BİLİŞİM SİSTEMİ ARACILIĞIYLA HAKSIZ YARAR SAĞLAMA SUÇU

EMRE İKBAL AÇIKGÖZ

TARAFINDAN

ANKARA YILDIRIM BEYAZIT ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜNE
SUNULAN TEZ

KAMU HUKUKU ANABİLİM DALI
YÜKSEK LİSANS TEZİ

HAZİRAN 2017

SOSYAL BİLİMLER ENSTİTÜSÜ ONAYI

Doç. Dr. Seyfullah YILDIRIM

Enstitü Müdür Vekili

Bu tezin yüksek lisans derecesi için gereken tüm şartları sağladığını tasdik ederim.

Prof. Dr. Yusuf Ziya TAŞKAN

Anabilim Dalı Başkanı

Okuduğumuz ve savunmasını dinlediğimiz bu tezin bir Yüksek Lisans derecesi için gereken tüm kapsam ve kalite şartlarını sağladığını beyan ederiz.

Yrd. Doç. Dr. Ömer ÇELEN

Danışman

JÜRİ ÜYELERİ

Prof. Dr. İlhan ÜZÜLMEZ
Gazi Üniversitesi Hukuk Fakültesi

Doç. Dr. Erdal YERDELEN
Ankara Yıldırım Beyazıt Üniversitesi Hukuk Fakültesi

Yrd. Doç. Dr. Ömer ÇELEN
Ankara Yıldırım Beyazıt Üniversitesi Hukuk Fakültesi

Bu tez içerisindeki bütün bilgilerin akademik kurallar ve etik davranış çerçevesinde elde edilerek sunulduğunu beyan ederim. Ayrıca bu kurallar ve davranışların gerektirdiği gibi bu çalışmada orijinal olmayan her tür kaynak ve sonuçlara tam olarak atıf ve referans yaptığımı da beyan ederim; aksi takdirde tüm yasal sorumluluğu kabul ediyorum.

Emre İkbal AÇIKGÖZ

ÖZET

BİLİŞİM SİSTEMİ ARACILIĞIYLA HAKSIZ YARAR SAĞLAMA SUÇU

AÇIKGÖZ, EMRE İKBAL
YÜKSEK LİSANS, KAMU HUKUKU
Tez Yöneticisi: Yrd. Doç. Dr. Ömer ÇELEN

Haziran 2017, 127 sayfa

Dijital teknolojideki baş döndürücü gelişme ve yenilikler, bilişim sistemlerinde de gerek nitelik gerekse nicelik boyutlarında kapsamlı değişim ve dönüşümlere yol açmış; bu gelişmelerin bir yan ürünü, deyim yerindeyse komplikasyonu ve yeni bir suç türü olarak bilişim suçları ortaya çıkmıştır. Gündelik hayatı kolaylaştıran vazgeçilmez unsurlar haline gelen bilişim sistemleri ne yazık ki suç işleme amacıyla kötüye de kullanılabilen elverişli araçlardır. Bu şekilde kötüye kullanımları engellemek üzere Türk Ceza Kanunu (TCK)'nda çeşitli bilişim suçları düzenleme altına alınmıştır. TCK madde 244, fıkra 4'te düzenlenen *"bilişim sistemi aracılığıyla haksız yarar sağlama"* da bu suçlardan biridir. Söz konusu suç, kanun koyucu tarafından, elde edilen haksız yararın başka bir suça vücut vermemesi durumunda uygulanacak şekilde düzenlenmiştir. Çalışmamızın amacı bu özellikli durum çerçevesinde söz konusu suçun uygulama alanını belirlemek; doktrine ve uygulamaya inceleme konusu suç türü bakımından bütüncül bir bakış açısı getirmektir.

Anahtar Kelimeler: *bilişim suçu, bilişim sistemi, haksız yarar sağlama, Türk Ceza Kanunu madde 244.*

ABSTRACT

THE CRIME OF UNFAIR BENEFIT THROUGH INFORMATION SYSTEM

AÇIKGÖZ, EMRE İKBAL
LL.M., Department of Public Law
Supervisor: Assis. Prof. Dr. Ömer ÇELEN

Haziran 2017, 127 sayfa

The dazzling developments and innovations in digital technology have caused comprehensive changes and transformations in both dimensions of quality and quantity also in information systems; as a by-product of these developments, so to say as a complication and as a new crime type, information crimes have arised. Information systems which became indispensable elements easening daily life, unfortunately are also convenient tools that can be misused for the purpose of committing crime. In order to prevent such misuses, various information crimes are put in order under Turkish Criminal Code (TCC). *"The crime of unfair benefit through information system"* regulated under article 244, paragraph 4 of TCC is also one of these crimes. The given crime is regulated by the law-maker in case to be implemented when the obtained unfair benefit is not creating another crime. The aim of this work is to define the scope of application of this given crime in frame of this specific situation; to bring a holistic view to the doctrine and application in regard to crime type as the research subject.

Keywords: *cybercrime, information system, unfair benefit, Turkish Criminal Code article 244.*

Anne ve Babama

TEŞEKKÜR

Değerli hocam ve tez danışmanım Yrd. Doç. Dr. Ömer ÇELEN'e araştırma sürecindeki rehberlikleri, tavsiyeleri, tenkitleri ve destekleri için şükranlarımı sunarım.

Bu çalışma, Ankara Yıldırım Beyazıt Üniversitesi Projeler Ofisi'nin 2017/3811 sayılı Lisansüstü Tez Projesi kapsamında desteklenmiştir.

İÇİNDEKİLER

KISALTMALAR LİSTESİ

AKSSS	Avrupa Konseyi Siber Suçlar Sözleşmesi
ARPANET	Advanced Research Project Authority Net
ATM	Automated Teller Machine
BKKK	Banka Kartları ve Kredi Kartları Kanunu
BM	Birleşmiş Milletler
bkz.	bakınız
CD	Ceza Dairesi
Çev.	Çeviren
E.	Esas
DDoS	Distributed Denial of Service
FSEK	Fikir ve Sanat Eserleri Kanunu
GPS	Global Positioning System
G8	Sekizler Grubu
IOT	Internet of Things
IP	Internet Protocol
K.	Karar
LAN	Local Area Network
m.	Madde
MILNET	Military Network
OECD	The Organisation for Economic Co-operation and Development
POS	Point of Sale
RFID	Radio-frequency identification
s.	Sayfa
s.e.t.	Son erişim tarihi
SSD	Solid State Disk
T.	Tarih
TBMM	Türkiye Büyük Millet Meclisi
TDK	Türk Dil Kurumu

TCK	5237 sayılı Türk Ceza Kanunu
TCP	Tranmission Control Protocol
Y.	Yargıtay
YCGK	Yargıtay Ceza Genel Kurulu
YKD	Yargıtay Kararları Dergisi
vd.	ve devamı
WAN	Wide Area Network

GİRİŞ

Teknolojik gelişmeler, geçmişten bugüne bir yandan insanların hayatını kolaylaştırırken diğer yandan insanlara zarar vermek isteyenler tarafından istismar edile gelmiştir. Günümüzde, bilişim sistemlerinin varlığı, insanlara iş ve gündelik hayatlarında büyük kolaylıklar sağlamaktadır. Özellikle dünyadaki bilişim sistemlerini birbirine bağlayan internet teknolojisi ile bilgiye erişim ve iletişim oldukça kolaylaşmıştır. Ancak aynı ağ üzerindeki siber dünyada para dahil her türlü değer ve bilginin depolanıyor oluşu, suç işleme niyetinde olan kimselere yeni fırsatlar sunmaktadır.

Bilişim sistemlerinin oluşturduğu siber dünyanın fiziki dünyadan ayrılan kimi özellikleri, söz konusu kimseler için uygun bir faaliyet ortamı sağlamaktadır. Öncelikle internetin tüm dünyayı saran bir ağ olması, siber dünyada ulusal sınırları önemsiz hale getirmektedir. Siber dünyanın olanaklarını kullanan faillerin suç işledikleri ülkede daha önce hiç bulunmamış olmaları dahi mümkündür. Ayrıca failler bulundukları ülkede suç işlemek istediklerinde dijital izlerini yok etmek için internetin olanaklarını kullanarak kendilerini bir başka ülkede gösterip *"anonimlik"* kazanabilmektedirler. Öte yandan siber dünya, suç işleme niyetinde olan kimselere amaçlarını büyük çabalar sarf etmeksizin gerçekleştirme imkânı sunmaktadır. Failler, bilgisayarları başında otururak geliştirdikleri kimi yöntemlerle güvenlik açıklarından yararlanıp, bazen milyonlarca kişinin banka hesaplarındaki paraları kendi hesaplarına transfer etmekte, bazen de bilişim sistemleri ile çalışan cihazlara dünya çapında kriz yaratacak derecede zarar verebilmektedirler[1].

Siber dünyanın sağladığı bu olanaklar kimi zaman sıradan bir suçlu tarafından, kimi zaman suç örgütleri ve teröristler tarafından, kimi zaman da devletler tarafından kullanılmaktadır. Ulus devletler artık siber dünyayı bir muharebe alanı olarak görmekte ve bu alanda savunma yatırımları yapmakta, siber ordular kurmaktadırlar. Öyle ki bununla ilgili olarak *"Harp Zamanında Sivillerin Korunmasına İlişkin 1949 tarihli Cenevre Sözleşmesi"*nden ilham

[1] Nitekim *"Goodman"*ın da belirttiği gibi: "*Her şey bağlantılı olduğunda herkes savunmasız hale geliyor."* (**Goodman, Marc**; Geleceğin Suçları, (C. Özdemir, Çev.) İstanbul 2016, s. 11)

alınarak, siber alanda da sivillerin korunmasına ilişkin uluslararası bir *"dijital Cenevre sözleşmesi"* imzalanması gerektiği ifade edilmektedir[2].

Bilişim sistemlerinin icadı ile ortaya çıkan siber dünyada; hırsızlık, dolandırıcılık, mala zarar verme, hakaret, tehdit gibi suçların işlenmesi mümkündür. Ayrıca bilişim sistemlerinin icadı ile söz konusu suçların yanı sıra bu dünyaya özgü – yeni, haksızlık teşkil eden davranışlar da ortaya çıkmış ve bu davranışlardan bazıları hukuk düzenlerince cezai yaptırım altına alınmıştır. Bu bağlamda, siber dünyada işlenen ve hukuk düzenlerince cezai yaptırım altına alınan bu haksız davranışlar, yeni bir suç türü olarak bilişim suçlarına vücut vermiştir.

Bilişim suçları, Türk Hukuku'nda ilk olarak 1991 yılında *"bilişim alanında suçlar"* başlığı altında 765 sayılı Türk Ceza Kanunu (TCK)'nda düzenleme alanı bulmuş ve aynı başlıkla bu suçlar 5237 sayılı yeni TCK'da da yerini almıştır. Bu çalışma kapsamında ele alınacak olan *"bilişim sistemi aracılığıyla haksız yarar sağlama suçu"* 5237 sayılı TCK'nın *"topluma karşı suçlar"* kısmında, *"bilişim alanında suçlar"* bölümünde, madde 244, fıkra 4'te düzenlenmiştir.

TCK'da hırsızlık, dolandırıcılık, güveni kötüye kullanma, zimmet gibi haksız yarar sağlamayı cezai yaptırım altına alan suçlar düzenlenmiştir. Bu bağlamda TCK m. 244/4'ün düzenlenme amacı, söz konusu suçlar bakımından tipiklik arz etmeyecek haksız yarar sağlamaya yönelik davranışları cezai yaptırım altına almaktır. Nitekim TCK m. 244/4'ün kanuni tanımında, işlenen fiil ile elde edilen haksız çıkarın başka bir suçu oluşturmaması halinde bu hükmün uygulanacağı düzenlenerek bu suça tali norm özelliği kazandırılmıştır.

Örneğin, bir bilişim sistemi vasıtasıyla; taşınır bir malı elde ederek ya da bir kimseyi hileli hareketlerle aldatarak, haksız bir yarar elde etmek mümkündür. Bu fiiller esasen malvarlığına karşı işlenen suçlardan olan hırsızlık ve dolandırıcılık suçları ile TCK'da cezai yaptırıma bağlanmıştır. Ancak bilişim sistemleri ile bir taşınır malı elde etmeksizin ya da bir kimseyi bu sistemlerle aldatmaksızın, bilişim sistemlerinin sağladığı kolaylıklardan istifade ederek haksız bir yarar elde edilmesi de mümkündür.

---

[2] **Smith, Brad**; "*The need for a Digital Geneva Convention*", Microsoft on the Issues, https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/, s.e.t: 30.05.2017.

TCK'da, bilişim sistemlerinin temel birimi ve bilginin *"makine dilinde"* ifade edilmiş biçimi olan *"veri"*ye müdahalede bulunarak bir haksız yarar sağlanmasının, malvarlığına karşı işlenen suçlar bağlamında cezai yaptırıma tabi tutulmadığı görülmektedir. Günümüzde bilginin ifade ettiği ekonomik değer göz önüne alındığında, bilişim sistemlerindeki veriler ile haksız bir yarar sağlanmasının cezai yaptırıma tabi tutulmaması düşünülemeyeceğinden, kanun koyucu bir boşluğu doldurmuş ve *"bilişim sistemi aracılığıyla haksız yarar sağlama suçu"*nu düzenlemiştir.

Çalışmamız iki bölümden oluşmaktadır: Birinci bölümde, inceleme konumuz olan suç açısından önem arz eden *"bilişim sistemi*" kavramı ve bununla bağlantılı kavramlar gözden geçirilmiş; genel olarak bilişim suçları ulusal ve uluslararası boyutuyla ele alınmıştır.

İkinci bölümde, *"bilişim sistemi aracılığıyla haksız yarar sağlama suçu"* bakımından korunan hukuki değer, suçun unsurları ile teşebbüs, iştirak ve içtima hususları ele alınmıştır. Bu bölümde, suçun tali norm oluşu dikkate alınarak, suçun uygulama alanının belirlenmesi amacıyla, içtima bahsi Yargıtay kararlarından örneklerle detaylıca incelenmeye çalışılmıştır. Son olarak bu bölümde inceleme konumuz olan suçun, bir bilişim suçu olmasına bağlı olarak ceza muhakemesi sürecinde ortaya çıkan özellikli durumlar ile yaptırım hususu ele alınmıştır.

BİRİNCİ BÖLÜM

BİLİŞİM SİSTEMLERİNE İLİŞKİN TEMEL KAVRAMLAR VE GENEL OLARAK BİLİŞİM SUÇLARI

1. BİLİŞİM SİSTEMLERİNE İLİŞKİN TEMEL KAVRAMLAR

1.1. Bilişim Kavramı

"Bilişim", genel olarak bilgisayarın icadı ile ortaya çıkan bir terimdir ve özel bir bilim dalını ifade eder[3]. Bilgisayarın icadı ile ortaya çıkan bu yeni bilim dalına ismini veren 1962 yılında fransız Philippe Dreyfus olmuştur. Dreyfus, "*information"* ve "*automatique"* kelimelerinden *"informatique"* kelimesini türeterek söz konusu bilim dalını ifade etmek üzere kullanmıştır[4]. Bu isim, 1967 yılında Fransız Akademisi tarafından da kabul görmüş[5], ardından diğer Avrupa ülkelerince de benimsenmiş[6] Türkçe'ye de *"enformatik"* olarak geçmiştir[7]. Ancak günümüz Türkçesi'nde söz konusu bilim dalı için bu isim yerine genel olarak *"bilişim"* kelimesinin tercih edildiği görülmektedir.

"Bilişim" ismi 1971'de, Hacettepe Üniversitesi'nden Prof. Dr. Aydın Köksal tarafından önerilmiştir[8]. Doktrinde *"bilişim"*in, *"bilim"* ve *"iletişim"* ifadelerinin kaynaştırılması ile

---

[3] **Aydın, Emin Doğan**; Bilişim Suçları ve Hukukuna Giriş, Ankara 1992, s. 3; **Dülger, Murat Volkan**; Bilişim Suçları ve İnternet İletişim Hukuku, Ankara 2015, s. 74; **Gürler, Fazıl**; Teknik ve Hukuksal Yönleriyle Bilişim Alanında Suçlar, Ankara 2015, s. 28-31; **Özbek, Veli Özer**; "*Banka Veya Kredi Kartlarının Kötüye Kullanılması Suçu (TCK m.245)*", Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, 2007, Cilt 9, Sayı Özel Sayı, s. 1023; **Taşkın, Şaban Cankat**; Bilişim Suçları, İstanbul 2008 s. 3–4; **Yenidünya, A. Caner/Değirmenci, Olgun**; Bilişim Suçları (Mukayeseli Hukukta ve Türk Hukukunda), İstanbul 2003, s. 27.

[4] **Ketizmen**, **Muammer**; Türk Ceza Hukukunda Bilişim Suçları, Ankara 2008, s. 10.

[5] **Ketizmen**, Bilişim Suçları, s. 10.

[6] İngilizce'de "*informatics",* Almanca'da "*informatiks",* İtalyanca'da ve İspanyolca'da "*informatica"* şeklinde ifade edilmiştir. (**Dülger**, Bilişim Suçları, s. 73; **Ifrah**, Bilgisayar Ne Sayar, s. 69.)

[7] **Nişanyan, Sevan**; Sözlerin Soyağacı: Çağdaş Türkçenin Etimolojik Sözlüğü, İstanbul 2009, s. 72.

[8] **Nişanyan**, Sözlerin Soyağacı, s. 72.

oluşturulduğunu ileri sürenler olmakla birlikte[9]; *"Köksal",* bilişim terimini, bilmek eyleminden dönüşlü/ işteş çatıyı kullanarak türettiğini belirtmiştir[10].

Bilişim terimi Türk Dil Kurumu güncel Türkçe sözlükte şu şekilde tanımlanmaktadır[11]: *"İnsanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimi, enformatik."*

Hukukçular tarafından bilişimin birden çok tanımı yapılmış olsa da esas itibariyle bu tanımlarda büyük bir farklılığa rastlanmaz[12]. Söz konusu tanımlardan yola çıkarak biz de bilişimi şu şekilde tanımlayabiliriz: Bilginin, elektronik sistemler vasıtasıyla elektronik hale/ elektronik veriye dönüştürülerek otomatik olarak işlenmesini, depolanmasını ve aktarılmasını konu alan bilim dalı.

---

9 **Özen, Muharrem/Baştürk, İhsan**; Temel Hak ve Özgürlükler Bağlamında Bilişim – İnternet ve Ceza Hukuku, Ankara 2011, s. 11.

10 **Köksal**, **Aydın**; Adı Bilgisayar Olsun, İstanbul 2010, s. 44.

11 www.tdk.gov.tr, s.e.t: 05.05.2017.

12 **Akbulut, Berrin**; "*Bilişim Suçları*", Selçuk Üniversitesi Hukuk Fakültesi Dergisi, 2000, Cilt 8, Sayı Milenyum Armağanı 1-2, s. 546: *"İnsanların 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 bilimidir.";*

Aydın, Bilişim Suçları ve Hukukuna Giriş, s. 3: *"Bilginin iletişim yapısı ve özellikleri; bilginin aktarılması, organize edilmesi, saklanması, tekrar elde edilmesi, değerlendirilmesi ve dağıtımı için gerekli kuram ve yöntemler ve öte yandan da; bilgiyi kaynağından alıp kullanıcıya aktaran ve genel sistem bilimi, sibernetik, otomasyon ile insanın çalışma çevrelerinde ki yerinde ve zamanında kullanılan teknolojileri temel alan bilgi sistemleri, şebekeleri, işlevleri, süreçleri ve etkinlikleridir. Kısaca, bu bilim ve teknoloji dalı bir veri işlem sürecidir.";*

Dülger, Bilişim Suçları, s. 73: *"Bilişim insanların teknik, ekonomik, siyasal ve toplumsal alanlardaki iletişiminde kullandığı bilginin, özellikle bilgisayar aracılığıyla düzenli ve akılcı biçimde işlenmesi, her türden düşünsel sürecin yapay olarak yeniden üretilmesi, bilginin bilgisayarda depolanması ve kullanıcıların erişimine açık bulundurulması bilimidir.";*

Gürler, Bilişim Alanında Suçlar, s. 30–31: *"İnsanlığın ortak mirası olarak binlerce yıl içinde ticari, teknik, ekonomik, hukuksal vb. tüm alanlarda üretebildiği ve bilimin ulaşabildiği her tür verinin, elektronik araçlarla, özellikle bilgisayarlar aracılığıyla elektronik/sayısal bir hale dönüştürülerek, düzenli ve akılcı bir biçimde toplanması, işlenmesi, kaydedilmesi, sınıflandırılması, saklanması, bilgi haline dönüştürülmesi ve tüm bu işlemlerin sonuçlarının doğrudan sunulmasını ya da ses, görüntü ve/veya veri taşıyabilen kablolu veya kablosuz iletişim hatları aracılığıyla aktarılmasını sağlayan bilim dalıdır.";*

Yazıcıoğlu, R. Yılmaz; Bilgisayar suçları: Kriminolojik, Sosyolojik ve Hukuki Boyutları ile, İstanbul 1997, s. 131: *"Bilişim bilgisayardan da faydalanmak suretiyle bilginin saklanması, iletilmesi ve işlenerek kullanılır hale gelmesini konu alan akademik ve mesleki disipline verilen addır.";*

Yenidünya/Değirmenci, Bilişim Suçları, s. 27: *"Bilişim; teknik ekonomik, sosyal, hukuki alandaki verinin, otomatik olarak işlenmesi saklanması, organize edilmesi, değerlendirilmesi ve aktarılması ile ilgili bilim dalıdır."*

Bilişim biliminin temel bir mühendislik alanı olarak konusu; verileri aktarabilen, depolayabilen ve algoritmalar yardımıyla verileri işleyebilen matematiksel makineler tasarlamaktır. Öte yandan yardımcı bir bilim dalı olarak da diğer bilimlerdeki olguların soyutlaştırıp algoritmalar yardımıyla işlenmesini mümkün kılar.[13]

1.2. Bilişim Sistemi ve Bilgisayar

*Dreyfus'*un *"informatique"* kelimesini türetişi/ tercih edişinin temelinde, bu bilim dalının esas olarak bilgilerin otomatik işleme tabi tutulması ile ilgileniyor oluşu vardır. Bilgilerin otomatik işleme tabi tutulması ise bilgisayarlar aracılığıyla gerçekleştirilebilen bir süreçtir.

Bilişim biliminin ortaya çıkmasında milat, denebilir ki, bilgisayarın icadıdır. Bilgisayar icat edilmeseydi böyle bir bilim dalından da bahsedilemezdi. Günümüzün modern bilgisayarları[14], kullanıcının bilgisayara girdiği bilgiyi farklı algoritmalardan geçirerek bir sonuca ulaşmakta ve bu süreç kullanıcı olmaksızın otomatik olarak gerçekleşmektedir.

Bilgisayarlar sadece elektrik sinyalleriyle çalışırlar. Bilgisayarın elektronik devreleri arasında 5 volt elektrik akışı olursa bu "1" olarak; hiç elektrik akışı olmazsa bu da "0" olarak algılanır. Bundan dolayı bilgisayarlarda işlem yapabilmek için ikilik sayı sistemine yani *"binary"* sistemine ihtiyaç vardır[15]. Bilgisayarların alfabesinde sadece 1'ler ve 0'lar bulunur; yani bilgisayarlar bütün işlemlerini 0 ve 1'leri yan yana getirerek yaparlar. Başka bir ifadeyle resimler, müzikler, videolar, yazılar; kısaca bilgisayar ekranında gördüğümüz her şey esasında 0 ve 1'lerin yan yana getirilmiş halidir. İşte bu 0 ve 1'ler makine dilini ifade ederler.[16]

Bilgisayarların temelde donanım ve yazılım olmak üzere iki bileşeni vardır. Donanım en basit ifadeyle bilgisayarın elle tutulabilen fiziksel kısımlarıdır[17]. Ekran, klavye, sabit disk, bellek, mikro işlemci gibi unsurlar bilgisayarın donanım bileşenine dahildir. Oysa yazılımlar bilgisayarın soyut yönünü oluştururlar ve belirli işlem veya işlemleri yapmak üzere

---

13 **Özbek**, Banka veya Kredi Kartlarının, s. 1023.

14 **Ören, Tuncer/Üney, Tuncer/Çölkesen, Rifat (Editörler)**; Türkiye Bilişim Ansiklopedisi, İstanbul 2006, s. 1030: ENIAC, elektrikle çalışan ve elektronik veri işleme kapasitesine sahip ilk bilgisayar olarak kabul edilmektedir. Amerika Birleşik Devletleri Ordusu için geliştirilen bu bilgisayar 167 m^2'lik bir alan kaplamaktaydı ve yaklaşık 30 ton ağırlığa sahipti.

15 **Karagülmez, Ali**; Bilişim Suçları ve Soruşturma – Kovuşturma Evreleri, Ankara 2014, s. 48.

16 Microsoft Açık Akademi, Eğitimler, https://www.acikakademi.com/portal/Course/12/bilgisayar-yazilim-ve-algoritma.aspx, s.e.t: 05.05.2017.

17 **Karagülmez**, Bilişim Suçları, s. 50.

bilgisayarlara kurulurlar[18]. Bir bilgisayarın kullanımı, temelde yazılımlara dayanır ve yazılımların oluşturulmasında özel bir dil kullanılır[19]. Bilgisayar, bu dili yukarıda açıklanan elektronik devreleri vasıtasıyla doğrudan uygulanabilen sınırlı bir komutlar dizisine çevirir. Bu anlamda bilgisayarın temel özelliği programlanabilmedir[20]. Dolayısıyla bilgisayarı, kısaca; *"aritmetik ve mantık işlem dizileriyle oluşturulmuş yazılımlara göre, verileri otomatik olarak işleyen makine"* olarak tanımlayabiliriz[21].

Elektromanyetik süreçlerden geçirilerek bilginin veri haline dönüştürülmesi ve otomatik işleme tabi tutulması işleminin bilgisayarlar aracılığıyla yapıldığını ifade ettik. Ancak özellikle hukuk literatüründe bilgileri otomatik işleme tabi tutan elektromanyetik araçlar için kullanılan ifadelerde bir birlik olmadığı görülmektedir.

Türk Hukuku'nda, ceza kanunlarına baktığımızda; 5237 sayılı Türk Ceza Kanunu'nda (TCK), 765 sayılı TCK'dan farklı olarak *"bilgileri otomatik işleme tabi tutan sistem"* ifadesi yerine *"bilişim sistemi"* ifadesi tercih edilmiştir. 765 sayılı TCK'daki ifade, Fransız Ceza Kanunu'ndaki ifadenin karşılığı olarak kullanılmıştır[22]. Fransa'da bilgisayar ifadesinin karşılığı olarak *"ordinateur"* ifadesi kullanılırken Fransız Ceza Kanunu'nda bunun yerine *"verileri otomatik işleme tabi tutan sistem"* ifadesi kullanılmıştır[23]. Avrupa Konseyi Siber Suçlar Sözleşmesi'nin (AKSSS) *"tanımlar"* başlıklı 1. maddesinde ise, *"bilişim sistemi"* terimi yerine *"bilgisayar sistemi"* terimi kullanılmış ve bu terim *"bir veya birden fazlası, bir program uyarınca otomatik veri işleyebilen herhangi bir cihaz veya birbiriyle bağlantılı veya ilgili bir grup cihazı ifade eder."* şeklinde tanımlanmıştır[24].

İnceleme konumuz olan, *"bilişim sistemi aracılığıyla haksız yarar sağlama* suçu"nda cezai sorumluluk açısından, bir bilişim sistemine müdahale ile haksız yarar sağlanması arandığı

---

18 **Karagülmez**, Bilişim Suçları, s. 50.

19 Yazılım dilleri: Düşük seviye: makine dili, assembly dili / Orta seviye: C, C# / Üst seviye: Visual Basic, Pascal (Microsoft Açık Akademi, Eğitimler, https://www.acikakademi.com/portal/Course/12/bilgisayar-yazilim-ve-algoritma.aspx, s.e.t: 05.05.2017.)

20 **Casey, Eoghan**; Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 3. bs., 2011, s. 87.

21 Büyük Larousse, Gelişim Yayınları, 1986; "*Bilgisayar*", s. 1639. TDK güncel sözlükte bilgisayar şu şekilde tanımlanmaktadır: *"Çok sayıda aritmetiksel veya mantıksal işlemlerden oluşan bir işi, önceden verilmiş bir programa göre yapıp sonuçlandıran elektronik araç, elektronik beyin."*

22 **Yazıcıoğlu**, Bilgisayar Suçları, s. 129.

23 **Erdoğan, Yavuz**; Türk Ceza Kanunu'nda Bilişim Suçları, İstanbul 2012, s. 12.

24 https://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss380.pdf, s.e.t: 02.05.2017.

için, öncelikle TCK'daki *"bilişim sistemi"* ifadesinin açıklığa kavuşturulması gerekmektedir.

Bilişimin bir bilim dalı olarak gelişmesi, bilgisayarın ortaya çıkışıyla aynı döneme denk geldiği için, bilgisayar ve bilişim genel olarak birlikte anılagelmiştir[25]. Ancak zaman içinde teknolojinin de gelişmesiyle *"bilgileri otomatik işleme tabi tutabilen"* yeni cihazlar ortaya çıkmış ve bilgisayar ifadesi bunları ifade etmekte yetersiz kalmıştır. *"Akıllı"* olarak nitelenen buzdolaplarını, televizyonları, tartıları, lambaları, prizleri yine aynı şekilde sesli yardım asistanlarını, kişisel sağlık takip cihazlarını, navigasyon cihazlarını ve cep telefonlarını bu cihazlara örnek olarak gösterebiliriz. Esas itibariyle bu cihazların çalışma mantıkları da bilgisayarlarla aynıdır[26]. Ancak bilgisayarlar dışında belli algoritmaya göre verileri işleyen diğer cihazlar, görecekleri fonksiyonlara göre özel bir programlama içerirken, bilgisayarlar genel programlama içerirler[27]. Öyle ki bir bilgisayar başka bir bilgisayarın çalışabilmesi için gerekli temel işletim sistemini oluşturabilirken, aynı işin söz konusu diğer cihazlar aracılığıyla yapılması mümkün değildir[28].

Bilişim sistemlerinin, doktrinde üç alt sınıfa ayrıldığı görülmektedir[29]. Bunlardan birincisi, açık bilgisayar sistemleri olarak isimlendirilen ve bilgisayar dediğimizde ilk aklımıza gelen, genel depolama diskleri, klavyeleri, monitörleri, fareleriyle günlük hayatta kullandığımız masaüstü veya taşınabilir bilgisayarlar ya da küçük ölçekli sunuculardır[30]. Dolayısıyla her bilgisayar bir bilişim siteminin parçası olduğu halde her bilişim sistem aygıtı bir bilgisayar değildir[31]. İkinci tür bilişim sistemleri ise iletişim teknolojisinin giderek dijitalleşmesi ve bilişim sistemlerinin iletişim amacıyla kullanılan iletişim araçlarına altyapı sağlamasının bir

---

[25] **Ketizmen**, Bilişim Suçları, s. 13: Örneğin; Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı md.2-d' de bilişim sistemi, *"Bilgisayar, çevre birimleri, iletişim altyapısı ve programlardan oluşan veri işleme, saklama ve iletmeye yönelik sistem"* olarak tanımlanmaktadır.

[26] Nitekim AKSSS m. 1'de de *"bilgisayar sistemi"* terimi tanımlanırken *"otomatik veri işleyebilen herhangi bir cihaz"* ifadesi kullanılmıştır.

[27] **Özen/Baştürk**, Bilişim – İnternet ve Ceza Hukuku, s. 10; **Tanrıkulu, Cengiz**; Computer Fraud, Ankara 2016, s. 12; **Yazıcıoğlu**, Bilgisayar suçları, s. 217; **Yenidünya, A. Caner**; "*Bilişim Sistemine Hukuka Aykırı Erişim Suçu*", Legal Fikri ve Sınai Haklar Dergisi, 2005, Sayı 4, s. 1029.

[28] Microsoft, Açık Akademi, Eğitimler, https://www.acikakademi.com/portal/Course/12/bilgisayar-yazilim-ve-algoritma.aspx, s.e.t: 05.05.2017.

[29] **Tanrıkulu, Cengiz**; Ceza Muhakemesi Hukukunda Bilişim Sistemlerinde Arama ve Elkoyma, Ankara 2014, s. 14.

[30] **Casey**, Digital Evidence and Computer Crime: Third Edition, s. 7; **Tanrıkulu**, Bilişim Sistemlerinde Arama ve Elkoyma, s. 14.

[31] **Değirmenci**, **Olgun**; Ceza Muhakemesinde Sayısal (Dijital) Delil, Ankara 2014 , s. 54.

sonucu olarak iletişim sistemleridir[32]. Üçüncü tür bilişim sistemleri ise gömülü bilişim sistemleridir. Bu bilişim sistemlerine navigasyon cihazlarını, özel amaçlı kullanılan el bilgisayarlarını, *"akıllı"* olarak nitelendirilen ev aletlerini örnek gösterebiliriz. Bu cihazların asıl fonksiyonları kullanım alanına göre farklılık arz etmekle birlikte bu cihazlar aynı zamanda bir bilişim sisteminin parçası olarak çalışmaktadırlar[33].

Bu açıklamalardan hareketle kanun koyucunun *bilgisayar – bilişim sistemi* ayrımında tercihini *"bilişim sistemi"*nden yana koymasının bu terimin daha geniş anlama[34] sahip olmasından kaynaklandığı söylenebilir. Bilişim sistemi terimindeki bilişim kelimesinin söz konusu bilim dalından hareketle kullanıldığı görülmektedir. Dolayısıyla hem *"bilgileri otomatik işleme tabi tutabilen"* halihazırda mevcut tüm cihazlar bu kapsama dahil edilmiş hem de ilerde icat edilmesi mümkün, bu özelliği taşıyacak olası cihazlar kapsam dışında bırakılmamıştır[35].

Özellikle günümüzde nesnelerin interneti (internet of things / IOT) olarak ifade edilen cihazların da bilişim sistemi kavramına dahil olduğunu belirtmek gerekir. *Internet of Things*, ifadesi ilk defa 1999 yılında *Kevin Ashton* tarafından, internet üzerinden radyo frekansı tanımlama teknolojisini (*RFID)* kullanarak fiziksel dünyaya bağlanan sistemleri ifade etmek için kullanılmıştır[36]. Nesnelerin interneti cihazları, üzerindeki sensörler yardımıyla dışarıdan aldığı verileri içerisinde daha önceden yazılmış algoritmalar yardımıyla otomatik olarak çözümleyerek elde ettiği sonuçları internet üzerinden kullanıcısına aktarmaktadır. Nesnelerin internetine günlük hayatımızda kullandığımız, internete bağlanabilen elektronik ev aletlerini, sesli yardım asistanlarını, kişisel sağlık takip cihazlarını örnek olarak gösterebiliriz.

Öte yandan, bilgisayar ve söz konusu diğer cihazların ürettikleri verileri başka bilgisayar veya cihazlara aktarmada kullanılan soyut veya somut ağlar da bilişim sistemi tanımına

---

[32] **Casey**, Digital Evidence and Computer Crime: Third Edition, s. 8; **Tanrıkulu**, Bilişim Sistemlerinde Arama ve Elkoyma, s. 14.

[33] **Casey**, Digital Evidence and Computer Crime: Third Edition, s. 8; **Tanrıkulu**, Bilişim Sistemlerinde Arama ve Elkoyma, s. 14.

[34] **Akbulut**, Bilişim Suçları, s. 546; **Dülger**, Bilişim Suçları, s. 74; **Erdoğan**, TCK'da Bilişim Suçları, s. 12; **Taşkın**, Bilişim Suçları, s. 4; **Yenidünya/Değirmenci**, Bilişim Suçları, s. 31.

[35] **Erdoğan**, TCK'da Bilişim Suçları, s. 12.

[36] **Juma, Mariam/Saleh, Hager/Suhail, Manal/Khalifa, Marwa**; "*What is Internet of Things?*", Times of Oman, http://timesofoman.com/article/97372/Technology/Oman-Technology:-What-is-Internet-of-Things, s.e.t: 29.03.2017.

dahildir[37]. Zira bilişim sistemi ile ifade edilmek istenen tekil bilgisayarlardan ziyade, bilgisayarların birbirine bağlı çevre birimleriyle oluşturduğu bir bütündür[38]. Bu anlamda bilgisayardan farklı olarak bilişim sistemi yalnız veri işlemeyi değil bunun yanında veri iletişimini de kapsar[39]. Dolayısıyla dünya üzerindeki en büyük ağ olan *"internet"* de bilişim sistemi kavramına dahildir[40].

Aynı şekilde CD (Compact Disc), Hard-Disk, SSD (Solid State Disk), hafıza kartları gibi veri taşıma araçlarının da bilişim sistemine dahil olduğu kanaatindeyiz. Zira nasıl ki internet veri iletişimi yönüyle bilişim sistemi kavramına dahil ise veri taşıma cihazları da veri depolama yönüyle bilişim sistemi kavramına dahildir. Veri taşıma cihazlarının esasen verileri otomatik işleme tabi tutma nitelikleri yoktur. Başka bir deyişle bir veri taşıma cihazı kullanıcının ona ilettiği bilgileri çeşitli algoritmalardan geçirerek bir sonuca otomatik olarak ulaşamaz. Dolayısıyla veri taşıma cihazları, aslında her zaman yardımcı cihaz konumundadırlar. Bu anlamda bir bilgisayar veya bilişim sistemi olmadan bu cihazların içerdiği verilerin insanlar tarafından okunması mümkün olmadığından bu cihazların da bilişim sistemi kavramına dahil olduğu kanaatindeyiz[41]. Ayrıca, hukuki koruma açısından bakıldığında; bilişim sistemi kavramının kullanıldığı kanuni düzenlemelerde, esas olarak bilişim sistemlerinin soyut bileşenlerinin, yani donanımlarından ziyade içerdikleri verilerin/ yazılımların korunduğu görülmektedir. Örneğin, TCK açısından bilişim sistemlerinin donanım unsuru mala zarar verme, hırsızlık, güveni kötüye kullanma gibi suçlar açısından korunurken; yazılım unsuru bilişim alanındaki suçlar bölümünde, bilişim sistemi ortak kavramı çerçevesinde ayrı bir korumaya tabi tutulmuştur. Dolayısıyla, veri taşıma cihazlarını bilişim sistemi kabul etmeyerek, bu cihazlarda yer alan verileri, hukuki koruma dışında bırakmanın yerinde olmayacağı kanaatindeyiz.

1.3. Bir Bilişim Sistemi Olarak İnternet

Bilgisayar ve programlanabilen diğer cihazların ürettikleri verileri başka bilgisayar veya cihazlara aktarmada kullanılan soyut veya somut ağların bilişim sistemine dahil olduğunu

---

37 **Yenidünya**, Hukuka Aykırı Erişim Suçu, s. 1030.

38 **Tanrıkulu**, Bilişim Sistemlerinde Arama ve Elkoyma, s. 13.

39 **Yenidünya**, Hukuka Aykırı Erişim Suçu, s. 1030.

40 **Ketizmen**, Bilişim Suçları, s. 20.

41 Karşı görüş için bkz. **Koca, Mahmut/Üzülmez, İlhan**; Türk Ceza Hukuku Özel Hükümler, Ankara 2016, s. 826.

ifade etmiştik. İşte bu anlamda neredeyse tüm bilişim sistemlerini birbirine bağlayan[42] internet de somut bir ağ olarak bilişim sistemine dahildir[43].

İnternet sözcüğü, *"international"* ve *"network"* sözcüklerinden türetilmiştir ve uluslararası ağ anlamına gelir. İnternetin icadı ABD'nin *"Advanced Research Project Authority Net"* (ARPANET) projesi temelinde mümkün olmuştur[44]. Söz konusu proje esas itibariyle askeri bir projedir[45]. 1960'lı yıllarda bilgisayarlar henüz bireyler arasında yaygınlaşmamışken devletler ve ticari şirketler bilgisayarlar arasında veri iletimini sağlayacak ağlar kullanmaktaydı ancak bu ağların temel iki handikabı vardı[46]. İlk olarak, veri iletiminde iki bilgisayarın aynı donanım ve yazılıma sahip olmaması ve her bilgisayarın kendine özgü bir ağ protokolü olması sebebiyle bu ağların kurulmasının ciddi ekonomik külfetleri vardı. Bu da bilgisayarlar arasındaki ağların yaygınlaşmasını engellemekteydi[47]. En önemli handikap ise bu dönemdeki ağların çalışabilmesi için bir ana bilgisayara ihtiyaç duyulmasıydı. Ana bilgisayarın çalışmaması durumunda bilgisayarlar arasındaki ağlar da fonksiyonlarını icra edemiyorlardı[48]. İşte söz konusu ağların bu dezavantajlarından dolayı soğuk savaş döneminde ABD Savunma Bakanlığı, herhangi bir nükleer saldırı durumunda bilgisayar sistemleri arasındaki iletişimin çökmemesi amacıyla ARPANET'i geliştirdi[49].

ARPANET projesi kapsamında farklı donanım ve yazılımlara sahip olsalar da bilgisayarlar arasında iletişimin sağlanabilmesi için ortak TCP (Tranmission Control Protocol) ve IP (Internet Protocol) ağ protokolleri geliştirildi[50]. IP bilginin makine diline yani dijital formata dönüştürülmesini, TCP ise dijital formata dönüştürülen bilginin yani verinin nihai iletim adresine ulaştırılmasını sağlıyordu[51]. Geliştirilen bu protokollerle dünya üzerindeki her

---

42 **Taşkın, Şaban Cankat**; İnternete Erişim Yasakları, Ankara 2016, s. 31.

43 **Yenidünya**, Hukuka Aykırı Erişim Suçu, s. 1031.

44 **Dülger**, Bilişim Suçları, s. 87; **Kaya, Mehmet Bedii**; Teknik ve Hukuki Boyutlarıyla İnternete Erişimin Engellenmesi, İstanbul 2010, s. 5; **Ketizmen,** Bilişim Suçları, s. 21; **Taşkın**, Bilişim Suçları, s. 13.

45 **Sınar**, **Hasan**; İnternet ve Ceza Hukuku, İstanbul 2001, s. 21.

46 **Kaya**, İnternete Erişimin Engellenmesi, s. 5.

47 **Kaya**, İnternete Erişimin Engellenmesi, s. 5.

48 **Kaya**, İnternete Erişimin Engellenmesi, s. 6.

49 **Dülger**, Bilişim Suçları, s. 87; **Kaya**, İnternete Erişimin Engellenmesi, s. 6.

50 **Karagülmez**, Bilişim Suçları, s. 34, 35; **Ryan**, **Johnny**; A History of the Internet and the Digital Future, Londra 2010, s. 90.

51 **Postel**, **J.**; "*Transmission Control Protocol*", https://tools.ietf.org/html/rfc793, s.e.t: 26.01.2017, s. 2; **Sınar**, İnternet ve Ceza Hukuku, s. 24.

bilgisayarın donanım ve yazılımı ne olursa olsun herhangi bir merkezi bilgisayara ihtiyaç duymaksızın internete bağlanabilmesi mümkün hale gelmiştir[52].

Askeri amaçlar için oluşturulan ARPANET, zamanla diğer kamu kurumlarının bilgisayarlar aracılığıyla iletişimini sağlayacak şekilde geliştirilmiştir. Daha sonra askeri amaçlarla kullanılan ağ, 1983 yılında MILNET olarak ayrılarak[53] ARPANET tamamen kamusal kullanıma açılmış ve internet kendisine her gün daha fazla bilgisayar eklenerek günümüzdeki devasa halini almıştır[54].

İnternet en yalın ifadesiyle birbirine uzak noktada bulunan bilişim sistemlerini birbirine bağlayan bir ağdır[55]. Bilişim sistemlerinde veya bir bilgisayarda işlenen verilerin dünyanın farklı yerlerindeki bilişim sistemi veya bilgisayara gönderilmesi ihtiyacı bu sistemleri birbirine bağlayacak ve bu iletişimi sağlayacak bilişim sistemi ağını (network) gerekli kılmıştır.

Bilişim sistemlerini birbirine bağlayan ağları kapsadıkları alan itibariyle ikiye ayırabiliriz. Birbirlerine yakın ve belli bir bölgede (örneğin bir binada veya binanın bir katında) bulunan bilişim sistemlerini birbirine bağlayan ağ sistemine LAN (Local Area Network – Yerel Ağ Alanı) denir. Diğer ağ türü ise WAN'dır (Wide Area Network – Geniş Alan Ağı)[56]. Geniş alan ağları, küçük ağların bir araya gelmesiyle oluşurlar. İşte İnternet de bu ikinci türe yani geniş alan ağına dahil bir ağdır ve neredeyse tüm dünyadaki bilişim sistemlerini birbirine bağlar[57].

Bilişim sistemlerini birbirine bağlayarak uluslararası bir iletişim ağı haline gelen internet, birçok avantajı beraberinde getirse de aynı zamanda suç oluşturan birçok fiilin gerçekleştirilmesi için uygun bir ortam da sağlamıştır[58].

---

52 **Dülger**, Bilişim Suçları, s. 86; **Kaya**, İnternete Erişimin Engellenmesi, s. 6.

53 **Ryan**, A History of the Internet, s. 90.

54 **Kaya**, İnternete Erişimin Engellenmesi, s. 6–7.

55 **Karagülmez**, Bilişim Suçları, s. 52.

56 **Ketizmen**, Bilişim Suçları, s. 20; **Yenidünya**, Hukuka Aykırı Erişim Suçu, s. 1031.

57 **Ketizmen**, Bilişim Suçları, s. 20; **Yenidünya**, Hukuka Aykırı Erişim Suçu, s. 1031.

58 **Mahmutoğlu**, **Fatih Selami**; "*Karşılaştırmalı Hukuk Bakımından İnternet Sujelerinin Ceza Sorumluluğu*", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, İnternet Özel Bölümü, 2001, Cilt LIX, Sayı 1–2, s. 39.

1.4. Bilişim Sisteminin Temel Birimi: Veri

Çalışma konumuz olan "*bilişim sistemleri aracılığıyla haksız yarar sağlama suçu"* bakımından önemli olan "*bilişim sistemi"* terimini yukarıda açıklamaya çalıştık. TCK m. 244'te suçun konusu *"bilişim sisteminin işleyişi* ve *sistemdeki veriler"* olarak belirlenmiştir[59]. Dolayısıyla *"veri"* terimini de kısaca açıklamakta yarar görmekteyiz. Veri, İngilizce *"data"* kelimesinin dilimizdeki karşılığıdır[60]. Çalışma konumuz itibariyle veri teriminden kasıt bilgisayar veya bilişim sistemi verisidir. Bilgisayar veya bilişim sistemi verileri kısaca bilginin belirli bir formata dönüştürülmüş halini ifade ederler[61] ve bilgisayarın veya bilişim sisteminin soyut yönüne dahildirler.

Bilgisayar verisi, kısaca, bilginin bilgisayarın anlayabileceği dile –yani makine diline– dönüştürülmüş halini ifade eder[62]. Makine dilinden maksat yukarıda açıklandığı üzere bilgisayarların çalışma mantığından kaynaklanan *"binary"* sistemi yani "0" ve "1"lerin oluşturduğu dildir.

Bilgisayar veya bilişim sistemi verisinin tanımı Türk Hukuku'nda 5651 sayılı *"İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun"* m.2/1-k bendinde, yukarıdaki açıklamalarımızla paralel olarak *"veri: bilgisayar tarafından üzerinde işlem yapılabilen her türlü değeri ifade eder."* şeklinde yapılmıştır. Aynı şekilde TCK m. 243'ün (bilişim sistemine girme suçu) gerekçesinde veri, *"sistem içindeki bütün soyut unsurlar, fıkrada geçen 'veri' teriminin kapsamındadır"* şeklinde ifade edilmiştir. AKSSS m. 1/b'de ise bilgisayar verisi, *"bilgisayar sisteminin bir işlevi yerine getirmesini mümkün kılan bir programı da kapsayan, olguların, bilginin veya kavramların bir bilgisayar sisteminde işlenmeye uygun haldeki her türlü temsilini ifade eder"* şeklinde tanımlanmıştır[63].

Bilgisayar veya bilişim sistemi verisinde, dikkat edilmesi gereken husus bu verilerin yalnızca bilgisayarlarda bulunmadığıdır. CD, Hard-Disk, SSD, hafıza kartları gibi veri

---

59 **Koca/Üzülmez**, Özel Hükümler, s. 826.

60 **Orta, Mesut**; Bilişim Suçları ve Adli Bilişim, Ankara 2015, s. 39.

61 **Ergün**, **İsmail**; Siber Suçların Cezalandırılması ve Türkiye'de Durum, Ankara 2008, s. 6; **Orta**, Bilişim Suçları ve Adli Bilişim, s. 39; **Tanrıkulu**, Computer Fraud, s. 12; **Yazıcıoğlu**, Bilgisayar Suçları, s. 29.

62 Microsoft Açık Akademi, Eğitimler, https://www.acikakademi.com/portal/Course/12/bilgisayar-yazilim-ve-algoritma.aspx, s.e.t: 02.05.2017

63 https://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss380.pdf, s.e.t: 02.05.2017.

taşıma araçlarında da bilgisayar verisi bulunur; her ne kadar bu araçlardaki veriler ancak bir bilgisayar veya bilişim sistemi yardımıyla insanlar için anlaşılabilir hale gelse de.

2. GENEL OLARAK BİLİŞİM SUÇLARI

2.1. Bilişim Suçu Kavramı

Modern bilgisayarın[64] ABD'de icat edilmesinin tabi bir sonucu olarak bilgisayarla ilgili bilinen ilk suç da ABD'de işlenmiştir. Literatürde bilinen ilk teknik bilişim veya bilgisayar suçu, 18 Ekim 1966 tarihli *"Minneapolis Tribune"de* yayınlanan *"bilgisayar uzmanı banka hesabında tahrifat yapmakla suçlanıyor"* başlıklı yazı ile kamuoyuna yansımıştır[65].

Öncelikle belirtmek gerekir ki nispeten yeni olan bu suçların ifade edilmesinde gerek Türk Hukuku'nda gerekse karşılaştırmalı hukukta bir terim birliği yoktur. Bu suçların anavatanı olan ABD'de bu suç türleri için yaygın olarak *"computer crime"* ifadesi kullanılmaktadır[66]. İngilizce'de ayrıca şu terimler de bu suçları ifade etmek için kullanılmıştır: *"computer-related crime"* (bilgisayarla bağlantılı suç), *"computer-assisted crime"* (bilgisayarla işlenen suç), *"crime against computer"* (bilgisayara karşı işlenen suç), *"cybercrime"* (siber suç), *"technological crime"* (teknolojik suç), *"high tech crime"* (yüksek teknoloji suçu), *"internet crime"* (internet suçu), *"digital crime"* (dijital suç), *"electronic crime"* (elektronik suç)[67].

İngilizce'de, *"computer-related crime"* terimi bilgisayarın bir şekilde dahil olduğu her suç için kullanılırken, *"computer crime"* terimi ise *"U.S. Computer Fraud and Abuse Act ve U.K. Computer Abuse Act"* kanunlarında tanımlanan suçlar için kullanılmaktadır. *"Cybercrime"* (siber suç) terimi ise bilgisayar ağları üzerinden işlenen suçları da kapsamına aldığından diğer terimlerden daha geniş bir anlama sahiptir. *"U.S. Department of Justice"*

---

64 **Ören/Üney/Çölkesen**, Türkiye Bilişim Ansiklopedisi, s. 1030: İlk modern bilgisayar (1947) ENIAC olarak kabul edilmektedir.

65 **Aydın**, Bilişim Suçları ve Hukukuna Giriş, s. 13; **Warrick**, **Patricia S.**; The Cybernetic Imagination in Science Fiction, Cambridge 1982, s. 124.

66 **Yazıcıoğlu**, Bilgisayar Suçları, s. 125.

67 **Erdoğan**, TCK'da Bilişim Suçları, s. 44; **McQuade**, **Samuel C.**; Encyclopedia of Cybercrime, Westport, Conn 2009, s. 44; **Yenidünya/Değirmenci**, Bilişim Suçları, s. 30.

ve Avrupa Konseyi'nin tercih ettiği terim de *"cybercrime"*dır. Nitekim Avrupa Konseyi bünyesinde imzalanan sözleşmenin adı da *"Convention on Cybercrime"*dır.[68]

ABD ile benzer şekilde Almanya'da da bu suç türleri bilgisayar üzerinden ifade edilmektedir. Alman hukuk doktrininde kullanılan ifade *"computer kriminalität"*dir[69]. Fransa'da ise *"la fraude informatique"* yani bilişim suçları ifadesi kullanılmaktadır[70].

Bu suçlar Türk Hukuku'nda ilk olarak 6 Haziran 1991 tarihli ve 3756 sayılı kanunun 765 sayılı TCK'da yaptığı değişiklik ile düzenleme alanı bulmuştur. Yapılan bu düzenleme ile 765 sayılı TCK'ya on birinci bap olarak *"bilişim alanında suçlar"* başlığı altında 525/a, 525/b, 525/c ve 525/d maddeleri eklenmiştir. 1 Haziran 2005 tarihli 5237 sayılı TCK'da bu bölüm aynı isimle yer almıştır. Böylece kanun koyucu *"bilgisayar"* ve *"bilişim/bilişim sistemi"* bakımından tercihini bilişimden yana koymuştur. Bu tercihte esasında ilgili maddelerin mehaz ülkesi olan Fransa'daki tercihin de etkili olduğu söylenebilir. Yukarıda açıklandığı üzere bilişim bilimine Fransızca'da, bilginin otomatik olarak işleme tabi tutulması dikkate alınarak, *"information"* ve "*automatique"* kelimelerinin birleşimi ile *"informatique"* terimi türetilmiştir. Fransız Ceza Kanunu'nda da buna paralel olarak bilgisayar (*ordinateur)* değil *"bilgileri otomatik işleme tabi tutan sistem"* ifadesi kullanılmıştır.

