SİSTEMİ ENGELLEME, BOZMA, VERİLERİ YOK ETME VEYA DEĞİŞTİRME

Doç. Dr. Berrin AKBULUT*

BLOCKING, DISRUPTING THE SYSTEM, DESTROYING OR CHANGING THE DATA

ÖZET

Bilişim alanında yaşanan gelişmelerin sonuçlarından biri de suçluluk alanında yaşananlardır. Klasik suçların yanında yeni suç işlenme şekilleri ortaya çıkmıştır. Bu suçlardan biri de Türk Ceza Kanununun 244. maddesinde düzenlenen sistemi engelleme, bozma, verileri yok etme veya değiştirme suçlarıdır. 244. maddenin ilk fıkrasında bilişim sisteminin işleyişinin engellenmesi veya bozulması suçu, ikinci fıkrasında ise bilişim sistemindeki verilerin bozulması, yok edilmesi, değiştirilmesi, erişilmez kılınması, sisteme veri yerleştirilmesi veya mevcut verilerin başka yere gönderilmesi suçu hükme bağlanmıştır. 3. fıkrada ise suçların nitelikli hali düzenlenmiştir.

Türk Ceza Kanununun 244. maddesinin 1. ve 2. fıkralarında düzenlenen suçlar, tarafı bulunduğumuz Siber Suç Sözleşmesinde de yer verilen suçlardır. Ancak doktrinde bazı yönlerden eleştirilmekte ve

* Selçuk Üniversitesi Hukuk Fakültesi Ceza ve Ceza Muhakemesi Hukuku Anabilim Dalı Öğretim Üyesi.

tartışmalara neden olmaktadır. Aşağıda her bir suç unsurlarıyla incelenirken eleştiriler ve tartışmalara yer verilecek, özellik arz eden hususlar belirtilecektir. Bu yapılırken suçlar ayrı ayrı incelenmeyecek, tekrara yer vermemek için aynı başlık altında, fakat ortak ve farklı hususları kapsayan açıklamalar yapılacaktır.

ANAHTAR KELİMELER: *Bilişim sistemi, veri, suç, nitelikli hal, Siber Suç Sözleşmesi.*

ABSTRACT

One of the consequences of the developments in the field of information is the experiences in the area of criminalness. Apart from classical crimes, new forms of crimes have emerged. One of these crimes is the crime of blocking, disrupting the system, destroying or changing the data, which is regulated in Article 244 of the Turkish Penal Code. In the first paragraph of Article 244, the crime of blocking or disrupting the information system is regulated; in the second paragraph, breaking down, destroying and changing the data, making the data inaccessible in the information system, placing of data into the system or sending of existing data to another are resolved. In the third paragraph of the article qualified version of the crimes is regulated.

Crimes which are regulated in the first and second paragraphs of the Article 244 of the Turkish Penal Code are also regulated in the Cyber Crime Convention. But in doctrine, it is criticized in some ways and causes debates. While examining the elements of crimes in the following, reviews and discussions will be included, issues which give important features will be noted. While doing this, the offenses will not be examined separately, but in order to avoid recurrence, explanations will be made under the same headline by covering common and different aspects.

KEYWORDS: *Information System, Data, Crime, Qualified Version, Cyber Crime Convention*.

GİRİŞ

İnsanlar bilginin işlenmesi, saklanması ve ona erişilmesiyle uzun yıllardan beri uğraşmaktadırlar. Zaman içinde bu konuda kolaylık sağlayacak çalışmalar yapılmıştır. 20. yüzyılın ortalarına gelindiğinde

bilginin işlenmesi ve değerlendirilmesi konusunda büyük bir gelişme olmuş ve bilgisayarlar üretilmeye başlanmıştır. Bilgisayarların üretilmesi ve insanlığın hizmetine sunulması yeni bir tehlike etkeninin varlığını da ortaya çıkarmıştır. Çünkü, bilgisayarlar bazı menfaatlerin ihlâl edilmesinde araç olarak kullanılmaya başlandığı gibi, sistemde veya bilgisayarlarda yer verilen verilere zarar verilmesi sonucunu da doğurmuştur. Başlangıçta bilgisayarla işlenen böyle bir suçluluk türünün olup olmadığı şüpheyle karşılanmışken, zamanla düzenlemeye gidilmesinin zorunlu olduğu anlaşılmıştır. Ceza Hukukunun genellikle maddî konuları korumaya alması, diğer konularla pek meşgul olmaması, ülkeleri bilişim suçları konusunda ayrı düzenleme yapma yoluna yöneltmiştir. Maddî konuları koruyan mevcut düzenlemeler bilişim suçlarına uygulanamamıştır. Örneğin, mala veya malvarlığına zarar verme niteliği taşıyan zarar verme fiilleri, sisteme veya verilere zarar vermeyle ilgili hareketlere uygulanamamıştır. Türkiye de bu ihtiyacı görerek 1991 yılında ilk düzenlemeyi yapmıştır. Türkiye'ye ilk bilgisayar 1960 yılında alınmasına rağmen, ilk düzenleme ancak 1991 yılında 3679 sayılı Kanunla yapılabilmiştir. Bilişim suçları Ceza Kanunumuzun "Bilişim Alanında Suçlar" adını taşıyan on birinci babında 4 madde halinde düzenlenmiş ve bunlardan biri de inceleme konumuz olan sistemi engelleme, bozma, verileri yok etme veya değiştirme suçlarıdır (m. 525/b-1). Bu düzenleme 1 Haziran 2005 tarihine kadar yürürlükte kalabilmiş, bu tarihte yeni bir Ceza Kanunu yürürlüğe girmiş ve inceleme konumuz suçlar da 244. maddenin 1. ve 2. fıkralarında düzenlenmiştir. Ceza Kanunumuzun Topluma Karşı Suçlar başlığını taşıyan üçüncü kısmın Bilişim Alanında Suçlar ismini taşıyan onuncu bölümünde sistemi engelleme, bozma, verileri yok etme veya değiştirme suçları hükme bağlanmıştır. Aşağıda bu suçlar incelenmeye çalışılacaktır. Ancak şu belirtilmelidir ki, getirilen düzenlemede 765 sayılı Kanunda bulunmayan ancak 5237 sayılı Kanunda yer verilen bazı kavramlar yönünden özellikle sorun içermektedir.

I. GENEL OLARAK

Sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu TCK'nın 244. maddesinde düzenlenmiştir. Bu maddeye göre, *"(1) Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır. (2) 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. (3) 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. (4) 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 beşbin güne kadar adlî para cezasına hükmolunur."

Maddede ilki birinci fıkrada, ikincisi 2. fıkrada, üçüncüsü ise 4. fıkrada yer alan üç ayrı suç düzenlenmiştir. Maddenin 3. fıkrasında ise, ilk iki fıkrada düzenlenen suçların nitelikli haline yer verilmiştir.

TCK'nın 244. maddesi 765 sayılı TCK'nın 525/b maddesinin karşılığını oluşturmaktadır. 244. maddenin ilk iki fıkrasındaki suçlar 765 sayılı Kanunda bazı farklarla 525/b maddesinin 1. fıkrasında aynı cezayla cezalandırılan tek suç olarak düzenlenmişti[1]. 5237 sayılı Kanunun 244. maddesinde, 765 sayılı Kanunun m. 525/b-1'de olan "başkasına zarar vermek veya kendisine veya başkasına yarar sağlamak maksadıyla" ibaresine yer verilmemiş ve m. 525/b-1'de olmayan erişilmez kılmak, sisteme veri yerleştirmek, var olan verileri başka bir yere gönderen kişi kavramları metne işlenmiştir. Ayrıca m. 525/b-1'de yer alan siteme zarar verme ifadesine 244. maddede yer verilmemiştir. TCK'nın 244. maddesinin 4. fıkrasında yere alan suç ise, 525/b'nin 2. fıkrasında maddenin 1. fıkrasına yollama yapılmaksızın ve başka bir suç oluşturmaması şartına bağlanmaksızın düzenlenmekteydi.

TCK'nın 244. maddesi, 765 sayılı Kanun döneminde hazırlanan 1997 ve 2003 tarihli Türk Ceza Kanunu Tasarıları (m. 348, m. 347)[2] esas

---

1 Ceza Kanunumuzun 525 b/1 maddesi, "Başkasına zarar vermek veya kendisine veya başkasına yarar sağlamak maksadıyla, bilgileri otomatik işleme tâbi tutmuş bir sistemi veya verileri veya diğer herhangi bir unsuru kısmen veya tamamen tahrip eden veya değiştiren veya silen veya sistemin işlemesine engel olan veya yanlış biçimde işlemesini sağlayan kimseye iki yıldan altı yıla kadar hapis ve beş milyon liradan elli milyon liraya kadar hapis cezası verilir" şeklinde düzenlenmiştir.

2 Tasarının 348. maddesi, "Bir bilişim sisteminin işleyişini engelleyen veya bozan kimseye bir yıldan üç yıla kadar hapis ve yüzmilyon liradan beşyüzmilyon liraya kadar ağır para cezası verilir. Bilişim sistemine hukuka

alınarak düzenlenmiştir. Her iki Tasarıda da bir bilişim sisteminin tahrip edilmesi, maddî unsuru oluşturan bir fiil olarak düzenlememiştir. Sisteme müdahale ile verilere müdahale 765 sayılı TCK'da olduğu gibi aynı suçun seçimlik unsurları olarak düzenlenmemiş, 5237 sayılı TCK gibi ayrı fıkralarda ayrı suçlar olarak hükme bağlanmışlardır. Bilişim sisteminin işleyişinin engellenmesi veya bozulması, 1. fıkrada suç olarak düzenlenmiştir. Ancak suçun karşılığı olan ceza, 5237 sayılı TCK'dan (m. 244/1'den) farklı olarak hem hapis cezası hem de para cezasını gerektiren suç olarak hükme bağlanmıştır. Hapis cezasının üst sınırı da 5237 sayılı Kanundan farklı olarak kaleme alınmıştır. Tasarılarda yer alan 347. ve 348. maddelerin 2. fıkralarında ise, verilere müdahale teşkil eden fiillere yer verilmiştir. Suçun oluşması için bilişim sistemine verileri sokmak veya sistemin içerdiği verileri yok etmek veya değiştirmek gerekmekteydi. 5237 sayılı TCK ise bu unsurlara ek olarak verilerin bozulmasını, erişilmez kılınmasını ve var olan verileri başka bir yere

---

aykırı olarak veriler sokan veya sistemin içerdiği verileri yok eden veya değiştiren kimseye üç yıldan altı yıla kadar hapis ve üçyüzmilyon liradan birmilyar liraya kadar ağır para cezası verilir.

Yukarıdaki fıkralarda belirtilen eylemlerle fail, başkasının zararına ve kendisinin veya başkasının yararına haksız bir menfaat sağlarsa iki yıldan beş yıla kadar hapis ve ikiyüzmilyon liradan birmilyar liraya kadar ağır para cezasına hükmedilir.

Bu suçlara teşebbüs halinde faillere tamamlanmış suçun cezası verili" şeklinde düzenlenmiştir.

Tasarının 347. maddesi, "Bir bilişim sisteminin işleyişini engelleyen veya bozan kimseye bir yıldan üç yıla kadar hapis ve üçmilyar liradan onbeşmilyar liraya kadar ağır para cezası verilir.

Bilişim sistemine hukuka aykırı olarak veriler sokan veya sistemin içerdiği verileri yok eden veya değiştiren kimseye üç yıldan altı yıla kadar hapis ve onmilyar liradan otuzmilyar liraya kadar ağır para cezası verilir.

Yukarıdaki fıkralarda belirtilen eylemlerle fail, başkasının zararına ve kendisinin veya başkasının yararına haksız bir çıkar sağlarsa iki yıldan altı yıla kadar hapis ve beşmilyar liradan yirmimilyar liraya kadar ağır para cezasına hükmedilir.

Bu suçlara teşebbüs halinde faillere tamamlanmış suçun cezası verili" şeklinde düzenlenmiştir.

gönderilmesini aramıştır. Ayrıca Tasarılarda yer verilen para cezaları 5237 sayılı Kanuna alınmamış ve hapis cezaları da farklı olarak belirlenmiştir. Bunun dışında Tasarılarda hukuka aykırılığa işaret eden kavrama da 244. maddenin 2. fıkrasında yer verilmemiştir. Tasarıların 347. ve 348. maddelerinin 3. fıkrasında ise, haksız çıkar sağlama suçu düzenlenmiştir. Bu suçun oluşması için TCK'nın 244. maddesinin 4. fıkrasında olduğu gibi 1. ve 2. fıkradaki fiillerle haksız çıkar sağlanması gerekmektedir. 765 sayılı Kanundan farklı olarak hangi fiillerle haksız çıkar sağlanması gerektiği maddelerde ifade edilmiştir. Ancak 5237 sayılı Kanundan farklı olarak suçun başkasının zararına işlenmesine yer verilmiştir. Suçun cezası 5237 sayılı TCK'da olduğu gibi Tasarılarda da hem hapis cezası hem de para cezası olarak öngörülmüştür. Hapis cezasının miktarı 347. maddede yer verildiği kabul edilmiştir. Para cezası sistemi 5237 sayılı Kanunda farklı kabul edildiği için bu konuda belirleme yapmıyoruz. Tasarılarda olmayan bir belirlemeye 5237 sayılı TCK'nın 244/4. maddesinde yer verilmiştir. Bu belirleme 1. ve 2. fıkrada tanımlanan fiillerin başka suç oluşturmaması gerektiğidir. Tasarılarda yer verilen, ancak 5237 sayılı TCK'ya alınmayan düzenleme ise her üç suça teşebbüsün tamamlanmış suç gibi cezalandırılacağına ilişkin hükümdür.

Türk Ceza Kanununun 244. maddesinde 3 ayrı suç düzenlenmekle beraber, sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu başlığı altında 4. fıkradaki suç belirtilmeyecek, söz konusu suç başka bir inceleme konusu yapılacaktır. Çalışmada 1. ve 2. fıkradaki suç aynı başlık altında bazı konularda tekrara yer vermemek için birlikte belirtilecektir. Dolayısıyla aşağıdaki belirlemeler bilişim sistemi aracılığıyla hukuka aykırı yarar sağlama suçuyla ilgili değildir.

Kanun koyucu bir bilgisayar sisteminin, gerek hukuka uygun veya hukuka aykırı olarak girilerek gerçekleştirilen kullanılmalarında gerek herhangi bir kullanılmanın söz konusu olmadığı durumlarda, sistemde yer alan verilerin veya bunlardan oluşan bilgilerin veya veri işleme olayının herhangi bir hakka veya yetkiye dayanmayan tecavüzlere karşı korunması için bu maddeyi kabul etmiştir. Çünkü kişisel alanda, idarede, ekonomide kullanılan bilgisayarların soyut unsurlarında veya veri işleme akışında meydana gelebilecek bir zarar olağanüstü boyutlara ulaşabilmektedir. Örneğin muhasebe ve ücret hesaplamaları yapılamamakta, büyük miktarda ekonomik kayıplar oluşabilmektedir. Ayrıca bu tür fiillerin işlenmesinin gelinen teknolojik gelişme göz

önünde tutulduğunda ne kadar kolay olduğu anlaşılacaktır. Virüsler, kurtçuklar, truva atları gibi programlarla gerçekleştirilen bu tür fiillere sıklıkla rastlamaktayız. Bu gibi programların gittikçe daha iyi konuma getirilmesi ve dolayısıyla da kötü niyetli bir kullanıcıların elinde çok büyük zararlara yol açılması söz konusu olabilecektir. İnternet aracılığıyla gönderilen virüsler birçok ülkedeki bilgisayarlardaki verilerde veya sistemlerde zararlara yol açmaktadır. Bu tür olayların belirli dönemlerde çok sık gündeme gelmesi nedeniyle, gazeteler haberi e-mail modası başlığıyla okuyuculara duyurmuşlardır. Türk kanun koyucusu da bu tür fiillerin işlenmesinin önlenmesi için önce 765 sayılı Kanuna 525/b-1 maddesini ilâve etmiş, 5237 sayılı Kanunda da 244. maddeyi yürürlüğe koymuştur. Mala zarar verme suçunu düzenleyen hükümler, yalnız mal niteliği taşıyan şeylere verilen zararlara uygulanabildiğinden mal niteliğinde kabul edilmeyen değerlerde oluşan zararlar için ayrıca düzenleme yapılması gereği ortaya çıkmıştır.

