İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi 3 (2), Güz 2016; 101-167

Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması*

Protection of Personal Data with Criminal Norms in the context of Protection of Personal Data Law and Turkish Criminal Code

Murat Volkan Dülger**

ABSTRACT

Protection of personal data, which can be defined as all kind of information relating to an identified or identifiable real person, is important in respect of the right to privacy and the right to respect for family life. The issue of protecting personal data is becoming more and more important nowadays; both individuals have many complaints arising from this subject in daily life and high level judicial organs take a legal attitude in this manner. In this direction, the field of the protection of personal data has been regulated by many supra-national organizations especially the Council of Europe and the European Union and states. Turkey has accepted the Law numbered 6698 on the Protection of Personal Data which regulates this area, albeit too late. Protection of personal data by criminal norms is provided by special provisions in the Turkish Criminal Code. The types of crime that should be addressed in this context are: The offense of Recording Personal Data, the offense of Illegal Delivery or Acqusition Of Personal Data and the offense of Non-Destruction of Data held in articles 135-138 of Turkish Criminal Code and the offense of Non-Destruction or Non-Anonymization of Personal Data held in article 17/2 of the Law numbered 6698.

Keywords: Personal data, right to privacy, data protection, crime against privacy, data processing, data subject.

Giriş

Kişisel veri, tartışmalı ve sınırları tam olarak çizilemeyen bir kavramdır; ancak yine de kısaca insana ait, bireyi tanımlayabilecek her türlü bilgi olarak tanımlanması mümkündür. Aslında insanın, insan olarak evrendeki yerini alması ve

* Makale gönderim tarihi: 30.11.2016. Makale kabul tarihi: 15.12.2016.

** Doç. Dr., İstanbul Medipol Üniversitesi Hukuk Fakültesi Ceza Hukuku, Ceza Muhakemesi Hukuku ve Bilişim Hukuku öğretim üyesi. İletişim: İstanbul Medipol Üniversitesi Hukuk Fakültesi - Kavacık Mah. Ekinciler Cad. No.19 Kavacık Kavşağı – Beykoz.

toplumdaki konumu, insana bağlı bazı değerleri kişisel veri haline getirir, örneğin kişinin adı, adresi, hastalıkları, medeni durumu, cinsel tercihleri hep kişisel veri olarak kabul edilen bilgilerdir. Ancak özellikle geçtiğimiz yüzyılda bilim ve teknolojideki gelişmeler ve bunun topluma ve toplumsal hayatı oluşturan bileşenlere yansıması daha pek çok bilgiyi kişisel veri haline getirmiştir. Bu bağlamda banka hesap numarası, sosyal güvenlik numarası, vatandaşlık numarası ve elektronik posta adresinin şifresi bunlara örnek olarak gösterilebilir. Buna göre kabaca kişisel verilerin ikiye ayrılması mümkündür, birinci grupta insanın varoluşundan kaynaklanan kişiliğine ilişkin bilgiler yer almakta, ikinci grupta ise insanın modern bilişim toplumunda yer alması nedeniyle kendisine verilen ya da çeşitli hizmetlere ulaşmasında kullanılan bilgiler yer almaktadır. Ancak bu ayrım kişisel verilerin değeri ve korunmaya hak kazanımları açısından bir fark yaratmaz[1].

I. Kişisel Veri Kavramının Ortaya Çıkışı ve Tek Başına Bir Hak Olup Olmadığı Tartışması

A. Kişisel Verilerin Ortaya Çıkış Süreci

Kişisel veriler, yukarıda belirtildiği üzere ilk insanlardan bu yana var ola gelmiştir. Ancak bilişim teknolojilerinin gelişmesi ve internetin yaygınlaşmasıyla kişisel verilerin varlığı ve önemi ortaya çıkan sorunlar nedeniyle daha iyi anlaşılmıştır. Zira daha önce az sayıdaki kişi ya da kurumun elinde yazılı halde dosyalanmış olan bu bilgiler bilgi teknolojilerinin gelişmesi ile sayısal ortama aktarılmış, internetin yaygınlaşması sonucunda da hukuka uygun ya da aykırı olarak ilgili ilgisiz herkesin erişimine açılmıştır[2]. Bunun yanı sıra çok büyük sayılardaki kişisel verilerin çok küçük alanlarda ve aygıtlarda depolanabilmesi, bilgisayarların işlemci hızlarının katlanarak artması sonucu, bu büyük miktardaki verilerin çok kısa bir zamanda ve kapsamlı olarak işlenebilmesi, bilgi kırıntılarından yola çıkılarak, bireylerin belirlenmesine ve sonrasında ilgili bireyle ilgili her türlü bilgiye erişilmesine yol açmıştır.

Kişisel veriler ile ilgili tehlikenin ortaya çıkış noktası da bu olmuştur. Zira ilgisiz kişilerin, kişisel verilere erişebileceği ve bunları kullanabileceği/yayabileceği endişesi dahi kişiler üzerinde gerçek bir tehdit oluşturur. Ayrıca bu verilerle sanal alanda verilerin gerçek sahibiymiş gibi profiller (sanal kişiler) oluşturulması ve bu profiller aracığıyla çeşitli hukuka aykırı eylemler gerçekleştirilmesi ve/veya suç işlenmesi de mümkündür ve bunların örnekleri sıklıkla görülmektedir. Bu durumda olayla hiçbir ilgisi olmayan gerçek veri sahibi bir anda suçun ve/veya

1 Murat Volkan Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, 6. Bası, Seçkin Yayıncılık, Ankara, 2015, s. 631, 632.

2 Dülger, *Bilişim Suçları*, s. 632.

hukuka aykırı eylemin faili olarak kendisini mahkeme karşısında sanık ve/veya davalı olarak bulabilmektedir. Bu durum bize kişisel verilerin korumasız bırakılmasının ne kadar ciddi sonuçlar doğurduğunu açık bir biçimde gösterir[3].

Kişisel verilerin korunmasının önemi, insan hakları ve bunların korunması bilincinin son elli yıl içinde gittikçe gelişmesine paralel olarak artmıştır. Bu bağlamda kişisel verilerin korunması hukuku da çeşitli dönemlere ayrılarak incelenir[4]. Ancak bu dönemlere ilişkin hangi ayrım benimsenirse benimsensin, kişisel verilerin korunmasının başlangıcı olarak tek bir dönem gösterilir. Buna göre bugün anlaşılan şekliyle kişisel verilerin korunmasın yönelik düzenlemeler ilk olarak bilişim teknolojilerinin gelişmesi ve yaygınlaşmasıyla birlikte 1960'lı yıllarda tartışılmaya, 1970'li yıllarda ise hukuksal düzenlemelerin konusunu oluşturmaya başlamıştır[5].

B. Kişisel Veri Kavramının Tek Başına Bir Hak Olup Olmadığı Tartışması

Kişisel verilerin korunması, insan haklarından olan özel hayat ve aile hayatına saygı hakkı bakımından önem arz eder. Özel hayata ve aile hayatına saygı hakkı, gerek Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesinde herkesin özel hayata ve aile hayatına saygı gösterilmesini isteme hakkına sahip olduğu belirtilerek, gerekse Anayasanın 20. maddesinde kişinin temel haklarından sayılarak güvence altına alınmıştır[6]. Dolayısıyla kişisel verilerin korunması hem ulusal üstü hukuk açısından bir insan hakkı, hem de ulusal hukuk açısından Anayasa normu ile düzenlenmiş bir temel hak ve özgürlüktür[7].

Öğretide kişisel verilerin, özel hayatın gizliliğinin korunmasının bir alt başlığı mı yoksa kendi başına bağımsız bir kavram mı olduğu konusunda iki farklı görüş bulunur. Bunlardan ilkinde, bir gerçek kişinin *"kendine özel olan ve gizli kalmasını isteyeceği hayat olaylarını"* koruyan özel hayatın gizliliği hakkının tanımı ve kişinin üçüncü kişilerin gözetimi ile denetimden uzak, insan onuruna uygun olarak yaşayabilmesini öngören amacı dikkate alındığında kişisel verilerin korunması kavramının, özel hayatın gizliliğinin korunmasının bir alt başlığı olduğunun kabul edilmesi gerektiği ifade edilir[8].

---

3 Dülger, s. *Bilişim Suçları*, 632.

4 Bu dönemler hakkında ayrıntılı açıklama için bkz: Elif Küzeci, *Kişisel Verilerin Korunması*, Turhan Kitapevi, Ankara, 2010, s. 106 – 116.

5 Küzeci, s. 106; Dülger, Bilişim Suçları, s. 632.

6 Handan Yokuş Sevük, "Tıp Ceza Hukukunda Kişisel Verilerin Açıklanması", *Tıp Ceza Hukukunun Güncel Sorunları*, Türkiye Barolar Birliği Yayını, Ankara, 2008, s. 782.

7 Dülger, *Bilişim Suçları*, 633. Kişisel verilerin korunmasının bir hak olarak tanımı ve niteliği hakkında ayrıntılı açıklamalar için bkz: Küzeci, s. 60 – 103.

8 Güçlü Akyürek, "Kişisel Veriler ve Özel Hayatın Gizliliği Hakkı", *Suç ve Ceza – Ceza Hukuku Dergisi*, Türk Ceza Hukuku Derneği yayını, S.3, Temmuz – Ağustos – Eylül 2011, s. 44.

İkinci görüşte ise, kişisel verilerin korunması hakkının ilk aşamada özel yaşamın gizliliği hakkı içinde değerlendirilebileceği, ancak gelişen teknoloji karşısında özel yaşamın gizliliği hakkına geleneksel yaklaşımla ve bu alanda benimsenen ilkelerle kişisel verilerin korunmasının yetersiz kaldığı, bu nedenle tarihsel süreç içersinde kendisinden daha köklü bir hak alanı olan özel yaşamın gizliliği hakkından ayrılmaya başladığı; bu anlamda kişisel verilerin korunmasının özel yaşamın gizliliği hakkının özellik taşıyan bir türü olduğu ve kendine özgü bazı gereklilikleri nedeniyle ayrı bir alan olarak algılanmaya başladığı, ancak bunların birbiriyle organik ilişkisi bulunan alanlar olduğu ifade edilir[9].

Ben bunlardan ikincisine katılmaktayım çünkü her ne kadar kişisel veriler özel hayatın gizliliği kavramının içinden çıkmış olsa da zamanla hem teknolojideki gelişmeler hem de bu verilerin sıklıkla hak ihlaline konu olması bu kavramın ayrı bir kimliğe kavuşmasına yol açmıştır. Ayrıca *"özel hayatın gizliliği"* kavramındaki *"gizlilik"* sözcüğü, kişisel verilerin korunmasıyla tam olarak örtüşmez. Zira korumaya alınan kişisel verilerin mutlaka gizli olması gerekmez, kişinin özel hayatına dahil olan ve bu alanda yer alan kişiler tarafından bilinen ancak gizli ya da sır olmayan bir bilginin, üçüncü kişilerle paylaşılması halinde bu bilgi, kişisel verilerin korunmasının kapsama alanından faydalanır; ancak bu gizliliğin korunması değildir, kendine özgü bir olgu olan kişisel verilerin korunmasıdır. Benzer şekilde kişisel verilerin korunmasına ilişkin suçlarda da korunan hukuksal değer "sır" olmayıp, verinin ilgilisi olan kişinin kişilik haklarıdır[10].

Kişisel veri; ceza hukuku, medeni hukuk, idare hukuku, ticaret hukuku, borçlar hukuku vb. gibi hemen tüm hukuk dallarının ilgi alanına giren çok geniş bir kavramdır. Ancak ilgi alanımızı oluşturan ceza hukuku disiplini açısından temel aldığımız hususun "suç" olgusu olması nedeniyle, bu çalışmada kişisel veri kavramını suça konu olmasıyla sınırlayarak inceleyeceğim. Bunun yanı sıra yakından ilgili olması nedeniyle yeri geldikçe özellikle 6698 sayılı Kişisel Verilerin Korunması Kanunu'nda yer alan idare hukukuna ilişkin düzenlemelere ve kabahatlere de (idari düzene aykırılıklar) değineceğim[11].

Burada karşımıza çıkan ilk soru *"kişisel veriyle korunması gereken bir hukuksal değerin olup olmadığıdır"*. Bunun cevabı ise yukarıda iki paragrafta açıkça yer görülür: Kişisel verilerin öneminin bu denli algılanmaya başlandığı ilk andan itibaren ceza hukukunun ve idare hukukunun (idari ceza hukukunun) koruma alanından yararlanması gerektiği konusunda bir şüphe bulunmaz. Buna göre öncelikli olarak suç tipiyle korumaya çalışılan kişisel verilerin ne olduğu,

9 Küzeci, s. 70.

10 Dülger, *Bilişim Suçları*, s. 633, 634.

11 Dülger, *Bilişim Suçları*, s. 634.

sınırlarının nerede başlayıp nerede bittiği ve bu kavramın kime ve neye göre tanımlanıp içeriğinin doldurulduğunun belirlenmesi gerekir. Bu yapıldıktan sonra ceza ve idare hukukuna ilişkin açıklamalara yer verilmesi daha anlamlı ve anlaşılır olacaktır[12].

II. Kişisel Veri ve Kişisel Verinin İşlenmesi Kavramlarının Tanımı

A. Kişisel Veri

Kişisel veri kavramı, İngilizce *"personal data"* kavramından gelmekte olup, yabancı dildeki kavramın içeriğini ve anlamını tam olarak karşılar. Bu alanda özellikle ülkemizin konuya ilişkin düzenlemelerinde ve mevzuat çalışmalarında dikkate alınan temel uluslararası düzenlemeler mevcuttur.

Bunlardan ilki ülkemizin de üyesi olduğu Avrupa Konseyi'nin üretimi olan 28.1.1981 tarihli ve 108 nolu *"Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme"*dir. Söz konusu sözleşme bu alandaki ilk uluslararası düzenleme olup, bu alanda yeknesak kurallar üretilmesinde temeli oluşturmuştur[13]. Sözleşmenin 2. maddesinde kişisel veri, *"kişiyi tanımlayan ya da tanımlayabilen her türlü bilgi"* olarak tanımlanmıştır.

Bu alandaki temel metinlerden ikincisi ise Avrupa Birliği üretimi olan 95/46/EC sayılı *"Avrupa Topluluğu Veri Koruma Direktifi'dir"*[14]. Bu direktifin 2. maddesinde kişisel veri *"doğrudan doğruya ya da dolaylı olarak bir gerçek kişi ile ilintili olabilecek ve onu belirlenebilir kılacak her türlü bilgi"* olarak tanımlanır[15]. Bu tanımın benzerleri çok sayıda ülke tarafından kabul edilmiş ve kendi iç hukuklarına aktarılmıştır. Nitekim kişisel veriler için hem uluslararası hem de ulusal öğretide bu tanım kullanılmaktadır. Ancak diğer yandan bu tanımın son derece geniş ve belirsiz olması nedeniyle eleştirilmiştir[16].

---

12 Dülger, *Bilişim Suçları*, s. 634.

13 Söz konusu sözleşme Türkiye tarafından 28.01.1981 tarihinde imzalanmış ve usulüne uygun olarak 30.1.2016 tarihli ve 6669 sayılı Yasa ile onaylanarak (onay yasası 18.2.2016 tarihli ve 29628 sayılı Resmî Gazete'de yayımlanmıştır) Avrupa Konseyi Genel Sekreterliği'ne depo edilmiş ve 1.9.2016 tarihi itibariyle Türkiye açısından yürürlüğe girmiştir. Sözleşmenin özgün metni ve onaylama tablosu için bkz: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM =8&DF=11/08/2011& CL=ENG

14 Avrupa Birliği'nde yeknesak bir hukuk düzenin yaratılmasında temel kaynak Avrupa Topluluğu'nun yürürlüğe koyduğu yönergelerdir. Bu doğrultuda, yeknesak bir veri koruması hukukunun oluşturulması çabaları 90'lı yıllarda ilk kazanımlarını ortaya çıkarmıştır. Veri Koruması Yönergesi'nin ilk taslağı 1990 tarihine dayanmaktadır. Bu taslak veri kroumasının topluluk bazında düzenlenmesinde başlangıç noktasını oluşturmaktadır. Konu hakkında ayrıntılı bilgi için bkz: Nilgün Başalp, *Kişisel Verilerin Korunması ve Saklanması*, Yetkin Yayınları, Ankara, 2004, s. 25 – 32.

15 Başalp, Kişisel Verilerin Korunması ve Saklanması, s. 33.

16 Ian J. Lloyd, *Information Technology Law*, 6th Edition, Oxford University Press, Oxford, 2011, s. 39.

Bu alana özgü üçüncü ve dördüncü temel metinler ise yine Avrupa Birliği tarafından 95/46/EC sayılı direktifin yerini almak üzere çıkarılan 2016 tarihli ve IP/12/46 sayılı direktif ve regülasyon (tüzük) tür. Bu düzenlemelerden Direktifin "Tanımlar" başlıklı 3. maddesinde öncelikle verinin konusu sonrasında kişisel veri şu şekilde tanımlanmaktadır: *"Veri sahibi", doğrudan ya da dolaylı olarak, makul bir şekilde bir kontrolör ya da diğer bir gerçek ya da tüzel kişi tarafından kullanılması muhtemel, kimlik numarası, konum bilgisi, çevrimiçi tanımlayıcı veya kişiye ait bir ya da birden fazla fiziksel, psikolojik, genetik, ruhsal, ekonomik, kültürel ya da sosyal tanımlayıcı işleve ilişkin, belirli ya da belirlenebilir bir gerçek kişidir"*. Aynı düzenlemede kişisel veri ise *"veri sahibine ilişkin herhangi bir veri anlamına gelir"* olarak düzenlenmiştir. Nitekim Regülasyonun da (Tüzük) "Tanımlar" başlıklı dördüncü maddesinde veri sahibi ve kişisel veri kavramları birebir aynı şekilde tanımlanmışlardır[17].

Bir kişinin belirlenebilir kılınması, verilerin doğrudan ya da dolaylı olarak bir gerçek kişiyle ilişkilendirilmesi suretiyle kişinin tanımlanabilmesi, yani şahsın o şahıs olduğunun ortaya çıkarılabilmesi özelliğini ifade eder. Örneğin verilerin bir kimlik numarasıyla ilişkilendirilmesi ya da kişinin psişik, psikolojik, fiziksel, ekonomik, kültürel veya sosyal kimliğini ifade eden, sağlık, genetik, etnik, dini, ailevi ve siyasi bilgilerinin bir ya da birden fazla unsuruna dayanarak tanımlanabilen gerçek ve/veya tüzel kişilere ilişkin herhangi bir bilgi kişisel veriyi gösterir. Başka bir ifade ile isim, telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, ses, parmak izleri, genetik bilgiler gibi özellikli bir içerik taşıyan veriler ile dolaylı olarak kişiyi belirlenebilir kılan ölçütlerin kombinasyonu (yaş, meslek, medeni durum, adres vb.) olan veriler kişisel veri kapsamında ele alınabilir[18]. Nitekim CMK'nın 80. maddesi gereğince bir suça ilişkin delil elde etmek için şüpheli, sanık veya diğer kişilerden alınan örnekler üzerinde yapılan genetik inceleme sonuçları kişisel veri niteliğindedir[19].

Ülkemizde kişisel verilerin korunması konusunda temel bir mevzuat oluşturmak üzere çalışmalar yapılmıştır. Adalet Bakanlığı tarafından oluşturulan bir komisyon tarafından üç yıllık bir çalışmanın sonucunda (önceden uzun yıllardır hazırlanan farklı tasarılar da olmakla birlikte) 2003 yılında *"Kişisel Verilerin Korunması Kanun Tasarısı"* hazırlanmıştır. Söz konusu tasarı genel olarak 108 nolu Avrupa Konseyi Sözleşmesi ve Avrupa Topluluğu Veri Koruma Yönergesi

17 Avrupa Birliği'nin kişisel verilerin korunmasına ilişkin 2016 tarihli Regülasyonunun (Tüzük) ve Direktifinin orijinal ve tam metinleri için bkz: http://ec.europa.eu/justice/data-protection/reform/index_en.htm; 3.11.2016.

18 Başalp, *Kişisel Verilerin Korunması ve Saklanması*, s. 33, 34.

19 Yokuş Sevük, s. 797; Dülger, *Bilişim Suçları*, s. 635.

temel alınarak hazırlanmış[20], ancak bu alandaki yoğun taleplere rağmen çeşitli gerekçelerle 2016 yılına kadar yasalaşamamıştır. Nihayetinde ülkemizin Avrupa Birliği'ne giriş sürecinde yeniden müzakerelere başlaması ve son açılan müzakere başlıklarının kişisel verilerin korunmasını da içermesi nedeniyle, söz konusu tasarıda değişiklikler yapılarak TBMM'ye sunulmuştur. Bu arada yasa yapılmadan önce ilk olarak Avrupa Konseyinin kişisel verilerin korunmasına ilişkin sözleşmenin onay yasası çıkarılmıştır. TBMM'ye sunulan yasa 6689 numarayla 24.3.2016 tarihinde meclis tarafından kabul edilmiş ve 7.4.2016 tarihli ve 29677 sayılı Resmi Gazete'de yayımlanarak, Yasanın 32. maddesi gereğince *"8 inci, 9 uncu, 11 inci, 13 üncü, 14 üncü, 15 inci, 16 ncı, 17 nci ve 18 inci maddeleri yayımı tarihinden altı ay sonra"* diğer maddeleri ise yayımlandığı tarihte yürürlüğe girmiştir.

6698 sayılı Yasanın 3. maddesinin 1. fıkrasının (d) bendinde kişisel veri, *"kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi"* şeklinde tanımlanmıştır. Bu maddenin gerekçesinde söz konusu kavram *"Kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade etmektedir. Bu bağlamda sadece bireyin adı, soyadı, doğum tarihi ve doğum yeri gibi onun kesin teşhisini sağlayan bilgiler değil, aynı zamanda kişinin fiziki, ailevi, ekonomik, sosyal ve sair özelliklerine ilişkin bilgiler de kişisel veridir. Bir kişinin belirli veya belirlenebilir olması, mevcut verilerin herhangi bir şekilde bir gerçek kişiyle ilişkilendirilmesi suretiyle, o kişinin tanımlanabilir hale getirilmesini ifade eder. Yani verilerin; kişinin fiziksel, ekonomik, kültürel, sosyal veya psikolojik kimliğini ifade eden somut bir içerik taşıması veya kimlik, vergi, sigorta numarası gibi herhangi bir kayıtla ilişkilendirilmesi sonucunda kişinin belirlenmesini sağlayan tüm halleri kapsar. İsim, telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler gibi veriler dolaylı da olsa kişiyi belirlenebilir kılabilme özellikleri nedeniyle kişisel verilerdir."* şeklinde açıklanmıştır.

Sağlık Bakanlığı tarafından hazırlanan ve 20.10.2016 tarihli ve 29863 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren *"Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik"* ile de 4. maddenin 1. fıkrasının (g) bendinde kişisel sağlık verisi *"kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü sağlık bilgisi"* olarak tanımlanmıştır. Dayanakları arasında 6698 sayılı Yasayı da gösteren bu yönetmelikte anılan yasaya paralel bir tanım yapılması son derece olağan ve yerindedir.

24.7.2012 tarih ve 28363 sayılı Resmi Gazete'de yayınlanarak yürürlüğe giren *"Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Giz-*

20 Başalp, *Kişisel Verilerin Korunması ve Saklanması*, s. 108.

liliğinin Korunması Hakkında Yönetmelik" ise bu alandaki bir başka düzenlemedir[21]. Yönetmeliğin 3. maddesinde kişisel bilgiler/veriler, *"belirli veya kimliği belirlenebilir gerçek ve tüzel kişilere ilişkin bütün bilgiler"* olarak tanımlanmıştır. Sonradan yürürlüğe giren bu yönetmelikteki tanımın da 6698 sayılı Yasanın tasarı halindeki kişisel veri tanımına uygun olarak düzenlendiği görülmektedir.

Bu açıklamalar sonucunda uluslararası düzenlemelerde, 6698 sayılı Yasada ve ilgili yönetmeliklerde yer alan tanımların aslında doğru bir seçim olduğu görülmektedir. Buna göre kişisel veri, *"belirli veya kimliği belirlenebilir gerçek kişiye ilişkin tüm veriler"* olarak tanımlanabilir[22]. Dolayısıyla kişisel veriden söz edilebilmesi için verinin gerçek bir kişiye ilişkin ve bu gerçek kişinin de söz konusu veriler kullanılmak suretiyle hali hazırda belirli ya da belirlenebilir nitelikte olması gerekir[23]. Daha geniş bir tanımla kişisel veri, bireyin kişisel, ailevi, mesleki her türlü ayırt edici özelliklerini ve niteliklerini göstermeye yarayan her türlü bilgidir[24]. Kişisel veri, belirli veya belirlenebilir bir kimsenin kimliğine, etkin kökenine, fiziksel özelliklerine, sağlık durumuna, genetik verilerine, öğrenim veya istihdam durumuna, ikamet adresine, kredi kartı bilgilerine, banka ve sigorta kayıtlarına, adli arşiv ve genel bilgi toplama kayıtlarına, düşünce ve inançlarına, alışveriş alışkanlıklarına, telefon rehberine, fotoğrafına, bilgisayarının IP adresine, parmak izine, cep telefonundan gönderdiği kısa mesajlarına, elektronik postalarına, sosyal paylaşım sitelerindeki aktivitelerine, en son gittiği restoran, bar ya da müzeye kadar ilgilisi olduğu ve kişiyi tanımlayan her türlü bilgidir[25]. Kişiyi dolaylı yollardan tanımlamak için alınan ve işlenen kamera kaydı, ses veya görüntü kaydı, biyometrik yöntemlerle tanımlama sağlayan parmak izi, yüz, iris, yazı, ses tanıma vb. yöntemlerle elde edilen bilgiler de kişisel veridir[26].

Nitekim YCGK da, 17.6.2014 tarihli, E. 2012/12-1510, K. 2014/331 sayılı ka-

---

21 Daha önce yürürlükte olan 6.2.2004 tarihli ve 25356 sayılı Resmi Gazete'de yayımlanan ""Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğin Korunması Hakkında Yönetmelik", 24.7.2012 tarihli yukarıda anılan yönetmeliğin 23. maddesiyle yürürlükten kaldırılmıştır. Yürürlükten kaldırılan yönetmeliğin 3. maddesinde kişisel veri şu şekilde tanımlanmaktaydı: *"tanımlanmış ya da doğrudan veya dolaylı olarak, bir kimlik numarası ya da fiziksel, psikolojik, zihinsel, ekonomik, kültürel ya da sosyal kimliğinin, sağlık, genetik, etnik, dini, ailevi ve siyasi bilgilerinin bir ya da birden fazla unsuruna dayanarak tanımlanabilen gerçek ve/veya tüzel kişilere ilişkin herhangi bir bilgi"*.

22 Benzer tanım için bkz: Lütfü Cihan Gülmez, "Kişisel Verilerimiz Korunuyor mu?", *Terazi Hukuk Dergisi*, Y.6, S.59, Temmuz 2011, s58; Küzeci, s. 9.

23 Dülger, *Bilişim Suçları*, s. 647.

24 A. Çiğdem Ayözger, *Kişisel Verilerin Korunması: Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil*, Beta, İstanbul, 2016, s. 6.

25 Aydın Akgül, *Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması*, Beta, İstanbul, 2014, s.8, 9; Ayözger, s. 6; Küzeci, s. 1, Llyod, s.42.

26 Lloyd, s. 41; Ayözger, s. 7; Akgül, s. 8, 9.

rarında başka bir çalışmamda yer vermiş olduğum yukarıda yer alan açıklamaya ve tanımlaya atıf yaparak kişisel verileri tanımlamıştır.

Özel Nitelikli Kişisel Veri ve Anonim Veri

Bazı kişisel veriler, ülkelerin mevzuatlarında ve uluslararası düzenlemelerde *"hassas veri"* olarak ifade edilmektedir. *Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Kişilerin Korunmasına Dair 108 sayılı Avrupa Konseyi Sözleşmesi*'nin 6. maddesinde *"özellikli veri kategorileri"* kavramı kullanılmıştır. KVKK'da ise *"hassas veri"* kavramı yerine *"özel nitelikli kişisel veri"* kavramı kullanılmıştır. 6698 sayılı Yasanın *"Özel nitelikli kişisel verilerin işlenme şartları"* başlıklı 6. maddesinin 1. fıkrasında özel nitelikli kişisel veriler tanımlanmıştır: *"Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir"*.