Türk doktrininde genel olarak kanundaki ifade benimsenmiş ve bilgisayar suçları terimi yerine bilişim suçları ifadesi kullanılmıştır[71]. Türk Hukuku açısından bilişim suçları ifadesi genel olarak ifade edildiği üzere bilgisayar suçlarından daha geniş bir anlama sahiptir. Bu durum da yukarıda açıklandığı üzere esasında bilişim sisteminin, bilgisayardan daha geniş bir anlama sahip olmasından kaynaklanır. Bizim de katıldığımız görüş bilişim suçu

---

68 **Casey**, Digital Evidence and Computer Crime: Third Edition, s. xxv.

69 **Önder**, **Ayhan**; Şahıslara ve Mala Karşı Cürümler ve Bilişim Alanında Suçlar, İstanbul 1994, s. 504.

70 **Özen/Baştürk**, Bilişim – İnternet ve Ceza Hukuku, s. 12.

71 Türk hukukunda *"bilişim suçları"* terimini benimseyen yazarlardan bir kısmı şu şekildedir: **Akarslan**, **Hüseyin**; Bilişim Suçları, Ankara 2015 s. 35; **Avşar, Zakir/Öngören, Gürsel**; Bilişim Hukuku, İstanbul 2010, s. 123; **Aydın**, Bilişim Suçları ve Hukukuna Giriş, s. 27; **Demir, Ömer/Arıç, Mehmet/Polat, Halil**; Bilişim Suçları ve Bilişim Yoluyla İşlenen Suçlar, Ankara 2015, s. 3; **Doğan**, **Ramazan**; Bilişim Suçları, Ankara 2014 s. 14; **Dülger**, Bilişim Suçları, s. 80; **Erdoğan**, TCK'da Bilişim Suçları, s. 47; **Gürler**, Bilişim Alanında Suçlar, s. 72; **Karagülmez**, Bilişim Suçları, s. 53; **Ketizmen**, Bilişim Suçları, s. 39; **Kurt**, **Levent**; Açıklamalı, İçtihatlı Tüm Yönleriyle Bilişim Suçları, Ankara 2005, s. 49; **Orta**, Bilişim Suçları ve Adli Bilişim, s. 75; **Parlar**, **Ali**; Türk Ceza Hukukunda Bilişim Suçları, Ankara 2015, s. 17; **Taşdemir**, **Kubilay**; Bilişim, Banka veya Kredi Kartlarının Kötüye Kullanılması ve Dolandırıcılık Suçları, Ankara 2009, s. 276; **Taşkın**, Bilişim Suçları, s. 10; **Yenidünya/Değirmenci**, Bilişim Suçları, s. 43.

ifadesinin yerinde olduğudur. Zira bilgisayarlar dışında bilişim ağları, veri taşıma cihazları ve bilgisayar gibi genel fonksiyon icra etmeyen cihazlar da bu suçların konusu olabilecek niteliktedirler.

Terim konusunda birlik sağlanamaması bir yana bilişim suçlarının sınırlarının çizilmesinde de doktrinde görüş birliği yoktur. Bilişim suçlarının sınırlarının çizilmesinde doktrinde farklı kriterler getirilmekte ve bu kriterlere göre bir suçun bilişim suçu olup olmadığı belirlenmektedir[72].

Bu kriterlerden ilki bilişim sisteminin araç veya amaç olarak kullanılmasını esas alır. Bu anlamda eğer bir bilişim sistemi suçta araç olarak kullanılıyor veya suç bir bilişim sistemini hedefliyorsa ortada bir bilişim suçu vardır[73]. İkinci kriter ise bilişim suçlarını meydana getirdiği malvarlığı ihlallerine göre ele alır. Buna göre bilişim sistemlerinde işlenen verilerin kullanılmasıyla meydana getirilen kasıtlı ve hukuka aykırı malvarlığı ihlalleri, bilişim suçudur ve bilişim suçu ancak bilişim sistemleri ile ilgili mülkiyet suçlarını kapsar. Üçüncü kriter, bilişim sistemleri ile ilgili herhangi bir bağlantısı bulunan suçları bilişim suçu olarak kabul eder[74]. Dördüncü kriter ise bilişim suçunda bilgisayarın veya daha doğru bir ifadeyle bilişim sisteminin kullanılmasını esas alır. Beşinci kriter ise suçu işleyen faili esas alır[75]. Buna göre bilişim suçları, ancak bilgisayardan veya bilişim dünyasından anlayan, bilgisayarı kullanabilen kimseler tarafından işlenebilen suçlardır. Günümüzde, bilgisayarın yaygınlaşması ve *"bilgisayardan anlama"*nın ayırt edici bir özellik olarak kabul edilememesinden dolayı bu kriterin geçerliliği bulunmamaktadır.

Doktrinde ifade edilen bu kriterler, bilişim suçunu tanımlamakta yetersiz kalmıştır. Bilgisayarla bağlantılı her suçu bilişim suçu kabul eden ya da bilgisayarla işlenen her suçu bilişim suçu sayan kriterler, bilişim suçu kavramının diğer klasik suçlardan farkını yeterince ortaya koyamamıştır. Bilişim sistemiyle malvarlığı ihlallerini esas alan kriter ise bilişim suçlarının alanını gereğinden fazla daraltmıştır.

---

[72] Bu kriterler için bkz. **Akbulut**, Bilişim Suçları, s. 550; **Dülger**, Bilişim Suçları, s. 82; **Kızıltan**, **Mehmet Burak**; 5237 Sayılı Türk Ceza Kanununda Bilişim Sistemine Girme, Sistemi Engelleme ve Bozma Suçları, Yayımlanmamış Yüksek Lisans Tezi, İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, İstanbul 2007, s. 21; **Yazıcıoğlu**, Bilgisayar Suçları, s. 137.

[73] **Akbulut**, Bilişim Suçları, s. 550.

[74] **Akbulut**, Bilişim Suçları, s. 550.

[75] **Akbulut**, Bilişim Suçları, s. 550.

Belirtmek gerekir ki bilişim suçlarını, doktrinde genel olarak ifade edildiği üzere dar anlamda bilişim suçları ve geniş anlamda bilişim suçları olmak üzere ikiye ayırmak gerekmektedir[76]. Dar anlamda bilişim suçlarından kasıt, bilişim sistemlerinin varlığı ile ortaya çıkmış suçlardır[77]. Geniş anlamda bilişim suçları ise klasik suçlar olarak ifade edebileceğimiz, bilişim sistemlerinin icadından önce de hukuk düzeninde bulunan suçların, bilişim sistemlerinin vasıta olarak kullanılmasıyla işlenmesidir[78]. Dolayısıyla bilişim suçu ifadesinden asıl olarak anlaşılması gerekenin dar anlamda bilişim suçu olduğu kanaatindeyiz.

Bilişim suçlarının tanımında dikkat edilmesi gereken nokta bu suçları klasik suçlardan ayıran özelliğini ortaya koymak yani klasik suçlardan hiçbir farkı olmayan suçları bilişim suçu olarak kabul etmemek ve gelişen ve değişen teknoloji karşısında da çabucak eskiyecek bir tanımdan kaçınmaktır. Bu durumda yapılacak tanımın temelinin bilgisayar veya bilişim sisteminin kendisine değil, bunlardaki veriye dayanması gerektiğini söyleyebiliriz. Zira bilişim suçlarında faillerin amacı esasen bilişim sistemleri değil, sistemdeki verilerdir. Yani bir bilişim sisteminin fiziki varlığı hedef alındığında bu esasında bir bilişim suçuna değil olsa olsa klasik suç tiplerinden mala zarar verme yahut hırsızlık gibi malvarlığına karşı suçlara vücut verecektir. Bu noktadan hareketle bilişim suçlarını, bilişim sistemlerindeki verilere karşı ya da sistemdeki veriler hedef alınmak suretiyle sisteme karşı, bunların güvenliğini ve bütünlüğünü bozacak nitelikteki suçlar olarak ifade edebiliriz.

2.2. Bilişim Suçlarının İşlenme Biçimleri

Bilişim suçlarını diğer suçlardan ayıran en önemli özellik bu suçların işlenme biçimlerinde karşımıza çıkar. Gerçekten bilişim suçlarında klasik suçlardan çok daha farklı bir fiil unsuru vardır. Zira kanunun öngördüğü tipik fiil esas itibariyle sanal alemde gerçekleşmektedir[79]. Örneğin bilişim sistemine girme suçunda, failin sisteme fiziki varlığı ile girmesi değil sistemin sanal/ dijital içeriğine dahil olması söz konusudur.

---

[76] **Avşar/Öngören**, Bilişim Hukuku, s. 124; **Dülger**, Bilişim Suçları, s. 83; **Ergün**, Siber Suçların, s. 29–32; **Gürler**, Bilişim Alanında Suçlar, s. 82.

[77] **Ergün**, Siber Suçların, s. 29; **Gürler**, Bilişim Alanında Suçlar, s. 82.

[78] **Gürler**, Bilişim Alanında Suçlar, s. 82.

[79] *"Bilişim suçlarında, klasik suçlardaki fiziki yapı yerine, soyut veya sanal bir alan söz konusudur."* (**Karagülmez**, Bilişim Suçları, s. 78.)

Bilişim suçlarının sanal alemde gerçekleşmesinin bir sonucu olarak failler, bu suçları çoğu zaman büyük çabalar sarf etmeksizin gerçekleştirmektedirler. Failin suçu işlemek için çaba sarf etmesi bir yana bu suçlar işlenme biçimi itibariyle milyonlarca kişiyi etkileyebilecek niteliğe sahiptirler. Dünyadaki neredeyse tüm bilişim sistemlerinin bağlı olduğu internetin varlığı da büyük çoğunlukla bilişim suçlarında neticenin, hareketin yapıldığı yerden farklı bir yerde/ yerlerde gerçekleşmesine neden olmaktadır[80]. Neticenin hareket yerinden farklı yerde gerçekleşmesi ve fiilin sanal alemde işlenmesi nedeniyle, suça ve suçluya ulaşma, klasik suçlara nazaran bilişim suçlarında daha zordur[81]. Hatta bu suçlarda çoğu zaman, mağdur kendisine karşı bir suç işlendiğinin farkında dahi olamamaktadır[82].

Bilişim suçlarını klasik suçlardan ayıran temel nokta işlenme biçimleri olduğu için; çalışmamızın bu bölümünde, bu suçların yaygın olan işlenme biçimlerine kısaca değinmeye çalışacağız.

Bilişim suçları genel olarak mağdurun bilişim sistemine bulaştırılan kötü amaçlı yazılımlarla işlenmektedir. Kötü amaçlı bilgisayar yazılımları için dünyada yaygın olarak *"malware"* ifadesi kullanılmaktadır. Bu ifade İngilizce, kötücül anlamına gelen *"malicious"* ve yazılım anlamına gelen *"sofware"* sözcüklerinden türetilmiştir[83]. Çalışmamız kapsamında *"malware"* yazılım türlerinin hepsine değinilmeyecektir. Esasen bu mümkün de değildir. Zira bilişim dünyasında hemen her gün, gayrikanuni amaçlarla üretilmiş ve henüz kamuoyuna yansımamış yeni yöntemler ve yazılımlar keşfedilmektedir.

Günümüzde *"malware"*ler[84], bir bilişim sisteminde veya ağda; zarar verme, bozma, çalma ve kanuna aykırı işlem yapma amacına yönelik çok çeşitli şekillerde karşımıza çıkmakta ise de temel olarak üç tür *"malware"*in bulunduğunu söyleyebiliriz: *"Bilgisayar virüsleri, truva atları ve solucanlar"*[85].

Ortaya çıkışı itibariyle bu kötücül yazılım türlerinden ilki *"bilgisayar veya bilişim virüsleri"*dir. Bilişim virüslerinin, aynen biyolojik dünyada olduğu gibi, aktif olabilmek ve

---

80 **Erdoğan**, TCK'da Bilişim Suçları, s. 365.

81 **Dülger**, Bilişim Suçları, s. 119.

82 **Doğan**, Bilişim Suçları, s. 20.

83 **Goodman**, Geleceğin Suçları, s. 25.

84 Siber güvenlik firması Kaspersky Lab, 2013 yılında her gün yaklaşık 200.000 yeni *"malware"* örneğini yok ettiğini açıklamıştır. Kaspersky Lab, Global Corporate IT Security Risk 2013, Mayıs 2013.

85 **Goodman**, Geleceğin Suçları, s. 26.

çoğalmak için başka bir yazılıma ihtiyaçları vardır. Bilişim virüsleri, bulaştıkları yazılımları ve en nihayetinde sistemin işletim sistemini çökertmeleri nedeniyle mağdura muhtemel en büyük zararı veren yazılım türlerinden biridir[86]. Dünyada bilinen ilk bilgisayar virüsü (*"Brain")* 1986 yılında 24 ve 17 yaşlarındaki iki Pakistanlı kardeş tarafından geliştirilmiştir[87]. Bu iki kardeşin asıl amaçları, uzun yıllar boyunca geliştirdikleri kendi meşru yazılımlarının korsan kopyalarının yapılmasını engellemekti. Esasen geliştirdikleri bu virüs zararsızdı, sadece yazılımlarının kopyalanması sırasında ekrana kaygı verici bir mesaj geliyor ve virüsün silinmesi için adres bilgilerinin paylaşılmasını talep ediyordu. Pakistanlı kardeşlerin bu kötücül yazılımı oluştururken hesaba katmadıkları şey ise yazılımın tıpkı biyolojik virüslerde olduğu gibi çoğalıp yayılma özelliğiydi. *"Brain",* o dönemin disket teknolojisi ile tüm dünyaya yayıldı ve ilk bilişim virüsü olarak tarihe geçti.

İkinci temel *"malware"* yazılım türü ismini Truva'ya giren yunanlıların efsanevi tahta atından alan truva atları yahut *"trojan"*lardır. Bu tür yazılımlar, virüs yazılımlarından farklı olarak meşru bir yazılım içerisinde gizlenirler ve hedef kullanıcı bu meşru yazılımı bilgisayarına kurduğunda aktif hale gelirler[88]. Yine virüslerden farklı olarak truva atları, başka dosyalara bulaşarak yayılmazlar. Genellikle internette ücretsiz yazılım sağlayan web sitelerinde ya da elektronik posta yoluyla kullanıcılar arasında yayılırlar. Truva atları genellikle kurulmuş oldukları bilgisayarda *"arka kapılar"* oluşturarak sisteme erişim yetkisi olmayan failin sistemi uzaktan kontrol etmesine yardımcı olurlar[89].

Üçüncü temel *"malware"* yazılım türü ise solucanlardır. Bu yazılımlar da esas olarak hedef bilişim sistemine zarar vermekle birlikte bilişim virüslerinden farklı olarak çoğalmak için konak programlara ihtiyaç duymazlar[90].

Genel olarak diğer *"malware"* yazılımlar da bu üç temel türün türevleri olarak görülebilir. Örneğin, *"mantık bombası"* (*logic bombs*) yazılımı truva atının bir türevidir. Aynı truva atında olduğu gibi mantık bombası da meşru bir yazılım içerisinde gizlenmekte ancak truva

---

86 **Dülger**, Bilişim Suçları, s. 128.

87 **Kersten**, **Jason**; "*How Two Pakistani Brothers Created the First PC Virus*", http://mentalfloss.com/article/12462/going-viral-how-two-pakistani-brothers-created-first-pc-virus (s.e.t: 28.03.2017).

88 **Bureau of Justice Statistics U.S. Departmant of Justice**; "*Classifying the Crime Section I*", Computer Crime: Criminal Justice Resource Manual, 1979, Cilt 1, s. 11.

89 **Dülger**, Bilişim Suçları, s. 120–121.

90 **Goodman**, Geleceğin Suçları, s. 26.

atları gibi meşru yazılımın bilgisayara kurulmasıyla aktif hale gelmemekte, kullanıcının fark etmeyeceği şekilde *"sessiz"* konumda kalmaktadır; ta ki daha önceden belirlenmiş özel durumların gerçekleşmesi veya belirlenen zamanın gelmesine kadar. Bu şartlar gerçekleştiğinde yararlı bir yazılım gibi görünen mantık bombası asıl görevini ifa etmekte ve tıpkı truva atı gibi zararlı yazılım olarak çalışmaktadır[91].

Uygulamada sık karşılaşılan diğer kötücül yazılımlara ve bilişim suçlarının işlenme biçimlerine örnek olarak şunlar gösterilebilir: ağ solucanları (network worms), tavşanlar (rabbits), bukalemunlar (chameleon), kök kullanıcı takımı (rootkit), gizlice dinleme – ağı koklama (sniffing), klavye dinleme sistemleri (keylogger), eşzamansız saldırılar (asynchronous attacks), istem dışı alınan elektronik postalar (spam), salam tekniği.[92]

Burada ayrıca uygulamada özellikle son dönemlerde çokça karşılaşılan oltalama *(*phishing*)* ve dağıtık servis dışı bırakma saldırılarına *(*Distributed Denial of Service – DDoS*)* değinmenin yararlı olacağı kanaatindeyiz. Oltalama saldırılarında esasen bir *"malware"* kullanıldığı söylenemez. Bu saldırıda temel olarak mağdurun aldatılması söz konusudur. Fail, mağdurun hesap veya sistem şifrelerine yahut onunla ilgili herhangi bir özel veriye ulaşmak amacıyla, ona resmi bir kurum veya kuruluşun internet sitesinin yahut yazılımının bir taklidini göndermekte ve ondan, buraya, söz konusu özel bilgilerini yazmasını talep etmektedir[93]. Taklit site veya yazılımın farkına varamayan mağdur da bilgilerini bu sistem üzerinden girmekte ve böylece fail, herhangi bir yazılıma ihtiyaç duymaksızın mağdurun özel bilgilerine ulaşmış olmaktadır. TCK bakımından da bu saldırılarda failin, hileli hareketlerle mağduru aldatarak yarar sağlaması söz konusu olduğundan dolandırıcılık suçunun oluşması olasıdır.

"DDoS"[94] saldırıları özellikle nesnelerin interneti cihazlarının yaygınlaşmasıyla gittikçe sık ve büyük zararlara yol açan bir saldırı haline gelmiştir. Nesnelerin interneti cihazlarının gittikçe kolay üretilir hale gelmesi, nispeten küçük girişimcilerin bu cihazlara ilgilerini artırmıştır. Ancak bu üreticiler bu cihazların üretiminde maliyet odaklı davranmakta,

---

91 **Dülger**, Bilişim Suçları, s. 127.

92 Detaylı bilgi için bkz. **Dülger**, Bilişim Suçları, s. 119–136.

93 **U.S. Dept. of Justice**; "*Electronic Crime Scene Investigation: A Guide for First Responders*", 2008, Cilt 1, s. 49–62.

94 **Orta**, Bilişim Suçları ve Adli Bilişim, s. 118: DDoS, Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği'nin 3. maddesinde g bendinde *'Dağıtık hizmet dışı bırakma'* şeklinde ifade edilmiştir.

sistemin güvenliğini sağlayacak gerekli önlemleri almamaktadırlar. Durumun farkında olan bilişim korsanları da uygun yazılımlarla artık sayıları milyonları bulan bu cihazları *"köleleştirmekte/ zombileştirmekte"* ve böylece amaçları doğrultusunda kullanmaktadırlar. *"DDoS"* saldırılarında köleleştirilen bilişim sistemleri hedef internet siteleri ve bilişim sistemlerine internet üzerinden bunların kapasitelerinin çok üzerinde taleplerde bulunarak, hedef sistemin gerçek kullanıcıların taleplerine cevap verememesine neden olmaktadır.[95]

"DDoS" saldırıları kimi zaman çok büyük zararlara neden olabilmektedir. Nitekim 21 Ekim 2016'da bir internet alan adı sağlayıcısı şirketine yapılan *"DDoS"* saldırısında neredeyse İnternet'in yarısına dünya genelinde erişim sağlanamamıştır[96].

2.3. Avrupa Konseyi Siber Suçlar Sözleşmesi Kapsamında Bilişim Suçları

2.3.1. Sözleşme'ye İlişkin Genel Açıklamalar

Bilgi teknolojilerinde son yıllarda meydana gelen inanılmaz gelişim, hem çok köklü hem de çok hızlı olmuştur. Bilgi teknolojilerinde meydana gelen bu gelişim, bilgiye erişimde coğrafi sınırların ortadan kalmasına, dünyanın küçük bir köy haline gelmesine neden olmuştur. Bu gelişimin bilgiye erişimdeki olumlu etkisinin yanı sıra, toplum hayatında yeni anti-sosyal davranışların ortaya çıkmasında da rolü vardır. Bir yandan klasik olarak niteleyebileceğimiz hırsızlık ve dolandırıcılık gibi suçlar oluşan bu yeni siber uzayda işlenir hale gelmiş bir yandan da bu alana özgü yeni suç tipleri ortaya çıkmıştır.[97]

Bilişim suçlarının kendine özgü doğalarından kaynaklanan özellikleri, bu suçlarla mücadelede ulusal düzlemde alınacak önlemlerin yetersiz kalmasına neden olmaktadır. Doktrinde bu yetersiz kalışın temel sebebi olarak, bilişim suçlarının coğrafi sınır tanımaması ve çok kısa sürede işlenebilir olması gösterilmektedir[98]. Gerçekten tüm dünyadaki bilişim sistemlerini birbirine bağlayan internet, bilişim suçlarının işlenmesinde coğrafi sınırları

---

95 *"DDoS"* hakkında detaylı bilgi için bkz. **Seungjoo Kim**, DDoS Attack on DNS using infected IoT Devices, https://www.slideshare.net/skim71/ddos-attack-on-dns-using-infected-iot-devices?ref, s.e.t 08.05.2017.

96 http://www.usatoday.com/story/tech/2016/10/21/cyber-attack-takes-down-east-coast-netflix-spotify-twitter/92507806, s.e.t 08.05.2017.

97 **Sokullu Akıncı, Füsun**; "*Avrupa Konseyi Siber Suç Sözleşmesinde Yer Alan Maddi Ceza Hukukuna İlişkin Düzenlemeler ve Özellikle İnternette Çocuk Pornografisi*", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, 2001, Cilt 59, Sayı 1–2, s. 11.

98 **Önok**, **Murat**; "*Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği*", Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, 2013, Cilt 19, Sayı 2 (Prof. Dr. Nur Centel'e Armağan), s. 1233–1234; **Sokullu Akıncı**, AKSSS Maddi Ceza Hukuku, s. 12.

ortadan kaldırmaktadır. Dolayısıyla bilişim suçlarıyla mücadelede ortaya çıkan temel problemlerden biri de devletlerin egemen eşitliği ilkesidir[99]. Bir devletin ulusal yargısı kural olarak kendi ülkesinde geçerlidir. Her ne kadar klasik suçlarla mücadelede uluslararası adli yardımlaşmayı mümkün kılacak anlaşmalar bulunsa da bu antlaşmalar bilişim suçları bakımından yetersiz kalmaktadır[100]. Zira bilişim suçlarında fail ile mağdur arasındaki mekân farkı klasik suçlara nazaran neredeyse bir zorunluluktur. Dolayısıyla bilişim suçları çoğu zaman bir mesafe suçu[101] olmaktadır[102]. Öyleyse bu suçlarla mücadelede klasik suçlar için olandan farklı bir iş birliğinin bulunması elzemdir.

Bilişim suçları, genellikle çok az masrafla çok kısa sürede işlenebilen ve büyük zararlara yol açabilen suçlardır[103]. Klasik suçlarda failin, suçu bir bedensel veya zihinsel emekle işlemesine karşılık, bilişim suçlarında failin bilgisayarının başında sadece tuşlara basarak belki milyonlarca kişinin etkilendiği büyük zararlara yol açması dikkate alındığında hız, kolaylık ve etkinin yaygınlığı açısından aradaki farkın kıyası gayrıkabil çapı ortaya çıkmaktadır[104]. Bilişim suçlarının çok kısa sürede işlenmesinin yanı sıra fail, bu suçlarda çoğunlukla anonimdir[105]. Bu kadar kolay ve az masrafla işlenen bilişim suçları ile mücadelede ise tam tersine, çok büyük emek ve masraflar gerekmektedir[106]. Bilişim

---

[99] **Önok**, Siber Suçlarla Mücadelede Uluslararası İşbirliği, s. 1234. **Pazarcı**, **Hüseyin**; Uluslararası Hukuk, Ankara 2015, s. 150: *"Her devletin egemen olmasının doğal sonucu egemen devletlerin eşitliğini gerektirmektedir. Bu olgu uluslararası hukuk açısından ilke olarak bütün devletlerin aynı hukuksal statüye sahip olduklarını belirtmektedir."*

[100] **Önok**, Siber Suçlarla Mücadelede Uluslararası İşbirliği, s. 1234.

[101] **Dönmezer, Sulhi/Erman, Sahir**; Nazari ve Tatbiki Ceza Hukuku - 1, İstanbul 2016, s. 318: *"Hareketin yapıldığı yer ile neticenin gerçekleştiği yer arasında yargısal veya siyasal sınırın bulunduğu 'mesafe suçları' ise bu konuda özellikli bir durum arz ederler."*

[102] **Sokullu Akıncı**, AKSSS Maddi Ceza Hukuku, s. 12.

[103] **Önok**, Siber Suçlarla Mücadelede Uluslararası İşbirliği, s. 1236.

[104] Örneğin, 21 Ekim 2016'da ABD'ye karşı gerçekleştirilen DDoS (Distributed Denial of Service) saldırılarında internetin neredeyse yarısına dünya genelinde erişim sağlanamamıştır. (http://www.usatoday.com/story/tech/2016/10/21/cyber-attack-takes-down-east-coast-netflix-spotify-twitter/92507806, s.e.t: 08.06.2017)

2001 yılında Avusturya'da bir *"hacker", "Maroochy Shire"* bölgesinin kanalizasyon arıtma tesisine siber saldırı düzenleyerek buranın kontrolünü ele geçirmiş ve milyonlarca litre kanalizasyon suyunu parklara ve nehirlere boşaltmıştır. (**Smith**, **Tony**; "*Hacker jailed for revenge sewage attacks*", The Register, https://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage, s.e.t: 02.06.2017).

[105] **Yılmaz**, **Sacit**; Türk Ceza Hukuku Sisteminde Siber Suçlarla Mücadele, Ankara 2016, s. 110: *"Siber suçlarla mücadelede fail veya faillerin belirlenmesinde yaşanan güçlük, soruşturmaların önündeki engellerden bir diğeridir. Kamuya açık internet alanları, NAT ve VPN olarak bilinen hizmetler ile kablosuz ağ bağlantısı gibi hizmetler, faillerin belirlenmesini engelleyen hizmetlerdir… Fail ya hiç kimlik kullanmamakta (ki bazı durumlarda kimliğe ihtiyaç duyulmamaktadır) ya da başkasına ait kimlik bilgilerini kullanmaktadır. Her iki durumda da siber saldırganın tespiti ve cezalandırılması olanaklı değildir."*

[106] **Önok**, Siber Suçlarla Mücadelede Uluslararası İşbirliği, s. 1235.

suçlarında, özellikle suça ve suçluya ulaşmada elektronik deliller çoğu zaman tek çare olmaktadır. Elektronik delillerin de elde edilmesi ve yargılamada hukuka uygun delil olması için de fiziki delillerden farklı olarak belli prosedürlerin takip edilmesi gerekmektedir[107]. Hatta bu ihtiyaç ortaya bir bilim dalı olarak adli bilişimi çıkarmıştır[108].

Bilişim suçlarının nispeten yeni suç tipleri olması da birtakım zorlukları beraberinde getirmektedir. Ceza-adalet sisteminde yer alan aktörler, konuya henüz yeterince aşina değillerdir ve özellikle bu alanın gerektirdiği temel teknik bilgiden yoksundurlar[109]. Diğer yandan farklı hukuk düzenlerinde bu suçlar bakımından maddi ceza hukukundaki farklılıklar da önemli bir problem olarak karşımıza çıkmaktadır[110]. Bu suçlar bakımından kimi hukuk düzenlerinde henüz kanuni düzenlemenin dahi yapılmamış olması failler açısından bir kurtarılmış bölge yaratmaktadır[111]. Failler, fiillerinin suç sayılmadığı bu ülkelerde bulunarak dünyanın her yerine internet aracılığıyla ulaşabilmekte ve bulunduğu yerde cezai yaptırıma tabi tutulmamaktadırlar. Böyle bir durumda suçluların iadesi için gerekli olan çifte cezalandırılabilirlik şartı da gerçekleşmediğinden, failin suçun mağdurunun bulunduğu ülkeye iadesi mümkün olamamaktadır[112]. Dolayısıyla suçla mücadelede etkili bir adli yardımlaşma için bilişim suçları bakımından, uluslararası düzlemde yeknesak bir tanım yapılmalı ve maddi ceza hukuku bakımından oluşan farklılıkları gidermek gerekmektedir[113].

Yukarıda değinilen nedenlerle birlikte, bilişim suçlarının sınır aşan yapısı, bu suçlarla mücadelede uluslararası düzeyde ortak çalışmaların yürütülmesini zorunlu kılmaktadır[114]. Bilişim suçları ile mücadelede Birleşmiş Milletler, Avrupa Birliği, Avrupa Konseyi, OECD, G8 gibi uluslararası kuruluşların çalışmaları bulunmaktadır. Bu çalışmalar içinde Avrupa Konseyi Siber Suçlar Sözleşmesini, diğer uluslararası çalışmalardan ayıran husus,

---

[107] **Başlar**, **Yusuf**; Ceza Yargılamasında Elektronik Delil, Ankara 2016, s. 24; **Henkoğlu, Türkay**; Adli Bilişim - Dijital Delillerin Elde Edilmesi ve Analizi, İstanbul 2014, s. 6–7; **Özen, Muharrem/Özocak, Gürkan**; "*Adli Bilişim, Elektronik Deliller ve Bilgisayarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK m. 134)*", Ankara Barosu Dergisi, 2015, Sayı 1, s. 57–58.

[108] **Henkoğlu**, Adli Bilişim, s. 2–3; **Özen/Özocak**, Adli Bilişim, s. 45.

[109] **Önok**, Siber Suçlarla Mücadelede Uluslararası İşbirliği, s. 1232.

[110] **Sokullu Akıncı**, AKSSS Maddi Ceza Hukuku, s. 12.

[111] **Önok**, Siber Suçlarla Mücadelede Uluslararası İşbirliği, s. 1236.

[112] **Önok**, Siber Suçlarla Mücadelede Uluslararası İşbirliği, s. 1236.

[113] **Sokullu Akıncı**, AKSSS Maddi Ceza Hukuku, s. 12; **Yılmaz**, Siber Suçlar, s. 165.

[114] **İçel**, **Kayıhan**; "*Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında Avrupa Siber Suç Politikasının Ana İlkeleri*", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, İnternet Özel Bölümü, 2001, Cilt LIX, Sayı 1–2, s. 5.

sözleşmeye taraf devletlerin, bilişim suçları bakımından kendi iç hukuklarında düzenleme yapmayı ve uluslararası adli iş birliğini taahhüt etmiş olmalarıdır. Söz konusu antlaşma her ne kadar Avrupa Konseyi nezdinde imzalanmış bir antlaşma olsa da bu antlaşmaya konsey üyesi olmayan ABD, Japonya, Güney Afrika, Kanada, Avusturalya ve İsrail de taraftır.

Avrupa Konseyi, sözleşmeyle sonuçlanan sürece, konseyin alt çalışma komitelerinden biri olan Avrupa Suç Sorunları Komitesi'nin (CDPC)[115] 1996 yılında siber suçlarla ilgilenecek bir uzmanlar komitesi kurulmasını önermesi ile başlamıştır. 1997 yılında Avrupa Konseyi Bakanlar Kurulu, söz konusu uzmanlar komitesini (PC–CY)[116] kurmuş ve komiteden siber suçlarla mücadeleye ilişkin bağlayıcı özelliğe sahip bir hukuki metin hazırlamasını istemiştir[117]. Bunun üzerine komite, taslak bir metin hazırlamış ve hazırlanan bu taslak 23 Kasım 2001'de Macaristan'ın başkenti Budapeşte'de imzaya açılmıştır. Türkiye sözleşmeyi 10.11.2010 tarihinde imzalamış, 29.09.2014 tarihinde onaylamış ve sözleşme 01.01.2015 tarihinde iç hukuk bağlamında yürürlüğe girmiştir[118]. 04.06.2017 tarihi itibariyle sözleşmeye taraf 55 ülke bulunmaktadır ve bu ülkelerin 12'si Avrupa Konseyi üyesi değildir[119].

Avrupa Konseyi Siber Suçlar Sözleşmesi (AKSSS) bilişim suçlarına yönelik imzalanmış ilk uluslararası sözleşmedir[120]. Ayrıca sözleşmeye Avrupa dışından ABD, Japonya, Kanada gibi ülkelerin de taraf olması söz konusu sözleşmenin bölgesel olmadığını, küresel bir sözleşme olduğunu ortaya koymaktadır.

2.3.2. Sözleşme'de Düzenlenen Bilişim Suçları

AKSSS kırk sekiz madde ve dört bölümden oluşmaktadır. Bu bölümler sırasıyla; terimler, ulusal düzeyde alınacak önlemler (maddi ceza hukuku ve usul hukuku), uluslararası iş birliği ve diğer hükümler şeklindedir.

---

115 The European Committee on Crime Problems.

116 Committee of Experts on Crime in Cyberspace.

117 **Dülger**, Bilişim Suçları, s. 105; **Önok**, Siber Suçlarla Mücadelede Uluslararası İşbirliği, s. 1241.

118 Çekinceler ve sözleşme metni için bkz. https://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss380.pdf, s.e.t: 08.05.2017.

119 https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=oiBOGx95, s.e.t: 04.06.2017.

120 **Sınar**, **Hasan**; "*Avrupa Konseyi Siber Suç Sözleşmesi Üzerine Bir Deneme*", Prof.Dr. Çetin ÖZEK Armağanı, İstanbul 2004, s. 773.

Sözleşme temel olarak şu ana ilkeler çerçevesinde şekillenmiştir[121]: Eylemin kasten işlenmesi ve hukuka aykırı olması; ceza sorumluluğunun sınırlarının çizilmesinde başta düşünce, kanaat ve iletişim özgürlüğü olmak üzere temel hak ve özgürlüklerin gereklerine uyulması; bilişim suçlarının belirlenip düzenlenmesinde ortak bir asgari standarda uyulması.

Terimler bölümünde; bilgisayar sistemi, bilgisayar verisi, hizmet sağlayıcı ve trafik verisi terimleri tanımlanmıştır. Ulusal düzeyde alınacak önlemlerden maddi ceza hukukuna ilişkin kısımda taraf devletlerin hangi fiilleri cezai yaptırım altına alacağı belirlenmiştir. Usul hukukuna ilişkin kısımda ise özellikle bilişim suçlarında suç delillerine ulaşmanın ve mahkeme önünde temsil edici, bütünlüğü bozulmamış delil elde etmenin zorluğu nedeniyle ulusal hukuka yön gösterici hükümler getirilmiştir[122]. Uluslararası iş birliği bölümünde ise klasik suçlardan farklı olarak bilişim suçlarına özgü uluslararası adli yardımlaşmaya ilişkin hükümler bulunmaktadır[123].

Çalışma konumuz açısından önem arz ettiğinden AKSSS'de düzenlenen suç tiplerini sıralamakta fayda görüyoruz. Zira Türkiye sözleşmeye taraf olmak bakımından, bu sözleşmedeki suçları, kendi iç hukukunda düzenlemeyi taahhüt etmiş bulunmaktadır. Bilişim suçları bölümünde inceleyeceğimiz Türk Hukuku'ndaki suç türleri bakımından, hangi suçun AKSSS'deki hangi düzenlemenin karşılığı olduğuna ilgili suçları incelerken değineceğiz. Sözleşmede tanımlanan suç tiplerini şu şekilde sıralayabiliriz:

- Bilgisayar verilerinin ve sistemlerinin gizliliğine, bütünlüğüne ve erişilebilirliğine yönelik suçlar[124]: Yasadışı erişim, yasadışı araya girme, verilere müdahale, sisteme müdahale, cihazların kötüye kullanımı.
- Bilgisayarla bağlantılı suçlar[125]: Bilgisayarla bağlantılı sahtecilik, bilgisayarla bağlantılı dolandırıcılık.
- İçerikle bağlantılı suçlar[126]: Çocuk pornografisiyle bağlantılı suçlar

[121] Detaylı bilgi için bkz. **İçel**, Avrupa Siber Suç Politikasının Ana İlkeleri, s. 6–10.

[122] Detaylı bilgi için bkz. **Keskin Kiziroğlu**, **Serap**; "*Avrupa Konseyi Siber Suç Sözleşmesinde Ceza Muhakemesine İlişkin Hükümlerin Değerlendirilmesi*", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, 2013, Cilt 59, Sayı 1–2, s. 155–180.

[123] Detaylı bilgi için bkz. **Önok**, Siber Suçlarla Mücadelede Uluslararası İşbirliği, s. 1229 - 1270.

[124] AKSSS m. 2-6.

[125] AKSSS m. 7-8.

[126] AKSSS m. 9.

- Telif hakkı ve bununla bağlantılı hakların ihlaline ilişkin suçlar[127].

2.4. 765 Sayılı TCK'da Düzenlenen Bilişim Suçları

Türk Hukuku'nda bilişim suçları, ilk defa 3756 sayılı kanun ile 06.06.1991 yılında düzenleme alanı bulmuştur[128]. 3756 sayılı kanun ile 765 sayılı Türk Ceza Kanunu'na 11. bap olarak bilişim alanında suçlar eklenmiştir. Bu suçlar 525/a, 525/b ve 525/c olmak üzere üç maddede düzenlenmiştir.

765 sayılı TCK'daki bilişim alanında suçlara ilişkin düzenlemelere, Fransız Ceza Kanunu Tasarısı kaynaklık etmiştir ve tasarıdaki bu suçlar ile ilgili düzenlemeler, neredeyse tamamen Türkçe'ye çevrilerek kanunlaştırılmıştır[129]. 5237 sayılı TCK'dan farklı olarak bilişim sistemi yerine *"bilgileri otomatik işleme tabi tutan sistem"* teriminin kullanılmasının nedeni de Fransız Ceza Kanunu Tasarısı'nın Türkçe'ye çevirisinden kaynaklanmaktadır[130]. Ancak Fransız Ceza Kanunu Tasarısı'nda bu suçların düzenlendiği bölüm için *"bilgileri otomatik işleme tabi tutan sistemlere karşı saldırılar"* başlığı kullanılsa da 765 sayılı TCK'da bundan farklı olarak 11. babın başlığı "*bilişim alanında suçlar"* olarak tercih edilmiş fakat madde metninde *"bilişim"* ifadesi yerine *"bilgileri otomatik işleme tabi tutan sistem"* ifadesi kullanılmıştır[131].

765 sayılı TCK'da bilişim alanında suçları beş başlık altında şu şekilde sıralayabiliriz[132]:

- Sistemden programları, verileri veya diğer herhangi bir unsuru ele geçirmek (m. 525/a/1)[133]
- Sistemdeki programları, verileri veya diğer herhangi bir unsuru başkasına zarar vermek amacıyla kullanmak, nakletmek, çoğaltmak (m. 525/a/2)[134]

---

[127] AKSSS m. 10.

[128] **Yenidünya/Değirmenci**, Bilişim Suçları, s. 28.

[129] **Dülger**, Bilişim Suçları, s. 237.

[130] **Gürler**, Bilişim Alanında Suçlar, s. 35; **Kurt**, Tüm Yönleriyle Bilişim Suçları, s. 124.

[131] **Gürler**, Bilişim Alanında Suçlar, s. 35; **Kurt**, Tüm Yönleriyle Bilişim Suçları, s. 125.

[132] **Dülger**, Bilişim Suçları, s. 239.

[133] Madde 525/a/1: "*Bilgileri otomatik olarak işleme tabi tutmuş bir sistemden,programları, verileri veya diğer herhangi bir unsuru hukuka aykırı olarak ele geçiren kimseye bir yıldan üç yıla kadar hapis ve birmilyon liradan onbeşmilyon liraya kadar ağır para cezası verilir."*

[134] Madde 525/a/2: *"Bilgileri otomatik işleme tabi tutmuş bir sistemde yer alan bir programı, verileri veya diğer herhangi bir unsuru başkasına zarar vermek üzere kullanan, nakleden veya çoğaltan kimseye de yukarıdaki fıkrada yazılı ceza verilir"*

- Verilere veya veri işleme zarar vermek (m. 525/b/1)[135]
- Bilişim sistemi aracılığıyla haksız yarar sağlama (m. 525/b/2)[136]
- Verilerde sahtekarlık yapılması ve oluşturulan sahte belgenin kullanılması (m. 525/c)[137]

5237 sayılı Türk Ceza Kanunu'ndan farklı olarak 765 sayılı Türk Ceza Kanunu'nda bilişim sistemine girmenin herhangi bir cezai yaptırıma tabi tutulmadığı görülmektedir[138]. Doktrinde eleştirilen bu durum 5237 sayılı TCK'da çözüme kavuşturulmuştur. Ayrıca 765 sayılı TCK'da banka veya kredi kartlarının kötüye kullanılmasına ilişkin bir düzenleme getirilmemiş, bunlarla ilgili suçlar bilişim sistemi aracılığıyla haksız yarar sağlama suçu içerisinde cezai yaptırıma tabi tutulmuştur[139].

Bu noktada çalışmamızda inceleyeceğimiz suç türünün sınırlarının çizilmesi açısından önem arz eden 5237 sayılı TCK'daki bilişim suçlarını inceleyeceğiz ve yeri geldikçe bu suçlar ile 765 sayılı TCK'da düzenlenen bilişim alanında suçları karşılaştıracağız.

2.5. 5237 Sayılı TCK'da Düzenlenen Bilişim Suçları

765 sayılı TCK'da ilk defa kanuni düzenleme alanı bulan bilişim alanında suçlar, 1 Haziran 2005'te yürürlüğe giren 5237 sayılı Türk Ceza Kanunu'nda da aynı isimle, yani *"bilişim alanında suçlar"* ismiyle, topluma karşı suçlar kısmının onuncu bölümünde düzenlenmiştir.

Yukarıda ifade edildiği üzere bilişim suçları, doktrindeki genel görüş göre, geniş anlamda ve dar anlamda olmak üzere ikiye ayrılmaktadır[140]. 5237 sayılı TCK'da da geniş anlamda ve dar anlamda bilişim suçlarının düzenleme alanı bulduğu görülmektedir. Söz gelimi hırsızlık

---

[135] Madde 525/b/1: *"Başkasına zarar vermek veya kendisine veya başkasına yarar sağlamak maksadıyla,bilgileri otomatik işleme tabi 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 beşmilyon liradan ellimilyon liraya kadar ağır para cezası verilir."*

[136] Madde 525/b/2: *"Bilgileri otomatik işleme tabi tutmuş bir sistemi kullanarak kendisi veya başkası lehine hukuka aykırı yarar sağlayan kimseye bir yıldan beş yıla kadar hapis ve ikimilyon liradan yirmimilyon liraya kadar ağır para cezası verilir"*

[137] Madde 525/c: "*Hukuk alanında delil olarak kullanılmak maksadıyla sahte bir belgeyi oluşturmak için bilgileri otomatik olarak işleme tabi tutan bir sisteme,verileri veya diğer unsurları yerleştiren veya var olan verileri,diğer unsurları tahrif eden kimseye bir yıldan üç yıla kadar,tahrif edilmiş olanları bilerek kullananlara altı aydan iki yıla kadar hapis cezası verilir."*

[138] **Koca/Üzülmez**, Özel Hükümler, s. 805.

[139] **Özbek**, Banka veya Kredi Kartlarının, s. 1020.

[140] **Avşar/Öngören**, Bilişim Hukuku, s. 124; **Dülger**, Bilişim Suçları, s. 83; **Ergün**, Siber Suçların, s. 29–32; **Gürler**, Bilişim Alanında Suçlar, s. 82.

suçu bu ayrıma göre klasik suç tiplerinden biridir. Bilişim sistemlerinin icadı ile bu suçun bilişim sistemlerinin vasıta olarak kullanılması suretiyle işlenmesi mümkün hale gelmiştir. Dolayısıyla bilişim sistemleri vasıtasıyla işlenen hırsızlık suçu, geniş anlamda bilişim suçuna dahildir[141].

5237 sayılı TCK'da dar anlamda bilişim suçları topluma karşı suçlar kısmının onuncu bölümünde, bilişim alanında suçlar olarak düzenlenmişken geniş anlamda bilişim suçları ayrı bir bölüm olarak düzenlenmemiş ve kimi klasik suçlarda bilişim sistemlerinin vasıta olarak kullanılması ağırlaştırıcı neden olarak öngörülmüştür. Örneğin hırsızlık (TCK m. 142/2-e) ve dolandırıcılık (TCK m. 158/1-f) suçlarının işlenmesinde bilişim sistemlerinin kullanılması cezayı ağırlaştırıcı neden olarak kabul edilmiştir.

765 sayılı TCK'da suçlar, korunan hukuki değere göre bir sınıflandırmaya tabi tutulmuşsa da *"bilişim alanında suçlar babı"*ndaki suçlar*, "bilgileri otomatik işleme tabi tutan sistem"* ortak kavramı ile bir araya getirilmiş suçlar olmuştur. Söz konusu bu husus, doktrinde kanunun genel yapısıyla çelişki ortaya çıkardığından eleştirilmiştir[142]. Bu eleştirileri göz önüne almış olacak ki kanun koyucu, 5237 sayılı TCK'da bilişim suçlarını mümkün olduğunca[143] korunan hukuki değere göre bir araya getirmiştir.

5237 sayılı TCK m. 243 vd. onuncu bölümde bir araya getirilen suç türleri, esasında birden fazla hukuki değeri koruyan, karma hukuki değere sahip suçlardır[144]. Karma hukuki değere sahip bu suçların ortak noktası bilişim sistemlerinin güvenilirliğine karşı işlenen suçlar olmasıdır[145]. Böylece günümüzde birçok gündelik, ekonomik, hukuksal işlemin yapıldığı

---

141 **Gül**, Doğrudan - Dolaylı Bilişim Suçları, s. 213.

142 Dülger'in 765 sayılı TCK ile ilgili olarak açıklamaları şu şekildedir: *"Verilerde sahtekarlık yapılması ve bilişim sistemi aracılığıyla hukuka aykırı yarar sağlanması suçları dışındaki diğer suç tiplerinde suçla korunan hukuksal değer karma nitelik göstermekte ve herhangi bir hukuksal değer diğerinden daha çok korunmayı gerektirecek bir nitelik göstermemektedir. Bu nedenle, verilerde sahtekarlık yapılması suçunun koruduğu hukuksal değere göre 'kamunun güvenine karşı suçlar' babında düzenlenmesi gerekirken 'bilişim alanında suçlar' babında düzenlenmesi ve bilişim sistemi aracılığıyla hukuka aykırı yarar sağlanması suçunun koruduğu hukuksal değere göre 'mala karşı suçlar' babında düzenlenmesi gerekirken yine 'bilişim alanında suçlar' babında düzenlenmesi hatalıdır."* (**Dülger**, Bilişim Suçları, s. 235.)

143 TCK m. 245 banka veya kredi kartlarının kötüye kullanılması suçunda korunan hukuksal değerin malvarlığı olduğundan bahisle bu suçun malvarlığına karşı suçlar bölümünde düzenlenmesi gerektiği doktrinde genel olarak ifade edilmektedir. Ayrıntılı bilgi için bkz. **Özbek**, Banka veya Kredi Kartlarının, s. 1021–1022.

144 **Erdoğan**, TCK'da Bilişim Suçları, s. 120; **Kurt**, Tüm Yönleriyle Bilişim Suçları, s. 148; **Parlar**, Bilişim Suçları, s. 15; **Taşdemir**, Bilişim, Banka veya Kredi Kartlarının Kötüye Kullanılması ve Dolandırıcılık Suçları, s. 255; **Taşkın**, Bilişim Suçları, s. 335.

145 **Dülger**, Bilişim Suçları, s. 234.

bilişim sistemlerine toplumda duyulan güven korunmuş olmaktadır. Kanaatimizce bu suçların, topluma karşı suçlar kısmında düzenlemesinin nedeni de budur.

5237 sayılı TCK'da bilişim alanında suçlar, 765 sayılı TCK'dan oldukça farklı düzenlenmiştir. Öncelikle *"bilgileri otomatik işleme tabi tutan sistem"* ifadesi yerine bilişim sistemi ifadesi tercih edilmiştir. Bu terim seçimi genel olarak doktrinde ilgili bilim dalının esas alınması ve böylece ileride ortaya çıkabilecek teknolojik gelişmeleri de içerebileceğinden olumlu karşılanmıştır[146]. Ancak önceki kanundan farklı olarak bu sefer gerekçede bilişim ifadesinin tanımı yapılmamıştır.

Önceki kanun döneminde sert bir şekilde eleştirildiğinden bilişim sistemine girme fiili, bu kez 5237 sayılı TCK'da kanuni düzenlemeye kavuşmuştur[147].

Suçun konusu olarak *"diğer herhangi bir unsur"* kavramı[148] kaldırılmıştır. Böylece kanaatimizce genel olarak bilişim suçlarında suçun konusu *"veri"*den ibaret kalmıştır. Yukarıda bilgisayar ve bilişim sistemini açılarken ifade ettiğimiz üzere bir bilişim sisteminin en temel birimi veridir. Veri olmaksızın bir bilişim sisteminden bahsetmemiz mümkün değildir. Dolayısıyla bir bilişim sisteminde, dar anlamda bilişim suçları bakımından, kanaatimizce veriden başka herhangi bir unsur bulunmamaktadır[149].

Yeni TCK'da öncekinden farklı olarak bilişim suçlarında dikkat çeken bir diğer düzenleme ise banka veya kredi kartlarının kötüye kullanılması suçunun ilk defa düzenlenmiş olmasıdır[150]. 765 sayılı TCK'da banka ve kredi kartlarının kötüye kullanılmasına ilişkin fiiller m. 525/b/2'de düzenlenen bilişim sistemi aracılığıyla haksız yarar sağlama suçuyla koruma altına alınmışken yeni kanunda bununla ilgili olarak özel bir suç türü ihdas edilmiştir[151].

---

[146] **Artuk, Mehmet Emin/Gökcen, Ahmet/Yenidünya, A. Caner**; Ceza Hukuku Özel Hükümler, Ankara 2015, s. 858.

[147] **Kurt**, Tüm Yönleriyle Bilişim Suçları, s. 136.

[148] Diğer herhangi bir unsur kavramı için bkz. **Dülger**, Bilişim Suçları, s. 83; **Kurt**, Tüm Yönleriyle Bilişim Suçları, s. 144.

[149] Bilişim sistemlerinin donanımlarına verilen fiziki zararların dar anlamda bilişim suçu olarak ifade edilemeyeceği, olsa olsa mala zarar verme suçuna vücut verileceği daha önce de ifade edilmişti.

[150] **Artuk/Gökcen/Yenidünya**, Özel Hükümler, s. 895; **Özbek**, Banka veya Kredi Kartlarının, s. 1020.

[151] **Artuk/Gökcen/Yenidünya**, Özel Hükümler, s. 895; **Özbek**, Banka veya Kredi Kartlarının, s. 1020.

Çalışmamızın ana konusunu teşkil eden 5237 sayılı TCK m. 244/4'te düzenlenen bilişim sistemi aracılığıyla haksız yarar sağlama suçunun 765 sayılı TCK'daki karşılığı (m. 525/b/2) benzer şekilde ifade edilmiş olsa da yeni kanunun bilişim alanında suçları düzenlemede tercih ettiği sistem ve ihdas edilen yeni suç türleri ile yeni TCK'daki suç, eski TCK'daki suçtan farklılaşmıştır. Bu husus çalışmamızın esas bölümünü teşkil eden ikinci bölümünde detaylıca ele alınacaktır.

Ayrıca 24.03.2016 tarihinde 6698 sayılı kanun ile TCK'nın bilişim alanında suçlar bölümüne *"veri nakillerini teknik araçlarla izleme"* (TCK m. 243/4) ve *"yasak cihaz veya programların üretilmesi ve ticareti"* (TCK m. 245/A) suçları eklenmiştir.

Bilişim sistemi ile haksız yarar sağlama suçunun unsurlarının açıklandığı ikinci bölüme geçmeden önce; inceleyeceğimiz suç türünün tali bir norm oluşunu dikkate alarak ve bu suçun uygulama alanının belirlenebilmesi amacıyla, diğer bilişim suçlarına kısaca değinilmesinde yarar görmekteyiz.

İnceleme konumuz olan bilişim sistemi aracılığıyla haksız yarar sağlama suçu kanunda tali norm olarak düzenlenmiştir[152]. Zira TCK m. 244/4'te failin bu suçtan sorumlu olabilmesi için işlenen fiille *"haksız bir çıkar sağlamasının başka bir suç oluşturmaması"* hükme bağlanmıştır. Dolayısıyla bilişim sistemi ile haksız yarar sağlama suçunun unsurlarının açıklandığı ikinci bölüme geçmeden önce; inceleyeceğimiz suç türünün uygulama alanının belirlenebilmesi amacıyla, diğer bilişim suçlarına kısaca değinilmesinde yarar görmekteyiz.