TCK'nın 244. maddesinde düzenlenen suçlara, Siber (Sanal Ortamda İşlenen) Suç Sözleşmesinin 4. ve 5. maddelerinde yer verilmiştir. 244. maddenin 2. fıkrasındaki suçun karşılığı 4. maddede verilere müdahale ismiyle, 1. fıkrasındaki suç ise Sözleşmenin 5. maddesinde sisteme müdahale başlığıyla düzenlenmiştir. Sıralamanın bu şekilde düzenlenmesinin nedeni, verilere müdahale etmek suretiyle sistemin işleyişinin engellenmesinin veya bozulmasının da sisteme müdahale çerçevesinde nitelendirilmesidir. Ceza Kanunumuzda ise sistemin işleyişinin engellenmesinin veya bozulmasının verilere müdahale edilmesi fiilleriyle bağlantılı olmasına ilişkin bir belirleme yapılmamış, tam tersine ilk suç belirlemesi sisteme müdahaleyle ilgili olarak gerçekleştirilmiştir. Sistemin işleyişini engelleyen veya bozan her hareket sorumluluk kapsamında kabul edilmiştir. Sözleşmeyle düzenlememiz arasındaki diğer bir farklılık da, sisteme veri yerleştirmek, var olan verileri başka bir yere göndermek fiilleri sözleşmede sisteme müdahalenin kapsamında belirtilirken, 244. maddede verileri yok etme veya değiştirmek kapsamında düzenlenmesidir. Diğer bir farklılıkta Sözleşmede her iki suç açısından da maddelerde yer alan fiillerin haksız gerçekleştirilmesi aranırken TCK'nın 244. maddesinde buna ilişkin bir belirlemeye yer verilmemiştir. Alman Ceza Kanununda da Siber Suç Sözleşmenin sıralaması geçerli olup, önce verilerin değiştirilmesi (m. 303 a), sonra bilgisayar sabotajı (m. 303 b) suçları düzenlenmiştir.

II. KORUNAN HUKUKİ DEĞER

Ceza Kanunumuz 244. maddesinde, bilişim sisteminin işleyişinin engellenmesi veya bozulması (f.1) ile sistemdeki verilerle ilgili bazı fiillere (f. 2) yer verilmiştir.

765 sayılı Türk Ceza Kanununun 525/b-1 maddesinde hem sisteme zarar vermeye yönelik fiillere hem soyut unsurlara yönelik hareketlere hem de sistemin işlemesine engel olan veya yanlış biçimde işlemesini sağlamaya yönelik davranışlara seçimlik olarak tek bir hükümde yer verilmişti. Bu durum m. 525/b-1'in koruduğu değerin ne olduğu konusunda tartışmalara yol açmış ve değişik görüşler ileri sürülmüştür. Bazı yazarlar, malikin veya sistemi kullananın bilgisayarın usulüne uygun olarak çalışmasındaki menfaatinin korunmak istendiğini ifade etmişlerdir. Bu görüşe göre fıkra, hem fizik hem de soyut unsurları korumaktadır[3]. Söz konusu görüşü kabul eden yazarlardan bazıları, sistemin çalışmasına yönelik fıkranın aynı zamanda mülkiyet hakkı ile ekonomik hakları da koruduğunu belirtmişlerdir[4]. Bazı yazarlar, sistemin çalışmasını engelleyecek tarzda fiziksel zarar vermelerin de maddeye girdiğini, bilişim sisteminin tamamen veya kısmen tahrip edilmiş olması şartıyla bilgisayar kasasının kaldırılıp atılması fiilleri de 525/b-1'yi ihlal ettiğini kabul etmektedir. Korunan hukuki değer, bilişim sisteminin ve özelinde de verilerin ve diğer unsurların dokunulmazlığıdır[5]. Bazı yazarlar ise, fıkrada kısmen zarar doğuran, kısmen de sistemdeki bilgilerden yararlanma imkânının ortadan kaldıran fiillere yer verildiği görüşünden hareketle, korunan hukuki değerin kişisel yararlar olduğunu ileri sürmüşlerdir[6]. TCK'nın 525/b-1 maddesinde bilgisayarın hem fizikî unsurlarına, hem de soyut unsurlarına yönelik hareketlere yer verilmesine

---

3 Dönmezer, Sulhi, Kişilere ve Mala Karşı Cürümler, Yeniden Gözden Geçirilmiş ve Yenilenmiş Onbeşinci Bası, İstanbul 1998, s. 528; Yazıcıoğlu, Yılmaz, Bilgisayar Suçları, Kriminolojik, Sosyolojik ve Hukukî Boyutları İle, İstanbul 1997, s. 259, 260.

4 Yazıcıoğlu, s. 260.

5 Karagülmez, Ali, Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri, Ankara 2005, s. 137.

6 Malkoç, İsmail/Güler, Mahmut, Uygulamada Türk Ceza Kanunu, Özel Hükümler (C. 4), Ankara 1997, s. 4747.

rağmen burada amacın bilgisayar ortamına yönelik fiillerin cezalandırılması olduğunu belirten diğer bazı yazarlar ise, korunan hukuki değerin bireyin malvarlığı olduğunu ifade etmişlerdir[7]. Biz ise kanunumuzun 525/b-1 maddesinin hem sistemin fizikî yapısına, hem de sistemde bulunan verilere yönelik fiilleri yaptırım altına almakla beraber, bilgisayarın "hardware" kısmına yönelik fiillere yer verilmesinin amacının, sistemin bütünlüğünü korumak değil, sistemin usulüne uygun olarak çalışmasını sağlamak olduğunu belirtmiştik. Bilgileri otomatik olarak işleme tâbi tutmuş sistem ister kişisel bir bilgisayar olsun, ister büyük kurum ve kuruluşların bilgisayar sistemleri olsun, tasarruf yetkilisinin verilerle meydana getirilmiş bilgilerin herhangi bir engel, arıza olmadan kullanılmasındaki ve sistemin arızasız çalışmasındaki yararın korunduğunu ifade etmiştik[8]. Veriler kişisel nitelikte olabileceği gibi, ekonomik değerde de olabilir. Mülga 765 sayılı TCK'nın 525/b-1

---

7 Ersoy, Yüksel, "Genel Hukukî Koruma Çerçevesinde Bilişim Suçları", Yılmaz Günal'a Armağan, Ankara 1994, C. 49, S. 6-12, s. 176, 177, 166.

8 Bu görüşle ilgili olarak bkz.: Schönke, Adolf/Schröder, Horst, Strafgesetzbuch, Kommentar, 25., neubearbeitete Auflage von Theodor Lenckner/Peter Cramer/Albin Eser/Walter Stree, München 1997, s. 2079, 2081; Dreher, Eduard/Herbert, Tröndle, Strafgesetzbuch und Nebengesetze, Kommentar, 47., neubearbeitete Auflage von Otto Schwarz begründeten Werkes, München 1995, § 303a, kn. 2, § 303 b, kn. 2; Otto, Harro, Grundkurs Strafrecht, Die einzelnen Delikte, 3. Auflage, Berlin/NewYork 1991, s. 185, 186; Möhrenschlager, Manfred, "Das neue Computerstrafrecht", wistra, 1986, Heft 4, s. 141, 142; Sondermann, Markus, Computerkriminalität, Die neuen Tatbestände der Datenveränderung gem. § 303a StGB und der Computersabotage gem. § 303 b StGB, Münster 1989, s. 25, 86; Hilgendorf, Eric, "Grundfälle zum Computerstrafrecht", JuS, 1996, Heft 10, s. 890 ; Hilgendorf, Eric, "Grundfälle zum Computerstrafrecht", JuS, 1996, Heft 12, s. 1082; Schulze Heiming, Ingeborg, Der strafrechtliche Schutz der Computerdaten gegen die Angriffsformen der Spionage, Sabotage und des Zeitdiebstahls, New York 1995, s. 165, 166, 196; Lackner, Karl/Kühl, Kristian, Strafgesetzbuch, 21. Aufl., München 1995, § 303 a, kn. 1, § 303 b, kn. 1; Gerhards, Thomas, Computerkriminalität und Sachbeschädigung, Mannheim 1993, s. 25; Wessels, Johannes, Strafrecht, Besonderer Teil/2, Straftaten gegen Vermögenswerte, 20. , neubearbeitete Auflage, Heidelberg, 1997, s. 13, 14.

maddesiyle veri nakil ağında veya bilgisayarda bulunan verilerin, veri tabanlarının ve veri bankalarında bulunan bilgilerin yetkili olmayan kişiler tarafından değiştirilmesi, silinmesi önlendiği gibi, sistemin işlemesinin kesintiye uğratılmasıyla oluşacak zararlar da engellenmektedir. Burada korunmak istenen şey, bazı yazarların belirttiği gibi sistemin fizikî varlığı değildir. Dolayısıyla, TCK'nın 525/b-1 maddesinin verilere zarar vermeyen veya veri işlemin yapılmasını engellemeyen fiilleri kapsamadığını dile getirmiştik. İçinde verilerin bulunmadığı bilgisayarların kırılması durumunda uygulanacak olan hükmün Türk Ceza Kanununun mala zarar vermeye ilişkin düzenlemesi olduğunu belirtmiştik[9]. Fiilin konuluş amacı, söz konusu fıkranın (525/b-1) gerekçesinde "madde birinci fıkrasında bir bakıma bilgileri otomatik işleme tâbi tutmuş sistemlere karşı işlenen suçları cezalandırmakta ve sistemlere yöneltilen ızrar fiillerini böylece ve ayrıca cezalandırmaktadır" şeklinde ifade edilmiştir[10].

5237 sayılı Türk Ceza Kanunu ise, 244. maddede sistemin işleyişini engelleyen veya bozan fiiller ile verilere müdahale niteliğinde fiilleri ayrı suçlar olarak düzenlemiş ve sisteme zarar vermeye yönelik ifadeye yer vermemiştir. Ancak korunan hukuki değer konusundaki farklı belirlemeler sona ermemiştir. Bazı yazarlara göre, maddede 2 temel hukuki değer korunmaktadır. Birincisi bilişim sisteminin ve verilerin güvenliğidir. İkincisi ise, mülkiyet hakkıdır. Zira TCK m. 244'de yer alan fiiller sahibinin bilişim sistemi ve veriler üzerindeki tasarruf yetkisine açık bir tecavüz niteliği taşımaktadır[11]. Bazı yazarlara göre, burada sistemlere yöneltilen ızrar fiillerinin özel bir suç haline getirilmesi söz konusu olup, hem bilişim sisteminin hem de bu sistem içerisinde yer alan veriler veya diğer unsurların zarar görmemesi hedeflenmektedir[12]. Bazı yazarlara göre ise, mala zarar verme suçunun özel görünüş biçimini

---

9 Akbulut, Berrin, Türk Ceza Hukukunda Bilişim Suçları, Yayınlanmamış Doktora Tezi, Konya 2000, s. 130.

10 Türk Ceza Kanunu Öntasarısı Gerekçesi, Ankara 1989, s. 392.

11 Özbek, Veli Özer/Doğan, Koray/Bacaksız, Pınar/Tepe, İlker, Türk Ceza Hukuku, Özel Hükümler, Genişletilmiş ve Güncellenmiş 10. Baskı, Ankara 2016, s. 945.

12 Karagülmez, s. 187.

oluşturan bu suçla mala zarar verme suçundaki mülkiyetin korunduğunu ifade etmektedirler[13]. TCK'nın 1 ve 2. fıkraları için ayrı ayrı belirleme yapan yazarlar ise, 1. fıkrada, bilgisayar sabotajı niteliğindeki fiiller önlenmekte ve bilişim sistemleri işletmecileri ile kullanıcılarının bu sistemleri uygun bir biçimde işletme haklarının korunduğunu, 2. fıkrada ise bilgisayar verilerini ve bilgisayar programlarını kasıtlı zarar verme girişimlerine karşı koruma altına alındığını belirtmektedirler. Ayrıca verilerin başka yere gönderilmesiyle özel hayatın gizliliğinin, sistemin işleyişi engellendiğinde veya bozulduğunda ise haberleşme özgürlüğü ihlal edilmektedir[14]. Korunan hukuki değerin karma nitelik gösterdiğini belirten yazarlar ise, veriler üzerinde tasarruf yetkisi olan kişilerin, verilerle oluşturulan değerlere herhangi bir arıza, engel ya da gecikme olmaksızın ulaşması ve kullanmasındaki çıkarı olduğunu ifade etmektedirler[15]. Diğer bazı yazarlar ise, 244. maddede düzenlenen suçlar aynı zamanda bireyin malvarlığı değerini de ihlal etmekle beraber, suçların düzenleme yeri göz önüne alındığında bireyin malvarlığından ziyade bilişim sistemlerinin doğru ve işlevine uygun bir şekilde işlemesindeki yararın korunduğunu belirtmektedirler[16]. Kanaatimizce 244. maddede iki ayrı suç düzenlendiğinden ayrı ayrı belirleme yapılmalıdır. Birinci fıkrada tüm bilişim sistemleri sahipleri, işletmecileri ile kullanıcılarının sistemin arızasız çalışmasındaki yararı korunmaktadır. Kanun koyucu sistemin işleyişinin engellenmesi veya bozulması ifadeleriyle herhangi bir problem olmadan sistemin çalışmasındaki yararı korumak istemiştir. İkinci fıkrada ise, veriler üzerinde tasarruf yetkisi olan kişilerin verilerin bozulmadan, engel çıkartılmadan, verilere müdahale olmadan kullanmasındaki yararı korunmaktadır. Biz belirlememizi tüm fiilleri göz önüne alarak yapıyorsak da, 2. fıkrada

---

13 Tezcan, Durmuş/Erdem, Mustafa Ruhan/Önok, Murat, Teorik ve Pratik Ceza Özel Hukuku, Güncellenmiş 13. Baskı, Ankara 2016, s. 954.

14 Artuk, Mehmet Emin/Gökcen, Ahmet/Yenidünya, A. Caner, Ceza Hukuku, Özel Hükümler, Yenilenmiş Gözden Geçirilmiş 15. Bası, Ankara 2015, s. 880, 886

15 Meran, Necati, Yeni Türk Ceza Kanununda Sahtecilik-Malvarlığı Bilişim Suçları ile Ekonomi ve Ticaret Alanında Suçlar, Ankara 2005, s. 370

16 Koca, Mahmut/Üzülmez, İlhan, Türk Ceza Hukuku, Özel Hükümler, Gözden Geçirilmiş ve Genişletilmiş 3. Baskı, Ankara 2016, s. 825.

sisteme veri yerleştirme veya var olan verileri başka bir yere gönderme hareketlerinin bu fıkrada düzenlenmesi doğru olmamıştır. Zira sisteme veri yerleştirme verilere müdahale edilmeden de, verilere zarar vermeden de (bozmadan, yok etmeden, değiştirmeden, erişilmez kılmadan da) yapılabilir, verilerin kullanılmasını da engellemeyebilir. 2. fıkrada yer alan ilk dört belirleme ise, verilerin kullanılmasına müdahale teşkil eden, verilere zarar verme niteliğe sahiptir. Eğer sisteme veri yerleştirmenin bu nitelikte olduğu düşünülerek düzenlemede yer alması söz konusuysa, gereksiz yere kullanılma söz konusudur. Zira sisteme veri yerleştirme, verileri değiştirme sonucunu doğuruyorsa ya da diğer belirlemeler kapsamına giriyorsa ayrıca sisteme veri yerleştirilmesi diye bir kavrama yer verilmemesi gerekmektedir. Bu nitelikte olmayan sisteme veri girilmesi kastediliyorsa da düzenleme yeri burası değildir. Çünkü sistemde var olan veriler üzerinde tasarruf etmeyi engelleyen bir yönü bulunmamaktadır. Ancak TCK'nın 244. maddesi açısından sisteme veri yerleştirmenin, sistemin işleyişinin engellenmesiyle veya 4. fıkradaki haksız çıkar sağlama suçuyla ilgisi olabilir. Dolayısıyla verilerin herhangi müdahale olmadan kullanılmasındaki yararı etkilemeyen, bu değeri koruyan diğer fiillerle herhangi bir ilgisi bulunmayan sisteme veri yerleştirmenin 2. fıkrada düzenlenmesi amaçla uygun olmayan bir belirleme niteliği taşımaktadır. Verileri başka yere göndermek de veriler yok edilmeksizin, bozulmaksızın veya değiştirmeksizin yapılabilir. Verilerin kullanılmasına engel olmaksızın da verilerin başka yere gönderilmesi söz konusu olabilir. Eğer bu nitelikte ise zaten ayrıca düzenlemesi gerekmiyor, mevcut fiiller amacı karşılıyor[17]. Bunlar olmadan gerçekleştiriliyorsa o zamanda düzenlemenin 2. fıkrayla ilgisi bulunmamaktadır. Düzenlemenin başka fıkrada veya başka bölüm ya da bölümlerde (kişisel veri, özel hayat, sır vb. niteliğinde olmasına göre) yapılması ya da değişikliğe gidilmesi uygun olurdu. Eğer sistemde var olan verilerin gönderilmesi sistemin işleyişini engelliyorsa veya bozuyorsa o zaman birinci fıkra çerçevesinde değerlendirmek gerekir. Şayet sisteme veri yerleştirme veya verileri başka yere gönderme fiilleri 4. fıkrayla bağlantılı olarak ifade edilmişse bunun yerinin ikici fıkra olmaması, 4. fıkrada hükme bağlanması gerekirdi. Mülkiyetin korunduğu

[17] Düzenlemeye yönelik benzer eleştiriler için bkz.: Özbek/Doğan/Bacaksız/Tepe, s. 953.

görüşüne ise katılmamaktayız. Zira hükümler yalnızca verilerin malikinin yaralarını korumamaktadır. Malik olmasa bile veriler üzerinde tasarruf yetkisi varsa bu kişilerin yararları da korunmaktadır. Dolayısıyla mülkiyetle bağlantılı değerlendirme yapılmasını benimsememekteyiz. Özel hayat veya haberleşmenin korunduğunu da düzenleme yeri itibariyle düşünmemekteyiz.

