Hakemli Araştırma Makalesi/Peer - Reviewed Research Article

TÜRK CEZA KANUNU'NDA DÜZENLENEN SİSTEMİ ENGELLEME, BOZMA, VERİLERİ YOK ETME VEYA DEĞİŞTİRME SUÇLARI (TCK m. 244/1-2)*

Crimes of Obstructing the System, Undoing the System, Undoing or Modifying Data, Regulated in the Turkish Penal Code (TCK 244/1-2)

Doç. Dr. Ahmet Hulusi AKKAŞ**

Melahat Şeyma DOĞRUOĞLU****

ÖZET

Günümüzde teknolojik gelişmelerin hız kazanmasıyla beraber, bilişim sistemleri bankacılık, iletişim, ulaşım, güvenlik, sağlık, eğitim,

* Bu makale Erciyes Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı'nda Doç. Dr. Ahmet Hulusi AKKAŞ'ın danışmanlığında yürütülen "Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme (TCK m. 244/1-2)" isimli yüksek lisans tezinden üretilmiştir.

** Doç. Dr., Erciyes Üniversitesi Hukuk Fakültesi, Ceza ve Ceza Muhakemesi ABD., e-posta: ahakkas@erciyes.edu.tr, ORCID: 0000-0001-5217-5951.

*** Yüksek Lisans Öğrencisi, Erciyes Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, e-posta: seymadogruoglu@gmail.com, ORCID: 0000-0001-6627-4360.

Makale Geliş Tarihi: 25.11.2024

Makale Kabul Tarihi: 24.03.2025

⇛ **Atıf Şekli:** Ahmet Hulusi Akkaş ve Melahat Şeyma Doğruoğlu "Türk Ceza Kanunu'nda Düzenlenen Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçları (TCK m. 244/1-2)", Erciyes Üniversitesi Hukuk Fakültesi Dergisi, 20/1 (2025): 185-216

ticaret ve sanayi gibi birçok alanda kullanılmaya başlanmış ve toplumsal hayatın vazgeçilmez bir unsuru haline gelmiştir. Kullanım alanının genişliği ve yaygınlığının art niyetli kişileri cezbetmesiyle, bilişim dünyası istismar edilmeye başlanmış ve bu durum, bu sistemlerin kullanıldığı birçok alanı tehlikeye sokmuştur. Bu tarz eylemlerin önlenmesi ve hukuki korumanın sağlanabilmesi için ise hem dünya genelinde hem de ülkemizde bilişim suçlarına yönelik düzenlemeler getirilmiş ve uluslararası anlaşmalar imzalanmıştır. Bu konuda yapılan önemli anlaşmalardan biri de; 2004 yılında yürürlüğe girmekle birlikte, ülkemizde onaylanıp yürürlüğe girmesi 2014 yılını bulan Avrupa Konseyi Siber Suç Sözleşmesi (AKSSS)'dir. AKSSS düzenlenmesine paralellik oluşturulan ve öğretide doğrudan bilişim suçları olarak isimlendirilen bilişim suçları Türk Ceza Kanunu (TCK)'nda "Topluma Karşı Suçlar" başlıklı üçüncü kısmın "Bilişim Alanında Suçlar" başlıklı onuncu bölümünde düzenlenmiştir. Bu bölümün içerisinde, yer alan bilişim suçlarından biri de TCK 244. maddede düzenlenen Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçları'dır. Söz konusu düzenleme AKSSS'nin 4. ve 5. maddelerinde yer alan sisteme müdahale ve verilere müdahale düzenlemelerine uyum sağlamaya yöneliktir. Ancak TCK m. 244 her ne kadar AKSSS baz alınarak getirilmiş bir düzenleme olsa da; doktrinde suçla korunan hukuki değer, suçun unsurları, nitelikli haller gibi birçok konuda tartışmalı hususlar görülmüş ve düzenlemeye eleştiriler getirilmiştir. Bu çalışmada TCK 244. maddede yer alan Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçları incelenecek olup, bu konularda doktrinde yer alan tartışmalı konulara ve düzenlemede eksik görülen hususlara yer verilecektir.

Anahtar Kelimeler: Bilişim Suçu, Verilere Müdahale, Sisteme Müdahale, Bilişim Sistemi, Sistemi Engelleme.

ABSTRACT

With the rapid advancement of technology in contemporary times, information systems have become integral to numerous sectors, including banking, communication, transportation, security, healthcare, education, commerce, and industry, establishing themselves as an indispensable component of societal life. The extensive scope and widespread adoption of these systems have attracted malicious actors, resulting in the exploitation of the information technology domain, thereby posing risks to the various fields reliant on these systems. To counter such activities and ensure legal protection, regulatory frameworks addressing cybercrimes have been established

both globally and within our country, complemented by the signing of international agreements. A notable example in this context is the European Council Cybercrime Convention (ECCC), which entered into force in 2004 and was ratified and implemented in our country in 2014. Cybercrimes, explicitly categorized as information technology offenses within legal scholarship and aligned with the ECCC provisions, are codified in the Turkish Penal Code (TPC) under Part Three, titled "Crimes Against Society," specifically in Section Ten, titled "Crimes in the Field of Information Technology." Among the offenses outlined in this section is the crime of Obstructing, Disrupting, Destroying, or Altering Data or Systems, as regulated by article 244 of the TPC. This provision is designed to conform to articles 4 and 5 of the ECCC, which address interference with systems and data, respectively. Nevertheless, despite being modeled on the ECCC, article 244 of the TPC has sparked considerable debate within the doctrine concerning several aspects, including the legal interests it seeks to protect, the constituent elements of the offense, aggravating circumstances, and other related issues, leading to various criticisms of the regulation. This study will analyze the crimes of Obstructing, Disrupting, Destroying, or Altering Data or Systems as stipulated in Article 244 of the TPC, shedding light on the contentious issues within the doctrine and addressing perceived deficiencies in the regulatory framework.

Key Words: Computer Crime, Data Interference, System Intervention, Information System, Blocking the System.

EXTENDED ABSTRACT

Today, rapid developments in Information Technology (IT) world allowed the usage of this technology intensively in many sectors such as banking, communication, transportation, security, health, education, trade and industry and made IT systems an integral part of people's life. This wide use of IT attracted cyber criminals. IT systems began to be exploited by them endangering the security of the sectors using this technology. In order to prevent such actions and provide legal protection, new regulations have been introduced against cyber-crimes both around the world and our country and relevant international agreements have been signed. One of the important agreements made on this subject is the Convention on Cybercrime (CETS 185). Although CETS 185 entered into force in 2004, it was approved and entered into force in our country in 2014.

Turkish Penal Code (TPC) has been modified based on CETS 185 and cyber-crimes are regulated in the tenth chapter titled "Crimes in the Field of Information Technology" of the third section titled "Crimes Against Society" of TPC. One of the cyber-crimes included in this section is the Crimes of Obstructing, Disrupting the System, Destroying or Changing Data and regulated in Article 244 of the TPC. The regulation in question aims to comply with the system intervention and data intervention regulations in Articles 4 and 5 of CETS 185.

However, although TPC 244 is a regulation based on CETS 185, issues such as the legal value protected by crime, the elements of the crime, the reasons affecting the crime have been identified and received criticism. In this study, the Crimes of Obstructing, Disrupting the System, Destroying or Changing the Data in TPC 244 will be examined, and criticism and issues that appeared missing in the regulation will be discussed. The crimes regulated in TPC 244 are arranged as optional. Obstruction and disruption of the system is in the first paragraph; Corrupting, destroying, changing, making data inaccessible, inserting data into the system and sending existing data to another place are the actions regulated in the second paragraph.

Different evaluations have been made in the doctrine regarding the legal value protected by these crimes, including ownership, the integrity and security of information systems, communication rights, the country's economy, public order and security, and the legal value protected has a mixed nature. The subject of the crime is information systems for the first paragraph, and the data in the system for the second paragraph. It is controversial whether the data in vehicles that serve as storage constitute the subject of this crime. In this regard, it should be stated that the data contained in devices that serve only storage purposes should not be evaluated within the scope of this article and that there is a lack of regulation in the law in terms of data in this scope. Again, there are different opinions in the doctrine as to whether physical damage to the system constitutes this crime. However, in our opinion, it is also possible to commit this crime through physical attack.

Anyone can be the perpetrator or victim of the crimes listed in TPC 244. In identifying the perpetrator and the victim, the owner of the system or data to which the action is directed and the individual rights of use, ownership and disposition are of importance. The owner of the saving authority must be determined according to the characteristics of each concrete case.

The status of legal entities as victims in the doctrine is controversial. Although there are opposing views, the dominant view is that legal entities have the title of victim in terms of these crimes. In the doctrine, this crime appeared as free-action and consequential, connected-action and pure-action as there are opinions that evaluate it in different ways. However, since the actions regulated in the article express a result and can be carried out in many different ways, it can be said that they are free-action and consequential crimes. It is also controversial in the doctrine whether the crime is a crime of danger or a crime of harm. However, the occurrence of any harm is not specifically sought in the text of the article. These crimes can be committed by action or negligence. Since the actions regulated in the second paragraph of TPC 244 can be committed with the crime in the first paragraph, the main distinction between the paragraphs emerges in terms of purpose.

Since our law does not specify whether the blocking action is permanent or temporary, there are different opinions on this issue in the doctrine. However, in the CEST 185 explanatory report, it is stated that the blocking must be serious. In our opinion, whether the blocking is temporary or permanent does not make a difference in terms of the blocking action. If the functioning of the system is slowed down, blocking will occur. It is also thought in the doctrine that committing this crime using more than one IT system or software should be regulated as a qualified case.

The fact that destroyed data can be recovered with special devices or methods reveals conflicting views in the doctrine on whether destruction has occurred or not. In our opinion, destruction occurs if the data can be recovered using special devices or methods. It does not matter whether the data is a copy or not. If the data is thrown into the recycle bin, destruction will not occur as long as the data remains there. There is a belief that moving the victim's data to another file in their system would also constitute this crime in terms of sending existing data elsewhere. In order to distinguish TPC 244/2 from TPC articles 135, 136 and 142, it is especially necessary to determine the nature of the data.

In the 3rd paragraph of TPC 244, committing crimes in TPC 244/1 and 2 on the systems of a bank, credit institution, public institution or organization is regulated as a qualified case. Although it is deemed appropriate to introduce such a regulation in the doctrine, it is not considered appropriate to limit institutions, and it is thought that the protection of the overall service should be ensured. It is al-

so stated that the fact that the perpetrator is a public, bank or credit institution official should be regulated as a qualified situation.

Although the issue of whether the regulation in TPC 244/4 a qualified crime or a separate crime is controversial in the doctrine, as stated in the first opinion, since the regulation maintains adherence to the basic crime type, it should be evaluated as a qualified situation. The crimes regulated in TPC 244 are crimes that can be committed intentionally and can also be committed with possible intent. Since there is no regulation regarding negligence, these crimes cannot be committed by negligence. Attempted crime is possible. In terms of participation, general provisions apply.

