge Yayınevi, Ankara 2015, s.1555; YARGITAY 12. CEZA DAİRESİ E. 2018/8369 K. 2019/8318 T. 10.7.2019

[421] Bkz. TCK'nin 109. maddesindeki kişiyi hürriyetinden yoksun kılma suçu

[422] Bkz. TCK'nin 117. maddesindeki iş ve çalışma hürriyetinin ihlali suçu

[423] Bkz. TCK'nin 91. maddesinin 5. fıkrası

[424] Demirbaş, s.252

[425] Artuk/Gökcen/Yenidünya, *Ceza Hukuku Genel Hükümler*, s.302

[426] İtişgen, s.191; Koca/ Üzülmez, *Kişisel Verilerin Kaydedilmesi Suçu*, s.73

[427] Ersan Şen, **Türk Ceza Hukuku Suçun Genel Esasları ve Unsurları**, Der Yayınları İstanbul 2002, s.390

aykırılığın varlığını ayrıca tespit etmelidir. Çünkü failin kastının suç tipindeki özel hukuka aykırılığı da içermesi aranmaktadır.[428]

İnceleme konumuz olan 136. maddedeki verileri hukuka aykırı olarak verme veya ele geçirme suçunda yasa koyucu hem madde başlığında hem de madde metninde hukuka aykırılığı ayrıca belirtmiştir. Bunun sonucunda ise kişinin cezalandırılmasında doğrudan kast aranacaktır. Şöyle ki cezalandırma açısından kişinin kişisel verileri başkasına verirken, yayarken veya ele geçirirken işlediği fiilin hukuka aykırı olduğunun bilincinde olması gerekecektir. Yargıtay'ın 136. maddede düzenlenen suçun manevi unsuruyla ilgili yeknesak bir uygulaması bulunmamakla birlikte hukuka aykırılıkla ilgili olarak aynı yönde kararlar verdiği görülmektedir. Örneğin kendisine karşı işlenen bir fiili delillendirme amacı güden veyahut açılmış olan bir davada delil olarak sunmak saikiyle hareket eden kişilerin fiillerinde hukuka aykırılık bilinci bulunmadığı yönünde hüküm kurulmaktadır. Yüksek Mahkeme bir kararında *"Ancak, kişinin, bir daha kanıt elde etme olanağının bulunmadığı ve yetkili makamlara başvurma imkanının olmadığı ani gelişen durumlarda, örneğin; kendisine karşı işlenmekte olan (cinsel saldırı, hakaret, tehdit, iftira veya şantaj gibi) bir suç söz konusu olduğunda ya da kendisine veya aile birliğine yönelen, onurunu zedeleyen, haksız bir saldırıyı önlemek için, kaybolma olasılığı bulunan kanıtların kaybolmasını engelleyip, yetkili makamlara sunarak güvence altına almak amacıyla, saldırıyı gerçekleştiren tarafın bilgisi ve rızası dışında, özel hayata ait bilgileri okuma, konuşma ve haberleşme içeriklerini veya özel hayata ilişkin ses ve görüntüleri dinleme, izleme ya da kaydetme, kişisel verileri kaydetme, ele geçirme ve yayma eylemlerinin hukuka aykırı olduğunu kabul etmek mümkün olmadığı gibi, esasen bu hallerde kişinin hukuka aykırı hareket ettiği bilinciyle davrandığından da söz edilemez."* şeklinde kanaat belirtmekle birlikte bu gibi durumlarda hukuka aykırılık bilincinin oluşmadığını kabul etmektedir.[429] Ayrıca Yüksek Mahkeme, aile birliğini korumaya yönelik davranışlarda da hukuka aykırılık bilincinin olmadığına hükmetmektedir.[430]

Son olarak belirtelim ki suçun neticesi sebebiyle ağırlaşmış haline kanunda yer verilmemiştir.

---

[428] YARGITAY 15. CEZA DAİRESİ E. 2015/1659 K. 2018/2748 T. 18.4.2018 *"...sanığın eylemiyle hukuka aykırı hareket ettiğini bildiği ya da bilebilecek durumda olduğunun da ayrıca tespit edilmesi gerekir."*

[429] YARGITAY 12. CEZA DAİRESİ E. 2019/2121 K. 2019/5170 T. 17.4.2019; Aynı yönde bkz. YARGITAY 12. CEZA DAİRESİ E. 2019/4369 K. 2019/8633 T. 11.9.2019; YARGITAY 12. CEZA DAİRESİ E. 2018/8358 K. 2019/9754 T. 2.10.2019

[430] YARGITAY 12. CEZA DAİRESİ E. 2015/10438 K. 2016/12933 T. 23.11.2016

4.3. Hukuka Aykırılık Unsuru

Suçun genel unsurlarından olan hukuka aykırılık, hukuk düzeninin tümünün somut olayda işlenen fiil hakkındaki değersizlik yargısı olarak ifade edilmektedir. Bu bağlamda söz konusu fiil, hukuk düzeninin tümü tarafından bir değerlendirmeye tabi tutulacak ve bu değerlendirmede hukuka uygunluk nedenine de rastlanmazsa fiilin suç teşkil edeceği söylenecektir.[431] Ancak unutmamak gerekir ki sözünü ettiğimiz değerlendirme işlemi sadece TCK ile sınırlanmamalıdır. Zira bir fiil ya hukuka uygundur ya da değildir.[432] Aksi halde ceza mevzuatı dışında yer alan hukuka uygunluk sebepleri sırf ceza hukuku alanı dışındaki disiplinlerde yer aldığı için dikkate alınmayacak ve böylece hukuk düzeninin birliği parçalanmış olacaktır ki bu sonuç kabul edilemez. Nitekim "*Hukuka aykırılık parçalanması mümkün bir mefhum değildir. Bir fiilin muayyen bir hukuk dalına nispetle hukuka uygun; başka bir hukuk sahasında ise hukuka aykırı olması bizatihi hukuk mefhumuna karşı gelen bir çelişme teşkil eder."*[433] İşte biz de çalışmamızın devamında kişisel verileri hukuka aykırı olarak verme, yayma veya ele geçirme suçu açısından hukuka aykırılık unsurunu ele alacak ve hukuk düzenimizde bu suç için öngörülmüş bulunan hukuka uygunluk sebeplerine değineceğiz.

Hukuka aykırılığın failin hareketi ile hukuk normu arasındaki tezatlık ilişkisi olduğunu yukarıda belirtmiştik. Aynı zamanda değinmek gerekir ki Ceza Kanunumuz, suçun unsurları arasında kabul edilen hukuka aykırılıktan geneli kapsayacak bir şekilde bahsetmemektedir. Aksine TCK'de, bazı suç tipleri düzenlenirken hukuka aykırılığı özellikle vurgulayan birtakım ifadeler kullanılmıştır. Bu suçlara örnek olarak *"yetkisiz olarak"* ibaresinin kullanıldığı 306. maddede yer alan yabancı devlet aleyhine asker toplama, *"hukuka aykırı olarak"* ifadesi ile hukuka aykırılığın ayrıca belirtildiği 109. maddedeki kişiyi hürriyetinden yoksun kılma, 120. maddedeki haksız arama, m.134/2'deki özel hayatın gizliliğini ihlal, 135. maddedeki kişisel verilerin kaydedilmesi ve çalışmamızın konusu olup 136. maddede düzenlenen verileri hukuka aykırı olarak verme veya ele geçirme suçu gösterilebilecektir. İşte kanun koyucunun hukuka aykırılığa suç tipinde değinilen şekillerde özellikle yer vermesi halinde hukuka özel aykırılıktan bahsedilecektir. Böylesi hallerde ilgili suçun madde metninde bu türden bir düzenlemenin tesadüfi olmadığı ve dahi belirli bir sebebin gözetilerek hukuka aykırılığın madde metnine

---

[431] Koca/ Üzülmez, *Türk Ceza Hukuku Genel Hükümler*, s.263; Nitekim yapılan araştırma sonucu herhangi bir hukuka auygunluk nedeni bulunursa somut vakıadaki fiil artık bir haksızlık oluşturmayacaktır. Bkz. Özgenç, s.279; Hukuka aykırılık, suça konu fiilin hukuk düzeni ile arasında meydana gelen zıtlığı/çelişkiyi ifade etmektedir. Bkz. Sulhi Dönmezer/Sahir Erman, **Nazari ve Tatbiki Ceza Hukuku Umumi Kısım**, Cilt 2, İstanbul 1969, s.12

[432] Hakeri, s.139; Özgenç, s.278; Aynı şekilde hukuka aykırılığı ortadan kaldıran sebebin Ceza Hukuku alanında mevcut olamaması da önemli değildir. Bkz. Sulhi Dönmezer/Sahir Erman, **Nazari ve Tatbiki Ceza Hukuku Umumi Kısım**, Cilt 2, İstanbul 1969, s.12

[433] Dönmezer/ Erman, *Nazari ve Tatbiki Ceza Hukuku Umumi Kısım*, s.11

dercedildiği kabul edilmektedir. Aslında hukuka aykırılık unsurunun tekrardan bu şekilde vurgulanması ile suçu işleyen failin *"hukuka aykırı olarak"*, "*görevlerinin gereklerine aykırı olarak", "yetkisiz olarak"* veya *"haksız olarak"* hareket etmeyi bilmesi ve istemesi aranmış olmaktadır. Yani failin doğrudan kastla hareket etmiş olması gerekmektedir. Zira bu gibi durumlarda suç ancak doğrudan kastla işlenecektir. Aynı şekilde yargılamayı yürüten hakim de failin suça konu fiili işlerken hukuka özel aykılığı bilip bilmediğini ve isteyip istemediğini araştıracaktır.[434]

Çalışmamıza konu 136. maddedeki verileri hukuka aykırı olarak verme veya ele geçirme suçunun düzenleniş şekline bakıldığında kanun koyucunun söz konusu suç tipinde hukuka aykırılığı ayrıca belirterek hukuka özel aykırılığı suçun oluşması açısından aradığı görülecektir. Bu bağlamda fail, suçu işlerken suça konu verileri hukuka aykırı olarak verdiğini, yaydığını veya ele geçirdiğini bilmeli ve istemelidir.[435] Aynı şekilde somut olayda herhangi bir hukuk dalında kabul edilmiş olan bir hukuka uygunluk sebebi olup olmadığı ve failin suça konu fiili işlerken hukuka aykırı olarak bu hareketi gerçekleştirdiğini bilip bilmediği tespit edilmelidir.[436] Zira artık hukuka özel aykırılık söz konusu olduğundan diğer suçlardan farklı olarak failin kastının hukuka aykırılığı da kapsaması gerekmekte ve yargılama aşamasında bu hususun ispatı aranmaktadır.[437]

4.3.1. Hukuka Uygunluk Nedenleri

Çalışmamızın bu kısmında öncelikle Türk Ceza Kanunu'nda sayılan hukuka uygunluk sebeplerine değinilecek olup ardından 6698 sayılı Kişisel Verilerin Korunması Kanunu'nda yer alan ve kişisel verilerin işlenmesini hukuka uygun hale getiren şartlara değinilecektir. Bu noktada ilk bölümde de vurguladığımız bir hususa değinmekte fayda görüyoruz. Şöyle ki kişisel verilerin işlenmesi kavramı, eserimizin konusunu oluşturan kişisel verilerin hukuka aykırı olarak verilmesi, yayılması veya ele geçirilmesi suçundaki seçimlik hareketlerin hepsini kapsamaktadır. Böylece kişisel verilerin işlenmesi bakımından öngörülen ve veri işleme faaliyetini hukuka uygun hale getiren KVKK'deki durumlar da TCK m.136'daki suç bakımından failin hareketini hukuka uygun hale getirecektir.

---

[434] Sulhi Dönmezer/ Sahir Erman, **Nazari ve Tatbiki Ceza Hukuku**, Cilt 2, 14. Bası, Der Yayınları, İstanbul 2019, s.251-252; Demirbaş, s.269; Özgenç, s.320; Özbek/ Doğan/ Bacaksız/ Tepe, *Türk Ceza Hukuku Genel Hükümler,* s. 278

[435] Soyaslan, s.366

[436] Sevük, s.498-499

[437] İçel, s.321

4.3.1.1. Mağdurun Rızası

İlgili kişinin rızası Türk Ceza Kanunu'nda hukuka uygunluk sebepleri arasında sayılmıştır. Bu husus, TCK m.26/2'de *"Kişinin üzerinde mutlak surette tasarruf edebileceği bir hakkına ilişkin olmak üzere, açıkladığı rızası çerçevesinde işlenen fiilden dolayı kimseye ceza verilmez."* şeklinde belirtilmiştir. Ceza Kanunumuzun yanı sıra ilgili kişinin rızası, bir hukuka uygunluk sebebi olarak 6698 sayılı Kişisel Verilerin Korunması Kanunu'nda "açık rıza" şeklinde düzenlenmiştir.[438] Açık rıza, KVKK m.3'te *"Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza"* olarak tanımlanmıştır. Bununla birlikte KVKK'de düzenlenen söz konusu rıza kavramı açısından bulunması gereken bazı özellikler aranmaktadır. Öncelikle rıza, belirli bir konuya ilişkin olmalı, ilgili kişi rızasını beyan etmeden önce konuyla ilgili bilgilendirilmiş olmalı ve son olarak söz konusu irade beyanı özgürce ve bir baskı/zorlamaya dayanmadan açıklanmalıdır. Bahse konu rıza hem genel nitelikteki kişisel veriler için hem de özel nitelikli kişisel veriler için bir hukuka uygunluk nedeni olarak kabul edilecektir.[439] Neticeten kişisel verileri verilmeden, yayılmadan veyahut ele geçirilmeden önce ilgili kişinin açık rıza göstermesi durumunda söz konusu fiiller artık hukuka uygun sayılacak ve 136. maddedeki suç oluşmayacaktır. Çalışmamızın birinci bölümünde açık rıza kavramı ayrıntısıyla açıklandığından bu kısımda sadece Açık Rıza başlığına atıfla yetiniyoruz.[440]

4.3.1.2. Kanun Hükmünün İcrası

Verilerin hukuka aykırı olarak verilmesi veya ele geçirilmesi suçu açısından uygulanacak olan ikinci hukuka uygunluk sebebi kanun hükmünün uygulandığı hallerdir. Kanun hükmünün icrası Türk Ceza Kanunu'nun 24. maddesinde *"Kanunun hükmünü yerine getiren kimseye ceza verilmez."* şeklinde açıklanmıştır. Bunun yanında kanun hükmünün uygulanması hali KVKK'de kişisel verilerin işlenmesi şartlarının sayıldığı 5. maddede de düzenlenmiştir. Buna göre kişisel veriler, kanunlarda açıkça öngörülmesi kaydıyla ilgili kişinin açık rızasına ihtiyaç duyulmaksızın işlenebilecektir. Tekrardan belirtmek gerekirse KVKK'deki işleme kavramına 136. maddede sayılan verme, yayma ve ele geçirme fiillerinin hepsi dahildir ve bu sebepledir ki Kişisel Verilerin Korunması Yasası'nda sayılan ve kişisel verilerin işlenmesinde hukuka uygunluk sebebi olarak kabul edilen haller meydana geldiğinde suç oluşmayacaktır.[441]

---

[438] Korkmaz, *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması* (2019), s.463

[439] Kişisel Verileri Koruma Kurumu, **Açık Rıza**, s.1-6

[440] Bkz. 6.6.1.1. Açık Rıza

[441] Korkmaz, *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması* (2019), s.467

Teknolojinin hızlı gelişimi sonucu kanun koyucu kişisel verilerin işlenmesine imkan tanıyan birçok yasal düzenleme yapmış ve bunun soncunda kanun hükmünün uygulanması şeklinde ortaya çıkan hukuka uygunluk nedeninin kapsamı bir hayli genişlemiştir. Biz bu kısımda çalışmamızın kapsamını fazla genişletmemek adına uygulama açısından en çok karşımıza çıkan kanun hükümlerini incelemeye çalışacağız.