III. SUÇUN UNSURLARI

A. Maddi unsur

1. Fail

Suçun faili herhangi bir kişi olabilir. Zira düzenlemelerde faille ilgili herhangi bir özelleştirmeye gidilmemiştir. Başkalarının haklarını ihlâl etmediği sürece failin kendi sisteminin işleyişini engellemesi veya bozması veya verilerine müdahale etmesi suç niteliğinde değildir. Maddede buna ilişkin belirleme yoksa da düzenleme amacından bu anlaşılmaktadır.

Türk Ceza Kanununun 244. maddesinde düzenlenen verilere veya sisteme müdahale niteliğindeki fiilleri gerçekleştiren ve fail olan kişinin tespiti için mülkiyet, kullanım veya tasarruf yetkisinin göz önünde bulundurulması gerekir. Örneğin TCK'nın 244. maddenin 2. fıkrasındaki suçun faili, veriler üzerinde tasarruf yetkisine sahip olmayan kişidir. Sistemin işleyişinin engellenmesi veya bozulması fiili açısından ise suçun faili sistemin sahibi veya kullananın dışındaki kişi veya tasarruf yetkilisi dışında bir kişi olabilir. Dolayısıyla, TCK'nın 244. maddesinde yer alan suçların işlenip işlenmediğinin tespitinde malik veya kullananın veya tasarruf yetkilisinin kim olduğu tespit edilmelidir. Örneğin bir sistemin sahibi olan kişi, sistemi kullanma hakkına sahip bir başkasının verilerine zarar verirse, TCK'nın 244. maddesinin 2. fıkrasındaki suçu işlemiş olur.

Verilere veya sistemin işleyişine zarar vermek suçunun işlenip işlenmediğinin tespitinde ayrıca, bilgisayarın kullanım hakkıyla ilgili değerlendirme yapılmalıdır. Bazen kişi veri taşıyıcısının sahibi olmakla beraber verilerin kullanımını üçüncü bir kişiye bırakabilmektedir. Örneğin programla birlikte bilgisayarın kullanılması için kiralanması söz konusu olabilmektedir. Eğer kullanan kişi bilgisayar malikinin sistem programına kasten bir zarar verirse, hareketi 244/2. madde kapsamında cezalandırılan bir fiil niteliği taşır. Uygulama programları açısından da 244. maddenin gerçekleşmesi söz konusu olabilir. Örneğin uygulama

programı sahibi, bunun kullanım hakkını başka birine bıraktıktan sonra, söz konusu programa zarar verirse fiili TCK m. 244/2 kapsamındadır[18]. Veri taşıyıcısının mülkiyeti ile kullanım hakkının birbirinden ayrıldığı durumlarda tasarruf yetkisi ilgililerin arasındaki hukuki ilişkiye göre belirlenmelidir. Sözleşmeye göre kullanım yetkilisi, devredilen verilerde ayni kullanım yetkililerinin yanına veya hatta yerine geçmişse, yani veriler üzerinde tasarruf yetkisine sahip olmuşsa verilere müdahale etmesi suç oluşturmaz. Buna karşılık veri taşıyıcısının sahibinin bir başkasının verilerdeki tasarruf yetkisini ihlal etmesi ve fail olabilmesi mümkündür[19]. Tasarruf yetkisi verilmemişse yalnızca verileri sisteme girme yetkisi verilmişse, kullanan kişinin verilere zarar vermesi TCK'nın 244. maddesinin 2. fıkrası kapsamına girecektir. Yani sipariş üzerine başkalarının verilerini işlemekle yükümlü olan kişiler de suçun faili olabilir. Bu kişiler kendisine verilen verilere zarar verirlerse, veriler üzerinde her tür yetkiye sahip olmadıklarından, onları belirli şartlar dahilinde kullanmakla yükümlü bulunduklarından fiilleri suç olarak kabul edilecektir[20]. Ancak bu tür fiillerde sipariş verenin verilerin bir kopyasını kendisinde alıkoyduğu görüşünden hareketle, sipariş alanın verilere zarar vermesinin suç oluşturmayacağı da belirtilmektedir[21]. Yetkisiz olarak başkasının veri taşıyıcısına kaydedilen verilere, veri taşıyıcısının hukuka uygun sahibinin zarar vermesi TCK'nın 244. maddesinin 2. fıkrası kapsamına girmemektedir. Örneğin bir hırsız tarafından çalınan veri taşıyıcısına (dizüstü bilgisayara) kaydedilen

---

18 Dreher/Tröndle, § 303 b, kn. 8.

19 Bkz.: Schönke, Adolf/Schröder, Horst/Lenckner, Theodor/Cramer, Peter/Stree, Walter, Strafgesetzbuch, Kommentar, 28., neubearbeitete Auflage von Eser, Albin/Heine, Günter/Perron, Walter/Sternberg Lieben, Detlev/Eisele, Jörg/Bosch, Nikolaus/Hecker, Bernd/Kinzig, Jörg/ Schittenhelm, Ulrike, München 2010, Stree/Hecker-Schönke/Schröder, § 303 a, kn. 3.

20 Rudolphi, Hans Joachim/Horn, Eckhard /Samson, Erich, Systematischer Kommentar, Strafgesetzbuch, Besonderer Teil (Band 2), 4. Auflage, Neuwied/ Kriftel 1991,Samson, SK, § 303 a, s. 4, 5.

21 Hilgendorf, 1996, Heft 10, s. 893.

verilerin veri taşıyıcısının sahibi tarafından silinmesi bu niteliktedir[22]. Yine başka birinin bilgisayarına yetkisiz olarak kurulan virüs cookie, truva atı gibi dosyaların silinmesi TCK'nın 244. maddesinin 2. fıkrası kapsamına girmez. Bunların dışında başka birinin veri taşıyıcısına yetkisiz olarak kopyalanan veriler üzerinde de verilerin sahibinin tasarruf yetkisi devam etmez. Dolayısıyla bu verilerin veri taşıyıcısı sahibi tarafından silinmesi durumunda TCK m. 244/2 oluşmaz[23].

2. Mağdur

Suçun mağduru verilere müdahale suçu açısından veriler üzerinde tasarruf yetkisine sahip olan kişi veya kişilerdir. Tasarruf yetkisine sahip olmayan verilerin ilgili olduğu kişi ise, suçun mağduru değildir[24]. Suçtan zarar gören olabilir. Sistemi engelleme veya bozma suçu açısından ise mağdur, sistemin kullanıcısı veya işleticisi veya sahibi olabilir. Mağdur ancak gerçek kişi olabileceğinden tüzel kişiler suçtan zarar gören olabilir. Dolayısıyla kamu kurum ve kuruluşlarının bilişim sistemlerine karşı fiillerin işlenmesi halinde toplumu oluşturan herkes suçun mağdurudur. Kısaca verilerin zararsızlık hakkı veya sistemin herhangi bir kesintiye uğramadan çalışmasındaki arızasızlık hakkı kime ait ise suçun mağduru da o kişidir[25].

Veriler üzerinde tasarruf yetkisinin kime ait olduğu doktrinde tartışmalıdır. Veriler veya kanunda belirtilen diğer soyut unsurlar medeni hukuk anlamında bir şey olmadıkları için mülkiyetle ilgili kurallar ceza hukukuna kolayca uygulanamamakta, dolayısıyla da veriler üzerinde tasarruf yetkisine sahip kişi mülkiyet ilişkisiyle belirlenememektedir. Mülkiyet ilişkisiyle belirlenemeyen verilerin yetkilisinin somut olayda

---

22 Samson, SK, § 303 a, s. 4, 5; Stree/Hecker-Schönke/Schröder, § 303 a, kn. 3.

23 Stree/Hecker-Schönke/Schröder, § 303 a, kn. 3.

24 Bkz.: Tröndle, Herbert/Fischer, Thomas, Strafgesetzbuch und Nebengesetze, 53. Auflage, München 2006, § 303 a, kn. 4; Stree/Hecker-Schönke/Schröder, § 303 a, kn. 3. Verilerin ilgili olduğu kişnin de suçtan zarar gören durumunda olabileceğine ilişkin olarak bkz.: Lackner, Karl/Kühl, Kristian, Strafgesetzbuch, 28. Aufl., München 2014, § 303 a, kn. 4; Möhrenschlager, s. 141.

25 Bkz.: Stree/Hecker-Schönke/Schröder, § 303 a, kn. 1

tespit edilmesi her zaman kolay olmadığından, bu konuda değişik kriterler ileri sürülmüştür[26]:

(1) Verilerin kazanılması. Bu görüşe göre veriler üzerinde tasarruf yetkisine sahip kişi, verileri hukuka uygun olarak iktisap eden kişidir. Kim hukuka uygun olarak verileri iktisap ederse, başka bir şey kararlaştırılmadığı sürece sınırsız tasarruf yetkisine sahiptir.

(2) Verilerin içeriğiyle ilgili olmak. Bu görüşü savunanlara göre verilerin hakkında bir şeyler söylediği kişi, yani verilerin içeriğinin ilgilisi tasarruf yetkisine sahiptir.

(3) Veri taşıyıcısındaki mülkiyet. Veri taşıyıcısının mülkiyeti kime aitse, verilerin tasarruf yetkisi de o kişiye aittir. Örneğin bir disket veya bilgisayar kime aitse içindeki veriler de onun tasarrufundadır.

(4) Verilerin fikrî hak sahibi. Veriler üzerinde tasarruf yetkisine sahip kişinin verilerin üreticisine göre tespit edilmesi gerektiğini belirten görüştür. Bu görüşe göre verilerin kime ait bulunduğu veya kiminle ilgili olduğuna bakılmaksızın, verilerle meydana getirilmiş bilginin üreticisi hangi kişiyse, tasarruf yetkisine de o kişi sahiptir.

(5) Verilerin kaydedilmesi. Bu görüş verilerin yüklenmesini (kaydedilmesine) veya nakledilmesini doğrudan gerçekleştiren kişinin, verilerin sahibi olduğunu ifade edenlerin savunduğu fikirdir. Bunlardan hiçbirisi tek başına veriler üzerinde tasarruf yetkisine sahip kişinin belirlenmesinde yeterli değildir. Birinci kriter ilk yetki sahibinin açıklanmasında, ikinci kriter verileri kaydeden ile ilgili olan kişinin farklı olduğu durumlarda, üçüncü kriter veri taşıyıcısının mülkiyetinin birine, verilerin başka birine ait olmasında, dördüncü kriter ceza kanununun fikrî hakları koruma kanunu bulunmamasında, son kriter ise verilerin kazanılması konusunda yetersiz kalmaktadır. Dolayısıyla yalnızca belirli kritere bağlı olarak belirleme yapılmamakta, diğer ölçütler de göz önünde tutulmaktadır[27].

---

26 Ayrıntılı bilgi için bkz.: Hilgendorf, 1996, Heft 10, s. 892, 893.

27 Bkz.: Stree/Hecker-Schönke/Schröder, § 303 a, kn. 3; Lackner/Kühl, § 202 a, kn. 1; Hilgendorf, Eric, "Grundfälle zum Computersstrafrecht", JuS, 1997, Heft 4, s. 324.

Tasarruf yetkisi noktasında malik benzeri (eigentümerähnlicher) veri tasarruf yetkisi belirlemesi yapılmaktadır[28]. Malik benzeri hak olarak veri tasarruf yetkisi karakteri, asıl veri tasarruf yetkisinin eşya hukukuyla ilişkili bilişim sistemiyle (veri taşıyıcısıyla) bağlantılı olarak belirlenmesini desteklemektedir. Bu nedenle tasarruf yetkisi bilişim sisteminin sahibine veya hukuka uygun zilyedine aittir. Bir kişi hem bilişim sisteminin maliki olabilir hem de veriler üzerinde tasarruf yetkisi bulunabilir. Ya da bilişim sisteminin maliki olmamakla beraber (mülkiyet başkasına ait olabilir), veriler üzerinde tasarruf yetkisine sahip olabilir. Örneğin birinden kiraladığı bilgisayara verilerini kaydettiğinde, bilgisayarın sahibi olmamakla beraber veriler üzerinde tasarruf yetkisine sahiptir. Bu verilere bir başkası tarafından zarar verildiğinde mağdur verileri kaydeden ve üzerinde tasarruf yetkisine sahip olan kişidir. Keza veri taşıyıcısının maliki başkası tarafından hukuka uygun olarak kaydedilen verilere zarar verirse 244. maddedeki/2. fıkradaki suçu işlemiş olur. Ancak daha önce de söylendiği gibi kendi veri taşıyıcısına bir başkası tarafından yetkisiz olarak kaydedilen verileri sildiğinde verileri kaydeden kişi tasarruf yetkisine sahip olmadığından suçun oluşması kabul edilmemektedir. Doktrinde tasarruf yetkilisinin kural olarak verileri kaydetme işini ilk olarak yapan kimse olduğu da belirtilmektedir[29]. E-mail gönderiminde gönderenin tasarruf yetkisi, mailin alıcının servis sağlayıcısının server'ına ulaştığı ana kadardır. Bu andan itibaren artık tasarruf yetkisi alıcıya aittir. Alıcının veriler üzerinde değişiklik yapması suç oluşturmayacaktır. Bir başkasının değişiklik yapması durumunda alıcı suçun mağduru olacaktır. Telefon kartı alan bir kişi, karta kaydedilen veriler üzerinde tasarruf yetkisine sahip olduğundan kart üzerinde teknik manipülasyon yaptığında 244. maddenin 2. fıkrası anlamında cezalandırılan bir fiil söz konusu değildir. Aynı şey sim kilidi gibi program kilidiyle donatılmış cep telefonu alıcısı için de geçerlidir. Burada veri taşıyıcısının mülkiyetinin değişimiyle işletim yazılımındaki tasarruf yetkisi de ona geçtiğinden verileri sildiğinde ve

---

28 Stree/Hecker-Schönke/Schröder, § 303 a, kn. 3; Hilgendorf, 1996, Heft 10, s. 892. Ayrıca Bkz.: Lenckner, Theodor/Winkelbauer , Wolfgang, "Computerkriminalität - Möglichkeiten und Grenzen des 2. WiKG (III)", CR, 1986, Heft 12, s. 829.

29 Hilgendorf, 1997, Heft 4, s. 326.

böylece sim kilidini işlevsiz hale getirdiğinde m. 244/2' yi ihlal etmiş olmaz[30]. Buna karşılık banka müşterisi ona banka tarafından devredilen karttaki veriler üzerinde tasarruf yetkisine sahip değildir[31].

3. Konu

Suçun konusu, TCK'nın 244. maddesinin 1. fıkrasındaki sistemi engelleme, bozma suçu açısından bilişim sisteminin işleyişi[32], 2. fıkrasındaki verileri yok etme, değiştirme suçu bakımından ise bilişim sistemindeki veriler (bozma, yok etme, değiştirme, erişilmez kılma ve verilerin başka yere gönderilmesi açısından) veya bilişim sistemine yerleştirilen veriler (sisteme veri yerleştirmek açısından) olarak ifade etmiştir.

Bilişim, insanların teknik, ekonomik ve toplumsal alanlardaki iletişimde kullandığı ve bilimin temeli olan bilginin elektronik araçlarla özellikle bilgisayarlar aracılığıyla işlenip, ses, görüntü ve veri taşıyan iletişim hatları aracılığıyla aktarılması bilimi olarak tanımlanmaktadır[33]. Tanımdan anlaşılacağı üzere bilişim, hem verilerin işlenmesini, yani veri işlemi hem de bilgi işlemin sonucunun aktarılmasını, yani veri iletişimini ifade eden bir kavramdır. Verilerin işlenmesi ve aktarılmasında kullanılan bileşenlerin, teknolojilerin bütününe ise bilişim sistemi adı verilmektedir. Yazılım, donanım, bilgisayar ağları, iletişim ekipmanları gibi araçlar bilişim sistemi kapsamı içine girmektedir. Görüldüğü gibi bilişim, birçok yapının bir araya gelmesinden oluşmaktadır. Bilgisayar bu yapılardan biridir. Bilişim, bilgisayarı da içine alan daha üst bir kavramdır. WAP uyumlu cep telefonları, üzerindeki WEB paneli sayesinde ağa bağlanıp bilgi aktarımı yapabilen elektronik ev aletleri, veri iletişimini sağlayan

---

30 Ancak bu konuda farklı görüş de ifade edilmektedir. Bunun için bkz.: Stree/Hecker-Schönke/Schröder, § 303 a, kn. 3.

31 Stree/Hecker-Schönke/Schröder, § 303 a, kn. 3.

32 Koca/Üzülmez, s. 826.

33 Bkz.: Kurtaran, Özlem Meltem/Çubukçu, Faruk, Ansiklopedik Bilgi İşlem Terimleri Sözlüğü, İstanbul 1991, s. 35; Gürsel, Mayda/Gürsel, İhsan, Büyük Bilgisayar Terimleri Sözlüğü, Ankara 1991, s. 158; Yarmalı, E. Sabri, Bilgisayar Terimleri Sözlüğü, İstanbul, (Birsen yayınevi), 1995, s. 143.

somut ve soyut ağlar bilişim sistemi içine girmektedir[34]. Kanunumuzda geniş bir kavramın ve yaşanacak gelişmeleri karşılayacak belirlemenin seçilmesi yerinde tercih olmuştur[35].