Özel nitelikli kişisel veriler, özellikle kişilerin ayrımcılığa maruz kalmalarını engellemek amacıyla özel bir koruma altına alınır. Kişinin dini ve felsefi inancı, ırk veya etnik kökeni, siyasi düşüncesi, dernek, vakıf ve sendika üyeliği, cinsel tercihleri, sağlık bilgileri, özel yaşamları ve hür türlü mahkûmiyetleri vb. ile ilgili bilgiler hassas kişisel veri olarak nitelendirilir. Özellikle İkinci Dünya Savaşı sonrasında ortaya çıkan ayrımcılık karşıtı ve insan onurunu korumayı amaçlayan düşüncenin bir yansıması olarak, özel nitelikli kişisel verilerin başkaları tarafından öğrenilmeleri halinde kişilerin mağduriyetlerine yol açılmasını engellemek amacıyla bunlar diğer verilere nazaran daha sıkı denetime tabi tutulurlar. Özellikle kişinin ırkına veya etnik kökenine ilişkin verilerin diğer kişisel verilerden ayrı bir düzenlemeye tabi tutulmasının nedeni, söz konusu kişilerin verilerinin devlet kurumları tarafından kötüye kullanılması endişesidir. Bu kaygının sebebi özellikle nüfus kayıtlarının ayrıntılı tutulması sonrası gerçekleşen Yahudi soykırımı gibi tarihsel olayların yaşanmış olmasıdır. Ulusal hukuk sistemleri açısından, bir kişisel verinin özel nitelikli olup olmadığı veri koruma otoritesinin ve nihai olarak mahkemelerin yorumuna bağlıdır. Avrupa Birliği Adalet Divanı *Lindquivist* kararında[27], hassas kişisel verilerin geniş yorumlanması gerektiğine karar vermiştir[28].

Avrupa Birliği Adalet Divanı'nın kişisel verilerin geniş yorumlanmasına ilişkin bu kararına rağmen, ülkemizde Anayasa Mahkemesi KVKK'nın yürürlüğünden önce vermiş olduğu bir kararında hem de özel nitelikli kişisel veri olan

27 Avrupa Adalet Divanı, Bodil Lindqvist v. İsveç, Dava No. C-101/01, 6.11.2003; karar için bkz: http://curia.europa.eu/juris/ liste.jsf?num=C-101/01; 3.11.2016.

28 Akgül, s. 17-20.

"biyometrik yöntemlerle kimlik doğrulamasının yapılmasının" kişisel veri olmadığını belirterek bu alana ilişkin yapılan yasal düzenlemenin Anayasanın 20. maddesine aykırı olmadığına karar vermiştir[29]. 6698 sayılı Yasanın 6. maddesinin 1. fıkrasında özel nitelikli kişisel veriler arasında açıkça *"biyometrik ve genetik veriler"* sayıldığı için artık bu kararının hukuki dayanaktan yoksun ve Yasanın yürürlüğe girdiği 7.4.2016 tarihinden itibaren hukuka aykırı olduğunu düşünüyorum.

Verinin belirli veya kimliği belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek veya kaynağı belirlenemeyecek hale getirilmesi sonucunda ortaya çıkan bilgiye *"anonim veri"* adı verilmektedir. İstatistik, araştırma, planlama vb. amaçlarla tutulan ve herhangi bir kişiyi belirtmekten ziyade kitlesel bilgi yığını olarak çıkan bu tür veriler, ilgili kişilerle ilişkilendirilmeleri mümkün olmadığından kişisel veri sayılmazlar[30]. Anonim veri, 6698 sayılı Yasanın "Tanımlar" başlıklı 3. maddesinin 1. fıkrasının (b) bendinde *"kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesi"* olarak tanımlanmıştır.

Kişisel Verinin İşlenmesi

Kişisel verilerin korunmasından bahsedebilmek için, öncelikle yukarıda tanımı verilen kişisel verilerin bir takım işlemlere tabi tutulması ve bunun sonucunda kullanılabilir, belli bir kişiyi tanımlayabilir, kendisinden anlamı sonuçlar çıkarılabilir hale gelmesi gerekir. Dolayısıyla kişisel verilerin işlenmesinin ne olduğunun da tanımlanması gerekir. Yukarıda andığımız sözleşme, yönerge, yasa ve yönetmeliklerde *kişisel verilerin işlenmesi* kavramı da tanımlanmıştır.

Avrupa Konseyi'nin 108 nolu *"Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme'sinde"* kişisel verilerin işlenmesi şu şekilde tanımlanmaktadır: *"Otomatik işleme, bir bütün veya parçalar halinde otomatik araçlarla gerçekleştirilmesi halinde aşağıdaki işlemleri içerir; verileri saklama, bu veriler üzerinde mantıksal ve/veya aritmetik işlemlerin gerçekleştirilmesi, verilerin değiştirilmesi, silinmesi, verilerin saklama yerlerinden geri alınarak/kurtarılarak yeniden kullanılması veya yayınlanması."*

Kişisel verilerin işlenmesi 95/46/EC sayılı *"Avrupa Topluluğu Veri Koruma Yönergesi'nin"* 2. maddesinde tanımlanmaktadır: Buna göre, işleme, otomatik ya da otomatik olmayan her türlü yöntemi içermektedir. Bu bağlamda, kişisel verilerin toplanması, elde edilmesi, kaydedilmesi, organize edilmesi, saklanması,

29 AYM, 19.3.2015, E. 2014/180, K. 2015/30, R.G. 3.4.2015-29315.

30 Başalp, Kişisel Verilerin Korunması ve Saklanması, s. 34.

değiştirilmesi, okunması, sorulması, kullanılması, transfer yoluyla başkalarına verilmesi, yayılması ya da hazır bulundurulması için yapılan işlemlerle bunların yanı sıra verilerin birleştirilmesi ya da ilişkilendirilmesi ve hatta bloke edilmesi, silinmesi ya da yok edilmesi suretiyle gerçekleştirilen her türlü işlemi içerir.

Avrupa Birliği tarafından 95/46/EC sayılı direktifin yerini almak üzere çıkarılan 2016 tarihli regülasyon (tüzük) ve IP/12/46 sayılı direktif ile de kişisel verilerin işlenmesi tanımlanmıştır. Direktifin "Tanımlar" başlıklı 3. maddesinde ve Regülasyonun yine "Tanımlar" başlıklı 4. maddesinde birebir aynı biçimde *"işleme; kişisel veri ya da bir takım kişisel veriler üzerinde; otomatik olsun ya da olmasın; aktarım, yayma veya diğer yollarla elde edilebilir hale getirme, sıraya koyma, birleştirme, sınırlama, silme veya yok etme suretiyle toplama, kayıt etme, düzenleme, yapılandırma, depolama, uyumlaştırma, değiştirme, geri kazanma, danışma, kullanma, açıklama gibi herhangi bir işlemde ya da bir takım işlemlerde bulunma"* olarak tanımlanmaktadır. Ayrıca Direktifin 3. maddesinin 4. fıkrasında *"işlemenin kısıtlanması, depolanmış kişisel verilerin gelecekte işlenmesinin sınırlanması amacıyla işaretlenmesi"* şeklinde tanımlanmıştır.

6698 sayılı *"Kişisel Verilerin Korunması Kanunu'nun"* 3. maddesinin 1. fıkrasının (e) bendinde kişisel verilerin işlenmesi *"kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem"* şeklinde tanımlanmıştır.

Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik'in 4. maddesinin 1. fıkrasının (ğ) bendi ile kişisel sağlık verilerinin işlenmesi, *"kişisel sağlık verilerinin 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 hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi sağlık verileri üzerinde gerçekleştirilen her türlü işlemi"* olarak tanımlanır. Görüldüğü ve olması gerektiği üzere, bu düzenleme 6698 sayılı Yasanın tanımıyla birebir aynıdır.

Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik'te ise kişisel verilerin işlenmesi 3. maddenin 1. fıkrasının (i) bendinde *"kişisel verilerin otomatik olan veya olmayan yollarla elde*

edilmesi, kaydedilmesi, depolanması, değiştirilmesi, silinmesi veya yok edilmesi, yeniden düzenlenmesi, açıklanması veya başka bir şekilde elde edilebilir hale getirilmesi, üçüncü kişilere aktarılması, kullanılmasının sınırlanması amacıyla işaretlenmesi, tasniflenmesi veya kullanılmasının engellenmesi gibi bu veriler üzerinde gerçekleştirilen işlem ya da işlemler bütünü" şeklinde tanımlanmıştır[31].

Kişisel verilerin toplanması, elde edilmesi, kaydedilmesi, düzenlenmesi, saklanması, değiştirilmesi, uyarlanması, birleştirilmesi, okunması, sorulması, kullanılması, açıklanması, erişilebilir hale getirilmesi, üçüncü kişilere aktarılması, yayılması, hazır bulundurulması veya anonimleştirilmesi için yapılan işlemlerin yanı sıra verilerin birleştirilmesi ya da ilişkilendirilmesi ve hatta bloke edilmesi, silinmesi ya da yok edilmesi suretiyle gerçekleştirilen her türlü işlem ya da işlemler bütünü kişisel verilerin işlenmesi tanımı kapsamında değerlendirilir. İşleme, otomatik ya da otomatik olmayan prosedürler yoluyla gerçekleştirilen kişisel verilerle ilgili olabilecek her türlü süreci içerir[32].

Otomatik işlemeden kasıt, verilerin otomasyon sistemlerinin kullanıldığı yöntemlerle işlenmesidir. Otomasyon, mekanik aygıtlarla yapılan işlemlere verilen addır, ancak bu yasa kapsamında bunun dijital (sayısal) işlemleri de içerecek şekilde anlaşılması gerekir, örneğin bilişim sistemleriyle yapılan bu tür işlemler de (ki uygulamada sıklıkla görülen budur) kişisel verilerin işlenmesi olarak kabul edilir. Bu sayede verilerin toplanmasından başlayarak geçtiği tüm aşamaları kapsayan bütün işlem basamakları ve yöntemleri koruma altına alınır. Nitekim 6698 sayılı Yasa ve ilgili yönetmeliklerle de yapılmaya çalışılan budur[33].

Tanımdan da anlaşıldığı üzere, verilerin işlenmesi otomatik/dijital bir prosedüre bağlı değildir. Örneğin; sorumlunun kişisel verileri ister yazılı belge üzerinden ister bilgisayar monitörü üzerinden okuması işlem tanımı içinde yer alır. Kişinin kendisi için tuttuğu özel kayıtlar ise kişisel verilerin işlenmesi olarak nitelendirilmez. Örneğin kişinin bilgisayarında tuttuğu adres defterleri vb. kişisel ya da ailevi nitelikteki ilişkiler sonucu tutulan kayıtlar bu kapsamda ele alınmaz. Tabii ki bu bilgiler mesleki ve ticari faaliyetler dahilinde işlenen kişisel verilerden ayrı olarak değerlendirilmeli ve bu tür verilerin belirsiz sayıda kişinin erişimine açık tutulması hali de hariç tutularak kişisel veri olarak düşünülmelidir. Nitekim 6698 sayılı Yasanın "İstisnalar" başlıklı 28. maddesinde 1. fıkrasının (a) ben-

31 Önceki yönetmeliğin 3. maddesinde kişisel verilerin işlenmesi *"otomatik olsun olmasın, toplama, kaydetme, hazırlama, yükleme, uyarlama, değiştirme, geri çağırma, danışma, kullanma, aktarma yoluyla açığa vurma, yayma ya da bunların dışında erişilebilir hale getirme, düzenleme, birleştirme, engelleme, silme gibi yollardan, kişisel bilgiler üzerinden yürütülmekte olan herhangi bir işlem ya da işlemler bütünü"* olarak tanımlanmıştır.

32 Dülger, *Bilişim Suçları*, s. 669.

33 Dülger, *Bilişim Suçları*, s. 669.

dinde *"Kişisel verilerin, üçüncü kişilere verilmemek ve veri güvenliğine ilişkin yükümlülüklere uyulmak kaydıyla gerçek kişiler tarafından tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında işlenmesi."* halinde anılan yasanın hükümlerinin uygulanmayacağı belirtilmiştir.

Anonim veriler üzerinde işlem yapılması da kişisel verilerin işlenmesi olarak kabul edilmez. Zira verinin sahibi ile veri arasındaki illiyet bağı kopmuş olduğundan, bu tür veriler üzerinde yapılan herhangi bir işlem kişi hak ve hürriyetlerinin ihlali sonucunu da doğurmaz[34]. Anonim verilerin işlenmesi 6698 sayılı Yasa tarafından öngörülerek "İstisnalar" başlıklı 28. maddesinde 1. fıkrasının (b) bendinde *"Kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi."* halinde anılan yasanın hükümlerinin uygulanmayacağı belirtilmiştir.

Ancak kişilerin ırk, siyasî düşünce, felsefî inanç, din, mezhep veya diğer inançları; dernek, vakıf ve sendika üyeliği, sağlık ve özel yaşamları ve hür türlü mahkûmiyetleri vb. ile ilgili kişisel veriler *"özel niteliği olan"* ya da *"hassas"* kişisel veriler olarak adlandırılmakta olup, genel kabul gören yaklaşıma göre bunlar da kişisel veri sayılır ancak hassas nitelikte olmaları nedeniyle bu verilerin işlenmesi kural olarak yasaktır[35]. Ancak istisnai olarak, kamu yararının gerektirmesi, kişinin rızasının alınması vb. bazı hallerde bu verilerin işlenmesine izin verilebilir[36]. 6698 sayılı Yasanın *"Özel nitelikli kişisel verilerin işlenme şartları"* başlıklı 6. maddesinin 2. fıkrasında özel nitelikli kişisel verilerin ilgilinin açık rızası olmaksızın işlenmesinin yasak olduğu açık bir biçimde ifade edilmiştir. Özel nitelikli kişisel verilerin işlenebileceği istisnalar 3. ve 4. fıkralarda şu şekilde belirtilmiştir: *"(3) Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir. (4) Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır".*

---

34 Uğur Ersoy, "Bir İnsan Hakları Kavramı Olarak Kişisel Verilerin Korunması", *Yayınlanmamış Yüksek Lisans Tezi*, Gazi Üniversitesi Sosyal Bilimler Enstitüsü Kamu Yönetimi Anabilim Dalı Siyaset ve Sosyal Bilimler Bilim Dalı, Ankara, 2009, s. 16.

35 Hassas kişisel veriler ve bunların işlenebileceği durumlar hakkında ayrıntılı açıklama için bkz: Cemil Kaya, "Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi", *İÜHFM*, C.LXIX, S.1 - 2, 2001, s. 317 - 334.

36 Ersoy, s. 16.

III. 6698 Sayılı Kişisel Verilerin Korunması Kanunu ile Getirilen Düzenlemelerin Genel Çerçevesi

6698 sayılı Yasanın hazırlanış öyküsü aslında oldukça eskilere dayanmaktadır. Yukarıda da görüldüğü üzere Türkiye, Avrupa Konseyi bu konudaki ilk sözleşmeyi 1981 yılında imzaya açıldığı gün ilk imzalayan devletlerden birisidir. Buna karşın sözleşme ancak 2016 yılı başında onaylanıp ülke açısından bağlayıcı hale gelmiştir. Sözleşmenin bu kadar geç onaylanmasındaki hukuki neden, öncesinde bir türlü Sözleşmedeki hak ve yükümlülükleri içeren bir yasanın hazırlanıp yürürlüğe sokulamamasıdır. Yine de yasanın hazırlık sürecinin Sözleşmenin imzalandığı tarih olan 1981 yılına götürülmesi mümkündür. Bunun yanı sıra benim takip edebildiğim kadarıyla en azından on yıldan beri bu konuda çeşitli yasa tasarısı hazırlama süreçleri yaşanmış, ancak politik, hukuki vb. nedenlerle bir türlü bu konuda bir yasa çıkarılamamıştır.

Aslında yasa metni ve öncesinde hazırlanan tasarılar incelendiğinde Avrupa Birliğinin 95/46/EC sayılı Direktifinin esas alındığı görülür. Nitekim bu yasanın yapılmasındaki temel amaçlardan birisi ve belki de en önemlisi AB adaylığı sürecinde AB'ye uyum çerçevesinde bu düzenlemenin yapılması gerekliliğidir. Ancak AB düzenlemelerinde kamu kurum ve kuruluşlarına (özellikle kolluk ve istihbarat kurumlarına) sınırlı istisnalar tanınmış ve bu konuda denetim getirilmiş olması, ayrıca veri koruma kurulunun siyasi otoriteden bağımsız özerk bir yapıda olması gerekliliği bu tür bir düzenleme getirmek istemeyen Türkiye açısından yasanın çıkmasının sürekli ertelenmesine yol açan en önemli faktör olmuştur. Sonuçta Avrupa Birliğinin 95/46/EC sayılı Direktifine tam olarak uyumlu olmayan Türk tipi bir kişisel verilerin korunması kanunu hazırlanmış ve yürürlüğe girmiştir.

Yasanın yürürlüğe konulmasındaki bu anlayış farkı başta olmak üzere eleştirilecek pek çok yanının olmasına karşın, olumlu taraflarının da belirtilmesi gerekir. Öncelikle bana göre bir, sıfırdan büyüktür. Anılan yasanın yürürlüğe girdiği 7.4.2016 tarihinden önce de ülkemizde kişisel veriler kaydedilmekte, yayılmakta, yok edilme, değiştirilmekte vb. yani kısacası her türlü kişisel veri hiçbir sınırlama ve düzenleme olmaksızın herkes tarafından işlenmekte ve kullanılmaktaydı. İşte bu yasa ile sınırlı da olsa bir düzenleme getirildi. Bundan sonra kişi ve kurumlar yukarıda belirttiğim sınırsızlıkta veri işleyemeyecekler, en azından yaptırımların ağırlığı nedeniyle bundan çekinecekler. Nitekim daha şimdiden özel sektörde pek çok kuruluş *"Kişisel Verilerin Korunması Kanuna Uyumluluk Süreci"*ne ilişkin politikalar oluşturmakta, iş işleyiş süreçlerini buna göre yeniden yapılandırmaya çalışmakta ve hatta bunu yapabilmek için danışmanlık hizmetleri almaktadır. Bu bile tek başına yapılanın olumlu bir adım olduğunu

göstermektedir. Ancak tabii ki bu olumlu taraflar, diğer yanda nesnel bir gözle bakıldığında açıkça görülen olumsuzlukları yok saymama neden olmamaktadır.

Yasaya getirilen önemli eleştirilerden biri; AB kendi direktifini değiştirmeye hazırlanıyorken yasanın eski direktif dikkate alınarak hazırlanmış olmasıdır. Nitekim 6698 sayılı Yasanın yürürlüğe girmesinden hemen bir hafta sonra Avrupa Parlamentosunda yapılan oylama ile yeni direktif ve regülasyon (tüzük) oylanmış ve kabul edilmiştir. Ancak bu direktifin tarihi 1995 yılıdır ve AB üyesi ülkelerin o tarihten bu yana yani tam yirmi bir yıldır bu konuda deneyimleri bulunmaktadır. İşte bu deneyim ve uyum sürecinden sonra arada geçen sürede bilişim teknolojilerindeki gelişmeler ve bu alandaki ihtiyaçlar da dikkate alınarak yeni bir çalışma yapılmış ve direktif güncellenmiş, bilişim dünyasındaki terminolojiyle mevcut sürüm yenisiyle yükseltilmiştir (upgrade). Beklentimiz ülkemiz açısından eski versiyona uyum sağlandıktan sonra, bir an önce yeni sürüme geçilerek mevzuat ve uygulama değişikliklerinin yapılmasıdır. Tabii ki daha en başta yeni sürümle başlamak en iyi seçenek, ancak eksiklikleri ve doğuştan eskiliğine rağmen ülkemiz gerçekleri dikkate alındığında hiç olmayan düzenlemenin çıkmış olması da teselli veren bir gelişme.

6698 sayılı Yasa bir bütün olarak kişisel verileri, bunların işlenmesini ve korunmasını tanımlayan, özellikle kişisel verilerin işlenmesinin ve korunmasının nasıl olacağının genel hatlarıyla çerçevesini belirleyen, bunun yanı sıra işleme ve koruma kurallarına uyulmaması halinde bunun yaptırımının ne olacağını tespit eden, bu alandaki temel düzenleyici yasadır. Yukarıda belirttiğim üzere öncelikle kişisel verinin ne olduğu, bu verilerin işlenmesini, korunmasını tanımlamış ve işleme /korumaya ilişkin kurallara uyulmadığı takdirde kabahatler hukuku bakımından (idari düzene aykırılıklar) bunun yaptırımını düzenlemiştir.

Yasanın getirdiği kişisel veri koruma ve işleme yöntemi ile yasanın getirdiği rejime uyum süreci bu çalışmanın kapsamı içinde olmadığı için ayrıca ve ayrıntılı olarak incelemiyorum. Aşağıda suçlar ve kabahatler açısından yeri geldikçe bunları değerlendirmeyi uygun buluyorum.

IV. Türk Ceza Kanunu'nda Yer Alan Kişisel Verilerin Korunmasına İlişkin Suçlar

A. Kişisel Verilerin Korunmasının Ceza Kanununda Düzenlenmesi Gerekliliği

Veri koruma hukuku, hangi kişisel verilerin kim tarafından ve kimin için elde edildiğinin, kim tarafından hangi amaçla ve ne süreyle işleneceğinin, kim ya da kimlere aktarılacağının ve ne zaman yok edileceğinin öğrenilmesi hakkını içerir. Üzülerek ifade etmeliyim ki Türk hukuk düzeninde kişisel verilerin korunması

konusu 6698 sayılı Yasa yürürlüğe girene, hatta Kişisel Verileri Koruma Kurulu üyeleri seçilmeye başlanıncaya kadar yeterli ve gerekli ilgiyi görmemiştir[37]. Ülkemizde uzun bir süre boyunca kişisel verilerin korunması alanında yeterli yasal düzenlemelerin bulunmaması nedeniyle bu konu öncelikle kişilik haklarının korunması konusunun altında incelenmiştir. Bu bağlamda kişisel verilerin korunması genel olarak Medeni Kanunun 24. maddesi altında değerlendirilir. Kişisel verilerin izinsiz ele geçirilmesi dolayısıyla kişilik hakkının ihlali halinde ihlalin özel hukuk açısından sonlandırılması ve zararın tazmini Medeni Kanunun 25 ve Borçlar Kanununun 41 vd. maddelerine göre gerçekleştirilir[38]. Dolayısıyla kişilik hakkı ihlali ve bunun sonuçlarıyla ilgili Medeni Kanun ve Borçlar Kanunu maddeleri, kişilik ihlali hangi araçla ve hangi alanda gerçekleşirse gerçekleşsin uygulama alanına sahiptir; çünkü ceza hukukunda geçerli olan suçta ve cezada kanunilik ilkesi özel hukukta geçerli değildir[39]. Bu yasaların ilgili maddelerinin yorum ve kıyas yoluyla kişisel verilerin kötüye kullanılması halinde uygulanması açıkça yazılmasa da kıyas ve yorum yoluyla mümkündür[40].

Kişisel verilerin bilişim sistemleri aracılığıyla ihlali, hukuka aykırı olarak ele geçirilmesi ve kötüye kullanılması gibi eylemlerin yukarıda anılan ilke nedeniyle ceza hukuku açısından ayrıca düzenlenmesi ve bu eylemlerin suç tipi haline getirilmesi gerekir[41]. Aksi takdirde kişisel verilerin ceza hukuku normlarıyla korunması mümkün olmaz. Bu açıdan Almanya'da bu alanda yapılan yasal düzenleme gibi, kişisel verilerin korunmasına ilişkin özel bir yasaya gereksinim olduğu belirtilmiştir[42]. Öte yandan ülkemizde bilişim suçları alanında yapılan ilk düzenlemeyi içeren 765 sayılı ETCK'nın 525 a/1 maddesinde düzenlenen *"verilerin ele geçirilmesi suçunun"* bu açıdan yeterli ve gerekli korumayı sağlamadığı ifade edilmiştir[43].

Kişisel verilerin ele geçirilmesi yoluyla kişilik haklarının ihlal edilmesi eylemlerinde dikkat edilmesi gereken bir diğer konu da, devletin resmi güvenlik kuruluşları dışında birçok kurum ve kuruluşun da bireyler hakkında özel

37 Dülger, *Bilişim Suçları*, s. 265.

38 Nilgün Başalp, "Kişisel Verilerin Korunması ve İnternet", *İnternet ve Hukuk*, Der: Yeşim M. Atamer, İstanbul Bilgi Üniversitesi Yayını, İstanbul, 2004, s. 6; Başalp, *Kişisel Verilerin Korunması ve Saklanması*, s. 100 – 103.

39 Sibel Özel, *Uluslararası Alanda Medya ve İnternette Kişilik Hakkının Korunması*, Seçkin Yayıncılık, Ankara, 2004, s.168.

40 Dülger, *Bilişim Suçları*, s. 670, 671.

41 Dülger, *Bilişim Suçları*, s. 671.

42 Yener Ünver, "Türk Ceza Kanunu'nun ve Ceza Kanunu Tasarısının İnternet Açısından Değerlendirilmesi", *İÜHFM*, C.LIX, S.1 – 2, İstanbul, 2001, s. 93, 94.

43 Yener Ünver, "Federal Almanya'da Terör ve Organize Suçluluk ile İlgili Düzenlemeler", *Prof. Dr. Nurullah Kunter'e Armağan*, İstanbul, İÜHF Eğitim Öğretim ve Yardımlaşma Vakfı Yayını, 1998, s. 437.

bilgiler toplaması ve bu bilgilerle kişilik haklarını ihlal etme olanağına sahip olmasıdır. Hastalar hakkında çok özel bilgileri bilişim sistemlerinde bulunduran hastaneler[44], DNA ve parmak izi analizi yapan ve bunun sonuçlarını bilişim sistemlerinde saklayan adli tıp kurumları, cep telefonu hattı işletmecisi olan şirketlerin bulundurdukları veriler ya da çok sayıda müşteri verisi tutan finans kurumları ile perakende satış şirketleri bunlara örnek olarak verilebilir[45]. Nitekim bir suça ilişkin delil elde etmek için şüpheli, sanık veya diğer kişilerden alınan örnekler üzerinde yapılan genetik inceleme sonuçları, kişisel veri niteliğindedir[46]. Bu nedenle kişisel verilerin korunması açısından yapılacak düzenlemede yalnızca resmi kuruluşların bu bilgileri toplaması ve kullanması konusundaki çerçeve değil, söz konusu bilgileri depolayıp kullanabilme yetkisine ve teknolojisine sahip kamu kuruluşları ve özel kuruluşlar açısından da yasal çerçeve belirlenmelidir[47].

Bu alandaki bir başka büyük sorun ise kimlik hırsızlığı olarak da bilinen internetteki kişisel verilerin ele geçirilmesi eylemlerinde, genellikle müşterilerin isminin, doğum tarihinin, sosyal güvenlik ya da vatandaşlık numaralarının, kredi kartı bilgilerinin, kendilerinin haberi olmaksızın elde edilmesidir[48]. Daha son-

---

44 "Tıp bilimi bakımından kişisel veriler, kişinin sağlık durumuna ilişkin verilerdir. Tıbbi veriler olarak da adlandırılan bu veriler, gerçek kişilerin sağlık durumuna ilişkin olup, tıp mesleği mensuplarınca edinilecek bilgilerdir. Avrupa Konseyi Bakanlar Komitesinin Tıbbi Veriler Hakkındaki (97) 5 sayılı Tavsiye Kararı'nın 1. maddesine göre, tıbbi veri bireyin sağlık durumu ile ilgili kişisel bilgileri ifade eder. Tıbbi veri kavramı aynı zamanda genetik verileri de kapsar. Sağlık ile ilgili kişisel nitelikteki veriler özel biteliği olan veriler olup, diğer kişisel verilere nazaran daha özel bir koruma gerektirmektedir. Gerçekten de kişinin sağlık durumu ilgili verilerin bir başka deyişle tıbbi verilerin kötüye kullanımının kişiye vereceği zarar da göz önüne alındığında, bu tür verilerin kaydının özel bir usule bağlanması ve belli amaçlarla sınırlandırılması yerinde olacaktır. Avrupa Konseyi Bakanlar Komitesi'nın (97) 5 sayılı Tavsiye Kararı'nın 3. maddesinde bu husus; *'Tıbbi verilerin toplanması ve işleme tabi tutulması sırasında temel hak ve özgürlüklere özellikle mahremiyete saygı hakkı sağlanmalıdır. Tıbbi veriler sadece iç hukuk tarafından sağlanan güvencelere uygun olarak toplanabilir ve işleme tabi tutulabilir.'* şeklinde vurgulanmıştır. Kişisel Verilerin Korunması Kanunu Tasarısı m.7/2-f'de, özel hayatın ve aile hayatının gizliliğinin korunmasını sağlayacak yeterli önlemlerin alınması şartıyla; sağlık ile ilgili kişisel verilerin *'koruyucu hekimlik, tıbbi teşhis, tedavi, bakım veya sağlık hizmetlerinin yürütülmesi amacıyla kişisel verilerin, sağlık kurumları, işyeri sağlık birimi oluşturmakla yükümlü işverenler, okullar ve üniversiteler tarafından ilgili kanunlara uygun olarak, hukuken veya meslek kurallarına göre sır saklama yükümlülüğü altında bulunan sağlık personeli tarafından'* işlenebileceği öngörülmektedir. Tıbbi verilerin otomatik olan veya olmayan yollarla kaydedilmesi ve depolanması mümkündür. Bu verileri elde etme, üçüncü kişilere aktarma, üzerinde değiştirme, silme, yok etme gibi işlemler ancak kanunların izin verdiği çerçevede ve hukuka uygun olduğu ölçüde yapılabilir." Yokuş Sevük, s. 786, 787.