Mevzuatımız açısından kişisel verilerin işlenmesine olanak sağlayan kanunlardan ilki ve en önemlisi 5271 sayılı Ceza Muhakemesi Kanunumuzdur. 5271 sayılı Ceza Muhakemesi Yasası'nın 75. maddesi ve devamında şüpheli, sanık ve diğer kişilerin beden muayenesi ve vücutlarından örnek alınması hükümleri düzenlenmiştir. Söz konusu hükümlere göre gerekli diğer şartların da yerine getirilmesi ile kişilerden kan veya benzeri biyolojik örnekleri ile saç, tükürük ve tırnak gibi örnekler alınabilecektir. Aynı doğrultuda 80. maddede 75, 76 ve 78'inci maddeler kapsamında alınan örnekler üzerinde yapılan inceleme sonuçlarının kişisel veri niteliği taşıdığı belirtilmiştir. Maddenin devamında ise bu örneklerin başkasına verilemeyeceği vurgulanmıştır. İşte söz konusu CMK hükümlerine uygun olarak kişisel verilerin işlenmesi durumunda hukuka uygunluk sebebi oluşacak ve 136. maddedeki suç meydana gelmeyecektir. Aksine bu hükümlere aykırı olarak önceden alınan örneklere ilişkin sonuçlar başkasına verilir, yayılır veyahut ele geçirilirse artık cezai sorumluluktan bahsedilebilecektir.[442]

İkinci olarak değinmemiz gereken kanun ise 5352 sayılı Adli Sicil Kanunu'dur. Adli Sicil Kanunu'nun 4. maddesinde adli sicile kaydedilecek bilgiler sayılmakla birlikte 7 ve 8. maddelerde adli sicil bilgilerinin verilebileceği kişiler sayılmıştır. Bu kapsamda *"Adlî sicil bilgileri, kullanılış amacı belirtilmek suretiyle ilgili kişiye veya vekâletnamede açıkça belirtilmek koşuluyla vekiline, kamu kurum ve kuruluşlarına ve kamu kurumu niteliğindeki meslek kuruluşlarına verilebilecektir."* Önemle belirtmek gerekir ki adli sicilde özel nitelikli veriler de yer almaktadır ve bu nedenle söz konusu verilerin verilmesi aşamasında son derece hassas davranılmalıdır. Zira bu aşamada yapılacak bir hata sonucu kişilerin hassas bilgileri yetkisiz kişilerin eline geçebilecektir. Ancak bahsettiğimiz kanun hükümlerine uygun olarak kişilere ait verilerin işleme tabi tutulduğu hallerde ise yasa kuralları uygulanmış olacağından artık 136. maddedeki suç oluşmayacaktır.[443]

Son yıllarda hızla gelişen alanlardan biri olan havacılık sektöründe gün geçtikçe artan yolcu sayısı bu alanda kişisel verilerin dolaşımını artırmıştır. Örneğin havayolu şirketleri kendi aralarında imzaladıkları sözleşmelerle yolcuların bilgilerinin karşılıklı paylaşımını sağlamakta

[442] Ali Parlar, **Açıklamalı-Atıflı-Uygulamalı Türk Ceza kanunu El Kitabı**, Bilge Yayınevi, Ankara 2018, s.652
[443] Sert, s.146

ve bu yolla birçok veri alınıp verilmektedir. Bunun sonucunda ise birçok ülkede yüz tanıma başta olmak üzere çok fazla çeşit ve sayıda kişisel veri işleyen taşımacılık işlemleri gerçekleştirilmekte ve aynı doğrultuda regülasyonlar hazırlanmaktadır. Aynı şekilde ülkemizde de 2920 sayılı Sivil Havacılık Kanunu'nda 2017 yılında 7061 sayılı Kanun ile yapılan değişiklikle seyahat edecek kişilerin bilgilerinin paylaşımına imkan sağlanmıştır. Nitekim Kanun'un 40. maddesinin beşinci fıkrasına göre *"Havayolu ile seyahat edecek kişilerin bilgileri kişilerin seyahatini kolaylaştırmak veya güvenlik ve risk değerlendirmesi yapmak amacıyla 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu çerçevesinde toplanabilir, kaydedilebilir, işlenebilir, paylaşılabilir, havacılık güvenliği ve emniyetini sağlamak üzere değerlendirilerek gereken tedbirler alınabilir."* Ayrıca yine aynı maddede talep olması durumunda yolcuların bilgilerinin kurumlarca ya da havayolu şirketlerince diğer ülkelerle İçişleri Bakanlığının uygunluk görüşü şartıyla paylaşılabileceği belirtilmiştir. Bu kapsamda bahsi geçen kanun hükmüne uygun olarak yapılacak kişisel veri paylaşımları 136. madde kapsamında değerlendirilemeyecektir. Zira artık kişisel veriler kanun hükmünün icrası kapsamında verilmektedir.

Son olarak değineceğimiz kanun 5490 sayılı Nüfus Hizmetleri Kanunu'dur. Nüfus Hizmetleri Kanunu, vatandaşlara ilişkin hassas veriler de dahil olmak üzere birçok bilginin işlenmesinin hukuki dayanağını oluşturmaktadır. Zira bu kanuna göre kişilerin kimlik numarası, dini, cinsiyeti gibi bilgileri başta olmak üzere fazla sayıda kişisel veri yetkili makamlarca işlenebilmektedir. Aynı şekilde kanunda bazı kişisel veri içeren kayıtların hangi makamlara verilebileceği de düzenlenmiştir. Bu bağlamda 44. maddede kişilerin nüfus kayıt örneğini almaya yetkili olan kişiler sayılmıştır. İşte kanun hükmüne uygun olarak söz konusu kayıtların yetkili makamlarca nüfus müdürlüklerinden alınması neticesinde inceleme konumuz olan verilerin hukuka aykırı olarak verilmesi, yayılması veya ele geçirilmesi suçu oluşmayacaktır.

4.3.1.3. Hayat veya Beden Bütünlüğünün Korunması İçin Zorunluluk

Kişisel Verilerin Korunması Kanunu'nda yer alan ve ilgili kişinin rızası alınmadan kişisel verilerinin işlenmesini sağlayan diğer bir hal *"Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması"* durumudur. Bu noktada gözden kaçırılmaması gereken husus ise özel nitelikli veriler açısından söz konusu hukuka uygunluk nedeninin uygulanmayacağıdır. Zira KVKK'nin 6.

maddesinde özel nitelikli veriler açısından işlenme şartları düzenlenmiş ve bu haller arasında zorunluluk durumuna yer verilmemiştir.[444]

Bahse konu hukuka uygunluk sebebinin oluşması ve böylece failin fiilinin hukuka aykırı olmaktan çıkması için iki şart bir arada bulunmalıdır. Bunlardan ilki kişinin veya başkasının hayatı veya beden bütünlüğünün koruma altına alınması için kişisel verilerin işlenmesinde somut olayda bir zaruret olmalı ve kişi, fiili imkansızlıktan ötürü rızasını açıklayamamalı veya onun rızasına hukuki geçerlilik tanınmamış olmalıdır. Söz konusu iki şart değerlendirilirken mutlak surette dikkat edilmesi gereken nokta kişisel verilerin işlenmesinde bir zorunluluk halinin meydana gelmiş olmasıdır.[445]

4.3.1.4. Bir Sözleşmenin Kurulması veya İfasında Gereklilik

6698 sayılı KVKK'de sayılan ve kişisel verilerin hukuka uygun bir şekilde işlenebileceği hallerden bir diğeri bir sözleşmenin kurulmasında veya ifası sırasında sözleşme taraflarına ilişkin verilerin işlenmesinde gereklilik olması durumudur. Örneğin taraflarca imzalanan sözleşme devlet kurumlarını ilgilendiriyor ve sözleşme hükümleri uyarınca taraflar birbirlerine ait kişisel verileri bu makamlara veriyor ise sözleşmenin ifası açısından bir gereklilik olduğu kabul edilecektir. Aynı şekilde bir turizm şirketinin düzenlediği gezilerdeki müşterilerine ait kişisel verileri o kişilerin kalacağı otellerle paylaşması durumunda yine sözleşmenin ifası sebebi karşımıza çıkacaktır. Tüm bu durumlarda ise hukuka uygunluk nedeninin meydana gelmiş olması suçun oluşmasını önleyecektir.[446] Sözleşmenin ifası ve kurulması açısından verilebilecek diğer örnekler ise internet üzerinden yapılan alışverişte müşterinin adres bilgisinin işlenmesi, şirket içinde verilecek eğitim için çalışanların kişisel bilgilerinin işlenmesi ve tedarikçilerle ilgili verilerin tutulması şeklinde artırılabilecektir.[447]

4.3.1.5. Hakkın Tesisi, Kullanılması ve Korunması İçin Zorunluluk

Verileri hukuka aykırı olarak verme veya ele geçirme suçu açısından geçerli olan bir diğer hukuka uygunluk nedeni bir hakkın tesisinde, kullanılmasında veyahut korunmasında veri işlemenin zaruret arz etmesi halidir. Örneğin şirket çalışanının açtığı davada ispat faaliyeti açısından bazı verilere başvurması veya kısıtlanan kişinin haklarının muhafazası açısından

[444] Korkmaz, *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması* (2019), s.470
[445] Küzeci, *Kişisel Verilerin Korunması*, s.343
[446] Korkmaz, *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması* (2019), s.470
[447] Küzeci, *Kişisel Verilerin Korunması*, s.344

kanuni temsilcinin kısıtlıya ait verileri tutması yahut basının kişilerin haber alma hakkı kapsamında verileri işlemesi gibi hallerde hukuka uyguluktan bahsedilecektir.[448]

Kişisel Verilerin Korunması Kanunu'nda tesis edilecek, kullanılacak veya korunacak olan hak için herhangi bir sınırlama getirilmemiştir. Aynı şekilde somut olayda verilerin işlenmesini hukuka uygun hale getirecek hakkın veri sorumlusuna ait olması da şart değildir. Nitekim veri sorumlusu haricinde üçüncü kişilerin de hakları açısından bir zaruret durumu hasıl olduğunda yine hukuka uygun bir işleme faaliyeti ortaya çıkacaktır.[449]

4.3.1.6.Veri Sorumlusunun Hukuki Yükümlülüğünü Yerine Getirmesi

Kişisel Verilerin Korunması Yasası'nda öngörülen hukuka uygunluk sebeplerinden biri de veri işleme faaliyetinin veri sorumlusunun hukuki yükümlülüklerini yerine getirebilmesi açısından zorunluluk arz etmesidir. Bu hukuka uygunluk sebebi sadece hassas veri niteliğinde olmayan veriler için öngörülmüştür.[450] Bu kapsamda örneğin bir şirketin kendi çalışanına yapacağı maaş ödemesi için banka hesap numarası, sosyal sigorta numarası gibi bilgileri işlemesi, rıza alınmaksızın gerçekleştirilebilen bir işleme faaliyeti olacaktır.[451]

Veri sorumlusu, hukuken kendisi için öngörülmüş yükümlülüğü gerçekleştirmek açısından zaruret bulunan durumlarda verisi işlenen kişinin rızasına dayanmaksızın bu bilgileri işleyebilecektir. Yukarıda bahsetmiş olduğumuz sözleşmenin ifası ve kanun hükmünün icrası başlıklı hukuka uygunluk nedenlerine benzemekle birlikte bu iki nedenin dışında kalan hukuki yükümlülükler için söz konusu hal öngörülmüştür. Bu bağlamda kanun dışındaki düzenlemeler, mahkeme kararları ve usulüne uygun verilmiş olan emir ve talimatlar doğrultusunda ilgili kişinin verileri işlenebilecektir. Örnek vermek gerekirse Cumhurbaşkanlığı kararnameleri, yönetmelikler gibi düzenleyici işlemlerin uygulanması ya da yargılamayı yürüten mahkemenin bilgi talep etmesi durumunda, BDDK, MASAK, SPK, SGK, EPDK gibi kuruluşların kişisel verilerin işlenmesine yol açacak kararlarının icrası sırasında hukuka uygun bir işleme faaliyeti meydana gelecektir. Son olarak belirtelim ki bir sözleşmenin gereği olarak ancak o sözleşmenin tarafı olmayan bir kişinin verileri işlenecek olursa burada sözleşmenin ifası değil hukuki yükümlülüğün yerine getirilmesi başlıklı hukuka uygunluk sebebi uygulanacaktır.[452]

---

[448] Türkiye Büyük Millet Meclisi, Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu, Madde Gerekçeleri, s.9; Dülger, *Kişisel Verilerin Korunması Hukuku,* s.411-412

[449] Dülger, *Kişisel Verilerin Korunması Hukuku*, s.411-412

[450] Korkmaz*, Kişisel Verilerin Ceza Hukuku Kapsamında Korunması* (2019), s.472

[451] Türkiye Büyük Millet Meclisi, Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu, Madde Gerekçeleri, s.9