It is possible to say that more than one situation may occur in terms of TPC 244 regarding the combination of crimes. Crimes in TPC 244/1-2 can be committed as a chain crime. Although there are different opinions if it is committed together with the crime listed in TPC 243, the Supreme Court of Appeals is of the opinion that TPC 244 should be applied. In our opinion, entering the system is not a necessary action in terms of TPC 244. In this case, it should be stated that a evaluation should be held according to the characteristics of the concrete case. Again, although there are different opinions about the perpetrator interfering with the data and forging documents, the Supreme Court of Appeals is of the opinion that TPC 244/2 should be applied.

In the relationship between TPC 244/4 and the qualified cases in TPC 142/1-e and TPC 158/1-f, if the action is within the scope of theft or fraud, the verdict will be based on theft or fraud, not TPC 244/4. If the subject of the crime is data, TPC 244/4 will occur, not the crime of theft. If fraudulent behavior is committed against the system rather than the real person, the action will be evaluated within the scope of TPC 244/4, not TPC 158/1-f.

It can be said that the main reason for the differences of opinion regarding the crimes regulated in Article 244 of the Turkish Penal Code is that the regulation is drawn in very general terms. Taking improvement suggestions into consideration is important both to ensure effective fight against crime and to protect the principle of legality.

GİRİŞ

Bilişim sistemleri kullanılarak ve bu sistemlere karşı yapılan saldırılarda artışla birlikte, bu tarz saldırılar dikkat çekmiş ve mal niteliğinde sayılmayan bilişim verileri mala zarar verme suçu kapsamında korunamadığından, soyut nitelikteki bu değerlerin korunması için yeni düzenleme getirilmesi zorunluluğu ortaya çıkmıştır[1]. Bu süreçte bilişim suçlarına ilişkin düzenleme eksikliği farklı devletlerce tespit edilmiş ve birçok devlet mevzuatlarında bu suçlara yönelik olarak yeni düzenlemeler oluşturulmuştur[2]. Kanun koyucumuz da bu eksikliği görerek Türk Ceza Kanunu'nda bilişim suçlarına yönelik düzenlemeler getirmiştir. Getirilen düzenlemelerle günümüzde sağlık, eğitim, savunma, sanayi, ulaşım vb. birçok alanda kullanılan; işleyişinde aksamaların görülmesi durumunda yıkıcı zarar tehlikesi bulunan bilişim sistemleri koruma altına alınmak istenmektedir. Bilişim sistemleri ve verilerin korunması amacıyla ortaya konan bu düzenlemelerden biri de sistemi engelleme, bozma, verileri yok etme ve değiştirme eylemlerine yönelik hükümlerdir. Ülkemizde buna ilişkin ilk düzenleme 1991 yılında 765 sayılı TCK'ya getirilen 525/b-1 maddesi olup[3], 5237 sayılı TCK ile bu madde yürürlükten kalkmıştır. Bu suçlar günümüzde 1997 ve 2003 tarihli TCK tasarıları esas alınarak hazırlanan[4], 5237 sayılı TCK'nın 244. maddesinde düzenlenmiş olup, madde metninde; "Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.

Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır.

Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır.

---

1 Berrin Akbulut, *Bilişim Alanında Suçlar*, (Ankara: Adalet Yayınevi, 2017), 176.

2 Muammer Ketizmen, "Türk Ceza Hukuku'nda Bilişim Suçları", (Doktora Tezi, Ankara Üniversitesi, 2006), 139.

3 Ketizmen, "Türk Ceza Hukuku'nda", 141.

4 Berrin Akbulut, "Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme", *Selçuk Üniversitesi Hukuk Fakültesi Dergisi*, 24/2 (2016), 10-11.

Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beş bin güne kadar adlî para cezasına hükmolunur." denilmek suretiyle yaptırıma bağlanmıştır.

İlk fıkrada "sistemin işleyişini engelleme, bozma", ikinci fıkrada "sistemdeki verileri bozma, yok etme, değiştirme, erişilmez kılma, sisteme veri yerleştirme, verileri başka yere gönderme" suç olarak düzenlenmiştir. Üçüncü fıkrada "ilk iki fıkradaki eylemlerin banka veya kredi kurumuna ya da kamu kurum veya kuruluşuna ait sistemler üzerinde işlenmesi" bir nitelikli hal olarak görülmüştür[5]. Dördüncü fıkrada başka suç oluşturmama şartı ile ilk iki fıkradaki eylemlerin işlenmesi suretiyle haksız çıkar sağlanması düzenlenmiş olup, nitelikli hal mi yoksa ayrı bağımsız bir suç mu olduğu doktrinde tartışmalıdır. TCK 244/1-2 AKSSS'nin dördüncü[6] ve beşinci[7] maddelerine uyum sağlamaya yönelik olup; TCK 244/1'de AKSSS madde 5'e paralel olarak bilişim sistemine müdahale eylemleri, TCK 244/2'de ise AKSSS madde 4'e paralel olarak sistemdeki verilere müdahale eylemleri düzenlenmiştir[8]. AKSSS'den farklı olarak verilere müdahalenin sisteme müdahaleden önce düzenlenmesindeki sıra TCK'da gözetilmemiş, sözleşmede eylemin haksız gerçekleştirilmesi aranmışken TCK'da böyle bir kıstas aranmamıştır[9]. Yine sözleşmede 4. maddede taraf

---

5 Veli Özer Özbek, Koray Doğan ve Pınar Bacaksız, *Türk Ceza Hukuku Özel hükümler*, (Ankara: Seçkin Yayınları, 2023), 1001.

6 AKSSS Madde 4: *1. Taraflardan her biri, bilgisayar verilerine haksız yere zarar verilmesi, verilerin silinmesi, tahrip edilmesi, değiştirilmesi veya engellenmesinin, kasten gerçekleştirildiği zaman, kendi iç hukuku kapsamında cezai suç olarak tanımlanması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir. 2. Taraflardan biri, 1. Paragrafta tanımlanan fiillerin ciddi zararla sonuçlanması gerektiğini şart koşma hakkını saklı tutabilir.*

7 AKSSS Madde 5:*Taraflardan her biri, bilgisayar sistemlerine veri girişi yaparak, bu verileri ileterek, bilgisayar verilerine zarar vererek, bunları silerek, tahrip ederek, değiştirerek veya engelleyerek bir bilgisayar sisteminin işleyişinin haksız yere engellenmesinin, kasten gerçekleştirildiği zaman, kendi iç hukuku kapsamında cezai suç olarak tanımlanması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir.*

8 Murat Volkan Dülger, *Bilişim Suçları Ve İnternet İletişim Hukuku*, (Ankara: Seçkin Yayınları, 2023), 333-334.

9 Akbulut, *Bilişim Alanında*, 177.

devletlere suç oluşumunda ciddi zarar şartı arayabilme imkanı verilmiş olsa da[10], TCK'da böyle bir şart aranmamıştır.

I. SUÇLA KORUNAN HUKUKİ DEĞER

İlk fıkrada sistem sahipleri, işletmecileri ve kullanıcılarının sistemin düzgünce çalışmasındaki yararlarının; ikinci fıkrada ise verilerin kullanımındaki faydanın korunduğu ifade edilmektedir[11]. Bazı yazarlar ise birinci fıkrada mülkiyet hakkının da korunduğunu[12], mülkiyet hakkı olmayan kullanıcıların ise sistem dokunulmazlığı, iletişim, teknolojik gelişim özgürlüğü gibi haklarının korunduğu; ikinci fıkrada ise duruma göre mülkiyet hakkının ya da fikri mülkiyet hakkının korunduğu düşüncesindedirler[13]. Bununla birlikte mülkiyetin korunduğu düşüncesine karşıt olan yazarlar ise TCK m. 244'ün malik olmayan kullanıcıları da koruması sebebi ile bu düşünceyi reddetmektedir[14]. Başka bir görüş ise suçun kanun sistematiğindeki yeri dikkate alındığında, malvarlığından ziyade, sistemin düzgün işleyişinin korunduğunu ifade etmektedir[15].

Bir diğer görüş bu suçları mala zarar verme suçunun özel şekli olarak görenlerden oluşmaktadır. Bu görüşe göre; suçun düzenlenmesinde sistemlerde yer alan yazılımsal süjelere yönelik eylemlerin klasik mala zarar verme suçu kapsamında görülüp görülemeyeceğine ilişkin tartışmalara son vermek amaçlandığından, korunan hukuki değer klasik mala zarar verme suçuna paralellik göstermektedir[16]. Buna göre, maddede düzenlenen eylemler mala zarar verme kapsamındaki eylemlerdir ve bu kapsamda malvarlığının korunması amaç-

10 Özbek, Doğan ve Bacaksız, *Türk Ceza Hukuku*, 1001.

11 Akbulut, *Bilişim Alanında*, 181.

12 Ö. Umut Eker, ""Türk Ceza Hukuku'nda Bilişim Suçları" Eski TCK Bağlamında Hukukumuzda Yer Alan İlk Düzenlemeler ve 5237 Sayılı Yeni Türk Ceza Kanunu'nun İlgili Hükümlerinin Yorumu", *Türkiye Barolar Birliği Dergisi*, 19/62 (2006): 124.

13 Demircan, *Bilişim Alanında Suçlar*, (İstanbul: Legal Yayıncılık, 2016), 86.; Ömer Demirci, *Bilişim Suçları ve Soruşturma Yöntemleri*, (Ankara: Seçkin Yayınları, 2022), 94.

14 Akbulut, *Bilişim Alanında*, 182.

15 Mahmut Koca ve İlhan Üzülmez, *Türk Ceza Hukuku Özel Hükümler*, (Ankara: Adalet Yayınevi, 2024), 1025.

16 Ketizmen, "Türk Ceza Hukuku'nda", 152.

lanmaktadır[17]. Mülkiyetin korunduğunu kabul eden görüş, TCK m. 244/4'ün haksız menfaat teminine ilişkin düzenlemesini bu suçlarla malvarlığının korunduğu noktasında önemli bir argüman olarak kullanmıştır[18]. Malvarlığının korunduğu görüşünde olan bazı yazarlar malvarlığı ile birlikte ayrıca sisteme olan güven[19], ile ekonomik düzenin de korunduğunu savunmaktadırlar[20].

