PART 15

CRIMES AGAINST TO PERSONAL DATA WITH IN THE SCOPE OF THE TURKISH PENAL CODE

TÜRK CEZA KANUNU KAPSAMINDA YER ALAN KİŞİSEL VERİLERE KARŞI SUÇLAR

--

ECE TAŞÇI AYDEMİR
SEDANUR ÖZÇELİK

ABSTRACT

Although developments in information and communication technologies have made our lives easier, increasing data flow has become almost uncontrollable. Because of this, the importance of the protection of personal data has increased and regulations for this have begun to be introduced all over the world. Likewise, Turkey, being a party to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, has introduced a number of measures to the Turkish Penal Code to include crimes against personal data. This study discusses "personal data", a relatively new concept in Turkish Law, and crimes regarding the protection of personal data in the Turkish Penal Code No. 5237.

KEYWORDS

PERSONAL DATA, CRIMES AGAINST TO PERSONAL DATA, TURKISH PENAL CODE, PRIVACY OF PRIVATE LIFE.

ÖZET

Bilgi ve iletişim teknolojilerindeki gelişme her ne kadar hayatımızı kolaylaştırsa da gün geçtikçe, veri akışı kontrol altına alınmaz hale gelmeye başlamıştır. Bu sebeple kişisel verilerin korunmasının önemi artmış ve dünyanın her yerinde bu konuyla ilgili düzenlemeler yapılmaya başlanmıştır. Türkiye'nin uluslararası alanda kabul edilmiş Kişisel Verilerin Otomatik Olarak İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Avrupa Konseyi Sözleşmesi'ne taraf olması ile Türkiye de aynı şekilde birtakım önlemler almış, Türk Ceza Kanunu kapsamına kişisel verilere karşı suçlar da dahil edilmiştir. Bu çalışmada; Türk Hukuku'na yakın tarihte girmiş kavramlardan biri olan "kişisel veri" ve 5237 sayılı Türk Ceza Kanunu'nda kişisel verilerin korunması alanında değerlendirilen suçlar ele alınmıştır.

ANAHTAR KELİMELER

KİŞİSEL VERİ, KİŞİSEL VERİLERE KARŞI SUÇLAR, TÜRK CEZA KANUNU, ÖZEL HAYATIN GİZLİLİĞİ.

PART 15

This article looks at crimes related to the protection of personal data and explains, first, the concept of personal data, followed by crimes, and elements of these crimes, against personal data as set out in Turkish Penal Code No.5237.

Kişisel verilerin korunmasına yönelik suçları ele alan bu makalede; öncelikle kişisel veri kavramına değinilecek, sonraki bölümlerde 5237 sayılı Türk Ceza Kanunu'nun kişisel verilere karşı suçların neler olduğu ve unsurları açıklanacaktır.

I. INTRODUCTION

As technology has rapidly developed and information has become global, personal information has become data that is easy to share and access. Although developments in technology benefit individuals, the transfer of information from paper to digital media increases the potential for violations against personal rights. For this reason, protection of personal data has become an obligation. The basis of the protection of personal data is the right to privacy regarding our private life. The right to privacy is a fundamental right guaranteed by certain laws and contracts all over the world. The European Convention on Human Rights ("ECHR") does not include a direct article on the protection of personal data, but applications to the European Court of Human Rights ("ECtHR") regarding personal data are examined[1] under Article 8 of the ECHR, "Respect for Private and Family Life" and the protection of private life[2]. Similarly, following the referendum held on September 12, 2010, the right to "request the protection of personal data" was added to Article 20 of the Turkish Constitution[3] under the title "Privacy of Private Life". This right, which is guaranteed by the Constitution, is supported by Law No. 6698 on the Protection of Personal Data ("KVKK") adopted in 2016. In addition to these regulations for the protection of personal data, it was necessary to define new types of crimes in order to protect individuals security. Accordingly, Turkish Penal Code No.5237, which entered into force on June 1, 2005, included crimes related to the protection of personal data in order to provide a legal basis for protection. This replaced Turkish Penal Code No.765, which did not address the issue.

This article looks at crimes related to the protection of personal data and explains, first, the concept of personal data, followed by crimes, and elements of these crimes, against personal data as set out in Turkish Penal Code No.5237.

II. DEFINITION OF PERSONAL DATA

The concept of personal data has recently entered the legal world following developments in science and technology. The first international studies on the protection of personal data were carried out by the Organization for Economic Cooperation and Development ("OECD")[4].

In the first article of the Guidelines on the Protection of Privacy and Transborder Flows

FOOTNOTE

1 Berrak Yılmaz, "Türk Anayasa Mahkemesi Ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması", Unpublished Phd Thesis, Ankara, 2019, pg. 33-36.

2 "Kişisel Verilerin Korunması Alanında Uluslararası ve Ulusal Düzenlemeler" https://www.kvkk.gov.tr/ (Date Accessed:04.03.2021)

3 Constitution of Republic Of Turkey, 20th Article.

4 Çiğdem Ayözger, "Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dâhil Kişisel Verilerin Korunması", Beta Press, İstanbul 2016, pg. 60.

I. GİRİŞ

Teknolojinin hızla geliştiği, dünya ile birlikte bilgilerinde küreselleştiği kişisel bilgiler; yakın dönemde paylaşılması ve ulaşılması kolay veriler haline gelmiştir. Günümüzde; teknolojide yaşanan bu tür gelişmeler her ne kadar kişilerin menfaatine yönelik olsa da, bilgilerin kâğıtların arasından dijital ortama aktarılması, hak ihlallerini artırmaktadır. Bu sebeple kişisel verilerin korunması bir zorunluluk haline gelmiştir. Kişisel verilerin korunmasının özü, özel hayatın gizliliğine dayanmaktadır. Özel hayatın gizliliği dünyanın her yerinde belli yasalarla ve sözleşmelerle güvence altına alınan, kişinin temel haklarından biridir. Bu kapsamda; Avrupa İnsan Hakları Sözleşmesi'nde ("AİHS") kişisel verilerin korunmasıyla ilgili doğrudan bir maddeye yer verilmemiş olmakla birlikte, Avrupa İnsan Hakları Mahkemesi ("AİHM") kişisel verilere ilişkin başvuruları Avrupa İnsan Hakları Sözleşmesi'nin "Özel ve Aile Hayatına Saygı Hakkı" başlıklı 8. maddesi kapsamında incelemekte[1] ve özel hayat alanı içinde değerlendirmektedir[2]. Benzer biçimde; T.C. Anayasası'nın 20. maddesi[3] ile "Özel Hayatın Gizliliği" başlığı altında düzenlenen bu hakkın kapsamına 12 Eylül 2010 tarihinde yapılan referandumla birlikte "kişisel verilerin korunmasını isteme" hakkı da eklenmiştir. Anayasamızla güvence altına alınmış bu hak, 2016 yılında kabul edilen 6698 Sayılı Kişisel Verilerin Korunması Kanunu ("KVKK") ile desteklenmiştir. Kişisel verilerin korunması yönünde yapılan bu düzenlemelerin yanında, kişilerin güvenliğini sağlamak ve korumak adına yeni suç tiplerinin yaratılması gerekmiştir. Buna istinaden hukuksal zeminin sağlanması adına 1 Haziran 2005 tarihinde yürürlüğe giren 5237 sayılı Türk Ceza Kanunu ile yürürlükten kalkmış olan 765 sayılı TCK'dan farklı olarak kişisel verilerin korunmasına ilişkin suçlara yer verilmiştir.

Kişisel verilerin korunmasına yönelik suçları ele alan bu makalede; öncelikle kişisel veri kavramına değinilecek, sonraki bölümlerde 5237 sayılı Türk Ceza Kanunu'nun kişisel verilere karşı suçların neler olduğu ve unsurları açıklanacaktır.