[452] Dülger, *Kişisel Verilerin Korunması Hukuku*, s.403

4.3.1.7. Veri Sorumlusunun Menfaatleri Açısından Zorunluluk

6698 sayılı Kanun'da yer alan hukuka uygunluk nedenlerinden bir diğeri veri sorumlusunun meşru menfaatleri açısından kişisel veri işlemenin zorunlu olması halidir. Söz konusu hukuka uygunluk sebebinden yararlanılabilmesi için verisi işlenen ilgili kişinin temel hak ve özgürlüklerine zarar verilmemelidir. Örneğin şirket organizasyonu kapsamında terfi, zam gibi konuların düzenlenmesi açısından ya da firmadaki görev dağılımlarının sağlıklı bir şekilde yapılabilmesi için çalışanların verilerinin işlenmesi durumunda rıza aranmaksızın bu faaliyet yürütülebilecektir. Verilen örneklerde veri sorumlusu olan şirket sahibi açısından liyakatli kişilerin terfi alması veyahut organizasyonun oluşturulması meşru menfaat sayılmaktadır. Ayrıca vurgulamak gerekir ki söz konusu işleme faaliyeti sırasında veri sorumlusu ve verisi işlenen kişilerin menfaatleri arasında bir dengesizlik oluşmamalıdır.[453]

4.3.1.8. Sağlık ve Cinsel Hayata İlişkin Verilerin İşlenmesi

Kişisel Verilerin Korunması Kanunu'nun 6'ncı maddesinde özel nitelikli verilerin işlenmesinin şartları düzenlenmiştir. Hassas veriler için de diğer verilerde olduğu gibi ana kural ilgili kişinin rızasının alınmasıdır. Ancak kanunda rızanın alınmadığı bazı durumlarda özel kategorideki verilerin işlenebileceği de hükme bağlanmıştır. Bu kapsamda sağlık ve cinsel hayat dışındaki hassas veriler kanunlarda öngörülen hallerde ilgili kişinin rızasına başvurulmadan işlenebilecektir. Sağlık ve cinsel hayata ilişkin veriler açısından ise iki şartın sağlanmasıyla rıza aranmaksızın bu bilgilerin işlenebileceği öngörülmüştür. Şöyle ki öncelikle saydığımız bu iki kategorideki veriler, *"kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla"* işlenmelidir. Amaç açısından getirilen bu koşulun yanı sıra diğer bir şart da bu verileri işleyebilecek kişiler yönünden getirilmiştir ve söz konusu işleme faaliyeti *"sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından"* gerçekleştirilmelidir. Tüm bu koşullar sağlandığında artık hukuka uygun bir veri işleme faaliyetinden bahsedilebilecektir.

[453] Türkiye Büyük Millet Meclisi, Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu, Madde Gerekçeleri, s.9

4.3.1.9. İlgili Kişinin Verilerini Alenileştirmesi

Kişisel Verilerin Korunması Kanunu kapsamında son olarak değineceğimiz hukuka uygunluk sebebi ilgili kişinin kendi kişisel verilerini alenileştirmesi halidir. Kanun koyucu veri öznesi tarafından kamuoyuna açıklanmış ve herkesçe bilinebilir hale gelmiş veriler açısından artık korunması gereken hukuki yararın kalktığını kabul ederek rıza aranmaksızın bu verilerin işleme faaliyetine konu edilebileceğini kabul etmiştir.[454] Bu gibi hallere örnek olarak kişinin sosyal medya hesabından herkese açık olarak yaptığı paylaşımlar yahut belirli bir iş dolayısıyla kendisiyle iletişim kurulması için iletişim bilgilerini alenileştirmesi verilebilecektir.[455]

Kişisel verilerin, sahibi olan kişi tarafından aleni hale getirilmesinde bazı hususlara dikkat etmekte fayda vardır. Öncelikle alenileştirme iradesi, ilgili kişi tarafından ortaya konulmuş olmalı ve veri öznesi dışındaki kişilerin söz konusu bilgileri aleni hale getirmesini izleyen veri işleme faaliyetinin hukuka uygun olmayacağı bilinmelidir. Bunun yanında kamuoyuna açıklanan bilgiler açısından ilgili kişinin alenileştirme amacı da göz önünde bulundurulmalı ve buna göre veri işleme faaliyeti yürütülmelidir. Nitekim ilgili kişinin hedeflediği amaç dışındaki veri işleme faaliyetleri hukuka uygun olmayacaktır. Zira kişinin kendi verilerini paylaşması o verilerin hiçbir kurala bağlı olmaksızın istenildiği gibi kullanılabileceği anlamına gelmemektedir. Bu noktada bahsi geçen amacın belirlenmesinde veri sahibinin açık beyanı önem taşımaktadır. Ancak ilgili kişiden bu beyan alınamayacak ise alenileştirme işleminin doğası ile birlikte dürüstlük kuralı da dikkate alınarak KVKK'nin dördüncü maddesinde yer alan genel ilkelere göre bir sonuca ulaşılmalıdır.[456] Neticeten veri öznesi tarafından kamuoyuyla paylaşılmış verilerin aleni hale getirilmesindeki amaç ile bağlı kalınarak sınırlı ve ölçülü bir şekilde söz konusu bilgiler işlenmelidir.[457]

---

[454] Türkiye Büyük Millet Meclisi, Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu, Madde Gerekçeleri, s.9

[455] Dülger, *Kişisel Verilerin Korunması Hukuku*, s.405

[456] Küzeci, *Kişisel Verilerin Korunması*; Dülger, *Kişisel Verilerin Korunması Hukuku*, s.405-406. Ayrıca yazar, toplu ve kamuya açık etkinlikerde kişilerin görüntülerinin çekilmesine yönelik olarak etkinliğe katılan davetlilerin, kendi verilerini o etkinliğe katılarak hali hazırda alenileştirmiş olduklarını ve buradaki hukuka uygunluk sebebinin verinin ilgili kişi tarafından alenileştirilmesi olduğunu vurgulamaktadır.

[457] Küzeci, *Kişisel Verilerin Korunması*, s.346

5. Suçun Özel Görünüş Biçimleri

5.1. Teşebbüs

Kişisel verileri hukuka aykırı olarak verme, yayma veya ele geçirme suçu, sırf hareket suçu olduğu için suçu meydana getiren icra hareketleri kısımlara bölünebildiği ölçüde bu suça teşebbüs mümkün olacaktır. Örneğin içerisinde kişisel veri olan elektronik sistemin şifresi verileceği sırada ya da kişilerin konuşma kayıtlarının başkasına teslimi sırasında failin yakalanması halinde suç teşebbüs aşamasında kalacaktır.[458] Yine aynı şekilde fail, kişisel verileri başkasına teslim etmek için harekete geçer ancak elinde olmayan nedenlerden dolayı verileri teslim edemez ise suç teşebbüs aşamasında kalacaktır. Teşebbüsün meydana gelmesi için hareketin otomatiklik içeren yöntemlerle işlenmesi şart değildir. Bu kapsamda örneğin mektup yoluyla veri iletimi de teşebbüse uygundur. Aynı şekilde kişisel veri içeren mektubun postada kaybolması da teşebbüs aşamasında kalmaya örnek olarak gösterilebilecektir.[459]

İnceleme konumuz olan suç açısından şartları oluştuğunda teşebbüs mümkün olduğu gibi somut olaya göre gönüllü vazgeçme hükümleri de tatbik edilebilecektir.[460] Örneğin fail verilerin bulunduğu sisteme girer ancak verilerin içeriklerine erişmek suretiyle bilgi sahibi olmadan bu verileri başkasına vermekten vazgeçerse 136. madde açısından gönüllü vazgeçme hükümleri uygulanacaktır. Bunun sonucunda ise faile kişisel verileri hukuka aykırı verme veya ele geçirme suçuna teşebbüsten ceza verilemeyecek ancak o ana kadarki eylemleri bilişim sistemine girme suçunu oluşturduğu için bu suçtan ceza verilecektir.[461] Aynı durum kişinin kendisine ait kişisel verileri değiştirmek suretiyle menfaat elde etme amacıyla sisteme girip eylemini tamamlamadan vazgeçmesi halinde de ortaya çıkacak ve 243-244. maddeler yönünden inceleme yapılacaktır.[462] Yargıtay ise kişilerin kredi/bankomat kart bilgilerinin kopyalanmasına ilişkin olarak sanıklardan ele geçirilen kopyalama düzeneklerinde kart sahiplerini ilgilendiren bir bilgi olması durumunda 136. madde uyarınca tamamlanmış suç hükümlerine göre cezalandırma yapılması gerektiğini belirtmektedir. Yine Yüksek Mahkeme bu türden olaylarda faillerin elinde bulunan kopyalama cihazlarında herhangi bir bilgiye ulaşılamaması halinde ise kişisel verilerin hukuka aykırı olarak

[458] Sevük, s.503; Dülger, *Kişisel Verilerin Korunması Hukuku*, s.748; Korkmaz, *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması* (2019), s.474; Yaşar/Gökcan/ Artuç, s.4128
[459] Korkmaz, *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması* (2019), s.474; Yılmaz, s.124
[460] Taşkın, s.108
[461] Korkmaz, *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması* (2019), s.474
[462] Bük, s.226

verilmesi veya ele geçirilmesi suçuna teşebbüsten hüküm kurulması gerektiğini ifade etmektedir.[463]

Son olarak değinmek gerekirse ele geçirme fiili açısından teşebbüs hali bazı özellikler arz etmektedir. Şöyle ki kişisel verilerin bulunduğu yere girilerek dolabı açmaya çalışma veya verilere erişmek için bilişim sistemine girmek ele geçirme fiili açısından teşebbüs aşamasında kalacaktır. Bu bağlamda şayet fail kişisel verilerin muhtevasına vakıf olur ancak onları bulunduğu yerden almaz veya o bilgileri bir yere kaydetmez ise ele geçirme açısından artık gönüllü vazgeçme hükümleri uygulanamayacaktır. Zira ele geçirme fiili bu bilgilerin öğrenilmesiyle artık tamamlanmış sayılır.[464] Aynı şekilde failin içine girdiği sistemden atılması suretiyle ele geçirmeyi gerçekleştiremediği durumda da teşebbüs hükümlerince cezalandırma yapılacaktır.[465]

5.2. İştirak

Kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçu iştirak açısından farklı bir özellik göstermemekle birlikte bu suça iştirakin her şekli mümkündür ve bu konuda genel hükümlerden yararlanılarak bir sonuca varılmalıdır. Bunun yanında suça iştirak edenlerin 137'nci maddede belirtilen kamu görevlisi veya belirli bir meslek veya sanat icra eden kişi olması durumunda bu kişilere söz konusu maddedeki ağırlaştırıcı hal göz önünde bulundurularak ceza verilecektir.[466] Ancak somut olayda failin işlediği fiiller hukuka uygun olarak meydana gelmiş ise bu fiile iştirak eden kişiler de cezalandırılmayacaktır. Ayrıca belirtelim ki bu suç birlikte işlenebilecek ve bu durumda suçu işleyen kişilerden her biri ayrı ayrı fail olarak sorumlu tutulacaktır.[467]

---

[463] YARGITAY 8. CEZA DAİRESİ E. 2018/6171 K. 2018/10436 T. 8.10.2018; YARGITAY 8. CEZA DAİRESİ E. 2016/12565 K. 2017/12892 T. 20.11.2017; YARGITAY 8. CEZA DAİRESİ; E. 2012/31924 K. 2014/1479 T. 23.1.2014

[464] Korkmaz, *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması* (2019), s.475

[465] Sarıusta, s.161

[466] Dülger, *Kişisel Verilerin Korunması Hukuku*, s.748; Özbek/ Doğan/ Bacaksız, *Türk Ceza Hukuku Özel Hükümler*, s.600; Ali Parlar, **Açıklamalı-Atıflı-Uygulamalı Türk Ceza kanunu El Kitabı**, Bilge Yayınevi, Ankara 2018, s.652; Artuç, *Kişilere Karşı Suçlar*, s.1649

[467] Sevük, s.503-504;*"Haberleşme sürecinin taraflarını ve zamanını gösteren bilgiler, "kişisel veri" kapsamında olup, katılan ...'nin ne zaman kiminle hangi sıklıkla ve ne kadar süreyle görüştüğüne dair 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 dair yerel mahkemenin kabulünde bir isabetsizlik görülmemiştir."* YARGITAY 12. CEZA DAİRESİ E. 2015/10994 K. 2017/635 T. 1.2.2017

Çalışmamızın konusunu oluşturan suç tipiyle ilgili olarak iştirak hükümleri açısından önem arz eden son bir konuya daha değinmekte fayda görmekteyiz. 136. maddedeki suça iştirak noktasında somut vakıada suçu işlemeye karar veren kişilerin daha önceden anlaşıp bu anlaşma doğrultusunda hareket edip etmediklerinin tespiti son derece mühimdir. Zira faillerin önceden anlaşıp anlaşmadıklarının tespit edilmesi suça iştirak etme noktasındaki niyetlerini göstermektedir. Şöyle ki mağdurun kişisel verileri ele geçirilir ve bu ele geçirilen veriler başka bir kişiye verilir ve o kişi de mağdurun verilerini yayarsa ve bu konuda da failler arasında önceden yapılan bir anlaşma yoksa iki ayrı suç oluşacaktır. Birinci fail, verileri ele geçirme fiilinden ikinci fail ise verileri yayma fiilinden dolayı cezalandırılacaktır. Buna karşın iki fail arasında söz konusu verileri ele geçirip yayma konusunda daha önceden yapılmış bir anlaşma var ise suça iştirak hükümleri uygulanacaktır. Ayrıca gerçekleştirilen hareketler arasındaki zaman farkının da faillerin bir suç işleme kararına dayanarak hareket edip etmediklerini tespit etmekte yol gösterici olacağını bu noktada unutmamak gerekir.[468]

5.3. İçtima

İçtima başlığı altında öncelikle zincirleme suç hükümlerine değinmek gerekmektedir. Kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçu aynı suç işleme kararı kapsamında değişik zamanlarda aynı kişiye karşı birden fazla kez işlenecek olursa zincirleme suç hükümleri uygulanacaktır. Örneğin bir kişinin kişisel veri niteliğindeki fotoğraflarının değişik zaman dilimlerinde sürekli olarak yayınlanması durumunda zincirleme suç meydana gelecek ve faile bu durum dikkate alınarak ceza verilecektir. Bu noktada maddedeki seçimlik hareketlerden birinin veya daha fazlasının işlenmesinin zincirleme suç açısından bir önemi yoktur ve TCK m.43/1'e göre cezalandırma yapılacaktır.[469] Ayrıca belirtmek gerekir ki 136. maddedeki seçimlik hareketlerin aynı anda birden fazlası işlenecek olursa tek bir suçtan cezalandırma yapılacak olup ceza verilirken alt sınırdan uzaklaşılabilecektir.