2.5.1. *"Bilişim Alanında Suçlar"* Bölümünde Düzenlenen Suçlar

TCK'nın genel sistematiğine uygun olarak bilişim alanında suçlar bölümündeki suçlar korunan hukuki değer kavramı ile bir araya getirilmiştir. Daha önce de ifade edildiği üzere bu suçlar karma hukuki değere sahip suçlardır[153] ve esas itibariyle bu suçların koruduğu

[152] **Artuk/Gökcen/Yenidünya**, Özel Hükümler, s. 892; **Erdoğan**, TCK'da Bilişim Suçları, s. 264; **Ketizmen**, Bilişim Suçları, s. 182; **Koca, Mahmut**; "*Hukukumuzda TCK'nın 244'ncü maddesi Kapsamında Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu*", 9-10 Ekim 2008 Yargıtay Bilişim Hukuku Konferansı, sunulmuş bildiri, Ankara, s. 97; **Özbek, Veli Özer/Doğan, Koray/Bacaksız, Pınar/Tepe, İlker**; Türk Ceza Hukuku Özel Hükümler, Ankara 2016, s. 955.

[153] **Erdoğan**, TCK'da Bilişim Suçları, s. 120; **Kurt**, Tüm Yönleriyle Bilişim Suçları, s. 148; **Parlar**, Bilişim Suçları, s. 15; **Taşdemir**, Bilişim, Banka veya Kredi Kartlarının Kötüye Kullanılması ve Dolandırıcılık Suçları, s. 255; **Taşkın**, Bilişim Suçları, s. 335.

ortak hukuki değer bilişim sistemlerinin doğru işleyeceğine dair toplumdaki güven duygusudur[154].

2.5.1.1. Bilişim Sistemine Girme veya Orada Kalma Suçu (TCK m. 243)

Bu suçta korunan hukuki değer karma nitelik arz etmektedir[155]. Öncelikle kişilerin özel hayatlarının gizliliği ve haberleşme özgürlükleri korunmaktadır[156]. Diğer yandan bilişim sisteminin güvenliği koruma altına alınmıştır[157].

Fail, madde metninde *"kimse"* ifadesi kullanıldığından herkes olabilir[158]. Hukuka aykırı olarak bilişim sistemine girilen veya bilişim sisteminde kalınmaya devam edilen kimse ise bu suçun mağdurudur[159].

Suçun konusu, bilişim sistemi ve sistemdeki verilerdir[160]. Bu noktada dikkat edilmesi gerekir ki bilişim sisteminin donanım unsuru, suçun konusu olmamakta sistemin yazılım unsuru yani sanal unsurları/sanal ortamı suçun konusunu oluşturmaktadır. Zira bilişim sistemine girmek veya orada kalmaktan kasıt, bilişim sisteminin fiziki varlığına girilmesi değil bilişim sisteminin sanal ortamına yani içindeki verilere girilmesidir[161]. Örneğin bir bilgisayarın kasasının açılarak içindeki donanım parçalarına ulaşılması bu suçu oluşturmayacak, olsa olsa mala zarar verme suçunu oluşturacaktır.

Suçun fiil unsurunda, doktrindeki görüşleri de dikkate alarak, 24.03.2016 tarihinde 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 30. maddesi ile değişikliğe gidilmiştir. Bu değişiklik ile bilişim sistemine girme *"ve"* kalmaya devam etme fiili girme *"veya"* kalmaya devam etme olarak değiştirilmiştir.

---

[154] **Dülger**, Bilişim Suçları, s. 234; **Koca/Üzülmez**, Özel Hükümler, s. 801: *"Bilişim sistemlerinin güvenliği, sistemin manipüle edilmeden doğru ir şekilde işlemesi, içerdiği verilerin bütünlüğü, sıhhati, kredi kartlarının kullanılma yoğunluğu ve ekonomik sistemdeki rolü nedeniyle, bu sistemlerini kötüye kullanılmasının önlenmesi toplumdaki herkesin yararınadır."*

[155] **Özbek/Doğan/Bacaksız/Tepe**, Özel Hükümler, s. 932.

[156] **Yenidünya**, Hukuka Aykırı Erişim Suçu, s. 1024.

[157] **Dülger**, Bilişim Suçları, s. 348; **Karagülmez**, Bilişim Suçları, s. 201; **Yenidünya**, Hukuka Aykırı Erişim Suçu, s. 1024.

[158] **Artuk/Gökcen/Yenidünya**, Özel Hükümler, s. 865; **Koca/Üzülmez**, Özel Hükümler, s. 808.

[159] **Yenidünya**, Hukuka Aykırı Erişim Suçu, s. 1027.

[160] **Soyaslan, Doğan**; Ceza Hukuku Özel Hükümler, Ankara 2016, s. 643.

[161] **Erdoğan**, **Yavuz**; "*Bilişim Sistemine Girme ve Kalma Suçu*", Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, 2010, Cilt 12, Sayı Özel, s. 1365.

Kanunun önceki halinde ve bağlacından ne anlaşılması gerektiği tartışma konusu olmuştu[162]. Ancak kanunun önceki halinin lafzından da anlaşıldığı üzere yalnızca sisteme girmek bu suça vücut vermeyecek failin aynı zamanda sisteme girdikten sonra belli bir süre kalmaya devam etmesi gerekecekti. Bu durum ise doktrinde eleştirilmiş, düzenlemenin yetersiz kaldığı ifade edilmiş, failin yalnızca sisteme girmesi ancak orada kalmaması durumunda cezalandırılmasının mümkün olmayacağı ifade edilmiştir[163]. Nitekim Avrupa Konseyi Siber Suçlar Sözleşmesi'nin 2. maddesinde hukuka aykırı erişimin suç olarak düzenlenmesi gerektiği hükme bağlanmışken, sistemde kalmaya ilişkin bir düzenleme getirilmemiştir[164].

Söz konusu düzenleme ile bu suç, seçimlik hareketli bir suç haline gelmiştir[165]. Bilişim sistemine girme seçimlik hareketi, sistemin tamamındaki veya bir kısmındaki verilerin içeriğine dahil olmadır[166]. Sistemde kalmaya devam etme seçimlik hareketi ise mütemadi hareketi gerektirmektedir[167]. Bu noktada sistemde kalmaya devam etme seçimlik hareketinin sisteme girme seçimlik hareketinden ayrı düşünülemeyeceği akla gelebilir. Gerçekten işlenen suçların çoğunda iki seçimlik hareket gerçekleşecek olsa da bu hareketlerin birbirinden ayrılması imkânsız değildir[168]. Örneğin, bir kimsenin kullandığı bilişim sistemi, bir başka bilişim sistemine bir yazılım hatası nedeniyle kendiliğinden girmiş yahut başka biri tarafından kullanılan bir bilişim sistemi vasıtasıyla sokulmuş olabilir. Bu durumu sonradan fark eden sistem sahibi, girilen sistemden çıkmamış ise bilişim sistemine girme seçimlik hareketini gerçekleştirmemiş ancak sistemde kalmaya devam etme hareketini gerçekleştirmiş olacaktır[169].

---

[162] Tartışmalar için bkz. **Dülger**, Bilişim Suçları, s. 365; **Koca/Üzülmez**, Özel Hükümler, s. 811; **Soyaslan**, Özel Hükümler, s. 635; **Taşkın**, Bilişim Suçları, s. 24–25; **Yenidünya**, Hukuka Aykırı Erişim Suçu, s. 1034.

[163] **Karagülmez**, Bilişim Suçları, s. 643.

[164] **Erdoğan**, Bilişim Sistemine Girme, s. 1369.

[165] **Özbek/Doğan/Bacaksız/Tepe**, Özel Hükümler, s. 936.

[166] **Yenidünya**, Hukuka Aykırı Erişim Suçu, s. 1037.

[167] **Yenidünya**, Hukuka Aykırı Erişim Suçu, s. 1034.

[168] **Koca/Üzülmez**, Özel Hükümler, s. 814.

[169] **Koca/Üzülmez**, Özel Hükümler, s. 814.

Bilişim sistemine zarar verme ya da verileri ele geçirme, suçun unsuru olarak kanunda aranmadığı için bu suç neticesiz suçlardandır[170]. Dolayısıyla bu suça teşebbüs, ancak hareket parçalara bölünebiliyorsa mümkündür[171].

Suçun manevi unsuru kasttır. Suçun oluşumu için failde özel bir saik veya amaç aranmamıştır. Ancak madde metninde *"hukuka aykırı olarak"* ifadesi kullanıldığından failin işlediği fiilin haksızlık teşkil ettiği hususunda bilgisi bulunmalıdır[172].

Bu suçta, fiilin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi hafifletici neden olarak düzenlenmiştir. Bu durumun hafifletici değil bilakis ağırlaştırıcı neden olması gerektiğini savunanlar[173] olmakla birlikte doktrindeki diğer bir görüşe göre düzenleme yerindedir zira bu sistemler üzerinde korunan hukuki değer, diğer sistemlerden farklı olarak nispeten daha düşüktür. Çünkü bu sistemlerde mahremiyet değil ekonomik çıkar korunmaktadır[174].

Fiil sebebiyle sistemin içerdiği verilerin yok olması veya değişmesi ise bu suçun neticesi sebebiyle ağırlaşmış halini oluşturur[175]. Burada dikkat edilmesi gereken husus failin kastının sistemdeki verilere zarar vermek olmaması gerektiğidir. Zira bu durumda bilişim sistemine girme suçu değil, TCK m. 244'teki sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu söz konusu olacaktır[176]. Öte yandan TCK m. 23 gereğince failin bu neticeden sorumlu olması için en azından taksirle hareket etmesi gerekecektir[177]. Kanunumuzun neticesi sebebiyle ağırlaşmış suçlar bakımından öngördüğü en azından

---

[170] **Dülger**, Bilişim Suçları, s. 369.

[171] **Özbek/Doğan/Bacaksız/Tepe**, Özel Hükümler, s. 941.

[172] **Koca/Üzülmez**, Özel Hükümler, s. 815.

[173] **Dülger**, Bilişim Suçları, s. 378; **Özbek/Doğan/Bacaksız/Tepe**, Özel Hükümler, s. 911.

[174] **Artuk/Gökcen/Yenidünya**, Özel Hükümler, s. 874; **Karagülmez**, Bilişim Suçları, s. 189; **Koca/Üzülmez**, Özel Hükümler, s. 816; **Pallı**, **Hayati**; Türk Hukukunda ve Mukayeseli Hukukta Bilişim Suçları, Yayımlanmamış Doktora Tezi, Erciyes Üniversitesi Sosyal Bilimler Enstitüsü, Kayseri 2008, s. 154.

[175] **Erdoğan**, Bilişim Sistemine Girme, s. 1402; **Soyaslan**, Özel Hükümler, s. 640. Neticesi sebebiyle ağırlaşmış suç için bkz. **Artuk, Mehmet Emin/Gökcen, Ahmet/Yenidünya, A.Caner**; Ceza Hukuku Genel Hükümler, Ankara 2016, s. 369–378.: *"Neticesi sebebiyle ağırlaşmış suçlarda ya failin hareketi sonucu kastettiğinden daha ağır bir netice ortaya çıkmakta, ya da suçun oluşması için arana neticeden daha ağır başka bir netice meydana gelmektedir."*

[176] **Yenidünya**, Hukuka Aykırı Erişim Suçu, s. 1041.

[177] **Dülger**, Bilişim Suçları, s. 371.

taksirle hareket etme unsuru, AKSSS'de temel ilke olarak kabul edilen, failin sorumluluğu için kasten hareket etmesi gerektiği ilkesine aykırı olması nedeniyle eleştirilmektedir[178].

Suçun temel halinin yaptırımı, bir yıla kadar hapis veya adli para cezasıdır. Suçun bedeli karşılığı yararlanılan sistemler hakkında işlenmesi halinde ceza yarı oranına kadar indirilir. Son olarak, sisteme girme fiili nedeniyle, sistemin içerdiği veriler yok olur veya değişirse failin sorumluluğu altı aydan iki yıla kadar hapis cezası olacaktır.

2.5.1.2. Veri Nakillerini Teknik Araçlarla İzleme Suçu (TCK m. 243/4)

24.03.2016 tarihinde 6698 sayılı kanun ile TCK m. 243'e 4. fıkra eklenmiştir. Bu fıkrada bilişim sistemine girmeksizin ağ üzerinden veri akışlarının izlenmesi hali ayrı bir suç olarak düzenlenmiştir[179]. Gerçekten bir bilişim ağı olan internete girilmesi hukuka aykırı olmadığından internet üzerinde herhangi bir kimsenin bilişim sistemine girmeden ağ üzerindeki verileri okuması (örneğin*, "sniffing*" yöntemiyle[180]) m. 243/1 anlamında bilişim sistemine girme suçunu oluşturmayacaktır. Yine bilişim sistemine girmeksizin internet üzerinden gönderilen kriptolu verilerin güvenliğini kırarak içeriğine erişilmesi durumunda da bilişim sistemine girme suçu söz konusu olmayacaktır. Bu hallerde verilere zarar verme de söz konusu olmadığından TCK m. 244 anlamında da tipiklik oluşmayacaktır. Dolayısıyla kanun koyucu getirilen bu düzenleme ile esasen söz konusu boşluğu doldurmuş ve veri iletişiminin gizliliğini ve mahremiyetini koruma altına almıştır[181]. Ağ üzerindeki verilerin izlenmesi fiilinin, bilişim sistemine girme suçuna nazaran daha ağır cezayı gerektirmesinin nedeni, ağ üzerinden gerçekleşen bu fiillerin, mağdurun sistemine girilmesi söz konusu olmadığından fark edilmelerinin çok zor oluşudur. Ayrıca bilişim sistemine girme suçundan farklı olarak bu suçta, sisteme girme fiili değil, veri nakillerini sisteme girmeksizin izleme fiili cezai yaptırım altına alınmıştır.

Söz konusu suçun düzenlenmesi ile Türkiye, AKSSS'ye taraf olmanın gerektirdiği yükümlülüğü yerine getirmiştir. Zira AKSSS *"yasadışı araya girme"* başlıklı 3.

---

[178] **Yenidünya**, Hukuka Aykırı Erişim Suçu, s. 1041.

[179] **Koca/Üzülmez**, Özel Hükümler, s. 820; **Özbek/Doğan/Bacaksız/Tepe**, Özel Hükümler, s. 938.

[180] **Akarslan**, Bilişim Suçları, s. 102: *"Gizlice dinleme (sniffing), bir bilgisayar ağında iletişim halindeki veriye erişmektir. Veri trafiğinin akmasına engel olunmadan verinin bir kopyası ağı gizlice dinleyen kişinin bilgisayarına yönlendirilir. Bir paket (ağ üzerinde veriler paketler halinde çalışır) koklayıcı ağ üzerindeki tüm trafiği kontrol etmek için bilgisayar içerisine yerleşir ve kendi kendine çalışır."*

[181] **Koca/Üzülmez**, Özel Hükümler, s. 820.

maddesinde[182] bilişim sistemine girilmeksizin teknik araçlarla veri nakillerini izleme fiilleri bakımından taraf devletlere düzenleme yapma yükümlülüğü getirmiştir[183].

Bu suç için yaptırım olarak bir yıldan üç yıla kadar hapis cezası öngörülmüştür.

2.5.1.3. Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu (TCK m. 244/1,2,3)

Bilişim sistemini engelleme, bozma; verileri yok etme veya değiştirme suçu TCK m. 244'te dört fıkra halinde düzenlenmiştir. Bu maddenin dördüncü fıkrası, doktrindeki genel kanaate göre ilk üç fıkradan bağımsız bir suç teşkil etmektedir[184]. Çalışmamızın esasını teşkil eden bu fıkrada; bilişim sistemi aracılığıyla haksız yarar sağlama suçunun fiil unsuru, bu maddenin ilk iki fıkrasındaki suçların, fiil unsuruna atıf yapılmak suretiyle düzenlenmiştir. Dolayısıyla TCK m. 244/1 ve 2'deki suçların fiil unsuru bu başlık altında incelenmeyecek olup, ikinci bölümde bilişim sistemi aracılığıyla haksız yarar sağlama suçunun unsurları kısmında detaylıca ele alınacaktır.

---

[182] AKSSS m. 3 Yasadışı araya girme: *"Taraflardan her biri, bilgisayar verileri taşıyan bir bilgisayar sisteminden elektromanyetik dalgalarla yayılma da dahil olmak üzere, bilgisayar verilerinin bir bilgisayar sisteminden diğer bir bilgisayar sistemine veya bir bilgisayar sisteminin kendi içinde umuma kapalı olarak iletimi esnasında teknik yöntemler kullanılarak gerçekleştirilen araya girme fiilinin, haksız yere ve kasten yapıldığı zaman, kendi iç hukuku kapsamından cezai suç olarak tanımlanması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir. Taraflardan biri, söz konusu suçun sahtekarlığa yönelik veya başka bir bilgisayar sistemine bağlı bir bilgisayar sistemiyle ilişkili olarak işlenmiş olmasını şart koşabilir."*

[183] **Koca/Üzülmez**, Özel Hükümler, s. 820.

[184] **Artuk/Gökcen/Yenidünya**, Özel Hükümler, s. 891; **Dülger**, Bilişim Suçları, s. 439; **Erdoğan**, TCK'da Bilişim Suçları, s. 247; **Gürler**, Bilişim Alanında Suçlar, s. 153; **Hafızoğulları, Zeki/Özen, Muharrem**; Türk Ceza Hukuku Özel Hükümler Topluma Karşı Suçlar, Ankara 2016, s. 457; **Ketizmen**, Bilişim Suçları, s. 148; **Koca/Üzülmez**, Özel Hükümler, s. 834; **Soyaslan**, Özel Hükümler, s. 651; **Taşkın**, Bilişim Suçları, s. 56; **Tezcan, Durmuş/Erdem, Mustafa Ruhan/Önok, R.Murat**; Teorik ve Pratik Ceza Özel Hukuku, Ankara 2010, s. 775; **Yılmaz**, **Sacit**; "*5237 Sayılı TCK'nın 244. Maddesinde Düzenlenen Bilişim Alanındaki Suçlar*", TBB Dergisi, 2011, Sayı 92, s. 86.

Kanun koyucu, TCK m. 244/1 ve 2'yi düzenlemekle AKSSS'nin 4.[185] ve 5.[186] maddelerinden kaynaklanan taahhüdünü yerine getirmiş bulunmaktadır[187].

1. ve 2. fıkra, doktrinde genel olarak kabul edildiği üzere farklı suçlardır[188]. Suçun konusu 1. fıkrada bilişim sistemlerinin işleyişi iken 2. fıkrada bilişim sistemindeki verilerdir[189].

Bu bölümdeki diğer suçlarda olduğu gibi bu iki suçta da korunan hukuki değer karma nitelik arz etmektedir. Bu suçlarla bir yandan toplumun bilişim sistemlerinin doğru işleyeceğine dair güven duygusu korunurken bir yandan da bilişim sistemleri ve bunların içerdiği verilerin kişinin malvarlığına dahil bir değer olarak korunması söz konusudur.[190]

Bu suçlarda kanun koyucu fail ve mağdur bakımından bir sınırlama getirmemiştir. Herkes bu suçların faili ve mağduru olabilir[191]. Bu anlamda, 1. fıkra için bilişim sistemi engellenen ya da bozulan kimse mağdur olurken; 2. fıkra için sistemdeki verileri yok edilen, bozulan, erişilmez kılınan, sistemine veri yerleştirilen ya da sistemde var olan verileri başka bir yere gönderilen kimse suçun mağduru olacaktır.

Birinci fıkrada yaptırım altına alınan, bilişim sisteminin engellenmesi veya bozulması neticelerine neden olabilecek fiiller iken; ikinci fıkrada, sistemdeki verilerin bozulması, yok edilmesi, değiştirilmesi, erişilmez kılınması, sisteme veri yerleştirilmesi, var olan verilerin

---

185 AKSSS m. 4 – Verilere Müdahale: *"Taraflardan her biri, bilgisayar verilerine haksız yere zarar verilmesi, verilerin silinmesi, tahrip edilmesi, değiştirilmesi veya engellenmesinin, kasten gerçekleştirdiği zaman, kendi iç hukuku kapsamında cezaî suç olarak tanımlanması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir.*

Taraflardan biri, 1. paragrafta tanımlanan fiillerin ciddi zararla sonuçlanması gerektiğini şart koşma hakkını saklı tutabilir."

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

187 **Avşar/Öngören**, Bilişim Hukuku, s. 135; **Erdoğan**, TCK'da Bilişim Suçları, s. 180; **Kurt**, Tüm Yönleriyle Bilişim Suçları, s. 160.

188 **Erdoğan**, TCK'da Bilişim Suçları, s. 180; **Karagülmez**, Bilişim Suçları, s. 236; **Kurt**, Tüm Yönleriyle Bilişim Suçları, s. 160; **Orta**, Bilişim Suçları ve Adli Bilişim, s. 117.

189 **Koca/Üzülmez**, Özel Hükümler, s. 826.

190 **Özbek/Doğan/Bacaksız/Tepe**, Özel Hükümler, s. 944.

191 **Artuk/Gökcen/Yenidünya**, Özel Hükümler, s. 882; **Gürler**, Bilişim Alanında Suçlar, s. 136; **Özbek/Doğan/Bacaksız/Tepe**, Özel Hükümler, s. 948.

başka bir yere gönderilmesi neticelerine neden olabilecek fiillerdir. Bu neticeler, çalışmamızın ikinci bölümde detaylı olarak ele alınacaktır.

Bu suçların manevi unsuru kasttır. Kastın dışında amaç veya saik gibi başka bir manevi unsur, suçun oluşumu açısından aranmamıştır[192].

TCK m. 244/3'te, TCK m. 244/1 ve 2. fıkradaki neticelerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde gerçekleştirilmesi hali, cezayı ağırlaştırıcı neden olarak öngörülmüştür.

Yukarıda da ifade edildiği üzere TCK m. 243/3, bilişim sistemine girme suçunun, neticesi sebebiyle ağırlaşmış halini teşkil etmektedir[193]. Bu anlamda failin kastının sistemdeki verilere zarar vermek yönünde olmaması gerekir. Zira bu durumda bilişim sistemine girme suçu değil, TCK m. 244'teki sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu söz konusu olacaktır[194]. Öte yandan TCK m. 43 gereğince failin bu neticeden sorumlu olması için en azından taksirle hareket etmesi gerekecektir.

Suçun yaptırımı olarak, bilişim sisteminin engellenmesi ve bozulması suçunda bir yıldan beş yıla kadar hapis cezası öngörülmüşken; verilerin yok edilmesi veya değiştirilmesi suçunda altı aydan üç yıla kadar hapis cezası öngörülmüştür. Bu suçların bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi durumunda ise ceza yarı oranında artırılmaktadır.

---

[192] **Özbek/Doğan/Bacaksız/Tepe**, Özel Hükümler, s. 961; **Soyaslan**, Özel Hükümler, s. 649.

[193] **Erdoğan**, Bilişim Sistemine Girme, s. 1402; **Soyaslan**, Özel Hükümler, s. 640.

[194] **Yenidünya**, Hukuka Aykırı Erişim Suçu, s. 1041. Yargıtay 12. CD 2016 tarihli bir kararında bir başkasının elektronik posta adresine yalnızca girilmesi burada bir değişiklik yapılmaması durumuna ilişiklin olarak fiilin bilişim sistemine girme suçunu oluşturacağına hükmetmiştir: *"Sanığın, katılan ile internette tanıştığı ve bir süre telefonda ve msn üzerinden görüntülü görüşerek arkadaşlık yürüttüğü, sanığın teklifi üzerine katılanın, kendisi, kızı ve sanık ile birlikte bir otelde yaklaşık 1 hafta süreyle tatil yaptıkları, arkadaşlıklarının bitmesi üzerine bilahare sanığın, katılanın kullandığı elektronik posta adresine rızası dışında birçok kez girdiği olayda, sanığın, bu şekildeki eyleminin TCK'nın 243/1. maddesine uyan bilişim sistemine girme suçunu oluşturduğu ve mahkemenin hükmün gerekçesinde de eylem bu şekilde kabul edildiği halde, sanık hakkında bilişim sistemine girme suçu yerine, TCK'nın 244. maddesinde düzenlenen sistemi engelleme, bozma, verileri yok etme veya değiştirme suçundan hüküm kurulmak suretiyle sanık hakkında fazla ceza tayini hatalıdır."* (*Y 12. CD, E. 2015/15933, K. 2016/277, T. 13.1.2016.* – kazanci.com, s.e.t: 19.03.2017).

2.5.1.4. Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu (TCK m. 245)

Bu suç türünün, 765 sayılı TCK'da tam olarak bir karşılığı bulunmamaktadır[195]. 765 sayılı TCK döneminde m. 525/b/2'de düzenlenen bilişim sistemi aracılığıyla haksız yarar sağlama suçunun banka ve kredi kartları aracılığıyla haksız yarar elde etmeyi kapsayıp kapsamadığı doktrinde tartışma konusu idi[196]. 2001 yılında Yargıtay Ceza Genel Kurulu (YCGK) bu hususta bir içtihadı birleştirme kararı vermiştir. 5237 sayılı TCK'da söz konusu bu karar göz önünde bulundurularak banka veya kredi kartlarının kötüye kullanılması suçu hırsızlık ve bilişim sistemi aracılığıyla haksız yarar sağlama suçundan bağımsız bir suç olarak düzenlenmiştir[197].

YCGK, *"sanığın haksız olarak ele geçirdiği bir başkasına ait kart ve şifreyi kullanarak bir bankanın iki farklı şubesindeki ATM makinesinden para çekip hukuka aykırı yarar sağlaması eylemi, TCK.nın 493/2. madde ve fıkrasındaki suçu değil aynı yasanın 525/b-3. madde ve fıkrasında düzenlenen, bilgileri otomatik işleme tabi tutmuş bir sistemi kullanarak hukuka aykırı yarar sağlamak suçunu oluşturur."* [198] ifadesiyle bu şekilde işlenen fiillerin hırsızlık suçuna vücut vermeyeceğini, bilgileri otomatik işleme tabi tutmuş bir sistemi kullanarak hukuka aykırı yarar sağlamak suçuna *(765 s. TCK m. 525/b-3)* vücut vereceğine hükmetmiştir.

TCK m. 245'te üç ayrı suç düzenlenmiştir. 1. fıkrada, gerçek bir banka veya kredi kartını kötüye kullanmak suçu; 2. fıkrada, sahte banka veya kredi kartı üretmek, satmak, devretmek, satın almak veya kabul etmek suçu; 3. fıkrada, sahte bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlamak suçu düzenlenmiştir.

Yukarıda incelenen suçlar gibi banka veya kredi kartlarının kötüye kullanılması suçu da 5237 sayılı TCK'nın topluma karşı suçlar kısmının bilişim alanında suçlar bölümünde düzenlenmiştir. Ancak düzenlendiği bölüm itibariyle bu suç tartışması konusu olmuştur. Doktrinde, bu suçun kişilere karşı suçlar kısmında malvarlığına karşı suçlar bölümünde

---

[195] **Özbek**, Banka veya Kredi Kartlarının, s. 1020.

[196] **Dülger**, Bilişim Suçları, s. 455; **Gürler**, Bilişim Alanında Suçlar, s. 160; **Özbek**, Banka veya Kredi Kartlarının, s. 1020.

[197] **Özbek/Doğan/Bacaksız/Tepe**, Özel Hükümler, s. 963.

[198] YCGK, 10.04.2001, E.2001/76-30, K.2001/757, YKD, Haziran 2001, s. 913 vd, Aktaran: **Özbek**, Banka veya Kredi Kartlarının, s. 1020.

düzenlenmesi gerektiği ifade edilmiştir[199]. Zira bu suçta aynı bölümde düzenlenen diğer suçlardan farklı olarak, karma hukuki değer bağlamında, bilişim sistemlerinin güvenilirliği korunmamaktadır[200]. Maddenin son fıkrasında düzenlenen etkin pişmanlık hükmü bakımından da suç ile korunan hukuki değerin malvarlığı olduğu ifade edilebilir[201] .

Kanaatimizce TCK m. 245'de düzenlenen banka veya kredi kartını kötüye kullanmak suçunun dar anlamda bir bilişim suçu olduğunu ve bilişim sistemlerinin güvenilirliğini koruduğunu söylemek mümkün değildir. Zira banka veya kredi kartının bir bilişim sistemi olduğunu söylemek ve bu kartların yetki dışı bilişim sistemlerinde yetki dışı kullanılmasında da kullanılan bilişim sistemlerinin güvenilirliğinin zedelendiğini söylemek mümkün değildir. Örneğin, kart hamilinden izinsiz kredi kartının alınarak yine onun izni olmadan bu kartla alışveriş yapılmasında kullanılan *"POS (Point of Sales Terminal – Satış Noktaları Terminali) cihazı"*nın güvenilirliğinin zedelendiği söylenemez. Dolayısıyla bu suçun dar anlamda bir bilişim suçu olduğu da söylenemez; çünkü, esasında bu suçun işlenmesinde duruma göre hırsızlık, dolandırıcılık, güveni kötüye kullanma ve sahtecilik suçlarının banka veya kredi kartıyla işlenmesi söz konusudur. Bu suçlardan farklı bir düzenlemenin yapılmasındaki amaç, esasında, bu suçların banka veya kredi kartları kullanılarak işlenmesi durumunda ortaya çıkabilecek tipikliğe ilişkin duraksamaları engellemektir. Ayrıca suçla korunan hukuki değer, sayılan suçlarla benzer şekilde bu suçta da malvarlığıdır[202]. Nitekim madde gerekçesinde bu durum şu şekilde ifade edilmiştir: *"Aslında hırsızlık, dolandırıcılık, güveni kötüye kullanma ve sahtecilik suçlarının ratio legis'lerinin tümünü de içeren bu fiillerin, duraksamaları ve içtihat farklılıklarını önlemek amacıyla, bağımsız suç hâline getirilmeleri uygun görülmüştür."*

TCK m. 245/1'de suç, başkasına ait bir banka veya kredi kartını bir şekilde ele geçiren kimsenin, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın

---

[199] **Dülger**, Bilişim Suçları, s. 458; **Özbek**, Banka veya Kredi Kartlarının, s. 1022.

[200] Karşı görüş için bkz. **Okuyucu Ergün**, **Güneş**; "*Banka veya Kredi Kartlarının Kötüye Kullanılması*", Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, 2013, Sayı 2 (Prof. Dr. Nur Centel'e Armağan), s. 1067. : *"Banka veya kredi kartlarının kötüye kullanılmasına ilişkin TCK m. 245 ile birden fazla hukuki varlık veya menfaat korunmaktadır. Zira söz konusu maddede öngörülen suçlar, bilişim sistemlerinin düzgün işlemesine ilişkin toplumsal menfaat, kamu güveni, kişilere ait malvarlığına ilişkin menfaat gibi çeşitli hukuki varlık veya menfaatleri ihlal etmektedir."*

[201] **Dülger**, Bilişim Suçları, s. 458; **Koca/Üzülmez**, Özel Hükümler, s. 846.

[202] **Dülger**, Bilişim Suçları, s. 458; **Karagülmez**, Bilişim Suçları, s. 289; **Kurt**, Tüm Yönleriyle Bilişim Suçları, s. 205.

kartı kullanması veya bunu üçüncü kişiye kullandırması ve bu yolla failin kendisi veya bir başkası için hukuka aykırı yarar sağlaması olarak tanımlanmıştır.

Banka ve kredi kartının tanımı 5464 sayılı Banka ve Kredi Kartları Kanunu'nda gösterilmiştir. Buna göre banka kartı *"Mevduat hesabı veya özel cari hesapların kullanımı dahil bankacılık hizmetlerinden yararlanmayı sağlayan kart"*tır. Kredi kartı ise *"Nakit kullanımı gerekmeksizin mal ve hizmet alımı veya nakit çekme olanağı sağlayan basılı kart veya fizikî varlığı bulunmayan kart numarası"*dır. Bu anlamda banka ve kredi kartı olarak kabul edilemeyecek telefon kartı, doğalgaz kartı, su kartı gibi kartların kötüye kullanılması bu suçu oluşturmayacaktır[203]. Ayrıca banka kartından farklı olarak kredi kartının *"fizikî varlığı bulunmayan kart numarası"*nı da içerdiği görülmektedir. Öyleyse kredi kartının *"aynının"* bulunmamasına rağmen kart numaralarının kötüye kullanılması durumunda da bu suç söz konusu olacaktır[204].

Suçun faili herkes olabilir[205]. Mağdur ise banka veya kredi kartı sahibi kimsedir. Doktrinde madde metninde geçen *"kart sahibi"* ifadesi eleştirilmiştir. Zira 5464 sayılı kanuna göre kartın mülkiyeti banka veya finans kuruluşuna aittir müşteriye sadece kartın kullanım hakkı verilmektedir. Dolayısıyla madde metininde geçen kart sahibinin kart hamili[206] olarak anlaşılması gerektiği ifade edilmiştir[207]. Bu anlamda kart hamilinin yanında kartın asıl sahibi olan banka veya finans kuruluşu da kendisine karşı duyulan güvenin zedelenmesi nedeniyle suçtan zarar görendir[208].

---

[203] **Özbek**, Banka veya Kredi Kartlarının, s. 1026.

[204] **Özbek/Doğan/Bacaksız/Tepe**, Özel Hükümler, s. 969. 5464 Sayılı Banka Kartları ve Kredi Kartları Kanunu m. 3/1-e: *"Kredi kartı: Nakit kullanımı gerekmeksizin mal ve hizmet alımı veya nakit çekme olanağı sağlayan basılı kartı veya fizikî varlığı bulunmayan kart numarasını ifade eder."*

[205] **Dülger**, Bilişim Suçları, s. 459; **Gürler**, Bilişim Alanında Suçlar, s. 165; **Koca/Üzülmez**, Özel Hükümler, s. 847; **Özbek**, Banka veya Kredi Kartlarının, s. 1028; **Taşkın**, Bilişim Suçları, s. 64.

[206] 5464 Sayılı Banka Kartları ve Kredi Kartları Kanunu m. 3/1-j: *"Kart hamili: Banka kartı veya kredi kartı hizmetlerinden yararlanan gerçek veya tüzel kişiyi ifade eder."*

[207] **Baş**, **Eylem**; Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu, Ankara 2015, s. 159.

[208] **Dülger**, Bilişim Suçları, s. 463; **Koca/Üzülmez**, Özel Hükümler, s. 848; **Taşkın**, Bilişim Suçları, s. 64. Ayrıca kart hamilinin yanında bankanın da suçun mağduru olduğuna ilişkin görüş için bkz. **Gürler**, Bilişim Alanında Suçlar, s. 166; **Özbek**, Banka veya Kredi Kartlarının, s. 1029.

Madde metninde kartın kendisine verilmesi gereken kişi ifadesinin kullanım amacı ise kartı henüz kendisine ulaşmamış müstakbel hamili de gerçekleştirilecek kötüye kullanımlar bakımından korumaya almaktır[209].

Madde metninde *"başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse"* ifadesi kullanılmıştır. Dolayısıyla failin banka veya kredi kartını nasıl ele geçirdiği önemli değildir[210]. Kart çalınarak, bulunarak hatta kart hamilinin rızasıyla failin eline geçmiş olabilir[211]. Yine kart henüz kullanıcısına ulaşmadan fail tarafından ele geçirilmiş de olabilir[212].

Kanun, suçun oluşumu için banka veya kredi kartını ele geçirmeyi yeterli görmemiş ayrıca kartın fail tarafından kendisi veya bir başkası lehine kullanılmasını da aramıştır[213]. İşte bu noktada kart hamilinin rızası bulunmamalıdır. Yani kart faile rıza ile verilmiş olsa da eğer kartın rıza dışında kullanımı söz konusu ise bu suç oluşacaktır[214]. Rızanın olmaması açıkça kanun hükmünde zikredilmiştir. Dolayısıyla rıza, bu suçta bir hukuka uygunluk nedeni değil, maddi unsurdur[215]. Kanunda, ele geçirme ve kullanma bakımından bir sınır getirilmediğinden söz konusu suç, serbest hareketli bir suçtur[216]. Ayrıca bu suç, failin veya bir başkasının yarar elde etmesi arandığından, neticeli suçlardandır[217].

Suçun manevi unsuru kasttır, taksirli hali kanunda düzenlenmemiştir.

Suçun yaptırımı olarak kanunda, üç yıldan altı yıla kadar hapis ve beş bin güne kadar adlî para cezası öngörülmüştür.

İkinci fıkrada, başkalarına ait bir banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üretmek, satmak, devretmek, satın almak veya kabul etmek ayrı bir suç olarak

---

209 **Koca/Üzülmez**, Özel Hükümler, s. 848; **Özbek**, Banka veya Kredi Kartlarının, s. 1030.

210 **Baş**, Banka veya Kredi Kartlarının, s. 142; **Dülger**, Bilişim Suçları, s. 470; **Gürler**, Bilişim Alanında Suçlar, s. 167; **Koca/Üzülmez**, Özel Hükümler, s. 851; **Özbek**, Banka veya Kredi Kartlarının, s. 1030; **Taşkın**, Bilişim Suçları, s. 68.

211 **Artuk/Gökcen/Yenidünya**, Özel Hükümler, s. 898.

212 **Özbek**, Banka veya Kredi Kartlarının, s. 1031.

213 **Koca/Üzülmez**, Özel Hükümler, s. 851.

214 **Artuk/Gökcen/Yenidünya**, Özel Hükümler, s. 898.

215 **Koca/Üzülmez**, Özel Hükümler, s. 855.

216 **Dülger**, Bilişim Suçları, s. 470; **Koca/Üzülmez**, Özel Hükümler, s. 849.

217 **Özbek**, Banka veya Kredi Kartlarının, s. 1030.

tanımlanmış ve yaptırım olarak, üç yıldan yedi yıla kadar hapis ve on bin güne kadar adlî para cezası öngörülmüştür.

Üçüncü fıkradaki suçta ise sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle yarar sağlamak cezai yaptırım altına alınmış ve yaptırım olarak, fiilin daha ağır bir cezayı gerektirmemesi şartıyla, dört yıldan sekiz yıla kadar hapis ve beş bine güne kadar adli para cezası öngörülmüştür. Bu suçta, ikinci fıkradan farklı olarak, bir banka hesabıyla ilişkilendirilmemiş bir kart üzerinde yapılan sahtecilik de cezai sorumluluğa neden olacaktır[218].

2.5.1.5. Yasak Cihaz veya Programların Üretilmesi ve Ticareti Suçu (TCK m. 245/A)

Yasak cihaz veya programların üretilmesi ve ticareti suçu TCK'da bilişim alanında suçlar bölümünde, banka veya kredi kartlarının kötüye kullanılması suçundan sonra gelmek üzere m. 245/A'da[219] düzenlenmiştir. Bu suç TCK'ya 24.03.2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 30. maddesinin 5. fıkrasıyla eklenmiştir.

Türkiye bu düzenleme ile, AKSSS'ye taraf olmanın gerektirdiği yükümlülüğünü yerine getirmiş bulunmaktadır. Zira AKSSS m. 6'da[220] *"cihazların kötüye kullanımı"*nın taraf devletlerce, kendi ülkelerinde cezai yaptırım altına alınacağı taahhüt edilmiştir.

Bu suç ile korunan hukuki değer toplumun bilişim sistemlerine olan güvenidir[221]. Günümüz toplumunda birçok işin bilişim sistemleri ile yürütüldüğü göz önüne alındığında işlenecek bilişim suçlarında hazırlık mahiyetinde olan fiillerin toplumun bu sistemlere duyduğu güveni korumak amacıyla cezai yaptırım altına alındığını ifade edebiliriz[222].

Suçun kanuni tanımında faile ilişkin özel bir şart getirilmediğini görmekteyiz. Dolayısıyla bu suçun faili herkes olabilir[223]. Mağdur ise, bu suçun işlenmesi ile henüz bir kimsenin

---

[218] **Erdoğan**, TCK'da Bilişim Suçları, s. 347.

[219] **TCK m. 245/A:** *"(1) Bir cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun; münhasıran bu Bölümde yer alan suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesi için 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, bir yıldan üç yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır."*

[220] https://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss380.pdf, s.e.t: 11.05.2017.

[221] **Koca/Üzülmez**, Özel Hükümler, s. 871.

[222] **Özbek/Doğan/Bacaksız/Tepe**, Özel Hükümler, s. 997.

[223] **Özbek/Doğan/Bacaksız/Tepe**, Özel Hükümler, s. 1001.

bilişim sistemine ya da diğer bir hakkına yönelik somut bir saldırı gerçekleşmediğinden, toplumu oluşturan herkestir[224].

Suçun konusu her türlü cihaz ve program değil; TCK'nın bilişim alanında yer alan suçlar ve bilişim sisteminin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesi amacıyla yapılmış bulunan cihazlar, bilgisayar programları, şifre veya sair güvenlik kodlarıdır[225].

Suçun fiil unsuru, kanunda seçimlik[226] olarak düzenlenmiştir. Bu seçimlik hareketler suçun konusunu oluşturan cihaz, program ve şifreyi; *imal etme, ithal etme, sevk etme, nakletme, depolama, kabul etme, satma, satışa arz etme, satın alma, başkalarına verme veya bulundurma*dır.

Manevi unsur açısından, bu suç ancak kasten işlenebilir; suçun taksirli hali kanunda düzenlenmemiştir. Ancak belirtmek gerekir ki AKSSS m.6 ile uyumlu biçimde suçun oluşumu bakımından TCK m. 245/A'da kastın varlığı yeterli görülmemiştir. Kanun, cihazın bilgisayar programının, şifrenin *"münhasıran bu bölümde yer alan suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesi için yapılması veya oluşturulması"* durumunda işlenen fiillerin suç oluşturacağını hükme bağlamıştır. Dolayısıyla üretme, ithal etme, satma, satın alma, depo etme, bulundurma fiilleri kanunda sayılan suçları işlemek maksadıyla yapılmalıdır[227]. Böyle bir düzenlemenin yapılması bu suç açısından elzemdir. Zira esasen bu suçta, işlenmesi amaçlanan suçların hazırlık hareketleri cezalandırılmaktadır[228].

Söz konusu suç, sırf hareket suçlarındandır. Dolayısıyla bu suça teşebbüs teorik açıdan ancak hareket parçalara bölünebiliyorsa mümkün olacaktır.

İştirak açısından bu suç bir özellik arz etmez[229]. Dikkat edilmesi gereken nokta, seçimlik hareketlerden bazılarının ancak çok failli şekilde işlenebilmesidir. Satın alma ve satışa arz

[224] **Koca/Üzülmez**, Özel Hükümler, s. 872.
[225] **Koca/Üzülmez**, Özel Hükümler, s. 872.
[226] **Koca/Üzülmez**, Özel Hükümler, s. 873; **Özbek/Doğan/Bacaksız/Tepe**, Özel Hükümler, s. 1001.
[227] **Koca/Üzülmez**, Özel Hükümler, s. 873.
[228] **Koca/Üzülmez**, Özel Hükümler, s. 872.
[229] **Özbek/Doğan/Bacaksız/Tepe**, Özel Hükümler, s. 1004.

etme seçimlik hareketleri ancak bu ilişkinin karşı tarafında birinin olması halinde mümkündür. Dolayısıyla satın alan da satan da bu suçun faili konumundadırlar.

Bu suçtaki seçimlik hareketler, kanunda sayılan suçların işlenmesi amacıyla yapılması gerektiğinden daha önce de ifade ettiğimiz gibi esasen kanunda sayılan suçların hazırlık hareketlerini teşkil etmektedir. Dolayısıyla fail bu hazırlık hareketleri ile birlikte kanunda sayılan suçları da işlediğinde hem bu suçtan hem de TCK m. 245/A'dan sorumlu olacaktır[230].

5846 sayılı FSEK m. 72'de[231] düzenlenen koruyucu programları etkisiz kılmaya yönelik hazırlık hareketleri suçu, TCK m. 245/A'ya göre özel norm[232] olduğundan bu iki suç arasında görünüşte içtima[233] söz konusudur. Bu husus, çalışmamızın ikinci bölümünün içtima bahsinde ayrıca ele alınacaktır.

Bu suç açısından yaptırım olarak bir yıldan beş yıla kadar hapis ve beşbin güne kadar adli para cezası öngörülmüştür.

2.5.2. Diğer Bilişim Suçları

Türk Ceza Kanunu'nda *"bilişim alanında suçlar bölümü"* dışında da bilişim suçları vardır. Ancak bu suçlar, bu bölümde düzenlenen suçlardan farklı olarak geniş anlamda bilişim suçuna dahildir[234].

TCK'nın *"özel hayata ve hayatın gizli alanına karşı suçlar"* bölümündeki haberleşmenin gizliliğini ihlal, özel hayatın gizliliğini ihlal, kişisel verilerin kaydedilmesi, kişisel verileri

---

230 **Özbek/Doğan/Bacaksız/Tepe**, Özel Hükümler, s. 1004.

231 ***Madde 72 – (Koruyucu programları etkisiz kılmaya yönelik hazırlık hareketleri)***
"Bir bilgisayar programının hukuka aykırı olarak çoğaltılmasının önüne geçmek amacıyla oluşturulmuş ilave programları etkisiz kılmaya yönelik program veya teknik donanımları üreten, satışa arz eden, satan veya kişisel kullanım amacı dışında elinde bulunduran kişi altı aydan iki yıla kadar hapis cezasıyla cezalandırılır."

232 **Koca/Üzülmez**, Özel Hükümler, s. 875.

233 **Koca/Üzülmez**, Genel Hükümler, s. 531.

234 TCK'da bilişim sistemi unsurlarının araç olarak kullanılabileceği geniş anlamda bilişim suçları arasından şu suçları sayabiliriz: Kamu Kurumu veya Kamu Kurumu Niteliğindeki Meslek Kuruluşlarının Faaliyetinin Engellenmesi (m.113), Hakaret (m.125), Haberleşmenin Gizliliğinin İhlali (m.132), Kişiler Arasındaki Konuşmaların Dinlenmesi ve Kayda Alınması (m.133), Özel Hayatın Gizliliğini İhlal (m.134), Kişisel Verilerin Kaydedilmesi (m.135), Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme (m.136), Verileri Yok Etmeme (m.138), Halk Arasında Korku ve Panik Yaratmak Amacıyla Tehdit (m.213), Suç İşlemeye Tahrik (m.214), Suçu ve Suçluyu Övme (m.215), Halkı Kin ve Düşmanlığa Tahrik veya Aşağılama (m.216), Kanunlara Uymamaya Tahrik (m.217), Müstehcenlik (m.226) ve Kumar Oynanması İçin Yer ve İmkan Sağlama (m.228) (**Ergün**, Siber Suçların, s. 84–85.)

hukuka aykırı olarak verme veya ele geçirme, kişisel verilerin yok edilmemesi suçları geniş anlamda bilişim suçlarındandır.

Diğer yandan tehdit, hakaret, müstehcenlik suçlarının da bilişim sistemleri ile işlenmesi mümkündür. Özellikle müstehcenlik suçu, çocuk pornografisi içeriklerinin engellenmesi bağlamında, uluslararası alanda, üzerinde en çok çalışma yapılan ve en etkili suçla mücadelenin yürütüldüğü bilişim suçudur.

Yukarıda sayılan suçlar bilişim sistemleri vasıta kılınarak işlenebilmektedir. Ancak kanun koyucu, bu suçlarda, bilişim sistemlerinin suçun işlenmesinde vasıta kılınmasını cezayı ağırlaştırıcı bir neden olarak görmemiştir. Bilişim sistemlerinin suçta araç olarak kullanılmasının nitelikli hal olarak kabul edildiği suçlar, TCK'da bilişim sistemi aracılığıyla işlenen hırsızlık suçu (m. 142/2-e) ve bilişim sistemi aracılığıyla işlenen dolandırıcılık suçu (m. 158/1-f) olmuştur.

İnceleme konumuz olan bilişim sistemleri aracılığıyla haksız yarar sağlama suçu (TCK m. 244/4) TCK'da tali norm olarak düzenlenmiştir[235]. Buna göre TCK m. 244/4'ün uygulama alanı bulabilmesi için işlenen fiil ile haksız bir yarar elde edilmesinin başka bir suça vücut vermemesi gerekmektedir. İşte bu anlamda bilişim sistemi aracılığıyla işlenen hırsızlık ve dolandırıcılık suçları inceleme konumuz olan suçun (TCK m. 244/4) asli normu olabilecek nitelikte suçlardır. Söz konusu suçlar çalışmamızın ikinci bölümünde içtima bahsinde bilişim sistemi aracılığıyla haksız yarar sağlama suçuyla karşılaştırmalı olarak ele alınacaktır.

[235] **Artuk/Gökcen/Yenidünya**, Özel Hükümler, s. 892; **Erdoğan**, TCK'da Bilişim Suçları, s. 264; **Ketizmen**, Bilişim Suçları, s. 182; **Koca**; Hukukumuzda TCK'nın 244'ncü maddesi, s. 97; **Özbek/Doğan/Bacaksız/Tepe**, Özel Hükümler, s. 955.

2.6. Özel Kanunlarda Düzenlenen Bilişim Suçları

Bilişim suçlarını içeren özel kanunları şu şekilde sıralayabiliriz: 5846 Sayılı Fikir ve Sanat Eserleri Kanunu[236], 5070 sayılı Elektronik İmza Kanunu[237], 6698 Sayılı Kişisel Verilerin Korunması Kanunu[238].

5846 Sayılı Fikir ve Sanat Eserleri Kanunu'nda yer alan bilişim suçları, büyük çoğunlukla haksız ekonomik çıkar elde etmek amacıyla işlendiğinden inceleme konumuz olan bilişim sistemi aracılığıyla haksız yarar elde etme suçu (TCK m. 244/4) ile bu suç arasındaki ilişki çalışmamızın ikinci bölümünün içtima bahsinde ayrıca ele alınacaktır.

[236] Mali, manevi ve bağlantılı haklara tecavüz suçları m. 71.
Koruyucu programları etkisiz kılmaya yönelik hazırlık hareketleri suçu m. 72

[237] Elektronik imza oluşturma verilerinin izinsiz kullanımı suçu, m. 16.
Elektronik sertifikalarda sahtekarlık suçu, m. 17.

[238] Kişisel veriyi silmeme veya anonim hâle getirmemem suçu, m. 17/2.

İKİNCİ BÖLÜM

BİLİŞİM SİSTEMİ ARACILIĞIYLA HAKSIZ YARAR SAĞLAMA SUÇU

1. SUÇ TİPİNE İLİŞKİN GENEL BİLGİLER

Çalışmamızın esasını teşkil eden *"bilişim sistemi aracılığıyla haksız yarar sağlama suçu",* 5237 sayılı Türk Ceza Kanunu'nda topluma karşı suçlar kısmında, onuncu bölüm olarak *"bilişim alanında suçlar"*da düzenlenmiştir. TCK m. 244/4'te düzenlenen bu suçun kanuni ifadesi şu şekildedir: *"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."*

Kanuni ifade incelendiğinde bu suç ile ilgili olarak öncelikle çözüme kavuşturulması gereken husus, söz konusu düzenlemenin bağımsız bir suç mu olduğu yoksa, bir ağırlaştırıcı sebep mi olduğudur. Kanunda *"yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle"* ifadesi kullanılmıştır. Söz konusu *"yukarıdaki fıkralar"* şu şekildedir: *"(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."*

Çalışmamız kapsamında bağımsız bir suç türü olarak ele alınan TCK m. 244'ün 4. fıkrası doktrinde kimi yazarlarca bağımsız bir suç olarak değil *"sistemi engelleme bozma* (244/1) ve *verileri yok etme veya değiştirme* (244/2)*"* suçlarının nitelikli hali olarak kabul edilmektedir[239]. Bu görüş sahiplerinden *Özbek/Doğan/Bacaksız/Tepe'nin* temel hareket

[239] **Avşar/Öngören**, Bilişim Hukuku, s. 139; **Ketizmen**, Bilişim Suçları, s. 156; **Kurt**, Tüm Yönleriyle Bilişim Suçları, s. 161; **Orta**, Bilişim Suçları ve Adli Bilişim, s. 118; **Özbek/Doğan/Bacaksız/Tepe**, Özel Hükümler, s. 921; **Taşdemir**, Bilişim, Banka veya Kredi Kartlarının Kötüye Kullanılması ve Dolandırıcılık Suçları, s. 276; **Pallı**, Bilişim Suçları, s. 167 *"Bu artırım sebebi, 765 sayılı yasanın 525/b-2 maddesine*

noktası yasa yapma tekniğidir. Buna göre öncelikle suçun temel şekli (suçun basit hali) oluşturulur, ardından bu temel şekli üzerinden suçun türemiş şekilleri (suçun nitelikli hali) meydana getirilir. Nitelikli hal, basit halin türemiş şekli olduğundan temel suç tipine bağlılık devam eder. TCK m. 244/4 bakımından da *"yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle"* ifadesi 1. ve 2. fıkralardaki suçlarla bağlantı noktası oluşturur[240].

Bizim de katıldığımız doktrindeki hâkim görüşe göre ise söz konusu fıkra, müstakil bir suç teşkil etmektedir[241]. Öncelikle belirtmek gerekir ki m. 244/4 bakımından maddi ve manevi unsur ile suçun konusu ilk iki fıkrada düzenlenen suçlardan farklıdır[242]. Zira bu suçta failin, ilk iki fıkradaki suçların fiil unsurundan farklı olarak, haksız bir çıkar elde etmesi de gerekmektedir[243]. Ayrıca manevi unsur bakımından failin kastı, haksız bir çıkar elde etmeye yönelmiş olmalıdır[244]. Suçun konusu ise 1. ve 2. fıkrada bilişim sistemi ve veri iken 4. fıkrada haksız yarardır. Bunlara ek olarak *"Erdoğan"*ın da belirttiği üzere kanun metnindeki *"başka bir suç oluşturmaması halinde"* ifadesi kanun koyucunun bu fıkrayı ayrı bir suç olarak düzenlediğini göstermektedir. Zira kıyaslamanın ancak eşitler arasında olabileceğini, bir nitelikli halin bir suç ile karşılaştırılamayacağını söyleyebiliriz[245]. Tek başına bir kıstas olarak kabul edilemese de kanun koyucunun yaptırım olarak oransal bir belirleme yapmayıp hapis cezasının aşağı ve yukarı sınırlarını belirtmesi de fıkranın bağımsız bir suç olduğuna delalet etmektedir. Son olarak ifade etmek gerekir ki Yargıtay tarafından da inceleme konumuz olan fıkra müstakil bir suç olarak kabul edilmektedir[246].