II. KİŞİSEL VERİ TANIMI

Bilim ve teknoloji çağının beraberinde getirdiği bir kavram olan kişisel veri kavramı, hukuk dünyasına da yakın zamanda girmiştir. Kişisel verilerin korunmasına dair uluslararası yapılan ilk çalışmalar Ekonomik İşbirliği ve Kalkınma Örgütü ("OECD") tarafından yapılmıştır[4].

OECD tarafından 1980 yılında kabul edilen Kişisel Verilerin Sınır Aşan Tra-

DİPNOT

1 Berrak Yılmaz, "Türk Anayasa Mahkemesi Ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması", Yayınlanmamış Doktora Tezi Ankara, 2019 ss. 33-36.

2 "Kişisel Verilerin Korunması Alanında Uluslararası ve Ulusal Düzenlemeler" https://www.kvkk.gov.tr/ (Erişim Tarihi:04.03.2021)

3 T.C. Anayasası md. 20: "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir.

4 Çiğdem Ayözger, Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dâhil Kişisel Verilerin Korunması, Beta Yayınları, İstanbul 2016, s. 60.

PART 15

of Personal Data, adopted by the OECD in 1980, personal data is defined as "any information relating to an identified or identifiable individual". The first binding contract accepted in the international arena on January 28, 1981 is the Council of Europe Convention on the Protection of Natural Persons During Automatic Processing of Personal Data[5]. According to this contract, personal data is "any information related to an identified or identifiable natural person"[6]. In the General Data Protection Regulation ("GDPR"), which has made a big impact worldwide and is accepted by the European Parliament, the definition of personal data is not essentially different from all other definitions: "any information relating to an identified or identifiable natural person an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person ". What the GDPR definition provides is a detailed definition including concrete examples[7]. As a result, this has become the generally accepted definition and the KVKK, currently in force in Turkey, states the definition of personal data similarly as "all kinds of information belonging to an identified or identifiable natural person".
A decision of the 12th Criminal Chamber of the Supreme Court states:
"From the concept of personal data, the identity information (such as identity number, name, surname, place of birth and date, name of mother and father), criminal record, which the person does not provide to the information of unauthorized third parties, discloses it to other people whenever he wants, but shares it with a limited environment, place of residence, educational status, occupation, bank account information, phone number, e-mail address, blood type, marital status, fingerprint, DNA, biological samples such as hair, saliva, nails, sexual and moral inclination, health information, ethnic It is necessary to understand all kinds of information belonging to a natural person, such as their origin, political, philosophical and religious view, trade union affiliations, that

fiği ve Verilerin Korunmasına İlişkin Kılavuz İlkeleri'nin birinci maddesinde kişisel veri "belirli veya belirlenebilir bir gerçek kişiye ilişkin tüm bilgiler" olarak tanımlanmıştır. Uluslararası alanda 28 Ocak 1981 yılında kabul edilmiş ilk bağlayıcı sözleşme ise Kişisel Verilerin Otomatik Olarak İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Avrupa Konseyi Sözleşmesi'dir[5]. Bu sözleşmeye göre, kişisel veri "kimliği belirtilen veya belirtilebilen gerçek kişiye ait her türlü bilgiler" dir[6]. Yine uluslararası alanda dünya genelinde ses getiren ve Avrupa Parlamentosu tarafından kabul edilen Genel Veri Koruma Tüzüğü'nde ("GDPR") kişisel verinin tanımı esasen farklılık göstermemekle birlikte "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi kişisel veriyi ifade etmekte olup, doğrudan veya dolaylı olarak, bir gerçek kişinin tanımlanmasına elverişli başta isim, kimlik numarası, konum/yer bilgisi, bir çevrimiçi tanımlayıcı yahut kişinin fiziki, fizyolojik, genetik, zihinsel, ekonomik, kültürel veya sosyal kimliğine özgü bir veya daha fazla hususa işaret eden her türlü veri" şeklinde tanımlanmıştır. Görüleceği üzere GDPR'de; kişisel verinin tanımı, soyut tanımın yanında örneklendirme yoluyla detaylandırılmıştır[7]. Bu tanım, genel kabul gören bir tanım olup, ülkemizde şuan yürürlükte bulunan KVKK'da kişisel verinin tanımı "kimliği belirli veya belirlenebilir gerçek kişiye ait her türlü bilgi" olarak benzer şekilde düzenlenmiştir.
Yargıtay; 12. Yargıtay Ceza Dairesi'nin uyuşmazlık konusu olay hakkında verdiği bir kararında,
"kişisel veri kavramından, kişinin, yetkisiz üçüncü kişilerin bilgisine sunmadığı, istediğinde başka kişilere açıklayarak ancak sınırlı bir çevre ile paylaştığı nüfus bilgileri (T.C. kimlik numarası, adı, soyadı, doğum yeri ve tarihi, anne ve baba adı gibi), adli sicil kaydı, yerleşim yeri, eğitim durumu, mesleği, banka hesap bilgileri, telefon numarası, elektronik posta adresi, kan grubu, medeni hali, parmak izi, DNA'sı, saç, tükürük, tırnak gibi biyolojik örnekleri, cinsel ve ahlaki eğilimi, sağlık bilgileri, etnik kökeni, siyasi, felsefi ve dini görüşü, sendikal bağlantıları gibi kişinin kimliğini belirleyen veya belirlenebilir kılan,

FOOTNOTE

5 Mahmut Koca, İlhan Üzülmez, "Kişisel Verilerin Kaydedilmesi Suçu (TCK m. 135)" Dokuz Eylül University Faculty of Law Journal, Prof. Dr. Durmuş TEZCAN'a Armağan, V. 21, Special İssue., 2019, pg. 71.

6 İbrahim Korkmaz, "Kişisel Verilerin Ceza Hukuku Kapsamında Korunması", Ankara, Seçkin Press, 2019, pg. 25.

7 General Data Protection Regulation, Çevrimiçi Erişim İçin Bkz: https://gdpr-info.eu/ (Date Accessed:11.02.2020).

8 12th Criminal Chamber of the Supreme Court, 18.09.2019 dated, 2018/8466 E. ve 2019/9054 K. numbered decision. www.kazanci.com, (Date Accessed: 05.03.2021)

9 http://sozluk.gov.tr/ (Date Accessed:11.02.2020)

10 Hüseyin Can Aksoy, "Kişisel Verilerin Korunması", Unpublished Master Thesis, Ankara University, 2008, pg. 18.

11 Aksoy, pg. 19.

determine the identity of the person or make them identifiable, distinguish the person from other individuals in the society and are suitable for revealing his qualities."[8]
This states that personal data can come from sampling. As can be seen, personal data cannot be narrowed down to stored information. On the contrary and in the scope of this article, personal data refers to all kinds of information belonging to a real person.

A. Elements of Personal Data

There seems to be a consensus on the definition of the concept of "personal data" in laws and contracts. On the basis of this definition, it can be said that the concept of personal data consists of three elements.

1. Information

First of all, when we look at the criteria required in law, there must be data. In the Turkish Language Institution Dictionary, the concept of data is defined as "information, data". What is meant by data is all kinds of information belonging to the person[9]. There is no difference between whether the data is objective or subjective, it is sufficient that it is personal data belonging to a person, including subjective information describing a person, for example, as rich or poor[10]. At the same time, data should be evaluated regardless of the environment where it is located. The fact that whether data is in the digital environment or on paper does not affect the feature of that data being personal data[11]. In addition, the type of data is also irrelevant. Written, audio, and visual, "all kinds of information" are also considered within the scope of personal data.