Failin tek bir fiille 136. maddedeki suçu aynı anda farklı kişilere karşı işlemesi halinde TCK m.43/2 uygulanacaktır. Bu durumda fail birden fazla kişiye ait kişisel verileri tek bir fiille başka bir kişiye teslim ederse zincirleme suç hükümleri tatbik edilecektir. Örneğin hastanede çalışan

[468] Korkmaz, *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması* (2019), s.475; Uyarer, s.222

[469] Sevük, s.504; Korkmaz, *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması* (2019), s.477; Failin ele geçirdiği kişisel verileri iki gün arayla kısım kısım başka kişilerle paylaşması durumunda da zincirleme suç oluşacaktır. Bkz. Sert, s.148

bir görevlinin psikaytri bölümündeki hastaların kişisel veri içeren dosyalarını başkasına göndermesi durumunda bir fiille birden fazla kişiye karşı aynı suç işlenmiş olacaktır.[470]

Fikri içtima konusu kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçu açısından çeşitli ihtimallerin ortaya çıktığı bir alan olması hasebiyle aşağıda ayrıntılı olarak incelenecektir. Bu bağlamda inceleme konumuz olan suçun diğer suç tipleri ile olan ilişkisini de göz önünde tutarak içtima bahsini açıklamaya çalışacağız.

Öncelikle 136. maddedeki suçun 135. maddede düzenlenen kişisel verilerin kaydedilmesi suçu ile karşı karşıya gelebileceğini belirtmemiz gerekir. Failin gerçekleştirdiği hareketin aynı zamanda kişisel verilerin hukuka aykırı olarak kaydedilmesi anlamına geldiği somut olaylarda fikri içtima uygulanacak ve faile daha ağır ceza öngörülen 136. madde uyarınca ceza verilecektir. Örneğin, mağdura ait verilerin herkesin erişimine açık bir internet sitesine kaydedilmesi ile kişisel veriler hem kaydedilmiş olacak hem de yayılmış olacaktır. Bu durumda kişisel verilerin hukuka aykırı olarak verilmesi veya ele geçirilmesi suçundan hüküm kurulacaktır.[471]

Ayrıca belirtmemiz gerekir ki kişisel verilerin kaydedilmesi suçu ile 136. maddedeki suç arasında geçit suç ilişkisi somut olayın özelliğine göre belirlenmelidir. Şayet fail, 136. maddedeki seçimlik hareketleri işlemek açısından kaydetme fiiline ihtiyaç duyuyor ve kaydetme açısından bir zorunluluk var ise geçit ilişkisi meydana gelecektir. Bunun sonucunda da faile sadece 136. madde uyarınca ceza verilecektir.[472] Ancak her zaman bahsi geçen iki suç tipi arasında geçit suç ilişkisi kurulamayabilir. Zira suça konu veriler kaydedilmeden de başkasına verilebilir, yayılabilir veya ele geçirilebilir. Örnek olarak ise bulut bilişiminde bulunan verilere erişmek için şifrelerin elde edilmesi ya da hali hazırda sanal ortamda kayıtlı kişisel verilerin yayılması durumu verilebilecektir. Tüm bu ihtimallerde kaydetme fiili işlenmeden 136. maddedeki fiiller işlenmiş olacaktır.[473] Son olarak belirtelim ki suça konu veriler farklı amaçlarla farklı bir zamanda ilk önce kaydedilir ve daha sonra 136. maddedeki seçimlik hareketler işlenirse ayrı ayrı iki suç oluşacaktır.[474]

Çalışmamızın konusunu oluşturan suç tipi açısından içtima bahsinde önem arz eden diğer bir suç ise Türk Ceza Kanunu'nun 243. maddesinde düzenlenen bilişim sistemine girme suçudur. Zira genellikle kişisel verileri ele geçirmek için bilişim sistemlerine girilmekte ardından

[470] Artuç, *Kişilere Karşı Suçlar*, s.1650; Sert, s.149
[471] Özbek/ Doğan/ Bacaksız, *Türk Ceza Hukuku Özel Hükümler*, s.600; Çakır, s.592
[472] Korkmaz, *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması* (2019), s.481
[473] Dülger, *Kişisel Verilerin Korunması Hukuku*, s.749
[474] Korkmaz, *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması* (2019), s.481; Çakır, s.591

sistemde mevcut olan bilgiler ele geçirilmektedir. Doktrinde kimi yazarlar söz konusu iki suç arasında geçit suç ilişkisi olduğunu ve failin yalnızca 136. madde uyarınca cezalandırılmasını savunurken[475] kimi yazarlar ise söz konusu iki suç arasında her durumda geçit-zorunluluk ilişkisi olmadığını, somut olayın özelliğine göre faile her iki suçtan da ceza verilebileceğini ifade etmişlerdir. Bunun sonucunda ise 243. maddedeki suç işlenmeden 136. maddedeki suç işlenemeyecekse ilk suç geçit suçu olarak kabul edilip yalnızca kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçundan hüküm kurulacak ancak iki suç arasında bir zorunluluk ilişkisi mevcut değilse (suçlar farklı saiklerle işlenmişse) faile her iki suçtan da ceza verilecektir.[476]

Kişisel verilerin hukuka aykırı olarak verilmesi veya ele geçirilmesi suçu ile içtima ilişkisi olabilecek diğer bir suç tipi ise TCK'nin 244. maddesindeki sistemi engelleme, bozma, verileri yok etme veya değiştirme suçunun 2. fıkrasında düzenlenmiştir. Bahsi geçen maddenin ikinci fıkrasında *"Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır."* hükmü yer almaktadır. Belirtmek gerekir ki 136. maddede sadece kişisel verilere ilişkin bir düzenleme yapılmış iken 244. maddenin bahsettiğimiz fıkrasında tüm veri çeşitleri kapsama dahil edilmiştir. Bunun yanında 244. maddede düzenlenen suç yalnızca bilişim sistemleri aracılığıyla işlenmekte iken 136. maddedeki suç farklı yollarla da işlenebilmektedir. Bu noktada şayet 244. maddenin 2'nci fıkrasında belirtilen başka bir yere gönderilen veriler kişisel veri vasfı taşıyor ise fail, tek bir fiille iki farklı suçu işlemiş olacak ve bu durumda cezası daha ağır olan suçtan cezalandırılacaktır.[477]

İçtima hükümlerinin uygulanabileceği diğer bir suç ise Türk Ceza Kanunu'nun 132. maddesinde yer alan haberleşmenin gizliliğini ihlal suçudur. Söz konusu maddenin ikinci fıkrasında kişilerin haberleşme içeriklerinin hukuka aykırı olarak ifşası düzenlenmiş iken aynı maddenin 3'üncü fıkrasında kendisiyle yapılan haberleşme içeriklerini haberleşmenin tarafı olan diğer kişinin rızası olmadan ifşa eden kişinin cezalandırılacağı hükme bağlanmıştır. Böylece bahsedilen maddelere göre ifşa edilen haberleşme içeriklerinin kişisel veri barındırması durumunda 136.

[475] Soyaslan, s.366

[476] Dülger, *Kişisel Verilerin Korunması Hukuku*, s.749; Korkmaz, *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması* (2019), s.482-483

[477] Korkmaz, *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması* (2019), s.483

maddedeki suç da meydana gelmiş olacaktır. Bu durumda ise fikri içtima hükümleri uyarınca ağır olan suçtan ceza verilmesi yoluna gidilecektir.[478]

Kişisel verilerin hukuka aykırı olarak verilmesi veya ele geçirilmesi suçu açısından en çok karşımıza çıkan sorunlardan biri ise TCK'nin 134. maddesinde düzenlenen özel hayatın gizliliğini ihlal suçu ile 136. maddedeki suçun aynı olayda değerlendirilmesi meselesidir. Daha önce de değindiğimiz üzere Yargıtay uygulamasına göre somut olayda kullanılan verinin niteliğine bakılarak bir değerlendirme yapılması gerekmektedir. Bu doğrultuda örneğin mağdura ait görüntü veya ses verisinin ifşası durumunda söz konusu görüntü ya da sesin yayılmasının 134. maddede düzenlenmesi nedeniyle ve bu verilerin (kişisel veri olduğunun kabulü ile birlikte) 136. madde anlamında kişisel veri olmadığı tespitinde bulunulduğu takdirde özel hayatın gizliliğini ihlal (m.134) suçundan hüküm kurulabileceği gibi suça konu görüntüler özel hayat kapsamında görülmeyip 136. maddenin uygulanması da gerekebilecektir. Bu türden vakıalarda paylaşılan verinin mağdurun başkalarının görmesini veya bilmesini isteyip istemeyeceği özel hayata ilişkin görüntü/ses olup olmadığı öncelikle tespit edilmelidir. Son olarak 134. maddedeki suçla bağlantılı olarak 132-134. maddeler arasında yer alan suçlara ilişkin olan şu hususa dikkat çekmek gerekir. Meydana gelen somut olayda failin eylemi şayet 132-134. maddelerde düzenlenen suç tiplerinde düzenlenmişse artık 136. maddeye başvurulmayacaktır.[479] Ancak yukarıda da vurguladığımız üzere aynı fiil ile hem 132-134. maddeler arasındaki suçlar hem de kişisel verilerin hukuka aykırı olarak verilmesi veya ele geçirilmesi suçu işlenecek olursa daha ağır cezayı gerektiren suçtan hüküm kurulacaktır.[480]

Mağdura ait verilerin açıklanması aynı zamanda hakaret suçunun oluşmasına da sebebiyet verecek olursa tek bir fiille birden fazla farklı suç meydana geleceğinden en ağır cezayı gerektiren suçtan cezalandırma yapılacaktır.[481]

Kamu görevlisinin başka bir kişiye verdiği veriler karşılığında o kişiden para veya para yerine ikame edilen bir değer almak suretiyle menfaat sağlaması durumunda ise rüşvet suçundan ceza verilmelidir.[482]

---

[478]Korkmaz, *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması* (2019), s.478. Yazar aynı şekilde TCK'nin 239. maddesinde düzenlenen ticarî sır, bankacılık sırrı veya müşteri sırrı niteliğindeki bilgi veya belgelerin açıklanması suçunda da şayet verilen veya ifşa edilen bilgiler arasında kişisel veriler var ise bu durumda 44. maddeye göre bir uygulama yapılmasını öngörmektedir. Bkz. s.481-482

[479] Artuç, *Kişilere Karşı Suçlar*, s.1650-1651

[480] Korkmaz, *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması*, s.478-479

[481] Sevük, s.504; Özbek/ Doğan/ Bacaksız, *Türk Ceza Hukuku Özel Hükümler*, s.600

[482] Artuç, *Kişilere Karşı Suçlar*, s.1650

Son olarak belirtelim ki Kişisel Verileri Koruma Kuruluna göre somut olayda işlenen fiil hem bir kabahat hem de bir suç meydana getirmekte ise sadece sübut bulan suç uyarınca cezalandırma yapılmalıdır.[483]

6. Yaptırım

Kişisel verileri verme, yayma veya ele geçirme suçunun yaptırımı iki yıldan dört yıla kadar hapis cezası olarak düzenlenmiştir. Daha önceden de değindiğimiz üzere 06.03.2014 tarihinde yürürlüğe giren 6526 sayılı Kanun ile suçun cezasının alt sınırı 1 yıldan 2 yıla çıkarılmıştır. Bu durumda fail, belirtilen yürürlük tarihinden önce suçu işlerse 1 yıldan 4 yıla kadar; şayet bu tarihten sonra işlerse 2 yıldan 4 yıla kadar hapis cezası ile cezalandırılacaktır.[484] Suçun konusu 5271 sayılı CMK'nin 236. maddesinin beşinci ve altıncı fıkraları uyarınca kayda alınan beyan ve görüntüler olursa cezada bir kat artırım yapılacaktır. Ayrıca 137. madde uyarınca suçun kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle işlenmesi veya belli bir meslek ve sanatın sağladığı kolaylıktan yararlanılmak suretiyle işlenmesi hallerinden biri mevcut ise verilecek ceza yarı oranında artırılacaktır.

Yapılan yargılama sonucunda faile verilecek ceza 1 yıldan az olursa 50. maddedeki seçenek yaptırımlara çevrilebilecektir. Ayrıca sonuç ceza 2 yıldan az olur ise hükmün açıklanmasının geri bırakılması veya erteleme kurumları uygulanabilecektir. Eklemek gerekir ki faile hapis cezası verilirse m.53/1'deki hak yoksunlukları hükmü gündeme gelecektir.[485]

Söz konusu suçun tüzel kişilerin bünyesinde işlenmesi durumunda TCK m.140 uyarınca bu tüzel kişiler hakkında 60'ıncı maddede düzenlenen güvenlik tedbirlerine hükmolunacaktır.[486]

7. Soruşturma Usulü

Verileri hukuka aykırı olarak verme veya ele geçirme suçu soruşturulması ve kovuşturulması resen yürütülen bir suç tipidir ve şikayet aranmamaktadır. Bu husus TCK m.139'da açıkça belirtilmiştir. Kamu görevlisi, görevi dolayısıyla söz konusu suçu işlerse 4483 sayılı Kanun uyarınca soruşturma izni alınması gerekecektir.[487] Ayrıca belirtmek gerekir ki bu suç, uzlaşma

---

[483] Kişisel Verileri Koruma Kurumu Yayınları, **6698 sayılı Kişisel Verilerin Korunması Kanununun Uygulanmasına Yönelik Soru Cevaplar**, s. 76.