Başka bir görüş ise bu suçlarla korunan hukuki değerin karma bir nitelik arz ettiğini savunmaktadır. Buna göre burada hem mülkiyetin hem de bilişim sistemi ve verilerin düzgün işleyişinin korunduğu ifade edilmektedir. Bu görüşe göre verilerin tamamı sistemin unsuru olmayıp bir kısmı sistemde tek başına mevcut unsurlar olduğundan, hem sistem hem de verilerin güvenliğinin korunduğu ifade edilmektedir[21]. Bununla birlikte bu suçlarla sistemin yalnızca veri veya yazılımlardan oluşan kısım değil, sistemin donanımı da korumaya dâhil edilmektedir[22]. Yargıtay ise bir kararında *"...Bilişim sistemlerinin veya verilerin zarar görmesi halinde, kişinin malvarlığında bir azalma meydana geleceği gibi toplumun, bilişim sistemlerinin işleyişine olan güvenleri ve ekonomik düzenin sağlıklı işleyişi etkilendiği, bilişim sistemlerinin zarar görmeden işler durumda bulunmasında toplumsal yarar olduğu için yasanın "topluma karşı işlenen suçlar" kısmına alınmıştır."*[23] diyerek karma görüşü benimsediğini göstermiştir.

Doktrinde yine bu suçlarla mülkiyet hakkı, bilişim sistemlerinin bütünlüğü ve güvenliği[24], iletişim hakları, ülke ekonomisi, kamu dü-

17 Ketizmen, "Türk Ceza Hukuku'nda", 152.

18 Mehmet Can Karagöz, "Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu (TCK m. 244)", (Yüksek Lisans Tezi, Akdeniz Üniversitesi, 2019), 111.

19 Ahmet Gül, *Doğrudan - Dolaylı Bilişim Suçları*, (Ankara: Seçkin Yayınları, 2021), 131.; Hasan Gerçeker, *Yorumlu ve Uygulamalı Türk Ceza Kanunu*, (Ankara: Seçkin Yayıncılık, 2022), 2207.

20 Cengiz Apaydın, *Bilişim Suçları ve Bilişim Ceza Hukuku*, (İstanbul: Acar Matbaacılık, 2017), 157.

21 Özbek, Doğan ve Bacaksız, *Türk Ceza Hukuku*, 1003.; Dülger, *Bilişim Suçları*, 335.

22 Dülger, *Bilişim Suçları*, 335.

23 11. Ceza Dairesi, 07.10.2009, E. 2009/1616, K. 2009/11328, https://kararara ma.yargitay.gov.tr/, 29.02.2024.

24 Karagöz, "Bilişim Sistemini", 112-113.

zeni ve güvenliği gibi[25] çeşitli korunan hukuki değer belirlemesi yapıldığı görülmektedir. Gerek madde gerekçesi gerekse doktrinde yer alan görüşler beraber değerlendirildiğinde ise; mülkiyet hakkının korunduğu görüşünün baskın olduğu söylenebilmektedir[26]. Doktrinde yer alan görüşler birlikte değerlendirildiğinde ise bu madde ile korunan birden fazla hukuki değerin olduğu söylenebilir. Bu suçlarla mülkiyet hakkı da korunmuş olmakla birlikte, korunan hukuki değerin yalnızca mülkiyet hakkı olduğu düşüncesi, toplum güveni, sistem bütünlüğü ve ekonomik düzen gibi korunmak istenen değerler ve taşıdıkları önemler dikkate alındığında eksik bir değerlendirmeyi ifade eder. Dolayısıyla kanaatimizce bu suçlarla korunan hukuki değer karma niteliktedir. TCK m. 244'ün temel aldığı maddeler olan AKSSS'nin 4. ve 5. maddelerinin açıklandığı raporda ise bu düzenlemelerde bilişim sistemlerine karşı gerçekleştirilecek haksız saldırıları önlemenin temel amaç olduğu belirtilmiştir[27].

II. SUÇUN MADDİ UNSURLARI

A. Suçun Konusu

TCK m. 244'ün ilk fıkrasında suçun konusunu bilişim sistemleri, ikinci fıkrada ise sistemde yer alan veriler oluşturmaktadır[28]. Bilişim sistemleri "bilişimde kullanılan bütün araç ve gereçlerin oluşturduğu sistemler"[29] olarak yahut "Verilere ilişkin bir takım saklama, nakletme, çoğaltma ve düzenleme gibi fonksiyonları otomatik gerçekleştiren sistemler"[30] olarak ifade edilebilir. Veri ise "Bir bilgisayar sisteminin belli bir işlevi yerine getirmesini sağlayan uygun programlar da içinde olmak üzere, bir bilgisayar sisteminde işlenmeye uygun biçimdeki her türlü bilgi veya kavramlar"[31] olarak tanımlanmaktadır. Öğretide bir

25 Apaydın, *Bilişim Suçları*, 160.

26 Sacit Yılmaz, "5237 Sayılı TCK'nın 244. Maddesinde Düzenlenen Bilişim Alanındaki Suçlar", *TBB Dergisi,* 92 (2011), 68.

27 Apaydın, *Bilişim Suçları*, 156-157.

28 Hasan Tahsin Gökcan ve Mustafa Artuç, Pratik Türk Ceza Kanunu, (Ankara: Adalet Yayınevi, 2023), 1322.; Nagihan Gün, "Türk Ceza Hukukunda Bilişim Suçları", (Yüksek Lisans Tezi, Çankaya Üniversitesi, 2020), 217.

29 TDK sözlük (Erişim Tarihi 13.01.2023), https://sozluk.gov.tr/

30 Özbek, Doğan ve Bacaksız, *Türk Ceza Hukuku*, 984.

31 "Council of Europe Convention on Cybercrime, Budapest, 23.XI.2001", (Erişim Tarihi 25.05.2023) https://www.coe.int/en/web/cybercrime/the-budapest-convention

görüş tarafından depolama işlevi gören araçlardaki veriler açısından bu suçun oluşmayacağı öne sürülmüş olup[32]; başka bir görüş ise aygıtlardaki verilerin de suçun konusu olarak kabulünün gerektiğini ve mala zarar verme suçuyla arasında fikri içtima yapılması gerektiğini savunmuştur[33]. Ancak madde lafzında "bir bilişim sistemindeki veriler" ifadesi kullanıldığından, burada bilişim sistemi olarak nitelendirilemeyecek, sadece depolama amacına hizmet eden aygıtlarda yer alan verilerin bu madde kapsamında değerlendirilmemesi gerekmektedir. Bu durumda depolama aygıtına yönelik eylem mala zarar verme suçu kapsamında olsa da aygıttaki verilerin taşıyabileceği önem dikkate alındığında, sistem haricindeki veriler yönünden bir düzenleme eksikliği bulunduğu ifade edilmelidir.

Öğretide bir görüş tarafından; içerisinde hiçbir veri bulunmayan ve çalışabilir durumda olmayan bir bilişim sisteminin bu suçun konusunu oluşturmayacağını, bu durumda mala zarar verme suçunun oluşacağını ifade edilmekte[34]; bir diğer görüş ise, içinde veri yer almasa dahi temel vazifelerini yerine getirebilecek sistemlerin suçun konusunu oluşturacağını ifade etmektedir[35]. Farklı bir görüş ise donanımsal unsurların bu suç kapsamında değil, mala zarar verme suçu kapsamında olduğunu, TCK m. 244'te yalnızca yazılıma yönelik eylemlerin cezalandırılmasının amaçlandığını savunmakta; failin kastının yazılıma mı yoksa donanıma mı zarar vermek olduğunun belirlenmesinin bu ayrımın sağlanması açısından önemli olduğunu ifade etmektedir[36]. Maddenin düzenlenme amacı bilişim sistemlerinin soyut unsurlarını, sistemin düzgün işleyişini ve sistemdeki verileri korumaktır. Bilişim sistemlerinin donanımsal yönü zaten mala zarar verme suçu ile koruma altındadır. Bu sebeple fiziki donanıma yönelik salt mala zarar verme amacıyla gerçekleştirilecek eylemler mala zarar verme

---

32 Durmuş Tezcan, Mustafa Ruhan Erdem ve Murat Önok, *Teorik ve Pratik Ceza Özel Hukuku,* (Ankara: Seçkin Yayıncılık, 2023), 1045.; Koca ve Üzülmez, *Türk Ceza Hukuku*, 1026-1027.; Ketizmen, "Türk Ceza Hukuku'nda", 178.

33 Akbulut, "Sistemi Engelleme", 27.

34 Dülger, *Bilişim Suçları*, 339.

35 Karagöz, "Bilişim Sistemini", 114.; Yavuz Erdoğan, "Türk Ceza Kanununda Bilişim Sistemini Engelleme Bozma Verileri Yok Etme Değiştirme Suçu", (Doktora tezi, Marmara Üniversitesi, 2011), 161-162.

36 Apaydın, *Bilişim Suçları*, 157.

suçu kapsamında değerlendirilmelidir. Bununla birlikte, gerçekleştirilen fiziksel saldırı sonucu sistemin soyut nitelikteki unsurlarına yönelik bir zarar meydana gelmişse bu durumda TCK m. 244/1-2 açısından failin olası kastı değerlendirilmelidir.

B. Fail

TCK m. 244'te fail yönünden herhangi bir özel nitelik belirtilmediğinden, herkes bu suçun faili olabilir. İnsan dışı varlıklarda iradi hareket serbestisi olduğu kabul edilmediğinden, bu suçun faili olamazlar[37]. Failin tespiti için eylemin yöneldiği sistemin ya da verinin, eylem her ikisine birden yönelikse her ikisinin ayrı ayrı kullanım, mülkiyet ve tasarruf haklarının sahibi belirlenmelidir[38]. Bir kişinin kendi veri ve sistemlerine zarar vermesi halinde, bu suç oluşmamakla birlikte[39], failin başkasının sistemindeki kendi verilerini yok etmek için sisteme zarar verirse TCK m. 244/1'de yer alan suç gerçekleşmiş olacaktır. Ancak doktrinde, veriler sistemden bütünüyle bağımsız düşünülemeyeceğinden faillik sıfatının oluşacağı ve kendiliğinden hak alma kapsamında eylemin hukuka uygunluk nedenleri noktasında tartışılması gerektiği düşüncesi de vardır[40].

Sistem sahibinin sistemin kullanımını diğer bir şahsa devretmesi hallerinde verilere zarar veren sistem sahibinin fail olarak eylemde bulunması hali TCK m. 244/2 kapsamında değerlendirilirken[41], kullanıcının fail olarak sisteme zarar vermesi eyleminde bulunması hali TCK m. 244/1 kapsamında değerlendirilir. Bu durumda tasarruf yetkisi hususu kişiler arasındaki hukuki ilişkiye göre belirlenmelidir[42]. Sözleşmede ayni kullanım geçişi de varsa verilere müdahale suç oluşturmayacak[43]; ancak tasarruf yetkisi verilmeyip sadece verileri sisteme girme yetkisi verilmişse kasti olarak verilere

37 Karagöz, "Bilişim Sistemini", 116.

38 Cengiz Apaydın, *Bilişim Sistemine Girme, Engelleme ve Bozma Suçları,* (Ankara: Seçkin Yayınları, 2023), 165. Hüseyin Akarslan, *Bilişim Suçları*, (Ankara: Seçkin Yayınları, 2015), 49. Dülger, *Bilişim Suçları*, 338.