---

karşılık olarak düzenlenmiş olmakla birlikte cezada adalet sağlamak amacıyla bağımsız bir suç olarak düzenlenmemiştir. Suçu oluşturan eylemler, önceki iki suçun eylemlerinden ibaret olup haksız yarar sağlanması diğer suçların ağırlatıcı sebebidir."

[240] Detaylı bilgi için bkz. **Özbek/Doğan/Bacaksız/Tepe**, Özel Hükümler, s. 954. Ancak bu yazarların ilgili eserlerinin başka bir bölümünde TCK m. 244/4'ün bileşik suç olduğu ifadesi bulunmaktadır. Bkz. **Özbek/Doğan/Bacaksız/Tepe**, Özel Hükümler, s. 962.

[241] **Artuk/Gökcen/Yenidünya**, Özel Hükümler, s. 891; **Dülger**, Bilişim Suçları, s. 439; **Erdoğan**, TCK'da Bilişim Suçları, s. 247; **Gürler**, Bilişim Alanında Suçlar, s. 153; **Hafızoğulları/Özen,** Topluma Karşı Suçlar, s. 457; **Ketizmen**, Bilişim Suçları, s. 148; **Koca/Üzülmez**, Özel Hükümler, s. 834; **Soyaslan**, Özel Hükümler, s. 651; **Taşkın**, Bilişim Suçları, s. 56; **Tezcan/Erdem, /Önok,** Ceza Özel, s. 775; **Yılmaz**, TCK'nın 244. Maddesinde Düzenlenen Bilişim Alanındaki Suçlar, s. 86.

[242] **Koca/Üzülmez**, Özel Hükümler, s. 834.

[243] **Artuk/Gökcen/Yenidünya**, Özel Hükümler, s. 892; **Koca/Üzülmez**, Özel Hükümler, s. 834; **Soyaslan**, Özel Hükümler, s. 652.

[244] **Koca/Üzülmez**, Özel Hükümler, s. 834.

[245] **Erdoğan**, TCK'da Bilişim Suçları, s. 223.

[246] Bu hususa ilişkin örnek karar: *"... bilişim sistemine hukuka aykırı müdahale suretiyle haksız çıkar sağlama suçundan hüküm kurulması hukuka aykırıdır." (Y 8. CD E. 2013/15238, K. 2014/9843, T. 16.4.2014*. – kazanci.com, s.e.t 14.05.2017*)*

Müstakil bir suç olarak değerlendirdiğimiz bilişim sistemleri ile haksız yarar sağlama suçunun 765 sayılı TCK'daki karşılığı, m. 525b'nin ikinci fıkrasıdır[247]. Eski Kanun döneminde söz konusu suçun uygulama alanının oldukça geniş olduğunu ifade etmek gerekir. 5237 sayılı TCK'da düzenlenen bilişim sistemi aracılığıyla hırsızlık (142/2-e) ve dolandırıcılık (158/1-f), banka veya kredi kartlarının kötüye kullanılması[248] (245) suçları bağlamındaki fiiller de 765 sayılı TCK m. 525b/2'nin[249] uygulama alanına dahil idi[250]. Esasen bu suç, 765 sayılı TCK'da, bilişim sistemlerinin soyut unsurunun yani verinin *"mal"* olarak kabul edilememesinden dolayı düzenleme alanı bulmuştur[251]. Zira örneğin, bir bilişim sistemindeki verinin ele geçirilerek hukuka aykırı yarar elde edilmesi durumunda suçun konusu olarak *"taşınır bir mal"* bulunmadığından hırsızlık suçu bakımından tipiklik oluşmayacaktır. 765 sayılı TCK'da bilişim sistemlerinin kullanılması suretiyle elde edilen hukuka aykırı her yarar, m 525b/2 kapsamında cezai yaptırıma tabi olmaktaydı. 5237 sayılı TCK'da ise suçun işlenebilmesi için ya sistemin işleyişinin engellenmesi veya bozulması (244/1) ya da bilişim sistemi içerisindeki verilerin bozulması, yok edilmesi, değiştirilmesi, sisteme veri yerleştirilmesi, var olan verilerin başka bir yere gönderilmesi (244/2) gerekmektedir. Dolayısıyla doktrinde ifade edildiği üzere bu düzenleme sonucunda suçun fiil unsuru sınırlandırılmış ve böylece belirlilik ilkesine uygun bir düzenleme yapılmıştır[252].

Birinci bölümde ifade ettiğimiz üzere AKSSS, taraf devletler bakımından sözleşmede düzenlenen suçları, iç hukuklarına dahil etme yükümlülüğü getirmektedir. AKSSS'ye taraf olan Türkiye bakımından da aynı yükümlülük söz konusudur. Bu yükümlülüğün bir sonucu olarak kanun koyucu, AKSSS m.8'de[253] düzenlenen *"bilgisayarla bağlantılı dolandırıcılık"*

---

[247] **Yılmaz**, TCK'nın 244. Maddesinde Düzenlenen Bilişim Alanındaki Suçlar, s. 86.

"… sanığın fiilinin kül halinde suç tarihinde yürürlükte bulunan 765 sayılı TCK.nun 525/b-2 (5237 sayılı TCK.nun 244/4 maddesine uygun "bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme suretiyle haksız çıkar sağlama") madde ve fıkrası kapsamında bilişim suçunu oluşturduğu…" (*Y 11. CD E. 2006/2734, K. 2008/7125, T. 1.7.2008*. – kazanci.com, s.e.t 14.05.2017).

[248] **Özbek**, Banka veya Kredi Kartlarının, s. 1020.

[249] 765 sayılı TCK m. 525b/2: *"Bilgileri otomatik işleme tabi tutmuş bir sistemi kullanarak kendisi veya başkası lehine hukuka aykırı yarar sağlayan kimseye bir yıldan beş yıla kadar hapis ve ikimilyon liradan yirmimilyon liraya kadar ağır para cezası verilir."*

[250] **Dülger**, Bilişim Suçları, s. 285.

[251] **Dülger**, Bilişim Suçları, s. 284; **Yazıcıoğlu**, Bilgisayar Suçları, s. 267.

[252] **Ketizmen**, Bilişim Suçları, s. 176, 177.

[253] AKSSS m. 8 Bilgisayarla Bağlantılı Dolandırıcılık

"Taraflardan her biri, aşağıda belirtilenler, kasten ve haksız yere gerçekleştirildiği zaman, bir başka şahsın mal kaybına sebebiyet verdiğinde, bunların kendi iç hukukunda cezaî suç olarak tanımlanması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir. Şahısların kendilerine veya bir başkasına haksız yere maddi menfaat sağlamak için hile veya sahtekârlık niyetiyle;

başlıklı hükmü inceleme konumuz olan *"bilişim sistemi aracılığıyla haksız yarar sağlama suçu"* (244/4) ile iç hukuka dahil etmiş bulunmaktadır[254].

AKSSS'de dikkat çeken husus madde başlığında *"bilgisayarla bağlantılı dolandırıcılık"* ifadesinin kullanmış olmasıdır. Türk doktrininde *"Yazıcıoğlu"* 765 sayılı TCK döneminde m. 525b/2'deki suçu *"bilgisayar marifetiyle dolandırıcılık"* olarak ifade etmiştir[255]. Yine aynı şekilde söz konusu suçun 765 sayılı TCK'da karşılığı olan m. 525b/2'nin gerekçesinde *"sistem marifetiyle dolandırıcılık eylemi"* ifadesi kullanılmıştır. Bu duruma esas olarak AKSSS'de suçun ifade ediliş tarzının yol açtığını düşünmekteyiz. Zira Türk Hukuku bakımından dolandırıcılık suçunun oluşabilmesi için bir kimseye yöneltilmiş hileli hareketler bulunmalıdır. 765 sayılı TCK döneminde 525b/2'deki suçun oldukça geniş ifade edilmiş olması nedeniyle dolandırıcılık suçu da bu kapsamda idi. Oysa 5237 sayılı TCK bakımından bilişim sistemleri aracılığıyla dolandırıcılık, ayrı bir suç olarak düzenlenmiş ve TCK m. 244/4'te ise sisteme veya verilere yönelik müdahale ile haksız yarar elde etme düzenlenmiştir. Dolayısıyla 5237 sayılı TCK'da suçun tanımında bilgisayar marifetiyle dolandırıcılık ifadesinin kullanılmaması yerinde olmuştur. Ancak ifade etmek gerekir ki karşılaştırmalı hukukta söz konusu suç, AKSSS ile uyumlu bir şekilde dolandırıcılık suçu kapsamında düzenleme alanı bulmuştur[256].

Kanuni düzenlemede dikkat çeken bir diğer husus ise *"başka bir suç oluşturmaması halinde"* ifadesidir. Bu ifade, içtima bahsinde detaylıca ele alınacak olmakla birlikte, kısaca kanun koyucunun bu hükümle inceleme konumuz olan suça tali norm niteliği kazandırdığını ifade edebiliriz[257]. Dolayısıyla TCK m. 244/4, bilişim sistemine müdahale ile haksız yarar sağlama fiillerine uygulanacak asıl hüküm değildir ve bu fiillere uygulanabilecek başka bir hüküm varsa öncelikle o hüküm uygulanacaktır[258].

---

a) bilgisayar sistemlerine veri girişi yapma, verileri değiştirme, silme veya engelleme;

b) bir bilgisayar sisteminin işleyişini herhangi bir müdahalede bulunma."

254 **Artuk/Gökcen/Yenidünya**, Özel Hükümler, s. 891.

255 **Yazıcıoğlu**, Bilgisayar Suçları, s. 267.

256 **Dülger**, Bilişim Suçları, s. 285. *"Bilişim sistemi aracılığıyla hukuka aykırı yarar elde etme suçuna karşılaştırmalı hukukta genellikle dolandırıcılık suçu kapsamında yer verilmektedir. Buna örnek olarak; Fransa CK. m. 323-3258, Alman CK. m. 263a, Danimarka CK. m. 284, Japon CK. m. 246-2, Finlandiya CK. 36. kısım m. 1, 2 ve 3, İsveç CK. 10. kısım m. 5, İtalyan CK. m. 604ter, Kanada CK. m. 301.2(1), Avustralya CK. m. 76 B (2) a-b, Hollanda CK. m. 326, Yunanistan CK. m. 386 a, Avusturya CK. m. 148b, Lüksemburg CK. m. 509.3, Norveç CK m. 270 verilebilir."*

257 **Ketizmen**, Bilişim Suçları, s. 178; **Koca**, Hukukumuzda TCK'nın 244'ncü maddesi, s. 97.

258 **Koca**, Hukukumuzda TCK'nın 244'ncü maddesi, s. 97.

Son olarak, *"Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı"* m. 19'da *"bilişim ortamında yarar sağlamak"* adıyla inceleme konumuz olan suça benzer bir suç düzenlenmiş ancak bu tasarı kanunlaşmamıştır[259].

2. KORUNAN HUKUKİ DEĞER

Suçla korunan hukuki değer, fiilin doğrudan doğruya ihlal ettiği hukuki varlık yahut değeri ifade eder[260]. Dolayısıyla kanunda suç olarak düzenlenen bir fiilin işlenmesi, aynı zamanda bir hukuki değeri ihlal etmektedir[261]. Bu nedenle herhangi bir hukuki değerle ilişkilendirilmeyen suçtan söz edilemez[262]. Suç teşkil eden fiillerin karşılığı olan her ceza hükmü bir ya da birden fazla hukuki değeri korur[263]. Hukuki değerler ise *"hukuk toplumundaki sosyal düzenin devamı için geçerliliği zorunlu olan ideal, manevi değerlerdir."*[264]

5237 sayılı TCK, suçların sınıflandırılmasında korunan hukuki değeri esas almıştır[265]. Örneğin *"kişilere karşı suçlar"* kısmında; kişilerin hayatı, vücut bütünlüğü, onuru koruma altına alınmıştır. Bu kısımda yer alan bölümler açısından da örneğin, hayata karşı suçlarda kişilerin hayat hakkı korunan hukuki değeri oluştururken; şerefe karşı suçlar bölümünde ise kişilerin onur, şeref, haysiyetleri koruma altına alınmıştır.

İnceleme konumuz olan suç, TCK'nın topluma karşı suçlar kısmının bilişim alanında suçlar bölümünde düzenlenmiştir. Bu bölümde bilişim sistemine girme, sisteme ve sistemdeki verilere zarar verme fiillerinin yanı sıra bilişim sistemleri aracılığıyla haksız yarar sağlama, banka veya kredi kartlarını kötüye kullanma ile bilişim sistemlerine hukuka aykırı müdahaleye izin veren yasak cihaz veya programları bulundurma, üretme, satma fiilleri de

---

[259] Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı m. 19: "*Bilişim sistemiyle kendisi veya başkası lehine haksız yarar sağlayan kişi, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, iki yıldan beş yıla kadar hapis ve bin günden beşbin güne kadar adlî para cezası ile cezalandırılır."*

[260] **Artuk, Mehmet Emin/Gökcen, Ahmet/Yenidünya, A. Caner**; Ceza Hukuku Genel Hükümler, Ankara 2016, s. 285; **Zafer, Hamide**; Ceza Hukuku Genel Hükümler TCK m. 1-75, İstanbul 2015, s. 148.

[261] **Erem, Faruk**; Türk Ceza Hukuku Genel Hükümler, Cilt 1, Ankara 1971, s. 253; **Özgenç, İzzet**; Türk Ceza Hukuku Genel Hükümler, Ankara 2016, s. 159.

[262] **Ünver**, **Yener**; Ceza Hukukuyla Korunması Amaçlanan Hukuksal Değer, Ankara 2003, s. 614.

[263] **Koca, Mahmut/Üzülmez, İlhan**; Türk Ceza Hukuku Genel Hükümler, Ankara 2016, s. 41; **Soyaslan, Doğan**; Ceza Hukuku Genel Hükümler, Ankara 2016, s. 237.

[264] **Özgenç**, Genel Hükümler, s. 159.

[265] **Artuk/Gökcen/Yenidünya**, Özel Hükümler, s. 5.

yaptırım altına alındığından bölüm başlığı, kapsayıcı olması için bilişim alanında suçlar, olarak tercih edilmiştir[266]. Birinci bölümde ifade edildiği üzere bu bölümde düzenlenen suçlarda dikkat çeken nokta, korunan hukuki değerin her suç için birden fazla olmasıdır[267]. Örneğin bilişim sistemine girme suçunda, bir yandan kişilerin özel hayatlarının gizliliği ve haberleşme özgürlükleri korunurken diğer yandan toplumda bilişim sistemlerinin doğru işleyeceğine dair güven korunmaktadır[268]. Dolayısıyla bu bölümdeki suçlarda korunan hukuki değerin karma nitelik taşıdığı ifade edilebilir. Zira bu bölümdeki suçlar için korunan özel bir hukuki değerin yanında toplumun bilişim sistemlerinin doğru işleyeceğine ilişkin güven duygusu da koruma altına alınmıştır. Esasen bu suçların topluma karşı suçlar kısmında düzenlenmesinin nedeni de budur. Ancak belirtmek gerekir ki *"bilişim alanında suçlar"* ifadesi korunan hukuki değere göre değil, suçun işleneceği alana göre bir isimlendirme olmuştur[269].

Bilişim sistemleri aracılığıyla haksız yarar sağlama suçu (244/4), düzenleniş şekli itibariyle, aynı maddenin 1. ve 2. fıkrasındaki suçların koruduğu hukuki değerleri de kapsamaktadır. Bilişim sisteminin işleyişinin engellenmesi veya bozulması ile verilerin yok edilmesi veya değiştirilmesi suçlarında (244/1, 2) bilişim sistemlerinin doğru ve sağlıklı biçimde işleyişi yani bilişim sisteminde bulunan verilerde hakkı olan kişinin dilediği zaman herhangi bir engelle karşılaşmaksızın verilerine ulaşabilmesi, bunlar üzerinde değişiklik yapabilmesi, kısaca, tasarrufta bulunabilmesi koruma altına alınmıştır[270]. Doktrinde, 1. ve 2. fıkradaki suçların, mala zarar verme suçunun özel bir türünü oluşturduğu ifade edilmiştir[271]. Kanun koyucunun, bu suçu mala zarar vermeden ayrı olarak düzenlemesinin nedeni bilişim sistemindeki verilerin *"mal"* olarak kabul edilememesidir[272]. Ancak bu fıkralarda yaptırım altına alınan fiiller bakımında suçun topluma karşı suçlar kısmında düzenlenmesi göz önüne alınarak kanun koyucunun, bu suçlara ilişkin düzenlemelerle, bilişim sistemi veya

---

[266] **Koca/Üzülmez**, Özel Hükümler, s. 801.

[267] **Dülger**, Bilişim Suçları, s. 348.

[268] **Yenidünya**, Hukuka Aykırı Erişim Suçu, s. 1024.

[269] **Koca/Üzülmez**, Özel Hükümler, s. 801, 802.

[270] **Artuk/Gökcen/Yenidünya**, Özel Hükümler, s. 879; **Dülger**, Bilişim Suçları, s. 411; **Gürler**, Bilişim Alanında Suçlar, s. 135; **Koca/Üzülmez**, Özel Hükümler, s. 825; **Soyaslan**, Özel Hükümler, s. 641.

[271] **Hafızoğulları/Özen**, Topluma Karşı Suçlar, s. 451; **Karagülmez**, Bilişim Suçları, s. 187; **Ketizmen**, Bilişim Suçları, s. 128; **Kurt**, Tüm Yönleriyle Bilişim Suçları, s. 161.

[272] **Tezcan/Erdem/Önok**, Ceza Özel, s. 773.

sistemdeki verilerin kişinin malvarlığına dahil bir değer saymaktan ziyade, bilişim sistemlerinin doğru ve güvenilir şekilde işleyişini korumak istediği anlaşılmaktadır[273].

TCK m. 244/1 ve 2 bakımından durum böyle iken bilişim sistemi aracılığıyla haksız yarar sağlama suçunda (244/4), bilişim sistemlerinin doğru ve sağlıklı işlemesine ilişkin toplumdaki güven duygusunun korunmasından ziyade kişilerin malvarlığı hukuki değeri koruma altına alınmıştır. Başka bir ifadeyle bu suçta, 1. ve 2. fıkralardaki suçların korunan hukuki değerleri mündemiç olsa da malvarlığı hukuki değeri ön plandadır[274]. Zira bu suçta haksız yarar sağlama, suçun fiil unsuruna dahil edilmiş böylece bilişim sistemlerinin malvarlığı değerine yönelik saldırılarda araç olarak kullanılmasının önüne geçilmek istenmiştir[275].

Malvarlığına karşı suçlar bölümünde düzenlenen, bilişim sistemi aracılığıyla işlenen hırsızlık ve dolandırıcılık gibi suçlar, sadece malvarlığı hukuki değerini korumaktadır. Ancak inceleme konumuz suçun topluma karşı suçlar kısmında düzenlenmesi göz önüne alındığında, korunan hukuki değerin sadece kişisel değil aynı zamanda toplumsal olduğu ifade edilebilir. Kanaatimizce bu suçun tali norm olarak düzenlenmesi de bu durumun bir kanıtıdır. Hırsızlık ve dolandırıcılık gibi malvarlığına karşı suçlar bakımından tipik olmayan fiiller bu madde uyarınca yaptırıma tabi tutulacak ve böylece toplumun bilişim sistemlerinin doğru işleyeceğine olan güvenleri koruma altına alınmış olacaktır.

3. SUÇUN UNSURLARI

Suçun unsurları doktrinde farklı şekillerde tasnif edilmiştir[276]. Çalışmamız kapsamında ise suçun unsurları, tipikliğin maddi unsurları, tipikliğin manevi unsuru ve hukuka aykırılık unsuru olarak ele alınmıştır[277].

---

[273] **Özbek/Doğan/Bacaksız/Tepe**, Özel Hükümler, s. 925.

[274] **Koca/Üzülmez**, Özel Hükümler, s. 839.

[275] **Ketizmen**, Bilişim Suçları, s. 63; **Tezcan/Erdem/Önok**, Ceza Özel, s. 773. Kimi yazarlarca bu suçla korunan hukuki değer, kişilerin özel hayatlarının gizliliğinden, malvarlığı haklarının korunmasına kadar geniş bir çerçevede ela alınmaktadır[275]. Bkz. **Artuk/Gökcen/Yenidünya**, Özel Hükümler, s. 891; **Doğan**, Bilişim Suçları, s. 146; **Erdoğan**, TCK'da Bilişim Suçları, s. 251; **Soyaslan**, Özel Hükümler, s. 651.

[276] Bu tasniflerin karşılaştırması için bkz. **Artuk/Gökcen/Yenidünya**, Genel Hükümler, s. 200–203.

[277] Bu tasnifte, "*Koca/Üzülmez"*in suçun unsurlarını tasnifi esas alınmıştır: **Koca/Üzülmez**, Genel Hükümler, s. 93.

3.1. Tipikliğin Maddi Unsurları

Tipikliğin maddi unsurları çalışmamız kapsamında; fail, suçun konusu, mağdur, fiil ve netice olarak ele alınmıştır.

3.1.1. Fail

TCK m. 37'de, suçun kanuni tanımındaki fiili gerçekleştiren kişi, fail olarak tanımlanmıştır. Türk Hukuku bakımından ancak bir gerçek kişi suçun faili olabilir. Anayasa'nın *"suç ve cezalara ilişkin esaslar"* başlığını taşıyan 38. maddesinin 7. fıkrasında *"ceza sorumluluğu şahsidir."* denerek, gerçek kişilerin işlediği fiillerden dolayı tüzel kişilerin cezalandırılamayacağı kabul edilmiş olmaktadır[278]. Aynı husus TCK m. 20'nin gerekçesinde de ifade edilmiştir: *"Sadece gerçek kişiler suçun faili olabilir ve sadece gerçek kişiler hakkında ceza yaptırımına hükmedilebilir."*

Her suçun mutlaka bir faili vardır[279] ve kural olarak suçlar herkes tarafından işlenebilir[280]. Ancak kanun koyucu bazı suçların, özel bir yükümlülük altında bulunan ve belli faillik vasfını taşıyan kimseler tarafından, işlenebileceğini öngörmüş olabilir ki bu suçlar doktrinde özgü suç veya mahsus suç olarak ifade edilmektedir[281].

Bilişim suçlarının sınırlarının çizilmesinde fail kriterini esas alan görüşün bugün için bir geçerliliği yoktur. Böyle bir görüşe esas olarak, bilgisayarın icadıyla ortaya çıkan bilişim suçlarının, başlangıçta sadece bilgisayar ile teknik anlamda bağlantılı kişilerce işlenebilmesi yol açmıştır. Ancak günümüz dünyasında bilgisayar veya bilişim sistemleri artık günlük hayatın olağan bir aracı konumundadır. Toplumun her kesiminden herkesin erişebildiği ve herkesin kullanabildiği bilişim sistemlerinin bu anlamda herkes tarafından kötüye

---

[278] **Hafızoğulları, Zeki/Özen, Muharrem**; Türk Ceza Hukuku Genel Hükümler, Ankara 2015, s. 349; **Yerdelen**, **Erdal**; Müsadere ve Mülkiyetin Kamuya Geçirilmesi, Ankara 2010, s. 18. Tüzel kişilerin suç faili olamayacağına ilişkin detaylı bilgi için bkz. **Özgenç**, Tüzel Kişinin Sorumluluk Ehliyeti - Anayasa Mahkemesi'nin Bir Kararı Üzerine Düşünceler, s. 319 vd.

[279] **Koca/Üzülmez**, Genel Hükümler, s. 108; **Soyaslan**, Genel Hükümler, s. 231; **Toroslu/Toroslu**, Genel Kısım, s. 105; **Zafer**, Genel Hükümler, s. 151.

[280] **Özgenç**, Genel Hükümler, s. 191; **Soyaslan**, Genel Hükümler, s. 231; **Toroslu, Nevzat/Toroslu, Haluk**; Ceza Hukuku Genel Kısım, Ankara 2016, s. 105.

[281] **Demirbaş, Timur**; Ceza Hukuku Genel Hükümler, Ankara 2016, s. 481; **İçel, Kayıhan/Sokullu Akıncı, Füsun/Özgenç, İzzet/Sözüer, Adem/Mahmutoğlu, Fatih Selami/Ünver, Yener**; Suç Teorisi, İstanbul 2000, s. 90; **Toroslu/Toroslu**, Genel Kısım, s. 105.

kullanılması mümkün hale gelmiştir[282]. Dolayısıyla artık bilişim suçlarını, beyaz yaka suçu (white-collar crime) olarak tanımlamak imkansızdır[283].

Bu noktada bilişim suçları ile ilgili *"hacker"* ifadesine de değinmek gerekir. Gündelik hayatta ve bilişim dünyası jargonunda bilişim sistemleri vasıtasıyla suç işleyen kimselere genellikle *"hacker"* denilmektedir[284]. Ancak belirtmek gerekir ki bu, bilişim suçlarının yalnızca *"hacker"* sıfatlı kimselerce işlenebileceği anlamına gelmez.

Bilişim sistemleri aracılığıyla haksız bir çıkar elde edilmesi bu anlamda herkes tarafından gerçekleştirilebilecek bir fiildir. Bu durumu göz önüne alan kanun koyucu TCK m. 244/4'te bilişim sistemi ile haksız yarar sağlama suçunu günümüz şartlarına uygun şekilde herkes tarafından işlenebilecek bir suç olarak düzenlemiştir. Kanuni tanımda *"... fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlaması..."* ifadesi buna işaret etmektedir.

Tüzel kişiler suç faili olamasalar da TCK m 20/2'de, bunlar hakkında güvenlik tedbirine hükmedilebileceği düzenlenmiştir[285]. Kanun koyucu, TCK m. 246 bakımından bilişim alanında suçlar bölümünde düzenlenen suçların işlenmesi ile tüzel kişi yararına haksız menfaat sağlanması durumunda bu tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerinin

---

[282] Örneğin, 15 yaşındaki bir çocuk, NASA'nın Uluslararası Uzay İstasyonunu destekleyen bilgisayarını uzaktan erişimle 21 gün kapatabilmiştir. Yine aynı çocuk Pentagon'un silah sistemleri bilgisayarına erişerek sisteme kendini bir çalışan olarak tanıtabilmiştir. (http://abcnews.go.com/Technology/story?id=119423&page=1, s.e.t: 06.03.2017)

[283] **Erdoğan**, TCK'da Bilişim Suçları, s. 157; **Eker, Ö.Umut**; "*Türk Ceza Hukuku'nda Bilişim Suçları Eski TCK Bağlamında Hukukumuzda Yer Alan İlk Düzenlemeler ve 5237 Sayılı Yeni Türk Ceza Kanunu'nun İlgili Hükümlerinin Yorumu*", TBB Dergisi, 2006, Sayı 62, s. 105: *"Kriminolojik açıdan bilişim suçları pek çok kere "beyaz yaka suçları" (white-collar crimes) kategorisinde değerlendirilmiştir. "Beyaz yaka suçları", şiddete dayanmayan ve genellikle suçlunun, mesleği dolayısıyla sahip olduğu bazı yetkileri ve avantajları kötüye kullanmasıyla ortaya çıkan zimmete geçirme, güveni kötüye kullanma benzeri suçlar olup iş dünyasında yaygın olarak rastlanan suçlardandır. Bu bağlamda bilişim suçları, genellikle ekonomik amaçlarla, maddi çıkar sağlamak için işlenmektedir ve dolayısıyla maddi ceza hukuku açısından mala/ mülkiyete karşı suçlar kategorisinde ele alındığı görülmektedir."*

[284] **Eralp**, Bilişim Terimleri Sözlüğü, s. 69: "*Hack, işletim sistemlerinin, daha genel bir ifadeyle sistemlerin doğasındaki açık kapıların kullanılarak bu açık kapılardan sızılmasıdır. Yani normalde erişim izni olmayan sistemlere, o sitemlerin güvenlik duvarının aşılarak girilmesidir. Bu eylemleri yapan kişilere de hacker denir."*

[285] *Özbek'e* göre suç adı verilen fiilin iki yaptırımı vardır ve bunlar ceza ile güvenlik tedbiridir. Tüzel kişilere güvenlik tedbirinin uygulanmasını kabul etmek tüzel kişilerin suç işleyebileceğini kabul etmek anlamına gelir. Tüzel kişiler suç işleyemeyeceğine göre onlar hakkında güvenlik tedbirine de hükmedilmemelidir. Tüzel kişiler hakkında ceza hukukunda değil hukukun diğer alanlarında yaptırımlar öngörülmelidir. (**Özbek**, **Veli Özer**; Türk Ceza Kanununun Anlamı, Ankara 2006, Cilt 1, s. 270.)

uygulanacağını hükme bağlamıştır. Bilişim alanında suçlar bölümünde düzenlenen TCK m. 244/4 bakımından da bu hüküm uygulama alanı bulacaktır.

3.1.2. Suçun Konusu

Her suçun muhakkak bir konusu vardır[286] ve bu konu tipik hareketin üzerinde icra edildiği, kişi veya şeyin maddi yapısını teşkil eder[287]. Ancak suçun konusu, her zaman maddi bünyeye sahip varlıkları ifade etmez[288]. Bazı suçlarda; şeref[289], soybağı[290], bilişim sistemi verisi[291] gibi maddi bünyeye sahip olmayan şeylerin de suçun konusu olduğu görülmektedir.

Suçun işlenmesi, konuya ya bir zarar vereceğinden ya da zarar tehlikesine neden olacağından, suç tipinde belirtilen hareketin yönelik olduğu konunun, bu hareketten etkileniş derecesine ve şeklinde göre suçları tehlike ve zarar suçları olarak ikiye ayırmak mümkündür[292]. Bu bağlamda zarar suçlarında, suçun konusu bir zarara uğratılırken, tehlike suçlarında, hareket suçun konusu bakımından bir tehlikeye neden olmaktadır[293].

Ayrıca korunan hukuki değer ile suçun konusu farklı kavramlardır[294]. Korunan hukuki değer, işlenen fiille ihlal edilen hukuki varlık veya menfaati ifade ederken; suçun konusu, hareketin yönelik olduğu kişi veya şeyi ifade eder[295]. Dolayısıyla tipik hareketin gerçekleştirilmesi ile suçun konusunun zarara uğratılması veya konu bakımından tehlikeye neden olunması durumunda korunan hukuki değer ihlal edilmiş olacaktır[296].

---

[286] **Erem**, Genel Hükümler Cilt 1, s. 250; **Koca/Üzülmez**, Genel Hükümler, s. 111; **Özgenç**, Genel Hükümler, s. 198. Aksi görüş için bkz. **Toroslu/Toroslu**, Genel Kısım, s. 109, 110.

[287] **Akbulut, Berrin**; Ceza Hukuku Genel Hükümler, Ankara 2016, s. 338; **Artuk/Gökcen/Yenidünya**, Genel Hükümler, s. 284; **Koca/Üzülmez**, Genel Hükümler, s. 112; **Özgenç**, Genel Hükümler, s. 198.

[288] **Akbulut**, Genel Hükümler, s. 338; **Artuk/Gökcen/Yenidünya**, Genel Hükümler, s. 285. Suçun üzerinde işlendiği şeyin maddi bünyesi olmayabileceğine ilişkin görüşün açıklaması için bkz. **Erem**, Genel Hükümler Cilt 1, s. 246.

[289] Hakaret suçunda, suçun konusu, yaşayan belli bir kişinin onuru şerefi ve saygınlığıdır. (**Koca/Üzülmez**, Genel Hükümler, s. 432.)

[290] Çocuğun soybağını değiştirme suçunda (TCK m. 231), suçun konusu, soybağıdır. (**Koca/Üzülmez**, Genel Hükümler, s. 739.)

[291] TCK m. 241/2 açısından suçun konusu, bilişim sistemi verisidir. (**Koca/Üzülmez**, Genel Hükümler, s. 826.)

[292] **Akbulut**, Genel Hükümler, s. 339; **Artuk/Gökcen/Yenidünya**, Genel Hükümler, s. 285.

[293] **İçel**, Genel Hükümler, s. 276; **Koca/Üzülmez**, Genel Hükümler, s. 113.

[294] **Koca/Üzülmez**, Genel Hükümler, s. 112; **Özgenç**, Genel Hükümler, s. 199.

[295] **Artuk/Gökcen/Yenidünya**, Genel Hükümler, s. 285.

[296] **Koca/Üzülmez**, Genel Hükümler, s. 112; **Özgenç**, Genel Hükümler, s. 199.

Bilişim sistemi ile haksız yarar sağlama suçunda, suçun konusu, birinci ve ikinci fıkradan farklı olarak, haksız şekilde sağlanan *"yarar"*dır[297]. Bu suçun unsuru olan sistemi engelleme, bozma, verileri yok etme veya değiştirme suçunda ise suçun konusunu, bilişim sistemlerinin işleyişi ve sistemdeki veriler oluşturmaktadır[298].

Failin kendisi veya başkası için sağladığı haksız yararın niteliği hususunda doktrinde tartışma vardır. Bir kısım yazar, sağlanan yararın maddi olabileceği gibi manevi olabileceğini de ifade ederken[299] bir kısım yazar ise sağlanan yararın yalnızca maddi – ekonomik nitelikte[300] olabileceğini savunmaktadır.

Kanaatimizce bu suçun konusu, yalnızca maddi – ekonomik nitelikteki yararlardır. Görüşümüzün temel noktası ise 244. maddenin ilk iki fıkrasında düzenlenen suçların, 4. fıkradaki suçun unsuru olması dolayısıyla manevi yararların bu madde kapsamına dahil edilmesi durumunda ilk iki fıkrada düzenlenen suçların uygulama alanının kalmayacağı yönündedir. Zira fail, olayların çoğunda bir manevi yarar elde etmek amacıyla suç işlemektedir. Örneğin, kişinin intikam almak için hasmının bilişim sistemini erişilemez kılması durumunda bir manevi yararı vardır ve eğer manevi yararı, 4. fıkra bağlamında değerlendirecek olursak, 1. ve 2. fıkranın uygulama alanı istisnai bir hal alacaktır. Öte yandan söz konusu suçun yaptırımı olarak hapis cezasının yanı sıra adli para cezasının öngörülmesi bu suçta maddi – ekonomik yararın elde edilmesi gerektiğine delalet

---

[297] **Doğan**, Bilişim Suçları, s. 147; **Dülger**, Bilişim Suçları, s. 443; **Erdoğan**, TCK'da Bilişim Suçları, s. 255; **Gürler**, Bilişim Alanında Suçlar, s. 155; **Koca/Üzülmez**, Özel Hükümler, s. 839; **Soyaslan**, Özel Hükümler, s. 652.

[298] **Erdoğan**, TCK'da Bilişim Suçları, s. 229.

[299] **Dülger**, Bilişim Suçları, s. 441; **Kurt**, Tüm Yönleriyle Bilişim Suçları, s. 175; **Özbek/Doğan/Bacaksız/Tepe**, Özel Hükümler, s. 955; **Soyaslan**, Özel Hükümler, s. 651; **Taşkın**, Bilişim Suçları, s. 58; **Yılmaz**, TCK'nın 244. Maddesinde Düzenlenen Bilişim Alanındaki Suçlar, s. 87.

Dülger'in konuyla ilgili açıklaması şu şekildedir: *"244. maddenin ifadesinden ve gerekçesinden çıkarılan sonuç 'dolandırıcılık, hırsızlık, güveni kötüye kullanma veya zimmet suçunun' bu madde kapsamı içinde olmadığıdır; söz konusu suç tiplerinden özellikle dolandırıcılık ve hırsızlık suçlarında malvarlığı korunmaktadır. İnceleme konusu suç tipini oluşturan eylemlerin gerçekleştirilmesi nedeniyle mağdurun malvarlığında bir zararın meydana gelmesi durumunda ise genellikle ya nitelikli dolandırıcılık suçu ya da nitelikli hırsızlık suçu gerçekleşmiş olacaktır. Bu iki suçtan birinin oluşmaması halinde ise, 244/4 söz konusu olabilecektir. Dolayısıyla sağlanan haksız yararının maddi bir yarar olmaması halinde 244/4'ün devreye girmesi pekala mümkün olabilmektedir. Dolayısıyla bu suç tipinin yeni düzenlemesi karşısında suçla korunan hukuksal değerin mağdurun manevi bir hakkının olması da olası görülmektedir. Ancak ilk paragrafta da belirttiğimiz üzere, suç tipinde kuramsal olarak bu yönde bir sınırlama olmamakla birlikte uygulamada genellikle suçun konusunu da oluşturan bu değer bir malvarlığı hakkı olmaktadır."* (**Dülger**, Bilişim Suçları, s. 441.)

[300] **Hafızoğulları/Özen**, Topluma Karşı Suçlar, s. 451; **Karagülmez**, Bilişim Suçları, s. 187; **Ketizmen**, Bilişim Suçları, s. 128; **Koca/Üzülmez**, Özel Hükümler, s. 839; **Tezcan/Erdem/Önok**, Ceza Özel, s. 775; **Yazıcıoğlu**, Bilgisayar Suçları, s. 260.

etmektedir. Zira adli para cezasının, hapis cezasının yanı sıra uygulanmasının öngörüldüğü suçlarda amaç, suçla elde edilen ekonomik çıkarın tespit edilip kazanç müsaderesine ilişkin hükümlerin uygulanamaması durumunda, suçtan elde edilen gelirin kişinin yanına kâr kalmamasını sağlamaktır[301]. Dolayısıyla haksız yarar sağlama fiilinin failin elde ettiği maddi – ekonomik yararlar bağlamında değerlendirilmesi, kanun koyucunun iradesine uygun olacaktır. Nitekim Yargıtay kararlarında da bu suçun uygulama alanı olarak failin elde ettiği maddi yararlara rastlanmaktadır[302]. Ayrıca bu suçun AKSSS'deki karşılığı olan 8. maddede fiil unsuru, maddi yarar elde etmeye yönelik şekilde düzenlenmiştir.

Failin sağladığı haksız yararın muhakkak para veya değerli eşya olması gerekmez. Failin sistem veya verilere karşı müdahale fiili sonucu aktiflerindeki bir artış veya pasiflerindeki bir azalış ya da ekonomik durumunda doğrudan veya dolaylı iyileşme getiren menfaat, TCK m. 244/4 anlamında maddi – ekonomik bir yarar teşkil edecektir[303]. Örneğin, failin borçlu olduğu kişinin bilişim sistemine girerek burada borcuna ilişkin verileri yok etmesi durumunda m. 244/4 anlamında maddi bir yarar elde etme söz konusu olacaktır[304].

Haksız çıkar sağlama bir başkasının malvarlığında azalmaya veya beklenen bir yarara engel olmaya neden olacağından, bilişim sistemleri aracılığıyla haksız yarar sağlama suçu bir zarar suçudur[305]. Ancak suçun maddi unsurunda, mağdurun zarara uğraması aranmadığından, suçun oluşumu için zararın gerçekleşip gerçekleşmediği araştırılmayacaktır.

---

[301] **Yerdelen**, **Erdal**; Cezanın Belirlenmesi (Türk- Alman Uygulaması), Ankara 2013, s. 338, 339.

[302] *"Suç tarihinde sanığın internet üzerinden girdiği şifre ile müştekinin GSM numarasından başka bir GSM numarasına, oradan da yine şifre vasıtasıyla kendi numarasına müştekinin bilgisi ve rızası dışında kontör transferi yapma şeklinde gerçekleşen eyleminin sistemi engelleme, bozma, verileri yok etme veya değiştirme 5237 Sayılı TCK'nın Md. 244/4'te yer alan suçun oluştuğu gözetilmelidir." (Y 13. CD E. 2011/26435, K. 2013/1955, T. 30.1.2013, kazanci.com – s.e.t. 19.05.2017)*

[303] **Koca/Üzülmez**, Özel Hükümler, s. 840.

[304] *"Bağ-Kur Aydın İl Müdürlüğü'nde memur olarak görev yapan sanığın, kendisine ait kullanıcı kodunu kullanmak suretiyle 'Bağ-Kur Sigortalı Bilgi Sistemi'ne girerek, sistemdeki eşi Aysel'e ait sigorta kayıtlarını, eşinin biriken pirim borcundan kurutulması amacıyla sildiği, oluşa uygun olarak kabul edilen sanığın bu eyleminin 765 sayılı TCK'nın 525/b-1. maddesinde yazılı 'başkasına yarar sağlamak amacıyla bilgileri otomatik işleme tabi tutmuş bir sistemin verilerini silmek" suçunu oluşturduğu ..." (Y 11. CD, 3876/12781, T. 04.12.2008,* Aktaran: **Taşdemir**, Bilişim, Banka veya Kredi Kartlarının Kötüye Kullanılması ve Dolandırıcılık Suçları, s. 296, 297.)

[305] Aynı yönde bkz. **Koca/Üzülmez**, Özel Hükümler, s. 840: *"Failin kendisine veya başkasına çıkar sağlaması suçun oluşması için yeterli olup, mağdurun bu fiil nedeniyle zarara uğraması aranmaz. Ancak bu durum suçun zarar suçu olarak nitelendirilmesine engel değildir."* Karşı yönde bkz. **Dülger**, Bilişim Suçları, s. 448: *"İşte yasanın düzenlenişinde failin elde ettiği bu hukuka aykırı yarar sonucunda mağdurda bir zararın oluşup oluşmadığına da bakılmamaktadır. Bu nedenle suç tipi aynı eylemleri içermesine rağmen 244. maddenin 1. ve 2. fıkralarında düzenlenen bilişim sisteminin işleyişinin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi suçundan farklı olarak bir zarar suçu değil tehlike suçudur."*

3.1.3. Mağdur

Her suçun muhakkak bir faili olduğu gibi bir de mağduru vardır[306]. Ceza hukuku anlamında suçun mağduru, *"suçun konusunun ait olduğu kişiyi veya kişileri ifade eder."*[307] Suçun konusu ise suç oluşturan hareketin, üzerinde icra edildiği kişi veya şey anlamına gelmektedir[308].

Özellikle suçun konusunun bir birey olması durumunda, konu ve mağdurun kesiştiği gözükse de esasında bunlar birbirinden farklı kavramlardır[309]. Örneğin, kasten öldürme suçunda, suçun konusu öldürülen kimsenin bedeni iken, suçun mağduru öldürülen kimsedir.

Suçun konusunun belli kişi veya kişilere ait olması durumunda suçun mağduru bu kişi veya kişilerdir. Ancak eğer suçun konusunun sahibi belli kişi veya kişiler değil de toplumu oluşturan herkes ise bu durumda toplumu oluşturan herkes bu suçun mağdurudur.[310]

Suçun mağduru ancak gerçek kişiler olabilir[311]. Gerçek kişiler dışında tüzel kişiler, yahut tüzel kişiliği olmamakla birlikte hukuki topluluklar, suçun mağduru olamazlar[312]. Mağdur ancak hareketin veya suçun üzerinde icra edildiği şeyin sahibi olan kimsedir. Doktrinde, tüzel kişilerin suçun mağduru olamayacağının benimsenmesinin sonucu olarak, mağduru belli kişi veya kişiler olmayan suçlar (örneğin topluma karşı suçlar) bakımından, toplumu oluşturan bireylerin her birinin suçun mağduru olarak kabul edildiği görülmektedir[313].

Mağdura ilişkin bu genel açıklamalar çerçevesinde; bilişim sistemi aracılığıyla haksız yarar sağlama suçunun mağduru, bilişim sistemi veya verilere müdahale sonucu malvarlığı

---

306 **Toroslu, Nevzat**; Cürümlerin Tasnifi Bakımından Suçun Hukuki Konusu, Ankara 1970, s. 174; **Zafer**, Genel Hükümler, s. 154.

307 **Artuk/Gökcen/Yenidünya**, Genel Hükümler, s. 288; **Özgenç**, Genel Hükümler, s. 202.

308 **Erem**, Genel Hükümler Cilt 2, s. 250; **Soyaslan**, Genel Hükümler, s. 233.

309 **Özgenç**, Genel Hükümler, s. 199; **Toroslu/Toroslu**, Genel Kısım, s. 109; **Zafer**, Genel Hükümler, s. 155.

310 **Artuk/Gökcen/Yenidünya**, Genel Hükümler, s. 289; **Koca/Üzülmez**, Genel Hükümler, s. 110; **Özgenç**, Genel Hükümler, s. 203,204.

311 **Akbulut**, Genel Hükümler, s. 337; **Artuk/Gökcen/Yenidünya**, Genel Hükümler, s. 288; **Koca/Üzülmez**, Genel Hükümler, s. 110; **Özgenç**, Genel Hükümler, s. 202.

312 **Akbulut**, Genel Hükümler, s. 337; **Artuk/Gökcen/Yenidünya**, Genel Hükümler, s. 288; **Koca/Üzülmez**, Genel Hükümler, s. 111; **Özgenç**, Genel Hükümler, s. 203. Aksi yönde bkz. **Demirbaş**, Genel Hükümler, s. 550; **Soyaslan**, Genel Hükümler, s. 232.

313 **Artuk/Gökcen/Yenidünya**, Genel Hükümler, s. 289; **Koca/Üzülmez**, Genel Hükümler, s. 110; **Özgenç**, Genel Hükümler, s. 203,204.

itibariyle zarar uğrayan gerçek kişidir[314]. Bu anlamda bu suçun mağduru herkes olabilir[315]. Suçla elde edilen çıkar bu suçun konusu olduğundan ve çıkar başkalarını malvarlığı itibariyle zarara uğratmak suretiyle gerçekleştiğinden söz konusu zararın sahipleri mağdur olmaktadır.

Ayrıca TCK m. 244/4'ün bir bileşik suç olması göz ününde bulundurularak, TCK m. 244/1 ve 2'deki suçlar bakımından mağdur olabileceklerin bu suçta da mağdur olarak kabul edilmesi gerekir[316]. Buna göre, malvarlığı itibariyle zarara uğrayan gerçek kişilerin yanında, bilişim sistemine ya da sistemdeki verilerine müdahale edilen gerçek kişiler de TCK m. 244/4 bağlamında mağdur olarak kabul edilecektir.

Suçun mağdurunun mutlaka bilişim sisteminin veya sistemdeki verilerin mülkiyetine yahut zilyetliğine sahip olması gerekmez[317]. Sistem veya veriler üzerinde, mülkiyet dışı hak sahibi olan kimseler de bu suçun mağduru olabileceklerdir. Zira bilişim sisteminin maliki ile sistemin içerdiği verilerin sahibinin aynı kişi olması her durumda mümkün değildir. Sisteme karşı yapılan müdahale fiilleri bakımından verilerin malikinin sistemin sahibi dışında biri olması durumunda mağdur hem veri sahibi hem de bilişim sisteminin sahibi olacaktır.

3.1.4. Fiil ve Netice

Kabul ettiğimiz görüşe göre fiil, *"kişinin iradesiyle hâkim olduğu, belli bir neticeyi gerçekleştirmeye matuf ve harici dünyada cereyan eden bir davranıştır*[318]*."*[319]

Bilişim sistemi ile haksız yarar sağlama suçu, TCK m. 244/4'te *"Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız çıkar sağlaması…"* şeklinde tanımlanmıştır. Kanuni tanımdan anlaşılacağı üzere aynı

---

[314] **Hafızoğulları/Özen**, Topluma Karşı Suçlar, s. 457; **Koca/Üzülmez**, Özel Hükümler, s. 839; **Soyaslan**, Özel Hükümler, s. 652; **Tezcan/Erdem/Önok**, Ceza Özel, s. 773. Karşı yönde bkz. **Artuk/Gökcen/Yenidünya**, Özel Hükümler, s. 893. *"Suç tipi, mağduru bakımından bir özellik göstermez. Failin müdahalede bulunarak haksız çıkar sağladığı bilişim sisteminin yahut verinin sahibi suçun mağdurudur."*

[315] **Artuk/Gökcen/Yenidünya**, Özel Hükümler, s. 893; **Dülger**, Bilişim Suçları, s. 442; **Gürler**, Bilişim Alanında Suçlar, s. 155; **Soyaslan**, Özel Hükümler, s. 652; Özel Hükümler, s. 839; **Taşkın**, Bilişim Suçları, s. 43.

[316] **Koca/Üzülmez**, Özel Hükümler, s. 839.

[317] **Dülger**, Bilişim Suçları, s. 442.

[318] **Özgenç**, Genel Hükümler, s. 162. Aynı yönde bkz. **Akbulut**, Genel Hükümler, s. 229; **Artuk/Gökcen/Yenidünya**, Genel Hükümler, s. 230; **Koca/Üzülmez**, Genel Hükümler, s. 95.

[319] Doktrindeki baskın olan *"hareket, nedensellik bağı ve netice"*nin fiili oluşturduğu görüşü için bkz. **Centel/Zafer/Çakmut**, Türk Ceza Hukukuna Giriş, s. 232; **Demirbaş**, Genel Hükümler, s. 220; **Hafızoğulları/Özen**, Genel Hükümler, s. 168; **Soyaslan**, Genel Hükümler, s. 199.

maddenin 1. ve 2. fıkrasındaki fiiller – üçüncü fıkra ilk iki fıkranın nitelikli halini teşkil etmektedir – bilişim sistemi ile haksız çıkar sağlama suçunun unsuru haline getirilmiştir. Bu anlamda kanun koyucunun TCK m. 244/4'te bir bileşik suç[320] oluşturduğunu ifade edebiliriz[321] [322].

Bileşik suçun tanımında suçu oluşturan hareketler, birden çok olabilir ki bu durumda çok hareketli bir suç söz konusu olur[323]. Bilişim sistemi ile haksız yarar sağlama suçunda failin öncelikle bu suça unsur olarak katılan sistemi engelleme, bozma; verileri yok etme veya değiştirme suçundaki fiillerden birini işlemesi ve ardından bu fiil sonucu haksız bir çıkar elde etmesi gerektiğinden, bu suç çok hareketli bir suçtur[324].

Bu anlamda öncelikle 244. maddenin 1. ve 2. fıkralarındaki fiilleri incelemek gerekir. TCK m. 244/1'de bilişim sisteminin işleyişinin engellenmesi veya bozulması yaptırım altına alınmıştır. 2. fıkrada ise bir bilişim sistemindeki verileri; bozmak yok etmek, değiştirmek, erişilmez kılmak ile sisteme veri yerleştirmek yahut sistemde var olan verileri başka bir yere göndermek fiilleri yaptırım altına alınmıştır. Kanaatimizce bu hususlar hareketin kendisi değil, neticeleri olduğundan, fail bu neticeleri gerçekleştirmeye elverişli her hareketle bu suçları işleyebilecektir ki bu durumda söz konusu suçlar serbest hareketli olmaktadırlar[325]. Fail icra edeceği herhangi bir hareketle bilişim sisteminin işleyişini engeller veya bozarsa yahut sistemdeki verileri bozar yok eder, değiştirir, erişilmez kılar veya sisteme veri

---

[320] **Özbek/Doğan/Bacaksız/Tepe**, Genel Hükümler, s. 591: Bileşik suçtan maksat kanunda başlı başına bir suç olarak düzenlenen bir fiilin yine kanunda başka bir suçun unsuru veya ağırlaştırıcı sebebi olarak belirlenmesidir. Başka bir suça unsur veya ağırlaştırıcı neden olarak katılan suç, bu norm içinde erimekte ve bağımsızlığını kaybetmektedir. Kanun koyucu bileşik suçu TCK m. 42'de şu şekilde tanımlamıştır: *"Biri diğerinin unsurunu veya ağırlaştırıcı nedenini oluşturması dolayısıyla tek fiil sayılan suça bileşik suç denir. Bu tür suçlarda içtima hükümleri uygulanmaz."* Unsur veya ağırlaştırıcı neden olarak katılan norm, oluşturulan yeni norm içinde eridiğinden artık bu durumda hukuken tek fiil ve tek suç bulunmaktadır.

[321] **Koca**, Hukukumuzda TCK'nın 244'ncü maddesi, s. 96.

[322] **Özbek/Doğan/Bacaksız/Tepe**, Özel Hükümler, s. 962. Bu yazarlar TCK m. 244/4'ü bağımsız bir suç olarak kabul etmez iken sistemi engellemek, bozmak, verileri yok etmek veya değiştirmek suçlarının içtima bahsinde 4. fıkranın bir bileşik suç olduğunu ifade etmektedirler.

[323] **Koca/Üzülmez**, Genel Hükümler, s. 532.

[324] **Artuk/Gökcen/Yenidünya**, Özel Hükümler, s. 892; **Dülger**, Bilişim Suçları, s. 443; **Gürler**, Bilişim Alanında Suçlar, s. 156; **Koca**, Hukukumuzda TCK'nın 244'ncü maddesi, s. 98; **Soyaslan**, Özel Hükümler, s. 652.

[325] **Dülger**, Bilişim Suçları, s. 417; **Erdoğan**, TCK'da Bilişim Suçları, s. 186; **Koca/Üzülmez**, Özel Hükümler, s. 827; **Pallı**, Bilişim Suçları, s. 170: "*Buna göre suçun hareket kısmı, sadece mausu tıklamak veya klavyeyi kullanmak olmakta fakat bu eylemler sonucunda sistem engellenmekte veya bozulmakta veya verilerin yok olması gibi değişik neticeler ortaya çıkmaktadır. Aksi takdirde failin, sistemi engellemeyi virüs kullanmak suretiyle bizzat kendinin sağlayabilmesi için kendisini dijitalize edip, sanal ortama aktarıp sistemi elleriyle engellemesi aranmalıdır. Bu mümkün olamadığından teknolojinin imkân tanıdığı sembolik hareketler ile eylem gerçekleştirilmekte ve sonuç elde edilmektedir."*

yerleştirir, sistemdeki verileri başka bir yere gönderirse 244. maddenin 1. veya 2. maddesinden sorumlu olacaktır.