[484] Artuç, *Kişilere Karşı Suçlar*, s.1651

[485] Artuç, *Kişilere Karşı Suçlar*, s.1651

[486] Ali Parlar, **Açıklamalı-Atıflı-Uygulamalı Türk Ceza kanunu El Kitabı**, Bilge Yayınevi, Ankara 2017, s.662

[487] Mustafa Artuç, **Pratik Türk Ceza Kanunu**, 5.Baskı, Ankara 2019, Adalet Yayınevi, s.767

hükümlerine tabi değildir. Dava zamanaşımı ise suçun temel şekli için TCK m.66/1-e uyarınca 8 yıl; 137.maddedeki nitelikli haller söz konusu ise 15 yıl olarak uygulanacaktır.[488]

8. Yetkili ve Görevli Mahkeme

Çalışmamızın konusu olan suç tipinin yargılaması 5235 sayılı Adli Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanun'un 11. maddesi uyarınca Asliye Ceza Mahkemesince yürütülecektir.[489] Yargılamayı yürütmekle yetkili mahkeme ise verme, yayma veya ele geçirme fiillerinin meydana geldiği yer mahkemesidir.[490]

[488] Sert, s.152
[489] Ali Parlar, *Açıklamalı-Atıflı-Uygulamalı Türk Ceza kanunu El Kitabı*, s.653
[490] Artuç, *Kişilere Karşı Suçlar*, s.1652

SONUÇ

Bilgi, var olduğu ilk zamandan bugüne dek insanoğlunu kendine sahip olması noktasında cezbetmiştir. Zira bilgi, elinde bulunan kişi açısından bir kudret kaynağıdır ve çeşitli formlara bürünerek karşımıza çıkmaktadır. Bu görünüş şekillerinden birisi de çalışmamızın ana kavramı olan kişisel veridir. İşlem hayatının hızı, hizmet sunumu ve istihbari faaliyet gibi nedenlerle her geçen gün daha fazla hayatımıza hakim olan veri kavramı artık hukuki düzenlemelerle birlikte yargı içtihatlarına da konu olmaktadır. Zira kişisel veri, insanın temel hak ve özgürlükleri arasında önemli bir yer tutan özel hayatın gizliliği ile yakından ilişkilidir. Bundan dolayıdır ki veri işleme faaliyetleri arttıkça kişisel alan ihlalleri artış göstermekte ve dinamik bir sosyal bilim dalı olan hukukun da ortaya çıkan yeni sorunlara çare bularak hak süjesi olan insanı koruması gerekmektedir. Tam bu noktada ortaya çıkan kişisel verilerin korunması hakkı ile özel hayat alanı, kişisel verileri işleyen organizasyonlara karşı korunmakta ve bireyin kişiliğini geliştirebilmesinin önü açılmaktadır.

Kişisel veri kavramı ulusal ve uluslararası mevzuatta *"Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi"* olarak tanımlanmaktadır. Bu anlamlandırmanın sonucunda kişisel verinin taşıması gereken bazı özellikler ortaya çıkmaktadır. Söz konusu ögeler sıralanacak olursa kimliği belirli veya belirlenebilir olma, gerçek kişiye ilişkin olma, bilgi niteliğinde olma şeklinde bir dizlim ortaya çıkacaktır. Kimliği belirli olma şartı kimliği somut bir şekilde ortada olan yani kim olduğunun tespit edilmesi için herhangi bir işleme/aşamaya ihtiyaç bulunmayan kişiyi ifade etmektedir. Kimliği belirlenebilir nitelikte olmak ise kişinin kimliğinin somutlaştırılması açısından elde bulunan verinin bazı aşamalardan geçmesi gerektiği anlamına gelmektedir. Gerçek kişi koşulu ise bizi iki ayrı sonuca götürmektedir. Bunlardan ilki tüzel kişilerin kişisel veriye sahip olamayacağı iken diğeri ise ölen kişilerin artık kişisel verinin öznesi olamayacağıdır. Her türlü bilgi şeklinde belirtilen üçüncü şart ise kişisel verinin bir bilgi çeşidi olduğunu ve teknolojinin gelişimine bağlı olarak genişleyebilecek bir kapsamı olduğunu belirtmektedir.

Kişisel veri kavramının aksine tahdidi olarak çeşitleri sayılan özel nitelik nitelikli veri ise Kişisel Verilerin Korunması Kanunu'nun 6. maddesinde düzenlenmiştir. Buna göre ırk, etnik köken, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançlar, kılık ve kıyafet, dernek, vakıf ya da sendika üyeliği, sağlık, cinsel hayat, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili veriler ile biyometrik ve genetik veriler hassas veri olarak kabul edilecektir. Özel kategorideki veriler açısından GDPR'ın tanımlamasına bakıldığında ise KVKK'de yer verilen

mezhep, kılık ve kıyafet, dernek ve vakıf üyeliği, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verilerin sayılmadığı ve cinsel yönelimin ise KVKK'den farklı olarak tanımın kapsamına dahil edildiği görülmektedir. Ceza mahkûmiyeti ve güvenlik tedbirlerini ilgilendiren verilerin de GDPR'ın 10. maddesinde ayrıca düzenlendiği görülmektedir. Hassas veriler, ilgili kişiye ilişkin önemli bilgiler ihtiva ettiğinden bu verilerin işlenmesinde son derece dikkatli olunmalıdır. Zira bahse konu veriler, veri öznesinin ayrımcılığa maruz kalmasına neden olabilecek ağırlıktadır. Bununla birlikte bu veri kategorisindeki veriler sınırlı sayıdadır ve kıyas yoluyla başka veriler söz konusu kategorinin kapsama dahil edilemeyecektir.

Kişisel verilerin işlenmesi, verilerin elde edilmesi ile başlayan ve bu bilgilerin, silinmesi veya yok edilmesine kadarki süreçte maruz kaldığı her türlü işlem olarak kabul edilmektedir. Kişisel verilerin işlenmesi ile ilgili olarak karşımıza çıkan fiillerin veri işleme faaliyeti kapsamında olup olmadığını belirlemek için öncelikle bu işlemin otomatiklik özelliği taşıyıp taşımadığına bakılmalıdır. Nitekim yasa otomatik yollarla işlemeyi otomatik olmayan yollarla işlemeden ayırmıştır. Otomatiklik kavramı ile kastedilen ise telefon ve bilgisayar gibi cihazların donanım ve yazılım özellikleri kullanılarak ve insan müdahalesi de olmadan yapılan işleme faaliyetidir. Bu bağlamda otomatik yöntemlerle yapılan işleme faaliyetlerinin hepsi KVKK kapsamında değerlendirilebilecek iken otomatik olmayan metodların uygulanmasında bir veri kayıt sisteminin varlığı aranacaktır. Veri kayıt sistemi ise işleme faaliyetine konu verilerin belirli kriterler gözetilerek yapılandırıldığı bir organizasyonu ifade etmektedir. Otomatik olmayan yöntemlerin kullanıldığı ve bir veri kayıt sisteminin de bulunmadığı durumlarda ise KVKK anlamında kişisel verilerin işlenmesinden söz edilemeyecektir. Ancak 6698 sayılı Kanun anlamında bir işleme faaliyetinin bulunmaması söz konusu eylemlerin diğer şartların da bulunması durumunda suç sayılmasına engel teşkil etmeyecektir. Zira TCK'deki verileri hukuka aykırı olarak verme veya ele geçirme suçu açısından KVKK'deki işleme kavramı baz alınmamaktadır.

Kişisel veri kavramı mevzuatımızda birçok yerde kendisine yer bulmakla birlikte ilk defa özel bir düzenlemeye konu olması 6698 sayılı Kişisel Verilerin Korunması Kanunu ile birlikte olmuştur. Aslında ülkemizde 1989 yılından itibaren çeşitli komisyonlar özel bir veri koruma yasası için toplanmış ancak çalışmalar ne yazık ki bir türlü nihayete erdirilememiştir. Bu kapsamda atılan önemli adımlardan biri ise 2010 yılında yapılan Anayasa değişikliği olmuştur. Söz konusu değişiklikle birlikte Anayasamızın Özel Hayatın Gizililiği başlıklı 20. maddesine herkesin kişisel verilerinin korunmasını isteme hakkına sahip olduğu ve kişisel verilerin ancak kanunda gösterilen hallerde veya açık rızaya bağlı olarak işlenebileceği hükmü dercedilmiştir.

Bunun yanı sıra Türk Medeni Kanunu ve Türk Borçlar Kanunu'nda da kişisel verileri ilgilendiren birtakım hükümler mevcuttur. Nitekim KVKK'nin 14. maddesinde kişilik hakları ihlal edilen kişilerin genel hükümlere göre tazminat isteme haklarının saklı tutulduğu belirtilerek TMK ve TBK kapsamında ilgili kişinin tazminat talep edebileceği hüküm altına alınmıştır. Ayrıca İş Kanunu'nda da işçi-işveren ilişkisi bağlamında taraflara kişisel verilerle ilgili çeşitli yükümlülükler yüklenmiş ve özellikle işçinin özlük dosyası ile ilgili durumlara dikkat çekilmiştir.

Kişisel verilerin korunması açısından şüphesiz mevzuatımızdaki en önemli düzenleme 6698 sayılı Kişisel Verilerin Korunması Kanunu'dur. Sonuçsuz kalan çeşitli kanunlaştırma çalışmalarının akabinde 6698 sayılı Kişisel Verilerin Korunması Kanunu 24 Mart 2016 tarihinde TBMM'de kabul edilerek yürürlüğe girmiştir. Kanunda ilk olarak bazı terimlerin tanımlamaları yapıldıktan sonra kişisel verilerin işlenme şartları, kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesi, kişisel verilerin aktarılmasına ilişkin hükümlere yer verilmiştir. Sonrasında veri sorumlusunun yükümlülüklerine, ilgili kişinin haklarına değinilip veri sorumlusuna başvuru ve veri sorumluları siciline ilişkin kurallar düzenlenmiştir. Yasanın son kısmında ise suçlar ve kabahatlerle birlikte Kişisel Verileri Koruma Kurumu'nun yapısına ilişkin düzenlemeler yer almıştır.

Kişisel Verilerin Korunması Kanunu yürürlüğe girmeden önce kişisel verileri koruma altına alan en önemli düzenlemeler Türk Ceza Kanunu'nda yer almıştır. Bu bağlamda 5237 sayılı Kanun'nda kişisel verileri münhasıran konu alan suç tipleri 135 ila 140. maddeler arasında düzenlenmiştir. 135. maddede "Kişisel verilerin kaydedilmesi", 136. maddede "Verileri hukuka aykırı olarak verme veya ele geçirme" ve 138. maddede "Verileri yok etmeme" suçlarına yer verilmiştir. Sayılan suçlar kişisel verileri doğrudan konu alırken bazı suçlar ise kişisel verilerin korunmasını dolaylı yoldan sağlamaktadır. Dolaylı koruma sağlayan suç tiplerine örnek olarak ise 134. maddede yer alan "Özel hayatın gizliliğini ihlal", 133. maddede yer alan "Kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması" ve 244. maddede yer alan "Sistemi engelleme, bozma, verileri yok etme veya değiştirme" gösterilebilecektir. Çalışmamızın konusunu ise 136. maddede düzenlenen verileri hukuka aykırı olarak verme veya ele geçirme suçu oluşturmaktadır.

Türk Ceza Kanunu'nun 136. maddesinde yer alan verileri hukuka aykırı olarak verme veya ele geçirme suçu ile ilgili olarak kişisel veri kavramının ceza kanununda tanımlanmamış olmasından dolayı suçta ve cezada kanunilik ilkesi gözetilerek Anayasa Mahkemesine iptal başvurusunda bulunulmuş ancak söz konusu başvuru reddedilmiştir. Bununla birlikte bahsi

geçen madde metninde günümüze dek iki kez değişiklik yapılmış ve bu değişikliklerden ilkinde 2014 yılında birinci fıkradaki fiillerin alt sınırı bir yıldan iki yıla çıkarılmıştır. 2019 yılında yapılan ikinci değişiklikle birlikte ise maddeye ikinci fıkra eklenmiş ve suçun konusuna bağlı olarak daha ağır cezayı gerektiren bir hal düzenlenmiştir. Madde metninin başlığında yayma fiiline yer verilmeyişi ve kişisel veri kavramı yerine sadece veri teriminin tercih edilmiş olması eleştirilere konu olmuştur.

Verileri hukuka aykırı olarak verme veya ele geçirme suçu ile korunan hukuki değer hakkında doktrinde çeşitli görüşler mevcuttur ancak söz konusu görüşler ve Yargıtay uygulaması da gözetildiğinde bu suç tipi ile özel olarak kişisel verilerin genelde ise kişilerin özel hayatının korunduğu söylenebilecektir. Bahse konu suç tipinin fiil unsuru, kişisel verilerin hukuka aykırı olarak bir başkasına verilmesi, yayılması veya ele geçirilmesidir. 136. maddedeki suç, soyut tehlike suçu olup meydana gelmesi açısından herhangi bir zarar aranmamaktadır. Ayrıca bu suç, maddede sayılan hareketlerin yapılmasıyla vücut bulmakla birlikte ek olarak bir netice aranmamaktadır ve bu haliyle sırf hareket suçu olarak karşımıza çıkmaktadır. Bunun yanında söz konusu suçun sübutunda kesintinin olup olmamasının dikkate alınmaması da bu suçun ani hareketli suçlar arasında değerlendirilmesini gerektirmektedir. Eklemek gerekirse 136. maddede sayılan hareketler seçimlik olarak düzenlenmiş olup bu fiillerin yalnızca birisinin veyahut aynı anda birkaçının işlenmesi tek suç oluşmasına neden olacaktır. Bu yönüyle de seçimlik hareketli bir suç özelliğinden bahsedilecektir. Son olarak değinmek gerekirse bahse konu suç, serbest hareketli ve aynı zamanda icrai bir suç tipi olarak değerlendirilmektedir.

Verileri hukuka aykırı olarak verme veya ele geçirme suçunun faili herkes olabilecektir. Bu yönüyle söz konusu suç, özgü suç özelliği göstermemektedir. Ancak 137. maddede sayılan kişilerin bu suçu işlemesi durumunda daha ağır ceza verilecektir. İnceleme konumuz olan suçun mağduru ise herkes olabilecektir. Bu noktada mağdurluk açısından suça konu veriye malik veya zilyet olma şartı aranmamakta yalnızca ilgili kişi olmak yeterli görülmektedir. Ayrıca vurgulayalım ki tüzel kişiler bu suçun mağduru olamamakla birlikte suçtan zarar gören olarak kabul edilebilecektir. 136. maddenin ikinci fıkrası gündeme geldiğinde ise suçun mağduru cinsel istismar ve cinsel saldırı suçları kendisine karşı işlenmekle birlikte beyan ve görüntüleri CMK m.236'ya göre kayda alınan kişiler olacaktır.

Çalışmamızın konusu olan suçla ilgili olarak Türk Ceza Kanunu'nda üç farklı nitelikli hal düzenlenmiştir. Bu nitelikli hallerin hepsi daha ağır cezayı gerektirmektedir. Bahsi geçen nitelikli hallerden ilki 136. maddenin ikinci fıkrasında yer almakta ve suçun konusunu ilgilendirmektedir. İkinci fıkraya göre suçun konusu Ceza Muhakemesi Kanunu'nun 236.

maddesinin 5. ve 6. fıkraları uyarınca kayda alınan beyan ve görüntüler ise faile verilecek cezada bir kat artırıma gidilecektir. Diğer nitelikli haller ise 137. maddede düzenlenen suçun kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle işlenmesi ve suçun belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenmesi durumlarıdır. Bu nitelikli haller meydana geldiğinde ise verilecek cezada yarı oranında artırım yapılacaktır.