Bilişim sisteminin neyi ifade etiği mevzuatımızda Ceza Muhakemesinde Ses ve Görüntü Bilişim Sisteminin Kullanılması Hakkında Yönetmelikte (m. 3/1-b) tanımlanmıştır. Buna göre, bilgisayar, çevre birimleri, iletişim altyapısı ve programlardan oluşan veri işleme, saklama ve iletmeye yönelik sistem, bilişim sistemini ifade etmektedir. Görüldüğü gibi bilişim sistemi, bilgisayar ve ona bağlantılı sistemleri ifade etmek için kullanılmıştır. Bilişim sistemi ayrıca 243. maddenin gerekçesinde de belirtilmiştir. Buna göre bilişim sisteminden maksat, verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tutma olanağı veren manyetik sistemlerdir. Mülga 765 sayılı Kanundaki düzenlemelerde tercih edilen otomatik işleme tabi tutma kavramına TCK'nın 243. maddenin gerekçesinde yer verilmiştir. 765 sayılı Kanunun gerekçesinde ise bilgileri otomatik işleme tâbi tutmuş kavramının bilgisayarları karşıladığı ifade edilmiştir. 765 sayılı TCK döneminde bilgisayarı karşılamak için düzenlemelerde yer verilen bilgileri otomatik işleme tabi tutmuş sistem ifadesi değişik nedenlerle eleştirilmiştir[36]. Kavram bilgisayarları karşılamakta tamamen yanlış bir ifade olmamakla beraber, bilgisayarları anlatmak bakımından yetersiz bir ifade olduğu görülmektedir. Çünkü birçok araçta bilgileri depo etme, bunları işleyebilme ve anlamlı sonuçlar üretme özelliği görebiliriz (hesap makineleri gibi). Ancak bunları bilgisayar olarak nitelendiremeyeceğimiz gibi, bilişim suçlarının işlenmesine imkân veren başka bir sistem özelliğine sahip olduğunu da söyleyemeyiz. Zira bunlar hafızalarında bulunan sabit programlarla belirli bir amaç doğrultusunda kullanılabilmeye uygun, bilgileri aktarma özelliğine sahip bulunmayan cihazlardır. Ayrıca bilgisayarların yalnızca manyetik özelliği bulunmamakta, elektronik, optik gibi nitelikleri de söz konusudur. Dolayısıyla bilişim suçlarının işlendiği bilgisayarları ifade etmeyen bu

---

34 Yenidünya, A. Caner/Değirmenci, Olgun, Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları, İstanbul 2003, s. 31.

35 Bkz.: Akbulut, s. 86.

36 Bu eleştiriler için bkz.: Akbulut, s. 84, 85.

kavramın daha uygun başka bir kavramla değiştirilmesinin uygun olduğunu belirtmiştik[37]. Bu anlamda kanunumuzun bilişim sistemi tercihinin yerinde olduğunu belirtmek istiyoruz. Siber Suç Sözleşmesi de bilişim sistemini değil, bilgisayar sistemi ifadesini kullanmış ve "bir veya birden fazlası, bir program uyarınca otomatik veri işleyebilen herhangi bir cihaz veya birbirleriyle bağlantılı veya ilgili bir grup cihazı ifade eder" şeklinde tanımlamıştır.

Veri işlemin esasını oluşturan veri (İng. data, Alm. Daten)[38], sistem içindeki bütün soyut unsurları ifade etmektedir (TCK m. 243 gerekçesi). Programlar da veri kavramı içindedir. Sisteme girilen, sistemde işlenen ve saklanan her tür değeri ifade etmektedir[39]. Bu kavramın kapsamına rakamlar, harfler dahil olduğu gibi, diğer birtakım özel simgeler de (virgül, nokta, noktalı virgül, tire, tırnak işareti gibi) dahildir. Söz konusu bu değerler, işlenecek konu için gerekli olan bilgileri oluştururlar ve değişik nesneler ve olaylar hakkında fikir verirler.

Doktrinde suçun konusunu oluşturan verilerin mutlaka bilişim sisteminde yer alan veriler olması gerektiği belirtilmektedir. Bu nedenle de disket, CD, flash bellek gibi yalnızca veri saklama işlevine sahip olan cihazlardaki verilere müdahale edilmesinin bu suçu oluşturmayacağı ifade edilmektedir. Bu cihazlara verilere ulaşılamaması amacıyla zarar verilmesinin veya fiziki olarak kullanılmasının engellenmesinin 244. maddedeki suçu oluşturmayacağı, mala zarar verme suçunu oluşturacağı ileri sürülmektedir[40]. Ancak bu görüşe katılmadığımızı belirtmek

---

37 Akbulut, s. 84, 85. Aynı yönde Yazıcıoğlu, s. 215.

38 Data ve daten kelimeleri hem tekil hem de çoğul anlamında kullanılmaktadır. Örneğin Almanca Daten kelimesi, Datum kelimesinin çoğulunu ifade etmektedir. Ancak bu ayrıma yazım esnasında pek riayet edildiği söylenemez.

39 Veri kavramının bilgi kavramıyla eşanlamlı olmayıp, her iki kavram farklı anlamlara gelmektedir. Nitekim bazı yazarlar da bunu ifade etmektedirler: Güder, Gazi, Bilgi İşlem Terimleri Sözlüğü, İstanbul 1986, s. 109; Kurtaran/Çubukçu, s. 177; Aydın, Emin D., Bilişim Suçları ve Hukukuna Giriş, Ankara 1992, s. 3; Babür, Zafer, Bilgisayarla İletişim, İstanbul 1995, s. 1. Buna göre veri işlenmemiş bilgiyi, bilgi ise verilerin veri işlem yardımıyla işlenerek anlamlı hale getirilmesini ifade etmektedir.

40 Koca/Üzülmez, s. 826, 827.

istiyoruz. Bilişim sistemi içinde yer alan donanım kavramı içine ana kart, ekran, yazıcı, ses sistemi, disk, disket, modem kartı, manyetik bant gibi maddî bünyeye sahip parçalar girmektedir. Dolayısıyla sistemde yer alan veri kavramıyla bilgisayarın hafızasında kayıtlı bulunan veriler anlaşıldığı gibi, anakart üzerindeki veri yollarına takılmak suretiyle kullanılan birimlerdeki (USB bellek aygıtı, cd-rom gibi) veriler de kabul edilmektedir. TCK'nın 244. maddesinin 2. fıkrasında yer alan seçimlik unsurlardan birinin gerçekleşmesi şartıyla sorunun içtima kapsamında değerlendirilmesi gerektiğini düşünüyoruz. Örneğin verilere zarar vermek amacıyla cihazlara zarar verilmesi halinde mala zarar verme suçu (TCK m. 151) ile 244. madde arasında fikri içtima ilişkisi söz konusu olacaktır.

2. Hareket ve Netice

a) Bilişim Sisteminin İşleyişinin Engellenmesi veya Bozulması

Ceza Kanunumuzun 244. maddesinin 1. fıkrasında düzenlenen suçun oluşması için sistemin işleyişinin engellenmesi veya bozulması gerekmektedir. Sistemin işleyişinin engellenmesi veya bozulması suçun netice unsurunu oluşturmaktadır. Dolayısıyla bu suç neticeli bir suç niteliğindedir[41]. Suçun bu neticeleri gerçekleştirmeye elverişli her tür hareketle işlenebilmesi mümkündür. Bu özelliği nedeniyle de suç, serbest hareketli suçtur[42].

Veri işlem yapılmasını, yani verilerin kullanılmasını, kaydedilmesini, depolanmasını, işlenmesini veya değerlendirilmesini veya veri aktarımını önlemeye yönelik her tür hareket **bilişim sisteminin işleyişinin engellenmesi kavramı** altına girmektedir. Kanun koyucu bazı hareketlerin cezasız kalmaması esasından yola çıkarak düzenlemede geniş bir kavrama yer vermiştir. Bilişim sistemine yapılan müdahale veri işlem yapılmasını kesintiye uğratmışsa veya önlemişse sistemin işlemesine engel olunmuştur. Bu anlamda sisteme ve unsurlarına zarar veren veya sistemin işlevde bulunmasını önleyen hareketler, sistemin işlemesine engel olmak kavramı altına girmektedir. Bilişim sisteminin

---

41 Akbulut, s. 200; Stree/Hecker-Schönke/Schröder, § 303 a, kn. 1; Koca/Üzülmez, s. 827. Sırf hareket suçu olduğuna ilişkin olarak bkz.: Özbek/Doğan/Bacaksız/Tepe, s. 951

42 Koca/Üzülmez, s. 827. Bağlı hareketli suç olduğuna ilişkin olarak bkz.: Özbek/Bacaksız/Doğan/Tepe, s. 951.

teknik fonksiyonuna zarar vermek, veri akışının kesilmesi, program verilerinin silinmesi veya değiştirilmesi suretiyle gerçekleştirilebilir. Yine DoS, DDoS saldırıları da sistemin işlemesine engel olmaktadır[43]. Keza bilişim tesisinin veya veri işlem taşıyıcısının yetkili kişinin tasarruf alanından uzaklaştırılması (gizlemek veya çalmak gibi), şifrenin değiştirilmesi veya şifre ilâvesiyle sistemin kullanılmasına engel konulması, programın bozulması, sistemin kilitlenmesi hareketleri de sistemin işlemesine engel olmak niteliği taşımaktadır[44]. Görüldüğü üzere sistemin işlemesine engel olma, sisteme fizikî etki şeklinde gerçekleştirilebileceği gibi, soyut unsurlara yapılan müdahalelerle de söz konusu olabilir. Verilerin bozulması, yok edilmesi, erişilmez kılınması, verilerin değiştirilmesi, sisteme veri yerleştirilmesi, sistemdeki verilerin iletilmesi suretiyle de sistemin işlemesine engel olunabilir. Burada önemli olan bilişim sisteminin işleyişini engellenmesi sonucunu doğuran bir hareketin yapılmış olmasıdır[45]. Sistem işliyor ancak yavaş işliyorsa sistemin işlemesi engellenmemiştir. Örneğin hatalı program teslimiyle bir firmanın işlemlerinin yavaş işlemesine neden olunmasında olduğu gibi[46]. Ancak doktrinde bazı yazarlar bu suçun konusunun sistemin soyut unsurları olduğunu, sistemin fiziki unsurlarına zarar vermenin bu suçu değil mala zarar verme suçunu oluşturduğunu ifade etmektedirler. Sistemin işleyişini sağlayan soyut unsurlara zarar verme fiillerinin ancak 244. maddedeki suçu oluşturacağını belirtmektedirler[47]. Siber suç sözleşmesinde olduğu gibi (m. 5) sadece sistemin soyut unsurlarına müdahale edilmek suretiyle sistemin işleyişinin engellenmesine yönelik

---

43 Stree/Hecker-Schönke/Schröder, § 303 b, kn. 9.

44 Bazı yazarlar, sistemi veya verileri tahrip etmeyen, yalnız sistemin kullanılmasını engelleyen bilgisayar virüsünün maddenin kapsamına girip girmediği konusuna açıklık getirilmediğini belirtmektedirler: Yücel, Mustafa T., "Bilişim Suçları", ABD, 1992, Yıl 49, S. 1-6, s. 505-512, s. 511. Ancak bu görüşe karşı söz konusu fiilin madde kapsamına girdiğinin kabul edilmesi gerektiği belirtilmiştir: Malkoç/Güler, s. 4762.

45 Bkz.: Akbulut, s. 139.

46 Hatalı programların teslimiyle ve sistemin kullanılmasına engel olunmasıyla ilgili olarak ayrıntılı bilgi için bkz.: Hilgendorf, 1996, Heft 12, s. 1084; Sondermann, s. 117-119; Schulze Heiming, s. 219.

47 Koca/Üzülmez, s. 827, 828.

sınırlayıcı belirleme 244. maddenin 1. fıkrasında bulunmadığından bu görüşe katılmıyoruz. Bilişim sistemi hem soyut (yazılım) hem de fiziki unsurlardan (donanımdan) oluşmaktadır. Fiziki unsurlarda gerçekleştirilen hareketlerle de sistemin işleyişi engellenebilir. Burada korunmak istenen sadece verile müdahale edilmeden sistemin usulüne uygun çalışması değil, herhangi bir problem olmadan sistemin çalışmasındaki yarardır. Dolayısıyla yalnızca soyut unsurlara müdahaleyle bunun sağlanamayacağını düşünüyoruz. Nitekim Alman Ceza Kanununun 303 b maddesinde veri işlem tesisine veya veri taşıyıcısına müdahalelerin de bilgisayar sabotajını oluşturacağı kabul edilmiştir. Bizim kanunumuz hareketleri tek tek saymayarak sadece neticeye yer vererek geniş belirleme yapmıştır. Ancak bu düzenleme kanunilik ilkesi açısından sorun doğuracak niteliktedir. Zira kanunilik ilkesinin sonuçlarından biri olan belirlilik ilkesi, haksızlık teşkil eden fiilin tam ve özenli bir dilde anlatılmasını istemektedir. Sınırları belirli olmayan hükümlerden oluşan normların, geniş yorumlama imkânı veren kavramların varlığı, belirlilik ilkesine aykırıdır. Siber Suç Sözleşmesinde veya Alman Ceza Kanunun 303 b maddesinde olduğu gibi bilişim sisteminin işleyişinin engellenmesi veya bozulmasının hangi fiillerle gerçekleştirileceğinin açıklığa kavuşturulması gerekmektedir.

765 sayılı TCK'nın 525/b-1 maddesinde bilgileri otomatik işleme tabi tutan sistemin tahrip edilmesi ayrıca seçimlik olarak sayılmıştı. Ancak o dönemde de sistemde oluşan zararın 525/b-1 maddesine göre suç oluşturabilmesi için sistemin içinde bulunan soyut unsurları, yani verileri etkilemesi, onlara zarar vermesi gerektiğini kabul etmiştik. Verilere zarar vermeyen hareketlerin 525/b-1 maddesi bakımından tahrip etmek değil, sistemin işlemesine engel olmak niteliği taşıdığını, çünkü kanun koyucu aynı fıkrada sistemin işlemesine engel olmak fiilini de ayrıca belirttiğinden, sistemde meydana gelen zarar nedeniyle sistemin düzenli çalışması, başka bir söyleyişle veri işlem yapılması engellenmişse hareket tahrip etmeyi değil, sistemin işlemesine engel olmayı oluşturduğunu belirtmiştik. Kanunumuzda, sistemin tahrip edilmesinin ayrıca düzenlenmesine gerek bulunmadığını, eğer tahriple verilerde bir zarar oluşmuşsa, bunun zaten verilerin tahrip edilmesi kavramına gireceğini, verilere bir zararın verilmesi söz konusu olmayıp da sistemin işlemesine engel olunmuşsa, bu da sistemin işlemesine engel

olmak kavramı içinde değerlendirileceğini ifade etmiştik. Her ikisi de söz konusu değilse yapılan hareket mala zarar verme suçunu oluşturacaktır.

Sistemin işlemesine engel olunmasının daimî veya geçici bir süre için olmasının önemi bulunmamaktadır[48].

Bilişim sisteminin işleyişinin geçici olarak engellenmesi durumunda da madde 244/1'deki suçun oluşacağını kabul etmekle birlikte, bilişim sisteminin işleyişinin her tür engellenmesinin cezalandırılmaması gerektiğini düşünüyoruz[49]. Kanunumuzda böyle bir sınırlandırma bulunmamakla beraber, sistemin işlemesini önemsiz ölçüde engelleyen veya birtakım değişikliklerle meydana getirilen durumun ortadan kalkmasına neden olan hallerin 244. maddenin cezalandırılması kapsamı dışında tutulması gerekir. Haksızlık içeriğinin azlığı nedeniyle ceza verilmemesi yoluna gidilmesi gerekir. Bu yönde bir belirlemeye suçla ilgili olarak yer verilmesinin uygun olacağını düşünüyoruz.