Aynı durum inceleme konumuz olan TCK m. 244/4 için de geçerlidir. Fail 1. ve 2. fıkrada sayılan neticelere herhangi bir hareketle neden olur ve bunun sonucunda kendisi veya başkası için haksız bir çıkar sağlarsa bu madde uyarınca sorumlu olacaktır. Bu anlamda haksız yarar sağlama, bu suçun netice unsurunu oluşturur[326].

TCK m. 244/4, bağlı hareketli[327] bir suçtur[328]. Zira fail haksız çıkarı, bilişim sisteminin işleyişini engelleyerek veya bozarak yahut sistemdeki verileri bozarak, yok ederek, değiştirerek, erişilmez kılarak veya sisteme veri yerleştirerek ya da var olan verileri bir başka yere göndererek elde etmelidir[329].

TCK m. 244/1 ve 2, inceleme konumuz olan suçun unsuru olduğundan öncelikle bu suçların fiil unsuru incelenecek ardından TCK m. 244/4 bağlamında haksız yarar sağlamadan ne anlaşılması gerektiği ortaya konulacaktır.

"Bilişim sisteminin işleyişinin engellenmesi" bakımından suçun oluşabilmesi için failin bu neticeyi gerçekleştirmeye elverişli hareketleri icra etmesi gerekmektedir. Engellemek, sözlükte, bir şeyin gerçekleşmesini veya yapılmasını önlemek olarak tanımlanmıştır. Öyleyse kanuni tanımda bilişim sisteminin engellenmesinden bahsedildiğine göre failin gerçekleştirdiği hareketin, bilişim sisteminin fonksiyonunu icra etmesini engellemesi gerekmektedir[330]. Bilişim sistemlerinin fonksiyonu ise bilgileri otomatik işleme tabi tutarak sisteme girilen bilgilerden çeşitli algoritmalar yardımıyla sonuç üretmesi, ürettiği sonuçları depolaması ve istenildiği zaman bu sonuçları kullanıcısına sunabilmesidir. İşte failin gerçekleştirdiği hareketle, bilişim sistemi bu fonksiyonlarını icra edemez ise bilişim sisteminin engellenmesi söz konusu olacaktır[331].

---

[326] **Soyaslan**, Özel Hükümler, s. 652.

[327] **Hafızoğulları/Özen**, Topluma Karşı Suçlar, s. 458; **Koca/Üzülmez**, Özel Hükümler, s. 840.

[328] *Erdoğan,* bu suçu serbest hareketli bir suç olarak değerlendirmektedir. Bunun sebebi olarak da maddenin birinci ve ikinci fıkralarında düzenlenen fiillerin kanunda neticelerinin belirtildiğini ve bu halde de bu neticelere yol açabilecek her türlü hareketle bu suçların işlenebileceğini göstermektedir. Bkz. **Erdoğan**, TCK'da Bilişim Suçları, s. 228.

[329] **Hafızoğulları/Özen**, Topluma Karşı Suçlar, s. 458.

[330] **Avşar/Öngören**, Bilişim Hukuku, s. 136.

[331] **Kurt**, Tüm Yönleriyle Bilişim Suçları, s. 164.

Kanun koyucu sistemin engellenmesi ve bozulmasını farklı neticeler olarak belirlediğinden, sistemi engelleme neticesinin sistemi tamamen çalışamaz hale getirmemesi gerekmektedir. Fail, bilişim sisteminin kendisinden beklenen fonksiyonlarını geçici süreyle durdurur yahut sistemin fonksiyonlarını gerçekleştirmesini yavaşlatır ise sistemi engelleme neticesini gerçekleştirmiş olacaktır[332]. Bu anlamda sistemi engellemenin kısa süreli veya uzun süreli olması suçun oluşumu için önem taşımaz. Örneğin, fail, mağdurun bilişim sistemine göndereceği bir *"malware"* ile sistemin internete bağlanmasını engelleyebilir yahut bu yazılımı mağdurun sisteminin arka planında çalışmasını sağlayarak sistemin yavaşlamasına neden olabilir. İşte bu fiiller ile failin maddi bir yarar elde etmesi durumunda da TCK m. 244/4 anlamında suç oluşacaktır.

"Bilişim sisteminin işleyişinin bozulması" bakımından suçun oluşabilmesi için failin yine bu neticeyi gerçekleştirmeye elverişli hareketleri icra etmesi gerekmektedir. Bozma, sözlükte, bir şeyi kendisinden beklenilen işi yapamayacak duruma getirmek olarak tanımlanmıştır. Bozma ve engelleme bakımından sözlükteki tanımlar karşılaştırıldığında, bozma eyleminin engelleme eylemini de kapsadığı görülmektedir. Dolayısıyla her bozma bir engelleme iken her engelleme bir bozma değildir[333]. Esasen bu durum bozmanın sürekli bir neticeyi doğurmasından kaynaklanmaktadır. Zira bozma eylemi ile bilişim sistemi artık kendisinden beklenen fonksiyonları yerine getiremeyecek bir hal almaktadır. Ancak engellemede, bilişim sisteminin fonksiyonlarını icra etmesi geçici bir süreyle mümkün olamamaktadır[334].

Bu netice bakımından dikkat edilmesi gereken, failin yapacağı müdahalenin sistemin tamamına yönelik olması gerekmediğidir[335]. Başka bir deyişle fail, fiili ile sistemin bir kısmını hedeflemiş olabilir. Ancak failin hedeflediği kısım sistemin mevcut durumu ile fonksiyonunu bir daha yerine getiremeyecek bir hale gelmesine neden oluyorsa söz konusu netice gerçekleştirilmiş olacaktır.

Suçun kanuni tanımında bozma ve engelleme neticelerinin bilişim sisteminin işleyişi üzerinden gerçekleşmesi gerektiği düzenlenmiştir. Yani fiil bir bilişim sisteminin *"işleyişinin"* engellenmesi veya bozulmasıdır. Dolayısıyla kanun koyucu sistemin işleyişi

---

[332] **Kurt**, Tüm Yönleriyle Bilişim Suçları, s. 164.

[333] **Karagülmez**, Bilişim Suçları, s. 238.

[334] **Özbek/Doğan/Bacaksız/Tepe**, Özel Hükümler, s. 949.

[335] **Karagülmez**, Bilişim Suçları, s. 238.

ifadesi ile bilişim sistemlerinin donanım unsurlarının değil, yazılım unsurunun engellenmesi veya bozulmasını, koruma altına almış olmaktadır[336]. Elbette bilişim sisteminin yazılım unsuruna yapılan müdahale ile donanım unsurlarının engellenmesi veya bozulması mümkündür. Örneğin, *"tavşan" (rabbit)* kötücül yazılımı, sistemin işlemcisine sürekli anlamsız komutlar vererek işlemcinin bilişim sisteminin normal işleyişini sağlayan komutları vermesini engellemekte ve giderek sistemin yavaş çalışmasına neden olarak en sonunda da sistemi çalışamaz hale getirmektedirler[337]. Ancak bu ve benzer örneklerde, bilgisayarın donanım unsuruna fiziki bir müdahale gerçekleşmemekte, yazılım unsuruna müdahale ile donanım unsuru çalışamaz hale gelmektedir. Bu anlamda bilişim sisteminin donanım unsuruna fiziki müdahaleler TCK m. 244 kapsamında yaptırım altına alınmış değildir. Zira bilişim sisteminin donanım unsuruna karşı müdahale fiilleri, TCK m. 151 *"mala zarar verme suçu"* kapsamında cezai koruma altına alınmıştır[338]. Zaten esas olarak, bilişim sistemlerinin soyut unsurunun yani yazılımının, *"mal"* niteliğinde kabul edilememesi, TCK m. 244'deki suçların düzenlenmesi gerekliliğini ortaya çıkarmıştır. Dolayısıyla gerekçedeki *"aracın fizik varlığı ve işlemesini sağlayan bütün diğer unsurları, söz konusu suçun konusunu oluşturmaktadır."* ifadesine katılmamaktayız.

TCK m. 244/2'de düzenlenen fiiller sistemdeki verilere zarar vermeye yönelik olabileceği gibi sistemdeki verileri başka bir yere göndermek ve sisteme veri yerleştirmek şeklinde de olabilir.

---

[336] **Koca/Üzülmez**, Özel Hükümler, s. 827. Aynı yönde bkz. **Ketizmen**, Bilişim Suçları, s. 133, 135; **Özbek/Doğan/Bacaksız/Tepe**, Özel Hükümler, s. 949: *"... bilişim sistemi dışındaki unsurlara yapılan müdahaleler m. 244 anlamında bozma ya da engelleme olarak kabul edilemez. Örneğin, taşınabilir bilgisayarın yere atılarak kırılması, klavyenin tuşlarının parçalanması gibi durumlar mala zarar verme suçunu oluşturur."* Karşı yönde bkz. **Dülger**, Bilişim Suçları, s. 418; **Karagülmez**, Bilişim Suçları, s. 238; **Soyaslan**, Özel Hükümler, s. 644; **Dülger**, Bilişim Suçları, s. 418: *"Sistemin işlemesinin engellenmesi bilişim sisteminin elektriğinin kesilmesi, sistemleri birbirine bağlayan kabloların çıkarılması, bilişim sisteminin donanımına ait bir unsurun çıkarılması gibi bilişim sisteminin somut unsurlarına yönelik eylemlerle gerçekleştirilebileceği gibi, sisteme bilişim virüsü ya da mantık bombası gibi zararlı bir yazılımın bulaştırılması ya da sistemde olmayan bir şifrenin sisteme yerleştirilmesi veya mevcut şifrenin değiştirilmesi gibi bilişim sisteminin soyut unsurlarına yönelik eylemlerle de gerçekleştirilebilecektir."*

[337] **Dülger**, Bilişim Suçları, s. 126.

[338] **Koca/Üzülmez**, Özel Hükümler, s. 827; **Hafızoğulları/Özen**, Topluma Karşı Suçlar, s. 453: *"Bir bilişim sisteminin donanımına zarar vermek, sonuçta bilişim sisteminin işlemesine zarar vermek olmakla birlikte; yorumda, zorunlu olarak suçun hukuki konusu göz önüne alındığında, işleyişine zarar verilen bilişim sisteminden, sistemin donanımı değil, yazılımı anlaşılmalıdır. Elbette, donanım, yani bilişim sistemini oluşturan her türlü fiziksel parça maldır, sistemde kullanılan enerji mal hükmündedir. Ancak, donanıma nasıl davranılacağını ve hangi işlemleri yapacağını anlatan yazılım, ekonomik bir değer olmakla birlikte ne maldır ne de mal hükmündedir."*

"Bilişim sistemindeki verileri bozma" neticesinde, failin verinin içeriğine veya yapısına müdahale etmek suretiyle veriyi kısmen yahut tamamen kullanılmaz hale getirmesi söz konusudur[339]. Yukarıda da ifade ettiğimiz üzere sisteme müdahale fiillerinin sistemin yazılım unsuru üzerinden olması gerektiğinden, failin esasen sistemin verilerine müdahale ile sistemi engelleme fiilini gerçekleştirmesi gerekmektedir. Dolayısıyla fail verileri bozma neticesi bakımından yapacağı müdahale sistemin tamamının engellenmesine ya da bozulmasına neden olmamalıdır[340]. Failin bu netice bakımından kastının sadece belli veri veya verilerin kullanılamaz hale getirilmesi yönünde olmalıdır.

*"Verilerin yok edilmesi"*den verinin mantıki yok edilmesi anlaşılmalıdır. Zira inceleme konumuz suçun koruduğu bilişim sisteminin donanım unsuru değil, yazılım unsurudur. Dolayısıyla verinin içinde bulunduğu veri taşıma cihazı veya bilişim sisteminin yok edilmesi durumunda bu netice gerçekleştirilmemiş, şartların oluşması durumunda mala zarar verme suçu gerçekleştirilmiş olacaktır. Bilişim dünyasında bir verinin geri döndürülemez şekilde yok edilmesi istisnai bir nitelik arz etmektedir. Verinin geri döndürülemez şekilde yok edilmesinin öncelikle veri taşıma cihazının fiziksel yok edilmesi ile mümkün olduğunu söyleyebiliriz. Ancak daha önce de ifade ettiğimiz üzere, inceleme konumuz olan suç tipi ile bilişim sistemlerinin sanal unsuru yani yazılım unsuru koruma altına alınmıştır.

Veri taşıma cihazının fiziksel olarak yok edilmesi veya manyetik müdahale dışında, verinin geri döndürülemez şekilde yok edilmesi ancak veri üzerine yeni veri yazılması ile mümkündür[341]. Bununla ilgili olarak ilk yöntem *"wipe"* etme işlemidir. *"Wipe"* etme işleminde uygun yazılımlarla veri taşıma cihazının tamamındaki mevcut veriler üzerine yeni veriler yazılmaktadır. Eğer *"wipe"* etme yazılımı, işini doğru yaparsa ilgili veri taşıma cihazındaki verilere ulaşılması günümüzün teknik imkanları ile mümkün değildir. *"Wipe"* etmeye benzer şekilde *"shred"* yönteminde de veri geri döndürülemez şekilde silinmektedir. Ancak bu yöntemin *"wipe"* etmeden farkı tüm veri taşıma cihazındaki verileri değil yalnız istenilen veriyi silmesidir.[342]

---

339 **Artuk/Gökcen/Yenidünya**, Özel Hükümler, s. 770; **Dülger**, Bilişim Suçları, s. 415; **Ketizmen**, Bilişim Suçları, s. 139; **Koca/Üzülmez**, Özel Hükümler, s. 829; **Özbek/Doğan/Bacaksız/Tepe**, Özel Hükümler, s. 923.

340 **Karagülmez**, Bilişim Suçları, s. 239.

341 **Dülger**, Bilişim Suçları, s. 421.

342 **Fisher**, Wipe vs Shred vs Delete vs Erase: What's the Difference?, https://www.lifewire.com/wipe-vs-shred-vs-delete-vs-erase-whats-the-difference-2619146, s.e.t. 19.05.2017.

Tüm bunlardan hareketle, verilerin yok edilmesi fiilinden kanun koyucunun verilerin geri döndürülemez şekilde silinmesini hükme bağladığı kanaatindeyiz[343]. Dolayısıyla veri sahibinin verisini sistemde daha önce konumlandırdığı yerde bulamaması sonucunu doğuracak hareketlerin, veriyi yok etme değil veriyi erişilmez kılma hareketini oluşturduğunu düşünmekteyiz. Zira verilerin erişilmez kılınması, verinin içeriğine ve yapısına müdahale edilmeksizin sistem kullanıcısının bu veriye istediği şartlarda ve olağan yollarla erişiminin engellenmesidir. Öyleyse kullanıcı verisini sistemde konumlandırdığı yerde bulamadığında verisine istediği zaman ve olağan şekilde ulaşamadığı, veriye ulaşmak için ayrıca bir çaba sarf etmesi gerektiği için; verinin yok edilmesinden değil erişilmez kılınmasından söz edebiliriz.

Bu anlamda verinin sistem içerisinde yerini değiştirmekten ibaret olan, veriyi geri dönüşüm kutusuna yahut geçici öğeler bölümüne göndermek eyleminin veriyi yok etme değil[344], veriyi erişilmez kılma neticesini oluşturacağı kanaatindeyiz[345]. Aynı durum verinin geri dönüşüm kutusundan veya geçici öğeler bölümünden silinmesi durumunda da geçerlidir. Zira bu durumda mağdur uygun yazılımlarla verisine tekrar kavuşabilme olanağına sahiptir[346].

"Verilerin değiştirilmesi" fiili *"var olan verinin kullanılmasını engellemeyen fakat verinin içeriğinin ya da kendisinin orijinalliğini ortadan kaldıran her türlü değişiklik"*[347] şeklinde

---

[343] Karşı yönde bkz. **Dülger**, Bilişim Suçları, s. 421: *"Verilerin gerçek anlamda silinmesi ise "wipe" denilen işlemle sabit diske elektromanyetik şok verilmesi ve sabit diskin katmanları üzerinde bulunan ve okuyucu kafanın izlediği çizgilerin (eski plaklardaki iğnenin üzerinden geçtiği çizgiler gibi) yok edilmesiyle gerçekleşmektedir. Buna göre söz konusu hareketin gerçekleşmiş olması için verilerin mantıksal olarak silinmesi yeterli olup mutlaka "wipe" işlemine tabi tutulmuş olması gerekmemektedir."*

[344] **Koca**, Hukukumuzda TCK'nın 244'ncü maddesi, s. 94; **Taşkın**, Bilişim Suçları, s. 47.

[345] Karşı yönde bkz. **Dülger**, Bilişim Suçları, s. 421 : *"Bu hareket açısından belirtilmesi gereken bir başka konu da, verilerin pek çok işletim yazılımında olduğu üzere yok etmek amacıyla "geri dönüşüm kutusuna" gönderilmesi ancak tamamen silinmemesi ya da bilişim sisteminde yüklü bulunan işletim sisteminin "geçici öğeler klasöründe" kopyası bulunan öğelerin silinmesi halinde yok etmek eyleminin gerçekleşmiş sayılıp sayılmayacağıdır. Yukarıda da belirtildiği üzere, bilişim sistemlerinde aslında gerçek anlamda bir silme işlemi değil mantıki bir silme söz konusu olmaktadır; bu da o verilere ulaşılmanın bir şekilde engellenmesiyle gerçekleşmektedir. Bu durumda da mağdurun verilerine ulaşamaması artık verilerin onun açısından yok edilmiş olması anlamına geleceğinden, yok etmek eylemi gerçekleşmiş olacaktır."*

[346] **Fisher**, Wipe vs Shred vs Delete vs Erase: What's the Difference?, https://www.lifewire.com/wipe-vs-shred-vs-delete-vs-erase-whats-the-difference-2619146, s.e.t: 19.05.2017.

[347] **Ketizmen**, Bilişim Suçları, s. 140.

ifade edilebilir. Değiştirme, sistemdeki veriyi tamamen yeni bir veri olarak ortaya çıkarabileceği gibi mevcut veriyi kısmen de etkileyebilir[348].

Verilerin değiştirilmesi ile haksız yarar elde etmeye ilişkin olarak Yargıtay'ın şu kararını örnek gösterebiliriz: *"TEDAŞ'ta görevli olan sanığın; kendisine ve 30 kişiye ait elektrik faturasıyla ilgili bilgisayardaki kayıtları silmek veya ödenmediği halde ödendi şeklinde değiştirmek suretiyle gerçekleşen eyleminin fatura borcunu sildiği her kişi için ayrı ayrı TCK nun 525/b-2, 80. maddeleri uyarınca ceza belirlenmesi gerektiğine"*[349] Bu olayda fail, bilişim sistemindeki verileri değiştirerek, TCK m. 244/2'deki *"sistemdeki verileri değiştirme"* neticesine neden olmuştur. Bu suçun, 765 sayılı TCK dönemindeki karşılığı ise TCK m. 525/b-2 olduğundan Yargıtay sorumluluğu bu madde uyarınca belirlemiştir.

"Verilerin erişilmez kılınması", verinin içeriğine ve yapısına müdahale edilmeksizin sistem kullanıcısının bu veriye istediği şartlarda ve olağan yollarla erişiminin engellenmesidir[350]. Verinin tamamına veya bir kısmına erişimin engellenmesi, bu fiil açısından önem taşımaz. Bu fiil ilgili veriye yahut verinin sistem içerisinde bulunduğu bölüme şifre koymak suretiyle icra edilebileceği gibi, verinin içeriği bozulmaksızın, kullanıcının olağan yollarla ulaşamayacağı şekilde sistem içerisindeki konumunun ve isminin değiştirilmesi ile de icra edilebilir. Bu noktada dikkat edilecek husus, suçun oluşumu için; veriye erişimin kesin bir biçimde engellenmesinin gerekmediği; kullanıcının istediği zaman ve olağan yollarla erişimini engellemenin yeterli olduğudur[351]. Ayrıca failin fiili, mağdurun sistemine uzaktan, yani sanal yollarla erişerek icra etmesi ile fiziken erişerek icra etmesi arasında bir fark bulunmamaktadır[352].

Söz konusu bu neticenin yargı kararlarına çokça yansıdığı görülmektedir. Özellikle mağdurun e-posta veya sosyal medya hesap şifrelerinin değiştirilerek mağdurun buralarda bulunan verilerine erişiminin engellenmesi ile uygulamada sıklıkla karşılaşılmaktadır.

Yargıtay 8. Ceza Dairesi, 2013 yılında verdiği bir kararında *"Oluşa, katılanın aşamalardaki anlatımlarına, sanığın babasına ait internet hesabından katılana ait elektronik posta*

---

348 **Kurt**, Tüm Yönleriyle Bilişim Suçları, s. 169.

349 *Y 11. CD, 6583/771, T. 30.01.2004,* Aktaran, **Ergün**, Siber Suçların, s. 99.

350 **Ketizmen**, Bilişim Suçları, s. 140; **Koca/Üzülmez**, Özel Hükümler, s. 830; **Özbek/Doğan/Bacaksız/Tepe**, Özel Hükümler, s. 952.

351 **Dülger**, Bilişim Suçları, s. 422.

352 **Ketizmen**, Bilişim Suçları, s. 140; **Kurt**, Tüm Yönleriyle Bilişim Suçları, s. 169.

hesabına bir çok kez girildiğine ilişkin Microsoft ve TİB'den gelen yazı yanıtlarına ve tüm dosya kapsamına göre; katılana ait elektronik posta hesabının şifresini ele geçirerek bu adrese giren ve şifreyi değiştirmek suretiyle katılanın elektronik postalarına erişimini engelleyen sanığın, eylemine uyan TCK.nun 244/2. maddesi uyarınca cezalandırılmasına karar verilmesi gerekirken yazılı gerekçeyle beraat hükmü kurulması,"[353] gerektiğine hükmetmiştir.

Yine aynı daire 2014 yılında verdiği bir kararında *"Katılana ait hotmail adresine hukuka aykırı olarak giren ve yeni şifre oluşturup katılanın erişimini engelleyerek e-mail adresini kullanan sanığın eylemine uyan TCK. nun 244/2. madde ve fıkrası uyarınca cezalandırılması gerektiği gözetilmeden yazılı şekilde yasal ve yeterli olmayan gerekçeyle beraatına hükmolunması,"*[354] gerektiği belirtilerek bu fiillerin elektronik hesaplara erişim engellenmesi oluşturacağını kabul etmiştir.

"Bilişim sistemine veri yerleştirmek"; sistem kullanıcısının rızası dışında, sisteme ve sistemdeki verilere zarar verilmeksizin, bilişim sisteminde daha önce var olmayan, sisteme yabancı bir veriyi bu sisteme eklemektir. Veri yerleştirme, sisteme girilerek veya girilmeden, fiziken müdahale ile yahut uzaktan erişim yoluyla gerçekleştirilebilir[355]. Fiziken müdahale yolunda fail sisteme herhangi bir veri taşıma aracıyla veri yerleştirebileceği gibi, bu araçları kullanmadan girdiği sistemdeki bir veriyi değiştirmeden yine o sistem aracılığıyla yeni bir veri de oluşturabilir.

"Bilişim sistemindeki verilerin başka bir yere gönderilmesi"[356] neticesinin verileri erişilmez kılma neticesinden farkını ortaya koyabilmek açısından; bu neticeyi failin verileri bulunduğu bilişim sisteminde farklı bir yere göndermesi şeklinde değil, sistem dışında farklı bir bilişim sistemine yahut veri taşıma cihazına aktarması, kaydetmesi ya da kopyalaması şeklinde anlamak gerektiği kanaatindeyiz. Bu çerçevede bilişim sistemindeki verilerin başka bir yere gönderilmesi neticesinin gerçekleştiğinin kabulü için mağdurun kendi verisine erişip erişemediğine ya da orijinal verinin yok edilip edilmediğine bakılmayacaktır.

---

[353] *Y 8. CD, E. 2012/31216, K. 2013/25978, T. 1.11.2013*. (kazanci.com s.e.t: 19.05.2017).

[354] *Y 8. CD E. 2013/771 K. 2014/15833 T. 23.6.2014*. (kazanci.com s.e.t: 19.05.2017)

[355] **Dülger**, Bilişim Suçları, s. 427.

[356] Bu netice, TBMM'ye 15.05.2003 tarihinde sunulan tasarının sistem ve veriye müdahaleyi düzenleyen 347. maddesinde yer almamaktadır. Bu netice, Adalet Komisyonunda maddeye eklenmiştir. Bkz. **Ketizmen**, Bilişim Suçları, s. 140.

Söz konusu durumu bir örnek üzerinden şu şekilde açıklığa kavuşturabiliriz: Eğer fail, mağdurun bilişim sistemindeki veriyi geri dönüşüm kutusuna ya da sistem içerisindeki başka bir bölüme veya klasöre gönderirse veriyi erişilmez kılma neticesini gerçekleştirmiş olacaktır. Ama eğer bu veriyi sistem içerisinde farklı bir yere değil de sisteme taktığı bir veri cihazına kaydederse, verilerin başka bir yere gönderilmesi neticesini gerçekleştirmiş olacaktır. Bu durumda mağdurun orijinal verisinin silinip silinmediği ya da yok edilip edilmediği önem taşımamaktadır. Eğer fail veri taşıma cihazına aktardıktan sonra orijinal veriyi yukarıda açıklanan yöntemlerle geri döndürülemez şekilde silerse, ayrıca veriyi yok etme neticesini gerçekleştirmiş olacaktır.

TCK m. 244/4'teki bilişim sistemi aracılığıyla haksız yarar sağlama bileşik suçunun ilk kısmını yukarıda açıkladığımız fiiller oluşturmaktadır. Failin, bilişim sistemi aracılığıyla haksız yarar sağlama suçundan sorumlu olabilmesi için bu sayılan fiillere ek olarak kendisi veya bir başkası için haksız bir çıkar da sağlamış olması gerekmektedir[357]. Haksız çıkar sağlama, bu suçta netice unsurunu teşkil etmektedir.

Suçun konusunda açıklandığı üzere, bu suç bakımından sorumluluk için, failin elde etmesi gereken yarar maddi – ekonomik nitelikte olmalıdır. Bu çerçevede örneğin, failin sırf kız arkadaşının başka şehre gitmemesi için onun ÖSYM şifresi ile üniversite sınavına ilişkin tercihlerini değiştirmesi durumunda failin manevi yarar elde ettiğinden bahisle TCK m. 244/4'ten sorumlu tutulması söz konusu olmayacaktır. Fail bu durumda *"verileri değiştirmek"* neticesini gerçekleştirmek bakımından TCK m. 244/2'den sorumlu olacaktır.

Suç, haksız çıkarın failin veya başkasının tasarruf alanına sokulması yahut çıkar üzerinde fail veya başkasının tasarruf edebilecek imkana kavuşmasıyla tamamlanır[358]. Hukuken tasvip edilmeyen her türlü menfaat, haksız çıkar teşkil edecektir. Çıkarın maddi – ekonomik olması, muhakkak failin veya başkasının malvarlığının aktiflerinin artması anlamına gelmemektedir. Fail veya bir başkasının malvarlığındaki pasiflerin azalması durumunda da

---

[357] Haksız yarar sağlamaya ilişkin olarak *"Tepe"* şu şekilde bir örnek vermektedir: *"İnternet ortamında gerçeklesen bir açık artırmada, katılımcılardan biri yönlendirdiği bir kötücül bir yazılımla online açık artırmanın yapıldığı programa müdahale edilip, ki bu müdahale sistemi engelleme veya bozma sekline olabilir, açık arttırmanın usulüne aykırı olarak sonlandırılması neticesinde haksız bir menfaat temin etmiş olsun. Yine aynı örnek üzerinden farklı bir ihtimal düşünülecek olursa, online açık artırmanın katılımcılarından biri, diğer katılımcılara yönlendirdiği bir virüs programıyla bu katılımcıların ethernet girişini devre dışı bırakarak internet bağlantılarını kesip açık artırmanın yapıldığı sistemden çıkmalarını sağlayarak bir haksız menfaat temin etsin."* (**Tepe**, İnternet Suçluluğu, s. 298.)

[358] **Koca/Üzülmez**, Özel Hükümler, s. 840.

maddi bir çıkar elde etme söz olacaktır. Aynı şekilde maddede ifade edilen neticelerle failin veya bir başkasının iş imkanına kavuşması durumunda da maddi – ekonomik bir çıkar elde edilmiş olacaktır[359].

Suçun tamamlanması için çıkarın elde edilmesi gerektiğinden, söz konusu suç neticeli suçlardandır. Çıkar elde edilememişse, netice gerçekleşmemiş ve böylece suç tamamlanmamış olacaktır ki bu durumda teşebbüs hükümlerinin uygulanması gerekecektir[360].

Kanundaki *"haksız bir çıkar sağlanmasının başka bir suç oluşturmaması halinde"* ifadesine Yargıtay kararlarıyla birlikte içtima bahsinde detaylıca değinileceği için burada sadece; inceleme konumuz olan suçun yaptırımının, suçun daha ağır cezayı gerektiren bir suç oluşturmaması halinde değil, fiilin bir başka suç oluşturmaması halinde uygulanacağını belirtmekle yetiniyoruz.

3.2. Tipikliğin Manevi Unsuru

Manevi unsur, kişi ile işlediği fiil arasındaki manevi bağı ifade etmektedir[361]. *"Bu bağ tesis edilmeden, gerçekleştirilen davranış fiil niteliğini taşımaz ve dolayısıyla, bir suçun varlığından söz edilemez."*[362].

TCK m. 22/1: *"suçun oluşması kastın varlığına bağlıdır"* hükmü uyarınca ceza hukukunda kural olarak manevi unsur kasttır, kanunda açıkça ve ayrıca belirtilmediği sürece taksirli hareketler cezalandırılmaz[363].

Doktrindeki baskın görüşe göre kast ve taksir haksızlığın işleniş şekli değil, birer kusur şeklidir[364]. Bizim de katıldığımız diğer bir görüş ise kast ve taksiri, birer kusur şekli olarak

---

[359] **Koca/Üzülmez**, Özel Hükümler, s. 840.

[360] **Koca, Mahmut**; "*Yargıtay Kararları Işığında Bilişim Sistemlerinin Kullanılması Suretiyle Haksız Yarar Sağlama Suçları*", Prof. Dr. Ali Güzel'e Armağan, İstanbul 2010, s. 1660.

[361] **Akbulut**, Genel Hükümler, s. 347; **Artuk/Gökcen/Yenidünya**, Özel Hükümler, s. 293; **Koca/Üzülmez**, Genel Hükümler, s. 139; **Özgenç**, Genel Hükümler, s. 221.

[362] **Özgenç**, Genel Hükümler, s. 221.

[363] **Artuk/Gökcen/Yenidünya**, Genel Hükümler, s. 297; **Koca/Üzülmez**, Genel Hükümler, s. 139; **Özgenç**, Genel Hükümler, s. 244.

[364] **Alacakaptan, Uğur**; Suçun Unsurları, Ankara 1961, s. 93; **Centel, Nur/Zafer, Hamide/Çakmut, Özlem**; Türk Ceza Hukukuna Giriş, İstanbul 2016, s. 350; **Demirbaş**, Genel Hükümler, s. 366; **Dönmezer/Erman**, Nazari ve Tatbiki Ceza Hukuku - 2, s. 226; **Hafızoğulları/Özen**, Genel Hükümler, s. 276; **İçel, Kayıhan**; Ceza Hukuku Genel Hükümler, İstanbul 2016, s. 426; **Öztürk, Bahri/Erdem, Mustafa Ruhan**;

değil, haksızlığın işleniş şekli veya haksızlığın unsuru olarak ele almaktadır[365]. Başka bir ifadeyle kast, kusurun bir unsuru veya türü olarak değil[366], suçun kanuni tanımındaki tipte belirtilen unsurları gerçekleştirme iradesini, fiilin ifade ettiği haksızlığın bir unsurunu teşkil etmektedir[367].

Bilişim sistemleri ile haksız yarar sağlama suçunda kanunda açıkça ve ayrıca suçun taksirli halinin de cezalandırılacağına ilişkin bir düzenleme olmadığından suç ancak kastla işlenebilecektir.

Ayrıca bazı suç tiplerinde kastın yanında suçun yapısal unsuru olarak sübjektif tipiklik unsurları da düzenlenebilir. Bu unsurlar özel bir maksat, özel bir bilme yahut failin özel bir saiki olarak karşımıza çıkabilir. Doktrinde kast için tipikliğin genel sübjektif unsuru ifadesi kullanılırken, saydığımız bu unsurlar için ise tipikliğin özel sübjektif unsuru ifadesi kullanılmaktadır.[368]

İnceleme konumuz olan suç tipi açısından doktrinde kastın yanında özel bir sübjektif unsurun tipikliğe dahil olup olmadığı hususunda tartışma vardır. Doktrinde bazı yazarlar suçun oluşumu için failin, genel kastının yanında kendisi veya başkasına yarar sağlama maksadının da bulunması gerektiğini ifade etmiştir[369]. Ancak kanaatimizce failin kendisi veya başkası için haksız çıkar sağlamasına ilişkin bilgi tipikliğin özel bir sübjektif unsuru

---

Uygulamalı Ceza Hukuku ve Güvenlik Tedbirleri Hukuku, Ankara 2016, s. 271; **Soyaslan**, Genel Hükümler, s. 417; **Toroslu/Toroslu**, Genel Kısım, s. 198.

[365] **Akbulut**, Genel Hükümler, s. 349; **Artuk/Gökcen/Yenidünya**, Genel Hükümler, s. 294; **Koca/Üzülmez**, Genel Hükümler, s. 143; **Özgenç**, Genel Hükümler, s. 223.

[366] **Koca/Üzülmez**, Genel Hükümler, s. 141: *"19. yüzyılda hakim olan pozitivizm düşüncesine dayanan klasik suç teorisi kastı, taksirle birlikte, bir kusurluluk şekli olarak ele almaktadır. Bu teori haksızlık ve kusur arasında çok keskin bir ayrım yapmakta, suçun tüm objektif unsurlarını haksızlık alanına, tüm sübjektif unsurlarını ise kusurluluk alanına dahil saymaktadır."*; **Özgenç**, Genel Hükümler, s. 223: *"Türk hukukunda halen kast ve taksirin, birer 'kusurluluk şekli' veya 'kusur türü' olduğu görüşü hakimdir."*; **Özgenç**, Genel Hükümler, s. 221: *"Ancak, belirtmek gerekir ki, manevi unsurla kusurluluğu da birbirine karıştırmamak gerekir. Bilahare izah edileceği gibi, kusurluluk, işlediği suç dolayısıyla kişinin kınanması, muaheze edilmesi gerektiği hususundaki yargıyı ifade etmektedir. Bu bakımdan kusurluluk, işlediği fiille irtibatlı olarak kişi açısından bulunulan bir değerlendirme yargısıdır ve dolayısıyla, suçun bir unsurunu oluşturmaz. Başka bir deyişle, kişi işlediği fiilden dolayı kusurlu bulunmasa bile, bu fiil suç olma özelliğini muhafaza eder. Buna karşılık, kanuni tanımda aranan manevi unsur gerçekleşmediği takdirde, suç oluşturan bir haksızlığın varlığından söz edilemez. Bu itibarla, yeni TCK'ya hâkim olan suç teorisinde, suçun manevi unsuru ile kusurluluk, birbirleriyle irtibatlı ve fakat, içerik ve fonksiyonları bakımından birbirinden ayrı kavramlar olarak anlaşılmalıdır."*

[367] **Koca/Üzülmez**, Genel Hükümler, s. 144.

[368] **Koca/Üzülmez**, Genel Hükümler, s. 242; **Önder**, Ceza Hukuku Dersleri, s. 304.

[369] **Doğan**, Bilişim Suçları, s. 149; **Karagülmez**, Bilişim Suçları, s. 190; **Kurt**, Tüm Yönleriyle Bilişim Suçları, s. 175; **Taşkın**, Bilişim Suçları, s. 59; **Yılmaz**, TCK'nın 244. Maddesinde Düzenlenen Bilişim Alanındaki Suçlar, s. 89.

olarak değil genel kast kapsamında değerlendirmelidir[370]. Zira bir kere kanun koyucu kastın yanında özel bir maksat, özel bir bilme yahut özel bir saik aradığında bunu kanunda açıkça ve ayrıca zikretmiştir. Örneğin, kanun koyucu hırsızlık suçunda, failin, başkasının taşınabilir malını zilyedinin rızası olmaksızın kendisine veya başkasına yarar sağlamak maksadıyla almasını öngörmüştür. Oysa inceleme konumuz olan suçun kanuni tanımında böyle bir ifade bulunmamaktadır[371]. Ayrıca haksız çıkar elde etme suçun fiil unsurunu teşkil etmektedir. Dolayısıyla failin kastı kendisi veya başkası için yarar elde ettiği bilgisini ve elde ettiği bu yararın haksız olduğu bilgisini de kapsamalıdır ki söz konusu bu durum kastın içeriğine dahildir[372].

Sonuç olarak suçun oluşabilmesi için fail, başkasının bilişim sistemini engellediğini, bozduğunu yahut sistemdeki verileri bozduğunu, değiştirdiğini, başka bir yere gönderdiğini ve bu fiilleri işlemek suretiyle kendisi veya başkası için haksız bir çıkar elde ettiğini bilmelidir. Yani çıkarın haksız olduğuna ilişkin faildeki bilgi kastın kapsamında değerlendirilmeli bunun yanında herhangi bir amaç ya da saik aranmamalıdır.

Bu suçta amaç veya saik aranmamakla birlikte, suçun olası kastla işlenemeyeceğini düşünmekteyiz. Zira failin kendisi veya başkası için sağladığı yararın haksız olduğuna ilişkin bilgisinin kasta dahil olması, manevi unsur bakımından olası kastın oluşumunu engellemektedir[373].

3.3. Hukuka Aykırılık Unsuru

Suçun hukuka aykırılık unsuru, işlenen fiilin bütün hukuk düzeni ile çelişki ve çatışma halinde olmasını ifade eder[374]. Hukuka aykırılığın esası hususunda doktrinde farklı görüşler bulunmaktadır[375]. Bizim de benimsediğimiz görüşe göre kanun koyucu tarafından karşılığında cezai yaptırım öngörülen tipik fiil hukuka aykırılığa karine teşkil etmektedir[376]. Tipik fiilin hukuka aykırılığa karine teşkil etmesi, tipik fiilin hukuka aykırılığının mutlak

---

370 **Artuk/Gökcen/Yenidünya**, Özel Hükümler, s. 893; **Dülger**, Bilişim Suçları, s. 450; **Koca/Üzülmez**, Özel Hükümler, s. 841; **Soyaslan**, Özel Hükümler, s. 649.

371 **Artuk/Gökcen/Yenidünya**, Özel Hükümler, s. 893.

372 **Koca/Üzülmez**, Özel Hükümler, s. 841.

373 **Koca/Üzülmez**, Özel Hükümler, s. 841.

374 **Alacakaptan**, Suçun Unsurları, s. 61; **Koca/Üzülmez**, Genel Hükümler, s. 255.

375 Bu görüşler için bkz. **Koca/Üzülmez**, Genel Hükümler, s. 255, 256.

376 **Centel/Zafer/Çakmut**, Türk Ceza Hukukuna Giriş, s. 285; **Koca/Üzülmez**, Özel Hükümler, s. 256.

olmadığını gösterir. Dolayısıyla bir fiil tipe uygun olmakla birlikte, bir hukuka uygunluk nedeninin varlığı durumunda fiilin hukuka aykırılığı ortadan kalkacaktır[377]. Esasen bu durum fiilin tüm hukuk düzenine aykırılık teşkil etmesi gerektiği mantıki çıkarımından kaynaklanmaktadır. Hukuk düzeninin bir kısmında icrasına cevaz verilen fiilin bir kısmında cevaz verilmemesi hukuk düzenindeki çelişki ve çatışmayı ifade eder. Hukuk düzeni bir bütün olduğuna göre bir hukuk dalında hukuka uygun olarak nitelendirilen fiil başka bir hukuk dalında hukuka aykırı olarak nitelendirilemez[378].

Yukarıda ifade ettiğimiz gibi tipik fiil, hukuka aykırılığa karine teşkil eder. Dolayısıyla suçun unsurlarında, öncelikle tipik fiilin gerçekleştirilip gerçekleştirilmediği ortaya konulmalı ardından bu fiili hukuka uygun hale getiren bir nedeninin bulunup bulunmadığı incelenmelidir. Ancak kanun koyucunun kimi suçlarda hukuka aykırılığa kanuni tanımda yer verdiği görülmektedir[379]. Örneğin, haberleşmenin engellenmesi (m.124/1) veya kişisel verilerin kaydedilmesi (m. 135) suçunda kanun koyucu suçun kanuni tanımında *"hukuka aykırı olarak"* ifadesini kullanmıştır. Böyle bir durumun suçun unsurlarının incelenmesinde ne gibi bir etkisi olduğunun ortaya konulması gerekmektedir. Zira inceleme konumuz olan suçun (m. 244/4) kanuni tanımında da *"haksız bir çıkar sağlanması"* ifadesi kullanılmıştır.

Suçun kanuni tanımında hukuka aykırılığa ilişkin bir ifadeye yer verilmesi durumunda suçun oluşumu için failin kastının, hukuka aykırılığı da kapsaması gerekmektedir[380]. Ancak doktrinde de ifade edildiği üzere söz konusu bu durum, ancak kanun koyucunun hukuka aykırılığı suçun geneli için değil, belli bir unsuru için aradığı durumlarda geçerlidir[381]. Örneğin, kişisel verileri hukuka aykırı kaydetme suçunda kanun koyucu, hukuka aykırılığı suçun belli bir unsuru için değil tamamı için aramıştır. Böyle bir durumda kanun koyucunun amacı hükmün uygulayıcısı hâkimin olayda bir hukuka uygunluk nedeninin var olabileceği hususunda dikkatini çekmektedir. Hukuka aykırılığın suçun geneli için arandığı suçlarda, kastın hukuka aykırılığı kapsaması gerekmez "*fakat kusur alanına ait olan haksızlık bilinci bakımından tipteki bu ifade bir bağlantı noktası oluşturur."*[382]

---

[377] **Alacakaptan**, Suçun Unsurları, s. 65; **Artuk/Gökcen/Yenidünya**, Genel Hükümler, s. 379.

[378] **Centel/Zafer/Çakmut**, Türk Ceza Hukukuna Giriş, s. 287.

[379] **Dönmezer/Erman**, Nazari ve Tatbiki Ceza Hukuku - 2, s. 19.

[380] **Dönmezer/Erman**, Nazari ve Tatbiki Ceza Hukuku - 2, s. 21.

[381] **Önder, Ayhan**; Ceza Hukuku Dersleri, İstanbul 1992, s. 216.

[382] **Koca/Üzülmez**, Genel Hükümler, s. 259.

İnceleme konumuz suç açısından bu durumu değerlendirdiğimizde kanuni tanımda *"haksız çıkar sağlanması"* ifadesinin sonucu olarak, kanun koyucunun suçun bir unsurunun, yani çıkar sağlama unsurunun haksız yani hukuka aykırı olması gerektiğini ifade etmiş olduğunu söyleyebiliriz[383]. Öyleyse inceleme konumuz suç için failin sağladığı çıkarın hukuka aykırı olduğu kastıyla hareket etmesi gerektiğini, dolayısıyla failin olası kastla hareket ettiği durumlarda suçun oluşmayacağını ifade edebiliriz[384].

Bilişim sistemi aracılığıyla haksız yarar sağlama suçu bakımından hukuka uygunluk nedeni olarak akla gelebilecek ilk neden mağdurun rızasıdır. Mağdurun rızası bakımından dikkat edilmesi gereken husus, bilişim sisteminin yahut verilerin malikinin rızasının her somut olay bakımından hukuka uygunluk nedeni oluşturmayacağıdır[385].

Bu suçun konusunu haksız şekilde elde edilen çıkar oluşturmaktadır. Dolayısıyla mağdur da kendisinin malvarlığından elde edilen çıkarın sahibidir. Yani suçun mağduru, bilişim sistemi veya verilere müdahale sonucu malvarlığı itibariyle zarar uğrayan gerçek kişidir[386]. Şu hâlde fiilin hukuka uygun olması için rıza gösterecek kimse de fiil sonucu malvarlığı itibariyle zarara uğrayacak kişi olmalıdır. Gerçekleştirilecek fiil sonucu, sistem ya da veri maliki kimsenin malvarlığı itibariyle zarara uğramayacak kişi olması durumunda, bu kimselerden alınan rıza, fiili hukuka uygun hale getirmeyecektir. Sonuç olarak her somut olayda rızayı verenin bu rızayı vermeye yetkili olup olmadığı araştırılmalıdır[387]. Örneğin bir bankanın, müşterilerinin hesap bilgilerini tuttuğu bilişim sistemine erişme ve bu verileri bir başka yere göndererek yarar elde etme hususunda verdiği rıza, fiili hukuka uygun hale getirmeyecektir. Zira bu fiil sonucu malvarlığı itibariyle zarara uğrayacak kimseler bankanın müşterileri olacağından, rıza verme yetkisi de bunlara ait olacaktır.

TCK m. 244/1 ve 2 açısından söz konusu olabilecek meşru savunma ve kanun hükmünün icrasının hukuka uygunluk nedenlerinin 4. fıkra bakımından da geçerli olup olamayacağını ortaya koymak gerekmektedir. Örneğin; failin, kendi bilişim sistemi veya verilerine uzaktan erişimle saldırı olması halinde karşı tarafın bilişim sistemi veya verilerine bu saldırıyla

---

383 **Koca/Üzülmez**, Genel Hükümler, s. 259.

384 **Özgenç**, Genel Hükümler, s. 294: *"Bu suretle, kanun koyucu, failin, işlediği fiilin, hukuka aykırı olduğunu bilmesini yani, işlediği fiilin hukuka aykırı olduğu hususunda doğrudan kastla hareket etmesini aramıştır."*

385 **Dülger**, Bilişim Suçları, s. 310; **Taşkın**, Bilişim Suçları, s. 59.

386 **Hafızoğulları/Özen**, Topluma Karşı Suçlar, s. 457; **Koca/Üzülmez**, Özel Hükümler, s. 839; **Soyaslan**, Özel Hükümler, s. 652; **Tezcan/Erdem/Önok**, Ceza Özel, s. 773.

387 **Doğan**, Bilişim Suçları, s. 150; **Taşkın**, Bilişim Suçları, s. 59.

orantılı biçimde karşı gerçekleştirdiği müdahale fiilleri, meşru savunma kapsamında hukuka uygun olacaktır. Ancak savunma fiili bu sınırı aşarak haksız bir yarar sağlamayı da kapsadığında artık meşru savunmadan bahsedilemeyecektir. Aynı şekilde örneğin, CMK m. 134 bağlamında bilgisayar ve bilgisayar kütüklerinde arama maksadıyla sistem sahibinin sisteminin erişilmez kılınması durumunda da fiil hukuka uygun olacaktır[388]. Ancak bu durumda yarar sağlama CMK m. 134'e dahil olmadığından fail bu suretle haksız yarar elde ederse TCK m. 244/4 kapsamında sorumlu olacaktır.

Özetle, söz konusu hukuka uygunluk nedenlerinin bilişim sistemi aracılığıyla haksız yarar sağlama suçu bakımından geçerli olamayacağı kanaatindeyiz. Zira meşru savunma bakımından failin, kendi sistemine saldıran karşı tarafın sistemini etkisiz kılmak amacıyla gerçekleştirdiği fiil ile maddi bir çıkar sağlaması halinde, savunmanın saldırıyla orantılı olmadığını ifade edebiliriz. TCK m. 244'ün 1. ve 2. fıkralarındaki fiiller ile defedilebilecek saldırı bakımından failin bu fiillerle bir de kendisi veya başkası için bir çıkar sağlaması durumunda bu çıkar haksız olacak ve dolayısıyla fiil hukuka uygun hale gelmeyecektir. Ancak failin gerçekleştirdiği savunma fiili ile aslında amaçlamadığı bir maddi çıkar kendiliğinden gerçekleşirse de failin kastı çıkar sağlamak olmadığı için suç oluşmayacaktır. Fail bu kapsamda olası kastla hareket etmiş olsa dahi suç oluşmayacaktır, zira failin elde edeceği çıkarın haksız olduğuna dair bir bilince sahip olması gerekmektedir ki, olası kastla harekette bu bilince sahip olunamayacağı açıktır. Ayrıca TCK m. 27/1'de hukuka uygunluk nedenlerinde sınırın kast olmaksızın aşılması durumunda fiil, taksirle işlendiğinde cezalandırılıyorsa failin bundan sorumlu olacağı düzenlenmiştir. Şu hâlde TCK m. 244/4'ün taksirli hali kanunda düzenlenmediğinden failin sınırın aşılmasında kasten hareket etmediği durumda bir sorumluluğu olmayacağı ifade edilebilir.

Aynı şekilde kanun hükmünün icrasında hukuka uygunluk nedeni bakımından da, kişilerin bilişim sistemlerine veya verilerine müdahale ile yarar elde edilmesine cevaz veren bir kanun hükmünün bulunmadığını düşünmekteyiz. Ancak yarar sağlama neticesine varmayacak müdahale fiillerinin, kanun hükmünün icrası kapsamında, hukuka uygun olacağı kanaatindeyiz.

[388] **Taşkın**, Bilişim Suçları, s. 51: Aynı şekilde, 5651 Sayılı Kanun'un 8.maddesi gereğince, sözgelimi çocukların cinsel istismarına yönelik yayın yapan internet sayfasına erişimin engellenmesi de kanun hükmünün icrası kapsamında bir hukuka uygunluk nedenidir.

4. SUÇUN NİTELİKLİ HALLERİ

Bilişim sistemleri aracılığıyla haksız yarar sağlama suçuna ilişkin herhangi bir nitelikli hal öngörülmemiştir. TCK m. 244/3'te düzenlenen nitelikli halin 4. fıkraya uygulanması mümkün değildir. Zira eğer kanun koyucu bu ağırlaştırıcı nedenin 4. fıkraya da uygulanmasını dileseydi, düzenlemeyi 4. fıkradan sonra gelmek üzere yapardı. Ayrıca 3. fıkranın *"Bu fiillerin ..."* ifadesi ile başlaması ağırlaştırıcı nedenin 1. ve 2. fıkradaki fiiller için öngörüldüğünü göstermektedir. Dolayısıyla ilk iki fıkrada gösterilen fiillerin bir banka veya kredi kurumuna[389] yahut bir kamu kurumu veya kamu kuruluşuna ait bilişim sistemlerine ya da bu sistemlerdeki verilere karşı gerçekleştirilmesi suretiyle haksız çıkar sağlanması durumunda cezada artırım yapılamayacaktır. Ancak bu durumda hakim, bir banka bilişim sistemi ya da bu sistemdeki veriler üzerinde suçun işlenmesini dikkate alarak cezanın belirlenmesinde (TCK m. 61) alt sınırdan uzaklaşabilecektir.

Ayrıca yukarıda detaylıca açıkladığımız üzere 4. fıkrayı, 1. ve 2. fıkradaki suçların ağırlaştırıcı nedeni olarak kabul eden görüşe katılmamaktayız[390].

Hırsızlık ve dolandırıcılık suçlarının bilişim sistemlerini araç olarak kullanmak suretiyle işlenmesi mümkündür. Hatta kanun koyucu bu durumu bir ağırlaştırıcı neden olarak görmüştür. Malvarlığına karşı suçlar bölümünde düzenlenen bu suçlarla ilgili olarak kanun koyucu suçu şikâyete tabi kılan ve cezayı azaltan nedenlere ayrı ayrı yer vermiştir. Buna göre bu suçlar, *"bir hukuki ilişkiye dayanan alacağı tahsil amacıyla",* gerçekleştirilmişse faile verilecek ceza hafifletilmekte ve suç şikâyete tabi olmaktadır. Doktrinde söz konusu bu hükümlerden hareket eden görüşe göre[391], bilişim sistemi ile haksız çıkar sağlama suçu bakımından da benzer bir hafifletici nedenin düzenlenmesi gerektiğini savunmaktadırlar[392].

---

[389] 5411 sayılı Bankacılık Kanunu m. 157: *"Bu Kanuna tâbi kuruluşlar, 5237 sayılı Türk Ceza Kanununun 244 üncü maddesinde tanımlanan sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu açısından banka veya kredi kurumu olarak kabul edilir."*

[390] Aksi yönde görüşler için bkz. **Avşar/Öngören**, Bilişim Hukuku, s. 139; **Kurt**, Tüm Yönleriyle Bilişim Suçları, s. 161; **Özbek/Doğan/Bacaksız/Tepe**, Özel Hükümler, s. 921; **Taşdemir**, Bilişim, Banka veya Kredi Kartlarının Kötüye Kullanılması ve Dolandırıcılık Suçları, s. 276.; **Pallı**, Bilişim Suçları, s. 167.

[391] **Kurt**, Tüm Yönleriyle Bilişim Suçları, s. 174, 175.