Verileri hukuka aykırı olarak verme veya ele geçirme suçunun manevi unsuru kasttır. Suç tipi düzenlenirken maddede hukuka aykırılığa özellikle yer verildiği içindir ki söz konusu suç ancak doğrudan kastla işlenebilecektir. Böylece failin maddede seçimlik olarak gösterilen suça konu fiilleri işlerken yaptığı hareketlerin hukuka aykırı olduğunun bilincinde olması gerekmektedir. Ayrıca suçun işlenmesi sırasında failin güttüğü saik önem taşımamaktadır ve söz konusu suçun neticesi sebebiyle ağırlaşmış hali de kanunda düzenlenmemiştir.

Eserimize konu suç tipi düzenlenirken hukuka aykırılığa madde metninde ayrıca yer verilmiş olması hukuka aykırılığın artık tipikliğin bir unsuru olmasını sağlamaktadır. Bahse konu hukuka aykırılığın aşılması ve fiilin suç oluşturmaması açısından ise hukuka uygunluk sebeplerine ihtiyaç duyulmaktadır. Bu kapsamda söz konusu suç açısından hukuka uygunluk nedenleri Türk Ceza Kanunu'nda sayılanlar ve Kişisel Verilerin Korunması Kanunu'nda sayılanlar olarak ikiye ayrılabilecektir. TCK'de sayılan hukuka uygunluk nedenleri mağdurun rızası ve kanun hükmünün icrası şeklinde sıralanabilecek iken KVKK'deki hukuka nedenleri kişinin kendisinin veya başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasında gerekli olma, hakkın tesisi, kullanılması ve korunması için zorunluluk olması, veri sorumlusunun hukuki yükümlülüğünü gerçekleştirmesi açısından zorunlu olması, veri sorumlusunun menfaatleri açısından zorunluluk bulunması, ilgili kişinin verilerini alenileştirmesi olarak belirtilebilecektir.

Verileri hukuka aykırı olarak verme, yayma veya ele geçirme suçu, sırf hareket suçu olduğu için suçu meydana getiren icra hareketleri kısımlara bölünebildiği ölçüde bu suça teşebbüs mümkün olacaktır. Ayrıca bu suça iştirakin her şekli mümkündür ve iştirak ile ilgili olarak genel hükümlere göre bir çözüme gidilecektir. Bu suç, aynı suç işleme kararı kapsamında değişik zamanlarda aynı kişiye karşı birden fazla kez işlenecek olursa zincirleme suç hükümleri uygulanacaktır. Nitekim failin söz konusu suçu tek bir fiille aynı anda farklı kişilere karşı işlemesi halinde de TCK m.43/2 uygulanacaktır. Fikri içtima açısından ise 136. maddedeki suç, en fazla karşımıza 135. maddedeki kişisel verileri kaydetme ve 134. maddedeki özel hayatın gizliliğini ihlal suçları ile birlikte çıkmaktadır. Kişisel verileri kaydetme suçu gündeme

geldiğinde 136. maddedeki suç ile arasındaki geçit suç ilişkisi incelenmesi gerekmekle birlikte özel hayatın gizliliğini ihlal suçu ile karşılaşıldığında suça konu verinin niteliğine bakılarak bir karar verilmelidir. Bu kapsamda somut olaydaki veriler özel hayat ile ilişkilendirilebilecek ve mağdurun başkasının görmesini istemeyeceği veri niteliğini taşıyor ise 134. madde uyarınca cezalandırma yapılacak iken aksi durumda 136. maddeye göre hüküm kurulacaktır. Ayrıca eklemek gerekirse 136. maddedeki suç ile 243. maddedeki bilişim sistemine girme suçu, 244. maddedeki sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu, 132. maddedeki haberleşmenin gizliliğini ihlal suçları ile birlikte hakaret ve rüşvet suçları arasında da fikri içtima ilişkisi somut olaya göre doğabilecektir. Böylesi durumlarda TCK m.44 uyarınca daha ağır cezayı gerektiren suçtan hüküm kurulacaktır. Son olarak eklemek gerekirse Kişisel Verileri Koruma Kuruluna göre bir fiil hem suç hem de kabahat oluşturuyor ise yalnızca meydana gelen suçtan cezalandırma yapılmalıdır.

Verileri hukuka aykırı olarak verme veya ele geçirme suçunun cezası 2 yıldan 4 yıla kadar hapis cezası olmakla birlikte suça konu veriler 136/2'de sayılan beyan ve görüntüler olursa cezada bir kat; suç 137. maddede belirtilen kişilerce işlenecek olursa cezada yarı oranında artırım yapılacaktır. Ayrıca somut olayın özelliklerine göre 140. madde uyarınca tüzel kişiler hakkında da güvenlik tedbirlerine hükmedilebilecektir. Son olarak belirtmek gerekirse 136. maddedeki suçun soruşturulması veya kovuşturulması şikayete tabi olmayıp yargılaması ise Asliye Ceza Mahkemelerince yürütülecektir.

KAYNAKÇA

- **2018 Child Identity Fraud Study**, Javelin Strategy&Research
- **2019 Identity Fraud Study: Fraudsters Seek New Targets and Victims Bear the Brunt**, Javelin Strategy&Research
- Ackoff Russell Lincoln, **From Data to Wisdom**, Journal of Applied Systems Analysis 3-9, 1989
- **Act CXII of 2011 on the right to informational self-determination and on the freedom of information, Enforcement of rights related to personal data after the death of the data subject**
- **Act of 29 November 2017 on personal data protection and amending and supplementing certain Acts Chapter Four Specific Situations of Lawfull Processing of Personal Data**
- Adalet Bakanlığı Tematik Bilgi Notu, Kişisel Verilerin Korunması, 2015
- Akgül Aydın, **Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması**, Beta Yayınları, İstanbul 2014
- Akgül Aydın, **Kişisel Verilerin Korunması Bağlamında Biyometrik Yöntemlerin Kullanımı ve Danıştay Yaklaşımı**, TBB Dergisi 2015 (118)
- Akgül Aydın, **Kişisel Verilerin Korunmasında Yeni Bir Hak: "Unutulma Hakkı" Ve AB Adalet Divanı'nın "Google Kararı"** (Hakemli Makale) TBB Dergisi 2016 (116)

- Akıncı Ayşe Nur, **Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi**, İktisadi Sektörler Ve Koordinasyon Genel Müdürlüğü Bilgi Toplumu Dairesi Başkanlığı, Haziran 2017
- Akkurt Sinan Sami, **Kişisel Sağlık Verilerinin İşlenmesine Ve Covıd19 Pandemisi Sürecinde Mobil Uygulamalarla Paylaşılmasına Hukukî Bir Bakış**, İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi Covid-19 Hukuk Özel Sayısı Yıl:19 Sayı:38 Yaz 2020/2 (Covid-19 Özel Ek)
- Akman Nurten İnce, **Mirasbırakanın Dijital Bilgilerinin Mirasçılara Geçişi (Dijital Tereke)**, İnönü Üniversitesi Hukuk Fakültesi Dergisi –İNÜHFD- Cilt:9 Sayı:2 Yıl 2018
- Akman Solak İnci, **Vergi Mahremiyetini İhlal (Doktora Tezi)**, Ankara 2012
- Allen G. Donald Department of Mathematics, Texas A&M University, **Hierarchy of Knowledge – from Data to Wisdom**, International Journal of Current Research in Multidisciplinary (IJCRM) ISSN: 2456-0979, Vol.2 pg. 15-23
- American Psychological Association. (2015). **APA dictionary of psychology (2nd ed.)**
- American Psychological Association. (2015). **Guidelines for Psychological Practice with Transgender and Gender Nonconforming People. American Psychologist, 70(9)**
- American Psychological Association & National Association of School Psychologists. (2015). **Resolution on gender and sexual orientation diversity in children and adolescents in schools.**

- American Psychological Association. (2012). **Guidelines for Psychological Practice with Lesbian, Gay, and Bisexual Clients. American Psychologist, 67(1)**
- Anayasa Mahkemesi Yayınları, **Anayasa Mahkemesi Kararları Dergisi**, Sayı 52/3 Cilt, Mayıs, 2017
- Anı Nevzat Ali, **Kişisel Verilerin İşlenmesi ve Açık Rıza**, Yüksek Lisans Tezi, İstanbul, 2018
- Archer Norm / Sproule Susan / Yuan Yufei / Guo Ken / Xiang Junlian, **Identity Theft and Fraud Evaluating and Managing Risk**, University of Ottawa Press (2012)
- Artuç Mustafa, **Pratik Türk Ceza Kanunu**, 5. Baskı, Ankara 2019, Adalet Yayınevi
- Artuç Mustafa, **Kişilere Karşı Suçlar**, Adalet Yayınevi, 2. Baskı, Ankara 2018
- Artuk/Gökcen/Yenidünya, **Ceza Hukuku Özel Hükümler**, 15. Baskı, Ekim 2016
- Artuk/Gökcen/Yenidünya, **Ceza Hukuku Genel Hükümler**, 10. Baskı, Ekim 2016
- **Article 2 of Law of 2 August 2002 on the Protection of Persons with regard to the Processing of Personal Data**
- Article 29 Data Protection Working Party, **Working Document on Genetic Data**, Adopted on 17 March 2004
- Article 29 Data Protection Working Party, **Opinion 1/2010 on the concepts of "controller" and "processor"**, February 2010,
- Article 29 Data Protection Working Party, **Opinion 5/2009 on online social networking**, Adopted on 12 June 2009
- Article 29 Data Protection Working Party**, Opinion 4/2007 on the concept of personal data**

- Article 29 Data Protection Working Party, **Guidelines on Personal data breach notification under Regulation 2016/679**, 6 February 2018
- Avcı Yasemin, **Kişisel Verilerin Korunması** (Yüksek Lisans Tezi- Konya 2019)
- Aydin Murat, **AGO Uygulaması İçin Temel Hukuk Bilgisi Kitabı**
- Aydın Sedat Erdem, **AİHM İçtihatları Bağlamında Kişisel Verilerin Kaydedilmesi Suçu**, 12 Levha Yayıncılık, Aralık 2015
- Aysun Melike Köse, **Kişisel Verilerin Kaydedilmesi Suçu**, Kasım 2018 Ankara
- Baskarada, Sasa & Koronios, Andy. (2013). **Data, Information, Knowledge, Wisdom (DIKW): A Semiotic Theoretical and Empirical Exploration of the Hierarchy and its Quality Dimension,** Australasian Journal of Information System
- Başbakanlık Kanunlar ve Kararlar Genel Müdürlüğü, **Kişisel Verilerin Korunması Kanunu Tasarısı** (2008) 1-576, 22.4.2008
- Belge Ayşe Merve, **Özellikle Kişisel Verilerin Korunması Kanunu Çerçevesinde İşçilerin Kişisel Verilerinin İhlâli Ve Korunması Yolları**, D.E.Ü. Hukuk Fakültesi Dergisi, Prof. Dr. Şeref ERTAŞ'a Armağan, C. 19, Özel Sayı-2017
- Bernstein, Jay H., **"The Data-Information-Knowledge-Wisdom Hierarchy and its Antithesis"** (2009). City University of New York (CUNY) Academic Works
- Bozkurt Habip, **Kişisel Verilerin İşlenmesinin Hukuki Boyutu**, Yüksek Lisans Tezi İstanbul, Mayıs, 2019
- Bös Mathias , **International Encyclopedia of the Social & Behavioral Sciences** (Second Edition) 2015, Pages 136-141

- Bradley Anna Spain, **Human Rights Racism**, Harvard Human Rights Journal / Vol. 32, 2019
- Buitelaar J. C. , **Post-mortem privacy and informational self-determination**, Tillburg University Ethics and Information Technology 2017
- Bulut Metin, **Özel Bir Hukuksal Koruma ve Veri Kategorisi Alanı: Hassas Kişisel Veriler**, 2020/3 Ankara Barosu Dergisi, Hakemli Makale
- Burk, Dan L., **Privacy and Property in the Global Datasphere** (April 28, 2005). Minnesota Legal Studies Research Paper No. 05-17
- Bük Alaattin, **Bilişim Alanında Kişisel Verilerin Korunması**, Seçkin Yayınları, Ankara 2018
- **Büyük Larousse Sözlük ve Ansiklopedisi**, 23. Cilt
- Canada Supreme Court, R. V.S.A.B, 2003 SCC 60
- Centel Nur, Zafer Hamide, Çakmut Özlem, **Türk Ceza Hukukuna Giriş**, Üçüncü Bası, Beta Yayınları
- Cinsel Eğitim Tedavi ve Araştırma Derneği (CETAD), **Bilgilendirme Dosyası – 1 Cinsel Yaşam ve Sorunları**
- **Commission Staff Working Paper Executive Summary Of The Impact Assessment**, Brussels, 25.1.2012 SEC(2012) 73 final
- Communication From The Commission To The European Parliament, The Council, The Economic And Social Committee And The Committee Of The Regions, **A comprehensive approach on personal data protection in the European Union**, Brussels, 4.11.2010 COM (2010) 609 final

- Conway Heather, Grattan Sheena, **The 'New' New Property: Dealing with Digital Assets on Death**
- Çağlar Ermağan Eda - Türk Tuğba, **İstismara Maruz Kalan Çocuklarla Adli Görüşme: NICHD Protokolü Önerisi**, TAAD, Yıl: 11, Sayı: 38 (Nisan 2019)
- Çakır Kerim, Kişisel Verilerin Kaydedilmesi Suçu, Antalya Bilim Üniversitesi Hukuk Fakültesi Dergisi, Cilt 8, Sayı:16, Aralık 2020
- Çekin Mesut Serdar, **Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku**, On İki Levha Yayınları, 3. Baskı, İstanbul 2020
- Çelik Nuri / Caniklioğlu Nurşen / Canbolat Talat, **İş Hukuku Dersleri**, Beta Yayınları, Ekim 2017
- Çelik Yeşim, **Özel Hayatın Gizliliğinin Yansıması Olarak Kişisel Verilerin Korunması ve Bu Bağlamda Unutulma Hakkı**, TAAD, Yıl:8, Sayı:32 (Ekim 2017)
- Çokmutlu Metin, **Türk Ceza Hukukunda Kişisel Verilerin Korunması**, Doktora Tezi, Kocaeli 2014
- **Danıştay Dergisi** Yıl: 2014 Sayı: 135, s.29-33
- **Danish Data Potection Act**
- **Data Protection Act 2018, Schedule 1 para. 22; Guidance on political campaigning, Draft framework code for consultation**, Information Commissioner's Office (ICO)
- **Definition And Dimensions Of Ethnicity: A Theoretical Framework In Challenges of Measuring an Ethnic World: Science, politics and reality:** Proceedings of the