2. Identified or Identifiable Person

Another element of the definition of personal data is whether the person is "identified or identifiable". The issue of how to determine whether a person is identified or identifiable is important because determining whether certain information comes within in the scope of personal data is based on whether it belongs to an identified or identifiable person. At this point, it is worth asking whether the informa-

kişiyi toplumda yer alan diğer bireylerden ayıran ve onun niteliklerini ortaya koymaya elverişli, gerçek kişiye ait her türlü bilginin anlaşılması gerekir"[8]
şeklinde kişisel verinin neler olabileceğini tek tek örnekleme olarak saymıştır. Görüldüğü üzere; kişisel veri saklanan bilgi olarak daraltılamamış, aksine gerçek kişiye ait her türlü bilginin bu kapsama dahil edileceği belirtilmiştir.

A. Kişisel Verinin Unsurları

Kanun ve sözleşmelerde "kişisel veri" kavramının tanımı üzerinde görüş birliği bulunduğu görünmektedir. Bu tanımdan yola çıkacak olursak, kişisel veri kavramının üç unsurdan oluştuğunu söyleyebiliriz:

1. Bilgi

Kanunda aranan kriterlere baktığımızda öncelikle bir verinin bulunması gerekmektedir. Veri kavramı TDK'da 'bilgi, data' şeklinde tanımlanmıştır[9]. Veriden kastedilen, kişiye ait her türlü bilgidir. Verinin nesnel ya da öznel olması arasında fark yoktur; kişiye ait, kişisel bir veri olması yeterlidir. Bir kimsenin zengin veya fakir olduğu gibi öznel bilgiler de kişisel veri kapmasına girmektedir[10]. Aynı zamanda verinin, bulunduğu ortamdan bağımsız olarak değerlendirilmesi gerekir. Verinin dijital ortamda veya kâğıt üzerinde yer almaması, o verinin kişisel veri olma özelliğini etkilemeyecektir[11]. Bunların yanında yine verinin türü de önemsizdir. Yazılı, sesli, resimli "her türlü bilgi" de kişisel veri kapsamında değerlendirilir.

2. Belirli veya Belirlenebilir Kişi

Kişisel veri tanımının diğer bir unsuru ise "belirli veya belirlenebilir" bir kişinin bulunmasıdır. Belirli veya belirlenebilir kişinin nasıl tespit edileceği önem arz etmektedir. Çünkü kişisel veri kapsamına giren bilgiler, ait oldukları kişinin, belirli veya belirlenebilir olmasının tespiti ile sağlanacaktır. Bu noktada tüzel kişilere ait bilgilerin kişisel veri kapsamında kalıp kalmayacağı tartışılabilir. Uluslа-

DİPNOT

5 Mahmut Koca, İlhan Üzülmez, "Kişisel Verilerin Kaydedilmesi Suçu (TCK m. 135)" Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, Prof. Dr. Durmuş TEZCAN'a Armağan, C. 21, Özel S., 2019, s. 71.

6 İbrahim Korkmaz, Kişisel Verilerin Ceza Hukuku Kapsamında Korunması, Ankara, Seçkin, 2019, s. 25.

7 General Data Protection Regulation, Çevrimiçi Erişim İçin Bkz: https://gdpr-info.eu/, Türkçe Metin İçin Bkz: https://www.kisiselverilerinkorunmasi.org/mevzuat/avrupa-birligi-genel-veri-koruma-tuzugu-gdpr-turkce-ceviri/ (Erişim Tarihi:11.02.2020).

8 Yargıtay 12. Ceza Dairesi'nin 18.09.2019 tarihli, 2018/8466 E. ve 2019/9054 K. Sayılı ilamı, www.kazanci.com, (Erişim Tarihi: 05.03.2021)

9 http://sozluk.gov.tr/ (Erişim Tarihi:11.02.2020)

10 Hüseyin Can Aksoy, "Kişisel Verilerin Korunması", Yayınlanmamış Yüksek Lisans Tezi, Ankara Üniversitesi, 2008, s. 18.

11 Aksoy, s. 19.

PART 15

tion of legal entities comes within the scope of personal data. Although there is no international consensus regarding this issue, only natural persons are mentioned in OECD and Council of Europe conventions. While the EU directive mentions natural persons, it is stated by EU that legal persons can be included in the regulations at national level[12].

Only real persons are mentioned in the KVKK and, in an application made on this issue, the Personal Data Protection Board decided that the information of legal entities does not come within this scope[13]. Data belonging to a legal person and data belonging to a real person within the legal person are different concepts. The protection of data belonging to legal entities generally comes under protection in connection with confidential business information. Information can be associated with a real and identified/identifiable person even if it belongs to a legal entity or comes within the body of a legal entity, and must be protected within the scope of personal data, as included in the KVKK. For example, the owner of data on a card containing an employee's corporate e-mail and phone number identifies a certain person. In this context, even though it is data within a legal entity, it should come within the scope of the protection of personal data. However, unrelated data such as the title of a trading company should be excluded from this scope[14].

3. Being Relevant

The last element according to the definition in the KVKK is that the information must be related to a real person. The connection between the person and the data can sometimes be established directly and sometimes indirectly. The relatedness element is determined by whether it is directly linked. Indirect links are where an individual is associated with information even though they may not be individually identifiable[15]. For example, information held in data concerns objects not individuals. These objects usually belong to someone and can be indirectly associated with that person. Being relevant can be in terms of "content", "purpose" and "result"[16]. For example, the information in a person's CV is linked to the person in terms of content. A Resume is part of a system established to provide a better and quicker service as your location can be detected so you are offered nearby locations.

rarası sözleşmelerde bu konuda mutabakat bulunmamakla birlikte; OECD ve Avrupa Konseyi tarafından düzenlenen sözleşmelerde sadece gerçek kişilerden bahsederken, AB tarafından çıkarılan yönergede gerçek kişilerden bahsedilmiş olmakla beraber ulusal düzeyde yer alan düzenlemelerle tüzel kişilerin de dâhil edilebileceği belirtilmiştir[12].

KVKK'da da sadece gerçek kişilerden bahsedilmiş olmakla beraber, bu konu üzerine yapılmış bir başvuruda, Kişisel Verileri Koruma Kurulu'nun tüzel kişilere ait bilgilerin bu kapsamda kalmayacağına dair kararı bulunmaktadır[13]. Tüzel kişiye ait veri ile tüzel kişi bünyesindeki gerçek kişiye ait veri farklı kavramlardır. Tüzel kişilere ait verilerin korunması, genel olarak ticari sır ile bağlantılı olarak koruma altına alınmaktadır. Tüzel kişilik bünyesinde bulunup, tüzel kişilere ait bilgiler dahi gerçek ve belirli bir kişiyle ilişkilendirilebiliyorsa, KVKK'da yer alan kişisel veri kapsamı dahilinde korunmalıdır. Örneğin bir firmanın çalışanının kurumsal e-posta ve telefon numarasının bulunduğu karttaki verilerin sahibi yine belirli bir kişidir ve bu bağlamda her ne kadar tüzel kişi bünyesinde bulunan bir veri de olsa, kişisel verilerin korunması kapsamında yer almalıdır. Bununla birlikte; bir ticaret şirketinin unvanı gibi kişiyle bağlantısı olmayan veriler, bu kapsam dışında tutulmalıdır[14].