45 Dülger, *Bilişim Suçları*, s. 671, 672.

46 Yokuş Sevük, s. 797.

47 Dülger, *Bilişim Suçları*, s. 672.

48 Ian Walden, *Computer Crimes and Digital Investigations*, Second Edition, Oxford University Press, Oxford, 2016, pn. 3.73 – 3.76; Jonathan Clough, *Principles of Cybercrime*, Second Edition, Cambridge University Press, Cambridge, 2015, s.238 – 254.

ra bu verilerle, haksız kazanç elde etmek üzere, bilişim sistemleri kullanılmak suretiyle gerçekleştirilen nitelikli dolandırıcılık da dahil olmak üzere pek suç işlenmektedir. Kredi kartı bilgileri ise çoğunlukla, müşteri hesaplarından nakit para transfer etmenin yanı sıra, müşterinin kredi kartının sahte bir kopyasının çıkartılmasında kullanılmaktadır[49].

Kişisel verilerin korunması konusu günümüzde gittikçe önem kazanmakta, hem bireyler günlük yaşamlarında bu konuda pek çok yakınmada bulunmakta hem de konu üst düzey yargı organlarının hukuksal tavır almalarına neden olmaktadır. Bunun önemli örneklerinden birini Facebook ve benzeri sosyal paylaşım sitelerinde kişisel verilerin sürekli tutulması oluşturur. En popüler sosyal medya sitelerinden birisi olan Facebook, kullanıcıların sildiği mesaj, fotoğraf ve videoları yine de kayıt altında tuttuğu öne sürülerek, yoğun biçimde eleştirilmektedir[50]. Eleştiriler Almanya'da temel insan haklarını korumakla yükümlü olan Anayasa Mahkemesi'nde de gündeme gelmiştir. Alman Federal Anayasa Mahkemesi Başkanı Andreas Voßkuhle, ünlü haber dergisi Focus'a verdiği röportajda, Facebook kullanımının riskler taşıdığına dikkat çekmiş, vatandaşların verilerini sildikten sonra da bunların Facebook tarafından kayıt altında tutulup tutulmadığını bilmediklerini belirtmiş ve konunun Anayasa Mahkemesi'ne taşınabileceğine işaret etmiştir. İnsan hakları örgütleri ve bilişim uzmanları, kullanıcılar tarafından silinen mesaj, fotoğraf ve videoların, Facebook tarafından tümüyle silinmediğini belirterek, bu uygulamaya son verilmesini talep etmektedirler. Andreas Voßkuhle, Anayasa Mahkemesi'nin gelecek dönemlerde Facebook uygulamalarının, vatandaşların *"kişisel verileri üzerinde tam kontrol sahibi olma hakkını"* ihlal edip etmediğinin incelenmesi ihtiyacını ortaya çıkarabileceğine dikkat çekmiştir. Nitekim Federal Alman Hükümeti, aralarında Facebook'un da bulunduğu bilişim ve sosyal medya devlerinin temsilcileri ile bir süredir görüşmeler yürütmektedir. Hükümet bu şirketlerin gönüllü olarak *"veri güvenliği kuralları"* belgesini kabul etmelerini ve yurttaşlara güvence vermelerini istemektedir. Facebook, son zamanlarda artan eleştiriler üzerine değişikliklere gitmiş ve kullanıcıların kendi bilgilerini paylaşırken daha tedbirli davranabilmesi için çeşitli yeni olanaklar sunmuştur[51]. Bu gelişmelerin sonunda bilişim alanında yeni bir hak türü ortaya çıkmıştır: Unutulma hakkı (right to

49 Ali Karagülmez, *Bilişim Suçları ve Soruşturma – Kovuşturma Evreleri*, 5. Bası, Seçkin Yayıncılık, Ankara, 2014, s. 451.

50 Wouter Martinus Petrus Steijn, "The Coast of Using Facebook: Assigning Value to Privacy Protection on Social Network Sites Against Data Mining, Identity Theft, and Social Conflict", *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*, Eds: Serge Gutwirth/Ronald Leenes/Paul De Hert, Springer, Heidelberg, 2016, s. 327.

51 "Kişisel Bilgiler Facebook'a Ne Lazım", *Esas, Aylık Hukuk Dergisi*, S. 2, Kasım 2011, s. 34.

be forgotten)[52]. Avrupa Adalet Divanı, unutulma hakkını tanıdığı ve tanımladığı Google Spain SL, Google Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja Gozáles kararında bu konuda AB Veri Koruma Direktifinin uygulamasına ışık tutacak tespitlerde bulunmuştur[53].

Yukarıda anılan görüş ve eleştiriler dikkate alınarak TCK'da, kişisel verilerin hukuka aykırı olarak kaydedilmesi, kullanılması veya açıklanması ve verilerin yok edilmemesi eylemleri ayrı maddeler halinde suç olarak düzenlenmiştir. Böylelikle ülkemiz ceza hukuku düzeni açısından önemli bir boşluk giderilmiştir[54]. Bu düzenlemenin bilişim suçları açısından olumlu taraflarından birisini de kişisel verilere ilişkin suç tiplerinin *"bilişim alanında suçlar"* başlıklı bölümde diğer suç tipleriyle bir arada değil, bu suçlarla korunan hukuksal değere göre, benzer hukuksal değerlerin korunduğu *"özel hayata ve hayatın gizli alanına karşı suçlar"* bölümünde düzenlenmiş olmasıdır[55]. Bu da, yasa koyucu tarafından yasaya yapma tekniği ve sistematik açısından doğru bir iş yapıldığını gösterir.

B. Kişisel Verilerin Korunmasına İlişkin Suçlar ve Unsurları

1. Türk Ceza Kanunu'nda Düzenlenen Suç Tipleri

Kişisel verilerin korunmasına ilişkin suç tipleri 5237 sayılı TCK'nın özel hükümlerin yani suç tiplerinin düzenlendiği ikinci kitabının *"kişilere karşı suçlar"* başlıklı ikinci kısmının *"özel hayata ve hayatın gizli alanına karşı suçlar"* başlıklı dokuzuncu bölümünde yer almaktadır. TCK'nın 135. maddesinde *"kişisel verilerin kaydedilmesi suçu"*, 136. maddesinde *"verileri hukuka aykırı olarak verme veya ele geçirme suçu"*, 137. maddede bu suçların nitelikli halleri, 138. maddede *"verilerin yok edilmemesi suçu"* 140. maddede ise bu suçlara ilişkin olarak tüzel kişiler hakkında uygulanacak güvenlik tedbirleri düzenlenmiştir.

KVKK'nın "Suçlar ve Kabahatler" başlıklı beşinci bölümünde "suçlar" başlıklı 17. maddenin 1. fıkrasında *"Kişisel verilere ilişkin suçlar bakımından 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununun 135 ila 140 ıncı madde*

---

52 Bu kavram için bkz: Meg Leta Jones, *Ctrl + Z: The Right to Be Forgotten*, New York University Press, New York, 2016, s. 1 vd.; Amitai Etzioni, *Privacy in a Cyber Age*, Palgrave Macmillan, New York, 2015, s.113-122; Cécile de Terwangne, "The Right to be Forgotten and Informational Autonomy in the igital Environment", *The Ethics of Memory in a Digital Age Interrogating the Right to be Forgotten*, Edited by Alessia Ghezzi, Ângela Guimarães Pereira, Lucia Vesnić-Alujević, European Commisson, Joint Research Centre, Palgrave Macmillan, 2014, s. 82 – 101; Yod-Samuel Martin, Jose M. Del Alamo, "Forget About Being Forgetten", *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*, Eds: Serge Gutwirth/Ronald Leenes/Paul De Hert, Springer, Heidelberg, 2016, s. 249 – 276.

53 Karar ve değerlendirmesi için bkz: Armağan Ebru Bozkurt Yüksel, *Bulut Bilişimde Kişisel Verilerin Korunması*, Yetkin, Ankara, 2016, s. 132 – 136.

54 Dülger, *Bilişim Suçları*, s. 673.

55 Dülger, *Bilişim Suçları*, s. 673.

hükümleri uygulanır." denilerek, anılan yasa çerçevesinde olsun ya da olmasın kişisel verilere ilişkin haksızlıklar açısından TCK'ya atıf yapılarak, anılan yasa öncesinde de yürürlükte olan suç tiplerinin uygulanmaya devam edileceği belirtilmiş, böylelikle 6698 sayılı Yasa ile TCK'nın 135 ile 140. maddeleri arasında doğrudan bağlantı kurulmuştur.

Maddenin ikinci fıkrasında ise *"Bu Kanunun 7 nci maddesi hükmüne aykırı olarak; kişisel verileri silmeyen veya anonim hâle getirmeyenler 5237 sayılı Kanunun 138 inci maddesine göre cezalandırılır."* denilmek suretiyle aslında benim çok öncesinde eksikliğini belirtmiş olduğum bir husus giderilmiştir. Bu konuya aşağıda tekrar döneceğim.

2. Korunan Hukuksal Değer

TCK'nın 135. maddesinde düzenlenen *"kişisel verilerin kaydedilmesi suçu"* ve 136. maddesindeki *"verileri hukuka aykırı olarak verme veya ele geçirme suçu"* ile ortak hukuksal değerler korunur. Yasanın sistematiğinden anlaşılacağı üzere bu suç tipleriyle genel olarak kişilerin özel hayatı ve hayatın gizli alanı, özel olarak ise kişisel veriler korunur[56].

Bu suçlarla hem Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesinde[57] bir insan hakkı ve hem de 1982 Anayasasının 20. maddesinde[58] bir temel hak ve

56 Dülger, *Bilişim Suçları*, s. 675, 704.

57 Madde 8 - Özel ve aile hayatına saygı hakkı: 1. Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir. 2. Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir.

58 Madde 20 - Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz. Adli soruşturma ve kovuşturmanın gerektirdiği istisnalar saklıdır.

Kanunun açıkça gösterdiği hallerde, usulüne göre verilmiş hâkim kararı olmadıkça; gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınan merciin emri bulunmadıkça, kimsenin üstü, özel kâğıtları ve eşyası aranamaz ve bunlara el konulamaz. Milli güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlakın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak, usulüne göre verilmiş hakim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde ve kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; kimsenin üstü, özel kağıtları ve eşyası aranamaz ve bunlara el konulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hakimin onayına sunulur. Hakim, kararını el koymadan itibaren kırksekiz saat içinde açıklar; aksi halde, el koyma kendiliğinden kalkar.

(Ek fıkra: 5982 - 7.5.2010 / m.2) Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.

özgürlük olarak belirtilen *"özel hayatın gizliliği hakkı"*, kişilerin özel yaşamına müdahale olanağı veren teknolojik gelişmeler karşısında söz konusu suç tipleriyle bir hukuksal değer olarak korunur[59]. Böylelikle hem AİHS hem de Anayasada düzenlenen bir insan hakkı ve temel hak ve özgürlük somut bir ceza hukuku normu ile korunmuş olur[60]. Nitekim Anayasanın 20. maddesine 7.5.2010 tarih ve 5982 sayılı Yasanın 2. maddesiyle eklenen 3. fıkra ile kişisel verilerin korunması temel bir hak ve özgürlük olarak, açıkça Anayasa normuna konu olan bir hak haline gelmiştir[61]. Ayrıca normda kişisel verilerin kendisinin korunması kadar, kişisel verilerin işlenmesi de düzenlenmiş ve koruma altına alınmıştır. Ayrıca Anayasanın 20. maddesinin 3. fıkrasının son tümcesinde kişisel verilerin korunmasına ilişkin esas ve usullerin yasa ile düzenlenmesi gerektiği belirtilir; bu konuda yasama organına verilen görev TCK'da yer alan incelemekte olduğumuz maddeler yanında 6698 sayılı Yasanın da yürürlüğe konulmasıyla yerine getirilmiştir.

Bu suç tipleriyle kişisel verilerin mi yoksa sır kapsamına giren bilgilerin mi korunduğu sorusu akla gelir. Bu suçların düzenlendiği "özel hayata ve hayatın gizli alanına karşı suçlar" başlıklı bölümde 765 sayılı ETCK'da "sırrın masuniyeti aleyhine cürümler" başlıklı fasılda düzenlenen bazı benzer suç tipleri yer alır. Buradan hareketle bu bölümde düzenlenen suçlarla sırrın dokunulmazlığının korunduğunu, nitekim 765 sayılı ETCK'da meslek sırrının açıklanması olarak düzenlenen bu suç tipinin, 5237 sayılı TCK'da verileri hukuka aykırı olarak verme veya ele geçirme suçu olarak 136. maddede düzenlendiğini belirten yazarlar bulunmaktadır[62]. Ancak bir sırrın varlığı, sahibinin açıklanmamasında yarar gördüğü ve başkaları tarafından daha önce bilinmeyen bir konunun varlığına bağlıdır[63]. Oysa TCK'nın 135. ve 136. maddelerinde kişisel verilerin hukuka aykırı olarak kaydedilmesi ve verilerin hukuka aykırı olarak verilmesi veya ele geçirilmesi aranmakta ancak söz konusu verilerin sır olarak nitelendirilen ve sahibinin diğer kişilerin erişimine ve öğrenmesine izin vermediği veri niteliğinde olması aranmaz. O halde bu suç tipleri açısından gerçek bir sırrın varlığı gerekmez, dolayısıyla kaydedilen kişisel bilginin sır olarak saklanması aranmaz.

---

59 Durmuş Tezcan, Mustafa Ruhan Erdem, R. Murat Önok, *Teorik ve Pratik Ceza Özel Hukuku*, 13. Bası, Seçkin Yayıncılık, Ankara, 2016, s.622.

60 Dülger, *Bilişim Suçları*, s.675. Aynı görüşte bkz: Karagülmez, s.446.

61 Bu konuda ayrıntılı bilgi için bkz: Küzeci, s. 267 – 270.

62 Hakan Hakeri, "Verileri Hukuka Aykırı Olarak Verme (Sır Saklama Yükümlülüğünün İhlali) Suçu", *Tıbbi Müdahaleden Kaynaklanan Hukuki Sorumluluk Sempozyumu*, 16 – 17 Ocak 2009, Mersin Barosu Yayını, Mersin, 2009, s. 127.

63 Süheyl Donay, *Meslek Sırrının Açıklanması Suçu*, Sulhi Garan Matbaası, İstanbul, 1978, s.5; Murat Volkan Dülger, "Bankacılık Sırrı ve Sırrın Açıklanmasına İlişkin Suçlar", *Banka ve Finans Hukuku, Panel ve Seminer Notları*, İstanbul Barosu Yayınları, 2009, s. 176.

Bu nedenle sırrın korunması bu suçlarla korunan hukuksal değeri oluşturmaz. Ancak genellikle sır niteliğindeki bilgilerin aynı zamanda kişisel veri niteliğinde olması mümkündür. Aynı anda hem kişisel veri hem de sır niteliğinde olan bir bilginin bu suç tiplerinin konusunu oluşturması halinde ise "sırrın varlığı", ancak dolaylı olarak korunan hukuksal bir değer olabilir[64].

Bu suç tipleriyle korunan hukuksal değer korunan verinin niteliğinde göre değişkenlik gösterebilir. Örneğin bireyin sağlık durumuna ilişkin bir verinin bu suçların konusunu oluşturması halinde korunan hukuksal değeri kişinin sağlık hakkı oluşturur. Çünkü normal şartlarda bir birey, ancak teşhis ve tedaviden dolayı kendisi bakımından kişisel zararların, zorlukların veya utançların ortaya çıkmayacağı güveniyle hekime gider. Sağlığına ilişkin bilgilerin başkalarıyla paylaşılabileceğini düşünen kişi tedaviden kaçınabilir[65]. İkinci olarak toplumun sağlık hakkı da korunur, zira toplumun sağlığı, sağlıklı bireylere bağlıdır. Son tahlilde bu suçların konusunu sağlıkla ilgili bir verinin oluşturması halinde korunan hukuksal değeri, hem bireylerin hem de toplumun sağlık hakkı oluşturur[66]. İşte bu nedenle 6698 sayılı Yasanın 30. maddesiyle TCK'nın 135. maddesine eklenen 2. fıkra ile özel nitelikli kişisel veri olan sağlık verilerine karşı suçun işlenmesi, cezayı artıran nitelikli hal olarak düzenlenmiştir. Çünkü bu takdirde hem daha nitelikli verilere karşı suç işlendiği için suçun haksızlık içeriği daha fazla olur hem de suçun bu tür yan etkilere yol açması söz konusu olabilir, dolayısıyla daha fazla cezaya layık olma söz konusu olur.

TCK'nın 138. maddesinde ise yasal süresi dolmasına rağmen kişisel verileri sistem içinden yok etmekle görevli olan kişilerin bu görevlerini yerine getirmemeleri durumu suç haline getirilmiştir[67]. İnsanlar doğaları gereği özgür varlıklardır. Bu nedenle sürekli olarak izlenen, haklarında bilgiler toplanan ve fişlenen bireyler olarak yaşamak istemezler. İnsanlarda sürekli izlendikleri duygusunun oluşturulması, içinde bulundukları siyasal sisteme karşı bir güvensizlik ve nefret duygusu yaratabilir[68]; yani insanlar güven içinde ve özgür bir şekilde yaşamak isterler[69]. İşte yaşamlarının belli bir kesitinde hukuka uygun bir biçimde de olsa bazı kişisel bilgileri veri olarak çeşitli sistemlere girilen bireylerin bu kişisel bilgilerinin bir zaman sonra bu sistemlerden çıkartılması gerekir. Bu verilerin

64 Dülger, *Bilişim Suçları*, s. 675, 676.

65 Küzeci, s. 56.

66 Hakeri, *Verileri Hukuka Aykırı Olarak Verme*, s. 127; Yokuş Sevük, s. 794, 795.

67 Olgun Değirmenci, "Bilişim Suçları", *Yayınlanmamış Yüksek Lisans Tezi*, Marmara Üniversitesi Sosyal Bilimler Enstitüsü Hukuk Anabilim Dalı Kamu Hukuku Bilim Dalı, İstanbul, 2002, s. 157.

68 Dülger, *Bilişim Suçları*, s. 718, 719.

69 İnsanların sürekli olarak izlendikleri ve fişlendikleri ütopik bir dünyayı ve bu dünyadaki insan davranışları göstermesi açısından bkz: George Orwell, *Bin Dokuz Yüz Seksen Dört*, Çev: Nuran Akgören, Can Yayınları, İstanbul, 1999.

yok edilmesini bireyler istediği gibi devletler de istemelidir. Çünkü vatandaşları hakkında sürekli bilgi toplayan ve bunları kaydeden, kısacası vatandaşlarını fişleyen bir devlet asla çoğulcu, özgürlükçü, demokratik bir hukuk devleti olamaz ve vatandaşlarını da bu çağdaş ilkelere bağlı bir toplum haline getiremez. İşte TCK'nın 138. maddesindeki suç tipiyle bunun önüne geçilmek istenmiştir[70].

Bu bağlamda söz konusu suç tipiyle iki ayrı hukuksal değerin korunduğu görülür: Bunlardan ilki *"hem kişisel verilerin bizatihi kendisi, hem de kişisel veriler açısından istenilen güvenlik"* ikincisi ise *"kamu idaresinin güvenilirliği ve işleyişidir"*[71].

Ancak kişisel verilerin korunması kavramı ve buna ilişkin suç tipleriyle korunan hukuksal değerler yukarıda yapılan açıklamalardan daha da derinde yer alır ve bunun insan olmaya ilişkin felsefi temelleri bulunur. 20. yüzyılın bir sonucu olan bilgi toplumunun üyesi olup olmama konusunda artık bireylerin bir seçim hakkı yoktur. Kişisel verilerin bir veya birden çok merkez tarafından, etkin ve etkili bir şekilde toplanabilmesi, işlenebilmesi, yayılabilmesi ve değerlendirebilmesi bireylerin sürekli izlendikleri duygusunu taşımalarına neden olmaktadır. Teknolojinin kuşattığı modern birey adeta çırılçıplak kalmıştır ve kendine ait mahrem alanı koruyabilmek ve farklı kılıklar içinde toplumsal yaşamını sürdürmek için bir koruma alanına gereksinim duyar. İşte genel olarak kişisel verilerin korunması kavramıyla özel olarak kişisel verilerin korunmasına ilişkin suç tipleriyle korunması amaçlanan temel değer aslında budur[72].

3. Tipiklik

a. Suçların Maddi Unsurları

(1). Fail ve Mağdur

Hem 135. maddede hem de 136. maddede düzenlenen suç tiplerinde fail ve mağdur herhangi bir özellik göstermez. Suç tanımlarında suçu işleyecek kişi açısından *"kimse"* sözcüğü kullanılarak bunun dışında herhangi bir özellik belirtilmediği için herkes bu suçların faili olabilir. Aynı durum suçların mağdurları açısından da geçerlidir. Bu suçların mağduru olunması için mutlaka bilişim sistemine kaydedilen verilerin maliki veya zilyedi olunması gerekmez; önemli olan kaydedilen kişisel verilerin bireyle ilgili olmasıdır[73].

TCK'nın 138. maddesinde düzenlenen kişisel verilerin yok edilmemesi suçunda ise fail *"verileri sistem içinde yok etmekle görevli olan"* kişidir. Bu görevi ise

70 Dülger, *Bilişim Suçları*, s. 719.

71 Dülger, *Bilişim Suçları*, s. 719, 720. Aynı görüşte bkz: Karagülmez, s. 468.

72 Küzeci, s. 59; Dülger, *Bilişim Suçları*, s. 677.

73 Dülger, *Bilişim Suçları*, s. 677, 704.

konuyla ilgili özel yasalarda belirtilir; ceza yasasında haklı olarak bu görevlerin hangi yasalar tarafından belirleneceği belirtilmemiş ve genel bir ifade kullanılmıştır. Her somut olay açısından bu yasa belirlenerek, kimlere nasıl bir veri yok etme görevi verildiği araştırılmalıdır. Ayrıca bu görevli her ne kadar bu görevi kamu adına yapmaktaysa da TCK'nın 6. maddesinde tanımı verilen "kamu görevlisi" sıfatını taşımak zorunda değildir. Bu suç tipi *"özel türde, kendine özgü bir görevi ihmal suçu"* olduğu için failin kamu görevlisi olması aranmaz. Dolayısıyla kişisel verilerle ilgili olarak düzenleme yapan bir yasada kamu görevlisi olmayan kişiler için de bu tür görevler verilebilir ve bunlar da inceleme konusu suçun faili olabilirler[74]. Nitekim 5271 sayılı Ceza Muhakemesi Kanunu'nun 137. maddesinin 3. fıkrası ile soruşturma yetki ve görevinde olanlara böyle bir yükümlülük getirilmiştir. Bu alandaki esas görevlendirme ise 6698 sayılı KVKK'nın *"Kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesi"* başlıklı 7. maddesiyle yapılmıştır. Buna göre *"(1) Bu Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir. (2) Kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesine ilişkin diğer kanunlarda yer alan hükümler saklıdır. (3) Kişisel verilerin silinmesine, yok edilmesine veya anonim hâle getirilmesine ilişkin usul ve esaslar yönetmelikle düzenlenir"*. Yasa, kişisel verilerin korunmasında pek çok konuda olduğu gibi bunda da sorumluluğu *"veri sorumlusuna"* vermiştir. Veri sorumlusu ise 6698 sayılı Yasanın 3. maddesinin 1. fıkrasının (1) bendine göre *"kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişidir"*. Yani gerçek veya tüzel kişi olmasına bakılmaksızın veriyi kim kaydediyorsa, kim işliyorsa, kim saklıyorsa ya da kim aktarıyorsa veri sorumlusu odur. Buna göre verileri TCK'nın 138. maddesine göre zamanı geldiğinde silmesi gereken de bu gerçek ya da tüzel kişidir. Veri sorumlusunun tüzel kişi olması halinde, veri sorumlusunun bu konuda belirleyeceği temsilci ve/veya görevlendireceği kişi veya kişiler suçun faili olacaktır. Dolayısıyla her somut olayda fail ya da faillerin 6698 sayılı Yasadaki düzenlemeler ve bu yasaya göre çıkarılacak yönetmelik hükümleri uyarınca titizlikle belirlenmesi gerekir. Özellikle veri sorumlusu tüzel kişi olduğunda -uygulamada özellikle iş kazalarında görüldüğü üzere- hiçbir araştırma ve ayrım yapılmaksızın tüzel kişinin tüm yönetim kurulu üyeleri ve/veya üst düzey yöneticileri hakkında sanık olarak dava açılmasından kaçınılması gerekir. Özel hukuktan kaynaklanan sorumluluklar ve kabahatler hukuku bakımından

74 Dülger, *Bilişim Suçları*, s. 720.

sorumlu tüzel kişinin kendisi olabilir, ancak TCK'nın benimsediği suç teorisinde tüzel kişilerin suçun faili olması mümkün değildir. TCK, objektif sorumluluğu, dolayısıyla üçüncü kişilerin hareketlerinden sorumluluğu ve kusursuz sorumluluğu da açıkça reddetmektedir. O halde savcılara ve soruşturma makamlarına düşen görev, bu konuda üstü körü değil, detaylı ve gerçekçi bir soruşturma yaparak gerçek sorumluların bulunması ve bunlar hakkında dava açılmasıdır. Aksi takdirde uygulamada sıklıkla gördüğümüz üzere ya suçsuzlar ceza almakta (topyekun cezalandırma) ya da gerçek suçlular beraat etmektedir (topyekun beraat).

Bu suç tiplerinde hem kişilerin verileri hem de bunların yok edilmesine ilişkin toplumda idareye duyulan güven korunduğu için; hem verilerin ilgilisi bireyler hem de toplumu oluşturan her birey suçun mağduru olurlar[75].

Yukarıda 138. madde açısından yapmış olduğum fail, mağdur ve suçun konusuna ilişkin açıklamalar 6698 sayılı KVKK'nın 17. maddesinin 2. fıkrasındaki suç açısından aynen geçerlidir.

(2). Suçun Konusu

TCK'nın 135, 136 ve 138. maddelerinde düzenlenen her üç suçun da konusunu, yani suçun üzerinde işlendiği nesneyi *"kişisel veriler"* oluşturur. Kişisel verinin tanımını çalışmanın ilk bölümünde ayrıntılı olarak yaptığım için tekrardan kaçınmak adına ilgili bölüme atıf yapmakla yetiniyorum.

Bu bilgilerin bir bilişim sisteminde yer alan, kullanılan ve aktarılan dijital (sayısal) veri formunda olması şart değildir; çünkü maddenin gerekçesinde *"verilerin sanal ortamda ya da somut kağıt üzerinde kayda alınması açısından fark gözetilmediği"* belirtilmiştir. Yani bu suç tiplerindeki veri kavramı dar anlamda *"bir bilişim sisteminde ya da veri taşıma aracında bulunan ve üzerinde işlem yapılan sayısal kod halinde bilgi"* değil, geniş anlamda her formda kayıt altına alınabilen *"her türlü bilgi"*dir[76].

Ancak öğretide bu suçun konuluş amacı gözetilerek kişiye ilişkin her türlü verinin değil, ancak başkalarının duymasını, öğrenmesini istemeyeceği bilgilerin bu kapsamda değerlendirilmesini gerektiğini, dolayısıyla bu kavramın sınırlandırılmasını gerektiğini, TCK'da esasen verilerin gizli olmasının aranmadığını, verinin kişisel olmasının yeterli görüldüğünü, bununla beraber, herkes tarafından bilinen veya kolaylıkla bilinmesi mümkün olan verilerin bu kapsamda kabul etmenin maddenin kapsamını oldukça genişleteceğini belirten yazarlar bulunur[77]. Ancak bana göre çalışmamın başında belirttiğim tanımın dışına çıkılarak

75 Dülger, *Bilişim Suçları*, s. 720.

76 Dülger, *Bilişim Suçları*, s. 678; Karagülmez, s. 448.

77 Hakeri, *Verileri Hukuka Aykırı Olarak Verme*, s. 128; Yokuş Sevük, s. 796.

bu kavramın sınırlandırılmasına gerek yoktur. Çünkü bu sınırlandırmanın kime ve neye göre yapılacağı belli değildir, böyle bir sınırlama suçta ve cezada kanunilik ilkesinin alt ilkesi olan belirlilik ilkesine aykırılık oluşturabilir. Öte yandan mağdurun rızası zaten bir hukuka uygunluk nedeni olduğu için, mağdurun saklanmasında ve bilinmesinde yarar görmediği bir verinin kaydedilmesi veya verilmesi konusundaki rızası, eylemi suç olmaktan çıkaracaktır[78].