39 Akbulut, *Bilişim Alanında*, 183.

40 Karagöz, "Bilişim Sistemini", 117.

41 Akbulut, *Bilişim Alanında*, 183.

42 Akbulut, "Sistemi Engelleme", 20.

43 Akbulut, "Sistemi Engelleme", 20.

zarar verilmesi durumunda TCK m. 244 kapsamında suç oluşacaktır[44]. Bu tip eylemler özellikle bulut bilişim sistemlerinin kullanımında görülmektedir[45].

Sisteme yetkisiz veri yüklenmesi gibi bir durumda, bu verilerin, sistem sahibi tarafından silinmesi ya da zarara uğratılması halinde veri sahibinin eylemi TCK m. 244/2 kapsamında suç oluşturmayacaktır[46]. Sisteme teknik destek için bir kimseye sınırlı müdahale yetkisi verilmesi gibi bir durumda ise bu kişinin kasten verileri yok etmesi ya da verilere zarar vermesi durumunda suç oluşacaktır[47].

C. Mağdur

TCK m. 244'te mağdur yönünden herhangi bir özel nitelik belirtilmediğinden, herkes bu suçun mağduru olabilir. Mağdur sıfatında olmak için mutlaka zarar gören sistemin yahut verilerin maliki ya da zilyedi olmak gerekmez[48]. Verilere müdahalede verilerin ilgili olduğu kişinin tasarruf yetkisi yoksa mağdur değil, suçtan zarar gören olabilir[49]. Sisteme müdahalede ise kullanıcı, işletici veya sistem sahibi mağdur olabilir[50]. Özetle, sistem ve verilerin arızasızlık hakkı kiminse suçun mağduru odur[51].

Doktrinde eylem sonucu zarar gören bilişim sistemi veya verilere herhangi şekilde ulaşmasında çıkarı olan ve tasarruf yetkisi bulunan kimsenin suçun mağduru olacağı ifade edilmektedir[52]. Aksine düşüncede ise; örneğin, finansal kiralamalarda kiralama şirketi her ne kadar sistemin maliki olsa da, verileri ve özel alanı ihlal edilen şirket olmadığından, mağdur sıfatı şirkette değil zilyetlik hakkı bulunan kiracıda olacaktır[53].

---

44 Akbulut, *Bilişim Alanında*, 183.

45 Dülger, *Bilişim Suçları*, 339.

46 Akbulut, *Bilişim Alanında*, 184-185.

47 Demircan, *Bilişim Alanında*, 89.

48 Dülger, *Bilişim Suçları*, 339.

49 Akbulut, "Sistemi Engelleme", 21. Akbulut, *Bilişim Alanında,* 185.

50 Akbulut, *Bilişim Alanında,* 185.

51 Akbulut, "Sistemi Engelleme", 21.

52 Dülger, *Bilişim Suçları*, 339.

53 Demircan, *Bilişim Alanında*, 89-90.

Doktrinde bir görüş ancak gerçek kişiler mağdur sıfatına sahip olabileceği düşüncesindeyken[54], diğer bir görüş tüzel kişilerin de mağdur sıfatına haiz olabileceği düşüncesinde olup[55], bu konu öğretide tartışmalı bir konudur. Bu konuda m. 244/3 açısından ilgili kurum veya kuruluşun mağdur olduğu düşüncesi öğretide baskındır[56]. Bu görüşe göre suçun doğası elverdiği ve niteliğine uygun düştüğü sürece tüzel kişiler de mağdur olarak değerlendirilebilecektir[57]. Yargıtay[58] ise bir kararında, sanığın aynı bankanın bir hesabından başka bir şubesindeki hesabına internet üzerinden havale gerçekleştirdiği iddiasıyla açılan davada, müşteki bankanın doğrudan suçtan zarar görmemesi sebebi ile hükmü temyiz hakkı bulunmadığına karar vermiştir.

Veriler mal vasfında görülemediğinden üzerindeki tasarruf yetkisinin sahibi konusunda doktrinde farklı kıstaslar öne sürülmüş, verileri hukuka uygun iktisap eden kişi, verilerin içeriğiyle ilgili olan kişi, veri taşıyıcısının maliki, verinin üreticisi, verilerin kaydını ya da naklini gerçekleştiren kişi olmak üzere kıstaslar ifade edilmiş ancak bu kıstaslar tek başına yeterli görülmedikleri için eleştirilmiş, sonuç olarak "malik benzeri yetki" şeklinde ifade edilerek birden fazla kıstas göz önünde bulundurulmuştur [59]. Ancak bu konuda tasarruf yetkisinin sahibi mevcut somut duruma göre değişiklik gösterebileceğinden, her somut olayın özelliklerine göre kendi içerisinde belirlenmesi gerekmektedir. Bu noktada tasarruf yetkisinin mutlak olup olmadığı da önemlidir.

---

54 Akbulut, *Bilişim Alanında*, 185.; Koca ve Üzülmez, *Türk Ceza Hukuku*, 1026.; Dülger, *Bilişim Suçları*, 270.; Gerçeker, *Yorumlu ve Uygulamalı*, 134.

55 Erdoğan, "Türk Ceza Kanununda", 1394.; Gözde Kaçmaz Keskin, *Türk ve Amerikan Hukukunda Tüzel Kişilerin Ceza Sorumluluğu*, (Ankara: Seçkin Yayıncılık, 2024), 185.; Eylem Baş, *Ceza Hukukunda Fail ve Mağdur*, (Ankara: Seçkin Yayıncılık, 2021), 742-743.; Gül, *Doğrudan Dolaylı*, 132.; Tezcan, Erdem ve Önok, *Teorik ve Pratik*, 1028.

56 Tezcan, Erdem ve Önok, *Teorik ve Pratik*, 1044.

57 Tuğrul Katoğlu, "Ceza Hukukunda Suçun Mağduru Kavramının Sınırları", *AÜHFD*, 61/2 (2012), 672.

58 Yargıtay 2. Ceza Dairesi, 01/06/2016, E. 2014/25924, K. 2016/10421, https://karararama.yargitay.gov.tr/, 29.02.2024.

59 Tartışmalar için bkz: Akbulut, *Bilişim Alanında*, 186-187.

D. Fiil

TCK m. 244 ilk fıkrada bilişim sisteminin işleyişini engelleme ve bozma; ikinci fıkrada ise sistemdeki verilerin bozulması, yok edilmesi, değiştirilmesi veya başka yere gönderilmesi seçimlik hareketli olarak düzenlenmiştir. Bilişim sisteminin amacına uygun faaliyet yürüttüğü sırada, dışarıdan gerçekleştirilen etkiyle, faaliyetinin kısmen veya tamamen durdurulmasına "engelleme", sisteme faaliyetini yürütemeyecek şekilde kısmen veya tamamen zarar verilmesine ise "bozma" denir[60]. Bu suç genellikle icrai hareketle işlenmekle birlikte, teknik sorumlunun güvenlik yazılımlarını kasten yüklememesi gibi hallerde olduğu gibi ihmalen de işlenebilir[61]. Doktrinde birden çok bilişim sistemi ya da yazılım kullanılarak gerçekleştirilen saldırılar için cezayı artıran nitelikli hal düzenlenmemesi bir eksiklik olarak değerlendirilmektedir[62].

Doktrinde bir görüşe göre işleyişi engelleme ile bilişim sistemini bozmayacak fakat sistemin faaliyetini düzgün şekilde yerine getirmesine engel olacak düzeyde her tür eylem bu kapsamda değerlendirilir[63]. Ancak bu görüşe karşın, sistem işleyişinin yavaşlatılmasını engellenme olarak değerlendirmeyen görüşler de bulunmaktadır[64]. Kanaatimizce engelleme bir şeyin fonksiyonunun tamamen kaybettirilmesinin yanında, fonksiyonunun önemli derecede azaltılması suretiyle de gerçekleşmektedir. Bu kapsamda; sistemin işleyişinin yavaşlatılması halinde de engelleme gerçekleşmiş olacaktır. Yargıtay'ın bir kararında[65]; sistemin çalışmasını ağırlaştıran ya da kilitleyen eylemler engelleme olarak değerlendirilmiştir.

Geçici ya da kalıcı engellemenin bir fark oluşturup oluşturmayacağı konusunda, bir görüşe göre kalıcı sonlandırma halinde eylem

---

60 Özbek, Doğan ve Bacaksız, *Türk Ceza Hukuku*, 1006.; Koca ve Üzülmez, *Türk Ceza Hukuku*, 1028.

61 Hasan Burak Öndin, "Türk Hukukunda Doğrudan Bilişim Suçları", (Yüksel Lisans Tezi, Anadolu Üniversitesi, 2017), 54.; Dülger, *Bilişim Suçları*, 343.

62 Ömer Demirci, *Bilişim Suçları*, 99.

63 Dülger, *Bilişim Suçları,* 342.

64 Akbulut, "Sistemi Engelleme", 28.

65 Yargıtay 11. Ceza Dairesi, 13.03.2013, E. 2011/2816, K. 2013/4065, https://kararara ma.yargitay.gov.tr/, 23.11.2024.

engelleme değil, bozma kapsamında değerlendirilmeli iken[66]; başka bir görüşe göre daimi ya da geçici engellemenin bir önemi olmamakla[67] birlikte, geçici engelleme önemsiz ölçüde ise haksızlık içeriği az olduğundan cezalandırma dışı bırakılmalıdır[68]. AKSSS'de ise açıklayıcı raporda taraf devletlerce engellemenin ciddi ölçüde olması şartı aranabileceği; bununla beraber asgari tahribatın dahi ciddi görülebileceği, yavaşlatma etkisi gösteren zararlı yazılım ya da saldırılarınsa ciddi olarak değerlendirilebileceği belirtilmiştir[69].

Failin saldırıları sonucu sisteme koyduğu engel ortadan kaldırıldığı takdirde sistem düzgün işleyişine devam ediyorsa bu durumda bozma değil engelleme kapsamında değerlendirilmesi gerektiği ifade edilmelidir. Bu anlamda engellemenin geçici ya da kalıcı olması engelleme eylemi açısından bir fark oluşturmaz, yalnızca somut cezanın belirlenmesinde dikkate alınması gerekir.

Doktrinde bir görüş, engelleme eyleminin fiziksel saldırılarla da gerçekleştirilebileceğini ifade etmekte[70], buna karşın başka bir görüş bu madde kapsamında engellemenin soyut unsurlara yönelik saldırılarla sınırlı olduğunu, fiziksel müdahalelerin mala zarar verme suçu kapsamında değerlendirilmesi gerektiğini savunmaktadır[71]. Ancak madde metninde soyut ya da somut herhangi bir eylem şekli belirtilmediğinden fiziksel saldırılar yoluyla da gerçekleştirilebileceği görülmektedir. Son olarak öğretide engellemeye ilişkin düzenlemenin kanunilik ilkesini zedelediğini, geniş yoruma imkan verdiğini, aslında bir netice olan engellemenin hangi eylemlerle gerçekleştirileceği ko-

66 Özbek, Doğan ve Bacaksız, *Türk Ceza Hukuku*, 1007.; Öndin, "Türk Hukukunda", 54.; Apaydın, *Bilişim Sistemine*, 172.; İrem Geçmez, *Bilişim Sistemini Engelleme, Bozma Verileri Yok Etme veya Değiştirme Suçları (TCK M. 244)*, (Ankara: Seçkin Yayınları, 2020), 82. Mert Çakıcı "Türk Ceza Kanunu M. 243 ve M. 244'te Düzenlenen Bilişim Suçları". Ceza Hukuku Dergisi, 9/24 (2014), 327.