3. İlişkin Olma

KVKK'da yer alan tanıma göre son unsur ise bilginin gerçek bir kişiye ilişkin olmasıdır. Bulunan verinin kişi ile bağlantılı olması gerekir. Kişi ile veri arasındaki bağlantı, kimi zaman doğrudan kurulabilirken kimi zaman dolaylı olarak kurulabilir. Doğrudan bağlantı kurulabilen haller, ilişkin olma unsurunu tamamlar. Kişilerin kimliğini tanımlamamakla birlikte kendisiyle ilgili herhangi bir kayıtla ilişkilendirilmesi durumunda, dolaylı olarak ilişkin olduğunu söylememiz gerekir[15]. Örneğin; veriler tarafından taşınan bilgiler, bireyleri değil, ilk etapta nesneleri ilgilendirir. Bu nesneler genellikle birisine aittir ve dolaylı yoldan o kişiyle ilişkilendirilebilir. İlişkin olma durumu "içerik", "amaç" ve "sonuç" yönünden olabilir[16]. Örneğin bir kişinin özgeçmişinde yer alan bilgiler, içerik yönüyle kişi ile bağlantılıdır. Bir uygulamanın sizin konumunuzu tespit ederek size en yakın mekânları sunması, daha kısa sürede daha iyi bir hizmet vermek amacıyla kurulmuş bir sistemdir.

The concept of "personal data" has a generally accepted definition in the light of the elements explained above. According to this definition, the concept of personal data is a very extensive concept, and the issue of which data comes within the scope of personal data is important. As technology develops daily and new systems are created, new aspects are added to the concept of personal data. For this reason, it is necessary for international conventions and laws to make such a wide definition and avoid a limited census.

"Kişisel veri" kavramı yukarıda açıklanan unsurlar ışığında genel olarak kabul görmüş bir tanıma sahiptir. Bu tanıma göre kişisel veri kavramı oldukça geniş bir kavram olup, hangi verilerin kişisel veri kapsamında kaldığı hususu önem arz etmektedir. Teknolojinin gelişmesi ve yeni sistemlerin oluşmasıyla kişisel veri kavramı içine her gün bir yenisi eklenmektedir. Bu sebeple uluslararası sözleşmelerde ve kanunlarda bu derece geniş bir tanımlama yapılması ve tahdidi bir sayımdan kaçınılması bilgi çağının bir gerekliliğidir.

It is necessary for international conventions and laws to make such a wide definition and avoid a limited census.

Uluslararası sözleşmelerde ve kanunlarda bu derece geniş bir tanımlama yapılması ve tahdidi bir sayımdan kaçınılması bilgi çağının bir gerekliliğidir.

III. CRIMES REGARDING THE PROTECTION OF PERSONAL DATA IN TURKISH CRIMINAL LAW

A. Offense of Recording Personal Data

Article 135 of the Turkish Penal Code ("TPC"), "recording personal data illegally" is regulated as a crime. In the first paragraph of the Article, the basic form of the crime is regulated and, in the second paragraph, the illegal recording of some private personal data is regulated to qualify as a crime. The legislator stated this on the grounds that this Article was prepared in order to prevent violations of rights that may occur due to the use of data within the body of some institutions and organizations for purposes other than their intended purpose or unlawfully giving them to third parties[17]. The TPC states that:
"(1) Any person who unlawfully records the personal data is punished with imprisonment from six months to three years.

III. KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN TÜRK CEZA KANUNU'NDA YER ALAN SUÇLAR

A. Kişisel Verilerin Kaydedilmesi Suçu

Türk Ceza Kanunu ("TCK") madde 135'te "kişisel verilerin hukuka aykırı olarak kaydedilmesi" suç olarak düzenlenmiştir. Maddenin birinci fıkrasında suçun temel şekli düzenlenmiş olup, ikinci fıkrasında özel nitelikteki bazı kişisel verilerin hukuka aykırı kaydedilmesi, suçun nitelikli hali olarak düzenlenmiştir. Kanun koyucu; bu maddenin, bazı kurum ve kuruluşların bünyesinde bulunan verileri amaçları dışında kullanmaları veya hukuka aykırı olarak üçüncü kişilere vermeleri sebebiyle oluşacak hak ihlallerinin önüne geçmek için düzenlendiğini gerekçede belirtmiştir[17]. TCK'nın kanun metninde düzenleniş şekli:
" (1) Hukuka aykırı olarak kişisel verileri kaydeden kimseye altı aydan üç yıla kadar hapis cezası verilir.

FOOTNOTE

12 Ahmet Boz, "Kişisel Verilerin Korunması: ABD ve AB Örnekleri", Unpublished Master Thesis, Police Academy, Ankara, 2014, pg. 8.

13 Decision number 2018/131 of the Personal Data Protection Board. (Date Accessed:04.03.2021)

14 Murat Volkan Dülger, Kişisel Verilerin Korunması Hukuku, İstanbul Law Academy, 2019, pg.10.

15 Dülger, pg.10.

16 Article 29 Working Party's opinion numbered "4/2007, 01248/07/EN WP 136", pg.10.

17 Justification of TPC Article 135.

DİPNOT

12 Ahmet Boz, "Kişisel Verilerin Korunması: ABD ve AB Örnekleri", Yayınlanmamış Yüksek Lisans Tezi, Polis Akademisi, Ankara, 2014, s. 8.

13 Kişisel Verileri Koruma Kurulu'nun 2018/131 no'lu kararı.(Erişim Tarihi:04.03.2021)

14 Murat Volkan Dülger, Kişisel Verilerin Korunması Hukuku, İstanbul: Hukuk Akademisi, 2019, s.10.

15 Dülger, s.10.

16 Avrupa 29. Veri Çalışma Grubu, "4/2007, 01248/07/EN WP 136 sayılı Kişisel Veri Kavramına İlişkin Görüş, s.10.

17 TCK, 135. mad., Kanun Gerekçesi.

PART 15

THE CRIME IN THIS INSTANCE RELATES TO PERSONAL DATA AND THAT HAS PARTICULAR MATERIAL ELEMENTS.

(2) Any person who records the political, philosophical or religious concepts of individuals, or personal information relating to their racial origins, ethical tendencies, health conditions or connections with syndicates is punished according to the provisions of the above subsection."

According to generally accepted opinion, the right to protect personal data is a legal value protected by the Article. This right was included in the fundamental right status by adding the right to protect personal data to Article 20 of the Turkish Constitution as a result of the referendum held in 2010. Another view is that the privacy of private life is a legal value protected by the Article because it comes under the heading "Crimes Against Private Life and Secret Spaces of Life"[18].

The crime in this instance relates to personal data and that has particular material elements. The scope of personal data has already been described above. However, the TPC does not include what should be understood from personal data. This issue has been discussed in the doctrine on the grounds that it is contrary to the principle of certainty of criminal law[19].

As stated in Article 135 of the TPC, "the person who records personal data", the perpetrator of the crime, does not have a feature and everyone can be the perpetrator of this crime. However, if this perpetrator is a public official, a special regulation is included in Article 137 of the TPC. According to this regulation, the commitment of this crime by a public official is regulated as a reason for an increase in the penalty[20]. Article 137 of the TPC is specific only at the point of determining the penalty.

The victim of the crime is the person whose personal data is recorded. It is understood from the definition of "all kinds of information belonging to a real person" in the KVKK[21] that the victim can only be a real person and that information on "moral tendency, sexual life, health status", in the second paragraph of Article 135, can only be information belonging to real persons[22].

According to the type of crime in the Article, the act of crime is the recording of personal data. Although the TPC does not specify what the act of recording covers, it should be understood here as the reuse of data or the preparation of data for others to use[23].

On the other hand, the crime in question is not a consequential crime and it does not matter whether the person was harmed as a result. For this reason, it is a danger crime[24].

The connection between the act and the perpetrator constitutes the moral element of the crime. The moral element of the crime of unlawful recording of personal data is intent[25]. This crime is not included as a crime that can be committed through negligence, a type of crime limited in law.

In addition, in order for a crime to occur, personal data must be recorded illegally. If a reason for compliance with the law is found in the recording of personal data, the incident does not constitute a crime. As stated in the justification of the article, it is not a crime to record personal data in cases where the person involved has given consent[26]. For this reason, the judge will have to investigate the illegality element on an individual basis.