Bu kapsamda örneğin tıp hukuku bakımından, hastaya ait olup, hekim ve diğer sağlık personeline aktarılan veya herhangi bir şekilde başkaları tarafından öğrenilmesi istenilmeyen bilgilerin kişisel veri olarak kabul edilmesi gerekir. Ayrıca sadece sağlık personeline aktarılan kişisel verilerin değil, kişinin bir hekimi, hastaneyi vs. ziyaret etmesinden kaynaklanan kayıtların da bu kapsamda kabul edilmesi gerekir[79]. Bunun kapsamı her somut olayda, verinin niteliği ve verinin ilgilisinin verinin korunmasına ilişkin iradesini yansıtan hareketlere göre belirlenmelidir. Dolayısıyla soyut genel bir sınırlama değil her olayın özelliğine göre bir yorum ve gerekirse somut sınırlama yapılmalıdır[80].

Kamuya mal olmuş kişisel verilerin suçun konusunu oluşturup oluşturmayacağı incelenmelidir. Benim görüşüm, bir şekilde kamuya mal olsa da örneğin sosyal medyada sınırlı bir arkadaş grubu içinde paylaşılsa da kişisel verinin koruma altında olduğu ve TCK'daki bu alana özgü suçların konusunu oluşturacağı yönünde idi[81]. Ancak 6698 sayılı KVKK'nın istisnaların yer aldığı 28. maddesinde *"Bu Kanunun amacına ve temel ilkelerine uygun ve orantılı olmak kaydıyla veri sorumlusunun aydınlatma yükümlülüğünü düzenleyen 10 uncu, zararın giderilmesini talep etme hakkı hariç, ilgili kişinin haklarını düzenleyen 11 inci ve Veri Sorumluları Siciline kayıt yükümlülüğünü düzenleyen 16 ncı maddeleri"*nin *"İlgili kişinin kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi"* halinde uygulanmayacağı belirtilmektedir. Dolayısıyla önceki görüşümü değiştirmek için bir neden bulunmamakta, ancak ayrım yapmak gerekli. 6689 sayılı Yasanın yukarıda anılan hükmünde belirtilen ve istisnai nitelikte bir durumun bulunması halinde söz konusu alenileşmiş kişisel veri suçun konusunu oluşturmaz. Ancak alenileşmiş de olsa istisna kapsamına girmeyen veya yasanın amacına ve temel ilkelerine uygun ve orantılı olmayan bir kişisel veri işlenmesi halinde (örneğin alenileşmiş bir resmin arkadaş bulma ya da pornografi sitesinde kullanılması gibi), bu veri kişisel verilerin korunmasına ilişkin suçların konusunu oluşturmaya devam eder.

Ancak verinin ne zaman alenileştiği ne zaman aleni olmadığı her somut olayda

78 Dülger, *Bilişim Suçları*, s. 678.

79 Hakeri, *Verileri Hukuka Aykırı Olarak Verme*, s. 128.

80 Dülger, *Bilişim Suçları*, s. 678.

81 Bkz: Dülger, *Bilişim Suçları*, s. 678.

ayrı ayrı değerlendirilmelidir. Örneğin bir avukatın ya da hekimin kartvizitinde yazılı olan cep telefonu numarası alenileşmiş kabul edilip suçun konusunu oluşturmaz iken, böyle bir mesleği olmayıp cep telefonu kartvizitine bastırmayan bir kişi açısından bu bilgi kişisel veri olmaya devam edecektir. Nitekim Yargıtay cep telefonu numarasını kişisel veri olarak kabul etmekte bu görüş doğrultusunda kararlar vermektedir:

"Somut olay incelendiğinde, sanık Turgut'un, ayrıldığı kız arkadaşı olan şikayetçinin, kendisinde kayıtlı olan kişisel veri niteliğindeki telefon numarasını, şikayetçinin rızası dışında diğer sanık Onur'a verdiği olayda; şikayetçinin telefon numarasını hukuka aykırı olarak yayan sanık Turgut ile telefon numarasını hukuka aykırı olarak ele geçiren sanık Onur'un eyleminin, TCK'nın 136/1. maddesine uyan verileri hukuka aykırı olarak verme veya ele geçirme suçunu oluşturacağı gözetilmeden, ayrı ayrı mahkumiyetleri yerine, "telefon numarası vermek şeklinde gerçekleşen eylemin kişisel verilerin ele geçirilmesi ve yayılması olarak değerlendirilemeyeceği" biçimindeki isabetsiz gerekçeyle beraatlerine karar verilmesi,(BOZMAYI) gerektirmiştir"[82].

"Oluşa ve kabule göre, mağdur Arzu ile bir dönem duygusal boyutta arkadaşlık ilişkisi olması nedeniyle mağdura ait elektronik posta adresinin ve bu adresle bağlantı kurulan facebook hesabının internet şifresini bilen sanık Ahmet'in, mağdurun kendisinden ayrılması üzerine, şifresini bildiği mağdurun facebook hesabına, onun bilgisi ve rızası dışında giriş yaparak, bu hesap üzerinden, mağdura ait cep telefonunun numarasını yayımladığı olayda, Mağdurun aktif kullanımında olan, herkes tarafından bilinmeyen veya kolaylıkla ulaşılması ve bilinmesi mümkün olmayan, ancak sınırlı bir çevre ile paylaştığı cep telefonunun numarasını hukuka aykırı olarak yayan sanığın eyleminin TCK'nın 136/1. maddesinde düzenlenen verileri hukuka aykırı olarak verme veya ele geçirme suçunu oluşturduğunun kabulünde bir isabetsizlik görülmediğinden, temyiz itirazlarının reddine"[83].

(3). Eylem

i. Kişisel Verilerin Kaydedilmesi Suçu Açısından

TCK'nın 135. maddesinde düzenlenen kişisel verilerin kaydedilmesi suçuyla her türlü kişisel verinin bilişim sistemlerine ya da yazılı kayıtlara hukuka aykırı olarak yerleştirilmesi suç haline getirilmiştir. Verilerin sanal ortamda ya da fiziksel olarak kâğıt üzerinde kayda alınması açısından fark gözetilmediği maddenin gerekçesinde belirtilmiştir. Buna göre verilerin kaydedilmesi bir bilişim

82 12. CD. 7.7.2014, E. 2014/607, K. 2014/16665.

83 12. CD. 17.11.2014, E. 2014/6748, K. 2014/22909.

sistemine ya da veri taşıma aracına sayısal kod halindeki dar anlamda verilerin girilmesi şeklinde olabileceği gibi, kişisel bilgilerin bir dosya kâğıdına el yazısı ya da daktilo ile geçirilmesi şeklinde de olabilecektir[84]. Kişisel verilerin kaydedilmesi suçu serbest hareketli bir suç tipi olarak düzenlenmiştir, bu nedenle verilerin kaydedilmesi işlemi nasıl yapılırsa yapılsın sonuç değişmez ve suç gerçekleşir[85].

Kayıt etme eylemi, bir bilişim sisteminde ya da yazılı olarak bulunmayan bir bilginin sisteme girilmesi ya da yazılı hale getirilmesi şeklinde olabileceği gibi aslında başka bir kaynakta hukuka uygun olarak bulunan bir bilginin bir bilişim sistemine ya da kişisel dosyaya hukuka aykırı şekilde girilmesi suretiyle de gerçekleştirilebilecektir.

Bu konuya ilişkin örnek Yargıtay kararı şu şekildedir:

"Dosya içeriği, sanıkların ikrar içeren anlatımları, el koyma tutanağı, adli bilişim büro amirliği inceleme raporu ve fotoğraflara göre; sanıkların oturdukları apartman dairesinin giriş kapısı gözetleme deliğine, dış koridoru ve katılanın karşı dairesinin giriş kapısını görecek şekilde kamera taktırarak, ses ve görüntü kaydı yaptıkları olayda; sanıklar her ne kadar güvenlik amacıyla kamera taktırdıklarını savunmuş iseler de, kameranın, daire içinden yerleştirildiği ve dışarıdan farkedilemediği, katılanın evine girip çıkanları görüntüleyebildiği ve karşı daire kapısının açılmasıyla evin içini de görüntüleyebileceği, çekilen ses ve görüntülerin evin içindeki kayıt cihazı yardımı ile kayıt altına alındığı ve aynı anda da televizyon ile seyredildiği nazara alındığında ve güvenlik kamerasının karşı dairenin giriş kapısını ve kapı açıldığında içerisini görecek şekilde değil sanıkların kendi dairesinin kapı önünü görecek şekilde konumlandırılması gerektiği gözetildiğinde, savunmalara itibar edilemeyeceği, katılanın, gün içerisinde kiminle, nasıl, ne zaman görüştüğü, ne yaptığı, evine kimlerin gelip gittiği gibi hususları tespit etmek amacıyla, sürekli takip, denetim ve gözetim almak suretiyle gerçekleştirdikleri eylemin, özel yaşam alanına girdiğinde şüphe bulunmayan faaliyet kapsamında olduğu ve TCK'nın 134/1. maddesinin 1. ve 2. cümlelerine uyan özel hayatın gizliliğini ihlal suçunu oluşturduğu gözetilmeden mahkumiyetleri yerine, suçun nitelendirilmesinde yanılgıya da düşülerek dosya kapsamıyla uyuşmayan yazılı düşüncelerle beraat kararı verilmesi, BOZMAYI gerektirmiştir"[86].

Kişisel verilerin kaydedilmesi suçu serbest hareketli bir suç tipi olarak düzenlenmiştir; bu nedenle verilerin kaydedilmesi işlemi nasıl yapılırsa yapılsın sonuç değişmeyecek ve suç gerçekleşmiş olacaktır[87].

---

84 Aynı görüşte bkz: Karagülmez, s. 448.

85 Dülger, *Bilişim Suçları*, s. 679.

86 12. CD. 22.12.2014, E. 2014/3486, K. 2014/26247.

87 Dülger, *Bilişim Suçları*, s. 680.

Günümüzde hastaneler, adli tıp kurumu, sendikalar vb. pek çok kurum tarafından kişilerin sağlık durumları, cinsel yaşamları, DNA örnekleri ya da siyasal düşünceleri gibi özellikle gizli kalmasını isteyeceği bilgiler veri halinde kaydedilmekte ve arşivlerde bulunmaktadır. İşte bu bilgilerin yasadan ya da kişinin verdiği izinden kaynaklanmayan bir şekilde hukuka aykırı olarak bilişim sistemine kaydedilmesi bu düzenlemeyle suç haline getirilmiştir. Böylelikle ister bireyler ister kurumlar olsun, kişiler hakkındaki bilgileri sanal ortamda ya da yazılı ortamda kayda girerken ya da arşivlerken daha dikkatli davranmak zorundadırlar[88].

Verilerin, bilişim sistemine, veri taşıma aracına veya bir kağıda işlenmesiyle kaydetme işlemi de gerçekleşmiş olur. Genellikle bu veriler ya bir bilgisayar klavyesi ya da bir daktilo kullanılarak öncelikle yazıya dökülür; bilişim sistemlerinde bu yazma işleminin bitip kayıt tuşuna basıldığı, klasik yöntemde ise yazma işleminin bittiği anda suç gerçekleşmiş olur. Benzer şekilde kişinin fotoğrafının çekildiği ya da sağlık test sonuçlarının alındığı ve sisteme aktarıldığı anda eylem gerçekleşmiş olur. Buna göre her somut olayda gerçekleştirilen harekete göre suç oluşturan eylemin gerçekleşme anı değişir. Ayrıca suçun oluşması için söz konusu kişisel verilerin yayınlanması ya da başkasının kullanımına açılması gerekmez. Yalnızca verilerin hukuka aykırı olarak kaydedilmesi suçun oluşumu için yeterlidir. Suçun gerçekleşmesi için maddede ayrıca bir zararın da meydana gelmesi aranmadığı için kayıt etme işlemin gerçekleşmesiyle suç meydana gelmiş olur[89]. Dolayısıyla bu bir soyut tehlike suçudur[90].

ii. Kişisel Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme Suçu Açısından

TCK'nın 136. maddesinde düzenlenen kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçunun eylemi olarak ise üç farklı seçimlik hareket tanımlanmıştır. Bunlar kişisel verilerin başkasına verilmesi, kişisel verilerin yayılması ve kişisel verilerin ele geçirilmesi hareketleridir. Bunlardan kişisel verilerin başkasına verilmesi çok çeşitli yöntemlerle gerçekleştirilebilir. Buna örnek olarak, yazılı verilerin elden ya da posta yoluyla verilmesi veya sanal ortamda kişisel verilerin taşınabilir bellek üzerine kaydedilerek ya da internet üzerinden elektronik posta içinde ya da ekinde gönderilmesi yoluyla verilmesi gösterilebilir. Kişisel verilerin bizzat sır saklama yükümlülüğü olan ancak söz konusu kişisel veriyi öğrenmesinde bir yarar bulunmayan ya da konuyla ilgisiz olan bir başka kişiye, örneğin hastanın tedavisine katılmayan bir hekime verilmesi de suç oluşturur. Ancak sağlık personelinin kendi arasında hastanın tedavisi amacıyla

88 Dülger, *Bilişim Suçları*, s. 680.

89 Dülger, *Bilişim Suçları*, s. 680, 681; Karagülmez, s. 448.

90 Dülger, *Bilişim Suçları*, s. 681.

bilgi alışverişi için hastaya ilişkin bazı verileri birbirine aktarması 136. maddede düzenlenen verme ve yayma olarak kabul edilmemelidir[91].

Kişisel verilerin başkasına verilmesi hareketinde yer alan "başkası" gerçek kişiler olabileceği gibi tüzel kişiler de olabilecektir. Failin kişisel verileri suçun mağduru dışındaki gerçek veya tüzel bir kişiye verileri vermesi halinde suç gerçekleşmiş olacaktır[92].

Bu konuda Yargıtay'ın vermiş olduğu örnek kararlar şu şekildedir:

"Somut olayda; sanığın, eski okul arkadaşı olan mağdurun, ad ve soyadı ve fotoğrafı ile internette facebook sosyal paylaşım sitesinde mağdur adına herkese açık sahte üye profili oluşturarak, profil sayfasında mağdurun telefon numarasını yayımlaması biçimindeki eyleminin, TCK'nın 136/1. maddesine uyan, verileri hukuka aykırı olarak verme veya ele geçirme suçunu oluşturduğu gözetilmeden, suçun nitelendirilmesinde yanılgıya düşülerek, olayda uygulama yeri bulunmayan aynı Kanunun 135/1. maddesi uyarınca hüküm kurulması, (BOZMAYI) gerektirmiştir"[93].

"Somut olayda; sanığın, tamir için katılanın kendisine bıraktığı dizüstü bilgisayarında bulunan fotoğrafları ile messenger programında oturum açmak için kullandığı elektronik posta adres ve şifrelerini mesleğinin sağladığı kolaylıktan yararlanarak ele geçirip veri taşımakta kullanılan flash diske aktararak, elektronik posta adres ve şifre bilgilerini kullanarak açtığı katılana ait messenger oturumunda, kendisine ait başka bir hesabı, katılanın hesabına arkadaş olarak eklemesi, bilahare katılanın elektronik posta adresinin şifresini değiştirerek messenger programına girişini engellemesi şeklindeki eyleminin, TCK'nın 136/1. maddesinde düzenlenen verileri hukuka aykırı olarak verme veya ele geçirme suçu ile TCK'nın 244. maddesinin 2. fıkrasında düzenlenen sistemi engelleme, bozma, verileri yok etme veya değiştirme suçunu oluşturduğu ve gerçek içtima kuralları uyarınca bu suçlardan ayrı ayrı sorumlu tutularak cezalandırılması gerektiği gözetilmeden, suçun nitelendirilmesinde ya-

91 Nitekim bu suç açısından sır niteliğindeki verilerin ilgisiz kişilere verilmemesi şeklindeki yükümlülük, hekimin amirlerine, şef hekime vs. karşı da geçerlidir. Ancak bu hekimler de hastaya tıbbi müdahele uygulayarak bu sırlara ulaşırlarsa veya ulaşmak durumunda kalırlarsa, o takdirde elbette bu kimselere karşı yükümlülük söz konusu olmayacaktır. Sır saklama yükümlülüğü hastane idaresine ve idari personele karşı da geçerlidir. Dolayısıyla hastane idaresinin, hasta dosyasının tümünün idareye verilmesine yönelik talimatları hukuka aykırıdır, zira hastanın zımni rızasının bunu da kapsadığı kabul edilemez. Hekimlerin hastanede yaptıkları bütün yazışmalar kural olarak hastane idaresinden saklanmalıdır. Sadece planlama, kontrol veya güvenlik gerekçeleriyle ve ancak bu amacın gerektirdiği bilgiler idareye aktarılabilir. Hasta protokol defterine yazılan hususlar da kişisel veri kapsamında olabilir. Hakeri, *Verileri Hukuka Aykırı Olarak Verme*, s. 129.

92 Dülger, *Bilişim Suçları*, s. 706; Karagülmez, s. 451.

93 12. CD. 23.6.2014, E. 2013/26654, K. 2014/15414.

nılgıya düşülerek kişisel verilerin kaydedilmesi suçundan yazılı şekilde hüküm kurulması, (BOZMAYI) gerektirmiştir"[94].

"Sanık ve katılan arasındaki boşanma davası 01.09.2010 tarihinde açılmış olup, şikayete konu facebook hesabına, 18.10.2010-19.10.2010, 23.11.2010-01.12.2010 tarihlerinde, sanığın abonesi olduğu telefona bağlı internet aracılığıyla İstanbul'daki ortak konuttan, 25.10.2010-26.10.2010 tarihinde Ankarada'ki internet kafeden, 19.02.2011-20.02.2011 tarihinde sanığın arkadaşının sahibi olduğu otelden erişim sağlandığının belirlenmiş olması, söz konusu hesaba anılan tarihlerde sanık tarafından giriş yapıldığının sanığın da kabulünün olması, aynı tarihlerde, katılanın Malatya'da görevli olması, tanıkların, katılanın iddialarını doğrular mahiyette anlatımda bulunmaları, kendisine ait facebook hesabı bulunan katılanın, yeni bir facebook hesabı açıp, şifresini bildiği bu hesabı, aleyhine boşanma davası açtığı ve fiilen ayrı yaşadığı sanıkla beraber kullanmaya devam etmesinin, müşterek hayat tecrübeleri ve dosya içeriği nazara alındığında, katılandan beklenen bir davranış biçimi olarak kabul edilemeyecek olması karşısında, sanığın, söz konusu hesabı ve hesaba ait şifreyi katılanla birlikte oluşturduklarına dair kendisini cezalandırılmaktan kurtarmaya yönelik, inandırıcılıktan uzak, soyut savunmalarına itibar edilemeyeceği, katılanın, özde değişmeyen, maddi delillerle ve tanıkların anlatımlarıyla da doğrulanan iddialarına üstünlük tanınarak, mevcut olan delillerin, iddiaya konu eylemi gerçekleştirenin sanık olduğunu açık ve net olarak ortaya koyduğu gözetilip, katılanın kişisel bilgilerini ve fotoğraflarını, belirli olmayan ve birden fazla kişi tarafından algılanabilme imkanı bulunan facebook adlı sosyal paylaşım sitesinde, hukuka aykırı olarak yayan sanığın, üzerine atılı TCK'nın 136/1. maddesindeki verileri hukuka aykırı olarak verme veya ele geçirme suçunun sübut bulduğunun kabul edilmesi gerekirken, delillerin takdirinde yanılgıya düşülerek, oluşa ve dosya kapsamına uygun düşmeyen yazılı gerekçelerle, sanık hakkında beraat kararı verilmesi, (BOZMAYI) gerektirmiştir"[95].

Kişisel verilerin yayılması da çok çeşitli şekillerde gerçekleştirilebilir. Bu; kişisel verilerin yazılı olarak mektup şeklinde birden fazla kişiye gönderilmesiyle gerçekleştirilebileceği gibi, internet üzerinden bir web sitesinde kişisel verileri başkaları için erişilebilir kılmak ya da bir forumda açıklamak suretiyle de gerçekleştirilebilir. Kişisel verilerin bir tek kişiye verilmesi veya açıklanması suçun oluşması açısından yeterlidir, herkesin öğrenmesi gerekmez[96]. Kişisel verilerin

94 12. CD. 7.4.2014, E. 2013/15899, K. 2014/8411.

95 12. CD. 22.9.2014, E. 2014/883, K. 2014/18388.

96 Hakeri, *Verileri Hukuka Aykırı Olarak Verme*, s. 129.

yayılması eylemi yazılı, görsel ya da sanal basın yoluyla da yapılabilir[97]. Verileri yaymadan kastedilen verilerin içeriğinin birçok kişinin öğrenebileceği şekilde başkalarının bilgisine sunulmasıdır; yaymaya örnek olarak kişisel verilerin bir yayında kimlik belirtmek suretiyle yayınlanması da gösterilebilir[98].

Bu suç tipinin üçüncü seçimlik hareketi olan kişisel verilerin ele geçirilmesi ise kişisel verilerin üzerinde yazılı olduğu belgelerin bulunduğu yerden alınması suretiyle meydana getirilebileceği gibi, verilerin kayıtlı olduğu bilişim sistemine girilerek verilerin bir depolama cihazına kaydedilmesi ve bu cihazın alınması yoluyla da yapılabilir[99].

Maddenin gerekçesinde de belirtildiği gibi başkasına verilen, yayılan ya da ele geçirilen verilerin hukuka uygun olarak kaydedilmiş olup olmamasının suçun oluşumu açısından bir etkisi bulunmaz. Verilerin nasıl kaydedildiği önemli olmaksızın yukarıda sayılan hareketlerin gerçekleştirilmesiyle eylem unsuru gerçekleşmiş olur. Bu suç tipi seçimlik hareketli bir suçtur; suçun maddi unsuru olarak yasada belirtilen kişisel verilerin başkasına verilmesi, yayılması ya da ele geçirilmesi hareketlerinden biri ya da bir kaçının aynı anda gerçekleştirilmesi durumunda tek bir suç işlenmiş olur ve faile tek suçun cezası verilir.

Bu suçun oluşması için failin yaptığı hareketlerin neticesinde bir zararın meydana gelmesi gerekmez. Yasanın metninin açık ifadesinden bunun bir soyut tehlike suçu olduğu anlaşılır, çünkü TCK'nın 136. maddesinde hareketler "veren, yayan ve ele geçiren" şeklinde gösterilmiş ancak bunların sonucunda bir zararın ortaya çıkması aranmamıştır. Burada özellikle belirtilmesi gereken konu "kişisel verilerin ele geçirilmesi" hareketi açısından yalnızca "öğrenmenin" ele geçirmek anlamına gelip gelmeyeceğidir. Bana göre yalnızca öğrenme eylemi, ele geçirme olarak kabul edilemez, dolayısıyla bu suç tipinde yer alan hareket tanımını karşılamaz. Örneğin tıp profesörü olan doktoru hastasına ilişkin teşhis ve tedaviyi içeren kayıtları öğrencilerine ders verdiği dokümanların arasında unutması, hocanın asistanının da dokümanları incelerken hastaya ait belgeleri görmesi ve durumu öğrenmesi halinde ele geçirme söz konusu olmaz[100].

iii. Kişisel Verilerin Yok Edilmemesi Suçu Açısından

Yasanın 138. maddesinde düzenlenen kişisel verilerin yok edilmemesi suçunun işlenebilmesi için öncelikle hukuka uygun olarak kaydedilmiş bir verinin söz konusu olması gerekir. Zira verilerin yok edilmemesi suçunun gerçekleşebilmesi

97 Dülger, *Bilişim Suçları*, s. 713.
98 Hakeri, *Verileri Hukuka Aykırı Olarak Verme*, s. 129.
99 Dülger, *Bilişim Suçları*, s. 713.
100 Dülger, *Bilişim Suçları*, s. 714.

için öncelikle *"kanunların belirlediği sürelerin geçmiş olması"* gerekir. Suç tipinin düzenlendiği maddenin başlangıcında yer alan bu ifade karışıklıklara yol açabilecek niteliktedir. Bu ifadeden kişisel verilerin sistemde kayıtlı olmasına izin verilen süre mi yoksa görevli kişiye verileri silme görevini yerine getirmesi için öngörülen süre mi anlaşılmalıdır? Görüldüğü üzere bu, sürenin belirlenmesi ve dolayısıyla suçun oluşumu açısından yanıtlanması gereken önemli bir sorudur.

Bu maddenin gerekçesinde yasa koyucunun amacını belirten bir açıklama bulunmamaktadır; ancak yasa koyucunun gereksiz bir düzenleme yapmayacağı düşüncesinden hareketle bu soruya verilecek yanıt, söz konusu süreyle kişisel verilerin sistemde kayıtlı olmasına izin verilen sürenin kastedildiğidir. Çünkü görevliye kişisel verileri yok etmesi bir başka deyişle görevini yerine getirmesi için öngörülen süre, yasa ile verilebileceği gibi bu konuyla ilgili bir yönetmelikle de verilebilir; hatta bu konuda açık bir süre belirtilmeyip amirin bu konudaki emrinden sonra makul bir süre geçmesi beklenebilir. Buna göre yasada belirtilen süre, kişisel verilerin sistemde kayıtlı olmasına izin verilen süredir. Bu sürenin dolmasından sonra veriler silinmiyorsa söz konusu ihmali hareket suçun eylem unsurunu oluşturmaktadır[101]. Örneğin Sağlık Bakanlığı tarafından yayınlanan "Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik'in" kişisel sağlık verilerinin silinmesi başlıklı 9. maddesinin 3. fıkrasında *"Merkezi sağlık veri sistemine aktarılan veriler, aktarımın yapıldığı tarihten 10 yıl sonra yerel veri tabanından silinebilir."* denilmek suretiyle bu süre açıkça belirtilmiştir. Buna göre anılan sürenin geçmesine rağmen sağlık verilerinin silinmemesi halinde, kişisel sağlık verilerini silmek yetkili olan görevliler ihmal suretiyle bu suçu işlemiş olurlar.

Bu konuda yanıtlanması gereken bir diğer soru ise suç tanımında geçen *"kanun"* sözcüğünden neyin anlaşılması gerektiğidir. Bunun dar yorumlanarak yalnızca teknik anlamda TBMM tarafından çıkarılan *"yasa"* niteliğindeki hukuk normlarının anlaşılması halinde suç tipinin uygulama alanı gereksiz yere oldukça daraltılmış olur. Dolayısıyla bu sözcükten tüzük, yönetmelik, yönerge gibi genel düzenleyici işlem niteliğindeki yazılı hukuk normları da anlaşılmalıdır[102]. Ancak suçta kanunilik ilkesi ve genişletici yorum yasağı gereğince gelebilecek eleştirilere maruz kalmamak için maddenin yazılı hukuk kuralları olarak değiştirilmesi daha uygun bir çözüm olacaktır[103].

TCK'nın 138. maddesinde düzenlenen verileri yok etmeme suçu, failin görevinin gereği olan işlemi, yani verilerin sistemden yok edilmesi işlemini yapma-

101 Dülger, *Bilişim Suçları*, s. 721, 722.
102 Karagülmez, s. 469.
103 Dülger, *Bilişim Suçları*, s. 722.

masıyla işlenebilir. Verilerin yok edilmesinin nasıl gerçekleştirileceği ise söz konusu görevin verildiği yasa ya da yönetmelikte gösterilmelidir. Çünkü verilerin sistemden yok edilmesi çok çeşitli şekillerde olabilir. Örneğin veriler yazılı halde bulunuyorsa yakmak suretiyle ya da veriler bir bilişim sisteminde sanal veri olarak bulunuyorsa bunların silinmesi ya da verilerin üzerinde bulunduğu taşınabilir bellek, cd ya da sabit diskin kırılması suretiyle verilerin yok edilmesi görevi yerine getirilebilir[104]. Nitekim 6698 sayılı KVKK'da da bu açıklamalarıma paralel bir düzenleme yapılmıştır. Yasanın *"Kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesi"* başlıklı 7. maddesinde kişisel verilerin silinmesi genel olarak tanımlandıktan sonra verilerin nasıl silineceği yönetmeliklere bırakılmıştır. Buna göre: *"(1) Bu Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir. (2) Kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesine ilişkin diğer kanunlarda yer alan hükümler saklıdır. (3) Kişisel verilerin silinmesine, yok edilmesine veya anonim hâle getirilmesine ilişkin usul ve esaslar yönetmelikle düzenlenir"*.