Joint Canada-United States Conference on the Measurement of Ethnicity April 1-3, 1992, pages 407-27

- Demirbaş Timur, **Ceza Hukuku Genel Hükümler**, Seçkin Yayınları, 14. Baskı, Ankara 2019
- Determann Lothar, **Kişisel Verilerin Korunması Uygulama Kılavuzu**, 1. Baskı, İstanbul, Ocak- 2020, s.24
- Develioğlu Hüseyin Murat, **6698 Sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku**
- **Direcıve 2002/58/EC Of The European Parliament And Of The Council Of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector**
- Dorrothy J. Glancy, **Personal Information as Intellectual Property**
- Dönmezer Sulhi / Erman Sahir, **Nazari ve Tatbiki Ceza Hukuku**, Umumi Kısım, Cilt 2, İstanbul 1969
- Dönmezer Sulhi / Erman Sahir, **Nazari ve Tatbiki Ceza Hukuku**, Genel Kısım, Cilt 1, İstanbul 1973
- Dural Mustafa / Öğüz Tufan, **Türk Özel Hukuku** Cilt 2, Kişiler Hukuku, Ekim 2015, Filiz Kitabevi
- Dülger Murat Volkan, **Kişisel Verilerin Korunması Hukuku, Hukuk Akademisi**, 3. Baskı, İstanbul 2020

- Dülger Murat Volkan, **Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması**, İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi 3 (2), Güz 2016
- Dülger Volkan, **Bilişim Suçları ve İnternet İletişim Hukuku, Seçkin Yayınevi**, Ankara, 2014, 4. Bası
- EDPB, **Guidelines 3/2019 on processing of personal data through video devices** Version 2.0Adopted on 29 January 2020
- Edwards Lilian and Harbinja Edina, **Protecting Post-Mortem Privacy: Reconsiderıng The Privacy İnterests of the Deceased in a Digital World**
- Erbaş Gökhan, **6698 sayılı Kişisel Verilerin Korunması Kanunu Kapsamında İşçinin Elektronik Ortamda Gözetlenmesi**, Hacettepe HFD, 7(1) 2017, 97-108
- Erdinç, G. H., **Ölçülülük İlkesi ve Açık Rıza Kapsamında Biyometrik Verilerin İşlenmesi** Kişisel Verileri Koruma Dergisi, Cilt: 2, Sayı: 1, s.14 (2020).
- Erem Faruk / Toroslu Nevzat, **Türk Ceza Hukuku Özel Hükümler**, Ankara 1973
- European Commission, **European network of legal experts in gender equality and non-discrimination, The meaning of racial or ethnic origin in EU law: between stereotypes and identities**
- European Parliament, **Draft GDPR Adopted by European Parliament**, Article 12, Wednesday, 12 March 2014 – Strasbourg
- European Union Agency for Fundamental Rights, **EU LGBT survey European Union lesbian, gay, bisexual and transgender survey Results at a glance**,2013

- European Data Protection Board, **Guidelines 8/2020 on the targeting of social media users** Version 1.0 Adopted on 2 September 2020,
- European Data Protection Supervisor, **Annual Report 2017**
- European Court of Justice, **Guide on Article 9 of the European Convention on Human Rights**, Updated on 31 August 2020
- European Court of Human Rights, **Guide on Article 8 of the European Convention on Human Rights**, August 2020
- **Factsheet Intersex**, United Nations Human Rights
- Federal Trade Commission, **Identity Theft What To Know What To Do**
- Fierro Paolino, **The General Data Protection Regulation (GDPR): From static to dynamic compliance**, Law and Economics Yearly Review, Volume 6 – Part 2 – 2017
- Fricke Martin, **The Knowledge Pyramid: A Critique of the DIKW Hierarchy** 2008, University of Arizona
- **Gazetta Ufficiale**, 4 Settembre 2018, Anno 159° - Numero 205
- Gerçeker Hasan, **Yorumlu Uygulamalı Türk Ceza Kanunu**, Cilt 1, 5. Baskı, Seçkin Yayınları, Ankara 2020
- Gu, Ji-Fa. (2013). **Data, Information, Knowledge, Wisdom and Meta-Synthesis of Wisdom-Comment on Wisdom Global and Wisdom Cities**, Procedia Computer Science
- Gülener Serdar, **Dijital Hafızadan Silinmeyi İstemek: Temel Bir İnsan Hakkı Olarak "Unutulma Hakkı"**, TBB Dergisi 2012 (102)

- Gültaş Veysel, **Özel Hayata Karşı Suçlar**, Bilge Yayınevi, Ankara 2016
- Gürpınar Damla, **Kişisel Verilerin Korunamamasından Doğan Hukuki Sorumluluk**, D.E.Ü. Hukuk Fakültesi Dergisi, Prof. Dr. Şeref ERTAŞ'a Armağan, C. 19, Özel Sayı-2017
- Hafızoğulları Zeki, Güngör Devrim, **Türk Ceza Hukukunda Suçların Tasnifi** (Hakemli Makale), TBB Dergisi, 2007 Sayı 69
- Hafızoğulları Zeki / Özen Muharrem, **Türk Ceza Hukuku Genel Hükümler**, 12. Baskı, Ankara Ekim 2019
- Hafızoğulları Zeki, Özen Muharrem, **Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar,** Ankara Barosu Dergisi, Yıl:67, Sayı: 4, Güz 2009
- Hakeri Hakan, **Ceza Hukuku Genel Hükümler**, Adalet Yayınevi, Ankara 2013
- Halıcıoğlu Mesut, **Türk Hukukunda Veri Sorumlusu Kavramı**, Yüksek Lisans Tezi Ankara 2019
- Henkoğlu Türkay, **Hassas Bilgi Varlıklarının Ve Kişisel Verilerin Hukuksal Düzenlemeler ile Korunması ve Bu Kapsamda Üniversiteler İçin Bilgi Güvenliği Politikasının Geliştirilmesi**, Doktora Tezi, Ankara, 2015
- Henkoğlu Halise Şerefoğlu, **Unutulma Hakkı: Dijitalleşme Sürecinde Bilgiye ErişimÖzgürlüğünü Tehdit Eder mi?**, Bilgi Sistemleri Ve Bilişim Yönetimi Beklentiler ve Yeni Yaklaşımlar
- Hoofnagle, C. J., van der Sloot, B., & Zuiderveen Borgesius, F. (2019). **The European Union General Data Protection Regulation: What It Is And What It Means**.

Information & Communications Technology Law, 28(1), 65-98, University of Amsterdam

- **House Of Lords Opınıons Of The Lords Of Appeal For Judgment In The Cause Campbell (Appellant) v. MGN Limited (Respondents)** [2004] UKHL
- **In Re Northwest Airlines Privacy Litigation**, United States District Court D.Minnesota, 6 June 2004, 2004 WL 1278459
- İçel/ Özgenç/ Sözüer/ Mahmutoğlu/ Ünver, **Suç Teorisi**, İstanbul 1999
- İçel Kayıhan, **Ceza Hukuku Genel Hükümler**, 2018 Beta Yayınları
- İleri Çiğdem, **Dijital Miras - Alman Federal Mahkemesi'nin "Facebook" Kararı Üzerine Bir İnceleme**, TBB Dergisi 2020 (146),
- İmançlı Canan, **Kişisel Sağlık Verilerinin Korunamamasından Doğan Özel Hukuk Sorumluluğu**, Yüksek Lisans Tezi, İstanbul -2019
- İtişgen Rezzan, **Türk Ceza Hukukunda Kişisel Verileri Hukuka Aykırı Olarak Verme Veya Ele Geçirme Suçu**, TAAD, Yıl:6, Sayı:23 (Ekim 2015)
- İzgi M. Cumhur, **Mahremiyet Kavramı Bağlamında Kişisel Sağlık Verileri**, Türkiye Biyoetik Dergisi, 2014 Vol. 1, No. 1
- Jennex, Murray. (2017). **Big Data, the Internet of Things, and the Revised Knowledge Pyramid.** ACM SIGMIS Database: the DATABASE for Advances in Information Systems
- Jonathan Hey, December 2004, **The Data, Information, Knowledge, Wisdom Chain:The Metaphorical link**

- Junior Diego , Santos Silva , Palomares Nathalia , Normando David , Cardoso Cátia, Quintão Abdo, **Race versus ethnicity: Differing for better application**, Dental Press J. Orthod. vol.15 no.3 Maringá jun. 2010
- Kaplan Bonnie, **How Should Health Data Be Used? Privacy, Secondary Use And Big Data Sales**, Yale Isps-Bioethics Working Paper, October 2014
- Karaarslan Enis / Ergin Ali Murat / Turğut Nalin / Kılıç Özgür, **Elektronik Sağlık Kayıtlarının Gizlilik ve Mahremiyeti**, Conference Paper, December 2015
- Karagülmez Ali, **Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri**, Seçkin Yayınları, Ankara 2009
- Kaya, Mehmet Bedii, Unutulma Hakkı: AİHM'in Unutulma Hakkına Yaklaşımı
- Kaya Kübra, **Özel Hayatın Gizliliği Hakkı ile Kişisel Verilerin Korunması Hakkı Bağlamında Ortaya Çıkan Bir Hak Olarak Unutulma Hakkının Değerlendirilmesi**, TİHEK Akademi Dergisi, Yıl:5 Sayı:8 -2022
- Keyman Selahattin, **Cürmi Fiilin Yapısal Unsuru Olarak Hareket**, AHFD XL 1-4(1988)
- Kılınç Doğan, **Anayasal Bir Hak Olarak Kişisel Verilerin Korunması**, AÜHFD, 61 (3) 2012:1089-1169
- Kişisel Verileri Koruma Kurumu, **6698 sayılı Kişisel Verilerin Korunması Kanununun Uygulanmasına Yönelik Soru Cevaplar**
- Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi**, Aralık 2019, Ankara

- Kişisel Verileri Koruma Kurumu, **Unutulma Hakkı (Unutulma Hakkının Arama Motorları Özelinde Değerlendirilmesi**
- Kişisel Verileri Koruma Kurumu, **Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)**, KVKK Yayınları, Ocak 2018, Ankara
- Kişisel Verileri Koruma Kurumu, **6698 Sayılı Kanun'da Yer Alan Temel Kavramlar**
- Kişisel Verileri Koruma Kurumu, **Anayasal Bir Hak Olarak Kişisel Verilerin Korunmasını İsteme Hakkı**, s.4-6
- Kişisel Verileri Koruma Kurumu, **Veri Sorumluları Sicili**
- Kişisel Verileri Koruma Kurumu, **Kanun Kapsamındaki Hak ve Yükümlülükler**
- Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin Korunması Kanununa Duyulan İhtiyaç**
- Kişisel Verileri Koruma Kurumu, **6698 Sayılı Kişisel Verilerin Korunması Kanun'unun Amacı Ve Kapsamı**
- Kişisel Verileri Koruma Kurumu, **Açık Rıza**
- Kişisel Verileri Koruma Kurumu, **Veri Sorumlusu ve Veri İşleyen**
- Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin Korunması Kanunu Hakkında Sıkça Sorulan Sorular**, KVKK Yayınları, Mart 2018, Ankara
- Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler**
- Koca Mahmut / Üzülmez İlhan, **Kişisel Verilerin Kaydedilmesi Suçu** (Hakemli Makale), D.E.Ü. Hukuk Fakültesi Dergisi, Prof. Dr. Durmuş TEZCAN'a Armağan, C.21, Özel S., 2019

- Koca Mahmut / Üzülmez İlhan, **Türk Ceza Hukuku Genel Hükümler**, Seçkin Yayıncılık, . Eylül 2017 Ankara
- Korkmaz İbrahim, **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, Doktora Tezi, Ankara 2017
- Korkmaz İbrahim, **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, Seçkin Yayınları, Nisan 2017
- Korkmaz İbrahim, **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, Seçkin Yayınları, 2019-Ankara
- Kristof Kathy, **Identity Theft Has Never Been More Rampant** (www.cbsnews.com)
- Kuner Christopher, **The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law**, Copyrıght 2012 By The Bureau Of National Affairs, Inc. Pvlr Issn 1538-3423
- Kuner Christopher, **The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law, Privacy and Security Law Report,** Bloomberg BNA
- Kuşkonmaz Elif Mendos, **Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması**, Yüksek Lisans Tezi, İstanbul 2013
- Küçük Tevfik Sönmez, **Bir Anayasal Hak Olarak Unutulma Hakkı**, Avrupa Ve Türk Hukukunda Kişisel Verilerin Korunmasına İlişkin Güncel Sorunlar Uluslararası Sempozyum (Bildiri Özetleri)
- Küzeci Elif, **Kişisel Verilerin Korunması**, 3. Bası, Ankara 2019

- Küzeci Elif, **Türkiye'de Sağlık Verilerinin Korunması: Hukuksal Çerçeve**, Kişisel Sağlık Verileri Ulusal Kongresi, Nisan 2016, İstanbul Türk Tabipleri Birliği Yayınları
- KVKK Yayınları, **6698 Sayılı Kişisel Verilerin Korunması Kanunu Hakkında Doğru Bilinen Yanlışlar**, No: 31 Nisan 2020, Ankara,
- KVKK Yayınları, Kişisel Verilerin Korunması Kanunu ve Getirdikleri, no: 26, s.13
- KVKK Yayınları, **100 Soruda Kişisel Verilerin Korunması Kanunu**, Nisan 2018, Ankara
- Laudon Kenneth C., Laudon Jane P**., Management Information Systems, Managing the Digital Firm**,12 th Edition
- Litman Jessica, **Information Privacy/Information Property**, Stanford Law Review [Vol. 52:1283, s.1287
- Kang Jerry, **Information Privacy in Cyberspace Transactions**, Stanford Law Review [Vol. 50:1193, s.1246-1248
- M. Victor Jacob, **The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy,** The Yale Law Journal, 123:513 2013
- Malgieri Gianclaudio, **R.I.P.: Rest in Privacy or Rest in (Quasi-)Property? Personal data protection of deceased data subjects between theoretical scenarios and national solutions**
- Malgieri, Gianclaudio, **Property and (Intellectual) Ownership of Consumers' Information: A New Taxonomy for Personal Data** (April 20, 2016). Privacy in Germany - PinG, n. 4, 2016, 133 ff