FOOTNOTE

18 Dülger, pg. 310.

19 Nil Melek Gültekin, "Kişisel Verilerin Ceza Hukuku Yönünden Korunması", Unpublished Master Thesis, Galatasaray University, Galatasaray Üniversitesi, 2012, pg. 122.

20 Elif Mendos Kuşkonmaz, "Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması", Unpublished Master Thesis, İstanbul University, 2013, pg.138.

21 Şeyma Sert, Kişisel Verilerin TCK Kapsamında Korunması, Ankara, Seçkin Press, 2019, pg. 107.

22 Gültekin, pg. 129.

23 Hasan Gerçeker, Yorumlu ve Uygulamalı Türk Ceza Kanunu, Ankara, Seçkin Press ,2018, pg. 1410.

24 Melike Aysun Köse, Kişisel Verilerin Kaydedilmesi Suçu, Ankara, Seçkin Press ,2018, pg. 121.

25 Gerçeker, pg. 1411.

26 Justification of TPC Article 135.

(2) Kişilerin siyasi, felsefî veya dinî görüşlerine, ırkî kökenlerine; hukuka aykırı olarak ahlâkî eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimse, yukarıdaki fıkra hükmüne göre cezalandırılır." şeklindedir.

Maddeyle korunan hukuki değer; kabul edilen genel görüşe göre, kişisel verilerin korunması hakkıdır. Bu hak; 2010'da gerçekleştirilen referandum sonucu Anayasamızın 20. maddesine kişisel verilerin korunması hakkı eklenerek, temel hak statüsüne dâhil edilmiştir. Diğer bir görüşe göre ise; burada korunan hukuki değer "Özel hayata ve Hayatın Gizli Alanlarına Karşı Suçlar" başlığı altında yer aldığı için özel hayatın gizliliğidir [18].

Suçun maddi unsurlarına değinecek olursak; suçun konusunu, kişisel veriler oluşturmaktadır. Kişisel verinin kapsamı ilk bölümde anlatıldığı üzere tekrar bu bölüm de anlatılmayacaktır. Ancak kişisel veriden ne anlaşılması gerektiği TCK'da yer almadığı gerekçesiyle doktrinde tartışma konusu olmuş, bu durumun ceza hukukunun belirlilik ilkesine aykırı düştüğü savunulmuştur[19].

TCK'nın 135. maddesinde 'kişisel verileri kaydeden kimse' olarak belirtildiği üzere, suçun faili bir özellik arz etmemekte olup herkes bu suçun faili olabilmektedir. Ancak bu kişinin kamu görevlisi olması durumunda TCK 137. maddede özel bir düzenlemeye yer verilmiştir. Bu düzenlemeye göre, kamu görevlisinin bu suçu işlemesi ceza da artırım sebebi oluşturur[20]. TCK'nın 137. maddesi ise yalnızca cezanın belirlenmesi noktasında özellik arz edecektir.

Suçun mağduru, kişisel verileri kaydedilen kimsedir. KVKK'da yer alan 'gerçek kişiye ait her türlü bilgi' tanımından mağdurun ancak gerçek kişi olabileceği[21], bununla birlikte 135. maddenin ikinci fıkrasında yer alan 'ahlaki eğilim, cinsel yaşam, sağlık durumu' bilgilerinin de ancak gerçek kişilere ait bilgiler olabileceği anlaşılmaktadır. Bu maddeyle korunmak istenen gerçek kişilerdir[22].

Maddede yer alan suç tipine göre hareket, kişisel verilerin kaydedilmesidir. Kaydetmekten; kaydetme eyleminin neyi kapsadığı TCK'da belirtilmemiş olmakla beraber burada kaydetme eyleminde veriyi tekrar kullanmak veya başkalarının kullanacağı şekilde hazır etmek şeklinde anlaşılması gerekmektedir[23].

Öte yandan; söz konusu suç neticeli bir suç olmayıp, sonucunda kişinin zarara uğrayıp uğramadığının bir önemi bulunmayacaktır. Bu sebeple bir tehlike suçudur[24].

Gerçekleştirilen fiil ve fail arasındaki bağ, suçun manevi unsurunu oluşturmaktadır. Kişisel verilerin hukuka aykırı olarak kaydedilmesi suçunun manevi unsuru ise kasttır[25]. Kanunda taksirle işlenebilecek suç sayısı sınırlı sayıda olup, bu suç taksirle işlenebilen suçlar arasına girmemektedir.

Tüm bunların yanında suçun oluşması için kişisel verilerin hukuka aykırı olarak kaydedilmesi gerekmektedir. Eğer kişisel verinin kaydedilmesinde hukuka uygunluk sebebi bulunursa bu suç tipi oluşmamış olacaktır. Maddenin gerekçesinde de belirtildiği üzere kişinin rızasının bulunduğu durumlarda kişisel verilerinin kayda alınması suç teşkil etmeyecektir[26]. Bu sebeple hâkimin hukuka aykırılık unsurunu ayrıca araştırması gerekecektir.

SUÇUN MADDİ UNSURLARINA DEĞİNECEK OLURSAK; SUÇUN KONUSUNU, KİŞİSEL VERİLER OLUŞTURMAKTADIR.

DİPNOT

18 Dülger, s. 310.

19 Nil Melek Gültekin, "Kişisel Verilerin Ceza Hukuku Yönünden Korunması", Yayınlanmamış Yüksek Lisans Tezi, Galatasaray Üniversitesi, 2012, s. 122.

20 Elif Mendos Kuşkonmaz, "Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması", Yayınlanmamış Yüksek Lisans Tezi, İstanbul Üniversitesi, 2013, s.138.

21 Şeyma Sert, Kişisel Verilerin TCK Kapsamında Korunması, Ankara, Seçkin, 2019, s. 107.

22 Gültekin, s. 129.

23 Hasan Gerçeker, Yorumlu ve Uygulamalı Türk Ceza Kanunu, Ankara, Seçkin,2018, s. 1410.

24 Melike Aysun Köse, Kişisel Verilerin Kaydedilmesi Suçu, Ankara, Seçkin,2018, s. 121.

25 Gerçeker, s. 1411.

26 TCK m.135, Kanun Gerekçesi.

PART 15

ARTICLE 136 OF THE TURKISH PENAL CODE STIPULATES THAT THE PERSON WHO "UNLAWFULLY DELIVERS DATA TO ANOTHER PERSON, OR PUBLISHES OR ACQUIRES THE SAME THROUGH ILLEGAL MEANS" WILL BE PUNISHED.

In the KVKK, processing of personal data is defined as "any operation which is performed upon personal data such as collection, recording, storage, preservation, alteration, adaptation, disclosure, transfer, retrieval, making available for collection, categorization or blocking its use by wholly or partly automatic means or otherwise than by automatic means which form part of a filing system"[27] and the act of recording is also defined as the processing of personal data. In this context, whether the data processing principles in the KVKK have been complied with must be examined in order to save the personal data protected within the scope of the KVKK in accordance with the law. This issue is important in terms of evaluating "illegality", which is one of the elements of the crime.

B. The Offense of Providing or Acquiring Data Unlawfully

Article 136 of the Turkish Penal Code stipulates that the person who "unlawfully delivers data to another person, or publishes or acquires the same through illegal means" will be punished. As stated in the justification of the Article, the person who unlawfully obtains or transfers personal data "whether it has been recorded in accordance with the law or not" will be punished regardless of Article 135. Although the data is initially recorded in accordance with the law, the person who spreads this data in various ways is the perpetrator of a crime. For example, illegally transferring information given by a patient in hospital to other institutions constitutes a crime based on the fact that while the data was legally obtained, it was shared illegally. The form of the article is regulated in the TPC:
(1) Any person who unlawfully delivers data to another person, or publishes or acquires the same through illegal means is punished with imprisonment from one year to four years.