67 Demircan, *Bilişim Alanında*, 93.; Akbulut, "Sistemi Engelleme", 30.; Gün, "*Türk Ceza Hukukunda*", 222.; Demirci, *Bilişim Suçları*, 98.

68 Akbulut, *Bilişim Alanında*, 193.

69 Burak Cesur Aköz, "Türk Ceza Kanunu Kapsamında Bilişim Suç Ve Cezaları İle Örnek Yargısal Kararların Analizi Ve Mevzuat Önerileri", (Bilişim Uzmanlığı Tezi, Bilgi Teknolojileri Ve İletişim Kurumu, 2018), 111.

70 Dülger, *Bilişim Suçları*, 343.

71 Koca ve Üzülmez, *Türk Ceza Hukuku*, 1028-1029.

nusunda AKSSS'deki gibi açıklık sağlanması gerektiğini belirten görüşler vardır[72].

Bozma eylemini ise Yargıtay; durmadan daha ileri bir şekilde çökertme, işlemez hale getirme ve hatta fiziki olarak zarara uğratma olarak ifade etmiştir[73]. Sistemin bozulması zaruri olarak sistemin engellenmesine de sebep olmaktadır[74]. Ancak burada önemli husus, fiziki zararın "sistemin işleyişine" verilmesidir[75]. Yani verilen fiziki zararın sistemin işleyişini bozmaya yönelik olarak verilmesi gerekmektedir. Sistem unsurlarından bir kısmının bozulması sistemin tümünü etkiliyorsa, sistem beklenen işlevini yerine getiremiyorsa o halde bu suç kapsamında değerlendirilir[76]. Sistemin yanlış işlemesinin sağlanması da sistemi bozma olup, bozmanın tamamen yahut kısmen olması önem arz etmemektedir[77].

TCK m. 244/2 seçimlik hareketli bir suç olarak düzenlenmiş olup, sayılan verileri bozma, yok etme, erişilmez kılma ve değiştirme fiilleri verilerin kullanımına engel olmayı amaçlarken; sayılan diğer eylemler bu amacı gütmez[78]. Genellikle icrai hareketle işlenseler de ihmali hareketle de işlenebilirler[79]. Doktrinde bir görüşe göre, ikinci fıkra eylemleriyle ile ilk fıkradaki suç gerçekleştirilebileceğinden fıkralar arasındaki temel ayrım maksat yönünden ortaya çıkmaktadır; hangi fıkranın uygulanacağının belirlenmesi failin kastına bağlıdır[80]. Ancak doktrinde bir görüş, bu halde artık 2. fıkradaki suçun değil, 1. fıkradaki suçun oluşacağı kanaatindedir[81]. Bu konuda failin kastına göre değerlendirilme yapılması gerektiği ifade edilmelidir.

---

72 Akbulut, "Sistemi Engelleme", 29.; Akbulut, *Bilişim Alanında*, 191-192.

73 Y. 11. D., K. 2013/4065.

74 Apaydın, *Bilişim Suçları*, 185.; Koca ve Üzülmez, *Türk Ceza Hukuku*, 1028

75 Demircan, *Bilişim Alanında*, 94.

76 Dülger, *Bilişim Suçları*, 344.

77 Akbulut, *Bilişim Alanında*, 194-195.

78 Akbulut, *Bilişim Alanında*, 195.

79 Akbulut, *Bilişim Alanında*, 195. Erdoğan, "Türk Ceza Kanunu'nda", 194.

80 Dülger, *Bilişim Suçları*, 345.

81 Tezcan, Erdem ve Önok, *Teorik ve Pratik*, 1046-1048.; Koca ve Üzülmez, *Türk Ceza Hukuku*, 1030. Erdoğan, "Türk Ceza Kanunu'nda", 172.

Verileri bozma; verilerin özgülendiği amaçla kullanılmasının tamamen veya kısmen önüne geçer nitelikte verilere zarar verilmesidir[82]. Verileri yok etme; verilerin ortadan kaldırılması, silinmesi anlamına gelmekle birlikte; Bir görüşe göre verinin tüm izlerinin depolama ünitesinden silinmesi anlamına gelen fiziksel ve verinin erişim anahtarının silinmesi anlamına gelen mantıksal silme ayrımında maddede kastedilen mantıksal anlamda silme iken[83], diğer görüş maddenin her iki tip yok etme şeklini de kapsadığını ifade etmekte[84], başka bir görüş ise verilerin tam ve telafisi olmayacak şekilde tanınmaz biçime getirilmesi olarak değerlendirmekte ve kopyası bulunan verinin silinmesi durumunda yok etmenin gerçekleşmiş olmayacağını ifade etmektedir[85]. Bir görüşe göre veri geri dönüşüm kutusuna atıldığında sistemde bulunmaya devam ettiğinden yok edilmiş olmayacaktır[86]. Başka bir görüşe göreyse böyle bir durumda yok etme gerçekleşmiştir[87]. Verinin yok etme halinde özel cihaz veya yöntemlerle geri getirilebilecek olması durumunda bir görüş yok etme eyleminin gerçekleşmeyeceğini savunurken[88], başka bir görüş maddede veriye ulaşmayı güçleştirecek eylemlerin kastedildiğinden bahisle suçun oluşmasını engellemediğini savunmaktadır[89]. Bu konuda her iki tip silme türü ile de yok etme gerçekleşmiş olacağı ifade edilmelidir. Verinin özel cihaz ya da yöntemlerle geri getirilebilecek olması halinde de yok etme gerçekleşmiş olur. Verinin kopya olması ya da kopyasının bulunması ise önem arz etmez. Verinin geri dönüşüm kutusuna atılması durumunda ise veri dönüşüm kutusunda kaldığı süre müddetince yok edilmiş olmaz, bu durumda var olan veriyi başka yere gönderme söz konusu olur.

---

82 Akbulut, *Bilişim Alanında*, 196.; Koca ve Üzülmez, *Türk Ceza Hukuku*, 1030.; Ketizmen, "Türk Ceza Hukuku'nda", 171.; Özbek, Doğan ve Bacaksız, *Türk Ceza Hukuku*, 1009.

83 Erdoğan, "Türk Ceza Kanunu'nda", 197.; Demircan, *Bilişim Alanında*, 97.

84 Yılmaz, "5237 Sayılı", 73.

85 Akbulut, "Sistemi Engelleme", 33.; Akbulut, *Bilişim Alanında,* 197.

86 Alaattin Bük, *Bilişim Alanında Kişisel Verilerin Korunması*, (Ankara: Seçkin Yayınları, 2018), 122.; Demirci, *Bilişim Suçları*, 100.; Koca ve Üzülmez, *Türk Ceza Hukuku*, 1030.

87 Erdoğan, "Türk Ceza Kanunu'nda", 198.

88 İrem Geçmez, *Bilişim sistemini*, 117.; Akbulut, *Bilişim Alanında*, 196-197.

89 Koca ve Üzülmez, *Türk Ceza Hukuku*, 1030.

Verileri değiştirme, veriye başka bir biçim verme, başka görünüme veyahut duruma getirme ve yeni içerik kazandırmayı ifade etmektedir[90]. Verileri erişilmez kılma, bir sistemde yahut veri aracında bulunan verilere ilgilisi olduğu kişinin potansiyel erişim imkânının ortadan kaldırılarak istediği an ve yerde ulaşmasının engellenmesidir[91]. Erişilmez kılma virüs, şifre koyma, veri silme, başka yere taşıma[92], sistem gücünü kesme[93] gibi birçok şekilde gerçekleştirilebilir.

Sisteme veri yerleştirmede fail sisteme hukuka uygun girip girmemesinin bir önemi olmaksızın[94] sistemde mevcut olmayan dış verilerin sisteme girilmesi bu suçu oluşturur[95]. Var olan verileri başka yere gönderme, sistemdeki verileri başka sisteme ya da veri taşıma aracına taşımak yahut kopyalamak eylemlerinde bulunmaktır[96]. Mağdurun verisinin yine mağdurun sistemindeki başka bir dosyaya taşınmasının da bu suçu oluşturacağı düşüncesinde olan görüşler mevcuttur[97]. TCK'nın 135, 136 ve 142. maddesinden ayırt edilebilmesi için verilerin niteliğinin belirlenmesi gerekmektedir[98].

E. Netice

Bu suçların netice unsuru doktrinde tartışmalı olup ilk görüşe göre; iki suç tipinde de yer alan yok etme, engel olma bozma, gönderme ifadeleri aslında ortaya çıkan neticelerdir[99]. Neticeli suç olduğunu savunan başka bir görüşe göre eylem sonucu zarar da oluşacağından bu suç bir zarar suçudur[100]. Neticeli suç olduğunu savunan diğer bir

90 Akbulut, *Bilişim Alanında,* 199.

91 Dülger, *Bilişim Suçları*, 347.

92 Dülger, *Bilişim Suçları*, 347.

93 Akbulut, *Bilişim Alanında,* 200.

94 Dülger, *Bilişim Suçları*, 350.; Koca ve Üzülmez, *Türk Ceza Hukuku*, 1030.

95 Akbulut, *Bilişim Alanında*, 202.

96 Dülger, *Bilişim Suçları*, 351.; Koca ve Üzülmez, *Türk Ceza Hukuku*, 1030.

97 Erdoğan, "Türk Ceza Kanunu'nda", 203.; Öndin, "Türk Hukukunda", 60-61.; Bük, *Bilişim Alanında*, 123.

98 Dülger, *Bilişim Suçları,* 351.

99 Dülger, *Bilişim Suçları*, 355.; Akbulut, *Bilişim Alanında*, 190.; Koca ve Üzülmez, *Türk Ceza Hukuku*, 1027.; Erdoğan, "Türk Ceza Kanunu'nda", 192.

100 Erdoğan, "Türk Ceza Kanunu'nda", 212.; Benzer şekilde; Geçmez, *Bilişim Sistemini*, 86.; Öndin, "Türk Hukukunda", 55.; Gün, "*Türk Ceza Hukukunda*", 220.; Demircan, *Bilişim Alanında*, 101.

görüşe göre ise maddede böyle bir zarar şartı aranmadığından bu suç tehlike suçudur[101]. İkinci görüşe göre ise; suç tipinde neticenin gerçekleşmesi yahut zarar aranmaz, suç sırf hareket suçudur[102].