Verileri yok etmeme suçu ihmali hareketle gerçekleştirilir. Yasaların belirlediği süre sonunda, eğer bu yasalarda verilerin yok edilmesi için belirli bir süre öngörülmüşse bu süre içinde, eğer böyle bir süre öngörülmemişse işin niteliğine göre makul bir süre içerisinde verileri yok etme eyleminin gerçekleştirilmesi gerekir. Bu sürelerin geçmesine rağmen hala verilerin yok edilmemesi durumunda ise suç gerçekleşmiş olur. Bunun dışında verileri yok etmekle görevli kişinin açıkça bu işlemi gerçekleştirmeyeceğini söylemesi ya da bunun bir emirle kendisine bildirilmesine rağmen amirinin emrini yerine getirmeyeceğini ifade etmesi halinde de bu sürelerin geçmesine gerek olmaksızın suç gerçekleşmiş olacaktır[105].

Ancak suçun gerçekleşmesi için mutlaka bir hukuk normunda verilerin kayıtlı tutulacağı sürelerin ve bu sürenin sonunda verinin yok edilmesi gerektiğinin açık ve anlaşılabilir bir biçimde düzenlenmiş olması gerekir. Yazılı hukuk normunda verinin sınırlı süreyle kayıtlı tutulacağının belirtilmesi ve sürenin bitiminin belirgin olması yeterli ve gereklidir. Böyle bir süre ve kişisel verinin yok edilmesini emreden bir düzenlemenin bulunmaması halinde TCK'nın 138. maddedeki suçun işlerlik kazanması mümkün değildir. Örneğin 5271 sayılı Ceza Muhakemesi Kanunu'nun 37. maddesinin 3. fıkrasında yer alan *"135'inci maddeye göre verilen kararın uygulanması sırasında şüpheli hakkında kovuşturmaya yer olmadığına dair karar verilmesi ya da aynı maddenin birinci fıkrasına göre hakim onayı-*

104 Dülger, *Bilişim Suçları*, s. 722.

105 Dülger, *Bilişim Suçları*, s. 722.

nın alınamaması halinde, bunun uygulanmasına Cumhuriyet savcısı tarafından derhal son verilir. Bu durumda, yapılan tespit veya dinlemeye ilişkin kayıtlar Cumhuriyet savcısının denetimi altında en geç on gün içinde yok edilerek, durum bir tutanakla tespit edilir" düzenlemesinde elde edilen bilgilerin yok edilmesi için belirli bir süre öngörülmüştür. Elde edilen bu bilgilerin içinde kişisel verilerin yer alması ve diğer şartların gerçekleşmesi neticesinde öngörülen sürenin sonunda bu verilerin yok edilmemesi halinde 138. madde tanımlı olan suç gerçekleşmiş olur[106].

Verileri yok etmeme suçu açısından ayrıca bir netice aranmaz. Söz konusu ihmali hareketin yapılmasıyla suç gerçekleşmiş olur. Dolayısıyla bu suç, zarar suçu olmadığı gibi soyut tehlike suçudur.

iv. 6698 sayılı KVKK m.17/2'de Düzenlenen Kişisel Verilerin Silinmemesi veya Anonim Hale Getirilmemesi Suçu Açısından

6698 sayılı KVKK'nın 17. maddesinin 2. fıkrası gereğince *"Bu Kanunun 7 nci maddesi hükmüne aykırı olarak; kişisel verileri silmeyen veya anonim hâle getirmeyenler 5237 sayılı Kanunun 138 inci maddesine göre cezalandırılır"*. Yasanın 7. maddesinde ise yukarıda da belirttiğimiz üzere kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesinden veri sorumlusunun yükümlü olduğu belirtilmektedir. Veri sorumlusunun niteliği ise Yasanın 3. maddesinin 1. fıkrasının (ı) bendinde düzenlenmiştir. Buna göre suç tipi anılan maddeler ve atıflar birlikte okunduğunda şu tipi şu şekilde olmalıdır:

"6698 sayılı Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebepleri ortadan kalkan kişisel verilerin resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinmemesi, yok edilmemesi veya anonim hâle getirilmemesi halinde veri sorumlusu gerçek kişi ise bu kişiye, tüzel kişi ise yetkili ve görevli organ ve/veya temsilcilerine bir yıldan iki yıla kadar hapis cezası verilir."

Öncelikle ifade etmeliyim ki bu suç, TCK m.138'de düzenlenen suça benzer ancak farklı bir suç tipidir. Eğer yasa koyucu 6698 sayılı Yasanın 7. maddesine aykırılık halinde suçun tüm unsurları ile birlikte 138. maddenin uygulanmasını isteseydi "*5237 sayılı Kanunun 138 inci maddesi uygulanır"* ifadesini kullanırdı. Oysa yasa koyucu bunu yapmamış, 6698 sayılı KVKK'nın 17/2, 7 ve 3. maddelerinin birlikte uygulanmasıyla farklı bir suç tipi oluşturmuş ve "*5237 sayılı Kanunun 138 inci maddesine göre cezalandırılır"* ifadesini kullanmak suretiyle yalnızca yaptırım açısından TCK'nın 138. maddesinin uygulanacağını belirtmiştir. Dolayısıyla söz konusu düzenlemenin bu şekilde anlaşılması ve buna göre yorum yapılması gerektiği düşüncesindeyim.

106 Karagülmez, s. 469, 470.

Eylem unsuru açısından bu suç, ihmali hareketle işlenir ve seçimlik hareketlidir. Seçimlik hareketler *yok etmemek*, *silmemek* ve *anonim hale getirmemek*tir. Bunlardan yok etmemenin ve silmemenin nasıl gerçekleştirileceği 6698 sayılı Yasada tanımlanmamıştır. Yok etmemek hareketi TCK'nın 138. maddesinde de suçu oluşturan hareket olarak tanımlandığı ve bu suçtakiyle aynı anlamda kullanıldığı için anılan maddeye ilişkin yapmış olduğum açıklamalara atıfta bulunuyorum.

Silmek sözcüğü bilişim terimi olarak *"bir ya da birden çok bellek yerinin genellikle sıfır ya da boşluk damgası ile gösterilen, belirli bir duruma getirilmesi"* olarak tanımlanır. Yani ilgili verinin, verilerin nerede tutulduğunu gösteren fihristten / aktif dizinden (active directory) bağlantısının kaldırılması ya da verinin üzerine bir başka verinin yazılması kısacası erişilmek istenilen veriye erişim olanağının ortadan kaldırılması (veri kurtarma yöntemlerine başvurmaksızın erişilebilirliğin kaldırılması) halinde silme hareketi gerçekleşir. İşte failin bu hareketi, bunu yapmaya yönelik bir yükümlülüğünü bulunmasına rağmen yapmaması halinde silmemek hareketi meydana gelir.

Anonimleştirmek ise 6698 sayılı KVKK'nın 3. maddesinin 1. fıkrasının (b) bendinde tanımlanır. Buna göre anonim hâle getirme, *"kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesi"*dir. Dolayısıyla bu işlemi yapmakla yükümlü olan kişinin, kişisel verileri gerçek kişiyle ilişkilendirilemeyecek hale getirmemesi halinde bu hareket söz konusu olur. Anonimleştirme halinde elde kalan istatistiki bilgidir; bu bilginin tıbbi, finansal ya da kriminolojik çalışmalarda kullanılması mümkündür ve suç oluşturmaz, zira belli bir kişiyi göstermez.

Kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesi yükümlülüğü genel olarak 6698 sayılı KVKK'nın 7. maddesiyle veri sorumlusu gerçek ve tüzel kişilere getirilmiştir. Kanunumuzun kabul ettiği suç teorisine göre tüzel kişiler suçun faili olamayacağına göre veri sorumlusu tüzel kişiler açısından bu işlemden kimin ya da kimlerin sorumlu olduğunun açıkça belirlenmesi gerekir. TCK'nın 138. maddesi açısından yapmış olduğum açıklamalar bu madde için de geçerlidir. KVKK'nın 7. maddesinin 1. fıkrasına göre kanun hükümlerine uygun olarak işlenmiş ancak işlenmesini gerektiren sebepler ortadan kalkmış kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinmeli, yok edilmeli veya anonim hâle getirilmelidir. Aynı maddenin 2. fıkrasıyla bu hususlara ilişkin diğer kanunlarda yer alan hükümlerin saklı olduğu düzenlenmiştir. 3. fıkrada ise kişisel verilerin silinmesinin, yok edilmesinin veya anonim hâle getirilmesinin yönteminin çıkarılacak yönetmeliklerle düzenleneceği belirtilmiş-

tir. Dolayısıyla bu suçun oluşması için ihlal edilmesi gerekli olan yükümlülük KVKK'nın 7. maddesi ve ilgili yönetmeliklerle belirlenecektir.

(4). Suçların Nitelikli Halleri

TCK'nın 135. maddenin 2. fıkrasında suçun "nitelikli kişisel veriler" hakkında işlenmesi cezayı artıran nitelikli hal olarak düzenlenmiştir. Bilişim Suçları ve İnternet İletişim Hukuku isimli kitabımın 6698 sayılı Yasanın yürürlüğe girmesinden önce yapılan tüm basılarında bu konuyu eleştiri konusu yapmıştım[107]. Nihayet Avrupa Siber Suç Sözleşmesine uyumluluk için TCK'da ve CMK'da yapılması gereken düzenlemeler için Adalet Bakanlığı Kanunlar Genel Müdürlüğü tarafından oluşturulan ve benim de yer alarak bu madde ve diğer başka maddelere ilişkin düşüncelerimi paylaştığım bir komisyon tarafından hazırlanan metin üzerine, 6698 sayılı Yasanın 30. maddesiyle TCK'da çeşitli değişiklikler yapılarak bu ve benzeri hatalı hükümler değiştirilmiş ve olması gereken bazı hükümler eklenmiştir.

6698 sayılı Yasanın 30. maddesiyle TCK'nın 135. maddesinin 2. fıkrasında yapılan değişiklikle, söz konusu fıkra *"kişisel verinin, kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması durumunda birinci fıkra uyarınca verilecek ceza yarı oranında artırılır"* haline getirilmiştir. Böylelikle hüküm olması gerektiği hale getirilmiş ve 6689 sayılı Yasanın 3. Maddesinde özel nitelikli kişisel veriler olarak tanımlanan kişisel verilere karşı hukuka aykırı kaydetme suçunun işlenmesi cezayı artıran nitelikli hal olarak düzenlenmiştir. Anılan kişisel verilerin niteliği gereği bunlara karşı işlenen suçun haksızlık içeriğinin daha fazla olması nedeniyle suçun cezasının artırılması yoluna gidilmiştir.

Bu fıkrada yer alan konulardan örneğin sağlık durumu bilgisi, bir kişiye yönelik olarak değil *"x bölgesinde ... hastalığı yaygındır"* şeklinde anonim veri olarak kaydedilmişse yani istatistiki bir bilgi niteliğinde ise bu fıkraya göre suç oluşmaz. Çünkü bu durumda bilgi, kişisel veri niteliğinde kayıt edilmemiştir[108].

---

107 "Meclis alt komisyonu tarafından kabul edilen ceza yasası tasarısında bu nitelikli kişisel verilerin suçun konusunu oluşturması hali cezanın artırılmasına neden olan nitelikli hal olarak öngörülmüştü. Ancak Adalet Komisyonu tarafından genel kurula gönderilen ve genel kurulda kabul edilerek yasalaşan metinde nitelikli kişisel verilerin suçun konusunu oluşturması hali cezayı artıran nitelikli hal olarak öngörülmemiştir. Bu durumda söz konusu verileri ayrıca belirtmenin de yasa yapma tekniği açısından bir anlamı kalmamıştır. Oysaki alt komisyonda kabul edilen metinde olduğu gibi bu verilerin suçun konusunu oluşturması halinin cezayı artıran nitelikli hal olarak öngörülmesi daha yerinde bir düzenleme olacaktı". Dülger, *Bilişim Suçları*, s. 681, 682.

108 Karagülmez, s. 447.

TCK'nın 137. maddesinde "nitelikli haller" başlığı altında özel hayata ve hayatın gizli alanına karşı suçlar bölümünde yer alan suçlar için failin sıfatından kaynaklanan cezayı artırıcı nitelikli haller öngörülmüştür. 137. maddenin "a" bendine göre 135. ve 136. maddelerde düzenlenen suçların bir kamu görevlisi tarafından ve görevinin verdiği yetkinin kötüye kullanılması suretiyle işlenmesi halinde failin cezası artırılarak verilecektir. TCK açısından kamu görevlisinin tanımı 6. maddenin "c" bendinde verilmiştir. Buna göre *"kamu görevlisi deyiminden; kamusal faaliyetin yürütülmesine atama veya seçilme yoluyla ya da herhangi bir surette sürekli, süreli ya da geçici olarak katılan kişi"* anlaşılacaktır. Bu bağlamda örneğin sağlık personeli açısından hemen bütün olaylarda bu nitelikli halin gerçekleşmesi söz konusu olabilecektir[109]. Benzer şekilde yaptığı görevinin niteliği gereği bazı durumlarda ceza hukuku açısından kamu görevlisi sayılan avukatın, görevi gereği bulundurduğu ve/veya işlediği bir kişisel veriyi veri sahibinin açık rızası olmadan veya kanunların kendisine verdiği yetkinin dışında açıklaması ya da üçüncü bir kişiye vermesi halinde suçun nitelikli hali oluşur.

137. maddenin "b" bendine göre ise belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle bu suçun işlenmesi halinde faile cezası yine artırılarak verilir. Burada geçen "belli bir meslek ve sanat" kavramından kişisel veri kaydeden, işleyen ve aktaran her türlü iş kolu anlaşılabilir; bunun içine özellikle sağlık/medikal, finans, sigorta, perakende, her sektörün insan kaynakları ve bilişim sektörü girebilir. Buna göre söz konusu nitelikli hallerden herhangi birisinin gerçekleşmesi halinde faile verilecek ceza yarı oranında artırılır. Yukarıdaki örnekten devam edersek, avukatın kamu görevlisi sıfatıyla hareket etmediği bir esnada, örneğin hukuki bir konu ile ilgili kitap ya da makale yazarken, avukat olmasının sağladığı kolaylıkla görev üstlendiği davalardaki kişilerin kişisel verilerini bu çalışmaya alması halinde bu nitelikli hali oluşur.

TCK'nın 138. maddesine 21.2.2014 tarih ve 6526 sayılı Yasanın 5. maddesiyle eklenen ikinci fıkra ile *"Suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması hâlinde verilecek ceza bir kat artırılır"* hükmü getirilmiştir. Böylelikle verilerin yok edilmemesi suçu için cezayı artıran nitelikli bir hal öngörülmüştür. Örneğin 5271 sayılı Ceza Muhakemesi Kanunu'nun 137. maddesinin 3. fıkrasında yer alan *"135'inci maddeye göre verilen kararın uygulanması sırasında şüpheli hakkında kovuşturmaya yer olmadığına dair karar verilmesi ya da aynı maddenin birinci fıkrasına göre hakim onayının alınamaması halinde, bunun uygulanmasına Cumhuriyet savcısı tarafından derhal son verilir. Bu durum-*

109 Hakeri, *Verileri Hukuka Aykırı Olarak Verme*, s. 131.

da, yapılan tespit veya dinlemeye ilişkin kayıtlar Cumhuriyet savcısının denetimi altında en geç on gün içinde yok edilerek, durum bir tutanakla tespit edilir" düzenlemesinde elde edilen bilgilerin yok edilmesi için belirli bir süre öngörülmüştür. Elde edilen bu bilgilerin içinde kişisel verilerin yer alması ve diğer şartların gerçekleşmesi neticesinde öngörülen sürenin sonunda bu verilerin yok edilmemesi halinde 138. maddede tanımlı olan suç gerçekleşmiş olur[110] ve söz konusu nitelikli hal gereğince suçun cezası artırılarak verilir. Bu düzenlemeyi olumlu bulduğumu ve soruşturma makamlarını görevlerini ihmal etmemeleri ve/veya kötüye kullanmamaları noktasında dikkatli davranmaya yönelteceğinde etkili olacağını düşündüğümü ifade etmeliyim.

Suçun nitelikli halleri açısından karşımıza çıkan bir diğer soru, 6698 sayılı KVKK'nın 17. maddesinin 2. fıkrası gereğince *"Bu Kanunun 7 nci maddesi hükmüne aykırı olarak; kişisel verileri silmeyen veya anonim hâle getirmeyenler 5237 sayılı Kanunun 138 inci maddesine göre cezalandırılır"* hükmünün, 138. maddenin 2. fıkrasında yer alan suçun nitelikli halini kapsayıp kapsamadığıdır. Hükümde cezalandırma için fıkra ayrımı yapılmaksızın 138. maddenin uygulanacağının ifade edilmesi ve suçun nitelikli halinin de cezalandırmaya ilişkin bir hüküm olması nedeniyle teorik olarak KVKK'nın 17. maddesinin 2. fıkrasında yer alan suç açısından 138. maddenin 2. fıkrasının uygulanabileceğini düşünüyorum. Ancak uygulamada soruşturma makamı olan savcılık ve onun yardımcısı olan kolluk güçleri ile kovuşturma makamı olan mahkemeler ve hakimlikler kişisel veri kaydetme vb. işlemleri özellikle CMK ve diğer yasalardan aldıkları yetki uyarınca gerçekleştirirler. Bu şekilde soruşturma veya kovuşturma amacıyla kişisel veri kaydedilmesi ya da işlenmesi ise 6698 sayılı Yasanın 28. maddesinin 1. fıkrasının (d) bendi uyarınca 6698 sayılı Yasanın uygulama kapsamı açısından istisna tutulmuştur. Dolayısıyla TCK'nın 138/2. maddesinde belirtilen kişisel veriler 6698 sayılı Yasanın istisnasını oluştururlar. O halde hukuka uygun olarak soruşturma veya kovuşturma için kişisel veri kaydeden ya da işleyen makamların, bunların yok edilmesi için öngörülen süre geçmesine rağmen bunu yapmamaları halinde bunlar hakkında 6698 sayılı Yasanın 17. maddesinin 2. fıkrasının atfıyla TCK'nın 138. maddesinin 2. fıkrası değil, gerçekleştirdikleri ihmali hareket sadece TCK'nın 138. maddesinin 1. fıkrasını ihlal ettiği için bunun nitelikli hali olan 138. maddenin 2. fıkrası doğrudan uygulanmalıdır. Bu durum sonuç cezayı etkilememekle beraber, hükümlerin doğru belirlenmesi ve hukuka uygunluğun sağlanması için gereklidir; dolayısıyla böyle bir durum söz konusu olduğunda davanın bu maddeden açılması ve ispat gerçekleşirse hükmün de bu maddeden kurulması gerekir.

110 Karagülmez, s. 470.

b. Suçların Manevi Unsurları

İnceleme konusu dört suçun da manevi unsurunu kast oluşturur. TCK'da ya da KVKK'da manevi unsur açısından başkaca bir özellik aranmamıştır. Suçların işlenmesi için kast aranması ve bu konuda başka bir özellik belirtilmemesi nedeniyle bu suçların taksirle işlenmesi mümkün değildir[111].

4. Hukuka Aykırılık Unsurları

a. TCK'nın 135. ve 136/1 Maddelerindeki "Hukuka Aykırı Olarak" İfadesinin Hukuki Niteliği

Öğretide benim de katıldığım azınlıkta olan görüşe göre, bazen suç tipinde bu ve buna benzer kavramların, hukuka uygunluk nedenin yokluğuna işaret etmek üzere, gereksiz kullanıldığı, burada yasa koyucunun, yargıcı, hukuka uygunluk nedenlerinin varlığı konusu üzerinde hassasiyetle durması konusunda uyardığı ancak bu tür bir hukuka aykırılığın failin kastının kapsamında olmasının da gerekmediği, dolayısıyla bunun suç tanımına ait olmadığı ifade edilmektedir. Nitekim TCK'nın 135. ve 136/1 maddelerindeki suçlarda *"hukuka aykırı olarak"* ifadesi bu anlamda kullanılmıştır[112]. Dolayısıyla benim kabul ettiğim görüşe göre suç tanımında yer alan bu ifadenin özel bir anlamı olmayıp, bunlar suç tipine dahil değildir. Gerçekten de uygulamada, böyle bir ifadenin yer aldığı suç tipine ilişkin herhangi bir yargılamada, pek çok ispat zorluğunun yanında iddia makamına ve yargıca bir de failin hukuka aykırı olarak hareket ettiğinin özellikle ispatlanması külfetinin yüklenmesi söz konusu yargılamaları kilitleyecektir. Nitekim bu tür suçlara ilişkin yargılamada hiçbir zaman failin özellikle hukuka aykırı olarak hareket ettiğinin ispatlanmasına ilişkin bir çalışma yapılmamakta, bu tür bir ifadeyi içeremeyen diğer suçlarda olduğu gibi, hukuka aykırılık bir karine olarak kabul edilmekte, bir hukuka uygunluk sebebinin varlığının söz konusu olması halinde ise bu durum araştırılmaktadır. Zira tipiklik hukuka aykırılığın karinesidir, tipik eylem gerçekleşmişse, hukuka aykırılığın da gerçekleşmiş olduğu kabul edilir, bunun ayrıca ispatına gerek yoktur. Bunun aksine bir hukuka uygunluk nedeni varsa (ki bu da kasta dahildir) söz konusu hukuka uygunluk nedeninin kendine özgü şartları ve failin bunu bilerek hareketini gerçekleştirdiği ispat edilmelidir.

Kişisel verilerin kaydedilmesi suçunun düzenlendiği 135. maddenin 2. fıkrasında nitelikli kişisel veriler ayrıca düzenlenirken *"kişilerin siyasi, felsefi veya dinsel görüşlerine ve ırksal kökenlerine"* ilişkin verilerin kaydedilmesi eylemi açısından failin yaptığı eylemin hukuka aykırı olduğunu bilmesi hali ayrıca aran-

111 Dülger, *Bilişim Suçları*, s. 681; Hakeri, *Verileri Hukuka Aykırı Olarak Verme*, s. 129; Yokuş Sevük, s. 801.

112 Hakan Hakeri, *Ceza Hukuku Genel Hükümler*, 19. Bası, Adalet Yayınevi, Ankara, 2016, s.241.

mamıştır. Düzenlemenin bu şekli dahi 1. fıkrada kullanılan *"hukuka aykırı olarak"* ibaresinin gereksiz yere kullanıldığını gösterir. Ancak diğer görüşü savunan yazarlar, 2. fıkrada yasa koyucunun failin hukuka aykırılık bilinciyle hareket edip etmediğinin araştırılmasını gereksiz bulduğunu, failin bu durumda hukuka aykırı olarak hareket ettiğini kabul ettiğini; buna göre failin hareketinin bitmesiyle suçun gerçekleşmiş olacağını ve artık yargılama esnasında failin hukuka aykırı bir eylem yaptığını bilerek hareket ettiğinin ayrıca ispat edilmesinin gerekmediğini ifade etmektedirler[113]. Yukarıda da belirttiğim üzere ben bu görüşe katılmıyorum.

b. Kişisel Verilerin Kaydedilmesi Suçu Açısından

Kişisel verilerin kaydedilmesi suçunda mağdurun rızası ya da yasayla verilen yetki eylemi hukuka uygun hale getirir. Kişinin, verinin sahibi ya da ilgilisi tarafından verilen bir izne dayanarak verileri kaydetmesi ya da verileri kaydetmekle görevli bir kişinin yasadan aldığı yetkiye dayanarak aynı eylemi gerçekleştirmesi durumunda suç oluşmaz.

(1). Mağdurun Rızası

i. Rızanın Bulunması Gereken An ve Şekli

Mağdurun rızasına dayanan hukuka uygunluk sebebinde rızanın suçun işlendiği anda mevcut bulunması gerekir; ayrıca bu rızanın açık ya da zımni şekilde verilmesi özellik arz etmez, her iki şekilde verilen rıza da geçerlidir. Kişinin banka görevlisinin uzattığı "müşteri hakkında bilgi edinme formunu" doldurması halinde izin verilmiş kabul edilmelidir. Ancak 6698 sayılı Yasa ile bu yasanın kapsamında işlenen kişisel veriler için –istisnalar dışında– veri ilgilisinin açık rızası arandığı ve yasanın 17. maddesiyle kişisel verilere ilişkin suçlar bakımından TCK'nın 135-140. maddelerinin uygulanacağı belirtildiği için; 6698 sayılı Yasanın uygulamasına giren kişisel veriler için, yine bu yasayla açık rızanın aranmasının gerekmediği istisnai haller dışında, verinin işlenmesi (kaydedilmesi, kopyalanması, aktarılması vs.) veri ilgilisinin açık rızası gerekir. Dolayısıyla 135 ve 136. maddelere göre hukuka uygunluk nedenin varlığının tespiti bakımından bu sınırlamalar dahilinde açık rızanın var olup olmadığı her somut olay açısından değerlendirilmelidir. 6698 sayılı Yasaya tabi olmayan ya da istisnalara tabi olan kişisel veriler açısından ise zımni rıza geçerli olacaktır.

ii. Kişisel Verinin Veri İlgilisi Tarafından Alenileştirilmiş Olması

Kişisel veriler, kişinin üzerinde mutlak surette üzerinde tasarruf edebileceği haklardandır[114]. Ben, Bilişim Suçları ve İnternet İletişim Hukuku isimli ki-

113 Benzer görüşte: Karagülmez, s. 448.

114 Karagülmez, s. 448.

tabımda, kişinin kendisiyle ilgili kişisel verileri internet ortamında ve herkesin ayrıca izin almaya gerek kalmaksızın verileri kopyalayabildiği bir web sayfasına koyması durumunda, bu verilerin başkalarınca alınıp kaydedilmesinin suç oluşturup oluşturmayacağı tartışılmalı olduğunu; öğretide farklı görüş olarak Karagülmez'in, kişisel verilerin bu nitelikteki bir mecrada internet ortamında paylaşan kişinin, bunun başkalarınca kaydedilmesine de rıza göstermiş olduğunu ifade ettiğini [115]; bu görüşe katılmadığımı zira kişisel verinin, sosyal medyada paylaşılmış olması, bunun herkes tarafından kullanılabileceği anlamına gelmediğini; kamuya mal olmuş kişiler bunun istisnasını oluşturmakla birlikte, bu kişiler açısından bile özel hayatlarının gizli alanını ilgilendiren veriler açısından bu istisnanın geçerli olmadığını; buna göre sosyal medyada yayınlanmış da olsa, kişisel verinin üçüncü bir kişi tarafından, verinin ilgilisinin açık rızası olmaksızın kullanılması halinde bunun suç oluşturacağını belirtmiş ve bu suçun işlendiği iddiasıyla açılan bir davada bilirkişi olarak görevlendirilmem üzerine vermiş olduğum raporu da alıntılayarak bu konudaki görüşlerimi açıklamıştım[116]. Nitekim Yargıtay'ın da benzer yönde kararları bulunmaktadır:

"Oluşa ve dosya kapsamına göre; mankenlik mesleğini icra etmesi ve 2009 yılında yapılan bir güzellik yarışmasında ikinci olmasından dolayı kamuoyu tarafından tanınan, özellikle magazin basını tarafından zaman zaman haberleri yapılan katılan Senem ile onunla aynı mesleği icra eden tanık Ebru'nun, facebook adlı sosyal paylaşım sitesinde birbirlerini arkadaş olarak ekledikleri, tanık Ebru'nun, üniversite öğrencisi olan sanık Serap ile aynı evi paylaştığı 2009 yılı Haziran ayında, facebook oturumunu açık bırakmasından faydalanan sanık Serap'ın, tanık Ebru'dan habersiz, onun arkadaş listesinde yer alan katılan Senem'in sayfasına girip, katılana ait 20 adet fotoğrafı, kendi elektronik posta hesabına gönderdikten sonra, aynı sitede, katılan adına ve onun bilgisi dışında oluşturduğu sahte profile, ele geçirdiği katılana ait fotoğrafları koymak suretiyle verileri hukuka aykırı olarak verme veya ele geçirme suçunu işlediği iddia ve kabulüne konu olayda, Katılanın rızasına aykırı olarak ele geçirdiği fotoğraflarını, onun isim ve soy ismiyle birlikte, belirli olmayan ve birden fazla kişi tarafından algılanabilme imkanı bulunan facebook adlı sosyal paylaşım sitesinde, hukuka aykırı olarak yayan sanığın eyleminin verileri hukuka aykırı olarak verme veya ele geçirme suçunu oluşturduğunun kabulünde bir isabetsizlik görülmediğinden, temyiz itirazlarının reddine"[117].