The legal value protected by the Article is the right to protect personal data regulated in Article 20 of the Constitution as in Article 135 of the TPC. According to another view[28], it can be stated that the legal value protected here is the privacy of private life.

KVKK'da; "kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem" kişisel verilerin işlenmesi[27] olarak tanımlanmış ve veri kaydetme fiili de işleme faaliyeti olarak kabul edilmiştir. Bu bağlamda özellikle KVKK kapsamı dahilinde koruma altına alınan kişisel verilerin hukuka uygun kaydedilmesi için KVVK'daki veri işleme ilkelerine uyulup uyulmadığı incelenmelidir. Bu husus, suçun unsurlarından olan "hukuka aykırılık"ın değerlendirilmesi bakımından önem arz etmektedir.

B. Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme Suçu

Türk Ceza Kanunu'nun 136. maddesinde "kişisel verileri hukuka aykırı olarak veren, yayan veya ele geçiren" kişinin cezalandırılacağı düzenlenmiştir. Madde gerekçesinde belirtildiği üzere "hukuka uygun olarak kaydedilmiş olsun veya olmasın" kişisel veriyi hukuka aykırı olarak ele geçiren veya veren kişi 135. maddeden bağımsız olarak cezalandırılacaktır. Her ne kadar başlangıçta hukuka uygun olarak kaydedilmiş bir veri bulunsa da, bu veriyi muhtelif yollarla yayan kişi suçun faili olacaktır. Örneğin, hastanın hastaneye verdiği bilgilerin hukuka aykırı olarak başka kurumlara aktarılması, verinin hukuka uygun olarak elde edildiği, fakat hukuka aykırı olarak vermesinden hareketle bu suçu oluşturacaktır. Maddenin TCK'da düzenleniş şekli:
"Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, bir yıldan dört yıla kadar hapis cezası ile cezalandırılır."
şeklindedir.

Maddeyle korunan hukuki değer TCK'nın 135. maddesinde olduğu gibi Anayasa'mızın 20. maddesinde düzenlenmiş olan kişisel verilerin korunması hakkıdır. Diğer bir görüşe[28] göre ise burada korunan hukuki değerin özel hayatın gizliliği olduğunu belirtmiştik.

FOOTNOTE

27 Law No:6698 Article 3.

28 Dülger, pg. 346

29 Gerçeker, pg.1430.

30 Metin Çokmutlu, "Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması", Unpublished PhD Thesis, Kocaeli University, 2014, pg. 216.

31 Sert, pg.107.

32 Gerçeker, pg.1430.

33 Justification of TPC Article 136.

As in Article 135, the subject of the crime of unlawfully giving or obtaining personal data is the personal data. The scope of the concept of personal data is specified in the first section.

The text of the Article mentions "the person who unlawfully gives, spreads or seizes personal data to another person". There is no special classification: anyone can be the perpetrator of the crime regulated in Article 136. For this reason, it isn't a special offence[29]. However, as in the crime of recording personal data, if a public officer commits the crime of unlawfully delivering or acquiring personal data, this will be reason for increasing the penalty. In addition, legal entities cannot be perpetrators of this crime, but the security measure for legal entities in Article 140 of the TPC can be applied when conditions are met[30].

Anyone can be the victim of the crime of giving or obtaining personal data. However, in order to be a victim, the personal data involved must be associated with that person. At the same time, as we have already pointed out, personal data must belong to a real person, as defined in the KVKK[31].

Three actions are included in Article 136 of the TPC: delivering data an another person, publishing data, and aquiring data. Each of them constitutes the movement element of the crime.

A crime occurs with any of these acts, making this an optional mobile crime. However, the legislator has not regulated the acts of giving, spreading, and seizing. "It can be defined as giving; offering something of someone's to someone else, spreading; submitting to more than one a person's information, obtaining; a person obtaining information that is in the possession of another with or without his/her consent."[32] Also, as stated in the justification of the Article[33], it is not important that the personal data was originally recorded in accordance with the law. The important thing for a crime to occur is that the specified actions are done illegally.

Kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçunun konusu, 135. maddede olduğu gibi kişisel verilerdir. Kişisel veri kavramının kapsamı birinci bölümde belirtilmiştir.

Madde metninde "Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi" den bahsedilmektedir. Burada özel bir tasnif yapılmamıştır; bu sebeple 136. maddede düzenlenen suçun faili herkes olabilir. Bu sebeple, özgü suç değildir[29]. Ancak kişisel verilerin kaydedilmesi suçunda olduğu gibi kamu görevlisinin kişisel verilerin hukuka aykırı olarak verme veya ele geçirme suçunu işlemesi halinde cezada artırım sebebi olacaktır. Bunun yanında tüzel kişiler bu suçun faili olamayacaktır. Fakat; TCK'nın 140. maddesinde yer alan tüzel kişiler hakkında güvenlik tedbiri, şartları sağlandığında uygulanabilecektir[30].

Kişisel verileri verme veya ele geçirme suçunun mağduru herkes olabilecektir. Ancak mağdur olabilmek için kişisel verinin mutlaka o kişi ile ilişkilendirilebilir olması gerekmektedir. Aynı zamanda daha önce de belirttiğimiz üzere KVKK'da yer alan tanıma binaen kişisel verinin gerçek bir kişiye ait olması gerekmektedir[31].

TCK'nın 136. maddesinde üç harekete yer verilmiştir. Bunlar verme, yayma ve ele geçirme şeklinde düzenlenmiştir. Her biri suçun hareket unsurunu oluşturmaktadır.

Bu fiillerden herhangi birinin yapılmasıyla suç oluşacaktır. Bu sebeple, seçimlik hareketli bir suçtur. Bunun yanında, kanun koyucu; verme, yayma ve ele geçirme fiillerinin nasıl olması gerektiğini düzenlememiştir. "Verme; bir kimsenin elindeki bir şey başkasına sunması, yayma; birden fazla kişinin bilgisine sunması, ele geçirme; bir kimsenin bir başkasının elinde olan bir bilgiyi onun rızasıyla veya rızası olmaksızın elde etmesi şeklinde tanımlanabilir."[32]. Ayrıca madde gerekçesinde[33] de belirtildiği üzere; kişisel verinin başlangıçta hukuka uygun olarak kaydedilmiş olması önem taşımamaktadır. Suçun oluşması için önemli olan belirtilen eylemlerin hukuka aykırı olarak yapılmasıdır.

TÜRK CEZA KANUNU'NUN 136. MADDESİNDE "KİŞİSEL VERİLERİ HUKUKA AYKIRI OLARAK VEREN, YAYAN VEYA ELE GEÇİREN" KİŞİNİN CEZALANDIRILACAĞI DÜZENLENMİŞTİR.

DİPNOT

27 Kişisel Verilerin Korunması Kanunu, mad. 3.

28 Dülger, s. 346

29 Gerçeker, s.1430.

30 Metin Çokmutlu, "Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması", Yayınlanmamış Doktora Tezi, Kocaeli Üniversitesi, 2014, s. 216.

31 Sert, s.107.

32 Gerçeker, s.1430.

33 TCK'nın 136 mad. Kanun Gerekçesi.

PART 15

In order for the mentioned type of crime to occur, illegal actions must be taken. The fact that one of the optional movements has been made does not meet the condition of illegality. Therefore, a judge also needs to investigate the illegality element. For example, the crime in question does not occur where an authority arising from the law is used in the capture of a person's personal data in order to carry out a law enforcement activity[34]. In terms of the moral element, it is a crime that can only be committed intentionally.