Bilişim sisteminin işleyişinin bozulması ise, sistemin çalışma şeklinin bozulması, sistemin yapması gerekenden farklı şeyleri yapmasının sağlanmasını ifade etmektedir. Kısaca bilişim sisteminin veri işlem yapmasının, verileri aktarmasının sistemden beklenildiği şekilde gerçekleştiremeyecek, eskisi gibi yapamayacak hale getirilmesini

---

48 Dönmezer, s. 528; Yazıcıoğlu, s. 263.

49 Doktrinde bu tür fiiller değişik şekillerde nitelendirilmektedir. İçel'e göre, meydana getirilen zararın veya tehlikenin belirli bir ağırlıkta bulunması suçun gerçekleşip gerçekleşmemesine etki etmektedir. Örneğin hiçbir değeri olmayan basit bir kağıt parçasının çalınması halinde hırsızlık suçu oluşmayacaktır. Yazar suçun oluşmasını önleyen bu özelliğe suçun niceliği adını vermektedir. Bir suçun tipe uygun, hukuka aykırı ve kusurlu oluşu o suçun niteliği özelliğini, gerçekleştirilen zararın veya tehlikenin belirli ağırlıkta olması ise, suçun niceliği özelliğini oluşturmaktadır (İçel, Kayıhan, Suçların İçtimaı, İstanbul 1972, s. 26). Özgenç'e göre ise, zararın çok az olması durumunda kanunda belirtilen suç gerçekleşmekte, ancak fiilin haksızlık muhtevasında önemli derecede azalma olmaktadır. Bu nedenle zararın az olması failin cezalandırılmasına etki etmelidir. Bu etki ya failin cezalandırılmasını önleyecek ya da cezanın belirli bir miktarda indirilmesini sağlayacaktır (Özgenç, İzzet, Uygulamalı Ceza Hukuku, Çözümlü Örnek Olaylar ve Karar Tahlilleri, Gözden Geçirilmiş ve Genişletilmiş 2. Bası, İstanbul 1998, s. 109, 127, 145.

belirtmektedir[50]. Bu herhangi bir şekilde gerçekleştirilebilir. Sistemin fizikî unsurlarına zarar vererek veya fizikî varlığına zarar vermeden yalnız soyut unsurlarına yapılacak müdahaleyle bilişim sisteminin işlemesinin bozulması sağlanabilir[51]. Örneğin sistemin parçalarının değiştirilmesi veya verilerin değiştirilmesi veya bazı verilerin silinmesi veya hatalı program teslimi veya virüs göndermek suretiyle bilişim sisteminin işleyişinin bozulması söz konusu olabilir. Sistemin yanlış işlemesinin sağlanması da sistemin işleyişinin bozulması kapsamına girmektedir. Bilişim sisteminin normal yapması gerekeni yapamayacak hale getirilmesi sağlanıyorsa sistemin işleyişi bozulmuştur. Sistemin kendisinden isteneni tamamen veya kısmen yerine getiremeyecek olması bozulma açısından önemsizdir. Sistemin işleyişinin bozulması durumunda sistemin işleyişinin engellenmesi de söz konusu olabilmektedir. Ancak her engelleme durumunda sistemin bozulması gerçekleşmediği için kanun koyucu ayrı belirleme yapmıştır[52].

b) Bilişim sistemindeki verilerin bozulması, yok edilmesi, değiştirilmesi, erişilmez kılınması, sisteme veri yerleştirilmesi veya mevcut verilerin başka yere gönderilmesi

Ceza Kanunumuzun 244. maddesinin ikinci fıkrasında düzenlenen bilişim sistemindeki verilerin bozulması, yok edilmesi, değiştirilmesi, erişilmez kılınması, sisteme veri yerleştirilmesi veya mevcut verilerin başka yere gönderilmesi suçu, birinci fıkradan sonra düzenlenmiştir. Aslında ilk fıkrada düzenlenmesi yoluna gidilmesi daha doğru olurdu. Zira sistemin engellenmesi veya bozulması fiilleri 1. fıkrada belirtilen fiillerle de gerçekleştirilebilmektedir. TCK'nın 1. ve 2. fıkrasının yer değiştirmesi düzenleme şekli itibariyle daha yerinde bir düzenleme niteliği taşıyacaktır.

Kanun koyucu 2. fıkrada verilerin kullanılmasına müdahale niteliği taşıyan belirlemelere yer verdiği gibi bu nitelikte olmayan hareketlere de yer vermiştir. Verilerin bozulması, yok edilmesi, erişilmez kılınması, değiştirilmesi, verilerin istenen amaç

50 Bozmak için bkz.: http://tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.581c3db859b712.08285126 (E.T.03.11.2016)

51 Farklı düşünce için bkz.: Yazıcıoğlu, s. 263.

52 Bkz.: Koca/Üzülmez, s. 828.

doğrultusunda kullanılmasına engel olma niteliği taşırken, sisteme veri yerleştirilmesi veya verilerin başka yere gönderilmesi bu nitelikte değildir.

Verilerin bozulması, verilerin kullanılabilirliğine zarar verilmesidir. Fıkrada kullanılan verilerin bozulması kavramı, bir neticeyi ifade etmektedir. Zarar niteliği taşıyan neticedir. Verilerin belirlenen amaç doğrultusunda kullanılmasının tamamen veya kısmen ortadan kaldırılmasını sağlayacak şekilde verilere zarar verilmesini ifade etmektedir[53]. Verilerin bozulmasında, veriler artık usulüne uygun olarak kullanılamayacak hale getirilmektedir[54]. Örneğin birbirine bağlı veri cümlelerinin yerlerinin değiştirilerek anlamının karıştırılması[55] veya ilâve şeylerin katılması veya veri cümlelerinden tek tek verilerin silinmesi suretiyle verilerin kullanılabilirliğine zarar verilmesi verilerin bozulması anlamındadır[56]. Keza virüs programları da verilerin bozulmasında kullanılan diğer bir yöntemdir.

Verilerin yok edilmesi, verilerin varlığının ortadan kaldırılmasıdır. Bilişim siteminde depolanmış verilerin tamamen ve telafisi olmayacak şekilde tanınmaz hale getirilmesidir[57]. Verilerin ortadan kaldırılmasını, yani veri cümlelerinin veya verilerin oluşturduğu bilgilerin, işaretlemelerin ortadan kaldırılmasını veya verilerin üzerine yeni veriler geçirilmesi suretiyle aslî içeriğinin artık tamamen mevcut olmaması halini ifade etmektedir[58]. Verilerin yok edilmesinde verilerin

---

53 Dreher/Tröndle, § 303a, kn. 7; Tröndle/Fischer, § 303a, kn. 11; Samson, SK, § 303a, s. 5.

54 Stree/Hecker-Schönke/Schröder, § 303 a, kn. 7.

55 Dreher/Tröndle, § 303a, kn. 7, 8; Tröndle/Fischer, § 303a, kn. 11.

56 Schulze Heiming, s. 180; Sondermann, s. 57.

57 Stree/Hecker-Schönke/Schröder, § 303 a, kn. 5; Dreher/Tröndle, § 303a, kn. 5;Tröndle/Fischer, § 303 a, kn. 9; Samson, SK, § 303 a, s. 5; Haβ, Gerhard, Der strafrechtliche Schutz von Computerprogrammen, Rechtsschutz und Verwertung von Computerprogrammen, 2., völlig überarbeitete und erweiterte Auflage, Köln 1993, s. 498; Lackner/Kühl, § 303 a, kn. 3; Lenckner/ Winkelbauer, s. 824, 829.

58 Schulze Heiming, s. 173, 175.

varlığı ortadan kaldırıldığı için tekrar yinelenmesi söz konusu değildir[59]. Örneğin, cracker'ler vasıtasıyla kopya engelinin kaldırılması, mobil telefonlardaki sim kilidinin kaldırılması bu niteliktedir[60]. Yok edilen bilgilerin birtakım yardımcı aletler aracılığıyla geri getirilebilmesi durumunda suçun oluşup oluşmayacağı tartışmalıdır. Bazı yazarlar bazı araçlar yardımıyla geri getirilme imkanı varsa, telâfisi mümkün olmayacak şekilde tanınamaz yapmanın gerçekleşmediğini kabul etmektedir[61]. Buna karşılık doktrinde bazı yazarlar verilerin geriye dönüşü imkansız olacak şekilde yok edilmesinin gerekmediği, veriye erişim için girilen komutun sonuçsuz kalacak şekilde kayıtlardan silinmesinin yeterli olduğu ifade edilmektedir[62]. Bazı yazarlar ise, verilerin ortadan kaldırılmasının, verilere normal yollardan ulaşılmasının güçleştirilmesi şeklinde değerlendirilmesi gerektiğini, ortadan kaldırılan verilere bazı araçlarla veya programlarla ulaşılabilme imkanının varlığının suçun oluşmasını engellemeyeceğini belirtmektedirler[63]. Biz ilk görüşe katılıyoruz ve geri getirme imkanı varsa verilerin yok edilmesinin söz konusu olmadığını ifade ediyoruz. Başka seçimlik unsurlar kapsamına, örneğin şartları taşıyorsa verilerin erişilmez kılınmasına girebileceğini düşünüyoruz.

Verilerin yok edilmesi herhangi bir şekilde gerçekleştirilebilir. Silmek suretiyle de veriler yok edilebilir[64]. Ancak kısmî silmeler, yok etme kavramı içine girmez. Yalnızca veri taşıyıcısındaki bilgilerin silinmesi de verilerin yok edilmiş sayılması için yeterli değildir[65]. Kopyası bulunan verilerin silinmesi durumunda, verilerin yok edilmesi gerçekleşmez[66]. Ancak güvenlik kopyası bulunan verilerin silinmesinin verilerin yok edilmesi anlamını taşıyacağı, tipikliğin gerçekleşeceği ifade

59 Tröndle/Fischer, § 303 a, kn. 9.

60 Lackner/Kühl, § 303 a, kn. 3.

61 Schulze Heiming, s. 173

62 Özbek/Doğan/Bacaksız/Tepe, s. 952.

63 Koca/Üzülmez, s. 830.

64 Koca/Üzülmez, s. 830.

65 Schulze Heiming, s. 173. Ayrıca bkz: Sondermann, s. 48, 49, 50.

66 Hilgendorf, 1996, Heft 10, s. 893.

edilmektedir[67]. Virüsler aracılığıyla, bilişim sistemine zarar vermekle de veriler yok edilebilir[68]. Ancak bu nitelikteki fiilin sistemin işleyişinin engellenmesi veya bozulması kapsamında olmaması gerekir.

Verilerin değiştirilmesi, kaydedilmiş verilerin başka bir bilgi içeriği almasını ifade etmektedir[69]. Başka bir söyleyişle, yeni bir bilginin oluşmasını sağlayan her tür hareket değiştirmek olarak kabul edilmektedir. Kaydedilmiş verilerin içerik değiştirilmesinin her formu verilerin değiştirilmesidir. Bunun yanında içerik değiştirmeksizin başka bir program dili[70] koduna çevirme veya şifrenin ve şifresiz yazının değişimi de verilerin değiştirilmesi kapsamındadır[71]. Bunlara göre verilerin içeriğinin tamamen değiştirilmesi veya veri sonuçlarının değiştirilmesi veya program dilinin değiştirilmesi veya verilerin metin içindeki yerlerinin değiştirilmesi veya verilerin kısmî silinmesi veya verilere ilave şeylerin katılması, yeni bir bilginin oluşturulmasını sağlayan hareketlerdir. Verilerin tamamen silinmesi de bazı durumlarda değiştirmek olarak kabul edilmektedir. Her ne kadar verilerin tamamen ve geri getirilemez şekilde silinmesi verilerin yok edilmesi kapsamı içinde yer almakla ve değiştirmek olarak kabul edilmemekle beraber eğer silinen veriler yeni bir şey ifade ediyorsa, yani silinmeden olumlu bir sonuç çıkıyorsa bu da değiştirmek anlamında değerlendirilmektedir[72].

Verilerin izinsiz şekilde kopyalanması verilerin değiştirilmesi kapsamında değildir. Mevcut verilerde değişiklik yapmak suretiyle

---

67 Sondermann, s. 45 vd; Stree/Hecker-Schönke/Schröder, § 303 a, kn. 5; Kindhäuser, Urs/Neumann, Ulfrid/Paeffgen, Hans-Ullric, Strafgesetzbuch, Band 3, 4. Auflage, Baden-Baden 2013, § 303 a, kn. 7.

68 Stree/Hecker-Schönke/Schröder, § 303 a, kn. 5; Tröndle/Fischer, § 303 a, kn. 9.

69 Stree/Hecker-Schönke/Schröder, § 303 a, kn. 8.

70 Ancak program değişikliklerinde ara sonucun değiştirilmesinin değiştirme olarak kabul edilip edilmeyeceği tartışmalıdır. İtiraz, değiştirmenin söz konusu olması için kaydetmenin varlığının olması gerektiği noktasında toplanmaktadır. Ayrıntılı bilgi için bkz.: Schulze Heiming, s. 183.

71 Dreher/Tröndle, § 303a, kn. 8; Tröndle/Fischer, § 303 a, kn. 12; Hilgendorf, Heft 10, s. 891.

72 Möhrenschlager, s. 141.

başkasına ait WLAN'ın kullanılması söz konusu olmuşsa verilerde değişiklik söz konusudur. Ancak fail verilerde değişiklik yapmamış, internete yalnızca giriş yapmışsa 244. madde kapsamında değildir[73].

Değiştirmenin orijinal verilerde yapılması gerekir. Kopya edilmiş verilerde yapılan değişikliklerde m. 244/2 uygulanmaz[74].

Verilerin erişilmez kılınması, yetkili kişinin verilere ulaşmasının ortadan kaldırılması suretiyle verileri kullanmasının engellenmesidir[75]. Yetkilinin somut kullanım iradesinin tespiti zorunlu değildir. Yetkili kişinin potansiyel erişim imkanının kaldırılması yeterlidir[76]. Herhangi bir şekilde gerçekleştirilebilir. Virüs saldırısı veya spamming denilen hususlarla gerçekleştirilebilir[77]. Verilere ulaşmak için mevcut olan bağın ortadan kaldırılması suretiyle de veriler erişilmez kılınabilir. Bu durumda verilere ulaşmak isteyen kişi bağın koparılması nedeniyle ancak emek ve masrafla söz konusu bilgileri elde edebilmektedir[78]. Şifre engeli koymak veya dosya isimlerini değiştirmek, dosyaları gizlemek, veri taşıyıcısına elkoymak, elektronik postaları gizlemek, içindekileri silmek gibi yollarla verilerin erişilmez kılınması gerçekleştirilebilir[79].

Doktrinde silme kavramı fiziki silme ve mantıki silme diye ikiye ayrılmaktaydı. Fiziki silme verilerin fiziken ortadan kaldırılmasını, yok edilmesini ifade ederken, mantıki (veya mecazi) silme ise veriler ortadan kaldırılmamakla birlikte kişi verilere ulaşamamaktadır[80]. Dolayısıyla da düzenlemede silme ifadesi geçiyorsa silmenin hangisini ifade ettiği tartışılmaktaydı. Doktrinde silme kavramının anlamı noktasında çoğunlukla kabul edilen görüş, meydana getirilen tanınmazlığın fizikî

---

73 Stree/Hecker-Schönke/Schröder, § 303 a, kn. 8.

74 Hilgendorf, 1996, Heft 10, s. 890; Tröndle/Fischer, § 303 a, kn. 12.

75 Stree/Hecker-Schönke/Schröder, § 303 a, kn. 6; Lackner/Kühl, § 303 a, kn. 3.

76 Stree/Hecker-Schönke/Schröder, § 303 a, kn. 6.

77 Lackner/Kühl, § 303 a, kn. 3.

78 Bkz.: Schulze Heiming, s. 174.

79 Tröndle/Fischer, § 303 a, kn. 10.

80 Bkz.: Akbulut, s. 136, 137.

anlamda olması gerektiğidir. Bu görüşe göre mantıkî anlamda silmek, silmek kavramına dahil olmayıp, gizlemek kavramı içine girmektedir[81]. Ancak bu ayrımın bugün doktrinde ifade edilmediği söylenebilir[82]. 765 sayılı Ceza Kanunumuzda, verilere veya veri işleme zarar vermek suçunda verilerin gizlenmesi veya başka bir şekilde yetkilinin verileri kullanmaktan mahrum bırakılması maddî unsuru oluşturan bir seçenek olarak düzenleme kapsamına alınmamıştı. Düzenlemede silmek kavramı yer almaktaydı. Biz de bu nedenle silmek kavramını sınırlayıcı yoruma tâbi tutmamızı gerektiren herhangi bir neden bulunmadığını, silmek kavramını geniş yorumlayarak verilerin fiziki olarak ortadan kaldırılması yanında, verilere ulaşmanın engellenmesinin de bu kapsamda nitelendirilmesi gerektiğini belirtmiştik. 5237 sayılı Kanunumuz verilerin erişilmez kılınmasını açıkça düzenleyerek bu sorunu ortadan kaldırmıştır. Dolayısıyla güvenlik engellerinin veya şifrenin değiştirilmesi suretiyle veya başka yollarla yetkili kişi verilere ulaşamıyorsa verilere ulaşım engellenmiştir. Verilere ulaşımın engellenmesinin ne suretle olduğu önemli değildir. Yeni giriş engeli yaratılmışsa veya belirli şekilde kaydedilmiş verilerin adresleri silinmişse verilere ulaşım engellenmiştir[83]. Keza verilerin silinmesi suretiyle mağdur verilere belirli süre erişememiş, ancak daha sonra verileri tekrar elde etmişse veriler erişilmez kılınmıştır.

Verilerden yararlanılmasına engel oluşturucu hareketlerin ne kadar süre için olması gerektiği konusunda farklı görüşler bulunmaktadır. Bazı yazarlar verilerin erişilmez kılınmasının sürekli olması gerektiğini belirtirken[84], bazı yazarlar geçici bir süre verilerin kullanılmasının engellenmesinin bu fiil açısından yeterli olduğunu ifade etmektedirler[85]. Genel görüş olarak geçici sürede de suçun oluştuğu kabul edilmekle birlikte, bu süreden ne anlaşılması gerektiği belirli değildir. Bir görüş

---

81 Schulze Heiming, s. 175.

82 Stree/Hecker-Schönke/Schröder, § 303 a, kn. 6; Lackner/Kühl, § 303 a, kn. 3; Kindhäuser/Neumann/Paeffgen, § 303 a, kn. 8.