Birinci fıkrada sistemin engellenmesi ve bozulması, ikinci fıkrada verileri bozma, yok etme, değiştirme, erişilmez kılma, sisteme veri yerleştirme ve var olan verileri başka bir yere gönderme eylemleri aslında bir netice ifade ettiğinden, zararlı yazılım kullanarak yahut bunun gibi farklı birçok şekilde gerçekleştirilebileceğinden, bu suçların serbest hareketli ve neticeli suçlar olduğu söylenebilir. Özellikle bir zararın ortaya çıkması ise aranmamakta olup, şart değildir. AKSSS'de de böyle bir şart aranmamıştır[103].

F. Nitelikli Haller

TCK m.244/3'te, ilk iki fıkradaki suçların bir banka, kredi kurumu, kamu kurum veya kuruluşuna ait sistemler üzerinde işlenmesi halinde faile verilecek cezanın yarı oranında arttırılması öngörülerek bu suçların nitelikli hali düzenlenmiştir.

765 sayılı TCK döneminde, ortaya çıkabilecek zararın büyüklüğü göz önünde bulundurulmayarak kişisel bilgisayarlar ile kurumsal bilgisayarlar arasında ayrım yapılmamış olması doktrinde eleştiri konusu olmuştu[104]. 5237 sayılı TCK ile birlikte ise bu eleştirilerin dikkate alındığı ve söz konusu düzenleme ile bu konudaki eksikliğin giderildiği görülmektedir. Ancak doktrinde maddede kurum sınırlaması yapılmasının doğru olmadığı ve özel diğer şirket veya işletmelerin de bu kapsama alınması gerektiği vurgulanmıştır[105]. Benzer başka bir görüş ise düzenlemenin kamu özel ayrımı yapılmaksızın top yekûn hizmetin korunmasına yönelik olması gerektiği vurgusu yapılmıştır[106]. Yine doktrinde bu nitelikli halle birlikte, kamu, banka ya da kre-

---

101 Apaydın, *Bilişim Suçları*, 189.

102 Çakıcı, "Türk Ceza Kanunu", 329.; Özbek, Doğan ve Bacaksız, *Türk Ceza Hukuku*, 1009. Hayati Pallı, "Türk Hukukunda ve Mukayeseli Hukukta Bilişim Suçları", (Yüksek Lisans Tezi, Erciyes Üniversitesi, 2008)", 170.

103 Pallı, "Türk Hukukunda", 170.

104 Dülger, *Bilişim Suçları*, 356.

105 Akbulut, *Bilişim Alanında*, 205-206.

106 Gün, "Türk Ceza Hukukunda", 240.

di kurumu görevlilerinin içeriden eylemde veya ihmalde bulunarak bu suçları işlemesinin de nitelikli hal olarak düzenlemesi gerektiği düşünülmektedir[107].

3713 sayılı Terörle Mücadele Kanunu'nun 4. maddesinde TCK m. 244'teki suçların terör amacıyla işlenmesi hali TCK m. 244'e ilişkin bir başka nitelikli hal olarak düzenlenmiştir.

Bilişim sistemi aracılığıyla haksız çıkar sağlamanın düzenlendiği TCK m. 244/4'ün nitelikli hal mi yoksa ayrı bir suç mu olduğu konusunda doktrinde görüş ayrılıkları bulunmakta olup; fıkrada TCK m. 244/1 ve 2'de tanımlanan fiillerle kişinin kendisi ya da başkası yararına haksız çıkar sağlamasının başka bir suç oluşturmaması halinde TCK m. 244/4 kapsamında cezalandırılacağı düzenlenmiştir. TCK m. 244/4'ü cezayı artıran bir nitelikli hal olarak gören görüşe[108] göre TCK m. 244/4 ile temel suç tipine bağlılık devam ettirilmekte ve bu haliyle 1. ve 2. fıkraların nitelikli halini oluşturmaktadır. İkinci görüşe göre[109] ise, TCK m. 244/4 ile ilk iki fıkradaki suçlardan ihlal şekilleri ve korunan hukuki değerler yönünden ayrılan, haksız çıkar sağlama yönüyle kendi temel şekli unsurları bulunan, TCK m. 244/1-2'deki unsurları da kapsayarak bileşik suç niteliği taşıyan ayrı bir suçtur. Bu konuda ilk görüşün de ifade ettiği üzere söz konusu düzenleme temel suç tipine bağlılığı devam ettirmekte olduğundan, TCK m. 244/4'ün TCK 244/1-2'nin nitelikli hali olduğu ifade edilebilir. Bu ayrımın önemi ise suça teşebbüs açısından ortaya çıkmakta, nitelikli hal olarak kabulü halinde teşebbüs mümkün olmamaktadır[110].

III. SUÇUN MANEVİ UNSURU

TCK m. 244/1-2'de düzenlenen suçlar kasten işlenebilen suçlar olup taksire ilişkin düzenleme bulunmadığından taksirle işlenemez. Failin saiki eyleminin ilki iki fıkradan hangisine girdiğinin tespitinde

---

107 Dülger, *Bilişim Suçları*, 357.; Apaydın, "Bilişim Sistemine", 174.; Erdoğan, "Türk Ceza Kanunu'nda", 166.

108 Özbek, Doğan ve Bacaksız, *Türk Ceza Hukuku*, 1012-1013.; B. Zakir Avşar ve Gürsel Öngören, *Bilişim Hukuku*, (İstanbul: Türkiye Bankalar Birliği, 2010), 139.; Çakıcı, "Türk Ceza Kanunu", 335.

109 Akbulut, *Bilişim Alanında,* 217.; Erdoğan, "Türk Ceza Kanunu'nda", 223.; Koca ve Üzülmez, *Türk Ceza Hukuku*, 1034-1035.; Dülger, *Bilişim Suçları*, 364-365.

110 Özbek, Doğan ve Bacaksız, *Türk Ceza Hukuku*, 1013.

dikkate alınır[111]. Failin olası kastla hareket etmesi de suçun oluşması için yeterli olup[112], örneğin; zararlı yazılımlar yoluyla sisteme girerek sistemdeki verileri incelemek amacıyla hareket eden fail, bu eylemiyle sistemin işleyişine yahut verilere zarar verebileceğini öngörmekte ancak bu durumun gerçekleşmesini umursamayarak hareket etmekte ise ve eylemi sonucunda sisteme zarar verme eylemi gerçekleştiyse bu durumda söz konusu suç oluşacaktır. Burada kasten hareketin söz konusu olabilmesi için suçun kanuni tanımında yer alan eylemlerin failce gerçekleşme ihtimalinin bilinmesi yeterlidir[113].

IV. HUKUKA AYKIRILIK UNSURU

TCK m. 244'te yer alan suçların gerçekleşebilmesi için fiilin hukuka aykırı olması, hukuka uygunluk nedenlerinin bulunmaması gerekir. Bu suçlar için ilgilisinin rızası, görevin ifası/ kanun hükmünün icrası[114] ile meşru savunma hukuka uygunluk nedenlerinden birinin bulunması mümkün olabilir[115].

Görevin ifası hukuka uygunluk nedenine örnek olarak CMK m. 134'te yer alan kolluğun delil elde etmesine yönelik eylemler verilebilir. Meşru savunma ise saldırıyı engellemeye yönelik orantılı hukuka uygun karşı saldırı şeklinde gerçekleştirilebilir.

V. SUÇUN ÖZEL GÖRÜNÜŞ BİÇİMLERİ

A. Teşebbüs ve Suça İştirak

TCK m. 244'te yer alan suçlara teşebbüs mümkündür. TCK m. 244 açısından iştirak yönünden herhangi bir özel düzenleme bulunmamaktadır. İştirake ilişkin genel hükümler uygulanır.

B. Suçların İçtimaı

Suçların içtimaı konusunda TCK m. 244'te yer alan suçlar açısından birden fazla durumun gerçekleşebileceğini söylemek mümkündür. TCK m. 244/1-2' ile TCK m. 243'te yer alan suçun birlikte işlen-

111 Dülger, *Bilişim Suçları,* 357.

112 Koca ve Üzülmez, *Türk Ceza Hukuku*, 1031.

113 Akbulut, *Bilişim Alanında*, 203.

114 Koca ve Üzülmez, *Türk Ceza Hukuku*, 1032.

115 Erdoğan, "Türk Ceza Kanunu'nda", 164.

mesi halinde fikri içtima uygulanması[116], geçitli suç olarak görülmeleri[117], failin kastına göre belirleme yapılması[118], ile tüketen-tüketilen norm ilişkisi olarak ele alınması[119] olmak üzere farklı görüşler bulunmaktadır. Yargıtay[120] ise bu hallerde TCK m. 244'ün uygulanması gerektiği kanaatindedir. Bu konuda TCK m. 244 açısından sisteme girme zaruri bir eylem olmadığından, somut olayın özelliklerine göre değerlendirilerek, tek fiille her iki suç tipinin ihlalinin söz konusu olması halinde fikri içtima yapılması gerektiği ifade edilmelidir.

TCK m. 245/A ile TCK m. 244'ün beraber işlenmesi durumunda TCK m. 245/A'da hazırlık hareketleri ayrı ve bağımsız suç olarak düzenlendiğinden, bu suçlar yönünden gerçek içtima söz konusu olacaktır[121]. Failin tek eylemiyle TCK m. 244/2 ile TCK m. 267-271'deki suçları birlikte işlenirse farklı neviden fikri içtima uygulanarak en ağır suçtan ceza verilecektir[122].

TCK m. 244/1-2'deki suçlar zincirleme suç şeklinde işlenebilmekle birlikte, bunun için aynı suçun ihlal edilmesi gerekir, ancak TCK m. 244/1 ile TCK m. 244/2'nin peş peşe ihlal edilmesi örneğindeki gibi, koruduğu hukuki değer farklı olan suçların bir arada işlenmesi halinde zincirleme suç hükümleri uygulanmaz[123].

TCK m. 244/1 ve 2'deki suçların birlikte gerçekleştirilmesi durumunda doktrinde bir görüş, tek eylemle farklı suçlar gerçekleştirildiğinden fikri içtima uygulanması gerektiği[124]; başka bir görüş ise 2. fıkradaki hareketlerle TCK m. 244/1'deki suç gerçekleştirildiyse bu-

---

116 Koca ve Üzülmez, *Türk Ceza Hukuku*, 1033.; Akbulut, *Bilişim Alanında*, 211-212.; Apaydın, *Bilişim Suçları*, 182.; Geçmez, *Bilişim Sistemini*, 104.

117 Yılmaz, "5237 Sayılı", 83.; Erdoğan, "Türk Ceza Kanunu'nda", 171.; Bük, *Bilişim Alanında*, 125.; Gül, *Doğrudan Dolaylı*, 140

118 Özbek, Doğan ve Bacaksız, *Türk Ceza Hukuku*, 1000

119 Fatih Selami Mahmutoğlu, "Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi", *Journal of İstanbul University Law Faculty*, 71/1 (2013): 869.