C. The Offense of Failing to Destroy Data

The crime of not destroying personal data, regulated in Article 138 of the TPC, is a crime regulated in order to prevent personal data being processed due to some need and that personal data being held by unauthorized third parties after that need no longer exists, in violation of rigths[35]. While the basic form of the crime is regulated in the first paragraph of Article 138, the second paragraph regulates the existence of personal data of a special nature as qualified state in accordance with the provision of the law. In the text of the Article, the crime is stated as:
(1) Any person who fails to destroy data in accordance with the prescribed procedures, before the expiry of the legally prescribed period for destruction, shall be sentenced to a penalty of imprisonment for a term of one to two years.
(2) Where the subject of the offence remains within the scope of the information to be removed or eliminated under the provisions of the Code of Criminal Procedure, the penalty to be imposed shall be increased by one fold.

As mentioned in other crimes related to the protection of personal data, the legal value protected is the right to protect personal data. Another view states that[36], since the substance is within the scope of the privacy of private life, the legal value protected here is, again, the privacy of private life.

Personal data constitutes the subject of the mentioned crime. The types of crimes mentioned above are exactly the same in terms of subject. The point to note here in terms of this type of crime is whether it is only related to data processed automatically. Article 138 of the TPC mentions “destroying data within the system”. However, such a statement was not included in the crimes examined above. For this reason, it should be accepted that the "system" mentioned in Article 138 is an informatics or automatic system[37]. A contrary view states that although the term of destruction in the system is mentioned in the text of the law, the personal data registered outside the system also constitutes the subject of this crime[38].

If we examine the crime in terms of the perpetrator, the Article states “For those who are obliged to destroy,” the person is the perpetrator. According to this regulation, since the perpetrator has a special character, the crime is a specific crime and cannot be committed by everyone. Because of the fact that there is no requirement that the perpetrator is a public officer, the aggravating provision in Article 137 of the TPC is not valid for this crime.

There are different opinions about the victim of the crime. According to one view, the victim of this crime is the person whose personal data is not destroyed[39]. According to another view, the victim of this crime is not a particularindividual because trust in the public administration is protected[40].

The element that differs in terms of all three crimes is the act of the crime. The offense contained in Article 138 states that if the personal data recorded is saved in an information system and is not deleted from there, or if it is saved on a certain document, when the document is destroyed, the data can remain. In other words, the behavior that constitutes the element of action in terms of this crime is not an execution but a negligent behavior. With no retention requirement, the data for such activities must be deleted in a way that it cannot be accessed later. Otherwise, the crime of not destroying the data will occur[41].

Here, while TPC Article 138 only deals with data that is not deleted even though the periods specified by law have passed, a new type of crime has been created with Article

FOOTNOTE

34 Çokmutlu, pg. 224.

35 Sert, pg.152.

36 Dülger, pg. 360.

37 Kuşkonmaz, pg. 162.

38 Murat Volkan Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, Ankara:Seçkin Press, 2015, pg.722.

39 Gerçeker, pg.1435.

40 Dülger, Kişisel Verilerin Korunması, pg.362.

41 Muammer Ketizmen, “Türk Ceza Hukukunda Bilişim Suçları”, PhD Thesis, Ankara University, pg.301.

Söz konusu suç tipinin oluşabilmesi için hukuka aykırı olarak belirtilen eylemlerin yapılmış olması gerekir. Sırf seçimlik hareketlerden birinin yapılmış olması, hukuka aykırılık koşulunu sağlamayacaktır. Bu sebeple, hâkimin ayrıca hukuka aykırılık unsurunu araştırması gerekmektedir. Örneğin; bir kolluk faaliyetinin yerine getirilmesi amacıyla bir kimsenin kişisel verilerinin ele geçirilmesinde kanundan kaynaklanan bir yetki kullanıldığı için söz konusu suç oluşmayacaktır[34]. Manevi unsur açısından ise yalnızca kastla işlenebilecek bir suçtur.

C. Verileri Yok Etmeme Suçu

TCK’nın 138. maddesinde düzenlenmiş olan kişisel verileri yok etmeme suçu bazı ihtiyaçlar nedeniyle işlenmesi hukuka uygun olan kişisel verilerin, mevcut ihtiyacın ortadan kalkması dolayısıyla yetkisiz üçüncü kişilerin elinde bulunan kişisel verilerin hak ihlallerine yol açmasını önlemek amacıyla düzenlenmiş bir suç tipidir[35]. 138. maddenin ilk fıkrasında suçun temel şekli düzenlenirken, ikinci fıkrada kanun hükmüne göre özel nitelikte bir kişisel verinin bulunması durumu nitelikli hal olarak düzenlenmiştir. Suçun madde metninde düzenleniş şekli:
“(1) Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde bir yıldan iki yıla kadar hapis cezası verilir.
(2) (Suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması hâlinde verilecek ceza bir kat artırılır.” şeklindedir.

Kişisel verilerin korunmasıyla alakalı diğer suçlarda da bahsedildiği üzere burada korunan hukuki değer kişisel verilerin korunması hakkıdır. Başka bir görüşe göre[36] ise madde özel hayatın gizliliği kapsamında yer aldığı için yine burada korunan hukuki değer; özel hayatın gizliliğidir.

Söz konusu suçun konusunu kişisel veriler oluşturmaktadır. Yukarıda da bahsettiğimiz suç tipleri konu açısından tamamen aynıdır. Burada dikkat edilmesi gereken nokta, konunun bu suç tipi açısından yalnızca otomatik yolla işlenen verilere ilişkin olup olmadığıdır. TCK 138. maddede “verileri sistem içinde yok etmek”ten söz edilmektedir. Ancak yukarıda incelenen suçlarda ise bu şekilde bir ifadeye yer verilmemiştir. Bu sebeple 138. maddede geçen “sistem”in bilişim veya otomatik sistem olduğunun kabulü gerekir[37]. Aksi yönde bir görüşe göre ise; kanun metninde sistem içinde yok etme ifadesi geçiyor olsa da, sistem dışında kayıtlı olan kişisel verilerin de bu suçun konusunu oluşturacağı şeklindedir[38].

Suçu fail açısından inceleyecek olursak; maddede geçen “yok etmekle yükümlü olan” kişi faildir. Bu düzenlemeye göre, failin özel bir niteliği bulunduğundan; suç, özgü bir suçtur ve herkes tarafından işlenemez. Failin kamu görevlisi olması gibi bir koşul bulunmadığından TCK’nın 137. maddesindeki ağırlaştırıcı hüküm bu suç için geçerli olmayacaktır.

Suçun mağduru konusunda farklı görüşler bulunmaktadır. Bir görüşe göre bu suçun mağduru, kişisel verileri silinmeyen kişidir[39]. Diğer bir görüşe göre ise; bu suçun mağduru belli bir birey değildir, çünkü bu suç tipiyle kamu idaresine duyulan güvende korunmaktadır[40].

Her üç suç bakımından ayrılan unsur, suçun hareket unsurudur. 138. maddede yer alan suç; kaydedilen kişisel veriler bir bilişim sistemine kaydedilmişse buradan silinmemeleri, belli bir belge üzerine kaydedilmişlerse belgenin imha edilmemesi şeklinde gerçekleşebilir. Bir diğer anlatımla, bu suç bakımından hareket unsurunu oluşturan davranış icrai bir davranış değil, ihmali bir davranıştır. Saklama zorunluluğunun ortadan kalkmasıyla, bu tür faaliyetler için verinin daha sonra ulaşılamayacak şekilde silinmiş olması gerekir. Aksi takdirde verileri yok etmeme suçu oluşacaktır[41].

Burada; TCK madde 138 sadece kanunların belirlediği süreler geçmiş olmasına rağmen silinmeyen verileri konu alırken, KVKK’nın 17/2 maddesi ile yeni bir suç tipi oluşturul-

DİPNOT

34 Çokmutlu, s. 224.