- Malgieri, Gianclaudio, **Property and (Intellectual) Ownership of Consumers' Information: A New Taxonomy for Personal Data** (April 20, 2016). Privacy in Germany - PinG, n. 4, 2016, 133 ff
- Manav Eda, **İş İlişkisinde İşçinin Kişisel Verilerinin Korunması**, Gazi Üniversitesi Hukuk Fakültesi Dergisi C. XIX, Y. 2015, Sayı: 2
- Moore Adam D. **Intellectual Property and Information Control: Philosophic Foundations and Contemporary Issues**, April 2004
- Moore Adam D. **Privacy, Intellectual Property, and Hacking: Evaluating Free Access Arguments**
- Nakar Sharon & Greenbaum Dov, **Now You See Me. Now You Still Do: Facial Recognition Technology And The Growing Lack Of Privacy**, Boston University Journal Of Science & Technology Law
- Nalbantoğlu Seray, **Bir Temel Hak Olarak Unutulma hakkı**, TAAD, Yıl:9, Sayı:35 (Temmuz 2018),
- Official Journal of the European Union, **Regulation (EU) 2016/679 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 and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Recital 14**,
- Orhan Gülçin / Ulukol Betül / Canbaz Hayri, **Çocuk İzlem Merkezi Modeli Ve Bu Modelde Gözlenen Sorunlar**, Kriz Dergisi 27 (3)

- Öngün Ayözger Çiğdem, **Kişisel Verilerin Korunması Hukuku**, 2. Baskı, İstanbul-2019
- Özbek Veli Özer / Doğan Koray / Bacaksız Pınar / Tepe İlker, **Türk Ceza Hukuku Genel Hükümler**, Seçkin Yayınları, Eylül 2018-Ankara
- Özbek Veli Özer / Doğan Koray / Bacaksız Pınar, **Türk Ceza Hukuku Özel Hükümler**, 14. Baskı, Ankara 2019, Seçkin Yayıncılık
- Özgenç İzzet, **Türk Ceza Hukuku Genel Hükümler**, Eylül 2019, Seçkin Yayıncılık
- Parlar Ali, **Açıklamalı-Atıflı-Uygulamalı Türk Ceza kanunu El Kitabı**, Bilge Yayınevi, Ankara 2018
- Parlar Ali, **Açıklamalı-Atıflı-Uygulamalı Türk Ceza kanunu El Kitabı**, Bilge Yayınevi, Ankara 2017
- Parlar Ali, **Türk Ceza Kanunu Şerhi**, Cilt 2, Bilge Yayınevi, Ankara 2015
- Parlar Ali / Öztürk Mustafa, **Doğrudan ve Dolaylı Bilişim Suçları ve Bilişim Sistemleri Aracılığıyla İşlenen Suçlar**, Aristo Yayınevi, Mart 2020 İstanbul
- PATTI Francesco Paolo & BARTOLINI Francesca, **Digital Inheritance and Post Mortem Data Protection: The Italian Reform**, European Review of Private Law 5-2019 [1181–1194], 2019 Kluwer Law International BV, The Netherlands
- Pager, Devah, and Hana Shepherd. 2008. **"The Sociology of Discrimination: Racial Discrimination in Employment, Housing, Credit, and Consumer Markets"**. Annual Review of Sociolgy, Harvard University
- Polat Yeliz, **4857 Sayılı İş Kanunu'na Göre İşçi Özlük Dosyası**, Yüksek Lisans Tezi, İstanbul, 2011

- Publications Office of the European Union, **Handbook on European data protection law** 2018 Edition
- Radin Tara J. , **Identity Theft** (www.britannica.com)
- Ratcliffe Peter, University of Warwick, **"Ethnic group"**, Sociopedia.isa 2014
- Rishikeshav Regmi, **Ethnicity And Identity, Occasional Papers in Sociology and Anthropology**, Vol.8 2003 p.1-11
- Robertson, Terry Dwain (2013) **"The Data/Information/Knowledge/Wisdom Hierarchy Goes to Seminary,"** Advances in the Study of Information and Religion: Vol. 3, Article 7
- Sağlık Bakanlığı, **e-nabız Kullanım Kılavuzu**, 2018
- Sarıusta Kader, **Kişisel Verilerin Ceza Hukuku Yoluyla Korunması**, Yüksek Lisans Tezi, Gaziantep Temmuz 2018
- Sami Sinan, **Akkurt Kişisel Veri Kavramının Hukuki Niteliğine İlişkin Yaklaşımlara Mukayeseli Bir Bakış**, Kişisel Verileri Koruma Dergisi, Cilt: 2, Sayı: 1
- Schwartz Paul M., **Property, Privacy, And Personal Data**, Harvard Law Review [Vol. 117:2055,
- Schwartz Paul M., **The EU-U.S. Privacy Collision: A Turn To Institutions And Procedures**, Harvard Law Review [Vol. 126:1966,s.1969]
- Serozan Rona, **Medeni Hukuk Genel Bölüm/Kişiler Hukuku,** 5. Bası, İstanbul 2014
- Sert Şeyma, **Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması**, Seçkin Yayınları, Şubat 2019 Ankara

- Sevimli K. Ahmet, **İşçinin Özel Yaşamına Müdahalenin Sınırları**, Doktora Tezi
- Sevük Handan Yokuş, **Türk Ceza Hukuku, Özel Hükümler**, Adalet Yayınevi, Ankara 2020
- Sınar Hasan, **Kişisel Verileri Hukuka Aykırı Olarak Verme, Yayma veya Ele Geçirme Suçu (TCK Md. 136)**, Kişisel Verileri Koruma Dergisi, Cilt: 2, Sayı: 1
- Smith Anthony D., **Ethnic Origins of Nations**, Blackwell Publishing, 1986
- Solmaz Başak / Tekin Gökhan / Herzem Züleyha / Demir Muhammed, **İnternet ve Sosyal Medya Kullanımı Üzerine Bir Uygulama**, Selçuk Üniversitesi İletişim Fakültesi Akademik Dergisi, Cilt 7, Sayı 4 (2013)
- Solove Daniel J., **Privacy and Power: Computer Databases and Metaphors for Information Privacy**, Stanford Law Review [Vol. 53:1393, s.1446
- Soo Sandra - Lee Jin, Mountain Joanna, Koenig Barbara A., **The Meanings of "Race" in the New Genomics: Implications for Health Disparities Research,** Volume 1 Issue 1 Yale Journal of Health Policy, Law, and Ethics Article 3 2001,
- Soyaslan Doğan, **Ceza Hukuku Özel Hükümler**, 13. Baskı, Ankara 2020
- Şahbaz İbrahim, **Açıklamalı ve İçtihatlı Türk Ceza Kanunu**, 1. Cilt, Ankara 2016
- Şen Ersan, **Türk Ceza Hukuku Suçun Genel Esasları ve Unsurları**, Der Yayınları İstanbul 2002
- Şık Eser, **İşverenin Özlük Dosyası Düzenleme Borcu**, Yüksek Lisans Tezi, İZMİR – 2012

- Taner Fahri Gökçen, **Kırılgan Mağdurun Beyanının CMK'nın 236. maddesi Uyarınca Alınması Ve Uygulanan Özel Usuller Karşısında Savunma Hakkının Dengelenmesi**, TBB Dergisi 2021 (153)
- Taşkın Şaban Cankat, **Bilişim Suçları**, Bursa 2008, Beta Yayınları
- Tekin Nurullah, **Kişisel Verilerin Korunması İle İlgili Türkiye'deki Kanun Tasarısının Avrupa Birliği Veri Koruma Direktifi Işığında Değerlendirilmesi**, Ulusal Hakemli Uyuşmazlık Mahkemesi Dergisi, Aralık 2011, 4. Sayı
- Thaarup Sidsel, **Implementing Post-Mortem Privacy in a Digital Age a thesis on post-mortem data protection**, January 2018, IT University of Copenhagen
- The OECD Privacy Framework, **Chapter 3. Original Explanatory Memorandum To The OECD Privacy Guidelines (1980)**, 2013,
- Toroslu Haluk / Toroslu Nevzat, **Ceza Hukuku Genel Kısım**, Savaş Kitapevi, Ankara 2018
- Tümer Günay, **TDV İslam Ansiklopedisi**, TDV İslâm Araştırmaları Merkezi, 1992
- Türkiye Bankalar Birliği, **Dolandırcılık Eylemleri ve Korunma Yöntemleri**, Aralık 2015
- Türkiye Büyük Millet Meclisi, **5237 sayılı Türk Ceza Kanunu Genel Gerekçesi**, Mayıs 2003
- Türkiye Büyük Millet Meclisi, **6526 sayılı Terörle Mücadele Kanunu Ve Ceza Muhakemesi Kanunu İle Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun'un Teklif Metni**, Yasama Dönemi:24 Yasama Yılı: 4 Sıra Sayısı: 560

- Türkiye Büyük Millet Meclisi, **7188 Sayılı Ceza Muhakemesi Kanunu Ve Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun'un Teklif Metni**, Yasama Dönemi:27 Yasama Yılı: 3
- Türkiye Büyük Millet Meclisi, **7/11/1982 Tarihli ve 2709 Sayılı Türkiye Cumhuriyeti Anayasasının Bazı Maddelerinde Değişiklik Yapılması Hakkında Kanun Teklifi ve Anayasa Komisyonu Raporu (2/656)**
- Türkiye Büyük Millet Meclisi, **Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu**
- Türk Dil Kurumu, **Büyük Türkçe Sözlük**
- Türk Dil Kurumu, **Güncel Türkçe Sözlük**
- Türkmen Sevgi, **Özel Nitelikli Kişisel Verilerin İşlenmesinde Açık Rızanın Aranmadığı Haller**, Yüksek Lisans Tezi, İSTANBUL – 2019
- UN Economic and Social Council, **Commentary on Proposed Amendments**, E/CN.4/Sub.2/1988/22
- UN Economic and Social Council, **Guidelines Concerning Computerized Personal Data Files** E/CN.4/Sub.2/1988/22 21 July 1988
- UNESCO, **The Race Question In Modern Science, The Race Concept Results of an İnquiry**, Paris, 1952
- United Nations, **Chapter 13 The Right To Equality And Non-Discrimination In The Administration Of Justice, Human Rights in the Administration of Justice: A Manual on Human Rights for Judges, Prosecutors and Lawyers**

- U.S. Gov't Accountability Office, **Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace** (2013)
- Uyarer Sinem Göçmen, **Kişisel Verilerin Korunması**, Ağustos 2019, Seçkin Yayıncılık
- Uyarer Sinem Göçmen, **Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması**, Seçkin Yayınları, Ankara 2019
- Ünlütürk, Ö. (2015). **"Irk" Kavramının Tarihsel Gelişimi ve Adli Antropolojide Kullanımı**. Antropoloji, (29), 93-116
- Ünver Yener, **Hukuk Felsefesi ve Sosyolojisi Arkivi**, 8. Kitap, İstanbul Barosu, İstanbul 2003
- Üzüm İlyas, **TDV İslam Ansiklopedisi**, 2004, YDV İslam Araştırmaları Merkezi
- Vuraloğlu Mehmet Oğuz, **Kişisel Verilerin İşlenmesi Suretiyle Kişilik Hakkı İhlâlinde Kazancın Devri Talebi**, YÜHFD Cilt: XV Sayı:1 (2018)
- **We Are Social and Hootsuite Report**, Digital In 2018
- Weisbaum Herb, **More Than 1 Million Children Were Victims Of ID Theft Last Year** (www.nbcnews.com)
- Welinder Yanna, Harvard Journal of Law & Technology Volume 26, Number 1 Fall 2012, **A Face Tells More Than A Thousand Posts: Developing Face Recognition Privacy In Social Networks**
- World Medical Association, **Declaration Of Taipei On Ethical Considerations Regarding Health Databases And Biobanks**, October2002

- Yaşar Osman, Gökcan Hasan Tahsin, Artuç Mustafa, **Yorumlu – Uygulamalı Türk Ceza Kanunu**, Ankara 2010
- Yıldırım/Yasin/Kaman/Özdemir/Üstün/Okay Tekinsoy, **İdare Hukuku**, Ekim 2016
- Yılmaz Sabire Sanem, **Tıp Alanında Kişisel Verilerin Açıklanması Suçu**, Nisan 2019 Ankara
- Zins Chaim, **Conceptual Approaches for Defining Data, Information, and Knowledge, Journal of the American Society for Information Science and Technology**, 58(4):479–493, 2007
- Zorer Umut, **COVID-19 Pandemisinde Temas Takip Uygulamaları Ve Gözetim Toplumu**, Covıd-19 Pandemisinde Dijital Dönüşüm ve Hukuk, İstanbul Barosu – 2021
- https://www.merriam-webster.com/dictionary/datum
- https://dictionary.cambridge.org/dictionary/english/datum
- https://www.kvkk.gov.tr/Icerik/2034/Ilgili-Kisi-Kimdir
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/do-data-protection-rules-apply-data-about company_en
- https://www.hukukihaber.net/kisisel-verilerin-korunmasi-kurulunun-02042020-tarihinde-yayimlanan-2019138-206-273-297-333-ve-202034-41-43-58-65-67-sayili-kararlarina-iliskin-degerlendirme-makale,7651.html
- https://www.siviltoplum.gov.tr/siyasi-partilere-iliskin-istatistikler
- https://cdn.vgm.gov.tr/genelicerik/genelicerik_945_290519/06-yil-icinde-kurulan-yeni-vakif-sayilari-2001-050.pdf

- https://www.siviltoplum.gov.tr/dernek-sayilari
- https://www.siviltoplum.gov.tr/sendikalara-iliskin-istatistikler
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-constitutes-data-processing_en
- https://www.cbsnews.com/news/social-media-is-a-tool-of-the-cia-seriously/
- https://www.kvkk.gov.tr/Icerik/6723/Uzaktan-Egitim-Platformlari-Hakkinda-Kamuoyu-Duyurusu
- https://www.dw.com/tr/%C3%A7in-vatanda%C5%9Fa-not-sistemine-ge%C3%A7iyor/av-43809155
- https://www.kvkk.gov.tr/Icerik/6856/WHATSAPP-UYGULAMASI-HAKKINDA-KAMUOYU-DUYURUSU
- https://www.bbc.com/news/technology-43649018
- https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en