Yukarıda kamuya mal olmuş kişisel verilerin suçun konusunu oluşturup

115 Karagülmez, s. 449.

116 Bkz: Dülger, *Bilişim Suçları*, s. 684-695.

117 12. CD. 17.2.2014, E. 2013/7765, K. 2014/3758.

oluşturmayacağı hususunda buna ilişkin görüşlerimi belirtmiştim. 6698 sayılı KVKK'nın istisnaların yer aldığı 28. maddesinde *"Bu Kanunun amacına ve temel ilkelerine uygun ve orantılı olmak kaydıyla veri sorumlusunun aydınlatma yükümlülüğünü düzenleyen 10 uncu, zararın giderilmesini talep etme hakkı hariç, ilgili kişinin haklarını düzenleyen 11 inci ve Veri Sorumluları Siciline kayıt yükümlülüğünü düzenleyen 16 ncı maddeleri"*nin *"İlgili kişinin kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi"* halinde uygulanmayacağı belirtilmektedir. Nitekim 6698 sayılı KVKK yürürlüğe girmeden önce de Yargıtay'ın görüşü ve uygulaması bu yönde idi:

"Sanığın, katılanın, internette facebook hesabındaki herkese açık profil resmini kopyalayarak rıza olmaksızın kendi facebook hesabına koyduğu olayda; resmin ele geçirilemediği ve içeriğinin belirlenemediği gözetildiğinde, sanık tarafından, katılanın sürekli takip, denetim ve gözetim altına alınması sonucu elde edilmiş özel hayatın gizliliğini ihlale yol açacak bir görüntü bulunmadığı gibi; katılanın, facebooktaki profil resmi, katılanın başkalarınca görülmesi ve bilinmesini istemediği, hukuk tarafından gizliliği ve korunması temel bir şahsiyet hakkı kabul edilmiş özel yaşam alanına ilişkin görüntü olarak değerlendirilemeyeceğinden, atılı suçun yasal unsurları itibariyle oluşmadığı; TCK'nın 136. maddesindeki verileri hukuka aykırı olarak verme veya ele geçirme suçu yönünden değerlendirme yapıldığında, katılanın facebook hesabındaki resmi kişisel veri kapsamında kabul edilebilir ise de; sanığın, resmi, katılanın internette facebook hesabındaki herkese açık profil resminden elde etmesi ve katılana ait başkaca bir kişisel bilgiye yer vermeden kendi facebook hesabına koyması nedeniyle hukuka aykırı olarak ele geçirme ve yaymadan da söz edilemeyeceğinden, bu suçun da unsurlarının oluşmayacağı anlaşılmakla; beraati yerine yazılı düşüncelerle mahkumiyetine karar verilmesi, (BOZMAYI) gerektirmiştir"[118].

"Oluşa ve dosya kapsamına göre, bir avukatlık bürosunda takip elemanı olarak çalışan sanığın, avukat olan katılanın facebook adlı sosyal paylaşım sitesinde yer alan resmini, onun sayfasından temin edip, aynı sitede, bir ön ad ile beraber katılanın adı ve soyadını taşıyan sahte hesap bir açarak, bu hesap üzerinden, ele geçirdiği katılana ait resmi, onun bilgisi ve rızası dışında yayımladığı olayda; Katılanın resmini, belirli olmayan ve birden fazla kişi tarafından algılanabilme imkanı bulunan facebook adlı sosyal paylaşım sitesinde, hukuka aykırı olarak yayan sanığın eyleminin, verileri hukuka aykırı olarak verme veya ele geçirme suçunu oluşturduğunun kabulünde bir isabetsizlik görülmediğinden, Yapılan yargılamaya, toplanıp karar yerinde gösterilen delillere, mahkemenin kovuşturma sonuçlarına uygun olarak oluşan kanaat ve

118 12. CD. 13.10.2014, E. 2014/4081, K. 2014/19490.

takdirine, incelenen dosya kapsamına göre, sanığın, bir nedene dayanmayan diğer temyiz itirazlarının reddine"[119].

Buna göre kamusal alanda paylaşılan kişisel verilere ilişkin ayrım yapmak gerekir. 6689 sayılı Yasanın yukarıda anılan hükmünde belirtilen ve istisnai nitelikte bir durumun bulunması halinde söz konusu alenileşmiş kişisel veri suçun konusunu oluşturmaz. Ancak alenileşmiş de olsa istisna kapsamına girmeyen veya yasanın amacına ve temel ilkelerine uygun ve orantılı olmayan[120] bir kişisel verinin işlenmesi halinde (örneğin alenileşmiş bir resmin arkadaş bulma ya da pornografi sitesinde kullanılması gibi), bu veri kişisel verilerin korunmasına ilişkin suçların konusunu oluşturmaya devam eder. Dolayısıyla kişinin kendisinin paylaşmış olmasına rağmen, kişinin rızasının açıkça olmadığı ya da rızasının olmadığının anlaşıldığı, kişisel verinin paylaşılması amacına aykırı bir biçimde işlenmesi halinde suçun oluştuğu kabul edilmelidir. Nitekim benzer bir olayda bir genç kızın kendi sitesinde yayınladığı resimler, çocuk yaştaki arkadaşları tarafından resimlerin üzerine kızın ağzından yazılmış baloncuklar eklenerek bir başka sitede kamuya açık şekilde yayınlanmıştır. Yargıtay bu durumda kişisel verinin hala koruma altında olduğunu gösteren örnek bir karar vermiştir:

"İncelenen dosya kapsamına göre; suça sürüklenen çocukların katılan mağdure Seren'in "facebook" adlı sosyal paylaşım sitesindeki hesabında bulunan fotoğraflarını kullanarak, aynı sitede "Serenözipek_efkandemirbolatsekskardeşliği" adında başka bir sayfa oluşturdukları, bu sayfada mağdurenin çeşitli yerlerde çekilmiş fotoğraflarını yayınlayarak fotoğrafların içerisine konuşma baloncukları yerleştirip mağdurenin ağzından, kendisi konuşuyormuş gibi, mağdurenin şeref ve saygınlığına zarar verecek nitelikte müstehcen içerikte sözler yazmak suretiyle hakarette bulundukları iddiasıyla açılan davada, yapılan yargılama sonucunda, hakaret suçu sabit görülerek suça sürüklenen çocuklar hakkında hükmün açıklanmasının geri bırakılmasına karar verildiği, TCK'nın 135 ve 136. maddelerinden açılan davada ise suça sürüklenen çocukların beraatine karar verilmiş ise de, katılan mağdurenin kendi hesabında yer alan resimlerini isim ve soy ismi anlaşılacak şekilde herkesin paylaşımına sunan suça sürüklenen çocukların eyleminin, TCK'nın 136/1. maddesinde düzenlenen verileri hukuka aykırı olarak verme veya ele geçirme suçunu oluşturacağı gözetilmeden, yasal olmayan ve dosya kapsamına uygun düşmeyen gerekçelerle suça sürüklenen çocukların beraatlerine karar verilmesi kanuna aykırı, (BOZMAYI) gerektirmiştir"[121].

---

119 12. CD. 23.6.2014, E. 2013/27402, K. 2014/15379.

120 6698 sayılı KVKK'nın 4. maddesinde tanımlanan kişisel verilerin işlenmesinin genel ilkelerinin teori alt yapısı hakkında açıklamalar için bkz: Ayözger, s. 124 vd.

121 12. CD. 10.2.2014, E. 2013/10707, K. 2014/.

iii. 6698 sayılı KVKK'ya Uyarınca Kişisel Verilerin İşlenmesi İçin Açık Rıza Aranmayan Haller

TCK'nın 135. maddesinde yer alan kişisel verilerin kaydedilmesi ve 136. maddesinde yer alan başkasına verme, yayma veya ele geçirme hareketleri 6698 sayılı KVKK'nın 3/1/e maddesinde *"kişisel verilerin işlenmesi"* olarak tanımlanmıştır[122]. Aynı yasanın *"genel ilkeler"* başlıklı 4. maddesinde *"Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir."* denildikten sonra *"kişisel verilerin işlenme şartları"* başlıklı 5/1. maddesinde kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği düzenlenmiştir. Şu şartlardan en azından birinin varlığı hâlinde ise ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkün olacaktır: *a) Kanunlarda açıkça öngörülmesi. b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması. c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması. ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması. d) İlgili kişinin kendisi tarafından alenileştirilmiş olması. e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması. f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.* İşte bu durumların her biri TCK'nın 135 ve 136. maddeleri için de hukuka uygunluk nedeni oluşturur.

iv. 6698 sayılı KVKK'ya Uyarınca Özel Nitelikli Kişisel Verilerin İşlenmesi İçin Açık Rıza Aranmayan Haller

6698 sayılı KVKK'nın 6/1. maddesinde özel nitelikli kişisel verilerin neler olduğu belirtildikten sonra[123], bunların işlenme şartları 6/2. maddesinde düzenlenmiştir. Buna göre özel nitelikli kişisel verilerin ilgilinin açık rızası olmaksızın işlenmesi yasaktır. 6/3. maddeye göre birinci fıkrada sayılan sağlık ve cinsel hayata ilişkin kişisel veriler dışındakiler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilirler. Sağlık ve cinsel hayata ilişkin kişisel

122 "e) Kişisel verilerin işlenmesi: Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi, …".

123 Madde 6/1 "Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir".

veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilirler. 6/4. maddesi gereğince özel nitelikli kişisel verilerin işlenmesinde, ayrıca kişisel Verilerin Korunması Kurulu tarafından belirlenen yeterli önlemlerin alınmasının şart olduğu belirtilmiştir. Makalenin yazımı aşamasında bu kurulun üyeleri henüz yeni atanmıştı ve kurul faaliyetine başlamamıştı. Dolayısıyla kurulun hali hazırda almış olduğu bir karar da bulunmamaktadır. Ancak kurul faaliyete başlayıp da kişisel verilerin korunmasına ilişkin kararlar aldığında, yapılan veri işleme hareketlerinin hukuka uygun olması için söz konusu kurul kararlarına da uyulması gerekecektir. Aksi takdirde kişisel veri işleme hukuka aykırı olacak ve suç oluşturacaktır.

(2). Yasanın Verdiği Yetkiye Dayanılması

Yasanın verdiği yetkiye dayanılarak kişisel verilerin kaydedilmesi diğer bir hukuka uygunluk sebebidir. Bu durum TCK'nın 135. maddesinin gerekçesinde ve 6698 sayılı Yasanın 5. maddesinde belirtilmiştir.

i. CMK Uyarınca Bilişim Sistemlerinde Arama ve Elkoyma Tedbirinin Uygulanması

Bu bağlamda 5271 sayılı Ceza Muhakemesi Kanunu'nun *"Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma"* kenar başlıklı 134. maddesinin 3. fıkrasındaki *"bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır"* hükmü gereğince, bunların içinde kişisel veriler de yer alabilir. Ancak bu durumda yasadan kaynaklanan bir yetkinin kullanılması söz konusu olduğu için 135 ve 136. maddelerdeki suçlar oluşmaz[124]. Nitekim yukarıda da belirttiğim üzere kişisel verilerin soruşturma ve kovuşturma (özel hukuk açısından yargılama) ve infaz makamları tarafından işlenmesi KVKK'nın 28/1/d maddesi gereğince yasanın istisnasını oluşturur. Yani anılan makamlar tarafından kişisel verilerin görev gereği ve ilgili mevzuatın sınırlı içinde işlenmesi bir hukuka uygunluk nedenidir.

ii. Devletin İstihbarat Faaliyetleri Kapsamında Kişisel Verilerin İşlenmesi

Bu maddenin uygulaması açısından tartışılması gereken bir başka durum da 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu çerçevesinde faaliyetlerini yürüten MİT'in bu yasanın 4. maddesine göre ifa ettiği

124 Dülger, *Bilişim Suçları*, s.695, 696; Karagülmez, s. 451.

görevleri esnasında kişisel verileri kaydetmesinin bir hukuka uygunluk nedeni oluşturup oluşturmadığıdır. Kişisel verilerin işlenmesi, MİT'in kuruluş yasasının 4. maddesinde sayılan görevleri arasında sayılabilir. Devlet adına istihbarat toplamak ve bunu değerlendirmekle görevli bir kurum olan MİT'in söz konusu 4. maddede belirtilen görevleri çerçevesinde ve bu görevleri yerine getirmek amacıyla kişisel verileri kaydetmesi tartışmasız olarak TCK'nın 135. maddesinde düzenlenen kişisel verilerin kaydedilmesi suçu açısından bir hukuka uygunluk nedeni oluşturur ve MİT mensuplarının buna ilişkin çalışmaları nedeniyle gerçekleştirdikleri eylemler suç olarak değerlendirilmez[125]. Nitekim 6698 sayılı Yasanın 28/1/ç maddesiyle *"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"* istisna olarak düzenlenmiş, dolayısıyla istihbarat faaliyetleri açısından bir hukuka uygunluk nedeni yaratılmıştır. Ancak bunların kişinin dokunulması yasak olan yaşamın gizli alanına ilişkin olması ya da gizli alan dahil olmasa dahi toplanan bilgilerin bir dönem ülkemizde sıklıkla görüldüğü gibi basında yayınlanmak üzere verilmesi hukuka uygun olmayacak ve suç gerçekleşmiş olacaktır.

İlke olarak bu durum Emniyet Genel Müdürlüğü, Jandarma Genel Komutanlığı, Sahil Güvenlik Komutanlığı vb. diğer kolluk güçleri açısından geçerli değildir. Çünkü MİT'in topladığı bilgiler kendi yasasında belirtilen devlet yetkililerine sunulur ve devletin politikalarına yön vermek amacıyla kullanılır. Oysa kolluk güçlerinin topladığı istihbari bilgiler operasyonel amaçlarla ve şüpheli kişiler hakkında soruşturma yürütülmesi ve ileride davada delil olarak kullanılmak amacıyla toplanır. Dolayısıyla bu kurumların CMK'daki düzenlemelere uyulmadan hakim kararı olmaksızın kişisel veri niteliğindeki bilgileri işlemesi mümkün olmamalı, bunun yapılması ilgililer açısından suç oluşturmalı ve veriler hukuka aykırı delil oldukları için delil yasağı kapsamında değerlendirilip soruşturma ve kovuşturmada kullanılmamalıdır.

Uygulamada ise sadece Polis Vazife ve Salahiyet Kanunu'nun ek 7. maddesinde geçen *"istihbarat faaliyetlerinde bulunur"* hükmü esas alınarak, istihbarat niteliğinde iletişimin denetlenmesi yapılmakta ve kişisel veriler kaydedilmekteydi. Ancak buna rağmen söz konusu kurumların tamamı istihbari amaçlı dinleme yapmakta ve kişisel veri niteliğindeki bu bilgileri kaydetmekteydi.

Bu alandaki hukuksal zemin ilk olarak 3.7.2005 tarih ve 5397 sayılı yasa ile oluşturulmuştur. Bu yasa ile Polis Vazife ve Salahiyet Kanunu'nun ek 7. maddesine ve 10.3.1983 tarihli ve 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri

125 Dülger, *Bilişim Suçları*, s.696.

Kanununa eklemeler yapılmış ve 1.11.1983 tarihli ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanununun 6. maddesinin 1. fıkrası değiştirilerek maddeye bazı fıkralar eklenmiştir. Böylelikle bir soruşturma başlamadan da iletişimin denetlenmesi ve söz konusu kişisel verilerin kaydedilmesi olanağı sağlanmıştır. 6698 sayılı Yasanın yukarıda aktardığım 28/1/ç – d maddesiyle kolluk güçlerinin yaptığı bu işlemler, genel ilkelere uygun olmak şartıyla, tamamen yasal bir zemine oturtulmuştur.

Ancak bir konunun yasal bir dayanağının olması ve bu dayanağa göre işlem yapılması her halükarda bunun hukuka uygun olduğu anlamı gelmez. Bu düzenleme, kişisel veriler alanındaki uluslararası düzenlemelere ve bu alanda kabul edilen evrensel ilkelere aykırıdır, dolayısıyla hukuka da aykırıdır. Özellikle ülkemiz gibi kolluk güçlerinin hesap verme alışkanlığının olmadığı, iç ve dış deneti mekanizmalarının ya olması gerektiği gibi oluşturulmadığı ya da oluşturulanların olması gibi çalıştırılmadığı bir sistemde bu düzenleme kötüye kullanımlara son derece açıktır. Hiç ummamakla birlikte -zira bu durum mevcut iktidara göre değişen bir durum olmayıp ülkemizde her devirde her iktidar devrinde görülen genel bir anlayışın ürünüdür- bu düzenlemenin ya kaldırılmasını ya da kolluk güçlerinin bu alandaki faaliyetlerinin denetlenmesi gerektiğini düşünüyor ve öneriyorum. Nitekim Birleşik Krallık'ta (İngiltere) polisin yürüttüğü bu tür özel muhakeme tedbirleri ya da işlemler bu alana özgü oluşturulan bağımsız komisyonlar tarafından denetlenmekte ve raporlanmaktadır. Hatta bazı durumlarda bu komisyonların ön izni olmadan polis bu tür tedbirleri alamamaktadır. Komisyonun uygun bulmadığı yönetmelerle elde edilen deliler soruşturma ve kovuşturmada kullanılmamaktadır[126]. Demokratik ve hukukun üstünlüğünü benimsemiş bir ülkede ve siyasal sistemlerde bu tür yapılara olan ihtiyaç kaçınılmazdır.

iii. CMK'nın 135. Maddesi Uyarınca Sinyal Bilgilerinin Değerlendirilmesi

Burada değinmek istediğim bir diğer husus ise CMK'nın 135. maddesinde düzenlenen sinyal bilgilerinin değerlendirilmesi konusudur. Özel haberleşmenin gizliliği ve kişisel verilerin korunması birbiriyle sıkı bağları olan iki kavramdır. Gelişen bilişim teknolojilerine bağlı olarak verilerin izlenmesi, toplanması ve saklanması kolaylaşmış ve bu işlemlerin maliyetleri düşmüştür. Buna bağlı olarak söz konusu işlemlerin kolaylaşması, iletişimin içeriğinin dinlenmesi ve kaydedilmesi yanında, bunların sinyal bilgilerinin özellikle geçmişe doğru değerlendirilmesi ya da sinyal bilgileri kullanılarak şüphelilerin yerinin tespit edilmesi gibi yeni olanak ve tartışma noktalarının çıkmasına da neden olmuştur. Özel haberleşmenin içeriği yanında, özel iletişime ilişkin çeşitli verilerin kayde-

126 Buna ilişkin örnekler için bkz: Walden, pn. 4.46- 4.64.

dilmesi de önemli bir sorundur. Bu bağlamda iletişimin doğrudan içeriğinin yani *"ne"* konuşulduğunun değil, telefon aramaları ya da posta gönderim kayıtlarının, bir başka deyişle *"kiminle"*, *"ne sıklıkla"*, *"ne kadar süreyle"* ve *"nereden"* konuşulduğu bilgisinin özellikle soruşturma aşamasında son derece önemli olduğu ve birçok ceza davasında bunların delil olarak sanığın önüne koyulduğu ve ispat vasıtası olarak kullanıldığı görülmektedir. Bunun bir benzeri, özellikle bilişim suçları veya bilişim sistemleri kullanılarak işlenen suçlarda, gönderilen elektronik postalar ve ziyaret edilen web siteleri açısından söz konusu olmaktadır[127].

Bu bağlamda birçok soruşturma ve kovuşturmada mahkemelerce verilen iletişimin tespiti kararlarında *"kararın verildiği tarihin öncesine ilişkin"* telefon işletmecileri tarafından kayıt edilen sinyal bilgilerinin istenildiği, hatta bazı soruşturma ve kovuşturmalarda ise böyle bir mahkeme kararı olmaksızın dahi söz konusu verilerin dosyaya delil olarak kolluk tarafından konulduğu görülmektedir. Öncelikle ifade etmeliyim ki söz konusu sinyal bilgileri (cep telefonu vb. her türlü elektronik ve dijital araç vb.) de kişisel veri niteliğindedir ve bunların kayıt altına alınması ancak yasa ve ilgili mevzuat ile yapılan bir düzenlemenin buna izin vermesi ile olur.

5.11.2008 tarihli ve 5809 sayılı *Elektronik Haberleşme Kanununun* 6, 8, 9, 10, 11, 12 ve 60. maddelerine dayanılarak hazırlanan *"Elektronik Haberleşme Sektörüne İlişkin Yetkilendirme Yönetmeliği"*nin 19/1/f. maddesine göre[128] trafik bilgileri şu biçim ve sürede muhafaza edilebilirler: *"Erişim sağlayıcı olan veya telefon hizmeti sunan işletmeci, taraflara ilişkin IP adresi, port aralığı, verilen hizmetin başlama ve bitiş zamanı, yararlanılan hizmetin türü, aktarılan veri miktarı, kullanıcı sayısı ve abone kimlik bilgileri ile altyapısı üzerinden gerçekleşen görüşmelere ait trafik bilgilerini iki yıl süreyle; kullanıcı bilgilerini ise ilgili mevzuatta belirtilen zamanaşımı süresi boyunca muhafaza etmekle yükümlüdür"*. Buna göre sinyal bilgilerinin kayıt edilmesi ve iki yıl süreyle muhafaza edilmesi erişim sağlayıcılar ve telefon hizmeti sunan işletmeciler tarafından bir yükümlülük olarak düzenlenmiştir. Ancak bu düzenlemenin başlı başına hukuka aykırı olduğu ifade etmeliyim. Söz konusu yönetmelik bu alandaki Avrupa Birliği Direktifine uyumlu olarak hazırlanmıştır[129]. Ancak pek çok Avrupa Birliği üyesi ülke, Veri Saklama Direktifi uyarınca yapılacak iç hukuk düzenlemesinin, işlenmiş kişisel verilerin gereğinden fazla sistemde tutulmasını gerektirdiği bunun da özel hayatın gizliliğini ihlal edeceği endişesiyle iç hukuklarına almamışlardır. Benzer kaygılarla harekete eden Avrupa Adalet Divanı,

127 Küzeci, s. 98.

128 Değişik: Resmi Gazete 11.6.201, 29739.

129 *Data Retention Directive (Veri Saklama Direktifi)*, 2006/24/EC.

8.4.2014 tarihli kararı ile Veri Koruma Direktifini hükümsüz hale getirmiştir. Divan kararında, Veri Saklama Direktifinin iki temel hak olan özel hayatın gizliliği ve kişisel verilerin korunması hakkını ağır şekilde ihlal ettiğini; söz konusu kişisel verilerin saklanmasının kamu güvenliği ve ciddi suçlarla mücadele için gerekli olduğunu fakat Veri Saklama Direktifinde bu amaçla yeterli sınırlama yapılmadığını ve kapsamının iyi belirlenemediğini belirterek, direktifin orantısız olduğu kararını vermiştir. Öte yandan veri saklamanın ve ulusal makamlara bilgi aktarımının zorunlu tutulmasının ciddi bir hak ihlali oluşturduğunu ifade etmiştir[130]. Dolayısıyla ülkemizde elektronik haberleşme sektöründe kişisel verilerin saklanmasını düzenlemesinin dayanağı olan direktif yukarıda anılan ve benim de katıldığım gerekçelerle iptal edilmiştir. Ancak ülkemizde hala yürürlüktedir ve aşağıda açıklayacağım üzere, bu yönetmeliğe dayanılarak elde edilen sinyal bilgileri yani kişisel veriler, delil olarak soruşturma ve kovuşturma aşamalarında, hatta ispat için hükmün gerekçesinde kullanılmaktadır[131].

Buradan hareketle kişilerin söz konusu kişisel veri niteliğindeki verilerinin bu mevzuat dışında işlenmesi TCK m.135 ve 136. madde tanımlı suçları oluşturacağı ve ayrıca sürenin dolmasına rağmen bunların yok edilmemesi veya anonimleştirmemesi halinde ise duruma göre ya KVVK m. 17/2 ya da TCK m.138'i oluşacağı sonucuna ulaşırız.

Öte yandan kanaatimce bunun bir mahkeme kararıyla geçmişe yönelik istenmesi de telefon işletmecileri açısından yaptıkları eylemleri hukuka uygun hale getirmez, zira savcılıkların ya da mahkemelerin geçmişe yönelik böyle bir talepte bulunmalarının yasal bir dayanağı yoktur. CMK'nın 135. maddesinde geçmişe yönelik sinyal bilgilerinin istenebileceği ve değerlendirilebileceğine ilişkin bir düzenleme bulunmaz. Ancak uygulamada CMK m. 135/1'de yer alan *"sinyal bilgileri değerlendirilebilir"* ifadesinden yola çıkılarak adeta geçmişe yönelik olarak böyle bir yetki varmış gibi hareket edilmekte ve telefon işletmecilerinden yukarıda yönetmelikte yere alan yetki uyarınca tutmak zorunda oldukları (ve hizmetlerini ücretlendirirken kullandıkları) sinyal bilgileri (ki ilgili kişi açısından aynı

130 Ayözger, s.174.

131 Yazarından aynen alıntıladığım şu satırlar durumun vehametini ortaya koymaktadır: "... veri saklama yükümlülüğü, kişisel verilerin korunması hakkı ve bu hakkın temelinde yatan özel hayatın gizliliği hakkının sınırlandırılmasıdır. Uusal metinlerde yer alan hakların sınırlandırılması şartlarını haiz hallerde, elektronik haberleşme sektöründeki kişisel verilerin belirli bir süre saklanması mümkündür. Fakat sınırlandırma nedeninin açıkça belirtilmesi ve buna ilişkin kanuni düzenemenin yapılması gereklidir. Sınırlandırma amacı belirtilmeden ve yönetmelik ile getirilen hükümlere dayanılarak kişisel verilerin saklanması, açıkça hukuka aykırıdır. İptal edilmesinin en önemli nedeni, amacının sınırlarının iyi çizilememesi olan Veri Saklama Direktfiyle uyumlu düzenlenen EHSKVİY'nin verilerin saklanması amacına ilişkin hiçbr hüküm içermemesi, hukuki garabettir". Ayözger, s.174, 175.

zamanda kişisel veri oluştururlar) istenmekte ve soruşturma ile kovuşturmada, hatta ispatta bir sübut aracı olarak kullanılmaktadır. Oysa ceza muhakemesi hukukunda da "sınırlı yasallık ilkesi" geçerlidir. Temel hak ve özgürlükleri sınırlayan düzenlemeler, ki koruma tedbirlerinin tamamı bu niteliktedir, ancak yasa ile düzenlenip, değiştirilebilirler ve kaldırılabilirler. Ayrıca ceza muhakemesi hukukundaki bir diğer önemli ilke koruma tedbirlerinin geçmişe değil ileriye yönelik olarak uygulanabilmeleridir. Oysa CMK'nın 135. maddesinde sinyal bilgilerinin değerlendirilmesi tedbiri açısından, bunun geçmişe yürüyebileceğine ilişkin bir düzenleme bulunmaz. O halde soruşturma ve kovuşturma makamları yasal dayanağı olmayan ve dolayısıyla hukuka aykırı bir işlem yapmaktadırlar. Gecikmesinde sakınca bulunan hallerde savcılığın normal şartlarda ise hakimin kararı öncesi kaydedilen sinyal bilgilerinin, savcılık ya da mahkeme kararı ile dosyaya girse dahi delil olarak kullanılmaları ve hükme esas alınmaları hukuka aykırı delil ve delil yasaklarının düzenlendiği CMK'nın 206/2, 217/2 ve 230 maddeleri ve Yargıtay'ın bu konudaki yerleşik kararları gereğince mümkün değildir. Dolayısıyla bu yolla elde edilen delillerin kendisi ve bunlardan yola çıkılarak elde edilen türev deliller de (zehirli ağacın meyvesi öğretisi gereği) hukuka aykırıdır ve ceza muhakemesinin hiçbir aşamasında kullanılamazlar[132].