35 Sert, s.152.

36 Dülger, s. 360.

37 Kuşkonmaz, s. 162.

38 Murat Volkan Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, Ankara:Seçkin, 2015, s.722.

39 Gerçeker, s.1435.

40 Dülger, Kişisel Verilerin Korunması, s.362.

41 Muammer Ketizmen, “Türk Ceza Hukukunda Bilişim Suçları”, Doktora Tezi, Ankara Üniversitesi, s.301.

PART 15

THE CRIME OF FAILING TO DESTROY PERSONAL DATA IS NOT A CRIME THAT CAN BE COMMITTED BY NEGLIGENCE. FOR THIS REASON, THE MORAL ELEMENT IS INTENT.

17/2 of the KVKK, and, accordingly, deletion is mentioned in Article 7 of the KVKK, whose procedures and principles are determined by regulation, and in the event of failure to comply with the rules of destruction or anonymization, Article 138 of the TPCapplies.

Unlike the other two crimes mentioned above, the crime of not destroying data does not consider the consent of the victim as a reason for compliance with the law[42].

The crime of failing to destroy personal data is not a crime that can be committed by negligence. For this reason, the moral element is intent.

IV. CONCLUSION

An important step for the protection of personal data in Turkey was the addition of articles protecting personal data to the Turkish Penal Code No.5237. In order for these laws to be implemented, the concept of personal data must be well understood. Although the Turkish Penal Code does not include a definition of personal data, it is understood as the concept of personal data defined in the KVKK. Based on the definition made in the Court of Cassation's case law and the

muş olup buna göre KVKK'nın 7'inci maddesinde değinilen ve usul ve esasları yönetmelikle belirlenecek olan silme, yok etme veya anonim hale getirme kurallarına uyulmaması halinde de TCK madde 138'in uygulanacağı hüküm altına alınmıştır.

Verileri yok etmeme suçu, yukarıda sayılan diğer iki suçtan farklı olarak mağdurun rızasını hukuka uygunluk sebebi olarak görmemektedir[42].

Kişisel verileri yok etmeme suçu, taksirle işlenebilen bir suç değildir. Bu sebeple manevi unsuru kasttır.

IV. SONUÇ

5237 sayılı Türk Ceza Kanunu'nun kapsamına kişisel verileri koruyan maddelerin eklenmesi, kişisel verilerin korunması adına önemli bir adımdır. Bu kanunların uygulanabilmesi için kişisel veri kavramının iyi bir şekilde anlaşılması gerekmektedir. Her ne kadar TCK kişisel verinin tanımına yer vermemiş ise de KVKK'da yapılmış olan tanımdan hareket ederek nelerin kişisel veri kavramına dahil olacağı anlaşılmaktadır. Gerek Yargıtay içtihatlarında yapılan tanımdan gerekse KVKK'daki tanımdan hare-

FOOTNOTE

42 Dülger, Kişisel Verilerin Korunması, pg. 368.

definition in the KVKK, illegal seizure of data that can be considered personal data, giving it to someone else, spreading, recording, or not deleting it despite the need for it to be deleted is regulated as a crime in the TPC. In order for these five acts to be committed as a crime, they must be carried out unlawfully. Here, the regulations that should be taken into account when determining illegality are, again, the regulations in the KVKK.

ketle kişisel veri olduğu değerlendirilebilecek verilerin, hukuka aykırı olarak ele geçirilmesi, başkasına verilmesi, yayılması, kaydedilmesi veya silinmesi gerektiği halde silinmemesi kanun koyucu tarafından TCK'da suç olarak düzenlenmiştir. Sayılan bu beş eylemin suça vücut verebilmesi için mutlaka hukuka aykırı olarak gerçekleştirilmesi gerekmektedir. Burada hukuka aykırılığı belirlerken baz alınması gereken düzenleme yine KVKK'daki düzenlemeler olacaktır.

KİŞİSEL VERİLERİ YOK ETMEME SUÇU, TAKSİRLE İŞLENEBİLEN BİR SUÇ DEĞİLDİR. BU SEBEPLE MANEVİ UNSURU KASTTIR.

BIBLIOGRAPHY

AHMET BOZ, Kişisel Verilerin Korunması: ABD ve AB Örnekleri, Unpublished Master Thesis, Police Academy, Ankara, 2014.

AYŞE ÇİĞDEM AYÖZGER, Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dâhil Kişisel Verilerin Korunması, Beta Press, İstanbul, 2016.

ELİF MENDOS KUŞKONMAZ, Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması, Master Thesis, İstanbul University, 2013.

HASAN GERÇEKER, Yorumlu ve Uygulamalı Türk Ceza Kanunu, Seçkin Press, Ankara, 2018.

İBRAHİM KORKMAZ, Kişisel Verilerin Ceza Hukuku Kapsamında Korunması, Ankara, Seçkin Press, 2019.

Kişisel Verileri Koruma Kurulu'nun 19.11.2018 tarihli, 2018/131 no'lu kararı.

MELİKE AYSUN KÖSE, Kişisel Verilerin Kaydedilmesi Suçu, Seçkin Press, Ankara, 2018.

METİN ÇOKMUTLU, Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması, PhD Thesis, Kocaeli University, 2014.

MUAMMER KETİZMEN, Türk Ceza Hukukunda Bilişim Suçları, PhD Thesis, Ankara University, 2006.

MURAT VOLKAN DÜLGER, Bilişim Suçları ve İnternet İletişim Hukuku, Seçkin Press, Ankara, 2015.

MURAT VOLKAN DÜLGER, Kişisel Verilerin Korunması Hukuku, İstanbul Law Academy, İstanbul, 2019.

NİL MELEK GÜLTEKİN, Kişisel Verilerin Ceza Hukuku Yönünden Korunması, Master Thesis, Galatasaray University, 2012.

ŞEYMA SERT, Kişisel Verilerin TCK Kapsamında Korunması, Ankara, Seçkin Press, 2019.

KAYNAKÇA

AHMET BOZ, Kişisel Verilerin Korunması: ABD ve AB Örnekleri, Yüksek Lisans Tezi, Polis Akademisi, Ankara, 2014.

AYŞE ÇİĞDEM AYÖZGER, Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dâhil Kişisel Verilerin Korunması, Beta Yayınları, İstanbul, 2016.

ELİF MENDOS KUŞKONMAZ, Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması, Yüksek Lisans Tezi, İstanbul Üniversitesi, 2013.

HASAN GERÇEKER, Yorumlu ve Uygulamalı Türk Ceza Kanunu, Seçkin Yayıncılık, Ankara, 2018.

İBRAHİM KORKMAZ, Kişisel Verilerin Ceza Hukuku Kapsamında Korunması, Ankara, Seçkin, 2019.

Kişisel Verileri Koruma Kurulu'nun 19.11.2018 tarihli, 2018/131 no'lu kararı.

MELİKE AYSUN KÖSE, Kişisel Verilerin Kaydedilmesi Suçu, Seçkin Yayıncılık, Ankara, 2018.

METİN ÇOKMUTLU, Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması, Doktora Tezi, Kocaeli Üniversitesi, 2014.

MUAMMER KETİZMEN, Türk Ceza Hukukunda Bilişim Suçları, Doktora Tezi, Ankara Üniversitesi, 2006.

MURAT VOLKAN DÜLGER, Bilişim Suçları ve İnternet İletişim Hukuku, Seçkin Yayıncılık, Ankara, 2015.

MURAT VOLKAN DÜLGER, Kişisel Verilerin Korunması Hukuku, İstanbul Hukuk Akademisi, İstanbul, 2019.

NİL MELEK GÜLTEKİN, Kişisel Verilerin Ceza Hukuku Yönünden Korunması, Yüksek Lisans Tezi, Galatasaray Üniversitesi, 2012.

ŞEYMA SERT, Kişisel Verilerin TCK Kapsamında Korunması, Ankara, Seçkin Yayıncılık, 2019.

DİPNOT

42 Dülger, Kişisel Verilerin Korunması, s. 368.