[392] **Taşkın**, Bilişim Suçları, s. 51: *"Bir görüş, bilişim suçlarında da hırsızlıkta, dolandırıcılıkta ve yağmada olduğu gibi, kişinin hukuki alacağını tahsil etmek amacıyla bilişim suçu işlemesinin indirim nedeni sayılması gerektiğinden bahsetmekte ve sattığı bir yazılımın parasını vermeyen müşterisinin programını ağ üzerinden sisteme girerek silen satıcıya tam ceza verilmesini çelişki olarak değerlendirmekte ve TCK'ya bu durumu indirim nedeni sayan bir düzenleme konmasını savunmaktadır. Buna benzer bir yaklaşım da yazılım geliştiricisi olan bir kişinin, bu yazılımını lisanssız kullanan kişinin sistemine "mantık bombası" göndererek; o kişinin sistemindeki lisanssız yazılımı yok etmesi ama sisteme zarar vermemesi örneğinde*

Ancak söz konusu böyle bir düzenleme kanunda bulunmadığından fiilin, bir hukuki ilişkiye dayanan alacağı tahsil amacıyla gerçekleştirilmesi durumunda cezada indirime gidilemeyecektir[393].

5. TEŞEBBÜS

Failin, suçun icrasına elverişli hareketlerle başlaması ancak elinde olmayan sebeplerle suçu tamamlayamaması durumunda teşebbüs halinde kalmış suç söz konusudur[394]. Suçun tamamlanmasından maksat, sırf hareket suçlarında icra hareketlerinin tamamlanması, kanuni tanımda ayrıca neticeye yer veren suçlarda ise neticenin gerçekleşmesidir[395].

Kural olarak fail suçun kanuni tanımındaki unsurları gerçekleştirdiğinde yani suç tamamlandığında cezai yaptırıma tabi tutulabilir. Ancak TCK m. 35'de, suç tamamlanmasa bile icra hareketlerine başlanmış ise faile icrasına başlanan suçun cezasının indirilerek verildiği görülmektedir. Dolayısıyla esasen teşebbüs hükümleri sorumluluğu genişletici bir özelliğe sahiptir. Zira fail, aslında kanunda suç olarak tanımlanan fiili gerçekleştirmemiş olsa da cezalandırılmaktadır.[396]

Bilişim sistemi ile haksız yarar sağlama suçunda, kanundaki düzenleme itibariyle teşebbüs hususu özellik arz etmektedir. Öncelikle bu suçun, failin TCK m. 244/1 ve 2'deki neticeleri gerçekleştirmek suretiyle kendisi veya başkası için haksız bir çıkar sağlaması ile tamamlanacağını ifade etmek gerekir. Bu anlamda söz konusu suç neticeli bir suçtur[397]. Dolayısıyla fail 1. ve 2. fıkradaki neticeleri gerçekleştirmesine karşın kendisi veya başkası için yarar elde edememişse – yani neticeyi gerçekleştirememişse – fiil, TCK m. 244/4'e teşebbüs aşamasında kalmış olacaktır. Ancak dikkat edilecek olursa söz konusu durumda failin gerçekleştirdiği hareket 1. ve 2. fıkra bakımından tipik bir harekettir yani fail aslında

---

somutlaştırılmaktadır ki buna benzer bir olay İrlanda mahkemeleri tarafından hukuka uygunluk nedeni sayılmıştır."

393 TCK m. 61/10: *"Kanunda açıkça yazılmış olmadıkça cezalar ne artırılabilir, ne eksiltilebilir, ne de değiştirilebilir."*

394 **Akbulut**, Genel Hükümler, s. 548; **Artuk/Gökcen/Yenidünya**, Genel Hükümler, s. 586; **Koca/Üzülmez**, Genel Hükümler, s. 398; **Özgenç**, Genel Hükümler, s. 461.

395 **Artuk/Gökcen/Yenidünya**, Genel Hükümler, s. 252.

396 **Hafızoğulları/Özen**, Genel Hükümler, s. 308.

397 **Dülger**, Bilişim Suçları, s. 448.

bu durumda 1. ve 2. fıkradaki suçları tamamlamıştır. Öyleyse failin sorumluluğu bu ilk iki fıkradan mı yoksa 4. fıkraya teşebbüsten mi olacaktır?

Failin sorumluluğunu belirleyebilmek için manevi unsura başvurulması gerekmekte, failin hangi suçu işlemeyi kastettiği ortaya konulmalıdır[398]. Eğer fail, 4. fıkradaki suçu işlemeyi yani söz konusu fiiller ile kendisi veya başkası için haksız çıkar elde etmeyi kastetmiş ancak bu çıkarı elde edememişse failin sorumluluğu 4. fıkraya teşebbüsten olacaktır[399]. Buna karşılık failin çıkar elde etmeye yönelik kastı yok ve 1. ve 2. fıkralardaki fiilleri işlemek suretiyle çıkar da elde etmemişse bu halde failin sorumluluğu 244/1 veya 2'den dolayı olacaktır.

Her ne kadar TCK m. 244/4 bakımından suçun oluşumu veya teşebbüs hükümlerinin uygulanabilmesi için failin kastının haksız çıkar sağlamaya yönelik olması gerektiğini ifade etsek de manevi unsur açısından bu durumda özel bir maksadın varlığının gerekli olmadığı, haksız çıkar sağlama fiilinin suçun maddi unsurunda yer aldığı için nedeniyle bu hususun kast içerisinde değerlendirilmesi gerektiği görüşündeyiz.[400]

Ayrıca belirtmek gerekir ki failin bilişim sistemine girmesi, ancak sisteme veya sistemdeki verilere zarar vermeksizin sistemden çıkması halinde, TCK m. 244/4 anlamında suçun icrasına başlanmadığı için suça teşebbüs de gerçekleşmemiş olacaktır.

Nitekim Yargıtay 12. Ceza Dairesi 2016 tarihli kararında failin, mağdurun sosyal medya hesabına girmesi ancak burada bir değişiklik yapmaması durumuna ilişkin olarak fiilin, TCK m. 243 uyarınca bilişim sistemine girme suçunu oluşturacağına hükmetmiştir. Yüksek mahkemenin kararına göre, *"Sanığın, katılan ile internette tanıştığı ve bir süre telefonda ve msn üzerinden görüntülü görüşerek arkadaşlık yürüttüğü, sanığın teklifi üzerine katılanın, kendisi, kızı ve sanık ile birlikte bir otelde yaklaşık 1 hafta süreyle tatil yaptıkları, arkadaşlıklarının bitmesi üzerine bilahare sanığın, katılanın kullandığı elektronik posta adresine rızası dışında birçok kez girdiği olayda, sanığın, bu şekildeki eyleminin TCK'nın 243/1. maddesine uyan bilişim sistemine girme suçunu oluşturduğu ve mahkemenin hükmün gerekçesinde de eylem bu şekilde kabul edildiği halde, sanık hakkında bilişim sistemine*

[398] **Hafızoğulları/Özen**, Genel Hükümler, s. 309: *"Teşebbüsün olması için, ortada, failin '…işlemeyi kastettiği bir suç' mevcut olmalıdır."*

[399] **Koca/Üzülmez**, Özel Hükümler, s. 841.

[400] **Koca/Üzülmez**, Özel Hükümler, s. 841.

girme suçu yerine, TCK'nın 244. maddesinde düzenlenen sistemi engelleme, bozma, verileri yok etme veya değiştirme suçundan hüküm kurulmak suretiyle sanık hakkında fazla ceza tayini hatalıdır."[401]

6. İŞTİRAK

Kanunda tek bir faille işlenebilen bir suçu, birden çok failin, aralarındaki anlaşma ve iş birliği sonucunda fiilin oluşumuna illi değeri haiz katkıda bulunarak gerçekleştirmesi halinde suça iştirak söz konusu olmaktadır[402].

5237 sayılı TCK'da, fiili hakimiyet teorisi[403] çerçevesinde belirlenecek iştirak şekilleri; faillik (m. 37), azmettirme (m.38) ve yardım etme (m. 39) olarak düzenlenmiştir[404].

Buna göre, bilişim sistemi aracılığıyla haksız yarar sağlama suçuna iştirakin her türüyle katılmak mümkündür. Örneğin, bu suçun işlenmesi bakımından, faile cihaz, bilgisayar programı, şifre veya sair güvenlik kodunun sağlanması durumunda, bunu sağlayan kimse bu suçta yardım eden sıfatını haiz olabilecektir. Ancak faile sağlanan cihaz, bilgisayar programı, şifre veya sair güvenlik kodu bu suçun işlenebilmesi bakımından zaruret arz ediyorsa[405] bunları sağlayan kimsenin bu defa müşterek fail olması gündeme gelecektir. Ayrıca bu örnekte yardım etme iştirak şekli ile ilgili olarak dikkat edilmesi gereken husus; sağlanan cihaz, bilgisayar programı, şifre veya sair güvenlik kodunun TCK'nın *"bilişim alanında suçlar"* bölümünde düzenlenen suçlar ya da bilişim sistemlerinin araç olarak

---

401 *Y 12. CD, E. 2015/15933, K. 2016/277, T. 13.1.2016*. (kazanci.com – s.e.t: 15.05.2017.)

402 **Artuk/Gökcen/Yenidünya**, Genel Hükümler, s. 630; **İçel**, Genel Hükümler, s. 531; **Özgenç**, **İzzet**; Suça İştirakin Hukuki Esası ve Faillik, İstanbul 1996, s. 19.

403 **Çelen**, **Ömer**; Bir İştirak Şekli Olarak Yardım Etme (Asli Fail Yardım Eden Ayrımı), Yayımlanmamış Doktora Tezi, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Konya 2015, s. 61, 62: *"Buna göre, suçun gerçekleştirilmesine katılanlardan, kanuni tanımda yer alan fiil üzerinde hâkimiyet kuran kişiler, 'fail' olarak sorumlu olurlar. Faillik, TCK'nın 37. maddesi ile düzenlenmiştir. Maddenin ilk fıkrasında 'Suçun kanuni tanımında yer alan fiili birlikte gerçekleştiren kişilerden her birinin fail olarak' sorumlu olacağı belirtilmiştir. Buna göre, suçun kanuni tanımında yer alan fiilin, bizzat ve tek bir kişi tarafından gerçekleştirilmesi halinde kişi işlenen suçta 'tek başına (müstakil) fail' olarak sorumlu olacaktır. Fail kanuni tanımda yer alan fiili tek başına gerçekleştirebileceği gibi başkalarıyla birlikte de gerçekleştirebilir. Kanuni tanımda unsurları gösterilen fiili birden fazla kişinin gerçekleştirmesi halinde ise bu kişilerin her biri 'müşterek fail' olarak sorumlu tutulacaktır. Maddenin ikinci fıkrası ile 'suçun işlenmesinde bir başkasını araç olarak kullanan kişinin fail olarak sorumlu tutulacağı' belirtilerek dolaylı faillik hali düzenlenmiştir."*

404 **Çelen**, Bir İştirak Şekli Olarak Yardım Etme, s. 61.

405 **Özgenç**, Genel Hükümler, s. 502, 503: *"*Müşterek hâkimiyetin kurulup kurulmadığının tayininde suç ortaklarının suçun icrasındaki rol dağılımlar ve suçun işlenişine katkının arz ettiği önem, zaruret, göz önünde bulundurulacaktır.*"*

kullanılması suretiyle işlenebilen diğer suçların işlenmesi için *"yapılmamış"* veya *"oluşturulmamış"* olması gerektiğidir. Zira aksi durumda, failliğin şerikliğe asliliği kuralı gereğince[406], yasak cihaz veya programları başkasına verme suçuna (TCK m. 245/A) faillikten sorumluluk gündeme gelecektir. Ancak bu unsurların sağlanması TCK m. 244/4'e müşterek faillik arz ediyorsa bu defa fail, hem TCK m. 245/A'dan hem TCK m. 244/4'ten sorumlu olacaktır.

7. İÇTİMA

Suça iştirakte, birden fazla failin bir suçta birleşmesi söz konusu iken suçların içtimaında, suçların bir failde toplanması söz konusudur[407]. Ceza hukukunun temel ilkelerinden biri olan *"kaç tane fiil varsa o kadar suç, kaç tane suç varsa o kadar ceza vardır"* ilkesi uyarınca ceza hukukunda cezaların içtimaı yani gerçek içtima kural olup, buna göre işlenen her bir suçtan dolayı ayrı cezaya hükmedilir ve her bir ceza bağımsızlığını korur[408]. Dolayısıyla suçların içtimaına ilişkin düzenlemeler, fail lehine getirilmiş istisnalardır[409].

Suçların içtimaı şekillerinden biri olan bileşik suçta, kanunda bağımsız bir suç olarak tanımlanan fiil, bir başka suçun temel veya nitelikli halinin unsurunu oluşturmakta ve fail, unsur olan bu suçtan dolayı ayrıca sorumlu olmamaktadır[410]. Nitekim TCK m. 42'de bu tür suçlarda içtima hükümlerinin uygulanmayacağı düzenlenmiştir[411]. Bu çerçevede fail esasen birden fazla suç icra etmiş olsa da kanundan dolayı bu suçlar, hukuki anlamda tek fiil ve tek suç olarak kabul edilmekte ve faile tek bir ceza verilmektedir[412].

Bilişim sistemi aracılığıyla haksız yarar sağlama suçu, bir bileşik suçtur. TCK m. 244/4'te yer alan *"yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle haksız bir çıkar sağlanmasının"* ifadesiyle kanun koyucu, aynı maddenin 1. ve 2. fıkrasındaki bilişim sistemini engelleme, bozma ve verileri yok etme veya değiştirme suçlarını, 4. fıkradaki

---

406 **Önder**, Ceza Hukuku Dersleri, s. 455.

407 **Hakeri**, Genel Hükümler, s. 595.

408 **Artuk/Gökcen/Yenidünya**, Genel Hükümler, s. 688; **Göktürk**, **Neslihan**; Fikri İçtima, Ankara 2013, s. 6; **Hakeri**, Genel Hükümler, s. 595.

409 **Hakeri**, Genel Hükümler, s. 595.

410 **Özgenç**, Genel Hükümler, s. 567, 568.

411 TCK m. 42: *"Biri diğerinin unsurunu veya ağırlaştırıcı nedenini oluşturması dolayısıyla tek fiil sayılan suça bileşik suç denir. Bu tür suçlarda içtima hükümleri uygulanmaz."*

412 **Göktürk**, Fikri İçtima, s. 132. Fiil tekliği – fiil çokluğu ayrımı hakkında detaylı bilgi için bkz. **Koca/Üzülmez**, Genel Hükümler, s. 490–497.

suçun unsuru olarak belirlemiştir[413]. Dolayısıyla failin, TCK m. 244/1 ve 2'deki fiilleri işlemek suretiyle kendisi veya başkası yararına haksız bir çıkar sağlaması halinde sorumluluğu, yalnızca 4. fıkradan olacak, ayrıca 1. ve 2. fıkra bakımından cezaya hükmedilemeyecektir[414].

Suçların içtimaı şekillerinden bir diğeri ise zincirleme suçtur. Zincirleme suçta bileşik suçtan farklı olarak birbirinden farklı suçların birden fazla işlenmesi değil, aynı suçun birden fazla işlenmesi söz konusudur[415]. Ancak TCK m. 43/1'e göre failin birden fazla işlediği aynı suç bakımından zincirleme suç hükümlerinden yararlanabilmesi için bu suçları aynı kişiye karşı ve aynı suç işleme kararı kapsamında farklı zamanlarda işlemesi gerekmektedir. Bu şartların gerçekleşmesi halinde kanuna göre faile dörtte birinden dörtte üçüne kadar artırılarak tek bir ceza verilecektir.

Bilişim sistemi aracılığıyla haksız yarar sağlama suçu için zincirleme suç hükümlerinin uygulanması mümkündür[416]. Örneğin, fail aynı kişiye ait bir bilişim sistemindeki verileri aynı suç işleme iradesiyle farklı zamanlarda birden çok bir bilişim sistemine aktararak kendisi veya başkası yararına haksız çıkar elde edebilir. Bu durumda failin sorumluluğu, TCK m. 43 uyarınca, TCK m. 244/4'ün cezasının dörtte birinden dörtte üçüne kadar artırılmış şeklinden olacaktır.

Suçların içtimaı şekillerinden sonuncusu, fikri içtimadır[417]. *"Fikri içtima, tek fiilde birden fazla suçun birleşmesi; tek ve aynı fiil ile aynı suçun birden fazla (aynı nev'iden fikri içtima) yahut birden fazla farklı suçun (farklı nev'iden fikri içtima) işlenmesidir."*[418]. Dolayısıyla fikri içtimada temel husus, tek fiil ile birden fazla suçun işlenmesidir[419]. Tanımdan da anlaşılacağı üzere tek fiil ile aynı suçun birden fazla işlenmesi durumunda aynı neviden fikri içtima hali söz konusu olurken, tek fiille birden fazla farklı suçun işlenmesi durumunda ise farklı neviden fikri içtima hali söz konusu olmaktadır. TCK m. 43/2'de aynı neviden fikri

---

413 **Erdoğan**, TCK'da Bilişim Suçları, s. 262; **Koca/Üzülmez**, Özel Hükümler, s. 834.

414 **Artuk/Gökcen/Yenidünya**, Özel Hükümler, s. 894.

415 **Özgenç**, Genel Hükümler, s. 572.

416 **Artuk/Gökcen/Yenidünya**, Özel Hükümler, s. 894.

417 Fikri içtimaın hukuki niteliği hakkında detaylı bilgi için bkz. **Göktürk**, Fikri İçtima, s. 61–63; **Koca**, Fikri İçtima, s. 199.

418 **Göktürk**, Fikri İçtima, s. 59.

419 Fiil tekliği – fiil çokluğu ayrımı hakkında detaylı bilgi için bkz. **Koca/Üzülmez**, Genel Hükümler, s. 490 – 497. Kanaatimizce fiil tekliğinden anlaşılması gereken, hareketin tekliğidir.

içtima hali, aynı suçun birden fazla kişiye karşı tek bir fiille işlenmesi şeklinde düzenlenmiştir. TCK m. 43/2, bir fikri içtima hali olmasına rağmen kanunun zincirleme suç başlıklı 43. maddesinde düzenlenmesi doktrinde eleştirilmektedir[420].

Bilişim sistemi aracılığıyla haksız yarar sağlama suçunun, tek bir hareketle birden fazla kişiye karşı işlenmesi mümkündür. Bu hususa ilişkin olarak tipik bir örnek olarak *"wipe"* işlemini gösterebiliriz. Yukarıda da açıklandığı üzere *"wipe"* işlemi TCK m. 244/2 anlamında verileri yok etme neticesini oluşturabilecek nitelikte bir fiildir. Fail bu işlemle veri saklama kapasitesine sahip bir diskteki tüm veriler üzerine yeni veri yazmak suretiyle mevcut verileri geri döndürülemez biçimde silmektedir. İşte bu duruma ilişkin olarak fail, bir diski *"wipe"* işlemine tabi tuttuğunda eğer diskteki veriler birden fazla kişiye aitse ve fail bu işlem sonucu kendisi veya başkası yararına haksız çıkar elde ediyorsa, aynı neviden fikri içtima hali söz konusu olacak ve faile TCK m. 244/4'teki ceza dörtte birinden dörtte üçüne kadar artırılarak verilecektir.

Farklı neviden fikri içtimada ise tek bir fiil ile birden fazla farklı suçun işlenmesi söz konusudur[421]. TCK m. 44'te işlenen tek bir fiille birden fazla farklı suçun oluşması durumunda, failin en ağır cezayı gerektiren suçtan dolayı sorumlu olacağı hükme bağlanmıştır. Farklı neviden fikri içtima hükmünün uygulanmasında dikkat edilmesi gereken en önemli nokta tek fiille işlenen birden fazla farklı suçun, görünüşte içtima ilişkisi içerisinde olmamasıdır[422]. Görünüşte içtima halinde suçların çokluğu sadece görünüşte olup, fiile uygulanacak olan esasen bu normlardan sadece biridir[423]. Görünüşte içtima halinde de fail esasen tek fiil ile birden fazla suç işlemektedir ancak işlenen bu suçlar arasında özel norm – genel norm, asli norm – tali norm ya da tüketen norm – tüketilen norm ilişkisinin bulunması aslında faile uygulanabilecek tek bir normun olduğunu göstermektedir[424]. Örneğin, asli norm – tali norm ikilisinde failin işlediği fiilin iki norma da aykırılık teşkil etmesi durumunda asli

---

[420] **Özgenç**, Genel Hükümler, s. 596: *"Zincirleme suç ile aynı neviden fikri içtima arasındaki tek müştereklik, cezada yapılabilecek artırıma ilişkin oranların aynı olmasından ibarettir. Aslında birbirlerinden farklı durumlara ilişkin iki ayrı içtima hükmünün ayrı maddelerde düzenlenmesi daha yerinde olurdu. Ancak, Yeni TCK'ya ilişkin olarak TBMM Adalet Komisyonundaki çalışmalarımız sırasında bunu izahta karşılaştığımız güçlük nedeniyle, her iki içtima durumunu aynı madde altında düzenlemek mecburiyetinde kalmış bulunmaktayız."*

[421] **Göktürk**, Fikri İçtima, s. 180.

[422] **Göktürk**, Fikri İçtima, s. 74.

[423] **İçel ve diğerleri**, Suç Teorisi, s. 457.

[424] **Hakeri**, Genel Hükümler, s. 639.

normun önceliği ilkesi gereği failin sorumluluğu bu norm üzerinden belirlenecektir[425]. Asli norm ve tali norm fikri içtima ilişkisine girerek failin daha ağır cezayı gerektiren suçtan dolayı sorumluluğuna neden olmayacaktır[426].

İnceleme konumuz olan bilişim sistemi aracılığıyla haksız yarar sağlama suçu kanunda tali norm olarak düzenlenmiştir[427]. Zira TCK m. 244/4'te failin bu suçtan sorumlu olabilmesi için işlenen fiille *"haksız bir çıkar sağlamasının başka bir suç oluşturmaması"* hükme bağlanmıştır. Dolayısıyla bilişim sistemi aracılığıyla haksız çıkar sağlanması ile ilgili başka bir suçun işlenmesi durumda bu suçlardan hangisinin cezasının daha ağır olduğunda bakılmaksızın failin, işlenen diğer suçtan sorumlu olacağını ifade edebiliriz[428].

TCK m. 244/4'ün tali norm olarak düzenlenmesi bu suç ile başka suçların farklı neviden fikri içtima ilişkisine girmeyeceği anlamına gelmez. Buna göre haksız bir çıkar sağlamanın suçun kanuni tanımında düzenlenmediği suçlar ile TCK m. 244/4'ün, farklı neviden fikri içtima ilişkisine girmesi olanaklıdır. Zira TCK m. 244/4'te bu hükmün uygulanabilmesi için *"haksız çıkar sağlama"*nın başka bir suça vücut vermemesi aranmıştır.

TCK m. 244/4'ün gerekçesinde *"ancak, bu fıkra hükmüne istinaden cezaya hükmedilebilmesi için, fiilin daha ağır cezayı gerektiren başka bir suç oluşturmaması gerekir."* ifadesi kullanılmıştır. Bu anlamda gerekçe ile hükmün çeliştiği görülmektedir[429]. Hükümde, TCK m. 244/4'ten sorumluluk için haksız çıkar sağlamanın daha ağır bir cezayı gerektiren başka bir suç oluşturmaması değil, daha ağır veya hafif herhangi bir başka suç oluşturmaması öngörülmüştür. Şu hâlde gerekçenin bağlayıcı olmaması nedeniyle gerekçeye itibar

---

425 **İçel**, Genel Hükümler, s. 608; **Koca/Üzülmez**, Genel Hükümler, s. 535.

426 **İçel ve diğerleri**, Suç Teorisi, s. 457.

427 **Artuk/Gökcen/Yenidünya**, Özel Hükümler, s. 892; **Erdoğan**, TCK'da Bilişim Suçları, s. 264; **Ketizmen**, Bilişim Suçları, s. 182; **Koca**, Hukukumuzda TCK'nın 244'ncü maddesi, s. 97; **Özbek/Doğan/Bacaksız/Tepe**, Özel Hükümler, s. 955.

428 **Koca**, Hukukumuzda TCK'nın 244'ncü maddesi, s. 97.

429 **Doğan**, Bilişim Suçları, s. 143: *"Açıklanan çelişkinin giderilmesi için TCK'nın 244. maddesinin 4. fıkrasındaki 'fiilin başka bir suç oluşturmaması' ibaresinin, gerekçede geçen 'fiilin daha ağır cezayı gerektiren başka bir suç oluşturmaması' ibaresi ile değiştirilmesi gerekir. Böyle bir düzenleme hem ceza kanunumuzun genel sistematiğine hem de TCK'nın 44. maddesinde geçen 'işlediği bir fiil ile birden fazla farklı suçun oluşmasına sebebiyet veren kişi, bunlardan en ağır cezayı gerektiren suçtan dolayı' sorumlu tutulacağı hükmüne de uygun olacaktır."*

edilmemeli ve bu suçtan sorumluluk için fiilin herhangi başka bir suç oluşturmaması gerektiği kabul edilmelidir[430].

Aşağıda TCK m. 244/4'ün asli normu olabilecek nitelikteki suçlar ile bu hüküm karşılaştırmalı olarak ele alınacaktır.

7.1. Bilişim Sistemi Aracılığıyla İşlenen Dolandırıcılık Suçu Açısından

TCK m. 158/1-f'de dolandırıcılık suçunun, bilişim sistemleri yahut banka veya kredi kurumlarının araç olarak kullanılması suretiyle işlenmesini nitelikli dolandırıcılık suçu olarak hükme bağlanmıştır[431]. Dolayısıyla bilişim sistemi vasıtasıyla işlenen dolandırıcılık suçu, bilişim sistemi aracılığıyla haksız yarar elde etme suçunun asli normu olabilecek nitelikte bir suçtur. Zira dolandırıcılık suçunun oluşması için failin, hileli davranışlarla bir kimseyi aldatıp kendisi veya başkasına yarar sağlaması gerekmektedir[432]. Haksız yarar sağlama ve bilişim sistemlerinin vasıta olarak kullanılması bu iki suçun kesişim noktasıdır. Bu iki suçu birbirinden ayıran nokta ise dolandırıcılık suçundaki hileli davranışlarla bir kimseyi aldatma unsurudur.

Öyleyse bilişim sistemi vasıtasıyla bir kimse hileli davranışlarla aldatılıyorsa hem TCK m. 158/1-f'deki suçun hem de TCK m. 244/4'teki suçun oluşması muhtemeldir ancak bu halde TCK m. 244/4'ün tali norm olması nedeniyle fiile uygulanacak tek norm TCK m. 158/1-f olacaktır[433]. Bu anlamda, farklı neviden fikri içtima kuralı uyarınca hangi suçun cezasının daha ağır olduğuna bakılmayacaktır.

---

[430] **Dülger**, Bilişim Suçları, s. 453; **Karagülmez**, Bilişim Suçları, s. 245; **Tepe**, İnternet Suçluluğu, s. 297. Karşı yönde bkz. **Hafızoğulları/Özen**, Topluma Karşı Suçlar, s. 459: *"Kanun, failin davranışı, ancak 'başka bir suç oluşturmaması halinde' bu suçtan ceza verilmemesini öngörmektedir. 'Başka bir suç oluşturmaması' ibaresinde 'fiilin daha ağır cezayı gerektiren' biçiminde bir nitelendirmeye yer verilmiş değildir. Oysa, gerekçede, 'ancak, bu fıkra hükmüne istinaden cezaya hükmedilebilmesi için, fiilin daha ağır cezayı gerektiren başka bir suç oluşturmaması gerekir' denmektedir. Madem ortada 'tamamlayıcı bir hüküm' bulunmaktadır, öyleyse herhalde, doğru olanı, hükmün gerekçede belirtilen biçimde anlaşılmasıdır."*

[431] TCK m. 158/1-f'nin gerekçesi: *"Dolandırıcılık suçunun, bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle işlenmesi de, birinci fıkranın (f) bendinde bu suçun bir nitelikli unsuru olarak kabul edilmiştir. Bilişim sistemlerinin ya da birer güven kurumu olan banka veya kredi kurumlarının araç olarak kullanılması, dolandırıcılık suçunun işlenmesi açısından önemli bir kolaylık sağlamaktadır. Banka ve kredi kurumları açısından dikkat edilmesi gereken husus, bu kurumları temsilen, bu kurumlar adına hareket eden kişilerin başkalarını kolaylıkla aldatabilmeleridir."*

[432] **Özbek/Doğan/Bacaksız/Tepe**, Özel Hükümler, s. 699.

[433] **Doğan**, Bilişim Suçları, s. 152.

Doktrinde bilişim sistemi aracılığıyla dolandırıcılık suçunun işlenemeyeceğini kabul eden yazarların temel hareket noktaları, dolandırıcılık suçunun oluşabilmesi için gerçek bir kişiye yöneltilmiş hileli davranışın bulunması gerektiği ve dolayısıyla bilişim sistemine yöneltilmiş hileli davranışların dolandırıcılık suçuna vücut vermeyeceği yönündedir[434]. Ancak kanaatimizce bu suçta bilişim sistemlerinin değil, bu sistemler vasıtasıyla gerçek kişilerin aldatılması söz konusu olduğundan bu suçun TCK m. 158/1-f'de düzenlenen şekliyle işlenmesi mümkündür.

Kanaatimizce bilişim sistemleri aracılığıyla dolandırıcılığın, kanunda ağırlaştırıcı neden olarak düzenlenmesi yerinde olmuştur. Öncelikle ifade etmek gerekir ki TCK m. 244/4'ün oluşabilmesi için aynı maddenin 1. ve 2. fıkralarındaki bilişim sistemi veya sistemdeki veriye müdahale neticelerinin gerçekleştirilmesi gerekmektedir[435]. Dolayısıyla söz konusu ağırlaştırıcı neden olmasaydı, bu müdahale fiilleri olmadan bilişim sistemi aracılığıyla dolandırıcılık suçunun işlenmesi durumunda, fail dolandırıcılık suçunun temel halinden sorumlu olacaktı. Dolandırıcılık suçunun temel hali ise gerek nitelikli dolandırıcılık suçunun gerekse de bilişim sistemleri aracılığıyla haksız yarar sağlama suçunun cezasından daha az bir cezayı gerektirmektedir. Gerekçede belirtildiği üzere bilişim sistemlerinin dolandırıcılık suçunda kullanılması faile bir kolaylık sağlamaktadır; öyleyse suçun bu sistemler vasıtasıyla işlenmesinin daha ağır bir ceza ile karşılanması yerinde olmuştur[436].

---

[434] **Ünver**, **Yener**; "*Türk Ceza Kanunu'nun ve Ceza Kanunu Tasarısı'nın İnternet Açısından Değerlendirilmesi*", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, 2013, Cilt 59, Sayı 1–2, s. 98; **Özbek**, Banka veya Kredi Kartlarının, s. 1059: *"Bilindiği üzere dolandırıcılık suçunun islendiğinin kabulü için "hileli davranışların bir kimseyi aldatmış" olması gerekir. Dolayısıyla aldatmaya yönelik hareketler bir 'kişi'ye yani bir insana yöneliktir. Halbuki bu nitelikli hal bakımından söz konusu olan dolandırıcılık eyleminin bilişim sistemi üzerinde gerçekleştirilmesidir. Deyim yerinde ise bu durumda "bilgisayar ya da bilişim sistemi" dolandırılmaktadır. Nitekim bazı ülkelerde bu halin örneğin Al.CK'da olduğu gibi "bilgisayar dolandırıcılığı" olarak düzenlenmiş olması bundandır. Bu halde ise artık m.158 değil, m. 244'den söz etmek gerekir. Hukukumuzda bilgisayar dolandırıcılığı olarak da adlandırılabilecek olan düzenleme m.244'tür. Bu durumda TCK m. 244 karsısında, TCK m.142/2-e ve m.158/1-f hükümlerinin uygulama alanı bulması mümkün değildir."*

[435] **Ketizmen**, Bilişim Suçları, s. 183, 184: *"... bir sisteme ya da sistem içerisindeki veriye müdahale teşkil etmeyen fakat bir bilişim sisteminin kullanılması sonucunda yarar sağlama hallerini kapsayan fiillerin, klasik dolandırıcılık suçu kapsamında değerlendirilmesi mümkündür. Bir bankanın müşterileri hakkında bilgi güncellemesi yapacağı gerekçesiyle ve ilgili bilgilerin gönderilmesine ilişkin e-postaların gönderilmesi sonucu ya da internet üzerinden alışveriş imkânı sağlayan bir sitenin taklit edilmesi sonucunda, buradan alışveriş yapılabileceğine ilişkin hileli hareketlerle kişileri aldatıp yarar sağlama halleri klasik dolandırıcılık suçu kapsamında değerlendirilir. Bu olasılıkta da yarar yanında bir zararın oluşması dolandırıcılık suçunun teşebbüs aşamasında kalması ya da tamamlanmış olması bakımında önem arz etmektedir. Her iki ihtimalde de TCK'nın 157. maddesinin 'f' bendinde düzenlenen dolandırıcılık suçu söz konusudur."*

[436] **Erdoğan**, TCK'da Bilişim Suçları, s. 269.

Dolandırıcılık suçunda korunan hukuki değer, bir yandan kişinin malvarlığı iken diğer yandan, hileli davranışlarla mağdurun aldatılmış olması nedeniyle, irade özgürlüğüdür[437]. Yani dolandırıcılık suçunda gerçek bir kişinin iradesinin fesada uğratılması suretiyle hukuka aykırı yarar elde etme söz konusudur[438]. Dolayısıyla bilişim sistemi aracılığıyla dolandırıcılık suçunun oluşabilmesi için bir bilişim sisteminin "*aldatılması"* değil bir gerçek kişinin bilişim sistemleri vasıtasıyla aldatılması gerekmektedir[439].

Yargıtay da dolandırıcılık suçunda hileli hareketlerle gerçek bir kişinin aldatılması gerekliliğinden hareketle TCK m. 158/1-f ve TCK m. 244/4'teki suçların uygulama alanını belirlemektedir[440]. Buna göre hileli hareketlerle gerçek bir kişiyi aldatma söz konusu değil ve fakat bilişim sistemi veya sistemdeki verilere müdahale ile haksız bir yarar elde etme söz konusu ise failin sorumluluğu TCK m. 244/4'ten olacaktır. Başka bir ifadeyle failin bilişim sistemine veya sistemdeki veriye müdahalesi ile haksız yarar kendiliğinden ortaya çıkıyorsa TCK m. 244/4'ten sorumluluk söz konusu olurken; müdahale ile araya gerçek bir kişi giriyor ve bu gerçek kişinin iradesi fesada uğratılıyorsa TCK m. 158/1-f'den sorumluluk olacaktır[441].

Yargıtay Ceza Genel Kurulu, 25.05.2010 tarihli bir kararında söz konusu bu kıstastan hareket etmiş ve olayda gerçek bir kişiye yöneltiliş hileli hareket bulunmadığından, fiilin bilişim sistemi aracılığıyla dolandırıcılık (158/1-f) değil, bilişim sistemi ile haksız yarar sağlama suçu (244/4) olduğuna hükmetmiştir. Yüksek mahkeme, *"Dolandırıcılık suçu; hileli davranışlarla bir kişinin aldatılıp onun veya bir başkasının zararına, failin kendisine veya bir başkasına yarar sağlaması suretiyle oluşur. Suçun maddi unsurunu oluşturan*

---

437 **Koca/Üzülmez**, Özel Hükümler, s. 646.

438 **Başbüyük**, Hırsızlık ve Dolandırıcılık Suçlarının Bilişim Sistemlerinin, s. 177.

439 **Erdoğan**, TCK'da Bilişim Suçları, s. 270.

440 *"Gerçek bir kişiyle karşı karşıya gelmeden, yüz yüze veya telefon, bilgisayar, bilgi geçer gibi bir başka vasıta kullanılarak görüşmeden, konuşmadan, kişilere yönelik hileli davranışlarla aldatılmadan sadece bilişim sistemi kullanılarak doğrudan doğruya çıkar sağlanması halinde 'bilişim sistemine girerek haksız çıkar sağlama suçu' gerçekleşecektir." (Y 11. CD, E. 2009/1616, K. 2009/11328, T. 7.10.2009*, kazanci.com – s.e.t: 18.05.2017.)

"Şikayetçi ile eşinin internet ortamında MSN'de iletişim yaptıkları sırada müştekinin eşine ait elektronik posta adresine ait şifreyi bir şekilde elde edip şikayetçi ile sanki eşiymiş gibi görüşmeye devam ederek onu kandırıp cep telefonu için kontör isteyip şikayetçinin MSN'den gönderdiği kontörleri satmak suretiyle haksız yarar sağlayan sanığın eyleminin bilişim sisteminin araç olarak kullanılması suretiyle 5237 sayılı TCK'nın 158/1-f maddesindeki dolandırıcılık suçunu oluşturduğu gözetilmeden yazılı şekilde karar verilmesi ..." Y 11. CD E. 2007/5048 K. 2010/3253 T. 18.03.2010, Aktaran: **Erdoğan**, TCK'da Bilişim Suçları, s. 267.)

441 **Erdoğan**, TCK'da Bilişim Suçları, s. 271–273.

hareketlerin, gerçek bir kişiye yöneltilmiş olması, onun kandırılarak çıkar sağlanması gerekir. Gerçek bir kişiyle karşı karşıya gelmeden, yüz yüze veya telefon, bilgisayar, bilgi geçer gibi bir başka vasıta kullanılarak görüşmeden, konuşmadan, hileli davranışlarla gerçek kişiler dolandırılmadan sadece bilişim sistemi kullanılarak doğrudan doğruya çıkar sağlanması halinde 'bilişim sistemine girerek haksız çıkar sağlama suçu' gerçekleşecektir. Somut olayda oluşa uygun kabule göre; Kayseri PTT Müdürlüğü Otomasyon Bölümü'nde bilgisayar teknisyeni olarak görev yapan sanık M.Ö.Ö. ile Kayseri'de bulunan özel bir dershanede öğretmen olan diğer sanık A.K.'nın fikir ve eylem birliği içerisinde hareket ederek, 2002 yılının Mayıs ve Eylül ayları arasında Sivas, İstanbul-Fatih, Beyazıt, Bağcılar, Zeytinburnu, Küçükçekmece, Sefaköy, Merter, Bayrampaşa, Aksaray, Mecidiyeköy, Avcılar ve Kağıthane, Ankara- Ulus, Kızılay, Ahmetler, Emek ve Keçiören PTT merkezlerinden kabul işlemi yapılan bir kısım para havaleleri tutarlarına, PTT online sistemi veri tabanına girilmek suretiyle rakam ilave edilerek ödeme merkezlerince, gerçekte havale edilenden 10 veya 100 kat fazla tutarda ödeme yapılmasını sağlayarak haksız menfaat temin eden sanıkların eylemlerinin tamamen bilişim ortamında gerçekleştirilmiş olması, gerçek kişiye karşı yöneltilen her hangi hileli bir davranışın bulunmaması nedeniyle 765 sayılı TCK'nun 525/b-2. maddesindeki (5237 sayılı TCK.nun 244/4 md) bilişim suçunu oluşturacağı gözetilmeden yazılı şekilde hüküm kurulması…"[442] demek suretiyle yerel mahkeme kararını bozmuştur. Karara işlenen fiilin dolandırıcılık suçu teşkil etmeyeceği yönünden katılsak da bu fiilin TCK m. 244/4 bakımından tipik olduğu yönünden katılmamaktayız. Kanaatimizce işlenen fiille amaç taşınır mal olan paranın elde edilmesi olduğundan, sorumluluğun aşağıda ayrıca incelenen bilişim sistemi aracılığıyla işlenen hırsızlık suçundan (TCK m. 142/2-e) belirlenmesi gerekirdi.

7.2. Bilişim Sistemi Aracılığıyla İşlenen Hırsızlık Suçu Açısından

Hırsızlık suçunun temel şekli, TCK m. 141'de *"Zilyedinin rızası olmadan başkasına ait taşınır bir malı, kendisine veya başkasına bir yarar sağlamak maksadıyla bulunduğu yerden alan kimseye bir yıldan üç yıla kadar hapis cezası verilir."* şeklinde düzenlenmiştir. Bu anlamda hırsızlık suçunun unsurları: yarar sağlamak maksadıyla, taşınır bir malın, zilyedinin

[442] *YCGK, E. 2010/11-25, K. 2010/123, T. 25.5.2010* (kazanci.com – s.e.t: 16.05.2017).

rızası hilafına, bulunduğu yerden alınmasıdır[443]. TCK m. 142/2-e'de ise hırsızlık suçunun bilişim sistemleri aracılığıyla işlenmesi ağırlaştırıcı neden olarak kabul edilmiştir.

Hırsızlık suçunun *"yarar sağlamak maksadına"* ilişkin unsuru, bilişim sistemi ile haksız yarar sağlama suçu ile kesişim noktasını oluşturmaktadır. Dolayısıyla TCK m. 142/2-e, TCK m.244/4'ün asli normu olabilecek nitelikte bir suçtur.

Bilişim sisteminin araç olarak kullanılması suretiyle haksız yarar elde edilmesinde, TCK m. 142/2-e'nin asli norm olarak uygulanabilmesi için öncelikle hırsızlık suçunun temel haline ilişkin unsurların mevcudiyeti gerekmektedir. Suçun temel halinin oluşabilmesi için ise fail elde edeceği yararı, bir taşınır malın bulunduğu yerden alınması suretiyle gerçekleştirmelidir.[444]

TCK m. 244/4'de suçun oluşabilmesi ise failin bilişim sistemini engellemek, bozmak ya da sistemdeki verileri yok etmek veya değiştirmek suretiyle kendisine haksız bir çıkar sağlamasına bağlıdır. Dolayısıyla TCK m. 244/4'ten sorumluluk için failin bilişim sistemindeki verilere müdahale etmesi gerektiğinden esasen TCK m. 244/4'te taşınır bir mala müdahale söz konusu değildir. Örneğin, failin sistemde var olan verileri başka bir yere göndermesi durumunda, gönderilen verilerin bir taşınır mal olarak kabul edilmesi mümkün değildir. Birinci bölümde ifade ettiğimiz üzere bilgisayar verisi, bilginin elektronik formata – *"makine diline"* – dönüştürülmüş hâlini ifade eder ki bu durumda verinin, bir taşınır mal olarak kabul edilmesi mümkün değildir[445]. Zira taşınır mal, uzayda yer kaplayan, gözle görülüp elle tutulabilen, başlı başına var olan, hakimiyet altına alınabilen maddi cisimdir[446]. Dolayısıyla bilgisayar verisi bu özelliklere sahip olmadığından hırsızlık suçunun konusunu oluşturması mümkün değildir.

Doktrinde, yaşadığımız bilgi çağında, bilgisayar verilerinin ekonomik değerinin bulunmasının bir sonucu olarak bu verilerin hırsızlık suçunun konusu olabileceğini ifade eden yazarlar bulunmaktadır[447]. Kanaatimizce yaşadığımız çağda, bilgisayar verilerinin

---

443 **Yenidünya**, **A. Caner**; Yargıtay Kararları Işığında Hırsızlık Suçu, Ankara 2013, s. 9.

444 **Başbüyük**, Hırsızlık ve Dolandırıcılık Suçlarının Bilişim Sistemlerinin, s. 157.

445 **Tezcan/Erdem/Önok**, Ceza Özel, s. 776.

446 **Yenidünya**, Hırsızlık Suçu, s. 25.

447 **Dülger**, Bilişim Suçları, s. 576; **Karagülmez**, Bilişim Suçları, s. 217: *"TCK'nın 142/2-e maddesinde 'bilişim sistemlerinin kullanılması suretiyle hırsızlık 'tan söz edilmektedir. Burada, bilişim sisteminin sağladığı benzersiz olanaklar nedeniyle, hırsızlık suçunun çok daha kolay işlenebilmesi olgusu gözetilmektedir. Düzenlemede esas olan, verinin çalınmasından önce, hırsızlık suçunda bilişim sisteminin*

ekonomik değerinden hareketle bu verilerin hırsızlık suçunun konusu olabileceğini kabul etmek, suçta ve cezada kanunilik ilkesine aykırılık teşkil edecektir. Zira yukarıda belirttiğimiz üzere bir suçun nitelikli halinden sorumluluk için öncelikle suçun temel halinin unsurlarının gerçekleştirilmesi gerekmektedir. Hırsızlık suçunun temel halinin gerçekleşmesi için de, fiil taşınır mal üzerinde icra edilmelidir[448]. Oysa bilgisayar verisinin, fiziki-maddi varlığından bahsetmek mümkün değildir. Ayrıca verinin taşınır bir mal olmaması bir yana esasen, hırsızlık suçundaki taşınır malı bulunduğu yerden alma unsurunun da bir veri üzerinde gerçekleştirilmesi mümkün değildir. Fail, bir bilgisayar verisini *"bulunduğu yerden aldığında"* veri silinmemekte, sahibinin hâkimiyetinden çıkmamakta, fail sadece bu verinin bir kopyasını kendi hakimiyetine almaktadır[449]. Zira, çalışmamızın önceki bölümlerinde açıklandığı üzere, bir bilgisayar verisinin kalıcı bir şekilde yok edilmesi için başka özel yöntemlere ihtiyaç vardır[450]. Bu açıklamalar doğrultusunda, verinin taşınır mal olarak kabulünün TCK m. 2/3 hükmü ile yasaklanan kıyas kapsamında bir yorum oluşturacağı kanaatindeyiz.

Burada ortaya konması gereken husus TCK m. 142/2-e'nin uygulama alanının neye göre belirleneceğidir. Zira verinin hırsızlık suçuna konu olabilmesi ile hırsızlık suçuna konu taşınabilir malların bilişim sistemleri aracılığıyla elde edilmesi ayrı hususlardır[451].

Hırsızlık suçunda bilişim sistemleri, faile, fiziken ekonomik değer taşıyan taşınabilir eşyayla (hisse senedi, para, altın gibi) ve zilyediyle karşı karşıya gelmeden, bu eşyayı, bulunduğu yerden alarak kendi hakimiyet sahasına sokmasına imkân vermektedir[452]. *"Burada en önemli ölçüt ise sağlanan ekonomik yararın dış dünyada maddi bünyeye sahip bir eşya ile ilgili olması gerektiğidir"*[453]. Dolayısıyla bilişim sistemi vasıta olarak kullanılıyor ve bu

---

kullanılmış olmasıdır. Diğer yandan, nasıl ki elektrik enerjisi nesnel bir yapıya sahip olmadığı halde hırsızlığa konu olabiliyorsa, 'veri' için de benzer yaklaşım pekâlâ mümkündür. Kaldı ki 'veri'nin de sonuçta ekonomik bir değeri vardır. Yaşamakta olduğumuz bilgi çağının bir gereği olarak yeni bir yaklaşımla veri, hırsızlık suçuna konu olabilecektir."

[448] **Başbüyük**, İnternet Bankacılığı Aracılığıyla Yapılan Hukuka Aykırı Havalenin Bilişim Suçları, s. 207.

[449] **Başbüyük**, Hırsızlık ve Dolandırıcılık Suçlarının Bilişim Sistemlerinin, s. 165.

[450] Detaylı bilgi için bkz. *"3.1.4 Fiil ve Netice"* başlığı, verilerin yok edilmesi hususu.

[451] **Başbüyük**, Hırsızlık ve Dolandırıcılık Suçlarının Bilişim Sistemlerinin, s. 157; **Özbek/Doğan/Bacaksız/Tepe**, Özel Hükümler, s. 607; **Parlar**, Bilişim Suçları, s. 106: *"Bu nitelikli hırsızlığın oluşabilmesi için, bir kimsenin zilyedi olduğu bir malın 'bilişim sistemleri kullanılarak' ondan alınması veya o mal üzerinde fiili hakimiyet kurulması gerekmektedir. Diğer bir deyişle, burada kastedilen husus, bilişim sisteminin kullanılması suretiyle, verilerin değil, taşınabilir şeylerin çalınmasıdır."*

[452] **Yenidünya**, Hırsızlık Suçu, s. 69.

[453] **Koca/Üzülmez**, Özel Hükümler, s. 837.

suretle dış dünyada maddi bünyeye sahip bir eşya alınıyorsa işlenen fiil TCK m. 142/2-e bağlamında tipik olacaktır. Zira bu durumda bilişim sistemi taşınır malın alınması bakımından sadece araç fonksiyonu görmektedir[454].

Bu hususla ilgili olarak uygulamada ve Yargıtay kararlarında sıkça karşımıza çıkan durum internet bankacılığı[455] vasıtasıyla haksız para transferidir. Failin, internet bankacılığı vasıtasıyla bir başkasının hesabından kendisinin veya bir başkasının hesabına para transfer etmesi durumunda hangi suçun oluşacağının ortaya konulması gerekir.

Başkasının banka hesabına internet üzerinden girerek, failin kendisinin veya bir başkasının hesabına para göndermesi durumuna ilişkin olarak Yargıtay'ın 6. ve 11. Ceza Daireleri arasında görüş farklılığı vardı. Yargıtay 6. Ceza Dairesi bu şekilde gerçekleştirilen fiiller bakımından TCK m. 142/2-e hükmünün uygulanması gerektiğini belirtirken, Yargıtay 11. Ceza Dairesi TCK m. 244/4 hükmünün uygulanması gerektiği görüşündeydi[456].

Konuya ilişkin Yargıtay 6. Ceza Dairesinin 02.06.2008 tarihindeki kararı şu şekildedir: *"Sanığın internet bankacılığı hizmetinden yararlanan yakınanın şifresini elde ederek hesap bilgilerine ulaştıktan sonra, ... Bankası Galatasaray Şubesi'nde bulunan hesabındaki 5800 YTL.yi oluşturduğu sahte kimliğe havale çıkarttığı, bu eylemin sistemi engelleme, bozma, verileri yok etme veya değiştirmenin söz konusu olmadığı anlaşıldığından; ... bilişim sisteminin kullanılması suretiyle işlenen hırsızlık suçunun, sanık tarafından yakınanın hesabından paranın başkası adına havale edilmesi anında tamamlandığı gözetilmeyerek, eylemin kalkışma aşamasında kaldığının kabul edilmesi, karşı temyiz olmadığından bozma nedeni yapılmamıştır"*[457]. Yüksek mahkeme bu kararında, internet bankacılığı ile havalede sistemi engelleme, bozma; verileri yok etme değiştirme suçlarının fiil unsurları gerçekleşmediğinden sorumluluğun TCK m. 244/4'ten değil TCK m. 142/2-e'den olacağını hükme bağlamıştır.

Buna karşın Yargıtay 11. Ceza Dairesinin 27.04.2009 tarihindeki kararı ise şu şekildedir: *"Sanıkların fikir ve eylem birliği içinde hareket ederek, katılan S'nin Y. Bankası Manisa*

---

454 **Koca**, Bilişim Sistemlerinin Kullanılması Suretiyle Haksız Yarar, s. 1657.

455 **Eralp**, **Özgür**; İnternet Bankacılığı ve Kredi Kartı Dolandırıcılığının Teknik, Hukuki ve Cezai Boyutu, 2012, s. 6 *"İnternet bankacılığı, uzaktan erişimi sağlayan internetin kullanılması yoluyla bankacılık işlemlerinin yapılması olarak tanımlanabilir."*

456 **Koca/Üzülmez**, Özel Hükümler, s. 836.

457 *Y 6. CD, E. 555, K. 12249, T. 19.6.2014,* Aktaran: **Karagülmez**, Bilişim Suçları, s. 250, 251.

Şubesindeki banka hesabına ait 'interaktif bankacılık' şifresini kırarak internet aracılığı ile hesapta bulunan parasını sanıklardan Y'nin A. Bank Bakırköy Şubesindeki şirket hesabına havale ederek bu hesaptan parayı çekmelerinden ibaret eylemlerinin 5237 sayılı TCK'nın 244/4. maddesindeki suçu oluşturduğu gözetilmeden, suçların nitelendirilmesinde yanılgıya düşülerek hırsızlık suçlarından yazılı şekilde hüküm kurulması ..."[458] Yüksek mahkeme, bu kararında internet bankacılığı şifresinin kırılarak sisteme girilmek suretiyle hukuka aykırı havale fiilini hırsızlık suçu olarak değil, TCK m. 244/4'teki suç olarak değerlendirmiştir.

Yargıtay Ceza Daireleri arasındaki bu görüş ayrılığının ardından, Yargıtay Ceza Genel Kurulu 2009 yılında verdiği kararında internet bankacılığı üzerinden gerçekleştirilen bu tür haksız para transferi işlemlerinde, TCK m. 244/4 anlamında bir veri transferinin değil, bu veriyle temsil edilen paranın mal edinilmek istendiği ve dolayısıyla bu tür olaylarda TCK m. 142/2-e anlamında bilişim sistemi aracılığıyla hırsızlık suçunun oluşacağını hükme bağlamıştır. Bu karara göre: *"Sanık Volkan'ın; firari Saim ile birlikte hareket ederek, daha önceden haksız bir şekilde ele geçirdikleri katılan firmanın internet bankacılık şifresini kullanmak suretiyle, katılanın Ş bank Ankara K ... Şubesindeki hesabından 10. 750 YTL'yi Ş ... bank-İstanbul Z Şubesinde sanık Volkan adına açtırdıkları hesaba havale edip, aynı gün banka şubesinden çekmek şeklinde gerçekleştirdiği eylemdeki kastı, katılan firmanın banka hesabında bulunan, taşınır nitelikteki parayı bilişim sistemini kullanmak suretiyle kendi banka hesaplarına geçirmeye, katılanın rızasına aykırı olarak malvarlığında azalmaya neden olmaya; başka bir anlatımla var olan veriyi başka bir yere göndermekten ziyade, bu verinin temsil ettiği parayı alarak mal edinmeye yöneliktir. Kaldı ki sanığın katılanın internet bankacılık hesabında bulunan parasına ulaşmak için bilişim sistemlerini araç olarak kullanmaktan başka alternatifi de yoktur. Dolayısıyla olayımızda, 5237 sayılı TCY'nin 142/2-e maddesinde düzenlenmiş bulunan "bilişim sistemi kullanılmak suretiyle hırsızlık" suçunun gerçekleştiği kabul edilmelidir. Şu halde, sanığın eyleminin 5237 sayılı TCY'nin 142/2-e maddesindeki nitelikli hırsızlık suçunu oluşturduğunun kabul edilmesi karşısında; 244. maddenin 4. fıkrası uyarınca uygulama yapma olanağı da bulunmamaktadır."*[459]

---

[458] *Y 11. CD, E. 964, K. 4877, T. 27.4.2009,* Aktaran: **Taşdemir**, Bilişim, Banka veya Kredi Kartlarının Kötüye Kullanılması ve Dolandırıcılık Suçları, s. 295, 296.