Buna karşın uygulama bu şekilde olmamakta HTS raporu denen bu sinyal bilgileri hem ceza hem de özel hukuk yargılamalarında delil olarak kullanılmaktadır. İşin ilginci bunların dosyaya getirtilmesini hukuka uygun bulan Yargıtay, bunların kişisel veri olduğunu kabul edip, dosyadan çıkartılarak üçüncü kişilere verilmesini suç olarak kabul etmektedir:

"Somut olayda; sanık ile katılanın resmi nikahlı evli olup aralarında boşanma davası bulunduğu, dava sırasında sanığın talebi üzerine katılanın kullanmakta olduğu cep telefonu hattının son 2 yıla ait ayrıntılı görüşme dökümlerini içerir HTS raporlarının getirtilerek dava dosyasına konulduğu, sanığın, HTS raporlarını dava dosyasından alarak katılanın babası Ali ile abisi Mehmet'e gönderdiği olayda; katılanın kim ile ne zaman, hangi sıklıkla, hangi süreyle görüştüğüne ilişkin görüşme dökümlerini içerir HTS raporları kişisel veri kapsamında olup, sanığın, kişisel veri niteliğindeki HTS raporlarını hukuka uygun bir şekilde elde etmesine rağmen, kaydedilmiş haliyle hukuka aykırı olarak yaydığı, eyleminin TCK'nın 136/1. maddesine uyan verileri hukuka aykırı olarak verme veya ele geçirme suçunu oluşturduğu ve bu suçtan sorumlu tutularak cezalandırılmasına karar verilmesi gerektiği gözetilmeden, suçun

132 Hukuka aykırı delil, delil yasakları ve zehirli ağacın meyvesi öğretisi hakkında ayrıntılı açıklamalar içib bkz: Murat Volkan Dülger, *Ceza Muhakemesi Hukukunda Dışlama Kuralı ve Hukuka Aykırı Delillerin Uzak Etkisi (Zehirli Ağacın Meyvesi Öğretisi)*, Seçkin Yayıncılık, Ankara, 2014, s. 106 vd.

nitelendirilmesinde yanılgıya düşülerek yazılı şekilde hüküm kurulması, (BOZMAYI) gerektirmiştir"[133].

Ancak suç soruşturmasında özellikle faillerin tespiti ve kovuşturma esnasında failin eylemle, suç ortaklarıyla ve/veya mağdurla bağlantısının ortaya konulabilmesi ve ispatın gerçekleştirilebilmesi için bu sinyal bilgilerinin elde edilmesi ve değerlendirilmesi son derece gerekli ve önemlidir. O halde CMK'nın 135. maddesi olması gereken hukuka göre değiştirilmeli, hali hazırda işleyen sisteme uyumlu hale getirilmelidir. Ancak olan hukuk ve halihazırda uygulanan işlemlerin hukuka aykırı olduğunu bir kez daha ifade etmeliyim.

Bu durumda CMK'nın yürürlükte bulunan 135. maddesi karşısında, olan hukuk açısından, telefon işletmecileri bu sinyal bilgilerini mahkemeye vermekle ayrıca TCK'nın 136. maddesinde tanılanan verileri hukuka aykırı olarak verme suçunu işlemektedirler. Öte yandan savcılıklar ve mahkemeler açısından da yine aynı maddede tanımlı verileri hukuka aykırı olarak ele geçirme suçu söz konusu olmaktadır. Dolayısıyla bu konuda bir an önce yasal düzenleme yapılması ve hukuka aykırılığın ortadan kaldırılması gerekir.

Dolayısıyla kamu otoritelerinin ya da özel kişilerin içeriğine bakmadığı gerekçesiyle, yasal bir dayanağı olmadan, keyfi bir biçimde, Anayasaya aykırı olarak veri trafiğini izleme ve bundan bazı sonuçlar çıkarma ve en önemlisi bunları hukuka uygun bir delilmiş gibi ceza muhakemesinde kullanma hak ve yetkisi bulunmamaktadır[134]. Nitekim AİHM'in de benzer yönde kararları bulunmaktadır[135].

iv. Özel Nitelikli Sağlık Verilerinin İşlenmesi

Kişisel verilerin korunması ve bunlara karşı işlenen suçlar açısından tartışılması gereken bir diğer konu hekime belirli hususları açıklama yönünde bir görev yüklendiğinde, yasa hükmünün yerine getirilmesinin bir hukuka uygunluk nedeni oluşturması, bunun yerine getirilmemesi halinde ise görevin yerine getirilmemesi nedeniyle suç oluşmasıdır. Örneğin TCK'nın 279. ve 280. maddeleri ile Umumi Hıfzıssıhha Kanunu'nun bildirime yönelik bazı hükümleri gereğince kişisel verilerin verilmesi suç oluşturmayacaktır[136].

6698 sayılı KVKK'nın 6/1. maddesinde sağlık verileri özel nitelikli kişisel veriler olarak tanımlandıktan sonra, 2. fıkrada bunların ancak ilgilisinin açık rı-

133 12. CD. 29.9.2014, E. 2014/5104, K. 2014/18858.

134 Benzer görüş için bkz: Küzeci, s. 98, 99. Ayrıca bkz: Kerem Altıparmak, "Büyük Biraderin Gözetiminden Çıkış: Telefonların İzlenmesinde Devletin Sorumluluğu", *Türkiye Barolar Birliği Dergisi*, S.63, Mart – Nisan 2006, s. 47.

135 Malone v. Birleşik Krallık, pr. 84. Türkçe çevirisi için bkz: Osman Doğru, *İnsan Hakları Avrupa Mahkemesi İçtihatları*, C.I, Legal Yayınevi, İstanbul, 2004, s. 764 – 779.

136 Hakeri, *Verileri Hukuka Aykırı Olarak Verme*, s. 131.

zasıyla işlenebileceği belirtilmiştir. Buna göre bu tür verilerin işlenmesinin hukuka uygun olabilmesi için açık rızanın varlığı gerekir. Ancak aynı maddenin 3. fıkrasının 1. tümcesinde birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel verilerin kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebileceği düzenlenmiştir. 3. fıkranın 2. tümcesinde ise sağlık ve cinsel hayata ilişkin kişisel verilerin ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebileceği belirtilmiştir. Bu açık düzenlemeden sonra hasta bilgilerinin kaydı için varsayılan rıza teorisini kullanmaya gerek yoktur[137]; yasa bunu zaten istisnalar arasında tutarak rıza aranmasına gerek olmayan haller arasına dahil etmiştir. Ayrıca aynı maddenin 4. fıkrasında, özel nitelikli kişisel verilerin işlenmesi için ayrıca Kişisel Verileri Koruma Kurulu tarafından belirlenen yeterli önlemlerin alınması şart olduğu da yer almaktadır. 6698 sayılı Yasa dayanarak yapılarak Sağlık Bakanlığı tarafından çıkarılan "Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik"in 7. maddesinde kişisel sağlık verilerinin işlenmesi düzenlenmiş olup, maddenin 1. ve 4. fıkraları dayanak yasanın yukarıda açıklanan 6. maddesiyle birebir aynıdır. Yönetmeliğin 7. maddesinin 2. fıkrasında ise *"Kişisel sağlık verilerinin, ilk fıkrada sayılan amaçlar dışında anonim hale getirilmeden işlenmesi için ilgili kişiye ait verilerin işlenme gerekçesi ile ilgili olarak ayrıntılı bir şekilde bilgilendirilmesi, yazılı rızasının alınması ve bu rızanın muhafaza edilmesi gerekir"* denilerek kişisel sağlık verilerinin anonimleştirilmesi, 3. fıkrasında *"İlgili kişi, aksi yönde bir hukukî düzenleme veya yargı kararı bulunmaması halinde verilerinin işlenmesi ve aktarılması için vermiş olduğu rızayı istediği zaman geri alabilir"* denilmek suretiyle kişisel sağlık verisinin işlenmesi için verilen rızanın geri alınması düzenlenmektedir. Rızanın geri alınması, o tarihe kadar yapılmış bulunan işlemler bakımından etkili olmaz. Buna göre kişisel sağlık verilerinin işlenmesi söz konusu olduğunda TCK m.135 ve 136. maddeler açısından bir hukuka uygunluk nedeninin var olup olmadığına tüm bu hükümler birlikte değerlendirilerek karar verilmelidir.

Bu bağlamda belirtmeliyiz ki; hekimler, diş hekimleri, eczacılar, ebeler ve bunların yardımcıları ile diğer tüm tıp meslek veya sanatları mensuplarının, bu sıfatları dolayısıyla hastaları ve bunların yakınları hakkında öğrendikleri bilgiler dolayısıyla CMK'nın 46/1-b maddesi gereğince tanıklıktan çekinme hakları bu-

137 Yasa öncesinde varsayılan rıza teorisi konuya getirilen açıklama için bkz: Sabire Sabem Yılmaz, *Tıp Alanında Kişisel Verilerin Açıklanması Suçu*, Seçkin, Ankara, 2014, s. 98, 99.

lunur. Ancak çekinme sebebi olmasına ve hastanın da tanıklığa ilişkin rızasının bulunmamasına rağmen hekimin tanıklık yapması durumunda hekim, kişisel verilerin açıklanması suçunu işlemiş olur[138]. Nitekim tıp mesleği mensuplarına sıfatları dolayısıyla ilişkide oldukları hastaları ve bunların yakınlarına ilişkin ceza soruşturması ve kovuşturmasında bilirkişilikten çekinme hakkı da tanınmıştır (CMK m.70/1). *Türk Tabipleri Birliği Hekimlik Meslek Etiği Kuralları* m.9/4'de de hekimin, tanık ya da bilirkişi olarak mahkemeye çağrıldığında olayın meslek sırrı olduğunu ileri sürerek bu görevlerinden çekilebileceği öngörülmüştür[139].

v. Kişilerin Siyasi, Felsefi veya Dini Görüşlerine ve Irki Kökenlerine İlişkin Bilgilerin Kayda Alınması Sorunu

CMK'nın 135/2. maddesinin gerekçesinde özellikle suçla mücadele bağlamında kişilerin ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgilerin kaydedilmesinin yasayla hukuka uygunluk nedeni olarak düzenlenebileceği ifade edilmektedir[140]. Buna göre kişilerin siyasi, felsefi veya dini görüşlerine ve ırki kökenlerine ilişkin bilgilerin kayda alınması her ne suretle olursa olsun bir hukuka uygunluk nedeni olarak kabul edilmemelidir. Ancak bu durumda TCK'nın 135/2. maddesi ile 6698 sayılı KVKK arasında bir çelişki bulunduğu görülür. Gerekçenin yorumundan yukarıda belirttiğim bazı kişisel verilerin işlenmesinin hiçbir şekilde bir hukuka uygunluk nedeni olarak kabul edilmemesi gerektiği sonucu çıkmasına karşın, KVKK tüm bunları kişisel veri olarak kabul etmiş ve hatta suç soruşturma ve kovuşturması ile istihbarat faaliyetleri gibi alanları istisna kapsamına alarak, bu tür verilerin işlenmesi için açık rızaya gerek olmadığını düzenlemiştir. Şüphesiz olması gereken hukuk açısından doğru olan TCK m.135/2. Maddenin gerekçesinin yorumlanması yoluyla varılan sonuçtur. Yürürlükte olan ve yaşamakta olduğumuz ise 6698 sayılı KVKK hükümleri ve zaten şimdiye kadar bu yönde yapılagelen işlemledir.

vi. Kamu ve Özel Sektörde Çalışanlara Verilen Bilişim Sistemlerindeki Kişisel Verilerin Akıbeti Sorunu

Bu başlık altında değinmek istediğim bir başka olasılık ise kamu görevlilerine ve işçilere çalıştıkları kurumlar veya işverenleri tarafından verilen bilgisayarlara

138 Hakeri, *Verileri Hukuka Aykırı Olarak Verme*, s. 127.

139 Yokuş Sevük, s. 791.

140 "Maddenin ikinci fıkrasında, kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine, ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kayda almak, suç olarak tanımlanmıştır. Ancak, bunlardan kişilerin ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kayda alınmasına kanunlarda özellikle suçlulukla mücadele bağlamında, suç ve suçluların ortaya çıkarılmasını sağlamak amacıyla belli ölçüde izin verilebilir. Bu durumlarda söz konusu suç oluşmayacaktır."

ya da elektronik posta hesaplarına kurumun/iş yerinin yetkili amiri veya denetimle görevli kişileri tarafından el konulması ve içindeki verilerin incelenmesi ve kaydedilmesi durumudur. Bu konuda iki farklı görüş bulunmaktadır. Bu görüşlerden ilkinde söz konusu bilgisayarların ve/veya elektronik postaların iş için verildiği ve içinde kişisel veri olsa dahi incelenebileceğidir[141]. Bu konudaki diğer görüş ise söz konusu bilgisayarların ve/veya elektronik posta hesaplarının veriliş amacı iş ile ilgili de olsa bunların kullanım alanının yalnızca iş ile sınırlanmasının mümkün olmadığı, bunlarla mutlaka kişisel iletişimin ya da işlemlerin yapıldığı, kişisel verilere ise rıza ya da mahkeme kararı olmaksızın el konulmasının ve ele geçirilmesinin mümkün olmadığıdır. Ben ikinci görüşte ileri sürülen görüşleri de dikkate almakla birlikte esasen birinci görüşe katılmaktayım. Zira kamu görevlisine ya da işçiye verilen bu bilgisayar ve/veya elektronik posta adresi kişinin özel işlerini yapması için değil, göreviyle ilgili işlerini yapması için verilmektedir. Kişi bu araçlarla dilerse ve işini aksatmamak şartıyla tabi ki kişisel işlerini de yapabilir. Ancak kendisine kullanmak üzere verilen bu araçların daima denetlenebileceğini ve içinde kişisel verisinin olduğu itirazını ileri süremeyeceğini bilmelidir. Bana göre bu durum hem kamu sektöründe kamu görevlileri hem de özel sektörde işçi – işveren ilişkileri çerçevesinde kabul edilmesi gereken, uygulaması da bu şekilde olan bir durumdur.

c. Kişisel Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme Suçu Açısından

Söz konusu hukuka uygunluk nedenleri 136. maddede düzenlenen kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçu açısından da geçerlidir.

TCK'nın 135. ve 136. maddelerdeki suçların tanımında failin eylemlerini *"hukuka aykırı olarak"* gerçekleştirmesi gerektiği ayrıca ifade edilmiştir. Bu ve benzer ifadelerin suç tanımında kullanılıyor olmasına ilişkin öğretide farklı görüşler ve gerekçeler ileri sürülmüştür[142]. Bazı yazarlar, bu gibi ifadelerin yer aldığı suç tiplerinde *"hukuka özel aykırılık"* durumunun söz konusu olduğunu, yasa koyucu burada failin özellikle hukuka aykırı olarak hareket edip etmediğinin araştırılmasını ve bunun ispatlanmasını istediğini, aksi takdirde yani failin hukuka aykırı olarak hareket ettiğinin ispat edilememesi halinde cezalandırılamayacağını,

141 Öğretide Erdoğan bu konuyu TCK'nın 243. maddesinde düzenlenen bilişim sistemine girme ve sistemde kalmaya devam etme suçu açısından incelemiş ve yukarıda belirtmiş olduğumuz görüşü savunmuştur. Ancak bize göre bu konunun incelenmesi gereken yer TCK'nın 135. ve 136. maddelerinde düzenlenen kişisel verilerin kaydedilmesi ve ele geçirilmesi suçlarının ilgili alt başlıklarıdır. Konuyla ilgili açıklamalar için bkz: Yavuz Erdoğan, *Türk Ceza Kanunu'nda Bilişim Suçları (Avrupa konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları ile)*, Legal, İstanbul, 2012, s. 161.

142 Bu görüşler ve gerekçeler için bkz: Kayıhan İçel, *Ceza Hukuku Genel Hükümler*, Yenilenmiş Bası, Beta Yayıncılık, İstanbul, 2016, s. 309 – 311.

suç tipinde failin eylemleri "hukuka aykırı olarak" gerçekleştirmesinin özellikle belirtilmesinin amacının bu olduğunu ifade etmektedirler[143]. Bazı yazarlar ise bununla doğrudan kastın işaret edildiğini, bu tür ifadelerin yer aldığı suçların ancak failin doğrudan kastıyla işlenebileceğini, dolayısıyla bu tür suçlara ilişkin yargılamalarda failin eylemini hukuka aykırı olduğunu bilerek gerçekleştirdiğinin araştırılması gerektiğini belirtmektedirler[144].

d. Kişisel Verilerin Yok Edilmemesi Suçu ve 6698 sayılı KVKK m.17/2'de Düzenlenen Kişisel Verilerin Silinmemesi veya Anonim Hale Getirilmemesi Suçu Açısından

Yasanın 138. maddesinde düzenlenen kişisel verilerin yok edilmemesi suçunda iki farklı hukuksal değerin korunduğu ve buna bağlı olarak hem kişisel verilerin ilgilisi olan birey, hem de toplumu oluşturan her birey suçun mağduru olduğu için; yok edilmeyen verilerin ilgilisi olmasına rağmen tek başına suçtan zarar gören kişinin rızası eylemi hukuka uygun hale getirmez[145]. Bunun dışında bu suç tipi açısından yasadan kaynaklanan başka bir hukuka uygunluk sebebi de bulunmaz. Ancak failin mücbir sebep halinde failin ceza hukuku anlamında hareket olarak kabul edebileceği iradi bir hareket bulunmadığı için suçun maddi unsurlarından hareket unsurunun eksikliği nedeniyle suç oluşmaz. Nitekim Yargıtay, eski ceza yasasında benzer suç tipini içeren 230. maddeye ilişkin vermiş olduğu kararlarında aynı yönde görüş bildirilmiştir[146]. Bu açıklamalar 6698 sayılı KVKK m.17/2'de düzenlenen kişisel verilerin silinmemesi veya anonim hale getirilmemesi suçu açısından da geçerlidir.

5. Suçların Özel Görünüş Biçimleri

a. Teşebbüs

TCK'nın 135. ve 136. maddelerinde düzenlenen her iki suç tipinin de teşebbüs aşamasında kalması mümkündür[147]. Teşebbüs hali, fail tarafından icra hareket-

143 Nur Centel, Hamide Zafer, Özlem Çakmut, *Türk Ceza Hukukuna Giriş*, 9. Bası, Beta Yayıncılık, İstanbul, 2016, s. 298; Veli Özer Özbek, M. Nihat Kanbur, Koray Doğan, Pınar Bacaksız, İlker Tepe, *Türk Ceza Hukuku Genel Hükümler*, 7. Bası, Seçkin Yayıncılık, Ankara, 2016, s. 288, 289.

144 İzzet Özgenç, *Türk Ceza Hukuku*, 12. Bası, Seçkin Yayıncılık, Ankara, 2016, s.295, 296.

145 Aynı görüşte bkz: Karagülmez, s. 476.

146 "Muhatabın Almanya'da işçi olarak çalışmakta bulunduğu sırada tebligatın yapılması için Tebligat Kanununun hükme esas alınan 16. ve 21'inci maddelerindeki şartların mevcut olmadığı ve böylece Almanya'da iş edinen şahsa gıyap kararını Türkiye'de tebliğ edememesi sebebiyle sanığın eyleminde görevi savsama suçunun unsurlarının bulunmadığı düşünülmeden yazılı şekilde (TCK nun 230/1'inci maddesiyle) mahkumiyet kararı verilmesi, bozmayı gerektirmiştir." 4. CD., Kt. 09.06.1976, E. 1976/4075, K. 1976/4100; akt: Sahir Erman, *Kamu İdaresine Karşı İşlenen Suçlar (TCK 202 – 281)*, Dünya Yayıncılık, İstanbul, 1992, s. 163, 164.

147 Yokuş Sevük, s. 809.

lerine başlandıktan sonra bu hareketlerin yarıda kalması şeklinde olabilir; çünkü suçun oluşu açısından ayrıca bir neticenin meydana gelmesi aranmadığı için hareketlerin tamamlanmasıyla suç oluşacaktır[148]. TCK'nın 138. maddesi ile 6698 sayılı KVKK m.17/2'de düzenlenen suçlar ise ihmal suretiyle işlenebilen suçlar olduğu için teşebbüse elverişli değildirler[149].

b. İştirak

TCK'nın 135, 136, 138 ve 6698 sayılı KVKK m.17/2. maddelerinde düzenlenen suçların iştirak halinde işlenmesi mümkündür ve iştirak açısından bir özellik göstermezler. Ancak TCK'nın 134, 135 ve 136. maddelerde düzenlenen suçlarda suça iştirak edenlerin kamu görevlisi sıfatını taşıması ya da bu konuyla ilgili belli bir meslek veya sanat sahibi olması halinde bu kişilere TCK'nın 137. maddesi gereğince ceza artırılarak verilir[150].

c. İçtima

TCK'nın 135. maddesinde yer alan kişisel verilerin kaydedilmesi suçu ile içtima sorunu ortaya çıkması en olası suç, 244. maddenin 1. ve 2. fıkralarında düzenlenen "Bilişim Sisteminin İşleyişinin Engellenmesi veya Bozulması Suçu ile Verilerin Yok Edilmesi veya Değiştirilmesi Suçu'dur". Özellikle 244. maddenin 2. fıkrasında "sisteme veri yerleştiren" ifadesiyle tanımlanan hareketle 135. maddenin eylem unsuru olan "verinin kaydedilmesi" aynı anlama gelir. Ancak iki suç tipi birlikte incelendiğinde 135. maddede kişisel verilerin, 244/2'de ise her türlü verinin suçun konusunu oluşturduğu, diğer yandan 244/2'de yalnızca bilişim sistemine veri yerleştirilmesi söz konusu iken 135. maddede bilişim sistemi olsun ya da olmasın kayıt yapmaya elverişli her türlü araca yapılan kaydın suçun eylem unsurunu oluşturduğu görülür. Buna göre suçun konusu yönünden yalnızca kişisel verileri kapsaması nedeniyle 135. madde, eylem unsuru yönünden yalnızca bilişim sistemlerine yapılan kaydı kapsaması nedeniyle 244. madde diğerine göre "özel norm" niteliğindedir. Bu iki suç tipi arasında öncelikle özel norm – genel norm ayrımına göre bir sonuca ulaşılmaya çalışılmalı, bunun mümkün olmaması halinde fikri içtima kuralı uygulanmalıdır[151].

Bir başka olasılık ise özellikle kişilerin özel yaşamına ilişkin verilerin kaydedilmesi ya da verilmesi halinde 135. maddenin mi yoksa 134. maddenin mi uygulanacağına ilişkindir. Kişiyi belirlenebilir kılan bilgilerin ötesinde, onun özel yaşamını ortaya koyan görüntü ve sesler –bunlar da aslında kişisel veri oluştur-

148 Dülger, *Bilişim Suçları*, s. 701, 702, 716.
149 Dülger, *Bilişim Suçları*, s. 724.
150 Dülger, *Bilişim Suçları*, s. 717.
151 Dülger, *Bilişim Suçları*, s.702.

makla birlikte– korunan hukuksal değerler de göz önünde bulundurulduğunda artık kişisel verilerin kaydedilmesi suçunu değil, özel hayatın gizliliğini ihlal suçunu oluşturacağını düşünmekteyim. Yargıtay bu konuya ilişkin vermiş olduğu kararında aynı hususa vurgu yaparak 134. maddenin uygulanması gerektiğini belirtmiştir:

"A) Sanık hakkında kişisel verilerin kaydedilmesi suçundan verilen beraat hükmüne yönelik temyiz istemlerinin incelenmesinde; 5237 sayılı TCK'nın 135. maddesinde düzenlenen "Kişisel verilerin kaydedilmesi" suçunun oluşabilmesi için belirli veya belirlenebilir bir kişiye ait her türlü bilginin, hukuka aykırı olarak kaydedilmesi gerekmekte olup; suçun maddi konusunu oluşturan "kişisel veri" kavramından, kişinin, yetkisiz üçüncü kişilerin bilgisine sunmadığı, istediğinde başka kişilere açıklayarak ancak sınırlı bir çevre ile paylaştığı, herkes tarafından bilinmeyen ve/veya kolaylıkla ulaşılması ve bilinmesi mümkün olmayan, kişinin kimliğini belirleyen veya belirlenebilir kılan, kişiyi toplumda yer alan diğer bireylerden ayıran ve onun niteliklerini ortaya koymaya elverişli, gerçek kişiye ait her türlü bilginin anlaşılması gerektiği; bir özel hayat görüntüsü ya da sesinin, "kişisel veri" olduğunda kuşku bulunmamakta ise de, kişinin özel hayatına ilişkin görüntüsü ya da sesinin, bilgisi dışında, resim çekme veya kaydetme özelliğine sahip aletle belli bir elektronik, dijital, manyetik yere sabitlenmesi eyleminin, 5237 sayılı TCK'nın 134/1. maddesinin 2. cümlesinde tanımlanan özel hayatın gizliliğini ihlal suçu kapsamında değerlendirilmesi gerektiği, kişinin özel hayatına ilişkin görüntü, fotoğraf ya da sesin, 5237 sayılı TCK'nın 135. maddesi kapsamında kişisel veri olarak kabul edilemeyeceği, iddiaya konu olayda, mağdurenin çıplak vaziyetteki görüntü ve fotoğraflarının kaydedilmesinden ibaret eylemin, "Kişisel verilerin kaydedilmesi" suçunu oluşturmayacağı, çekimin, mağdurenin bilgisi ve rızası kapsamında gerçekleşmesi nedeniyle, özel hayatın gizliliğini ihlal suçunun da oluşmadığı anlaşıldığından, yapılan yargılama sonucunda, sanığa yüklenen suçun yasal unsurlarının oluşmadığı gerekçeleri gösterilerek mahkemece kabul ve takdir kılınmış olduğundan, katılan vekili ile C.Savcısının sanığa atılı suçun sabit olduğuna ilişkin ve yerinde görülmeyen tüm temyiz itirazlarının reddiyle, 5271 sayılı CMK'nın 223/9. maddesi de nazara alınarak, hükmün isteme uygun olarak ONANMASINA,..."[152].

Bir başka olayda ise Yargıtay kişinin günlük kıyafetleriyle çektirmiş olduğu resimlerin yayınlanmasını özel hayatın gizliliğini ihlal olarak değerlendirmemiş ancak, kişisel verilerin hukuka aykırı olarak yayılmasını suçunun oluştuğuna karar vermiştir:

152 12. CD. 11.9.2012, E. 2012/17703, K. 2012/18222.

"Katılanın internette yer alan günlük kıyafetleriyle poz vermiş şekilde çektirdiği resminin, özel yaşam alanına ilişkin ve özel hayatının gizliliğini ihlal edecek nitelikte olmaması karşısında, sanığa isnat edilen özel hayatın gizliliğini ihlal suçunun yasal unsurlarının somut olayda gerçekleşmediği ve katılanın kişisel veri niteliğindeki resmini hukuka aykırı olarak yayımlayan sanığın eyleminin TCK'nın 136. maddesinde tanımlanan verileri hukuka aykırı olarak verme veya ele geçirme suçunu oluşturacağı gözetilmeden, aynı eylemden dolayı sanık hakkında kişisel verilerin kaydedilmesi suçundan beraat hükmü kurulup, yasal ve yeterli olmayan gerekçelere dayalı olarak, TCK'nın 134/2. maddesinde düzenlenen özel hayatın gizliliğini ihlal suçundan mahkumiyet kararı verilmesi, (BOZMAYI) gerektirmiştir" [153].

Bir olayda mağdurenin çıplak durumda görüntülerinin kaydedilmesi ve bunların yayılması üzerine yapılan yargılama neticesinde ilk derece mahkemesi doğru olarak mağdurenin rızası ile görüntü kaydedildiği için 136. maddenin oluşmadığından bahisle sanık hakkında beraat kararı vermiş; ancak Yargıtay yerinde olarak, görüntü rıza olsun ya da olmasın kaydedildikten sonra bunların yayılmasının 134/1-2. cümlede tanımlanan suçu oluşturacağından bahisle ilk derece mahkemesinin bu yönden bozulmasına karar vermiştir:

"C) Sanık hakkında verileri hukuka aykırı olarak verme veya ele geçirme suçundan verilen beraat hükmüne yönelik temyiz istemlerinin incelenmesine gelince; 5237 sayılı TCK'nın 136/1. maddesinde düzenlenen "Verileri hukuka aykırı olarak verme veya ele geçirme" suçunun oluşabilmesi için, belirli veya belirlenebilir bir kişiye ait her türlü bilginin, başkasına verilmesi, yayılması ya da ele geçirilmesi gerekmekte olup, bir özel hayat görüntüsü ya da sesinin kaydedilmesi 5237 sayılı TCK'nın 134/1. maddesinin 2. cümlesinde; özel hayata ilişkin görüntü ya da sesin, taksirle ya da tamamen hukuka uygun elde edilmiş olsa dahi, ilgilisinin bilgisi ve rızası dışında ifşa edilmesi, yani; yayılması, açığa vurulması, afişe edilmesi, ilan edilmesi, kamuoyuna duyurulması, aleniyet kazandırılması, özetle; içeriğini öğrenme yetkisi bulunmayan kişi veya kişilerin bilgisine sunulması 5237 sayılı TCK'nın 134/2. maddesinde suç olarak düzenlenmiştir. Dosya içeriğine göre sanığın, mağdurenin bilgisi dahilinde çıplak vaziyetteki görüntü ve fotoğraflarını kaydedip, elde ettiği kayıtlarla oluşturduğu CD'leri, mağdurenin rızası olmaksızın, değişik zamanlarda farklı kurumlara göndermek fiilinin 5237 sayılı TCK'nın 134/2. maddesi kapsamında değerlendirilmesi yerine yasal ve yeterli olmayan gerekçelerle, sanık hakkında beraat kararı verilmesi, ... bozmayı gerektirmiş,..."[154]

153 12. CD. 7.7.2014, E. 2013/27724, K. 2014/16601.