120 Yargıtay 8. Ceza Dairesi, 14.07.2014, E. 2013/3173, K. 2014/ 18506, https://kararara ma.yargitay.gov.tr/ 11.07.2024.

121 Akbulut, *Bilişim Alanında*, 212.

122 Dülger, *Bilişim Suçları*, 361.

123 Dülger, *Bilişim Suçları*, 360.

124 Erdoğan, "Türk Ceza Kanunu'nda", 214-215.; Bük, *Bilişim Alanında*, 120.

rada TCK m. 244/1'in uygulanması gerektiği düşüncesindedir[125]. Başka bir görüşe göre ise, ikinci fıkra eylemleriyle ile ilk fıkradaki suç gerçekleştirilebileceğinden fıkralar arasındaki temel ayrım maksat yönünden ortaya çıkmaktadır; hangi fıkranın uygulanacağının belirlenmesi failin kastına bağlıdır[126]. Bu konuda failin kastına göre belirleme yapılması gerektiği ifade edilmelidir.

TCK m. 244/2 ile TCK 151 arasında ise bir görüşe göre her iki madde de ihlal edildiğinden fikri içtima yapılması gerekirken[127], diğer görüşe göre TCK m. 244 özel bir mala zarar verme suçu olduğundan, burada özel düzenleme olan TCK m. 244'ün uygulanması gerekmektedir[128]. Başka bir görüşe göre ise failin kastının dikkate alınarak suçun belirlenmesi gerekmektedir[129]. Bu konuda failin kastına göre belirleme yapılması gerektiği ifade edilmelidir.

TCK m. 142/1-e'de ise hırsızlık suçunun bilişim sistemleri aracılığıyla işlenmesi nitelikli hali, TCK m. 158/1-f'de ise dolandırıcılık suçunun bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle işlenmesi nitelikli hali düzenlenmiştir. Bu kapsamda TCK m. 244/4'te yer alan düzenlemeyle TCK m. 142/1-e ile TCK m. 158/1-f'de yer alan nitelikli haller arasındaki ilişki önem arz etmektedir. Madde metni incelendiğinde TCK m. 244/4'teki düzenlemede yer aldığı üzere bu madde kapsamında gerçekleştirilen eylemin başka bir suç oluşturmaması halinde bu madde kapsamında cezalandırma söz konusu olacağından, eylemin hırsızlık veya dolandırıcılık suçu kapsamında değerlendirilecek olması halinde, TCK m. 244/4'ten değil, hırsızlık ya da dolandırıcılık suçlarından hüküm kurulacaktır. Doktrinde TCK m. 142/1-e ile TCK m. 158/1-f'de yer alan düzenlemelerin TCK m. 244/4'ün uygulama alanını daraltma amacı güttüğü ifade edilmektedir[130] TCK m. 244/4 ile hırsızlık suçu arasında ise; soyut nitelikteki veriler hırsızlık suçunun konusunu oluşturan mal kavramı içerisinde değerlendirilemeyeceğinden, verilere yönelik eylemler hırsızlık suçu kapsa-

125 Koca ve Üzülmez, *Türk Ceza Hukuku*, 1030.

126 Dülger, *Bilişim Suçları*, 345.

127 Akbulut, *Bilişim Alanında*, 210.

128 Mahmutoğlu, "Türk Ceza Kanunu'nda", 866.

129 Erdoğan, "Türk Ceza Kanunu'nda", 175-176.; Yılmaz, "5237 Sayılı", 82.

130 Koca ve Üzülmez, *Türk Ceza Hukuku*, 1034.

mında görülmemiş, TCK m. 244/4'ün konusunun veri olduğu ifade edilerek bu suçun oluştuğu kanısına varılmıştır[131]. TCK m. 244/4 ile dolandırıcılık suçu arasında ise; dolandırıcılık suçunda hileli davranışın gerçek iradeye yöneltilmesi gerektiğinden hileli hareketin sisteme karşı yapılması ile haksız bir kazanç elde edilmesi halinde, gerçek bir şahsa yönelik hileli bir davranış olmadığından, eylem TCK m. 244/4 kapsamında değerlendirilecektir[132].

VI. MUHAKEME

TCK m. 244/1-2'de yer alan her iki suç için de yalnızca hürriyeti bağlayıcı ceza öngörülmüştür. Doktrinde ise bu suçlar yönünden seçimlik ceza öngörülmesinin daha yerinde olacağı ifade edilmiş, ayrıca cezanın alt sınırının bu suçlardaki işlenme sıklığı ile ortaya çıkan zararın ağırlığı göz önünde bulundurulduğunda oldukça düşük kaldığı ifade edilmektedir[133]. Yine, verilerin mağdura göre önemli olması halinde verilecek cezanın arttırılmasını öngören bir düzenleme getirilmesinin yerinde olacağı ifade edilmiştir[134]. TCK m. 246'da ise tüzel kişilere yönelik güvenlik tedbirleri düzenlenmiştir.

TCK m. 244'te düzenlenen suçlar şikâyete tabi değildir. Görevli mahkeme Asliye Ceza Mahkemeleri, yetkili mahkeme ise suçun işlendiği yer mahkemesidir. Bu davalara, 1229 sayılı HSK kararı gereğince ihtisas mahkemelerince bakılacağı düzenlenmiştir[135].

SONUÇ

TCK m. 244/1-2'de yer alan suçlar AKSSS'nin 4. ve 5. maddelerine uyum sağlayacak şekilde düzenlenmek suretiyle kanunumuzda yer verilen bilişim suçlarıdır. Bu suçlarla korunan hukuki değer konusunda doktrinde mülkiyet hakkı, bilişim sistemlerinin bütünlüğü ve güvenliği, iletişim hakları, ülke ekonomisi, kamu düzeni ve güvenliği olmak üzere farklı değerlendirmeler yapılmış olup, korunan hukuki değerin karma nitelik arz etmektedir. Suçun konusu ilk fıkra için bili-

131 Yargıtay 13. Ceza Dairesi, 10.10.2017, E. 2016/2155, K. 2017/10403, https://karararama.yargitay.gov.tr/, 02.07.0024

132 Özbek, Doğan ve Bacaksız, *Türk Ceza Hukuku*, 748.

133 Akbulut, *Bilişim Alanında*, 212-214.

134 Dülger, *Bilişim Suçları*, 362-363.

135 Dülger, *Bilişim Suçları*, 363.

şim sistemleri, ikinci fıkra için ise sistemde yer alan verilerdir. Depolama işlevi gören araçlardaki verilerin bu suçun konusunu oluşturup oluşturmayacağı tartışmalıdır. Bu konuda sadece depolama amacına hizmet eden aygıtlarda yer alan verilerin bu madde kapsamında değerlendirilmemesi gerektiği ve kanunda bu kapsamdaki veriler açısından bir düzenleme eksikliği bulunduğu ifade edilmelidir. Yine sisteme verilen fiziki zararların bu suçu oluşturup oluşturmayacağı noktasında doktrinde farklı görüşler bulunmaktadır. Ancak kanaatimizce fiziksel saldırı yoluyla da bu suçun işlenmesi mümkündür.

TCK m. 244'te yer alan suçların faili ve mağduru herkes olabilir. Failin ve mağdurun tespitinde, eylemin yöneldiği sistemin ya da verinin, ayrı ayrı kullanım, mülkiyet ve tasarruf haklarının sahibi önem arz etmektedir. Tasarruf yetkisinin sahibi ise her somut olayın özelliklerine göre kendi içerisinde belirlenmelidir. Doktrinde tüzel kişilerin mağdurluk sıfatı ise tartışmalıdır. Karşıt görüşler olmakla beraber bu suçlar açısından tüzel kişilerin mağdurluk sıfatının var olduğu görüşü baskındır. Kanaatimizce TCK m. 20/2 gereği, tüzel kişilerin suç faili olması mümkün değildir.

TCK m. 244'te düzenlenen suçlar seçimlik hareketli olarak düzenlenmiştir. Sistemin engellenmesi ve bozulması ilk fıkrada; verileri bozma, yok etme, değiştirme, erişilmez kılma, sisteme veri yerleştirme ve var olan verileri başka bir yere gönderme ikinci fıkrada düzenlenen hareketlerdir. Doktrinde bu suçu serbest hareketli ve neticeli; bağlı hareketli; sırf hareket suçu olmak üzere farklı şekillerde değerlendiren görüşler bulunmaktadır. Ancak maddede düzenlenen eylemler bir netice ifade ettiğinden ve farklı birçok şekilde gerçekleştirilebileceğinden serbest hareketli ve neticeli suçlar olduğu söylenebilir. Yine suçun tehlike suçu mu yoksa zarar suçu mu olduğu da doktrinde tartışmalıdır. Ancak özellikle bir zararın ortaya çıkması madde metninde aranmamıştır. Bu suçlar icraen ve ihmalen işlenebilir. TCK m. 244'te ikinci fıkrada düzenlenen eylemler ile ilk fıkradaki suç gerçekleştirilebildiğinden fıkralar arasındaki temel ayrım maksat yönünden ortaya çıkmaktadır.

Engelleme eyleminde kanunumuzda engellemenin kalıcı ya da geçici olması noktasında bir belirleme yapılmamış olduğundan doktrinde bu konuda farklı görüşler bulunmakla beraber, AKSSS açıklayıcı raporunda engellemenin ciddi ölçüde olmasının aranabileceği belirtilmiştir.

Kanaatimizce engellemenin geçici ya da kalıcı olması engelleme eylemi açısından bir fark oluşturmaz. Sistemin işleyişinin yavaşlatılması halinde de engelleme gerçekleşmiş olacaktır. Doktrinde ayrıca bu suçun birden çok bilişim sistemi veya yazılım kullanılarak gerçekleştirilmesinin nitelikli hal olarak düzenlenmesi gerektiği de düşünülmektedir.

Yok edilen verinin özel cihaz ya da yöntemlerle geri getirilebilmesi durumu doktrinde yok etmenin gerçekleşip gerçekleşmediği noktasında zıt görüşler ortaya koymaktadır. Kanaatimizce verinin özel cihaz ya da yöntemlerle geri getirilebilecek olması halinde de yok etme gerçekleşmiş olur. Verinin kopya olması ya da kopyasının bulunması da önem arz etmez. Verinin geri dönüşüm kutusuna atılması durumunda veri orada kaldığı müddetçe yok etme eylemi gerçekleşmez. Var olan verileri başka yere gönderme eylemi açısından mağdurun verisinin sistemindeki başka bir dosyaya taşınmasının da bu suçu oluşturacağı düşüncesi bulunmaktadır. TCK m. 244/2'nin TCK m. 135, 136 ve 142. maddelerinden ayrılabilmesi için verilerin niteliğinin belirlenmesi özellikle gereklidir.