[459] *YCGK E. 2009/11-193 K. 2009/268 T. 17.11.2009* (Kararın tam metni için bkz. **Dülger**, Bilişim Suçları, s. 579–598.)

YCGK'nın 27.04.2009 tarihli bu kararından sonra Yargıtay Ceza Daireleri de istikrarlı bir şekilde internet bankacılığı aracılığıyla yapılan para transferi işlemlerini TCK m. 142/2-e kapsamında bilişim sistemi aracılığıyla hırsızlık suçu olarak kabul etmeye başlamıştır[460]. Kanaatimizce bu tür olaylara ilişkin YCGK'nın kararı yerindedir. Her ne kadar internet bankacılığı ile para transferi işlemlerinde esasen TCK m. 244 kapsamında sistemde var olan verilerin başka bir yere gönderilmesi söz konusu olsa da failin bu fiil ile elde etmek istediği hesaptaki verinin temsil ettiği para yani taşınır maldır[461]. TCK m. 142/2-e hükmünde *"bilişim sistemlerinin kullanılması suretiyle"* hırsızlık suçu düzenlendiğinden failin gerçekleştirdiği fiil, suçun kanuni tanımına uymaktadır. Zira fail, burada ilgili bankanın bilişim sistemlerini kullanarak taşınır bir malı bulunduğu yerden almış olmaktadır. Esasen söz konusu fiil, TCK m. 244/4 bağlamında da sistemde var olan verilerin başka bir yere gönderilmesi suretiyle haksız yarar sağlanması şeklinde tipiktir. Ancak TCK m. 244/4 kanunda tali norm olarak düzenlenmiştir. Dolayısıyla fiile uygulanacak hüküm TCK m. 142/2-e olmak durumundadır.[462]

Failin, internet bankacılığı dışında ATM'lere (Automated Teller Machine)[463] fiziki müdahale ile hukuka aykırı şekilde para elde etmesi de mümkündür. ATM'ler de bilgisayar verisini saklamak, işlemek, depolamak gibi özellikleri haiz olduğundan birer bilişim sistemidir[464]. Yargıtay 11. CD 2012 tarihindeki şu kararıyla: *"Sanıkların Oyakbank*

---

460 **Doğan**, Bilişim Suçları, s. 155; **Yılmaz**, TCK'nın 244. Maddesinde Düzenlenen Bilişim Alanındaki Suçlar, s. 94.

461 **Dülger**, Bilişim Suçları, s. 603; **Koca**, Bilişim Sistemlerinin Kullanılması Suretiyle Haksız Yarar, s. 1657.

462 *"Başbüyük"e* göre internet bankacılığı yoluyla yapılan havale durumunda fiil ne hırsızlık suçunu ne de TCK m.244/4'teki suçu oluşturur. Yazarın görüşü şu şekildedir: *"Banka havalesi, bir hesaptan diğer hesaba alacak kaydedilmesi suretiyle gerçekleşir ve bu esnada nesnel anlamda para tedavül etmez. Tedavül eden şey, alacak hakkını temsilen çıkartılan, nesnel bir varlığa sahip olmayan kaydi paradır. O halde banka havalesinin konusu ekonomik anlamda parasal bir değeri ifade etmekle birlikte, bu değer hırsızlık suçu anlamında taşınabilir bir mal değildir.*

Belirtmek gerekir ki, haksız bir şekilde ele geçirilen internet bankacılık şifresiyle, yine internet üzerinden söz konusu hesaba girmek suretiyle başka bir hesaba havale yapılması, TCK m. 244/4'te düzenlenen bilişim sistemleri aracılığıyla yarar sağlama suçunu da oluşturmamaktadır. Nitekim bu hüküm, hukuka aykırı olarak bilişim sistemlerin aracılığıyla elde edilen her türlü yararı değil; yalnızca bilişim sisteminin çalışma düzenini etkilemeye yönelik TCK m. 244/1 ve m. 244/2'deki seçimlik hareketler sonucunda elde edilen yararları kapsamaktadır. Söz konusu fiillerin cezalandırılması için, sisteme dışarıdan herhangi bir müdahalede bulunmaksızın, bilişim sistemlerinin hukuka aykırı olarak kullanılması suretiyle yarar elde edilmesinin de hüküm altına alınması gerekir." (**Başbüyük**, Hırsızlık ve Dolandırıcılık Suçlarının Bilişim Sistemlerinin, s. 188.)

463 **Değirmenci**, **Olgun**; "*Ceza Hukuku Açısından Kredi ve Banka Kartları*", Legal Hukuk Dergisi, 2003, Cilt 1, Sayı 1, s. 597: *"Kart hamillerinin banka ve kredi kartları aracılığıyla mevduat ve kredi kartları hesaplarına şifre aracılığı ile ulaşmalarını ve sunulan banka hizmetlerini kullanmalarını sağlayan elektronik cihazlardır."*

464 **Değirmenci**, Ceza Hukuku Açısından Kredi ve Banka Kartları, s. 606.

ATM'nin çalışmasındaki aksaklığı fark ederek, çeşitli zamanlarda para çekme işlemi sırasında ATM'ye fiziki müdahalede bulunmak suretiyle cihazın para bloke edilmiş gibi işlem görmesini sağlayıp, çektikleri paranın hesaptan düşmesini engelleyerek menfaat elde ettiklerinin iddia ve kabul olunması karşısında eylemlerinin 765 sayılı Türk Ceza Kanununun 525/b-1 (5237 sayılı TCK'nun 244/4) maddesindeki 'bilişim sistemini engellemek veya yanlış biçimde çalışmasını sağlamak suretiyle yarar sağlamak' suçuna uygun bulunduğu gözetilmeden yazılı şekilde 765 sayılı Türk Ceza Kanunun 525/b-2. maddesinden hüküm kurulmak suretiyle eksik ceza tayini,…"[465] bu şekilde ATM'ye fiziki müdahale ile paranın elde edilmesi durumunda bilişim sisteminin engellenmesi veya yanlış çalışmasını sağlamak suretiyle yarar sağlamanın söz konusu olduğunu ve bu nedenle failin sorumluluğunun TCK m. 244/4'ten olması gerektiğini hükme bağlamıştır.

ATM'ye fiziki müdahale ile hukuka aykırı olarak para çekilmesi durumunda fiil, hem TCK m. 244/4 hem de TCK m. 142/2-e anlamında tipiktir. Zira fail sistemi engelleyip haksız yarar sağlayarak TCK m. 244/4'deki suçu gerçekleştirmiş olmakta hem de zilyedinin rızası dışında taşınır bir malı bulunduğu yerden bilişim sistemi vasıtasıyla almaktadır. Bu ve bunun gibi durumlarda TCK m. 244/4'ün tali norm olmasından hareketle fiile uygulanacak hükmün TCK m. 142/2-e olduğu kanaatindeyiz[466].

7.3. Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu Açısından

Banka ve kredi kartlarının, bilişim sistemleri ve bu sistemlere bağlı olarak çalışan elektronik cihazlar (ATM, POS cihazı gibi) ile kullanılması nedeniyle aslında bilişim sistemlerinin birer parçasını oluşturmaktadırlar[467]. Dolayısıyla bu kartlar ile işlenen suçların da bilişim sistemi aracılığıyla haksız yarar sağlama suçuna vücut vermesi muhtemeldir. Nitekim 765 sayılı TCK döneminde banka veya kredi kartlarının kötüye kullanılmasına ilişkin ayrı bir suç bulunmadığından Yargıtay, bu kartlarla elde edilen haksız yararları, bilişim sistemi ile haksız yarar sağlama suçu (765 sayılı TCK m. 525/b-2) kapsamında değerlendirmekteydi[468].

---

[465] *Y 11. CD E. 2010/6346, K. 2012/3544, T. 13.3.2012,* Aktaran: **Yaşar, Osman/Gökcan, Hasan Tahsin/Artuç, Mustafa**; Yorumlu - Uygulamalı Türk Ceza Kanunu, Ankara 2014, s. 7334.

[466] **Dülger**, Bilişim Suçları, s. 447; **Koca**, Hukukumuzda TCK'nın 244'ncü maddesi, s. 97.

[467] **Başbüyük**, Hırsızlık ve Dolandırıcılık Suçlarının Bilişim Sistemlerinin, s. 179.

[468] *"…sanığın 20.07.2002 günü ölen babasına ait banka kartını tahsis eden katılan kuruma iade etmeyerek haksız surette elinde bulundurup ölü babası hesabına yatırılan 01.09.2002-30.11.2004 dönemini kapsayan maaşlarını çekmeye devam ettiğinin anlaşılmasına göre, suç tarihinde yürürlükte bulunan 765 sayılı*

Birinci bölümde ele alınan banka veya kredi kartlarının kötüye kullanılması suçunda TCK m. 245/1 ve 3, bilişim sistemi aracılığıyla haksız yarar sağlama suçunun asli normu olabilecek nitelikte suçlardır. Zira TCK m. 245/1'de başkasına ait banka veya kredi kartını her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimsenin kart sahibinin rızası olmaksızın bunu kullanarak kendisi veya başkasına *"yarar sağlaması"* suçun oluşumu için aranmıştır. Aynı şekilde 3. fıkrada da *"yarar sağlama"* fiilinin sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartı ile işlenmesi cezai yaptırım altına alınmıştır.

Bu suçlar ile TCK m. 244/4 bakımında ortak olabilecek nitelikteki fiiller, internet üzerinden kredi kartı ile alışveriş yapmak[469] ya da ATM[470] veya POS (Point of Sale) cihazlarından banka veya kredi kartı kullanarak işlem yapmaktır.

5464 sayılı Banka ve Kredi Kartları Kanunu'nda kredi kartı *"Nakit kullanımı gerekmeksizin mal ve hizmet alımı veya nakit çekme olanağı sağlayan basılı kart veya fizikî varlığı bulunmayan kart numarası"* şeklinde tanımlanmıştır. Dolayısıyla öncelikle, suçun fiziki varlığı bulunmayan kredi kartı numaraları ile işlenmesi durumunda da TCK m. 245/1'deki suçun oluşup oluşmayacağını belirlememiz gerekecektir.

Doktrinde bir görüşe göre failin fiziki varlığı bulunmayan kredi kartı numarasını bir şekilde ele geçirip bu numara ile internet üzerinden alışveriş yapması durumunda fiil, TCK m. 245/1'deki suçu değil; TCK m. 244/3 veya 4'teki suçu oluşturacaktır. *"Özbek"e* göre TCK m. 245/1'deki *"kartın kullanılması ya da kullandırılması"* ifadesinden kartın fiziki olarak kullanımının zorunlu olduğu sonucu çıkmaktadır. Şu hâlde kart bilgilerinin kullanılması suretiyle internetten alışveriş yapılması durumunda fiil, bilişim sistemindeki bir verinin gönderilmesi söz konusu olduğundan, TCK m. 244/3 bakımından tipiktir. Ayrıca eğer bu fiil

TCK'nın 525/b-2, 80 *(5237 sayılı Yasa'nın* 245*/1,* 43*) maddeleri kapsamındaki suçu oluşturduğu gözetilmeden…"* (*Y 11. CD, E. 2006/1891, K. 2008/1623, T. 18.3.2008* – kazanci.com s.e.t: 19.05.2017*)*

469 **Eralp**, İnternet Bankacılığı ve Kredi Kartı Dolandırıcılığı, s. 95: *"İnternetten alışveriş yöntemi: Bu yöntemin kullanılabilmesi için hiçbir araç veya karta ihtiyaç yoktur. Sadece kredi kartı bilgileri yeterlidir. İnternetten herhangi bir mal veya hizmet satın almak için kredi kartı numarası, kartın geçerlilik tarihi, kart sahibinin adı ve imza bandında bulunana güvenlik numarasının son 3 rakamı dışında başka bilgiye ihtiyaç yoktur."*

470 **Değirmenci**, Ceza Hukuku Açısından Kredi ve Banka Kartları, s. 597: *"Kart hamillerinin banka ve kredi kartları aracılığıyla mevduat ve kredi kartları hesaplarına şifre aracılığı ile ulaşmalarını ve sunulan banka hizmetlerini kullanmalarını sağlayan elektronik cihazlardır."*

ile haksız yarar elde etme de söz konusu ise failin sorumluluğu TCK m. 244/4'ten olacaktır[471].

Doktrindeki diğer görüşe göre ise ister kart fiziksel olarak ATM cihazına sokularak kullanılsın ister fiziksel olarak ele geçirilen kartın üzerindeki numaralar kullanılsın, isterse de fiziksel kart ele geçirilmeden bu karta ait bilgi ve numaraların ele geçirilmesiyle kullanılsın, sonuçta bir haksız yarar elde ediliyorsa TCK m. 245/1'in uygulanması gerekmektedir[472].

Kanaatimizce bu gibi hallerde 5464 sayılı BKKK göz önüne alındığında kredi kartı, banka kartından farklı olarak fiziki varlığı bulunmayan kart numarasını da içerdiğinden bu numaralar kullanılmak suretiyle yarar elde edilmesi durumunda fiil, TCK m. 245/1 anlamında tipiktir. TCK m. 244 bakımından ise kredi kartı bilgilerinin kullanıldığı sisteme veya o sistemdeki verilere müdahale edilmemektedir. TCK m. 244/2'deki *"sistemde var olan verileri başka bir yere gönderme"*nin de söz konusu olmadığını düşünmekteyiz. Kredi kartı, nakit kullanımı gerekmeksizin mal ve hizmet alımı ya da nakit çekme olanağı vermektedir. Ancak kredi kartı numaraları ile nakit çekme olanağı yoktur. Kredi kartı numaraları ile ancak internet üzerinden mal veya hizmet alımı yapılabilmektedir. Dolayısıyla kredi kartı numaraları ile alışverişin yapıldığı internet sitesinin bilişim sistemindeki herhangi bir veri başka bir yere gönderilmemekte sadece kart bilgilerinin kullanılmasıyla mal veya hizmetin karşılığı olarak ödeme gerçekleşmektedir.

Yargıtay söz konusu duruma ilişkin olarak istikrarlı bir şekilde banka veya kredi kartlarının kötüye kullanılmasına ilişkin suçun oluştuğu görüşündedir[473]. Yargıtay 11. CD 2013 yılında verdiği bir kararda banka veya kredi kartı ile haksız yarar sağlamanın TCK m. 244/4'deki suçu değil, TCK m. 245/1'deki suçu oluşturacağına hükmetmiştir. Yüksek mahkemenin kararı şu şekildedir: *"Sanığın müştekilere ait kredi kartı bilgilerini haksız şekilde ele geçirip bu bilgileri kullanarak internet üzerinden alışveriş yaptığının iddia edilmesi ve 5464 sayılı Banka Kartları ve Kredi Kartları Kanunun 3/e maddesi uyarınca 'Kredi kartının, nakit kullanımı gerekmeksizin mal ve hizmet alımı veya nakit çekme olanağı sağlayan basılı kartı veya fiziki varlığı bulunmayan kart numarasını' ifade etmesi karşısında, kredi kartı*

[471] **Özbek**, Banka veya Kredi Kartlarının, s. 1032.
[472] **Dülger**, Bilişim Suçları, s. 478.
[473] **Dülger**, Bilişim Suçları, s. 478.

bilgilerinden yararlanarak menfaat sağlanmasının kredi kartı gibi değerlendirilmesi gerektiği ve somut olayda kredi kartı sahibi sayısınca 5237 sayılı Türk Ceza Kanununu 245/1 maddesinde öngörülen banka veya kredi kartlarının kötüye kullanılması suçunun oluşacağı gözetilmeden, suç vasfında hataya düşülerek yazılı şekilde aynı Kanunun 244/4. maddesi gereğince mahkumiyetine karar verilmesi,"[474]. Buna göre kararda dikkat çeken bir diğer nokta ise kredi kartı numaralarının kullanılması suretiyle haksız yarar sağlamayı yüksek mahkemenin TCK m. 245/1 kapsamında değerlendirmesidir.

5464 sayılı BKKK'da banka kartının tanımında kart bilgilerinin tanıma dahil edilmemesi nedeniyle banka kartı bilgileri ile haksız yarar elde edilmesi durumunda ne olacağı doktrinde tartışmalıdır. Bir görüş, banka kartının kanunda kart bilgilerini içerecek şekilde tanımlanmaması dolayısıyla TCK m. 245/1'deki suçun oluşmayacağını ancak TCK m. 244'ten sorumluluğun söz konusu olabileceğini ifade ederken[475] diğer görüş ise banka kartı bilgilerinin kullanılması durumunda da TCK m. 245/1'deki suçun oluşacağını ifade etmektedir[476]. Kanaatimizce bu halde BKKK'da banka kartının tanımında kart bilgilerinin yer almaması nedeniyle, TCK m. 245 açısından banka kartının fiziki olarak kullanılması gerekmektedir. Dolayısıyla TCK m. 245'de *"kartın kullanılması ya da kullandırılması"* ifadesi bu durumda banka kartı bilgilerinin kullanılmasını kapsamayacaktır.

Failin ATM üzerinden ya da POS cihazından banka veya kredi kartını kullanarak kendisi veya başkası yararına haksız çıkar elde etmesi durumunda ise sisteme ya da sistemdeki verilere müdahalede (m. 244/1 ve 2) bulunmamaktadır. Dolayısıyla kanaatimizce bu gibi hallerde TCK m. 244/4 bakımından tipiklik oluşmadığından asli norm – tali norm araştırması yapılmayacaktır.

Konuyla ilgili Yargıtay 11. CD 2012 tarihli kararında; *"Katılanın olay günü saat 21:00 sıralarında Z. Bankasına ait ATM'den para çekmek için uğraştığı sırada, yanına gelen sanığın önceden ATM'nin kart yuvasına kurmuş olduğu düzenek sayesinde kartın sıkışmasını*

---

474 *Y 11. CD E. 2013/3461 K. 2013/9144 T. 31.5.2013* (**Yaşar/Gökcan/Artuç**, Yorumlu Uygulamalı TCK, s. 7334.)

475 **Erdoğan**, TCK'da Bilişim Suçları, s. 327.

476 **Dülger**, Bilişim Suçları, s. 478; **Ketizmen**, Bilişim Suçları, s. 187; **Karagülmez**, Bilişim Suçları, s. 301, 302.: *"Bize göre ister kart fiziksel olarak ATM cihazına sokularak kullanılsın ister fiziksel olarak ele geçirilen kartın üzerindeki numaralar kullanılsın, isterse de fiziksel kart ele geçirilmeden bu karta ait bilgi ve numaraların ele geçirilmesiyle kullanılsın, sonuçta bir haksız yarar elde ediliyorsa 245/1. maddenin uygulanması gerekmektedir."*

sağlayıp yardım bahanesiyle şifresini öğrendiği, katılanın olay yerinden ayrılmasından sonra ele geçirdiği bankamatik kartı ile katılana ait hesaptan birer dakika arayla üç defada toplam 2000 TL para çekmesi şeklindeki sanığın eyleminin TCK'nın 245/1. maddesinde tanımlanan 'banka ve kredi karı kartlarının kötüye kullanılması' suçunu oluşturduğu gözetilmeden yazılı şekilde TCK'nın 244/4. maddesi uyarınca hüküm kurulması, bozmayı gerektirmiştir."[477] ifadesiyle ele geçirilen kredi kartı ile ATM'den para çekilmesini TCK m. 245/1 kapsamında değerlendirmiştir.

7.4. Bilişim Sistemine Girme Suçu Açısından

Bilişim sistemine girme suçu (m. 243) ile bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme (m. 244) suçları arasındaki ilişki bakımından doktrinde farklı görüşler vardır.

Bir görüşe göre bilişim sistemine girme suçu diğer bilişim suçlarını işlemek bakımından çoğu zaman araç suç konumundadır[478]. Bu anlamda işlenmesi amaçlanan bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme suçları bakımından bilişim sistemine girme suçu geçit olma özelliği taşıdığından fail bilişim sistemine girme suçundan değil, sadece amaç suçtan dolayı sorumlu olacaktır[479].

Diğer görüşe göre[480] ise bu gibi hallerde farklı neviden fikri içtimanın varlığını kabul etmek gerekmektedir. Zira fikri içtimada bir suçun icra hareketlerinin bir başka suçun icra hareketleriyle kısmen veya tamamen örtüşmesi gerekli ve yeterlidir. Bir bilişim sistemindeki verileri değiştirmek isteyen fail, bu suçun (m.244) icra hareketlerini gerçekleştirirken sisteme de girmekte ve TCK m. 243'ü de ihlal etmektedir. Dolayısıyla failin bu suçlardan en ağır cezayı gerektiren TCK m. 244'ten sorumlu olması gerekmektedir.

Üçüncü bir görüşe göre[481] ise bu gibi hallerde ne bir geçit suç durumu söz konusudur ne de farklı neviden fikri içtima hali vardır. Buna göre bilişim sistemine girme suçu, TCK m.

---

477 *Y 11. CD, E. 2010/7414, K. 2012/9184, T. 17.5.2012,* Aktaran: **Dülger**, Bilişim Suçları, s. 483.

478 **Taşdemir**, Bilişim, Banka veya Kredi Kartlarının Kötüye Kullanılması ve Dolandırıcılık Suçları, s. 261; **Yenidünya**, Hukuka Aykırı Erişim Suçu, s. 1039.

479 **Soyaslan**, Özel Hükümler, s. 650.

480 **Koca**, Hukukumuzda TCK'nın 244'ncü maddesi, s. 96.

481 **Dülger**, Bilişim Suçları, s. 405: *"Bize göre burada geçit suçu durumu bulunmamaktadır, dolayısıyla şartları uymayan bir hukuki kurumun buraya uygulanarak çözüme gidilmesi uygun bir çözüm değildir. Öte yandan bize göre failin 'tek' eyleminden söz edilmesi de mümkün değildir, zira fail 244. maddedeki suçu sisteme girmek ve orada kalmak suretiyle işlediğinde farklı eylemler gerçekleştirmektedir, buna göre*

244'ün gerçekleştirilmesi için işlenmesi zorunlu bir suç değildir. Ayrıca bilişim sistemine girme ile sisteme ya da sistemdeki verilere müdahale iki farklı fiildir. Kanaatimizce de TCK m. 244'deki suçların işlenmesi için muhakkak bilişim sistemine girme fiilinin icra edilmesi gerekmemektedir. Örneğin, failin bir bilişim sisteminin işleyişini engellemek için gönderdiği bir bilişim virüsü, sistemin işleyişini engellediğinde bilişim sistemine girme söz konusu olmayacaktır. Zira birinci bölümde ifade edildiği üzere, bilişim sistemine girme fiili, sistemin sanal alanına, içerdiği verilere dahil olmadır. Suçla korunan hukuksal değer, özel hayatın gizliliğidir. Failin gönderdiği kötücül yazılım sadece sistemi bozmak için işlevsel ancak failin, sistemin içeriğine dahil olması, bu içeriği öğrenmesi bakımından işlevsel değil ise sisteme girme fiilinin gerçekleştirildiğinden bahsedilemeyecektir. Sisteme girme fiili için elverişli yazılımlar genellikle *"trojan"*lardır, zira bu yazılımlar bulaştığı sistemde arka kapılar oluşturarak failin bu sistemin içeriğine dahil olmasına imkân vermektedirler.

Öte yandan bu gibi hallerde failin tek fiilinden söz edilmesi de mümkün değildir. Zira bilişim sistemine girme ile sistemi engelleme, bozma; verileri yok etme veya değiştirme fiilleri farklı fiillerdir. Örneğin, fail mağdurun sitemine gönderdiği bir *"trojan"* ile sisteme girmiş ve orada kalmaya devam etmiş ve fakat sistemde bulunmasına rağmen TCK m. 244'deki fiilleri henüz gerçekleştirmemiş olabilir. Daha sonra mağdurun sisteminde *"trojan"* vasıtasıyla birtakım verileri değiştirerek kendine yarar sağlamış olabilir. Bu durumda sisteme girme ile veri değiştirmeyi tek fiil olarak kabul etmemiz mümkün değildir.

TCK m. 244'ün işlenmesi için muhakkak bilişim sistemine girme suçunun işlenmesi gerekmediğinden ve bu suçların koruduğu hukuki değerlerden yola çıkarsak, söz konusu fiillerin ayrı ayrı cezai sorumluluğa neden olması gerektiğini ifade edebiliriz. Zira bilişim sistemine girme suçunda özel hayatın gizliliği koruma altına alınmışken, TCK m. 244'te bilişim sistemlerinin güvenliğinin yanı sıra bu sistem ve sistemdeki veriler, kişinin malvarlığında bulunan bir değer olarak koruma altına alınmıştır. Şu hâlde fail, mağdurun sistemine girerek hem onun özel hayatının gizliliğini ihlal etmiş hem de sistemdeki verileri değiştirerek kendine haksız bir yarar sağladığı için mağdurun malvarlığına müdahalede bulunmuştur.

---

düşünsel birleşme kuralının da uygulanmaması gerekir. Bu bağlamda bize göre eylemler arasında zamansal açıdan yakınlık bulunması halinde 244/2 'den ceza verilmesi, zamansal açıdan yakınlık olmayıp farklı kastlarla hareket edildiğinin kabul edilmesi halinde ise her iki suçtan ayrı ayrı ceza verilmesi gerekmektedir."

Belirtmek gerekir ki, tüm bu açıklamaların geçerli olabilmesi için failin TCK m. 244'deki suçu işlemek bakımından kastının bulunması şarttır. Zira sisteme girme fiili sebebiyle sistemin içerdiği verilerin yok olması veya değişmesi, kanunda bu suçun neticesi sebebiyle ağırlaşmış hali olarak düzenlenmiştir (m. 243/3)[482]. Şu durumda failin, TCK m. 244'teki neticeleri gerçekleştirmek bakımından bir kastı yok iken sisteme girme fiili nedeniyle bu neticeler gerçekleşirse failin sorumluluğu TCK m. 243/3'ten olacaktır.

7.5. Fikir ve Sanat Eserleri Kanunu'ndaki Bilişim Suçları Açısından

Fikir ve Sanat Eserleri Kanunu (FSEK) m. 71'de düzenlenen manevi, mali ve bağlantılı haklara tecavüz suçlarında fail büyük çoğunlukla haksız ekonomik çıkar elde etmek amacıyla bu suçları işlemektedir ancak bu suçların kanuni tanımında haksız çıkar sağlama neticesine yer verilmemiştir. Dolayısıyla bu suçların TCK m. 244/4'ün asli normu olmadığını ifade edebiliriz. Zira TCK m. 244/4'te *"haksız bir çıkar sağlamasının başka bir suç oluşturmaması"* ifadesi kullanılmıştır.

5846 sayılı Fikir ve Sanat Eserleri Kanunu'nda 7.6.1995 tarihinde 4110 sayılı kanun ile FSEK m. 2[483] kapsamında ilim ve edebiyat eserlerine *"bilişim programları"* da dahil edilmiştir[484]. Ayrıca yine aynı kanun ile FSEK'in 6. maddesinin 1. fıkrasının 10. bendine "*bir bilgisayar programının uyarlanması, düzenlenmesi veya herhangi bir değişim yapılması"* ifadesi eklenerek işlenme[485] yoluyla elde edilen bilgisayar programlarının da eser kapsamında olacağı öngörülmüştür. Böylece bilişim yazılımları üzerindeki fikri haklar, FSEK korumasına alınmıştır[486].

---

[482] **Soyaslan**, Özel Hükümler, s. 640.

[483] ***5846 sayılı FSEK m.2/1 –*** *Herhangi bir şekilde dil ve yazı ile ifade olunan eserler ve her biçim altında ifade edilen bilgisayar programları ve bir sonraki aşamada program sonucu doğurması koşuluyla bunların hazırlık tasarımları,*

[484] **Bayamlıoğlu**, **İbrahim Emre**; Fikir ve Sanat Eserleri Hukukunda Teknolojik Koruma, İstanbul 2008, s. 244; **Çolak**, **Uğur**; "*Türk Hukukunda Bilgisayar Programlarının Ceza Hukuku Tedbirleri İle Korunması*", Legal Fikri ve Sınai Haklar Dergisi, 2016, Sayı 5, s. 116.

[485] *"İşleme, nitelik olarak asıl esere bağlı kalmak kaydıyla, orijinal bir eserin başka bir formda, yeni bir fikri ürüne dönüştürülmesidir. Başka bir eser şeklinde ortaya çıkan işleme, asıl eserin bir türevi olsa da, ekonomik olarak bağımsız şekilde değerlendirilmeye uygundur."* **Bayamlıoğlu**, Fikir ve Sanat Eserleri Hukukunda Teknolojik Koruma, s. 219; **Yenidünya, A. Caner**; "*5846 Sayılı Fikir ve Sanat Eserleri Kanunu'nda düzenlenen manevi ve mali haklara tecavüz suçları*", Erzincan Üniversitesi Hukuk Fakültesi Dergisi, 2006, Cilt 10, Sayı 3–4, s. 245.

[486] **Karagülmez**, Bilişim Suçları, s. 172; **Orta**, Bilişim Suçları ve Adli Bilişim, s. 134.

Bilişim programları, bilişim sistemindeki verilerden oluşan bir bütündür. Dolayısıyla bu programlara müdahale sonucu elde edilecek yararlar bakımından TCK m. 244/1 kapsamında bilişim sistemlerine müdahale sonucu değil, TCK m. 244/2 kapsamında sistemdeki verilere müdahale sonucu haksız yarar elde edilmesi söz konusu olabilecektir.

Bu anlamda FSEK/1-b.1 kapsamında hak sahibi kişilerin yazılı izni olmaksızın bir bilişim programını değiştirmek suretiyle haksız yarar elde etme durumunda, TCK m. 244/4 kapsamında sistemdeki verileri değiştirmek suretiyle haksız yarar elde etme de söz konusu olabilecektir.

Yine aynı madde kapsamında bilişim programlarını çoğaltmak, dağıtmak, her türlü işaret ses veya görüntü nakline yarayan araçlarla umuma iletmek ve yayımlamak fiillerinde, TCK m. 244/4 kapsamında sistemde var olan verileri bir başka yere göndermek suretiyle haksız yarar elde etme söz konusu olabilecektir.

Bu hallerde tek bir fiille birden fazla suçun işlenmesi söz konusu olacağından farklı neviden içtima kuralı (TCK m. 44) gereğince fail daha ağır cezayı gerektiren TCK m. 244/4'ten sorumlu olacaktır. Zira FSEK m. 71 kapsamında *"haksız yarar sağlama"* tipikliğe dahil edilmemiştir.

7.6. Diğer Bazı Suçlar Açısından

5411 sayılı Bankacılık Kanunu m. 160'da düzenlenen bankacılık zimmeti suçu[487], TCK m. 244/4'ün asli normu olabilecek nitelikte bir suçtur[488]. Bankacılık Kanunu m. 160'da bu suç, *"görevi nedeniyle zilyetliği kendisine devredilmiş olan veya koruma ve gözetimiyle yükümlü olduğu para veya para yerine geçen evrak veya senetleri veya diğer malları kendisinin ya da başkasının zimmetine geçiren banka yönetim kurulu başkan ve üyeleri ile diğer mensupları, altı yıldan oniki yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılacakları gibi bankanın uğradığı zararı tazmine mahkûm edilirler."* şeklinde düzenlenmiştir. Dolayısıyla koruma ve gözetimle yükümlü olan bir banka mensubu, çalıştığı bankanın mudilerine ait banka hesabına başka bir ifadeyle bilişim sistemine girerek, buradan kendisinin veya başkasının banka hesabına hukuka aykırı para transfer etmesi durumunda, hırsızlık suçunda açıkladığımız nedenlere paralel bir şekilde, bankacılık zimmeti suçundan

[487] Suç hakkında detaylı bilgi için bkz. **Donay**, Bankacılık Ceza Hukuku, s. 107–120.
[488] **Koca/Üzülmez**, Özel Hükümler, s. 836.

sorumlu olacaktır[489]. Zira her ne kadar internet bankacılığı ile para transferi işleminde esasen TCK m. 244 kapsamında sistemde var olan verilerin başka bir yere gönderilmesi hareketi mevcut olsa da failin söz konusu fiil ile elde etmek istediği hesaptaki verinin temsil ettiği paradır[490]. Ayrıca benzer bir fiilin kamu görevlisi tarafından işlenmesi durumunda da TCK m. 247[491] kapsamında zimmet suçu oluşacağını ifade edebiliriz.

Kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçu, TCK m. 136'da *"kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır."* şeklinde düzenlenmiştir. Buna göre failin bir bilişim sisteminde depolanan kişisel veriyi, bulunduğu sistemden başka bir bilişim sistemine *"göndermesi"* ve bu suretle haksız bir yarar elde etmesi durumunda, fiil hem TCK m. 136 hem de TCK m. 244/4 anlamında tipik olacaktır. Ancak TCK m. 136'da suçun oluşumu açısından haksız yarar sağlama aranmadığından bu suç TCK m. 244/4'ün asli normu olabilecek bir suç değildir. Zira TCK m. 244/4'te *"haksız bir çıkar sağlamasının başka bir suç oluşturmaması"* ifadesi kullanılmıştır. Dolayısıyla eğer bu fiil sonucunda *"haksız bir çıkar sağlanması"* neticesi gerçekleşirse tek fiil ile hem TCK m. 136 hem de TCK m. 244/4'deki suç oluşacağından farklı neviden fikri içtima kuralı (TCK m. 44) gereğince sorumluluk TCK m. 244/4'ten olacaktır.

---

489 *"TC Ziraat Bankasında görev yapan sanıkların, bankanın özel işlem servisinde emekli maaşı alanlar için çıkartılıp sahipleri tarafından alınmayan ve bankada bekleyen banka kart ve şifreleri kullanarak şubede bulunan gizli şifreli bilgisayardan geçerli kılıp şube dışındaki ATM makinelerinden çekerek, bu parayı mal edindiklerinin iddia edilmesi karşısında, Ceza Genel Kurulunun 08.02.2005 gün ve 2004/146 E. 2005/7 sayılı kararında da açıklandığı üzere sübutu halinde eylemin hüküm tarihinde yürürlükte olan 4389 sayılı Bankalar Kanunu'nun 22/3. madde ve fıkrasındaki (01.11.2005 tarihinde yürürlüğe giren 5411 saylı Bankacılık Kanunun 160. maddesindeki) suçu oluşturup oluşturmayacağının ve delillerin takdiri görevinin üst dereceli Ağır Ceza Mahkemesine ait olduğu"* (*Y 11. CD, E. 2007/2115, K. 2007/7433, T. 01.11.2007,* Aktaran: **Baş**, Banka veya Kredi Kartlarının, s. 342.)

490 **Dülger**, Bilişim Suçları, s. 603; **Koca**, Bilişim Sistemlerinin Kullanılması Suretiyle Haksız Yarar, s. 1657.

491 **TCK m. 247/1:***"Görevi nedeniyle zilyetliği kendisine devredilmiş olan veya koruma ve gözetimiyle görevli olduğu malı kendisinin veya başkasının zimmetine geçiren kamu görevlisi, beş yıldan oniki yıla kadar hapis cezası ile cezalandırılır."*

8. MUHAKEME VE YAPTIRIM

Bilişim sistemleri aracılığıyla haksız yarar sağlama suçu, dar anlamda bir bilişim suçudur. Başka bir ifadeyle bilişim sistemleri olmaksızın bu suçun işlenmesi mümkün değildir.

Bilişim suçlarının kendine özgü yapısı bu suçlarla mücadelede klasik suçlardan farklı bir usulü gerekli kılmaktadır. Bu gereklilik gerek suçun soruşturulmasından gerekse de kovuşturulmasında karşımıza çıkmaktadır. Biz de inceleme konumuz olan suç bağlamında bu başlıkta suçun soruşturulması ve kovuşturulması bakımından ortaya çıkacak özellikli durumları inceleyeceğiz. Ayrıca bu başlıkta TCK m. 244/4'ün tali norm olmasının suçun yaptırımı bakımından ortaya çıkarabileceği tutarsız durumlara işaret edeceğiz.

8.1. Muhakeme

Ceza muhakemesi; iddia, savunma ve yargılamadan oluşan ve soruşturma ile kovuşturma olmak üzere iki aşamada tamamlanan bir faaliyettir[492]. Soruşturma aşaması, davanın maddi gerçeğe uygun biçimde sonuçlandırılmasını sağlamaya yönelik olarak kovuşturma aşamasının hazırlık evresini oluşturur[493]. Bu anlamda soruşturma aşamasının, asıl işlevi delilleri arayıp bulmak ve koruma altına almaktır[494]. Soruşturma aşamasında toplanan delillerden iddiaların asılsız olduğu kanaatine varılırsa, muhakemede kovuşturma aşamasına geçilmeyecektir[495].

Suç haberinin alınmasıyla soruşturmanın mecburiliği ilkesi gereği, soruşturma savcılık tarafından resen başlatılır ve yürütülür[496]. Soruşturma sonucunda toplanan deliller, suçun işlendiği hususunda yeterli şüphe oluşturursa kovuşturma aşamasına yani kamu davasının açılması aşamasına geçilir[497]. Ancak bazı hallerde, soruşturmanın veya kovuşturmanın

---

[492] **Özbek, Veli Özer/Doğan, Koray/Bacaksız, Pınar/Tepe, İlker**; Ceza Muhakemesi Hukuku, Ankara 2017, s. 40, 41; **Toroslu, Nevzat/Feyzioğlu, Metin**; Ceza Muhakemesi Hukuku, Ankara 2016, s. 262.

[493] **Centel, Nur/Zafer, Hamide**; Ceza Muhakemesi Hukuku, İstanbul 2015, s. 79.

[494] **Centel/Zafer**, Ceza Muhakemesi Hukuku, s. 79; **Öztürk, Bahri/Tezcan, Durmuş/Erdem, Mustafa Ruhan/Sırma Gezer, Özge/Saygılar Kırıt, Yasemin/Özaydın, Özdem/… Erden Tütüncü, Efser**; Nazari ve Uygulamalı Ceza Muhakemesi Hukuku, Ankara 2016, s. 581.

[495] **Toroslu/Feyzioğlu**, Ceza Muhakemesi Hukuku, s. 271; **Soyaslan**, **Doğan**; Ceza Muhakemesi Hukuku, Ankara 2014, s. 364.

[496] **Centel/Zafer**, Ceza Muhakemesi Hukuku, s. 621.

[497] **Öztürk ve diğerleri**, Ceza Muhakemesi Hukuku, s. 602; **Yenisey, Feridun/Nuhoğlu, Ayşe**; Ceza Muhakemesi Hukuku, Ankara 2016, s. 558.

başlatılması belli koşulların gerçekleşmesine bağlı tutulmuş olabilir ki bunlara muhakeme şartları denir[498].

İnceleme konumuz suç açısından üzerinde durulması gereken muhakeme şartı, şikâyettir. Şikâyet, belli suçlardan zarar görenlerin ceza kovuşturmasının belli sakıncalarına karşı korunmaları amacı ile kanunla konulmuş bir engeli, suçun muhakemesinin yapılabilmesi için kaldırma işlemidir[499]. Bilişim sistemleri aracılığıyla haksız yarar sağlama suçunun (244/4) asli normu niteliğindeki bilişim sistemi aracılığıyla hırsızlık (m. 142/2-e) ve dolandırıcılık (158/1-f) suçlarının bir hukuki ilişkiye dayanan alacağı tahsil amacıyla işlenmesi bakımından, kanun koyucu şikâyet muhakeme şartının gerçekleşmesini aramışken inceleme konumuz suç bakımından böyle bir muhakeme şartı aramamıştır.

Bu bağlamda failin hukuki bir ilişkiye dayanan alacağı tahsil amacıyla işlediği fiil, hem bilişim sistemi aracılığıyla hırsızlık ya da dolandırıcılık hem de bilişim sistemi aracılığıyla haksız yarar sağlama suçunu oluşturduğu ve suçtan zarar görenin bu fiil ile ilgili şikâyette bulunmadığı durumda soruşturma ve kovuşturmanın TCK m. 244/4 bakımından icra edilip edilemeyeceğinin belirlenmesi gerekmektedir.

Öncelikle belirtmek gerekir ki fikri içtima ilişkisinden söz edebilmek için ilgili suç tipleri açısından aranan muhakeme şartlarının da gerçeklemesi gerekir[500]. Muhakeme şartlarının gerçekleşmediği suçlar, fikri içtima ilişkisinde göz önüne alınmazlar. Dolayısıyla tek fiille işlenen iki suçtan biri resen, diğeri şikâyete tabi olarak takip ediliyorsa, şikâyet şartı gerçekleşmeyen suç, fikri içtima ilişkisi içerisinde dikkate alınmayacak ve resen kovuşturulan suçun cezası daha hafif olsa dahi fail bu suçtan dolayı cezalandırılacaktır[501].

İnceleme konumuz olan suç ile bilişim sistemi aracılığıyla hırsızlık (TCK m. 142/2-e) ya da dolandırıcılık (TCK m. 158/1-f) suçları arasında ise bir fikri içtima değil, görünüşte içtima ilişkisi söz konusudur[502]. Dolayısıyla fikri içtima ilişkisinde geçerli olan söz konusu durumun bu suçlar bakımından uygulanmayacağı kanaatindeyiz. Zira TCK m. 244/4'ün asli normu olan bilişim sistemi aracılığıyla hırsızlık ve dolandırıcılık suçları, işlenen fiile

---

498 **Öztürk ve diğerleri**, Ceza Muhakemesi Hukuku , s. 44.

499 **Yenisey/Nuhoğlu**, Ceza Muhakemesi Hukuku, s. 575.

500 **Göktürk**, Fikri İçtima, s. 208.

501 **Göktürk**, Fikri İçtima, s. 208.

502 **Koca**, Hukukumuzda TCK'nın 244'ncü maddesi, s. 97.

uygulanacak tek normdur[503]. Şu hâlde fail bir hukuki ilişkiye dayanan alacağı tahsil amacıyla tek bir fiille hem TCK m. 244/4'ü hem de TCK m. 142/2-e ya da TCK m. 158/1-f'yi gerçekleştirmiş olsa ve suçtan zarar gören bu fiilden dolayı şikâyette bulunmamış olsa dahi failin TCK m. 244/4'ten sorumluluğu doğmayacaktır.

Çalışmamızın birinci bölümünde AKSSS bahsinde de belirtildiği üzere bilişim suçlarının kendine özgü yapısı bu suçlarla ilgili delil elde etme ve değerlendirmede özel bir usul gerekliliğini ortaya çıkarmıştır. Doktrinde konuyla ilgili olarak bir *bilişim suçlarıyla mücadele kanununun* gerekliliği ifade edilmektedir. Hatta bu ihtiyacı karşılamak için *"Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı"*nın 6. bölümünde *"Soruşturma ve Kovuşturma Usulleri"* başlığı düzenlenmiş ancak tasarı yasalaşmamıştır.

Bilişim suçlarının, suçla mücadelede ortaya çıkan, kendine has özellikleri çalışmamızın birinci bölümünün AKSSS bahsinde detaylıca ele alınmıştır. Bu bölümde ise bilişim suçları bakımından elde edilmesi gereken delillerin niteliği ve bu süreçte ortaya çıkacak sorunlara değinilecektir.

Ceza muhakemesinde delil serbestisi ilkesi geçerli olsa da bu serbesti sınırsız değildir. Zira delillerin maddi gerçeği ortaya çıkarabilecek nitelikte olması gerekmektedir[504]. Bunun için elde edilen delillerin, *gerçekçi, temsil edici, akılcı, elde edilebilir, kanuna uygun* ve *müşterek* olması gerekmektedir[505]. Bilişim suçlarında maddi gerçeğin ortaya çıkarılması için elde edilmesi gereken deliller ise büyük çoğunlukla *elektronik/dijital* delillerdir. Elektronik delil, ceza muhakemesinde maddi gerçeği tamamen veya kısmen ortaya çıkarabilecek nitelikte, elektronik ortamda tutulan, oluşturulan, depolanan, iletilen her türlü delildir[506]. Bu anlamda elektronik delil de esasında bir bilişim sistemi verisidir. Elektronik delil, elektronik verinin bulunduğu her ortamdan elde edilebilir. Bu ortamlara şunlar örnek verilebilir[507]:

---

503 **Hakeri**, Genel Hükümler, s. 639.

504 **Soyaslan**, Ceza Muhakemesi Hukuku, s. 438; **Şahin, Cumhur/Göktürk, Neslihan**; Ceza Muhakemesi Hukuku- II, Ankara 2017, s. 28.

505 Bu özelliklerin detaylı açıklaması için bkz. **Özen/Özocak**, Adli Bilişim, s. 57,58.

506 **Değirmenci**, Sayısal Delil, s. 31.

507 Detaylı bilgi için bkz. **Değirmenci**, Sayısal Delil, s. 143–158.

bilgisayarlar, veri taşıma araçları, taşınabilir telefonlar, bilişim sistemi ağları, GPS (Global Positioning System) cihazları, elektronik postalar, sosyal medya, bulut bilişim[508].

Elektronik delilin bir bilgisayar verisi olması bu delillerin öncelikle gözle görülemez nitelikte olmasına neden olmaktadır[509]. Elektronik delil insan için, ancak bir bilişim sistemi ile anlaşılabilir olmaktadır. Elektronik delillerin bu *"sanal"* niteliği bu delilleri hassas, kolay tahrif edilebilir, aslına uygun muhafazası zor ve yargı makamlarına izahı güç hale getirmektedir.

Elektronik delillerin bu özellikleri bir bilim dalı olarak adli bilişimi (computer forensics) ortaya çıkarmıştır[510]. Adli bilişim, *"mahkemelerde delil olarak kullanılabilmesi amacıyla bilişim sistemlerinde veya sistem aygıtlarında yer alan verinin bilimsel olarak analizi ve tetkiki süreci"* [511] olarak tanımlanmaktadır. Diğer bir deyişle, adli bilişim, muhakeme hukuku kurallarının sayısal ortama uyarlanmış şekli ya da sayısal ortamda delil elde etme yöntemidir[512]. Dolayısıyla adli bilişimin temel varlık sebebi, elektronik delillerin eksiksiz ve tarafsız bir şekilde adli birimlere sunulmasını sağlamaktır[513]. Adli bilişimin temel varlık sebebi bu olsa da esasen dünyada üzerinde anlaşılmış genel geçer bir elektronik delil araştırma yöntemi bulunmamaktadır[514].

Elektronik delillerin elde edilmesi ve değerlendirilmesi, teknik bilgiyi gerektirdiğinden kanun koyucu, 01.09.2016 tarihli 674 sayılı KHK ile 2659 sayılı Adli Tıp Kurumu Kanunu'nun 8. maddesinin birinci fıkrasına *"g"* bendi ekleyerek *"Adli Bilişim İhtisas Dairesi"*ni kurmuştur. 2659 sayılı Adli Tıp Kurumu Kanununun 22/A maddesine göre dairenin görevleri, *"Mahkemeler ile hakimlikler ve savcılıklar tarafından talep edilen bilişim ile ilgili konularda gerekli incelemeleri yapmak; veri toplama, işleme, depolama veya aktarma işlevi gören bilişim sistemleri ile her türlü sayısal ve elektronik materyal üzerinde inceleme, araştırma ve analizleri yapmak, sonuçlarını bir raporla tespit."* etmektir.

---

[508] **Başlar**, Ceza Yargılamasında Elektronik Delil, s. 76–84.

[509] **Balı**, **Yunus**; "*Adli Bilişim Rapor Metinlerinin Yargılama Sürecinde Kullanımı ve Anlamlandırılabilirliği*", Ses Görüntü ve Data İncelemeleri, Ankara 2008, s. 235: *"Hiçbir elektronik delil, diğer delillerle desteklenmediği sürece doğrudan kişilerle irtibatlandırılamaz. Diğer bir ifadeyle, elektronik deliller, DNA, parmak izi vs. biyolojik delillerde olduğu gibi bizi doğrudan bireye götürmez."*

[510] **Keser Berber, Leyla**; Adli Bilişim, Ankara 2004, s. 39.

[511] **Değirmenci**, Sayısal Delil, s. 66.

[512] **Özen/Baştürk**, Bilişim – İnternet ve Ceza Hukuku, s. 92.

[513] **Özen/Özocak**, Adli Bilişim, s. 45.

[514] **Tanrıkulu**, Bilişim Sistemlerinde Arama ve Elkoyma, s. 74.

Dolayısıyla elektronik delillerin toplanması ve değerlendirilmesi bakımından hâkim veya savcılar, bilirkişi olarak adli tıp kurumuna başvurduğunda konuyla ilgili olarak bu daire görev alacak ve bu daireden gelen rapor, bilirkişi görüşü[515] bağlamında delil olarak hükme esas alınabilecektir.

Türk Hukuku'nda elektronik delillerin elde edilmesi ilgili olarak temel kanuni düzenleme CMK m. 134'tür[516]. Bu madde uyarınca bir suç dolayısıyla yapılan soruşturmada şüphelinin kullandığı bilgisayarda arama yapılabilmesi için somut delillere dayanan kuvvetli şüphenin varlığı ve başka suretle delil elde etme imkanının bulunmaması şartı aranmıştır. Ayrıca elkoyma tedbiri açısından bu şartlara ek olarak bilgisayarın bulunduğu yerde şifresinin çözülememesi veya gizlenmiş bilgilere ulaşılamaması şartı öngörülmüştür. CMK m. 134 de her koruma tedbirinde olduğu gibi kişilerin temel hak ve özgürlüklerine müdahale niteliği taşımaktadır[517]. Bu koruma tedbirinde esasen kişilerin özel hayatlarının gizliliğine müdahale[518] söz konusu olduğundan kanun koyucu bu tedbirin uygulanmasında yukarıda sayılan ağır şartları gerekli görmüştür. Ayrıca elkoyma tedbiri açısından kanun koyucu elektronik delillerin hassas ve tahrif edilmeye müsait olması nedeniyle sistemdeki bütün verilerin yedeklemesinin yapılmasını ve yapılan bu yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilmesini öngörmüştür.

Elektronik delillerin elde edilebileceği tek koruma tedbiri, CMK m. 134 değildir. Bunun yanında *"telekomünikasyon yoluyla yapılan iletişimin denetlenmesi"* (CMK m. 135)[519] ve *"teknik araçlarla izleme"* (CMK m. 140)[520] koruma tedbirleri ile de elektronik veri elde edilmektedir.

Elektronik deliller; belge, beyan ve belirti delili ayrımında[521], kimi zaman belge delili niteliğinde kimi zaman belirti delili niteliğinde olmaktadır[522]. Örneğin, suçun işlendiği anı

---

[515] Bilirkişi görüşünün hukuki niteliğine ilişkin farklı görüşler için bkz. **Centel/Zafer**, Ceza Muhakemesi Hukuku, s. 274.

[516] **Yılmaz**, Siber Suçlar, s. 126.

[517] **Soyaslan**, Ceza Muhakemesi Hukuku, s. 275.

[518] **Öztürk ve diğerleri**, Ceza Muhakemesi Hukuku, s. 407.

[519] Detaylı bilgi için bkz. **Meran**, **Necati**; İletişimin Denetlenmesi, Gizli Soruşturmacı ve Teknik Takibin Hukuki Boyutu, Ankara 2015, s. 1–287.

[520] Detaylı bilgi için bkz. **Meran**, İletişimin Denetlenmesi, Gizli Soruşturmacı ve Teknik Takibin Hukuki Boyutu, s. 501–576.

[521] Bu ayrım için bkz. **Centel/Zafer**, Ceza Muhakemesi Hukuku, s. 223.

[522] **Değirmenci**, Sayısal Delil, s. 130.

kayda alan kameradaki delil, bir belge delili niteliği taşıyacakken; TCK m. 244/4'e ilişkin olarak, haksız yarar sağlanan sistemdeki sayısal izler, belirti delili niteliği taşıyacaktır[523]. Dolayısıyla her elektronik delil, esas uyuşmazlığı doğrudan çözmede yeterli olmadığından elektronik delillerin başka bir belge veya beyan deliliyle desteklenmesi gerekebilecektir.

Bilişim sistemi aracılığıyla haksız yarar sağlama suçu bakımından elde edilecek delillerin kanuna uygun ve dolayısıyla maddi gerçeği ortaya çıkarmaya elverişli olabilmesi için CMK m. 134'e uygun olması gerekmektedir. Aksi durumda elde edilen deliller, hukuka aykırı delil niteliğinde olacak ve hükme esas alınamayacaktır (CMK m. 206/2-a)[524].

Nitekim Yargıtay 19. CD 2015 tarihli bir kararında: *"Müşteki vekilinin şikayeti üzerine başlatılan soruşturmada, ... 1. Sulh Ceza Mahkemesi'nin 21/08/2009 tarihli, 2009/1034 D. İş sayılı kararında, CMK'nın* 119. *maddesi uyarınca sanık tarafından işletilen iki ayrı işyerinde arama yapılmasına karar verilmesine karşın, aynı işyerinde bulunan bilgisayarlar üzerinde arama yapılabilmesine olanak tanıyan CMK'nın* 134. *maddesine göre verilmiş bir arama kararı bulunmadığı anlaşılmakla, işyerinde bulunan bilgisayarlar üzerinde yapılan arama sonucunda elkonulan ve içerisinde müşteki firmaya ait lisanssız yazılımların olduğu belirtilen harddiskler ve CD'ler hukuka aykırı delil niteliğinde olup hükme esas alınamayacağından, sanık hakkında verilen beraat kararı usul ve yasaya uygundur."*[525] ifadesiyle CMK m. 134'e aykırı şekilde elde edilen delillerin hukuka aykırı olacağından bahisle bu delillerin hükme esas alınamayacağına hükmetmiştir.