154 12. CD. 11.9.2012, E. 2012/17703, K. 2012/18222.

Bu suçlar arasındaki en önemli bir içtima ilişkisi TCK'nın 138. maddesiyle KVKK'nın 17/2. maddesi arasındadır. Yukarıda da belirtiğim üzere, KVKK'nın 17/2. maddesi ile TCK m.138'de düzenlenen suçlar benzer ancak farklı bir suç tipleridir. Eğer yasa koyucu 6698 sayılı Yasanın 17/2. maddesine aykırılık halinde suçun tüm unsurları ile birlikte 138. maddenin uygulanmasını isteseydi "*5237 sayılı Kanunun 138 inci maddesi uygulanır*" ifadesini kullanırdı. Oysa yasa koyucu bunu yapmamış, 6698 sayılı KVKK'nın 17/2, 7 ve 3. maddelerinin birlikte uygulanmasıyla farklı bir suç tipi oluşturmuş ve "*5237 sayılı Kanunun 138 inci maddesine göre cezalandırılır*" ifadesini kullanmak suretiyle yalnızca yaptırım açısından TCK'nın 138. maddesinin uygulanacağını belirtmiştir. Ayrıca 138. maddeden farklı olarak, o maddede olmayan "anonimleştirmeyen" hareketine de yasa maddesinde yer vermiştir. Dolayısıyla söz konusu düzenlemenin bu şekilde anlaşılması ve buna göre yorum yapılması gerekir. Buna göre karşımıza çıkacak ihtimaller şunlardır:

Fail anonimleştirmesi gereken kişisel veriyi anonimleştirmemiş ise tartışma bulunmaz, bu hareketi yalnızca KVKK'nın 17/2. maddesi düzenlediği için bu madde uygulanır.

Fail silmesi gereken veriyi silmemişse, bu takdirde suçun konusuna bakılır. Eğer suçun konusunu oluşturan veri veya veri işleme faaliyeti 6698 sayılı KVKK'nın istisnaları içindeyse ve buna rağmen suç oluşuyorsa zaten yine uygulanabilecek tek norm vardır ve TCK'nın 138. maddesi uygulanır.

Silinmesi gerekirken silinmeyen kişisel veri 6698 sayılı KVKK'nın uygulandığı bir veri ise bu durumda hem KVKK'nın 17/2. maddesinin hem de TCK'nın 138. maddesi aynı anda uygulanabilir ve bu durumda fikri içtima kuralı uygulanabilir gibi görünse de bu hem teorik açıdan hatalı hem de bizi bir sonuca götürmeyen çözüm şeklidir. Bir çözüm getirmez zira KVKK'nın 17/2. maddesi ceza açısından TCK'nın 138. maddesine atıf yapmaktadır, dolayısıyla cezası daha ağır olan suçun tespiti bu açıdan olanaklı değildir. Öte yandan teorik açıdan hatalıdır, zira hem TCK ve hem de KVKK genel yasa formundadırlar ve aynı konuyu çok benzer şekilde biri diğerine ceza açısından atıf yaparak düzenlemektedir. Dolayısıyla sorun burada önceki genel yasa – sonraki genel yasa kuralından hareketle çözülmelidir. Buna göre hem TCK'nın 138 hem de KVKK'nın 17/2. maddelerinin kapsamında olan bir kişisel verinin silinmesi gerekirken silinmemesi halinde sonraki genel yasa olan KVKK'nın 17/2. maddesinin uygulanması gerekir.

Her dört suçun da zincirleme şekilde işlenmesi mümkündür. Ayrıca TCK 138 ve KVKK m.17/2. maddelerinde yer alan suçlar devam eden suç (mütemadi) niteliğindedirler; dolayısıyla bu suçun tamamlanma anı ile bitme anı farklıdır ve mütemadi suçlara ilişkin özellikler bu suçlar açısından geçerlidir. Öte yandan

135. ve 136. maddelerde düzenlenen suçların da devam eden suç şeklinde işlenmeleri mümkündür[155].

Kişisel verinin açıklanmasının aynı zamanda hakaret suçunu da oluşturması halinde, bir eylem ile birden fazla suçun oluşumuna neden olunduğu için, bu suçla hakaret suçu arasında fikri içtima söz konusudur. Failin sorumluluğu en ağır cezayı gerektiren suçtan olur[156]. Bu durumda kişisel verilerin açıklanması suçunun cezası daha fazla olduğu için faile bu suçtan dolayı ceza verilmesi gerekir. Nitekim Yargıtay da bu görüştedir:

"Dosya kapsamına göre; sanığın, kız arkadaşının husumetli olduğu mağdurlar adına, internette bir arkadaşlık sitesinde "Atesli_Dizdar" ve "Afet-i Derya" kullanıcı isimleri ile üyelik işlemleri yapıp, oluşturduğu profil sayfalarında, mağdurların şeref, onur ve saygınlığını rendice edecek nitelikte ibareler ile birlikte kişisel veri niteliğindeki fotoğraflarını ve telefon numaralarını ilgili siteye kaydedip, yayımlaması biçimindeki eyleminin, TCK'nın 135/1, 136/1 ve 125/2-1-4 maddelerine uyan, kişisel verilerin kaydedilmesi, verileri hukuka aykırı olarak verme veya ele geçirme ve hakaret suçlarını oluşturduğu, sanığın tek eyleminin kanundaki birden fazla suçları oluşturması nedeniyle TCK'nın 44. maddesinde düzenlenen fikri içtima kuralı uyarınca en ağır cezayı gerektiren TCK'nın 136/1. madde ve fıkrasında tanımlanan verileri hukuka aykırı olarak verme veya ele geçirme suçundan cezalandırılması gerektiği ve fikri içtima kuralı nazara alınmadan, daha hafif cezayı gerektiren TCK'nın 135/1. maddesi uyarınca hüküm kurulması, (BOZMAYI) gerektirmiştir"[157].

6. Yaptırım

İnceleme konusu her dört suç için de yasalarda yalnızca hürriyeti bağlayıcı ceza öngörülmüştür. Kişisel verilerin hukuka aykırı ele geçirilmesi suçunun cezası bir yıldan üç yıla kadar hapistir. Kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçunun cezası ise iki yıldan dört yıla kadar hapis cezasıdır. Kişisel verilerin yok edilmemesi suçunun cezası ise bir yıldan iki yıla kadar hapistir. KVKK'nın 17/2. maddesi ceza yönünden TCK'nın 138. maddesine atıf yaptığı için bu suçun cezası da bir yıldan iki yıla kadar hapistir.

Bunun yanı sıra kişisel verilerin hukuka aykırı ele geçirilmesi suçu açısından TCK'nın 135/2. maddesinde (yarısı kadar artırılır), kişisel verilerin hukuka aykırı ele geçirilmesi ile kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçu açısından TCK'nın 137. maddesinde (yarısı kadar artırılır), kişisel verilerin

155 Dülger, *Bilişim Suçları*, s. 702, 717.

156 Tezcan, Erdem, Önok, s. 632; Yokuş Sevük, s.810.

157 12. CD. 8.9.2014, E. 2014/1463, K. 2014/17262.

yok edilmemesi suçu ile kişisel verilerin silinmemesi ve anonim hale getirilmemesi suçları açısından TCK'nın 138/2. maddesinde (bir kat artırılır) cezayı artıran nitelikli haller öngörülmüştür.

TCK'nın 140. maddesi gereğince 135, 136 ve 138. maddelerde yer alan suçların işlenmesi neticesinde bundan herhangi bir tüzel kişinin hukuka aykırı yarar sağlaması halinde bunlara TCK'nın 60. maddesinde gösterilen kendilerine özgü güvenlik tedbirleri uygulanacaktır. KVKK'nın 17/2. maddesi açısından yalnızca cezalar açısından atıf yapılıp, güvenlik tedbirleri açısından bir düzenleme yapılmayarak tüzel kişilere yönelik bir düzenlemeye yer verilmediği için TCK'nın 60. maddesinin bu suç açısından uygulanması olanaklı değildir.

Bu suçlara bakmakla görevli mahkeme Asliye Ceza Mahkemesi'dir.

III. Sonuç Yerine: Kişisel Verilerin Korunması Alanındaki Sorunlar

6698 sayılı KVKK'nın 7.4.2016 tarihi itibariyle yürürlüğe girmesi ve Kişisel Veri Koruma Kurumu ve Kurulunun oluşturularak 1.1.2017 itibariyle kurul üyelerinin hepsinin seçilmiş olması ülkemizde kişisel verilerin korunması konusunda yeni bir dönemin başlangıcını ifade etmektedir. Böylelikle 7.4.2016 tarihine kadar özel olarak yalnızca TCK tarafından korunan kişisel veriler, artık hem ceza ve idare hukuku tarafından birlikte korunmakta hem de içi yalnızca tarafı olmadığımız uluslararası düzenlemeler ve öğreti tarafından doldurulan bu kavram ve bileşenleri artık bir yasa tarafından düzenlenmektedir. Böylelikle ceza hukuku açısından önemli olan belirlilik ilkesinin gereği de gerçekleşmiştir. Öte yandan 6698 sayılı Yasanın yasalaşmasının öncesinde Avrupa Konseyinin 108 sayılı Kişisel Verilerin Korunmasına İlişkin Sözleşmeyi uygun bulmamız da ülkemiz adına not edilmesi gereken önemli gelişmedir.

6698 sayılı KVKK'nın yürürlüğe girmiş olmasını ilke olarak olumlu bulmakla beraber, pek çok eksik ve hatalı düzenlemesinin olduğunu da belirtmeliyim. Yasanın uygulama kapsamı açısından istisnaların çok olması, özellikle kamu kurum ve kuruluşlarının bunlar içinde de kolluk güçlerinin ve istihbarat faaliyetlerinin tamamen yasa kapsamına dışına çıkarılmış olması kişisel verileri koruma hukukunu ruhuna aykırı düzenlemelerdir. Bu kişisel verileri toplayan ve işleyen kolluk ve istihbarat kuruluşlarında bu alana özgü iç ve dış denetimin olmaması, ülkemizde kamu kurum ve kuruluşların çoğunda hesap verme kültürünün oluşmaması uygulama açısından bu sorunları daha da artırmaktadır. Bir diğer önemli eleştiri konusu ise Kişisel Verileri Koruma Kurulu'nun çoğunluk üyelerinin siyasi iktidar ve çoğunluğu temsil eden parlamento grubu tarafından atanması ve özerk bir kurum olarak yapılandırılmamasıdır. Bu görünüşte de olsa kurumun ve kurulun tarafsızlığına gölge düşürmektedir. Arzu edilen, hem mevzuat, hem yapı hem de uygulama açısından bu kurumun ve kurulun tamamen

bağımsız olmasıdır. Ancak kurulun vereceği kararlar ve kurumun uygulamaları ile bu eleştiri olumlu ya da olumsuz anlamda netlik kazanacaktır. Dileğim bu eleştirimin tamamen boşa çıkmasıdır!

Bu başlık altında belirtilmesi gereken önemli bir husus yukarıda suç tiplerine ilişkin açıklamalarımda görüldüğü üzere suç tiplerinin düzenlenmesinde yalnızca kişisel verilerin hukuka aykırı yollardan ele geçirilmesi, yayılması ya da kayıtlı kişisel verilerin yok edilmemesinin ceza hukukunun koruması altına alınması ancak kişisel verilerin işlenmesinin bu koruma altına sokulmamasıdır. Oysa hukuka uygun olarak elde edilen ya da dağıtılan ve henüz yok edilmemesi gerekmeyen kişisel verilerin hukuka aykırı işlenmek suretiyle kötüye kullanılması da mümkündür. Bu durum düşünülmeyerek TCK'da gerekli suç tipine yer verilmemesi önemli bir eksiklik olarak görülmektedir. Bize göre kişisel verilerin hukuka aykırı olarak ve yetkisiz kişilerce işlenmesi de ayrı bir suç tipi haline getirilmelidir[158]. Zira 6698 sayılı KVKK'nın 3/1/e maddesinde kişisel verilerin işlenmesi TCK'nın 135 ve 136. maddelerinde yer alan hareketleri kapsayacak şekilde ancak onlardan daha geniş olarak düzenlenmiştir. Suç tiplerinin genişletilerek olmayan hareketler varmış gibi geniş yorumlanarak uygulanması ise suçtan ve cezada kanunilik ilkesi ve kıyasa varan genişletici yorum yasağı getiren TCK'nın 2/3. maddesi gereği yasaktır. Dolayısıyla anılan suçların kişisel verilerin işlenmesini kapsayacak şekilde yeniden düzenlenmesi gerekir.

Kişisel verilerin korunması konusunda, çıkarılacak yasa ve yönetmelikler, oluşturulacak kurum ve kurullar, ihlal halinde verilecek ciddi idari para cezaları ve hatta hapis cezaları hiçbir zaman tam bir çözüm ve ihlalleri önleme aracı olmayacaktır. Kişiler ve kurumlar öncelikle kullandıkları bilişim sistemlerinin güvenliğini sağlamak zorundadırlar. Bununla kastedilen sistemde bulunan verilerin ve sistemin kendisinin gizliliğinin, bütünlüğünün ve kullanıma yönelik her türlü tehlikelere karşı güvenliğinin sağlanmasıdır. Bunun için de kurumsal politikalar oluşturulmalı, kurum KVK politikasına ve ilgili mevzuata uyumlu hale getirilmeli ve uyumluluk düzenli olarak denetlenmelidir. Örneğin bir şirketin yönetim kurulu başkanı ve CEO'sundan kapıda içeri girenlerin kimliklerini alıp işleyen karşılama görevlisine kadar herkes bu politikanın uygulanması hususunda eğitimli ve istekli olmalıdır. Hem kamu sektörü hem de özel sektör iş yaptığı tüm çözüm ortakları, müşterileri, çalışanları vs.den bu alandaki mevzuata ve politikalara uyulmasını istemeli ve hatta buna uyumlu olduklarının kanıtlanmasını istemelidirler. Kurum içi uçtan uça uyumluluk ve sektör bazlı olarak tüm tarafların ve paydaşların uyumluluğu sağlanamadığı sürece kimse bu konuda rahat içinde olamayacaktır

158 Dülger, *Bilişim Suçları*, s. 725.

Alınacak güvenlik önemleriyle yalnızca verilerin korunmasına çalışılmamalıdır. Bu güvenlik önlemleriyle hem bilişim sistemleri için öngörülen güvenlik, hem sistemde bulunan verilerin gizliliği ve yetkisiz erişimlerin önlenmesi hem de sistemin kesintisiz olarak çalışması sağlanmalıdır[159]. Bugün için hem kamu hem de özel sektöre devredilmiş birçok kamu hizmeti tamamen bilişim sistemlerinin kontrolünde çalışmaktadır, bu sistemlerin çalışmasının kesintiye uğratılması toplumda büyük zararların doğmasına sebebiyet verebilir.

Ancak kişiler ve/veya kurumlar tarafından alınan bu önlemlere rağmen bilişim alanında tam güvenlik sağlanamamaktadır. Bilişim sistemlerinin güvenliği için geliştirilen bütün sistemlerin bir açığı bulunmakta ve bu açık nokta bulunarak sisteme girilmesi mümkün olmaktadır. Bu nedenden ötürü bilişim alanında kesin güvenlik değil, "en iyi güvenlik" sağlanmaya çalışılır. Bilişim suçlarının ve kişisel verilerin hukuka aykırı olarak ele geçirilmesinin önlenmesi ve bu eylemlere karşı iyi bir mücadelenin sağlanması için bireysel veya kurumsal bazda çalışan kullanıcıların, kendi sistemlerine uygun ve hem verileri hem de sistemin devamlılığını korumaya yönelik iyi bir güvenlik engeli oluşturmak ve kullanmak konusunda bilinçlendirilmeleri gerekir. Böylece bilişim alanında meydana gelen hukuka aykırı eylemlerin sayısında belirli bir azalma söz konusu olabilir. Kullanılacak bu güvenlik önlemleri gerçekleştirilen hukuka aykırı eylemleri de ortaya çıkaracağından, yeni ve daha etkili önlemlerin geliştirilmesinde etkili olacaktır[160].

Ülkeler bazında, bireylerin özel yaşamlarına müdahale etmeyi ve ülkelerinde bulunan insanları gözetlemeyi, fişlemeyi ve sürekli takibi bir yönetim şekli haline getiren devletlerde kişisel verilerin korunması ya hiç hukuksal düzenlenme konusu olmamıştır ya da bu düzenlemeler fiilen uygulanmamaktadır. Bazı ülkelerde ise devletin elindeki kişisel verilerin işlenmesine yönelik belirli güvenceler bulunurken, ekonomik gerekçelerle özel girişimlerin benzer uygulamalarına büyük oranda ılımlı yaklaşılmakta ya da göz yumulmaktadır. Kişisel verilerin korunması konusunda ciddi bir yaklaşım içinde bulunan ve önemli düzenlemelere sahip olan Avrupa Birliği'nde dahi konuya ilişkin pek çok sorun varlığını sürdürmektedir. Avrupa'nınki de dahil kişisel verilerin korunmasına ilişkin sistemlerin işlerliği önemli bir tartışma konusu oluşturmaktadır. Bu tartışmaların yoğunlaştığı hususlar ise kişisel verilerin korunmasının etkinliği, insan haklarına ve bireysel özgürlüklere uygunluğu, öte yandan ise bunların toplanması ve işlenmesinin ticaret ve suç ve suçlunun tespiti açısından son derece gerekli olmasıdır.

---

159 Berrin Akbulut, "Türk Ceza Hukukunda Bilişim Suçları", *Yayınlanmamış Doktora Tezi*, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Ceza ve Ceza Usul Hukuku Bilim Dalı, Konya, 1999, s. 245.

160 Dülger, *Bilişim Suçları*, s.726, 727.

KAYNAKLAR

- Akbulut, Berrin, "Türk Ceza Hukukunda Bilişim Suçları", *Yayınlanmamış Doktora Tezi*, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Ceza ve Ceza Usul Hukuku Bilim Dalı, Konya, 1999.
- Akgül, Aydın, *Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında, Kişisel Verilerin Korunması*, İstanbul, Beta Yayıncılık, 2014.
- Akyürek, Güçlü, "Kişisel Veriler ve Özel Hayatın Gizliliği Hakkı", *Suç ve Ceza – Ceza Hukuku Dergisi*, Türk Ceza Hukuku Derneği yayını, S.3, Temmuz – Ağustos – Eylül 2011, s.43 – 59.
- Altıparmak, Kerem, "Büyük Biraderin Gözetiminden Çıkış: Telefonların İzlenmesinde Devletin Sorumluluğu", *Türkiye Barolar Birliği Dergisi*, S.63, Mart – Nisan 2006, s.29 - 66.
- Ayözger, A. Çiğdem, *Kişisel Verilerin Korunması: Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil*, Beta, İstanbul, 2016.
- Başalp, Nilgün, *Kişisel Verilerin Korunması ve Saklanması*, Yetkin Yayınları, Ankara, 2004.
- Başalp, Nilgün, "Kişisel Verilerin Korunması ve İnternet" *İnternet ve Hukuk*, Der: Yeşim M. Atamer, İstanbul Bilgi Üniversitesi Yayını, İstanbul, 2004, s. 5 – 36.
- Bozkurt, Yüksel / Armağan, Ebru, *Bulut Bilişimde Kişisel Verilerin Korunması*, Ankara, Yetkin, 2016.
- Centel, Nur / Hamide, Zafer / Özlem, Çakmut, *Türk Ceza Hukukuna Giriş*, 9. Bası, Beta Yayıncılık, İstanbul, 2016.
- Clough, Jonathan, *Principles of Cybercrime*, Second Edition, Cambridge University Press, Cambridge, 2015.
- de Terwangne, Cécile, "The Right to be Forgotten and Informational Autonomy in the Digital Environment", *The Ethics of Memory in a Digital Age Interrogating the Right to be Forgotten*, Edited by Alessia Ghezzi/Ângela Guimarães Pereira/Lucia Vesnić-Alujević, European Commisson, Joint Research Centre, Palgrave Macmillan, 2014, s. 82 – 101.
- Değirmenci, Olgun, "Bilişim Suçları", *Yayınlanmamış Yüksek Lisans Tezi*, Marmara Üniversitesi Sosyal Bilimler Enstitüsü Hukuk Anabilim Dalı Kamu Hukuku Bilim Dalı, İstanbul, 2002.
- Doğru, Osman, *İnsan Hakları Avrupa Mahkemesi İçtihatları*, C.I, Legal Yayınevi, İstanbul, 2004.
- Donay, Süheyl, *Meslek Sırrının Açıklanması Suçu*, Sulhi Garan Matbaası, İstanbul, 1978.
- Dülger, Murat Volkan, *Bilişim Suçları ve İnternet İletişim Hukuku*, 6. Bası, Seçkin Yayıncılık, Ankara, 2015.
- Dülger, Murat Volkan, *Ceza Muhakemesi Hukukunda Dışlama Kuralı ve Hukuka Aykırı Delillerin Uzak Etkisi (Zehirli Ağacın Meyvesi Öğretisi)*, Seçkin Yayıncılık, Ankara, 2014.
- Dülger, Murat Volkan, "Bankacılık Sırrı ve Sırrın Açıklanmasına İlişkin Suçlar", *Banka ve Finans Hukuku, Panel ve Seminer Notları*, İstanbul Barosu Yayınları, 2009, s.169-204.
- Erdoğan, Yavuz, *Türk Ceza Kanunu'nda Bilişim Suçları (Avrupa konseyi Siber Suç*

Sözleşmesi ve Yargıtay Kararları ile), Legal, İstanbul, 2012.

- Erman, Sahir, *Kamu İdaresine Karşı İşlenen Suçlar (TCK 202 – 281)*, Dünya Yayıncılık, İstanbul, 1992.
- Ersoy, Uğur, "Bir İnsan Hakları Kavramı Olarak Kişisel Verilerin Korunması", *Yayınlanmamış Yüksek Lisans Tezi*, Gazi Üniversitesi Sosyal Bilimler Enstitüsü Kamu Yönetimi Anabilim Dalı Siyaset ve Sosyal Bilimler Bilim Dalı, Ankara, 2009.
- Etzioni, Amitai, *Privacy in a Cyber Age*, Palgrave Macmillan, New York, 2015.
- Gülmez, Lütfü Cihan, "Kişisel Verilerimiz Korunuyor mu?", *Terazi Hukuk Dergisi*, Y.6, S.59, Temmuz 2011, s. 57 - 65.
- Hakeri, Hakan, *Ceza Hukuku Genel Hükümler*, 19. Bası, Adalet Yayınevi, Ankara, 2016.
- Hakeri, Hakan, "Verileri Hukuka Aykırı Olarak Verme (Sır Saklama Yükümlülüğünün İhlali) Suçu", *Tıbbi Müdahaleden Kaynaklanan Hukuki Sorumluluk Sempozyumu, 16 – 17 Ocak 2009*, Mersin Barosu Yayını, Mersin, 2009, s. 126 - 131.
- İçel, Kayıhan, *Ceza Hukuku Genel Hükümler*, Yenilenmiş Bası, Beta Yayıncılık, İstanbul, 2016.
- Jones, Meg Leta, *Ctrl + Z: The Right to Be Forgotten*, New York University Press, New York, 2016.
- Karagülmez, Ali, *Bilişim Suçları ve Soruşturma – Kovuşturma Evreleri*, 5. Bası, Seçkin Yayıncılık, Ankara, 2014.
- Kaya, Cemil, "Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi, *İÜHFM*, C.LXIX, S.1 - 2, 2001, s. 317 - 334.
- Küzeci, Elif, *Kişisel Verilerin Korunması*, Turhan Kitapevi, Ankara, 2010.
- Lloyd, Ian J., *Information Technology Law*, 6th Edition, Oxford University Press, Oxford, 2011.
- Martin, Yod-Samuel/Jose M. Del Alamo, "Forget About Being Forgetten", *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*, Eds: Serge Gutwirth/Ronald Leenes/Paul De Hert, Springer, Heidelberg, 2016, s. 249 – 276.
- Orwell, George, *Bin Dokuz Yüz Seksen Dört*, Çev: Nuran Akgören, Can Yayınları, İstanbul, 1999.
- Özbek, Veli Özer / M. Nihat Kanbur / Koray Doğan / Pınar Bacaksız / İlker Tepe, *Türk Ceza Hukuku Genel Hükümler*, 7. Bası, Seçkin Yayıncılık, Ankara, 2016.
- Özel, Sibel, *Uluslararası Alanda Medya ve İnternette Kişilik Hakkının Korunması*, Seçkin Yayıncılık, Ankara, 2004.
- Özgenç, İzzet, *Türk Ceza Hukuku*, 12. Bası, Seçkin Yayıncılık, Ankara, 2016.
- Steijn, Wouter Martinus Petrus, "The Coast of Using Facebook: Assigning Value to Privacy Protection on Social Network Sites Against Data Mining, Identity Theft, and Social Conflict", *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*, Eds: Serge Gutwirth/Ronald Leenes/Paul De Hert, Springer, Heidelberg, 2016, s. 323-343.
- Tezcan, Durmuş / Mustafa Ruhan Erdem / R. Murat Önok, *Teorik ve Pratik Ceza Özel Hukuku*, 13. Bası, Seçkin Yayıncılık, Ankara, 2016.
- Ünver, Yener, "Türk Ceza Kanunu'nun ve Ceza Kanunu Tasarısının İnternet Açısın-

dan Değerlendirilmesi", *İÜHFM*, C.LIX, S.1 – 2, İstanbul, 2001, s.51 - 153.

- Ünver, Yener, "Federal Almanya'da Terör ve Organize Suçluluk ile İlgili Düzenlemeler", *Prof. Dr. Nurullah Kunter'e Armağan*, İÜHF Eğitim Öğretim ve Yardımlaşma Vakfı Yayını, İstanbul, 1998, s.385 - 464.
- Walden, Ian, *Computer Crimes and Digital Investigations*, Second Edition, Oxford University Press, Oxford, 2016.
- Yılmaz, Sabire Sabem, *Tıp Alanında Kişisel Verilerin Açıklanması Suçu*, Seçkin, Ankara, 2014.
- Yokuş Sevük, Handan, "Tıp Ceza Hukukunda Kişisel Verilerin Açıklanması", *Tıp Ceza Hukukunun Güncel Sorunları*, Türkiye Barolar Birliği Yayını, Ankara, 2008, s.782-811.

ÖZ

Belirli veya kimliği belirlenebilir gerçek kişiye ilişkin tüm veriler olarak tanımlanabilecek kişisel verilerin korunması, insan haklarından olan özel hayat ve aile hayatına saygı hakkı bakımından önem arz eder. Kişisel verilerin korunması konusu günümüzde gittikçe önem kazanmakta, hem bireyler günlük yaşamlarında bu konuda pek çok yakınmada bulunmakta hem de konu üst düzey yargı organlarının hukuksal tavır almalarına neden olmaktadır. Bu doğrultuda Avrupa Konseyi ve Avrupa Birliği başta olmak üzere pek çok ulusal üstü örgüt ve devlet tarafından kişisel verilerin korunması alanı düzenlenmiştir. Türkiye, geç kalınmış olsa da bu alanı düzenleyen 6698 sayılı Kişisel Verilerin Korunması Kanunu'nu kabul etmiştir. Kişisel verilerin ceza normlarıyla korunması ise Türk Ceza Kanunundaki suç tipleriyle sağlanmaktadır. Bu bağlamda ele alınması gereken suç tipleri: TCK 135-138. maddelerde düzenlenen Kişisel Verilerin Kaydedilmesi suçu, Verileri Hukuka Aykırı Olarak Verme Veya Ele Geçirme suçu ve Verilerin Yok Edilmemesi suçu ve 6698 sayılı Yasanın 17/2 maddesinde düzenlenen Kişisel Verilerin Silinmemesi veya Anonim Hale Getirilmemesi suçudur.

Anahtar Kelimeler: Kişisel veri, Özel hayatın gizliliği, Veri koruma, Özel hayata karşı suç, Verilerin işlenmesi, Veri sahibi.