83 Schulze Heiming, s. 178.

84 Samson, SK, § 303a, s. 5.

85 Dreher/Tröndle, § 303a, kn. 6; Lackner /Kühl, § 303 a, kn. 3; Haβ, s. 498 ; Hilgendorf, 1996, Heft 10, s. 891; Tröndle/Fischer, § 303a, kn. 10; Stree/Hecker-Schönke/Schröder, § 303 a, kn. 6.

sürenin önemli bir zamana tekâbül etmesini ararken[86], diğer bir görüş kullanılmamanın en azından kesin bir süreyi göstermesinin yeterli olduğunu belirtmektedir[87]. Kullanılmamanın sürekli olmasının aranmaması gerektiğini, zira geçici bir süre verilerin erişilmez yapılmasının da önemli bir zarara sebep olabileceğini belirtmek gerekir. Geçici olarak verilerin kullanılmasının engellenmesini kabul etmekle beraber, geçiciliği, önemsiz olmayan bir süre için verilere erişimin imkansız olması şeklinde anlıyoruz ve bu halde suçun oluşacağını kabul ediyoruz.

Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan hareketlerin gerçekleştiriliş biçimi önemli değildir. Verilere kullanılmasına müdahale niteliği taşıyan hareketler çoğunlukla icraî bir hareketle gerçekleştirilir. Ancak ihmali hareketle de suçun işlenmesi mümkündür. Eğer fail, belirli bir icrai davranışta bulunma hukuki yükümlülüğü altında olmasına rağmen verilerin kullanılmasına engel olucu hareketleri önlemiyorsa 2. fıkradaki suçu gerçekleştirmiş olacaktır. Örneğin belirli bir icrai davranışta bulunma yükümlülüğü olan garantörün, bilişim sistemindeki verileri etkileyecek virüs gönderildiğini tespit etmesine rağmen virüsün verilere zarar vermesini engellemediğinde 2. fıkra gereğince ihmalinden dolayı sorumlu olacaktır.

Buraya kadar m. 244/1 ve 2' de yer kavramlarla ilgili yapılan açıklamalardan sonra şu belirtilmelidir ki kavramların birbirinden ayrımını ve sınırlandırmasını yapmak kolay olmamaktadır. Çünkü yapılan bir hareket, maddede belirtilen kavramlardan birkaçının kapsamına girebilmektedir. Örneğin verileri yok etmek anlamına gelen bir hareket, aynı zamanda verileri bozmak niteliği taşıdığı gibi aynı zamanda sistemin işleyişine engel olmak unsurunu da gerçekleştirebilmektedir. Konunun çözümü hem içtima açısından hem de fıkraların düzenlediği kavramlar açısından yapılmalıdır. Önce gerçekleştirilen bir fiilin fıkralarda geçen ve seçimlik olan kavramların

---

86 Schlüchter, 2. WİKG, s. 73: Sondermann, s. 73; Wessels, Johannes/Hillenkamp, Thomas, Strafrecht, Besonderer Teil 2, Straftaten gegen Vermögenswerte, 39. Auflage, Heidelberg 2016, kn. 60; Kindhäuser/Neumann/Paeffgen , § 303 a, kn. 8.

87 Lenckner /Winkelbauer, s. 829.

hangisinin kapsamına girdiği tespit edilmelidir. Aynı fıkradaki birkaç kavramın kapsamına giriyorsa hangisinin daha özel olduğuna göre belirleme yapılmalıdır. Buna karşılık gerçekleştirilen fiil, hem 1. fıkranın hem de 2. fıkranın düzenlemesinde yer alan kavramların kapsamına giriyorsa sorun içtima kapsamında çözümlenmelidir[88].

Kanunda yer verilen ve bilişim sistemindeki verilerin kullanılmasına müdahale teşkil etmeyen kavramlardan birisi olan **sisteme veri yerleştirmek ise**, dış verilerin (sistemde bulunmayan) bilişim sistemine girilmesidir. Örneğin klavye suretiyle veya flash bellek, CD gibi veri taşıyıcıları aracılığıyla veriler sisteme girilmişse sisteme veri yerleştirilmiştir[89]. Keza internet ortamından sisteme veri yerleştirmek suretiyle suç gerçekleştirilebilir[90].

Var olan verileri başka yere göndermek ise, telekomünikasyon yolları üzerinden veya mevcut ağ içerisinde bir sistemdeki verilerin başka bir sisteme gönderilmesidir. W-LAN aracılığıyla gönderilmesi de bu hareket kapsamındadır[91]. Doktrinde verilerin bir veri taşıma cihazına gönderilmesi de verilerin başka yere gönderilmesi şeklinde nitelendirilmektedir[92].Bu hareketin oluşması açısından verilerin kopyasının gönderilmesi mi gerektiği, yoksa verilerin orijinalinin mi gönderilmesi gerektiği madde metninde herhangi bir ayırıcı belirleme olmadığı için anlaşılamamaktadır. Ancak orijinalinin gönderilmesi durumunda fıkrada geçen hareketlerin kapsamına giren bir durum oluşacaktır. Kopyalanması kastediliyorsa verileri başka yere göndermenin neden 2. fıkradaki suç kapsamında nitelendirildiği anlaşılamamaktadır. Çünkü verilerin kullanılmasına engel olmamakta, verilere zarar vermemektedir.

---

88 Almanya'daki durum için bkz.: Sondermann, s. 62,123 ; Schulze Heiming, s. 184, 185.

89 Stree/Hecker-Schönke/Schröder, § 303 b, kn. 7; Koca/Üzülmez, s. 830.

90 Koca/Üzülmez, s. 831.

91 Stree/Hecker-Schönke/Schröder, § 303 b, kn. 7.

92 Koca/Üzülmez, s. 831.

B. Manevî unsur

Türk Ceza Kanununun 244. maddesinin 1. ve 2. fıkralarında düzenlenen suçlar, kasten işlenebilir. Suçların oluşması için olası kast da yeterlidir. 765 sayılı Türk Ceza Kanununda (m. 525/b-1'de) zarar vermek veya yarar sağlamak maksadıyla hareket edilmesi gerekmekteydi. Doktrinde kanun koyucunun bu tercihi eleştirilmişti[93]. 1997 ve 2003 Tasarılarında verilere veya veri işleme zarar vermek suçunun karşılığı olarak düzenlenen 348. ve 347. maddelerin 1. ve 2. fıkralarında bu şekilde amaca yer verilmemiştir. Ancak 348. ve 347. maddelerin verilere müdahaleyi düzenleyen 2. fıkralarında fiilin hukuka aykırı olması şartı aranmıştı[94]. Mevcut düzenlemedeki verileri bozmak, yok etmek, değiştirmek veya erişilmez kılmak için amaca yer verilmemesi doğru olmakla beraber, sisteme veri yerleştirmek veya var olan verileri başka bir yere göndermek açısından kanun koyucunun neden bu kavramları 244. maddede düzenlediğini ortaya koyması gerekirdi. Sistemin işleyişinin engellenmesi amacıyla mı, yarar sağlamak amacıyla mı, mağdurun zararına olarak mı gerçekleştirilmesi gerektiğini açıklığa kavuşturması gerekmekteydi. Kavramların şu anki düzenleme şekli sorunlu nitelik taşımaktadır. Daha önce de kavramların 244. maddenin 2. fıkrasında yer verilmesini değişik gerekçelerle eleştirdiğimizden burada tekrara yer vermemek için ayrıntılara girmiyoruz.

Kast için suçun kanuni tanımında yer alan unsurların bilinmesi gerekir. Yani failin sistemdeki verilere değiştirdiğini, yok ettiğini, bozduğunu, erişilmez kıldığını, sistemin işleyişini engellediğini, sistemin işleyişini bozduğunu bilmelidir. Failin muhtemel bilmesi de yeterlidir. Hata halinde 30. madde hükmü uygulanır. Örneğin fail hareketinin hatalı olarak tasarruf hakkı içerisinde olduğunu kabul ediyorsa (kendi verilerini yok ettiğini zannediyorsa) kastı ortadan kaldıran tipiklik hatası söz

---

93 Bkz.: Önder, Ayhan, Şahıslara ve Mala Karşı Cürümler ve Bilişim Alanında Suçlar, İstanbul 1994, s. 508; Ersoy, s. 181.

94 Hukuka aykırılık ibaresine yer veren Almanya'da böyle bir kavrama yer verilmesinin eleştirisi ve tipikliğin unsuru mu yoksa genel hukuka aykırılık unsuru mu olduğu noktasında bkz.: Lackner /Kühl, § 303 a, kn. 4; Stree/Hecker-Schönke/Schröder, § 303 a, kn. 10; Kindhäuser/Neumann/Paeffgen , § 303 a, kn. 12. Ayrıca bu konuda ayrıntılı bilgi için bkz.: Gerhards, s. 70-81.

konusudur. Buna karşılık kulanım hakkı başkasına ait olmakla beraber veri taşıyıcısının maliki olarak verileri siler ve bunun tipikliği oluşturmadığını, tipikliğin ancak başkasına ait veri taşıyıcısındaki verilerin silinmesi halinde oluşacağını düşünüyorsa yorum hatası söz konusudur. Burada kastı ortadan kaldıran hata değil, yasak hatası söz konusudur[95].

Türk Ceza Kanununun 244. maddesinde verilere veya sisteme müdahale edilmesinin taksirli şekline yer verilmemiştir. Ancak verilere veya veri işleme zarar vermek suçu taksirle işlenebilir. Örneğin, fail ücret ödeyerek girdiği bir sitemdeki verilere dikkatsizlikle zarar vermiş olabilir[96]. Suçların taksirli şekline ilişkin bir belirleme olmadığından cezalandırılmaları söz konusu değildir. Buna karşılık sisteme hukuka aykırı giriş yapılması nedeniyle sitemdeki verilerin yok olması veya değişmesi hali, yani fiilin taksirli şekli TCK'nın 243. maddesinin 3. fıkrasında netice sebebiyle ağırlaşmış suç olarak yaptırım altına alınmıştır.

C. Hukuka Aykırılık

Hukuka uygunluk nedenlerinden ilgilinin rızasının gerçekleşmesi mümkündür. Yetkili kişi verilerin yok edilmesine, değiştirilmesine veya diğer fiillere rıza göstermişse suç oluşmayacaktır.

Görevin ifası kapsamında gerçekleştirilen fiiller de 244. madde çerçevesinde fiilin hukuka uygunluğunu sağlayacaktır. Örneğin 5651 sayılı Kanun gereğince erişimin engellenmesi kararının verilmesi ve bu kararın yerine getirilmesi durumunda fiil, sistemin işleyişinin engellenmesi suçunu oluşturmayacaktır[97]. Yine belirli döneme ait veya bazı şartların gerçekleşmesi şartıyla, vergi borçlarının silinmesi yolunda karar alınması ve buna dayanılarak yapılan düzenleme çerçevesinde vergi borçlarını silinmesi durumunda verileri silen kişi verileri yok etmekten sorumlu tutulmayacaktır.

---

95 Stree/Hecker-Schönke/Schröder, § 303 a, kn. 9.

96 Akbulut, s. 144.

97 Özbek/Doğan/Bacaksız/Tepe, s. 959, 960; Koca/Üzülmez, s. 831

IV. SUÇUN NİTELİKLİ HALİ

Ceza Kanunumuzun 244. maddesinin 3. fıkrasında, 244. maddenin 1. ve 2. fıkrasında yer alan fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde cezanın yarı oranında arttırılacağı düzenlenerek nitelikli hale yer verilmiştir.

Kanun koyucu nitelikli halin uygulanmasını yalnızca banka veya kredi kurumu ya da kamu kurum ve kuruluşlarıyla sınırlamıştır. Bu sınırlamanın yerinde olmadığını düşünüyoruz. Çünkü bir şirket veya işletme açısından da sistemin işleyişinin engellenmesi çok fazla önem taşıyabilir. Dolayısıyla da sınırlamanın sadece belirtilen kurumlarla ve kuruluşlarla ilgili yapılmaması gerekirdi. Ayrıca sabit artırım sisteminin kabul edilmesi de doğru olmamıştır. Artırım miktarında alt ve üst sınırın kabul edilmesi gerekirdi. Zira yukarıda belirtilen fiillerin gerçekleştirildiği bilişim sistemlerinin ve verilerin ait olduğu kurum ve kuruluşlar veya şirketlerin göz önüne alınması gerekirdi. Sistemler veya veriler farklı önemde olabilir ve verilen zararlar da farklı nicelikte olabilir. Doğrusu alt ve üst sınırlar arasında artırım miktarının belirlenmesi ve bu aralıklar arasında artırım yapılması noktasında hakime yetki verilmesinin kabul edilmesidir. Ayrıca sistemin işleyişinin engellenmesi ile verilere müdahale teşkil eden eylemler aynı ölçüde zarar verme niteliğinde değildir. Bunun dışında sistemin işleyişinin engellenmesi uzun süre devam edebilir. Artırım yapılırken bu hususların da göz önüne alınması gerekir. Bunlar dikkate alınmadan belirtilen kurum veya kuruluşların sistemlerinde gerçekleştirilen tüm fiillere aynı artırım oranını uygulamak yerinde bir tercih olmamıştır. Bunların dışında nitelikli halin kabul edilmesi yerinde olmuştur. Zirai kişisel bilgisayarını kullanan kişinin sisteminin işlemesinin engellenmesiyle veya verilerin kullanılmasının engellenmesiyle, bir bankanın veya kamu kurum ve kuruluşun sisteminin işlemesinin engellenmesi veya verilerine müdahale edilmesi aynı şey değildir. Özellikle belirtilmelidir ki kişisel bilgisayarlar için sistemin işlemesine engel olmanın uygulaması çok sınırlıyken, asıl düzenleme amacını oluşturması gereken bankalar veya kuruluşlar için aynı şey söylenemez. Onların sistemlerinin işlemesinin engellenmesinden doğan zararlar kişilere oranla çok büyük miktarlara ulaşabilmektedir. Örneğin merkezî bir bilgisayarın bulunduğu ve verilerin iletildiği bir

sistemde, iletimin yapılmasını sağlayan cihazın bozulması durumunda, veriler zarar görmemekle birlikte sistemin işlemesine engel olunmakta ve dolayısıyla sistemin sahibi kuruma oldukça büyük zarar verilebilmektedir.

Fıkrada geçen kamu kurumları[98] veya kuruluşları ifadesi merkezi idare, yerel yönetimler ve hizmet yerinden yönetim kuruluşları da dâhil olmak üzere tüm idari kuruluşların karşılığı olarak kullanılmaktadır[99]. Yani tüzel kişiliği olan, olmayan tüm idari kuruluşlar için geçerli bir kavramdır[100]. Cumhurbaşkanlığı, Başbakanlık, bakanlık gibi asli, Devlet Planlama Teşkilatı, Milli Güvenlik Kurulu, Sayıştay gibi yardımcı kuruluşlar; il ve ilçe idaresi, bölgesel örgütler şeklinde gruplandırılan merkezi idare, il özel idaresi, belediye idaresi, büyük şehir belediyesi, köy idaresi gibi yerel yönetimler, Vakıflar Genel Müdürlüğü, Karayolları Genel Müdürlüğü, Devlet Su İşleri Genel Müdürlüğü, Sosyal Hizmetler ve Çocuk Esirgeme Kurumu Genel Müdürlüğü, Orman Genel Müdürlüğü, T.C. Ziraat Bankası Genel Müdürlüğü, Devlet Malzeme Ofisi Genel Müdürlüğü, Makine ve Kimya Endüstrisi Kurumu, T.C. Sosyal Güvenlik Kurumu, Basın İlan Kurumu, TÜBİTAK, Türkiye Radyo ve Televizyon Kurumu, Üniversiteler gibi hizmet yerinden

---

98 Kamu kurumları kavramı, İdare Hukukunda tüm idari kuruluşlar için değil hizmet yerinden yönetim kuruluşları için kullanılan bir ifadedir: Özay, İl Han, Gün Işığında Yönetim, İstanbul 2002, s. 131; Günday, Metin, İdare Hukuku, 9. Baskı, Ankara 2004, s. 464.

99 İdare Hukukunda kamu kurumları ile kamu idareleri arasında yapılan ayrımın anayasal veya yasal dayanağı olmadığı için çeşitli mevzuatlarda (Ceza Kanunu gibi) kullanılan kamu müesseseleri kavramının çoğunlukla tüm idari kuruluşlar karşılığı olarak kullanıldığı belirtilmektedir. Günday, s. 464.

100 Tüzel kişiliği olanlar için kamu kurumu bu özelliği sahip olmayan örgütler içinse (Danıştay, Sayıştay, Devlet Denetleme Kurulu gibi) kamu kuruluşu kavramı da kullanılmaktadır. Ancak kamu kuruluşu kavramının hukuksal bir tanımı bulunmadığı yapılan ayrımın doktrinde göz önünde bulundurulabilecek bir öneri olduğu da ifade edilmektedir. Özay, s.132,133.

yönetim kuruluşları ve bağımsız idari kurumlar[101] 235. maddede geçen kamu kurum veya kuruluşları kapsamına girmektedir.