TCK m. 244/3'te TCK m. 244/1 ve 2'deki suçların bir banka, kredi kurumu, kamu kurum veya kuruluşuna ait sistemler üzerinde işlenmesi hali nitelikli hal olarak düzenlenmiştir. Doktrinde böyle bir düzenlemenin getirilmesi yerinde görülse de kurum sınırlaması yapılması doğru bulunmamakta, top yekûn hizmetin korunmasının sağlanması gerektiği düşünülmektedir. Yine failin kamu, banka ya da kredi kurumu görevlisi olmasının nitelikli hal olarak düzenlemesi gerektiği ifade edilmektedir.

TCK m. 244/4'te yer alan düzenlemenin nitelikli hal mi yoksa ayrı bir suç mu olduğu konusu doktrinde tartışmalı olmakla beraber ilk görüşte belirtildiği üzere düzenleme temel suç tipine bağlılığı devam ettirdiğinden, nitelikli hal olarak değerlendirilmesi gerekmektedir.

TCK m. 244'te düzenlenen suçlar kasten işlenebilen suçlar olup olası kastla da işlenebilir. Taksire ilişkin düzenleme ise bulunmadığından bu suçlar taksirle işlenememektedir. Suça teşebbüs mümkündür. İştirak yönünden ise genel hükümler geçerlidir.

Suçların içtimaı konusunda TCK m. 244 açısından birden fazla durumun gerçekleşebileceğini söylemek mümkündür. TCK m. 244/1-2'deki suçlar zincirleme suç şeklinde işlenebilmektedir. TCK m. 244/1-

2' ile TCK m. 243'te yer alan suçun birlikte işlenmesi halinde farklı görüşler bulunmakla beraber Yargıtay TCK m. 244'ün uygulanması gerektiği kanaatindedir. Kanaatimizce TCK m. 244 açısından sisteme girme zaruri bir eylem değildir. Bu durumda somut olayın özelliklerine göre içtima yapılması gerektiği ifade edilmelidir. TCK m. 245/A ile beraber işlenmesi durumunda gerçek içtima söz konusu olacak, tek eylemle TCK m. 244/2 ile TCK m. 267-271'deki suçlar birlikte işlenirse farklı neviden fikri içtima uygulanacaktır. TCK m. 244/2 ile TCK m. 151'de arasında ise bir görüş fikri içtima yapılması, diğer görüş TCK m. 244'ün uygulanması, başka bir görüş ise failin kastının dikkate alınması gerektiği kanaatindedir. Kanaatimizce failin kastına göre belirleme yapılması gerekmektedir. Failin verilere müdahale ederek sahte belge düzenlemesinde farklı görüşler bulunmakla beraber Yargıtay TCK m. 244/2'nin uygulanması gerektiği kanaatindedir. TCK m. 244/4'ün TCK m. 142/1-e ile TCK m. 158/1-f'de yer alan nitelikli hallerle arasındaki ilişkide eylem hırsızlık veya dolandırıcılık kapsamında ise TCK m. 244/4'ten değil, hırsızlık ya da dolandırıcılıktan hüküm kurulacaktır. Suçun konusu veri ise hırsızlık suçu değil, TCK m. 244/4 oluşacak; hileli davranış gerçek kişiye değil de sisteme karşı yapılmışsa eylem TCK m. 158/1-f değil, TCK m. 244/4 kapsamında değerlendirilecektir.

TCK m. 244'te düzenlenen suçlara yönelik görüş ayrılıklarının temel sebebinin düzenlemenin oldukça genel hatlarla çizilmesi olduğu söylenebilir. İyileştirme önerilerinin dikkate alınması hem suçla etkin mücadeleyi sağlamak hem de kanunilik ilkesi korumak açısından önem arz etmektedir.

YAZAR BEYANI	
Mali Destek/Teşekkür Beyanı:	Bulunmamaktadır.
Yazarların Katkıları	%50-%50
Çıkar Çatışması/Ortak Çıkar Beyanı	Yazarlar tarafından herhangi bir çıkar çatışması veya ortak çıkar beyan edilmemiştir. Birinci yazar Erciyes Üniversitesi Hukuk Fakültesinde öğretim üyesi olarak çalışmaktadır. Birinci yazar dergimiz editör kurulu ve yayın kurulunda görev yapmaktadır.
Etik Kurul Onayı:	Gerekmemektedir.

KAYNAKÇA

Akarslan, Hüseyin. Bilişim Suçları. Ankara: Seçkin Yayınları, 2015.

Akbulut, Berrin. Bilişim Alanında Suçlar. Ankara: Adalet Yayınevi, 2017.

Akbulut, Berrin. "Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme". Selçuk Üniversitesi Hukuk Fakültesi Dergisi. 24/2 (2016): 7-55.

Aköz, Burak Cesur. "Türk Ceza Kanunu Kapsamında Bilişim Suç ve Cezaları İle Örnek Yargısal Kararların Analizi Ve Mevzuat Önerileri". Bilişim Uzmanlığı Tezi, Bilgi Teknolojileri ve İletişim Kurumu, 2018.

Apaydın, Cengiz. Bilişim Sistemine Girme, Engelleme ve Bozma Suçları. Ankara: Seçkin Yayınları, 2023.

Apaydın, Cengiz. Bilişim Suçları ve Bilişim Ceza Hukuku. İstanbul: Acar Matbaacılık, 2017.Avşar, B. Z., &Öngören, G. (2010). Bilişim Hukuku. Türkiye Bankalar Birliği.

Baş, Eylem. Ceza Hukukunda Fail ve Mağdur. Ankara: Seçkin Yayıncılık, 2021.

Bük, Alaattin. Bilişim Alanında Kişisel Verilerin Korunması. Ankara: Seçkin Yayınları, 2018.

Çakıcı, Mert. "Türk Ceza Kanunu M. 243 ve M. 244'te Düzenlenen Bilişim Suçları". Ceza Hukuku Dergisi. 9/24 (2014): 307-349.

Demircan, Tunç. Bilişim Alanında Suçlar. İstanbul: Legal Yayıncılık, 2016.

Demirci, Ömer. Bilişim Suçları ve Soruşturma Yöntemleri. Ankara: Seçkin Yayınları, 2022.

Dülger, Murat Volkan. Bilişim Suçları ve İnternet İletişim Hukuku, Ankara: Seçkin Yayınları, 2022.

Eker, Ö. Umut. ""Türk Ceza Hukuku'nda Bilişim Suçları" Eski TCK Bağlamında Hukukumuzda Yer Alan İlk Düzenlemeler ve 5237 Sayılı Yeni Türk Ceza Kanunu'nun İlgili Hükümlerinin Yorumu". Türkiye Barolar Birliği Dergisi. 19/62 (2006): 101-131.

Erdoğan, Yavuz. "Bilişim Sistemine Girme ve Kalma Suçu", Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, 12/Özel Sayı (2010): 1363-1433.

Erdoğan, Yavuz. "Türk Ceza Kanununda bilişim sistemini engelleme bozma verileri yok etme değiştirme suçu". Doktora tezi, Marmara Üniversitesi, 2011.

Geçmez, İrem. Bilişim Sistemini Engelleme, Bozma Verileri Yok Etme veya Değiştirme Suçları (TCK M. 244). Ankara: Seçkin Yayınları, 2020.

Gerçeker, Hasan. Yorumlu ve Uygulamalı Türk Ceza Kanunu. Ankara: Seçkin Yayıncılık, 2022.

Gökcan, Hasan Tahsin ve Mustafa Artuç. Pratik Türk Ceza Kanunu. Ankara: Adalet Yayınevi, 2023.

Gül, Ahmet. Doğrudan Dolaylı Bilişim Suçları. Ankara: Seçkin Yayınları, 2021.

Gün, Nagihan. "Türk Ceza Hukukunda Bilişim Suçları". Yüksek Lisans Tezi, Çankaya Üniversitesi, 2020.

Kaçmaz Keskin, Gözde. Türk ve Amerikan Hukukunda Tüzel Kişilerin Ceza Sorumluluğu. Ankara: Seçkin Yayıncılık, 2024.

Karagöz, Mehmet Can. "Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu (TCK m. 244)". Yüksek Lisans Tezi, Akdeniz Üniversitesi, 2019.

Katoğlu, Tuğrul. "Ceza Hukukunda Suçun Mağduru Kavramının Sınırları". Atatürk Üniversitesi Hukuk Fakültesi Dergisi. 61/2 (2012): 657-693.

Ketizmen, Muammer. "Türk Ceza Hukuku'nda Bilişim Suçları". Doktora Tezi, Ankara Üniversitesi, 2006.

Koca, Mahmut ve İlhan Üzülmez. Türk Ceza Hukuku Özel Hükümler. Ankara: Adalet Yayınevi, 2024.

Mahmutoğlu, F. S. (2013). Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi. Journal of İstanbul University Law Faculty. 71(1), 855-889.

Mahmutoğlu, Fatih Selami. "Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi", Journal of İstanbul University Law Faculty. 71/1 (2013): 855-889.

Öndin, Hasan Burak. "Türk Hukukunda Doğrudan Bilişim Suçları". Yüksel Lisans Tezi, Anadolu Üniversitesi, 2017.

Özbek, Veli Özer, Koray Doğan ve Pınar Bacaksız. Türk Ceza Hukuku Özel Hükümler. Ankara: Seçkin Yayınları, 2022.

Pallı, Hayati. "Türk Hukukunda ve Mukayeseli Hukukta Bilişim Suçları". Yüksek Lisans Tezi, Erciyes Üniversitesi, 2008.

Tezcan, Durmuş, Mustafa Ruhan Erdem ve Murat Önok. Teorik ve Pratik Ceza Özel Hukuku. Ankara: Seçkin Yayıncılık, 2023.

The Council of Europe. (2001). Council of Europe Convention on Cybercrime. https://www.coe.int/en/web/cybercrime/the-budapest-convention

Türk Dil Kurumu. "Türk Dil Kurumu sözlüğü". Erişim Tarihi 13.01.2023, https://sozluk.gov.tr/

Yılmaz, Sacit. "5237 Sayılı TCK'nın 244. Maddesinde Düzenlenen Bilişim Alanındaki Suçlar". TBB Dergisi, 92 (2011), 62-100.

Yargıtay 2. Ceza Dairesi. K. 2016/10421. (01 Haziran 2016). https://karararama.yargitay.gov.tr/

Yargıtay 8. Ceza Dairesi. K. 2014/ 18506. (14 Temmuz 2014). https://karararama.yargitay.gov.tr/

Yargıtay 11. Ceza Dairesi. K. 2009/11328. (07 Ekim 2009). https://karararama.yargitay.gov.tr/

Yargıtay 11. Ceza Dairesi. K. 2013/4065. (13 Mart 2013). https://karararama.yargitay.gov.tr/

Yargıtay 13. Ceza Dairesi. K. 2017/10403. (10 Ekim 2017) https://karararama.yargitay.gov.tr/.