Nitelikli halin uygulanmasını sağlayan banka kavramı ise, mevduat bankaları ve katılım bankaları ile kalkınma ve yatırım bankalarını ifade etmektedir (Bankacılık Kanunu m.3). Kredi kurumu ise, mevduat bankalarını ve katılım bankalarını belirtmek için kullanılmaktadır (Bankacılık Kanunu m. 3). Tanımlamada geçen bankaların ne anlama geldiği de yine bankacılık kanununda düzenlenmiştir. Buna göre, mevduat bankası, bu Kanuna göre kendi nam ve hesabına mevduat kabul etmek ve kredi kullandırmak esas olmak üzere faaliyet gösteren kuruluşlar ile yurt dışında kurulu bu nitelikteki kuruluşların Türkiye'deki şubelerini; katılım bankası, bu Kanuna göre özel cari ve katılma hesapları yoluyla fon toplamak ve kredi kullandırmak esas olmak üzere faaliyet gösteren kuruluşlar ile yurt dışında kurulu bu nitelikteki kuruluşların Türkiye'deki şubelerini; kalkınma ve yatırım bankası ise, bu Kanuna göre mevduat veya katılım fonu kabul etme dışında; kredi kullandırmak esas olmak üzere faaliyet gösteren ve/veya özel kanunlarla kendilerine verilen görevleri yerine getiren kuruluşlar ile yurt dışında kurulu bu nitelikteki kuruluşların Türkiye'deki şubelerini ifade etmektedir (Bankacılık Kanunu m. 3).

V. TEŞEBBÜS

Türk Ceza Kanununun 244. maddesinin 1. ve 2. fıkralarında düzenlenen suçlarda teşebbüs gerçekleşebilir. Örneğin, failin sisteme yerleştirdiği bir virüs programının harekete geçer geçmez sistem sahibi tarafından fark edilerek, verilerde bir zarar oluşmadan veya müdahale olmadan virüsün yok edilmesi durumunda, fiil teşebbüs aşamasında kalmıştır. Keza kurulan virüs programları aracılığıyla sisteme girilen virüsün yok edilmesi durumunda teşebbüs söz konusudur. Yine DoS saldırısının fark edilip failin sistemin işleyişini engelleyememesi halinde fiil teşebbüs halinde kalmıştır.

TCK'nın 244. maddesinin 1. ve 2. fıkralarında yer verilen suçlardaki maddi unsura ilişkin yapılan belirlemeler seçimlik olarak sayıldığından herhangi birisinin gerçekleşmesi durumunda diğer seçimlik

[101] Hizmet yerinden yönetim, merkezi idare ve yerel yönetimler için bkz.: Günday, s. 353 vd.

belirlemeler teşebbüs halinde kalsa bile suç gerçekleşmiş sayılır. Örneğin, fail verilerin tamamını silmek isterken kısmi silmeyi gerçekleştirmişse, verilerin değiştirilmesi gerçekleştirilmiştir.

VI. İŞTİRAK

Türk Ceza Kanununun 244. maddesinde yer verilen suçlarda, faille ilgili özel bir belirleme yapılmamıştır. Dolayısıyla iştirak açısından TCK'nın 37 vd. maddeleri uygulanacaktır. Bu suçlarda iştirak şekillerinin gerçekleşmesi mümkündür.

VII. İÇTİMA

Sistemi engelleme, bozma, verileri yok etme veya değiştirme suçlarının zincirleme suç şeklinde işlenmesi mümkündür. Aynı kişiye karşı bir suç işleme kararıyla değişik zamanlarda gerçekleştirilmesi durumunda zincirleme suç kuralları uygulanacaktır. Nitekim Yargıtay verdiği bir kararda, "sanığın hizmetli olarak çalıştığı bankanın bilgisayar sistemine girerek usulüne uygun açılmış bir maaş kredi limitli bankomat 7/24 hesabı açması eylemi TCK'nın 525 b maddesinin 1. fıkrasında yazılı suçu oluşturur. Sanık bir suç işleme kararı ile Yasanın aynı hükmünü iki ayrı eylemle ihlâl ettiğinden teselsül uygulanmalıdır" gerekçesiyle yerel mahkemenin kararını bozmuştur[102].

Bir bilişim sisteminin işleyişinin engellenmesi veya bozulması suçu ile bilişim sistemindeki verilerin bozulması, yok edilmesi, değiştirilmesi veya erişilmez kılınması, sisteme veri yerleştirilmesi, var olan verilerin başka yere gönderilmesi suçu birlikte gerçekleşebilir. Örneğin verilerin yok edilmesi veya değiştirilmesi sonucunu doğuran hareket aynı zamanda sistemin işleyişinin engellenmesi neticesini de gerçekleştirmiş olabilir. Bu durumda sorun fikri içtima (TCK m. 44) hükümlerine göre çözümlenmelidir. Tek fiille farklı suçlar gerçekleştirilmiştir. Ancak doktrinde verilerin yok edilmesi veya değiştirilmesi veya bozulması veya erişilmez kılınması veya sisteme verilerin ilave edilmesi sitemin işleyişinin engellenmesi sonucunu doğurmuşsa 244. maddenin 2. fıkrasının değil, 1. fıkrasındaki suçun oluşacağını belirtmektedirler. 2. fıkradaki suçun oluşması için verilere

[102] 11. CD, 2.12.1997, 5052/6536, YKD, 1999, C. 25, S. 7, s. 1017,1018.

müdahale niteliği taşıyan hareketin bilişim sisteminin işleyişini engelleme boyutuna ulaşmaması gerektiğini ifade etmektedirler[103].

Ceza Kanunumuzun 244. maddesinin 1. ve 2. fıkrasındaki suçların, 4. fıkradaki bilişim sistemleri aracılığıyla hukuka aykırı çıkar sağlamak suçu arasındaki ilişki ise fiil tekliği ilişkisidir. Birden fazla fiil ve birden fazla suç bulunmayıp tek fiil ve tek suç bulunmaktadır. Çünkü 1. ve 2. fıkrada yer verilen fiiller 4. fıkradaki suçun unsuru niteliğindedir. Dolayısıyla verilere müdahale ederek veya sistemin işleyişini bozarak veya engelleyerek çıkar sağlayan kişi yalnızca 4. fıkradan cezalandırılacaktır[104].

Verilere veya veri işleme zarar vermek suçu ile TCK'nın 151. maddesindeki mala zarar verme suçu arasındaki ilişki ise, farklı alternatiflere göre incelenmesi gereken bir husustur. Örneğin failin bilişim sistemine zarar vermek suretiyle verileri de yok etmişse veya verileri bozmuşsa veya veri işlem yapılmasına engel olmuşsa içtima ilişkisinin ortaya konulması gerekir. Çünkü bu durumda fail, hem mala zarar verme suçunu hem de 244. maddeyi ihlâl etmiştir. Eğer fail, kendine ait bilişim sistemine zarar vermek suretiyle, sistemde bulunan başkasına ait verilere de zarar vermişse kendi malına zarar vermesi mala zarar verme suçunu oluşturmadığından yalnızca m. 244/2'yi ihlal etmiştir. Zira m. 151'e göre, suçun oluşması için başkasına ait taşınır veya taşınmaz mala zarar verilmesi gerekmektedir. Buna karşılık fail, başkasının mülkiyetinde olan bir sisteme zarar vermek suretiyle verileri yok etmişse hem mala zarar verme suçunu hem de m. 244/2'yi ihlal etmiştir. Suçlar tek fiille gerçekleştirildiğinden fikrî içtima hükümlerine göre sorumluluğun tayini gerekecektir. Keza sistemin başkasına ait, içindeki verilerin bir başkasına ait olması durumunda da aynı şey geçerlidir[105].

---

103 Koca/Üzülmez, s. 829; Karagülmez, s. 190.

104 Koca/Üzülmez, s. 833.

105 Aynı yönde Möhrenschlager, s. 142; Ersoy, s. 177; Tröndle/Fischer, § 303 a, kn. 16, § 303 b, kn. 19; Samson, SK, § 303b, s. 7, 8; Sondermann, s. 81, 82, 129; Schulze Heiming, s. 226; Lenckner /Winkelbauer, s. 831. Farklı düşünce için bkz. : Lackner /Kühl, § 303 a, kn. 7, § 303 b, kn. 10;

Failin verilere müdahale etmek (verileri değiştirmek veya veri yerleştirmek veya verileri yok etmek gibi) suretiyle sahte belge düzenlemesi halinde de fikri içtima kuralları gereğince en ağır cezayı gerektiren suçtan sorumlu olacaktır[106]. Doktrindeki bazı yazarlar ise bu durumda gerçek içtimanın uygulanacağını belirtmektedirler[107].

Türk Ceza Kanununun 244. maddesinde düzenlenen suçlar ile 243. maddede hükme bağlanan bilişim sistemine girme suçu arasında da fikri içtima kuralları uygulanmalıdır[108]. Doktrinde belirtilen durumda geçitli suç belirlemesi yapanlar olduğu gibi[109], failin kastına göre hangi suçun oluştuğunun belirlenmesi gerektiğini ifade edenler[110] ve gerçek içtimanın söz konusu olduğunu kabul edenler de[111] bulunmaktadır.

Türk Ceza Kanununun 244. maddesinde ifade edilen bilişim sisteminin işleyişinin engellenmesiyle haberleşmenin engellenmesi (TCK m. 124) de gerçekleştirilmiş olabilir. Tek fiille farklı suçların gerçekleştirilmesi söz konusu olduğundan fikri içtima kuralları uygulanmalıdır[112]. Aynı şekilde m. 136 ile m. 244 arasında da fikri içtima söz konusu olabilir.

Türk Ceza Kanununun 245/A maddesinde bilişim suçlarının düzenlendiği bölümde yer alan suçların işlenmesi için hazırlık hareketlerinin yapılması bağımsız suç olarak düzenlenmiştir. Dolayısıyla 244. maddede yer verilen suçların işlenmesi için bir cihazın, bilgisayar

---

Hilgendorf, 1996, Heft 12, s. 108; Yazıcıoğlu, s. 266; Malkoç/Güler, s. 4761.

106 Akbulut, s. 214.

107 Artuk/Gökcen/Yenidünya, s. 889.

108 Lackner/Kühl, § 303 a, kn. 7; Kindhäuser/Neumann/Paeffgen , § 303 a, kn. 20; Stree/Hecker-Schönke/Schröder, § 303 a, kn. 14; Koca/Üzülmez, s. 819.

109 Artuk/Gökcen/Yenidünya, s. 884.

110 Yazarlar geçitli suçun oluştuğunun söylenebileceğini belirtmekle beraber bu kurumu kabul etmediklerini, dolayısıyla kasta göre sorunun çözülebileceğini ifade etmektedirler: Özbek/Doğan/Bacaksız/Tepe, s. 942.

111 Meran, s. 368

112 Özbek/Doğan/Bacaksız/Tepe, s. 961.

programının, şifrenin veya sair güvenlik kodunun yapılması veya oluşturulması durumunda, bunları imal eden, ithal eden, sevk eden, nakleden, depolayan, kabul eden, satan, satışa arz eden, satın alan, başkalarına veren veya bulunduran kişi 245/A maddesiyle cezalandırılacaktır. Ayrıca fail TCK'nın 244. maddesindeki suçları da işlemişse gerçek içtima hükümleri uygulanacaktır.

VIII. YAPTIRIM VE KOVUŞTURMA

A. Yaptırım

1. Genel Olarak

Kanun koyucu bilişim suçlarını 1991 yılında 3756 sayılı Kanun'la yaptırıma bağlarken, mala zarar verme suçunda kabul ettiği esası, sabotaj ve verilere müdahale teşkil eden fiillerin aynı fıkrada aynı suç kapsamında düzenlediği 525/ b-1 açısından da benimsemiş ve cezasını hem hürriyeti bağlayıcı ceza hem de para cezası olarak öngörmüştür. Kanun koyucu bu belirlemeyi yaparken bilişim suçunun niteliğinden hareket etmiş, söz konusu suçun cezası ile klâsik anlamdaki benzerinin cezası arasında paralellik kurmuştur. 5237 sayılı Kanunda sabotaj fiilleri ile verilere müdahale teşkil eden fiilleri farklı fıkralarda ayrı suçlar olarak düzenlemiş, mala zarar verme suçunda kabul ettiği esası benimsememiş ve suçların cezasını yalnızca hapis cezası olarak düzenlemiş, para cezasına yer verilmemiştir. Oysa mala zarar verme suçunda hapis cezası ile adli para cezası seçimlik olarak öngörülmüştür. Kanaatimizce hapis cezası ile adli para cezasının seçimlik olarak öngörülmesi suçların niteliği açısından daha doğru olurdu. Alt sınır yönünden de fark yaratılmış, mala zarar verme suçunun alt sınırı 4 aydan başlarken verilere yok etme veya değiştirme suçunun alt sınırı 6 aydan başlamaktadır.

Getirilen cezaların türü ve miktarı ne olursa olsun suçların önlenmesi açısından yeterli olduğunu söylemek mümkün değildir. Bu, hem suçların niteliği açısından hem de takibi bakımından geçerlidir. Suçların çoğunlukla uzman kişiler tarafından gerçekleştirilmesi ve tespitinin zor olması, farklı ülkelerden işlenebilmesi kişilerin suç işlemesini engelleyeceği yerde arttırmaktadır. Ayrıca suçların adliyeye bildirilmesinde karşılaşılan sorunlar da suçların ve suçluların tespitinde olumsuz bir etken olarak karşımıza çıkmaktadır. Bilişimi suçlarının sayısı

ve zarar miktarı her geçen gün artmakla beraber, bunların çok az bir kısmı kovuşturma makamlarına ihbar edilmektedir. Bankalar ve ünlü firmalar bu tür olayları branşlarında ve müşterilerinin yanında güvenilmez iş ortağı ününü almamak için saklamakta ve sorunu kendi bünyeleri içinde halletmek yolunu tercih etmektedirler. Keza bu suçların bazen tesadüfen ortaya çıkması da suçların bilinmemesi açısından önemli bir etkendir. Belirtilen nedenlerle kovuşturma makamlarına çok az intikal eden bilişim suçlarının, "aysbergin zirvesini" oluşturduğu ifade edilmektedir[113]. Nitekim Amerika Birleşik Devletleri'nde 1997 ve 1998 yıllarının mart aylarında San Francisco'daki Bilgisayar Güvenlik Enstitüsü (The Computers Security Institute CSI) tarafından 500'ün üzerinde kuruluşla yapılan iki araştırmada[114], bilişim suçlarının işlenme oranlarının her geçen yıl daha fazla arttığı, bunların çok az kısmının adliyeye intikal ettiği ortaya çıkmıştır. 1998 yılındaki araştırmada, kuruluşların ancak % 17'sinin aleyhlerine işlenen bilişim suçlarını adliyeye bildirdikleri anlaşılmıştır.

2. Ceza

Türk Ceza Kanununun 244. maddesinde, bir bilişim sisteminin işleyişini engelleyen veya bozan kişinin, bir yıldan beş yıla kadar hapis cezası ile cezalandırılması kabul edilmiştir (f. 1). Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişinin ise, altı aydan üç yıla kadar hapis cezası ile cezalandırılması hükme bağlanmıştır (f. 2). Doktrinde suçların alt sınırlarının, işlenme sıklığı ve verdiği zararların ağırlığı göz önünde tutulduğunda az olduğu ifade edilmektedir[115].

Sistemi engelleme, bozma, verileri yok etme veya değiştirme fiillerinin bir banka veya kredi kurumuna ya da bir kamu kurum veya

---

113 Frey, Silvia, Computerkriminalität in eigentums – und vermögensstrafrechtlicher Sicht, München 1987, s. 17-19.

114 Communications Media Center at New York Law School: "Computer Crime Survey Released" (March 6, 1997), "Watch Group Reports Computer Crime Booming" (March 5, 1998), http:\\www.cmcnyls.edu\public\bullentins\CSISurv.htm.

115 Koca/Üzülmez, s. 833.

kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılacaktır. Daha önce de belirttiğimiz gibi bu belirleme hem sabit artırım oranının kabul edilmesi hem de yalnızca bazı kuruluşların belirtilmesi açısından yerinde olmamıştır.

B. Kovuşturma

Türk Ceza Kanununun 244. maddesinin 1. ve 2. fıkrasında yer alan suçlar resen takip edilen suçlardandır. Resen takip edilen bu suçların davasına, suçtan zarar gören kişilerin katılması mümkündür. Mağdur, suçtan zarar gören gerçek veya tüzel kişiler kamu davasına katılabilirler (CMK m. 237).

Bilişim suçlarının bazen şikâyet üzerine kovuşturulması mümkün olabilmektedir. Örneğin, yabancı bir ülkede bilişim suçlarından birini işleyen Türk vatandaşı failin daha sonra Türkiye'ye gelmesi durumunda, suçun takibi şikâyet üzerine yapılacaktır. Bu halde vatandaş iade edilmeyeceğinden, Türkiye'de yargılanması gerekmektedir. Türk Ceza Kanununun 11. maddesine göre, Bir Türk vatandaşı, 13. maddede yazılı suçlar dışında, Türk kanunlarına göre aşağı sınırı bir yıldan az olmayan hapis cezasını gerektiren bir suçu yabancı ülkede işlediği ve kendisi Türkiye'de bulunduğu takdirde Türk kanunlarına göre cezalandırılacaktır. Bu halde soruşturma ve kovuşturma yapılması şikayete bağlı değildir. Ancak suçun cezası, bir yıldan az hapis cezasını gerektirdiğinde resen soruşturma ve kovuşturma yapılamamakta, suçtan zarar görenin veya yabancı hükûmetin şikayeti gerekmektedir. (TCK m. 11/2). Bu durumda şikayet, vatandaşın Türkiye'ye girdiği tarihten itibaren altı ay içinde yapılmalıdır. Ceza Kanunumuzun 244. maddesinin 2. fıkrasındaki suçun cezası da altı aydan başladığından, alt sınır bir yıldan az olduğundan resen soruşturma ve kovuşturma yapılamayacak, suçtan zarar görenin veya yabancı hükümetin şikayeti aranacaktır. Dolayısıyla yabancı ülkede suç işleyip Türkiye'ye gelen Türk vatandaşı fail hakkında şikayet gerçekleşirse soruşturma ve kovuşturma yapılıp cezalandırılması söz konusu olacaktır. Yabancı ülkede işlenen suç, bilişim sisteminin işleyişinin engellenmesi veya bozulması suçu ise, bu suçun cezasının alt sınırı bir yıldan başladığından resen takibat yapılacaktır.

Görevli mahkeme, Adlî Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanunun 11. ve 12. maddeleri gereğince asliye ceza mahkemesidir.

Yetkili mahkeme ise CMK m. 12 gereğince suçun işlendiği yer mahkemesidir. Suçun işlendiği yer ise TCK m. 8'e göre belirlenecektir. Bu maddeye göre hareketin kısmen veya tamamen işlendiği veya neticenin gerçekleştiği yer suçun işlendiği yerdir. Dolayısıyla hareketin veya neticenin gerçekleştiği yerlerdeki mahkemeler yetkili mahkemelerdir. İnceleme konumuz olan suçlarda yer verilen unsurların çoğu, netice kapsamında yer aldığından hem bu neticelerin gerçekleştirildiği yerler hem de bu neticeleri gerçekleştiren hareketlerin yapıldığı yerler suçun işlendiği yerlerdir. Örneğin bilişim sisteminin işleyişinin engellenmesi veya bozulması veya sistemdeki verilerin yok edilmesi veya bozulması veya değiştirilmesi fiilleri netice kapsamında olduğundan hareketin veya neticeden birinin Türkiye'de gerçekleştirilmesi suçun işlendiği yerin Türkiye olması ve oradaki mahkemenin yetkili olması için yeterlidir. Buna karşılık verilerin başka yere gönderilmesinde suçun işlendiği yer ve yetkili mahkeme harekete göre belirlenecektir. Hareket gerçekleştirildiği yer, kişinin beden olarak bulunduğu yeri ifade etmektedir. Ancak hareket yeri, beden olarak bulunulan yer dışında hareketin aynı anda ortaya çıktığı yer veya hareketin kısımlara bölündüğü yeri de kapsamaktadır. Bilişim suçlarında kişinin beden olarak bulunduğu yer ile hareketin açığa çıktığı yerler çoğunlukla farklı yerlerdir. Bu nedenle her iki yer de hareket yeridir. Bir başka ifadeyle bilgisayar aracılığıyla interneti kullanan kişinin bu sırada fiziki olarak bulunduğu yer ile üzerinde suç teşkil eden hareketin gerçekleştirildiği amaç aracın bulunduğu yer birbirinden farklı olduğundan her iki yer de hareket yeridir. Her iki yerde de hareket gerçekleştirilmektedir[116]. Ancak doktrinde hareket ile neticenin farklı yerlerde gerçekleştirildiği suçlarda suçun işlendiği yerin tespitinin güçleştiği, hareketin gerçekleştirildiği yer tespit edilebiliyorsa yetkili mahkemenin hareketin gerçekleştirildiği yer mahkemesinin olması gerektiği, hareketin gerçekleştirildiği yer tespit edilemiyorsa neticenin gerçekleştiği yer mahkemesinin yetkili kabul edilmesi gerektiği ifade edilmektedir[117]. Ancak bu belirleme TCK'nın 8. maddesinin yaptığı

---

[116] Bu tespitle ilgili olarak bkz.: Özbek, Veli Özer, "İnternet Kullanımında Ortaya Çıkabilecek Bazı Ceza Hukuku Sorunları", DEÜHFD, 2002, C. 4, S. 1, s. 126, 127.

[117] Özbek/Doğan/Bacaksız/Tepe, s. 962.

düzenlemeye uygun değildir. Ülke içinde işlenmiş suçlarla ilgili ifade edildiği anlaşılan tespitin 8. maddeye uygun olarak hem hareket yeri hem de netice yeri esas alınarak yetkili mahkemenin belirlenmesi gerektiği düşünülmektedir. Ayrıca bu tespit farklı ülkelerle bağlantılı Türkiye'de (örneğin hareketin Almanya'da neticenin Türkiye'de gerçekleştiği) işlenen suçlar açısından da doğru sonuç vermeyecektir. Hareket veya neticeden birinin Türkiye de gerçekleşmesi şartıyla gerçekleştiği yer mahkemesi yetkili mahkeme kabul edilmelidir.

SONUÇ VE ÖNERİLER

Ceza Kanunumuzun 244. maddesinde/1-2 düzenlenen sistemi engelleme, bozma, verileri yok etme veya değiştirme suçları siber suç sözleşmesinin gereğini yerine getirmek ve bu suçların ihlal ettiği hukuki değerleri korumak adına Kanunumuzda yer verilen ve 1991 yılından beri var olan düzenlemelerdir. Ancak kanun koyucu 5237 sayılı Kanunda bu düzenlemeleri yaparken bize göre yerinde olmayan belirlemeler yapmıştır. Aşağıda bu belirlemeler ve çözüm önerileri ifade edilecektir.

1. Fıkraların düzenleme sırasının doğru olmadığı düşünülmektedir. 1. fıkrada sisteme müdahale, 2. fıkrada verilere müdahale niteliği taşıyan fiillere yer verilmiştir. Sisteme müdahale fiilleri verilere müdahale etmek suretiyle de gerçekleştirildiğinden sıralama açısından önce verilere müdahale daha sonra sabotaj fiilleri düzenlenmeliydi.

2. TCK'nın 244. maddesinin 1. fıkrasındaki düzenleme kanunilik ilkesi açısından sorun doğuracak niteliktedir. Sistemin işleyişinin engellenmesinin veya bozulmasının hangi fiillerle gerçekleştirileceğinin belirlilik ilkesi açısından ortaya konulması gerekmektedir.

3. 244. maddenin 2. fıkrasında sisteme veri yerleştirme veya var olan verileri başka bir yere gönderme hareketlerinin düzenlenmesi de doğru bir tercih olmamıştır. Bu belirtilen hareketlerin fıkrada belirtilen diğer fiillerle bir ilgisi bulunmamaktadır. Düzenleme amacı da anlaşılamamaktadır. Kavramların ya sistemin işleyişinin engellenmesi veya bozulmasıyla ilgili yapılması ya da başka fıkrada veya başka bölüm ya da bölümlerde (kişisel veri, özel hayat, sır vb. niteliğinde olmasına göre) düzenlenmesi (veya değişikliğe gidilmesi) uygun olurdu. Eğer mevcut 244. maddede var olması isteniyorsa neyin amaçlandığının belirtilmesi gerekir. Mevcut düzenlemedeki verileri bozmak, yok etmek,

değiştirmek veya erişilmez kılmak için amaca yer verilmemesi doğru olmakla beraber, sisteme veri yerleştirmek veya var olan verileri başka bir yere göndermek açısından belirlemeye gidilmesi doğru olacaktır.

4. Kanun koyucunun nitelikli halin uygulanmasını yalnızca banka veya kredi kurumu ya da kamu kurum ve kuruluşlarıyla sınırlaması da eksik düzenleme niteliği taşımaktadır. Çünkü bir şirket veya işletme açısından da sistemin işleyişinin engellenmesi çok fazla önem taşıyabilir. Dolayısıyla da sınırlama sadece belirtilen kurumlarla ve kuruluşlarla ilgili yapılmamalıydı.

5. Ayrıca sabit artırım sisteminin kabul edilmesi de doğru olmamıştır. Artırım miktarında alt ve üst sınırların kabul edilmesi gerekirdi. Zira yukarıda belirtilen fiillerin gerçekleştirildiği bilişim sistemlerinin ve verilerin ait olduğu kurum ve kuruluşların veya şirketlerin aynı önemde olmadığı, dolayısıyla zararların aynı ölçüde olmadığı veya sistemin işleyişinin engellenmesi ile verilere müdahalenin aynı nitelikte bulunmadığı, ortaya çıkan zararların farklı miktarda olabileceği, sistemin işleyişinin engellenmesinin veya müdahalenin farklı sürelerde gerçekleştirilebileceği hususları göz önüne alınarak alt ve üst sınırlar arasında artırım oranı kabul edilmeliydi. Bunlar dikkate alınmadan belirtilen kurum veya kuruluşların sistemlerinde gerçekleştirilen tüm fiillere aynı artırım oranının uygulanmasının kabul edilmesi yerinde bir tercih olmamıştır.

6. Suçların karşılığı olan cezanın yalnızca hapis cezası olarak kabul edilmesi de fiillerin zarar verme yönü göz önüne alındığında doğru gözükmemektedir. Aynı nitelikte olan mala zarar verme suçunda olduğu gibi bu suçlarda da hapis cezasının yanında adli para cezası öngörülmeliydi.

KAYNAKLAR

Akbulut, Berrin, Türk Ceza Hukukunda Bilişim Suçları, Yayınlanmamış Doktora Tezi, Konya 2000.

Artuk, Mehmet Emin/Gökcen, Ahmet/Yenidünya, A. Caner, Ceza Hukuku, Özel Hükümler, Yenilenmiş Gözden Geçirilmiş 15. Bası, Ankara 2015.

Aydın, Emin D., Bilişim Suçları ve Hukukuna Giriş, Ankara 1992.

Babür, Zafer, Bilgisayarla İletişim, İstanbul 1995.

Dönmezer, Sulhi, Kişilere ve Mala Karşı Cürümler, Yeniden Gözden Geçirilmiş ve Yenilenmiş Onbeşinci Bası, İstanbul 1998.

Dreher, Eduard/Herbert, Tröndle, Strafgesetzbuch und Nebengesetze, Kommentar, 47., neubearbeitete Auflage von Otto Schwarz begründeten Werkes, München 1995.

Ersoy, Yüksel, "Genel Hukukî Koruma Çerçevesinde Bilişim Suçları", Yılmaz Günal'a Armağan, Ankara 1994, C. 49, S. 6-12, s. 149-183.

Frey, Silvia, Computerkriminalität in eigentums – und vermögensstrafrechtlicher Sicht, München 1987.

Gerhards, Thomas, Computerkriminalität und Sachbeschädigung, Mannheim 1993.

Güder, Gazi, Bilgi İşlem Terimleri Sözlüğü, İstanbul 1986.

Gürsel, Mayda/Gürsel, İhsan, Büyük Bilgisayar Terimleri Sözlüğü, Ankara 1991.

Haβ, Gerhard, Der strafrechtliche Schutz von Computerprogrammen, Rechtsschutz und Verwertung von Computerprogrammen, 2., völlig überarbeitete und erweiterte Auflage, Köln 1993.

Hilgendorf, Eric, "Grundfälle zum Computerstrafrecht", JuS, 1996, Heft 10, s. 890-894.

Hilgendorf, Eric, "Grundfälle zum Computersstrafrecht", JuS, 1997, Heft 4, s. 323-331.

Hilgendorf, Eric, "Grundfälle zum Computerstrafrecht", JuS, 1996, Heft 12, s. 1082-1084.

İçel, Kayıhan, Suçların İçtiması, İstanbul 1972.

Karagülmez, Ali, Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri, Ankara 2005.

Kindhäuser, Urs/Neumann, Ulfrid/Paeffgen, Hans-Ullric, Strafgesetzbuch, Band 3, 4. Auflage, Baden-Baden 2013.

Koca, Mahmut/Üzülmez, İlhan, Türk Ceza Hukuku, Özel Hükümler, Gözden Geçirilmiş ve Genişletilmiş 3. Baskı, Ankara 2016.

Kurtaran, Özlem Meltem/Çubukçu, Faruk, Ansiklopedik Bilgi İşlem Terimleri Sözlüğü, İstanbul 1991.

Lackner, Karl/Kühl, Kristian, Strafgesetzbuch, 21. Aufl., München 1995.

Lackner, Karl/Kühl, Kristian, Strafgesetzbuch, 28. Aufl., München 2014.

Lenckner, Theodor/Winkelbauer, Wolfgang, "Computerkriminalität - Möglichkeiten und Grenzen des 2. WiKG (III)", CR, 1986, Heft 12, s. 824-831

Malkoç, İsmail/Güler, Mahmut, Uygulamada Türk Ceza Kanunu, Özel Hükümler (C. 4), Ankara 1997.

Meran, Necati, Yeni Türk Ceza Kanununda Sahtecilik-Malvarlığı Bilişim Suçları ile Ekonomi ve Ticaret Alanında Suçlar, Ankara 2005.

Möhrenschlager, Manfred, "Das neue Computerstrafrecht", wistra, 1986, Heft 4, s. 128-142.

Otto, Harro, Grundkurs Strafrecht, Die einzelnen Delikte, 3. Auflage, Berlin/NewYork 1991.

Önder, Ayhan, Şahıslara ve Mala Karşı Cürümler ve Bilişim Alanında Suçlar, İstanbul 1994.

Özay, İl Han, Gün Işığında Yönetim, İstanbul 2002.

Özbek, Veli Özer, "İnternet Kullanımında Ortaya Çıkabilecek Bazı Ceza Hukuku Sorunları", DEÜHFD, 2002, C. 4, S. 1, s. 101-158.

Özbek, Veli Özer/Doğan, Koray/Bacaksız, Pınar/Tepe, İlker, Türk Ceza Hukuku, Özel Hükümler, Genişletilmiş ve Güncellenmiş 10. Baskı, Ankara 2016.

Özgenç, İzzet, Uygulamalı Ceza Hukuku, Çözümlü Örnek Olaylar ve Karar Tahlilleri, Gözden Geçirilmiş ve Genişletilmiş 2. Bası, İstanbul 1998.

Rudolphi, Hans Joachim/Horn, Eckhard /Samson, Erich , Systematischer Kommentar, Strafgesetzbuch, Besonderer Teil (Band 2), 4. Auflage, Neuwied/ Kriftel 1991.

Schönke, Adolf/Schröder, Horst, Strafgesetzbuch, Kommentar, 25., neubearbeitete Auflage von Theodor Lenckner/Peter Cramer/Albin Eser/Walter Stree, München 1997.

Schönke, Adolf/Schröder, Horst/Lenckner, Theodor/Cramer, Peter/Stree, Walter, Strafgesetzbuch, Kommentar, 28., neubearbeitete Auflage von Eser, Albin/Heine, Günter/Perron, Walter/Sternberg Lieben, Detlev/Eisele, Jörg/Bosch, Nikolaus/Hecker, Bernd/Kinzig, Jörg/ Schittenhelm, Ulrike, München 2010.

Schulze Heiming, Ingeborg, Der strafrechtliche Schutz der Computerdaten gegen die Angriffsformen der Spionage, Sabotage und des Zeitdiebstahls, New York 1995.

Sondermann, Markus, Computerkriminalität, Die neuen Tatbestände der Datenveränderung gem. § 303a StGB und der Computersabotage gem. § 303 b StGB, Münster 1989.

Tezcan, Durmuş/Erdem, Mustafa Ruhan/Önok, Murat, Teorik ve Pratik Ceza Özel Hukuku, Güncellenmiş 13. Baskı, Ankara 2016.

Tröndle, Herbert/Fischer, Thomas, Strafgesetzbuch und Nebengesetze, 53. Auflage, München 2006.

Wessels, Johannes, Strafrecht, Besonderer Teil/2, Straftaten gegen Vermögenswerte, 20. , neubearbeitete Auflage, Heidelberg, 1997.

Wessels, Johannes/Hillenkamp, Thomas, Strafrecht, Besonderer Teil 2, Straftaten gegen Vermögenswerte, 39. Auflage, Heidelberg 2016.

Yarmalı, E. Sabri, Bilgisayar Terimleri Sözlüğü, İstanbul, (Birsen yayınevi), 1995.

Yazıcıoğlu, Yılmaz, Bilgisayar Suçları, Kriminolojik, Sosyolojik ve Hukukî Boyutları İle, İstanbul 1997.

Yenidünya, A. Caner/Değirmenci, Olgun, Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları, İstanbul 2003.

Yücel, Mustafa T., "Bilişim Suçları", ABD, 1992, Yıl 49, S. 1-6, s. 505-512.