Bu açıklamalardan hareketle, Cumhuriyet Savcısı, toplanan delillerle, bilişim sistemi aracılığıyla haksız yarar sağlama suçunun işlendiği hususunda yeterli şüphe oluştuğu kanaatine varırsa, kamu davasının mecburiliği ilkesi uyarınca (CMK m. 170/2), iddianame düzenlemek zorundadır[526]. Düzenlenen iddianamenin, mahkeme tarafından kabulü durumunda, yargılamada kovuşturma aşamasına geçilmiş olacak, başka bir ifadeyle kamu davası açılmış olacaktır (CMK m. 175)[527].

---

[523] **Değirmenci**, Sayısal Delil, s. 130.

[524] **Toroslu/Feyzioğlu**, Ceza Muhakemesi Hukuku, s. 174.

[525] *Y 19. CEZA DAİRESİ E. 2015/2092 K. 2015/1175 T. 6.5.2015*. (kazanci.com – s.e.t: 07.06.2017)

[526] **Özbek/Doğan/Bacaksız/Tepe**, Ceza Muhakemesi Hukuku, s. 574; **Soyaslan**, Ceza Muhakemesi Hukuku, s. 364.

[527] **Yenisey/Nuhoğlu**, Ceza Muhakemesi Hukuku, s. 692.

8.2. Görevli ve Yetkili Mahkeme

Ceza muhakemesi açısından görevli mahkeme, 5235 sayılı Adlî Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanun'un 8. vd maddeleri uyarınca belirlenmektedir[528]. TCK m. 244/4 bağlamında suçun yaptırımının üst sınırı 6 yıl hapis cezası olduğundan 5235 sayılı Kanun'un 11. 12. ve 14. maddeleri göz önünde bulundurularak, görevli mahkemenin asliye ceza mahkemesi olduğunu ifade edebiliriz.

TCK m. 244/4 için yetkili mahkemeyi belirlemek, görevli mahkemeyi belirlemekten daha güçtür. Zira söz konusu suç, çoğu zaman bir mesafe suçu[529] olarak karşımıza çıkmakta ve ülke içinde işlenen mesafe suçlarına ilişkin suçun işlendiği yer hususunda CMK'da bir düzenleme bulunmamaktadır.

Bilişim suçlarına ilişkin yetki ve uygulanacak kanun bakımından TCK ve CMK'da özel bir düzenleme yapılmamıştır. Milli yetkide genel kural olarak *"yer bakımından uygulama"* başlıklı TCK m.8'de *"Türkiye'de işlenen suçlar hakkında Türk kanunları uygulanır. Fiilin kısmen veya tamamen Türkiye'de işlenmesi veya neticenin Türkiye'de gerçekleşmesi halinde suç, Türkiye'de işlenmiş sayılır."* hükmüyle mülkilik ilkesi kabul edilmiş olmaktadır[530]. Buna göre fiil kısmen ya da tamamen Türkiye'de işlenmiş yahut netice Türkiye'de gerçekleşmiş ise fail ve mağdurun vatandaşlığına bakılmaksızın fiil ile ilgili olarak Türk Ceza Kanunu uygulama alanı bulacak ve Türk mahkemeleri yetkili olacaktır. Mülkilik ilkesinin yanı sıra suç Türkiye'de işlenmemiş olsa dahi faile göre şahsilik (TCK m.11), mağdura göre şahsilik (TCK m. 12) ve evrensellik ilkeleri (TCK m. 14) uyarınca da bazı suçlar açısından Türk Ceza Kanunu uygulama alanı bulacaktır[531].

Bilişim sistemi ile haksız yarar sağlama suçu bakımından da failin gerçekleştirdiği fiilin, failin ülke içinde ya da ülke dışında bulunmasına bakılmaksızın, bir kısmı Türkiye'de gerçekleşiyorsa TCK m. 244/4 uygulama alanı bulacaktır[532]. Bu durumda örneğin, ülke

---

[528] **Şahin**, **Cumhur**; Ceza Muhakemesi Hukuku- I, Ankara 2016, s. 219.

[529] **Dönmezer/Erman**, Nazari ve Tatbiki Ceza Hukuku, s. 318: *"Hareketin yapıldığı yer ile neticenin gerçekleştiği yer arasında yargısal veya siyasal sınırın bulunduğu 'mesafe suçları' ise bu konuda özellikli bir durum arz ederler."*

[530] **Centel/Zafer**, Ceza Muhakemesi Hukuku, s. 63; **Soyaslan**, Ceza Muhakemesi Hukuku, s. 98.

[531] Bu ilkeler hakkında detaylı bilgi için bkz. **Soyaslan**, Ceza Muhakemesi Hukuku, s. 101–110.

[532] **Dönmezer/Erman**, Nazari ve Tatbiki Ceza Hukuku, s. 327, 328: *"Özellikle güncel bir sorun, internet yoluyla işlenen suçlar bakımından suçun işlendiği yerin tespitidir. 2001 tarihli Avrupa Konseyi Siber Suç*

dışındaki bir fail, internet üzerinden ülke içindeki bir mağdurun bilişim sistemindeki verilere ulaşarak buradaki verileri ülke dışına aktarmak suretiyle bir yarar elde ediyorsa failin sorumluluğu TCK m. 244/4 bakımından doğacaktır. Zira bu durumda fail, ülke içindeki bir bilişim sistemine erişerek fiili gerçekleştirdiğinden, fiil kısmen ülke içinde gerçekleştirilmiş olacaktır.

Ülke içinde yetkili mahkemenin belirlenmesinde ise genel kural *"yetkili mahkeme"* başlıklı CMK m. 12'de *"(1) Davaya bakmak yetkisi, suçun işlendiği yer mahkemesine aittir. (2) Teşebbüste son icra hareketinin yapıldığı, kesintisiz suçlarda kesintinin gerçekleştiği ve zincirleme suçlarda son suçun işlendiği yer mahkemesi yetkilidir."* şeklinde düzenlenmiştir[533]. Ayrıca CMK m. 13'te suçun işlendiği yerin belli olmaması durumuna ilişkin olarak özel yetki kuralı getirilmiştir[534]. CMK m. 13'e göre bu durumda *"1) Suçun işlendiği yer belli değilse, şüpheli veya sanığın yakalandığı yer, yakalanmamışsa yerleşim yeri mahkemesi yetkilidir. (2) Şüpheli veya sanığın Türkiye'de yerleşim yeri yoksa Türkiye'de en son adresinin bulunduğu yer mahkemesi yetkilidir. (3) Mahkemenin bu suretle de belirlenmesi olanağı yoksa, ilk usul işleminin yapıldığı yer mahkemesi yetkilidir."*

CMK'nın yetkili mahkemeyi belirlemek için getirdiği *"suçun işlendiği yer"* ölçütü TCK m. 244/4 bakımından her zaman kesin sonuç verecek bir ölçüt değildir. Zira bu suçta, genel olarak bilişim suçlarında olduğu gibi, hareket ve netice çoğu zaman farklı yerlerde gerçekleşmektedir. Failin sisteme, sistemin bulunduğu yerde, fiziki müdahale ile suçu işlemesi durumunda böyle bir problem ortaya çıkmayacak olsa da suçun, sisteme uzaktan

---

Sözleşmesi'nde bu konuya dair bir hükme yer verilmediğinden, meseleyi TCK m. 8 çerçevesinde ele almak gerekmektedir. Aslında, İnternet içeriğine dünyadaki her ülkeden erişmek mümkündür; bu bakımdan, içeriğe ulaşma olanağı bulunan her ülkede suçun işlendiğini kabul etmek mümkün olabilirdi; ne var ki, bu çözüm yolu Türkiye'yi baş edilemeyecek bir yük altına sokabileceği ve uluslararası alanda ciddi yetki çatışmalarını doğuracağı için, doktrinde daha sınırlı bir yaklaşıma gidilmektedir. Bu bakımdan, bir görüşe göre, suç niteliği taşıyan internet içeriklerinin Türkiye'de bilgisayara veya 'server' a (sunucuya) yüklenmesi koşuluyla suçun Türkiye'de işlenmiş sayılabileceği savunulmaktadır. Daha geniş bir görüşe göreyse; sunucu yurt dışında olsa bile, verileri buna yüklemede araç olarak kullanılan ve failin fiziksel olarak başında bulunduğu bilgisayar Türkiye' de ise veya fiziksel olarak yabancı ülkede bulunan bir kimse Türkiye'de bulunan bir bilgisayar ağına dahil olup verileri yüklemişse ya da suç içerikli veri Türkiye'de kurulu bir sunucuya yüklenmişse, suç Türkiye'de işlenmiş sayılmalıdır. Kanaatimizce, yetki çatışmalarını önlemek ve bis in idem riskini en aza indirgemek açısından, yargılamayı gerçekleştirecek devlet ile fiil veya fail arasında bazı bağlantı noktalarının varlığını aramak yerinde olacaktır. Bu bakımdan, en azından, İnternet yoluyla işlenen suçları dünyanın her ülkesinde işlenmiş saymamak gerekir."

[533] **Özbek/Doğan/Bacaksız/Tepe**, Ceza Muhakemesi Hukuku, s. 632; **Öztürk ve diğerleri**, Ceza Muhakemesi Hukuku, s. 206.

[534] **Öztürk ve diğerleri**, Ceza Muhakemesi Hukuku, s. 206.

erişim yoluyla, söz gelimi internet vasıtasıyla, işlenmesi durumunda hareket ve netice farklı yerlerde gerçekleşeceğinden yetkili mahkemenin belirlenmesi problemi ortaya çıkacaktır[535].

Hareket ve neticenin farklı yerlerde gerçekleştiği suçlara ilişkin olarak suçun işlendiği yerin tespit edilmesinde doktrinde üç farklı görüş bulunmaktadır[536]. Birinci görüşe göre önemli olan insan iradesinin ortaya konulması olduğundan, suç, hareketin işlendiği yerde işlenmiştir. İkinci görüşe göre ise suçla korunması amaçlanan değer ancak neticenin doğmasıyla ihlal edildiğinden, suç, neticenin gerçekleştiği yerde işlenmiştir. Üçüncü ve karma görüşe göre ise bir ülke içerisinde gerçekleştirilen mesafe suçlarında suç hem hareketin gerçekleştirildiği yerde hem de neticenin gerçekleştiği yerde işlenmiştir[537]. Bu durumda iki yetkili mahkeme olur ki mahkemeler bu hususta anlaşarak, suçun kovuşturulması hususunda uygun mahkemeye karar vereceklerdir.

Kanaatimizce, TCK m. 244/4'ün ülke içinde bir mesafe suçu olarak işlenmesi halinde karma görüşe öncelik verilerek suçun hem hareketin gerçekleştirildiği yerde hem de neticenin gerçekleştirildiği yerde işlenmiş sayılması yerinde olacaktır. Zira böylece hem ülke içinde işlenen mesafe suçları ile bir kısmı ülke dışında işlenen mesafe suçlarında suçun işlendiği yerin tespitinde ortaya çıkacak çelişkinin önüne geçilmiş olacak[538] hem de bilişim suçlarında suçla mücadelede ortaya çıkan güçlükleri aşmak açısından hareketin gerçekleştirildiği ve neticenin gerçekleştiği yerlerden hangisinde ceza muhakemesi şartları olgunlaşmışsa orada suçun kovuşturulmasının yapılması imkânının önü açılmış olacaktır[539].

8.3. Yaptırım

Bilişim sistemi aracılığıyla haksız yarar sağlama suçunun yaptırımı, TCK m. 244/4'te iki yıldan altı yıla kadar hapis ve beşbin güne kadar adli para cezası olarak belirlenmiştir.

---

[535] **Erdoğan**, TCK'da Bilişim Suçları, s. 375: *"Yargıtay 5'nci Ceza Dairesi konuyla ilgili olarak, bu tür eylemlerde (merci tayinine ilişkin) 06.11.2006 gün ve 2006/11791 esas, 200/9930 karar sayılı ilamında, suç yerinin mağdur hesabın bulunduğu yer olduğunu belirtmesine rağmen, aynı daire kısa süre sonra 18.12.2006 gün ve 2006/12623 esas, 2006/10328 karar sayılı ilamında ise, bir önceki kararın tam aksine olarak, bu tür eylemlerde şüpheli hesabın bulunduğu yani paranın aktarıldığı yeri suç yeri olarak kabul etmiştir."*

[536] **Tepe**, İnternet Suçluluğu, s. 191, 192.

[537] **Dönmezer/Erman**, Nazari ve Tatbiki Ceza Hukuku - 1, s. 321.

[538] **Centel/Zafer**, Ceza Muhakemesi Hukuku, s. 560.

[539] **Tepe**, İnternet Suçluluğu, s. 193.

Hâkim, hapis cezasını TCK m. 61'e göre belirleyecek ve TCK m. 62 uyarınca takdiri indirim nedenlerinin varlığı halinde cezayı altıda birine kadar indirebilecektir. TCK m. 244/4'te suçun yaptırımı olarak hapis cezası ve adli para cezası birlikte gösterildiğinden CMK m. 231 kapsamında hükmün açıklanmasının geri bırakılması mümkün değildir[540]. Ancak TCK m. 51 kapsamında, iki yıl veya takdiri indirim nedeninin uygulanması suretiyle daha az hapis cezasına hükmedilmesi durumunda, adli para cezasından bağımsız olarak bu hapis cezasının ertelenmesi mümkün olacaktır[541].

Adli para cezasında ise hâkim, birim gün sayısını TCK m. 61/1'e göre temel ceza olarak belirleyecek ve ardından bir gün karşılığı ödenecek para miktarını, kişinin ekonomik durumu, malvarlığı ile bir günde kazandığı veya kazanması gereken gelire bakarak 20 TL ile 100 TL arasında belirleyecektir[542]. Birim gün sayısının alt sınırı TCK m. 244/4 belirlenmediğinden bu sınır beş gün olarak kabul edilecektir. Zira bu suçta adli para cezasının seçimlik olarak değil hapis cezasının yanı sıra uygulanacağı öngörülmüştür. Üst sınır ise maddede beş bin gün olarak belirlenmiştir.

Adli para cezasının, hapis cezasının yanı sıra uygulanmasının öngörüldüğü suçlarda amaç, suçla elde edilen ekonomik çıkarın tespit edilip kazanç müsaderesine ilişkin hükümlerin uygulanamaması durumunda, suçtan elde edilen gelirin kişinin yanına kâr kalmamasını sağlamaktır[543]. Bundan dolayı bu tür suçlarda genellikle adli para cezasının alt sınırı belirlenmemişken üst sınır da yüksek olarak belirlenmiştir[544]. Söz konusu yaptırımın TCK m. 244/4 bağlamında uygulanmasının amacı da budur zira bu suçta fail bilişim sistemi ile haksız ekonomik kazanç elde etmektedir. Buna göre suçtan elde edilen gelir, tamamen müsadere edilmişse, sanığa artık adli para cezasının verilmemesi düşünülebilir ancak kanun hükmü gereği bu artık mümkün olmadığından, sanığa en azından adli para cezasının kanundaki alt sınırını yani beş günü vermek yerinde olacaktır[545].

---

[540] **Centel/Zafer**, Ceza Muhakemesi Hukuku, s. 764: *"Kurum, suç karşılığında tek tip cezanın öngörüldüğü veya hapis cezası ile adli para cezasının seçimlik ceza olarak öngörüldüğü hallerde uygulanabilir."*

[541] **Koca/Üzülmez**, Genel Hükümler, s. 572: *"Eğer mahkûmiyet kararında hem adli para hem de hapis cezasına hükmedilmişse, sadece hapis cezası ertelenebilecektir."*

[542] **Yerdelen**, Cezanın Belirlenmesi, s. 338, 339.

[543] **Özgenç**, Genel Hükümler, s. 779.

[544] **Özgenç**, Genel Hükümler, s. 779.

[545] **Koca/Üzülmez**, Genel Hükümler, s. 656, 657.

Bilişim sistemleri aracılığıyla haksız yarar sağlama suçuna ilişkin herhangi bir nitelikli hal öngörülmemiştir. TCK m. 244/3'te düzenlenen nitelikli halin 4. fıkraya uygulanması mümkün değildir. Dolayısıyla ilk iki fıkrada gösterilen fiillerin bir banka veya kredi kurumuna yahut bir kamu kurumu veya kamu kuruluşuna ait bilişim sistemlerine ya da bu sistemlerdeki verilere karşı gerçekleştirilmesi suretiyle haksız çıkar sağlanması durumunda cezada artırım yapılamayacaktır.

Bilişim sistemi aracılığıyla haksız yarar sağlama suçunun, fiilin daha ağır ceza gerektiren başka bir suç oluşturmaması halinde değil de daha ağır veya hafif başka bir suç oluşturmaması halinde uygulanması yaptırım hususunda bazı çelişkiler meydana getirmektedir. Örneğin bilişim sistemi aracılığıyla hırsızlık suçunun, bir hukuki ilişkiye dayanan alacağı tahsil amacıyla gerçekleştirilmesi durumunda fail iki aydan bir yıla kadar hapis cezasına muhatap olacaktır. Oysa işlenen fiilin aynı zamanda TCK m. 244/4 bakımından tipik olduğu durumda, bu suçta böyle bir hafifletici neden öngörülmediğinden fail bu suçun yaptırımı olan iki yıldan altı yıla kadar hapis ve beş bin güne kadar adli para cezasından sorumlu olmayacaktır. Bu durum, TCK'nın tek fiil ile birden fazla suç oluşması durumunda failin bu suçlardan daha ağır cezayı gerektiren suçtan dolayı sorumlu olacağına ilişkin fikri içtima hükmüne aykırı olduğundan TCK'nın genel sistematiği açısından çelişki oluşturmaktadır. Maddenin gerekçesinde belirtilen daha ağır cezayı gerektiren başka bir suç oluşturmaması halinde TCK m. 244/4'ün uygulama alanı bulacağına ilişkin ifadeden yola çıkarak suçun uygulama alanını bu şekilde belirlemek, gerekçenin kanun hükmüne dahil olmaması sebebiyle mümkün değildir.

TCK m. 246'da *"bilişim alanında suçlar"* bölümünde düzenlenen suçların işlenmesi suretiyle, tüzel kişi yararına haksız menfaat sağlanması durumunda tüzel kişilere özgü güvenlik tedbirlerine hükmolunacağı belirtilmiştir. Dolayısıyla bilişim sistemi aracılığıyla haksız yarar sağlama suçu bakımından da tüzel kişilere özgü güvenlik tedbirlerine hükmetmek mümkündür. Tüzel kişilere özgü güvenlik tedbirleri TCK m. 60'a göre faaliyet izninin iptali ve müsaderedir[546]. Tüzel kişilere özgü güvenlik tedbirleri, TCK m. 60 uyarınca ancak özel hukuk tüzel kişileri hakkında ve bu tüzel kişilere, işlenen suç ile haksız bir menfaat elde edilmesi durumunda uygulanabilir[547].

[546] **Demirbaş**, Genel Hükümler, s. 661.

[547] **Akbulut**, Genel Hükümler, s. 826.

Faaliyet izninden maksat, TCK m. 60'da da belirtildiği üzere, bir kamu kurumunun verdiği faaliyet iznidir. Faaliyet izninin iptali güvenlik tedbirine hükmedilmesi halinde tüzel kişilik sona ermez[548]. Bu güvenlik tedbirine hükmedilebilmesi için suçun, tüzel kişinin organ veya temsilcisi tarafından gerçekleştirilmesi ve suçu işleyen ya da suça iştirak eden organ veya temsilci hakkında mahkumiyete karar verilmiş olması gerekmektedir[549]. Ayrıca organ veya temsilcinin işlediği suçun, faaliyet izninin sağladığı yetkinin kötüye kullanılması suretiyle işlenmesi gerekmektedir. Dolayısıyla işlenen suç ile verilen faaliyet izninin kullanılması arasında bir nedensellik bağının bulunması gerekmektedir[550].

Faaliyet izninin yanında tüzel kişi hakkında eşya veya kazanç müsaderesine hükmedilmesi de mümkündür. TCK m. 60/2'de müsadere için aranan tek şart işlenen suç ile tüzel kişi yararına bir menfaat elde edilmiş olmasıdır[551]. Buna göre, tüzel kişi yararına işlendiği belirlenen TCK m. 244/4 bakımından, müsadere hükümlerindeki koşulların da gerçekleşmesi şartıyla, suçla bağlantılı olan eşya veya maddi çıkarların müsaderesi mümkündür.

Ayrıca TCK m. 60/3'te lehine haksız menfaat elde edilen tüzel kişi hakkında güvenlik tedbirinin uygulanmasının işlenen fiile nazaran daha ağır sonuçlar ortaya çıkaracağı durumlarda hâkimin bu tedbirlere hükmetmeyebileceği ifade edilmiştir. Bu durumda hâkim, suçun verdiği zarar ile tedbirin verilmesi ile ortaya çıkacak zararı karşılaştırmalı ve tedbir uygulandığında daha büyük bir zarar ortaya çıkıyorsa, söz konusu tedbire hükmetmemelidir[552].

---

548 **Akbulut**, Genel Hükümler, s. 827.

549 **Öztürk/Erdem**, Ceza Hukuku ve Güvenlik Tedbirleri Hukuku, s. 535.

550 **Artuk/Gökcen/Yenidünya**, Genel Hükümler, s. 967.

551 **Öztürk/Erdem**, Ceza Hukuku ve Güvenlik Tedbirleri Hukuku, s. 535.

552 **Gedik, Doğan**; Müsadere, Ankara 2007, s. 154.

SONUÇ

"Bilişim sistemi aracılığıyla haksız yarar sağlama suçu", 5237 sayılı TCK'nın *"topluma karşı suçlar"* kısmının, onuncu bölümü olan *"bilişim alanında suçlar"*da yer almaktadır. TCK'nın 244. maddesinin 4. fıkrasındaki *"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."* düzenlemesi, kanuni tanımda geçen *"yukarıdaki fıkralarda tanımlanan fiiller"*den ya da suçlardan bağımsız bir suç teşkil etmektedir. Zira söz konusu bu düzenlemede, TCK m. 244/1 ve 2'den farklı bir maddi ve manevi unsur söz konusudur. Maddi unsurda, ilk iki fıkradaki fiillerin işlenmesi neticesinde haksız bir çıkar elde edilmeli; manevi unsurda ise kastın haksız bir çıkar elde etmeye yönelik olması gerekmektedir. Öte yandan kanun koyucunun TCK m. 244/4'ü, işlenen fiilin başka bir suç oluşturmaması halinde uygulanacak şekilde düzenlemesi ve yaptırım olarak oransal bir belirleme yapmayıp hapis cezasının aşağı ve yukarı sınırlarını belirlemesi de bu fıkranın bağımsız bir suç olduğuna işaret etmektedir.

AKSSS, taraf devletler bakımından sözleşmede düzenlenen suçları iç hukuklarına dahil etme yükümlülüğü getirmektedir. AKSSS'ye taraf olan Türkiye bakımından da aynı yükümlülük söz konusudur. Bu yükümlülüğün bir sonucu olarak kanun koyucu, AKSSS m.8'de düzenlenen *"bilgisayarla bağlantılı dolandırıcılık"* başlıklı hükmü inceleme konumuz olan TCK m. 244/4 ile iç hukuka dahil etmiş bulunmaktadır.

TCK m. 244/4, tali norm olarak düzenlenmiş bir suçtur. Bu suçun düzenlenmesindeki amaç esasen *"bilişim sistemi verisi"*nin, mal veya eşya olarak kabul edilememesinin bir sonucu olarak, bu verilerle, malvarlığına karşı suçlar açısından tipiklik arz etmeyen maddi bir menfaat elde edilmesi fiillerinin cezasız kalmamasını sağlamaktadır.

TCK m. 244/4'te bilişim sistemlerinin doğru ve sağlıklı işlemesine ilişkin toplumdaki güven duygusunun korunmasından ziyade kişilerin malvarlığı hukuki değeri koruma altına alınmıştır. Başka bir ifadeyle TCK m. 244/1 ve 2'deki suçların korunan hukuki değerleri bu

suçta mündemiç olsa da malvarlığı hukuki değeri bu suçta ön plandadır. Zira bu suçta haksız yarar sağlama, tipikliğe dahil edilmiş böylece bilişim sistemlerinin malvarlığı değerine yönelik saldırılarda, araç olarak kullanılmasının önüne geçilmek istenmiştir. Dolayısıyla malvarlığına karşı suçlar bölümünde düzenlenen bilişim sistemi aracılığıyla işlenen hırsızlık ve dolandırıcılık suçlarında korunan hukuki değer kişisel bir nitelik arz ederken inceleme konumuz suçta korunan hukuki değer sadece kişisel değil aynı zamanda toplumsal bir nitelik arz etmektedir.

Suçun konusu, doktrindeki hâkim görüşün de belirttiği üzere, failin hukuka aykırı sağladığı yarardır. Suçun tali norm olarak düzenlenmesi ve düzenlenmesindeki amaç ile suç ile korunan hukuksal değer göz önüne alındığında failin sağladığı hukuka aykırı yararın maddi nitelikte olması gerektiği ifade edilebilir. Manevi yararın da bu fıkra kapsamında değerlendirilmesi durumunda, olayların çoğunda faillerin manevi tatmin amacıyla suç işledikleri göz önüne alınarak, TCK m. 244/1 ve 2'deki suçların çok istisnai bir uygulama alanı bulacağı öngörülebilir. Öte yandan söz konusu suçun yaptırımı olarak hapis cezasının yanı sıra adli para cezasının da öngörülmesi bu suçta maddi yararın elde edilmesi gerektiğine işaret etmektedir. Zira adli para cezasının, hapis cezasının yanı sıra uygulanmasının öngörüldüğü suçlarda amaç, suçla elde edilen *"ekonomik çıkarın"* tespit edilip kazanç müsaderesine ilişkin hükümlerin uygulanamaması durumunda, suçtan elde edilen gelirin kişinin yanına kâr kalmamasını sağlamaktır.

Haksız yarar sağlama bir başkasının malvarlığında azalmaya veya beklenen bir yarara engel olmaya neden olacağından, bilişim sistemleri aracılığıyla haksız yarar sağlama bir zarar suçudur. Ancak suçun maddi unsurunda, mağdurun zarara uğraması aranmadığından suçun oluşumu için zararın gerçekleşip gerçekleşmediği araştırılmayacaktır.

Suçun mağduru, bilişim sistemi veya verilere müdahale sonucu malvarlığı itibariyle zarar uğrayan gerçek kişidir. Suçun mağdurunun muhakkak bilişim sisteminin veya sistemdeki verilerin mülkiyetine yahut zilyetliğine sahip olması gerekmez. Suçla elde edilen yarar bu suçun konusu olduğundan ve bu yarar başkalarını malvarlığı itibariyle zarara uğratmak suretiyle elde edildiğinden söz konusu zararın muhatapları mağdur olmaktadır.

TCK m. 244/4, bileşik suç olarak düzenlenmiştir. Buna göre bilişim sistemi ile haksız yarar sağlama suçunda (m. 244/4) failin öncelikle bu suça unsur olarak katılan sistemi engelleme, bozma (m. 244/1); verileri yok etme veya değiştirme (m. 244/2) suçlarındaki neticelerden

birini gerçekleştirmesi ve bunun sonucu olarak da haksız bir çıkar elde etmesi gerekmektedir. Haksız çıkar sağlama, bu suçta netice unsurunu teşkil etmektedir.

TCK m. 244/4, bağlı hareketli bir suçtur. Zira sağlanacak haksız çıkarın hangi hareketlerle gerçekleştirileceği kanunda öngörülmüştür. Buna göre fail haksız çıkarı, bilişim sisteminin işleyişini engelleyerek veya bozarak yahut sistemdeki verileri bozarak, yok ederek, değiştirerek, erişilmez kılarak veya sisteme veri yerleştirerek ya da var olan verileri bir başka yere göndererek elde etmelidir.

TCK m. 244/4, kasten işlenebilen bir suçtur. Bu kapsamda fail, başkasının bilişim sistemini engellediğini, bozduğunu yahut sistemdeki verileri bozduğunu, değiştirdiğini, başka bir yere gönderdiğini ve bu fiilleri işlemek suretiyle kendisi veya başkası için haksız bir yarar elde ettiğini bilmelidir. Yararım haksız olduğuna ilişkin faildeki bilgi, kastın kapsamında değerlendirilmeli, bunun yanında kanuni tanımda manevi unsur olarak amaç veya saike yer verilmediğinden ayrıca failin herhangi bir amaç ya da saikle hareket edip etmediği aranmamalıdır.

Hukuka aykırılık unsuru açısından, *"haksız çıkar sağlanması"* ifadesinin sonucu olarak, suçun kanuni tanımında yalnız yarar sağlama unsuruna ilişkin hukuka aykırılığa vurgu yapıldığından, failin kastının yararın hukuka aykırı olduğunu da kapsaması gerekecektir. Dolayısıyla bu suçun olası kastla işlenmesi mümkün değildir.

TCK m. 244/4 açısından ancak ilgilinin rızası (m. 26/6), bir hukuka uygunluk nedeni teşkil edebilir. Hakkın kullanımı (m. 26/1), meşru müdafaa (m. 25/1) ve kanun hükmünün icrası (m. 24/1) hukuka uygunluk nedenleri, TCK m. 244/1 ve 2 açısından geçerli olabilecek nitelikteyseler de TCK m. 244/4 açısından *"haksız çıkar sağlama*" unsuru bu nedenlerin gerçekleşmesine engel olmaktadır.

TCK m. 244/4 tali norm olarak düzenlenmiştir. Ancak, TCK m. 244/4'ün tali norm olarak düzenlenmesi bu suç ile başka suçların farklı neviden fikri içtima ilişkisine girmeyeceği anlamına gelmez. Buna göre haksız bir yarar sağlamanın suçun kanuni tanımında düzenlenmediği suçlar ile TCK m. 244/4'ün, farklı neviden fikri içtima ilişkisine girmesi olanaklıdır. Zira TCK m. 244/4'te bu hükmün uygulanabilmesi için *"haksız çıkar sağlama"*nın başka bir suça vücut vermemesi aranmıştır.

Bilişim sistemleri vasıta kılınarak gerçek bir kişinin aldatılıp haksız bir yarar elde edilmesi durumunda dolandırıcılık suçu (TCK m. 158/1-f) söz konusu olacak iken bilişim sistemleri vasıta kılınarak bir taşınır malın zilyedinin rızası dışında bulunduğu yerden alınması (örneğin internet bankacılığı yoluyla hukuka aykırı para transferi) durumunda ise hırsızlık (TCK m. 142/2-e) suçu söz konusu olacaktır. Bu hallerde esasen işlenen fiiller, TCK m. 244/4 açısından da tipiktir; ancak, suçun tali norm olması gereği bu madde uygulama alanı bulmayacaktır.

Failin, ATM üzerinden ya da POS cihazından banka veya kredi kartını kullanarak ya da fiziki varlığı bulunmayan kredi kartı numaraları ile internet alışverişi ile kendisi veya başkası yararına haksız çıkar elde etmesi durumunda, sisteme ya da sistemdeki verilere müdahale bulunmamaktadır. Dolayısıyla bu gibi hallerde TCK m. 244/4 bakımından tipiklik oluşmadığından asli norm – tali norm araştırması yapılmayacaktır.

TCK m. 244'ün işlenmesi için muhakkak bilişim sistemine girme suçunun (TCK m. 243) işlenmesi gerekmediğinden bu iki suç arasında geçit suç ilişkisi bulunmamaktadır. Ayrıca bilişim sistemine girme suçunda özel hayatın gizliliği koruma altına alınmışken, TCK m. 244'te bilişim sistemlerinin güvenliğinin yanı sıra bu sistem ve sistemdeki veriler, kişinin malvarlığında bulunan bir değer olarak koruma altına alınmıştır. Dolayısıyla bilişim sistemine girme (TCK m. 243) ile TCK m. 244'teki fiillerin işlenmesi halinde bu iki suçtan ayrı ayrı cezai sorumluluk söz konusu olacaktır.

Failin bir bilişim sisteminde depolanan kişisel veriyi, bulunduğu sistemden başka bir bilişim sistemine *"göndermesi"* ve bu suretle haksız bir yarar elde etmesi durumunda, tek fiil ile hem TCK m. 136 hem de TCK m. 244/4'deki suç oluşacağından farklı neviden fikri içtima kuralı (TCK m. 44) gereğince sorumluluk TCK m. 244/4'ten olacaktır. Zira TCK m. 136'da haksız yarar sağlama söz konusu olmadığından ve TCK m. 244/4'te *"haksız bir çıkar sağlamasının başka bir suç oluşturmaması"* ifadesi gereği bu suç, TCK m. 244/4'ün asli normu niteliğinde değildir. Aynı durum 5846 sayılı Fikir ve Sanat Eserleri Kanunu'nun 71. maddesi kapsamındaki bilişim suçları açısından da geçerlidir.

Tüm bunlardan hareketle *"bilişim sistemi ile haksız yarar sağlama suçu"*nun (TCK m. 244/4), bilişim sistemleri vasıtasıyla doğrudan doğruya elde edilecek para veya para yerine geçen evrak veya senetler ya da diğer mallar için uygulama alanı bulmayacağını ifade edebiliriz. Bu suç, failin dolaylı olarak elde edeceği maddi – ekonomik kazançlar

bakımından uygulama alanı bulabilecektir. Örneğin, fail bilişim sistemine ya da sistemdeki verilere müdahale ederek iş imkanına kavuştuğunda doğrudan para elde etmediğinden fiil, TCK m. 142/2-e bağlamında hırsızlık teşkil etmemektedir; ancak, TCK m. 244/4 bakımından tipiklik oluşmaktadır. Ayrıca, sırf bilişim sistemi verisinin içerdiği bilgilerin değerli olmasından kaynaklı haksız yarar sağlama fiilleri de bu madde kapsamında yaptırıma tabi olacaktır. Böylece kanun koyucu bilişim sistemi verisinin, *"mal"* olarak kabul edilememesinin sonucu olarak ortaya çıkabilecek haksız yarar sağlamaya yönelik fiiller bakımından kanunda boşluk bulunmamasını sağlamış olmaktadır. Dolayısıyla kanun koyucunun malvarlığına karşı suçlar dışında, bir yandan kişilerin malvarlığını diğer yandan toplumun bilişim sistemlerine olan güvenini koruyacak bu suç tipini düzenlemesi yerinde olmuştur.

Her ne kadar TCK m. 244/4'ün asli normu olabilecek nitelikteki suçların yaptırımları bu suçun yaptırımından genel olarak daha ağır olsa da bu suçların daha hafif cezayı gerektiren nitelikli hallerinin gerçekleşmesi durumunda, faile uygulanacak asli normun yaptırımı, TCK m. 244/4'ten daha hafif olmaktadır. Söz konusu bu durum ise TCK'nın tek fiil ile birden fazla suç oluşması durumunda failin bu suçlardan daha ağır cezayı gerektiren suçtan dolayı sorumlu olacağına ilişkin fikrî içtima hükmüne aykırı olduğundan kanunun genel sistematiği açısından çelişkilidir. Bu sebeple, bu suçun tali norm olmaktan çıkarılarak diğer suçlarla ilişkisinin genel içtima kuralına göre çözümlenmesi yoluna gidilmesinin daha uygun olacağı kanaatindeyiz.

Son olarak belirtmek gerekir ki yalnızca bilişim sistemine girme ile elde edilecek haksız yarar sağlama bakımından TCK'da herhangi bir suç düzenlenmemiştir. Bu suretle elde edilecek haksız yararlar, TCK m. 244/4 bağlamında tipiklik arz etmeyecektir. Zira TCK m. 244/4'ten sorumluluk için failin bilişim sisteminin işleyişine (TCK m. 244/1) ya da sistemdeki verilere (TCK m. 244/2) müdahale sonucu haksız yarar elde etmesi gerekmektedir. Dolayısıyla bu durumun cezai yaptırım dışında kalmaması için kanaatimizce, suçun kanuni düzenlemesinin bilişim sistemine girmek suretiyle elde edilecek haksız yararları da kapsayacak şekilde genişletilmesi yerinde olacaktır.

KAYNAKLAR

Akarslan, Hüseyin; Bilişim Suçları, Ankara 2015.

Akbulut, Berrin; "*Bilişim Suçları*", Selçuk Üniversitesi Hukuk Fakültesi Dergisi, 2000, Cilt 8, Sayı Milenyum Armağanı 1-2.

Akbulut, Berrin; Ceza Hukuku Genel Hükümler, Ankara 2016.

Alacakaptan, Uğur; Suçun Unsurları, Ankara 1961.

Artuk, Mehmet Emin/Gökcen, Ahmet/Yenidünya, A. Caner; Ceza Hukuku Özel Hükümler, Ankara 2015.

Artuk, Mehmet Emin/Gökcen, Ahmet/Yenidünya, A. Caner; Ceza Hukuku Genel Hükümler, Ankara 2016.

Avşar, Zakir/Öngören, Gürsel; Bilişim Hukuku, İstanbul 2010.

Aydın, Emin Doğan; Bilişim Suçları ve Hukukuna Giriş, Ankara 1992.

Balı, Yunus; "*Adli Bilişim Rapor Metinlerinin Yargılama Sürecinde Kullanımı ve Anlamlandırılabilirliği*", Ses Görüntü ve Data İncelemeleri, Ankara 2008.

Baş, Eylem; Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu, Ankara 2015.

Başbüyük, İsa; "*Hırsızlık ve Dolandırıcılık Suçlarının Bilişim Sistemlerinin Araç Olarak Kullanılması Suretiyle İşlenmesi*", Ceza Hukuku Dergisi, 2010, Sayı 14, s. 151–192.

Başbüyük, İsa; "*İnternet Bankacılığı Aracılığıyla Yapılan Hukuka Aykırı Havalenin Bilişim Suçları Bakımından Değerlendirilmesi*", Ceza Hukuku Dergisi, 2013, Sayı 21, s. 55–70.

Başlar, Yusuf; Ceza Yargılamasında Elektronik Delil, Ankara 2016.

Bayamlıoğlu, İbrahim Emre; Fikir ve Sanat Eserleri Hukukunda Teknolojik Koruma, İstanbul 2008.

Bureau of Justice Statistics U.S. Departmant of Justice; "*Classifying the Crime Section I*", Computer Crime: Criminal Justice Resource Manual, 1979, Cilt 1, s. 1–30.

Casey, Eoghan; Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 3. bs., 2011.

Centel, Nur/Zafer, Hamide; Ceza Muhakemesi Hukuku, İstanbul 2015.

Centel, Nur/Zafer, Hamide/Çakmut, Özlem; Türk Ceza Hukukuna Giriş, İstanbul 2016.

Çelen, Ömer; Bir İştirak Şekli Olarak Yardım Etme (Asli Fail Yardım Eden Ayrımı), Yayımlanmamış Doktora Tezi, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Konya 2015.

Çolak, Uğur; "*Türk Hukukunda Bilgisayar Programlarının Ceza Hukuku Tedbirleri İle Korunması*", Legal Fikri ve Sınai Haklar Dergisi, 2016, Sayı 5, s. 113–128.

Değirmenci, Olgun; "*Ceza Hukuku Açısından Kredi ve Banka Kartları*", Legal Hukuk Dergisi, 2003, Cilt 1, Sayı 1, s. 592–609.

Değirmenci, Olgun; Ceza Muhakemesinde Sayısal (Dijital) Delil, Ankara 2014.

Demir, Ömer/Arıç, Mehmet/Polat, Halil; Bilişim Suçları ve Bilişim Yoluyla İşlenen Suçlar, Ankara 2015.

Demirbaş, Timur; Ceza Hukuku Genel Hükümler, Ankara 2016.

Doğan, Ramazan; Bilişim Suçları, Ankara 2014.

Donay, Süheyl; Bankacılık Ceza Hukuku, İstanbul 2007.

Dönmezer, Sulhi/Erman, Sahir; Nazari ve Tatbiki Ceza Hukuku- 2, İstanbul 1983.

Dönmezer, Sulhi/Erman, Sahir; Nazari ve Tatbiki Ceza Hukuku- 1, İstanbul 2016.

Dülger, Murat Volkan; Bilişim Suçları ve İnternet İletişim Hukuku, Ankara 2015.

Eker, Ö. Umut; "*Türk Ceza Hukuku'nda Bilişim Suçları Eski TCK Bağlamında Hukukumuzda Yer Alan İlk Düzenlemeler ve 5237 Sayılı Yeni Türk Ceza Kanunu'nun İlgili Hükümlerinin Yorumu*", TBB Dergisi, 2006, Sayı 62.

Eralp, Özgür; Hukukçular İçin Bilişim Terimleri Sözlüğü, Ankara 2007.

Eralp, Özgür; İnternet Bankacılığı ve Kredi Kartı Dolandırıcılığının Teknik, Hukuki ve Cezai Boyutu, Ankara 2012.

Erdoğan, Yavuz; "*Bilişim Sistemine Girme ve Kalma Suçu*", Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, 2010, Cilt 12, Sayı Özel, s. 1363–1433.

Erdoğan, Yavuz; Türk Ceza Kanunu'nda Bilişim Suçları, İstanbul 2012.

Erem, Faruk; Türk Ceza Hukuku Genel Hükümler Cilt 1, Ankara 1971.

Erem, Faruk; Türk Ceza Hukuku Genel Hükümler Cilt 2, Ankara 1971.

Ergün, İsmail; Siber Suçların Cezalandırılması ve Türkiye'de Durum, Ankara 2008.

Fisher, Wipe vs Shred vs Delete vs Erase: What's the Difference?, https://www.lifewire.com/wipe-vs-shred-vs-delete-vs-erase-whats-the-difference-2619146.

Gedik, Doğan; Müsadere, Ankara 2007.

Goodman, Marc; Geleceğin Suçları, (C. Özdemir, Çev.) İstanbul 2016.

Göktürk, Neslihan; Fikri İçtima, Ankara 2013.

Gül, Ahmet; Doğrudan - Dolaylı Bilişim Suçları, Ankara 2016.

Gürler, Fazıl; Teknik ve Hukuksal Yönleriyle Bilişim Alanında Suçlar, Ankara 2015.

Hafızoğulları, Zeki/Özen, Muharrem; Türk Ceza Hukuku Genel Hükümler, Ankara 2015.

Hafızoğulları, Zeki/Özen, Muharrem; Türk Ceza Hukuku Özel Hükümler Topluma Karşı Suçlar, Ankara 2016.

Hakeri, Hakan; Ceza Hukuku Genel Hükümler, Ankara 2016.

Henkoğlu, Türkay; Adli Bilişim - Dijital Delillerin Elde Edilmesi ve Analizi, İstanbul 2014.

İçel, Kayıhan; "*Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında Avrupa Siber Suç Politikasının Ana İlkeleri*", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, İnternet Özel Bölümü, 2001, Cilt LIX, Sayı 1–2.

İçel, Kayıhan; Ceza Hukuku Genel Hükümler, İstanbul 2016.

İçel, Kayıhan/Sokullu Akıncı, Füsun/Özgenç, İzzet/Sözüer, Adem/Mahmutoğlu, Fatih Selami/Ünver, Yener; Suç Teorisi, İstanbul 2000.

Ifrah, Georges; Bilgisayar Ne Sayar, (K. Dinçer, Çev.) Ankara 2002.

Juma, Mariam/Saleh, Hager/Suhail, Manal/Khalifa, Marwa; "*What is Internet of Things?*", Times of Oman, http://timesofoman.com/article/97372/Technology/Oman-Technology:-What-is-Internet-of-Things.

Karagülmez, Ali; Bilişim Suçları ve Soruşturma – Kovuşturma Evreleri, Ankara 2014.

Kaya, Mehmet Bedii; Teknik ve Hukuki Boyutlarıyla İnternete Erişimin Engellenmesi, İstanbul 2010.

Kersten, Jason; "*How Two Pakistani Brothers Created the First PC Virus*", http://mentalfloss.com/article/12462/going-viral-how-two-pakistani-brothers-created-first-pc-virus.

Keser Berber, Leyla; Adli Bilişim, Ankara 2004.

Keskin Kiziroğlu, Serap; "*Avrupa Konseyi Siber Suç Sözleşmesinde Ceza Muhakemesine İlişkin Hükümlerin Değerlendirilmesi*", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, 2013, Cilt 59, Sayı 1–2, s. 155–180.

Ketizmen, Muammer; Türk Ceza Hukukunda Bilişim Suçları, Ankara 2008.

Kızıltan, Mehmet Burak; 5237 Sayılı Türk Ceza Kanununda Bilişim Sistemine Girme, Sistemi Engelleme ve Bozma Suçları, Yayımlanmamış Yüksek Lisans Tezi, İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, İstanbul 2007.

Koca, Mahmut; "*Fikri İçtima*", Ceza Hukuku Dergisi, 2007, Cilt 2, Sayı 4.

Koca, Mahmut; "*Hukukumuzda TCK'nın 244'ncü maddesi Kapsamında Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu*", 9-10 Ekim 2008 Yargıtay Bilişim Hukuku Konferansı, sunulmuş bildiri, Ankara.

Koca, Mahmut; "*Yargıtay Kararları Işığında Bilişim Sistemlerinin Kullanılması Suretiyle Haksız Yarar Sağlama Suçları*", Prof. Dr. Ali Güzel'e Armağan, İstanbul 2010.

Koca, Mahmut/Üzülmez, İlhan; Türk Ceza Hukuku Özel Hükümler, Ankara 2016.

Koca, Mahmut/Üzülmez, İlhan; Türk Ceza Hukuku Genel Hükümler, Ankara 2016.

Köksal, Aydın; Adı Bilgisayar Olsun, İstanbul 2010.

Kurt, Levent; Açıklamalı, İçtihatlı Tüm Yönleriyle Bilişim Suçları, Ankara 2005.

Mahmutoğlu, Fatih Selami; "*Karşılaştırmalı Hukuk Bakımından İnternet Sujelerinin Ceza Sorumluluğu*", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, İnternet Özel Bölümü, 2001, Cilt LIX, Sayı 1–2.

McQuade, Samuel C.; Encyclopedia of Cybercrime, Westport, Conn 2009.

Meran, Necati; Yeni Türk Ceza Kanunu'nda Sahtecilik – Malvarlığı – Bilişim Suçları İle Ekonomi ve Ticari Alanında Suçlar, Ankara 2008.

Meran, Necati; İletişimin Denetlenmesi, Gizli Soruşturmacı ve Teknik Takibin Hukuki Boyutu, Ankara 2015.

Microsoft Açık Akademi, Eğitimler, https://www.acikakademi.com /portal/Course/12/bilgisayar-yazilim-ve-algoritma.aspx

Nişanyan, Sevan; Sözlerin Soyağacı: Çağdaş Türkçenin Etimolojik Sözlüğü, İstanbul 2009.

Okuyucu Ergün, Güneş; "*Banka veya Kredi Kartlarının Kötüye Kullanılması*", Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, 2013, Sayı 2 (Prof. Dr. Nur Centel'e Armağan), s. 1065–1086.

Orta, Mesut; Bilişim Suçları ve Adli Bilişim, Ankara 2015.

Önder, Ayhan; Ceza Hukuku Dersleri, İstanbul 1992.

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

Önok, Murat; "*Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği*", Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, 2013, Cilt 19, Sayı 2 (Prof. Dr. Nur Centel'e Armağan), s. 1229–1270.

Ören, Tuncer/Üney, Tuncer/Çölkesen, Rifat (Editörler); Türkiye Bilişim Ansiklopedisi, İstanbul 2006.

Özbek, Veli Özer; Türk Ceza Kanununun Anlamı, Ankara 2006.

Özbek, Veli Özer; "*Banka Veya Kredi Kartlarının Kötüye Kullanılması Suçu (TCK m.245)*", Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, 2007, Cilt 9, Sayı Özel Sayı.

Özbek, Veli Özer/Doğan, Koray/Bacaksız, Pınar/Tepe, İlker; Türk Ceza Hukuku Genel Hükümler, 2013.

Özbek, Veli Özer/Doğan, Koray/Bacaksız, Pınar/Tepe, İlker; Türk Ceza Hukuku Özel Hükümler, Ankara 2016.

Özbek, Veli Özer/Doğan, Koray/Bacaksız, Pınar/Tepe, İlker; Ceza Muhakemesi Hukuku, Ankara 2017.

Özdilek, Ali Osman; Bilişim Suçları ve Hukuku, İstanbul 2006.

Özen, Muharrem/Baştürk, İhsan; Temel Hak ve Özgürlükler Bağlamında Bilişim – İnternet ve Ceza Hukuku, Ankara 2011.

Özen, Muharrem/Özocak, Gürkan; "*Adli Bilişim, Elektronik Deliller ve Bilgisayarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK m. 134)*", Ankara Barosu Dergisi, 2015, Sayı 1.

Özgenç, İzzet; "*Tüzel Kişinin Sorumluluk Ehliyeti Anayasa Mahkemesi'nin Bir Kararı Üzerine Düşünceler*", Reha Poroy'a Armağan, 1995, s. 319 vd.

Özgenç, İzzet; Suça İştirakin Hukuki Esası ve Faillik, İstanbul 1996.

Özgenç, İzzet; Türk Ceza Hukuku Genel Hükümler, Ankara 2016.

Öztürk, Bahri/Erdem, Mustafa Ruhan; Uygulamalı Ceza Hukuku ve Güvenlik Tedbirleri Hukuku, Ankara 2016.

Öztürk, Bahri/Tezcan, Durmuş/Erdem, Mustafa Ruhan/Sırma Gezer, Özge/Saygılar Kırıt, Yasemin/Özaydın, Özdem/… Erden Tütüncü, Efser; Nazari ve Uygulamalı Ceza Muhakemesi Hukuku, Ankara 2016.

Pallı, Hayati; Türk Hukukunda ve Mukayeseli Hukukta Bilişim Suçları, Yayımlanmamış Doktora Tezi, Erciyes Üniversitesi Sosyal Bilimler Enstitüsü, Kayseri 2008.

Parlar, Ali; Türk Ceza Hukukunda Bilişim Suçları, Ankara 2015.

Pazarcı, Hüseyin; Uluslararası Hukuk, Ankara 2015.

Postel, J.; "*Transmission Control Protocol*", https://tools.ietf.org/html/rfc793.

Ryan, Johnny; A History of the Internet and the Digital Future, Londra 2010.

Seungjoo Kim; DDoS Attack on DNS using infected IoT Devices, Engineering, https://www.slideshare.net/skim71/ddos-attack-on-dns-using-infected-iot-devices?ref.

Sınar, Hasan; İnternet ve Ceza Hukuku, İstanbul 2001.

Sınar, Hasan; "*Avrupa Konseyi Siber Suç Sözleşmesi Üzerine Bir Deneme*", Prof.Dr. Çetin ÖZEK Armağanı, İstanbul 2004, s. 765–787.

Smith, Tony; "*Hacker jailed for revenge sewage attacks*", The Register, 31 Ağustos 2001.

Sokullu Akıncı, Füsun; "*Avrupa Konseyi Siber Suç Sözleşmesinde Yer Alan Maddi Ceza Hukukuna İlişkin Düzenlemeler ve Özellikle İnternette Çocuk Pornografisi*", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, 2001, Cilt 59, Sayı 1–2, s. 11–38.

Soyaslan, Doğan; Ceza Muhakemesi Hukuku, Ankara 2014.

Soyaslan, Doğan; Ceza Hukuku Özel Hükümler, Ankara 2016.

Soyaslan, Doğan; Ceza Hukuku Genel Hükümler, Ankara 2016.

Şahin, Cumhur; Ceza Muhakemesi Hukuku - I, Ankara 2016.

Şahin, Cumhur/Göktürk, Neslihan; Ceza Muhakemesi Hukuku - II, Ankara 2017.

Tanrıkulu, Cengiz; Ceza Muhakemesi Hukukunda Bilişim Sistemlerinde Arama ve Elkoyma, Ankara 2014.

Tanrıkulu, Cengiz; Computer Fraud, Ankara 2016.

Taşdemir, Kubilay; Bilişim, Banka veya Kredi Kartlarının Kötüye Kullanılması ve Dolandırıcılık Suçları, Ankara 2009.

Taşkın, Şaban Cankat; Bilişim Suçları, İstanbul 2008.

Taşkın, Şaban Cankat; İnternete Erişim Yasakları, Ankara 2016.

Tepe, İlker; Modern Ceza Hukuku Anlayışında İnternet Suçluluğu ve Türk Ceza Hukukundaki Yansımaları, Yayımlanmamış Yüksek Lisans Tezi, Akdeniz Üniversitesi Sosyal Bilimler Enstitüsü, Antalya 2009.

Tezcan, Durmuş/Erdem, Mustafa Ruhan/Önok, R. Murat; Teorik ve Pratik Ceza Özel Hukuku, Ankara 2010.

Toroslu, Nevzat; Cürümlerin Tasnifi Bakımından Suçun Hukuki Konusu, Ankara 1970.

Toroslu, Nevzat/Feyzioğlu, Metin; Ceza Muhakemesi Hukuku, Ankara 2016.

Toroslu, Nevzat/Toroslu, Haluk; Ceza Hukuku Genel Kısım, Ankara 2016.

U.S. Department of Justice; "*Electronic Crime Scene Investigation: A Guide for First Responders*", 2008, Cilt 1, s. 49–62.

Ünver, Yener; Ceza Hukukuyla Korunması Amaçlanan Hukuksal Değer, Ankara 2003.

Ünver, Yener; "*Türk Ceza Kanunu'nun ve Ceza Kanunu Tasarısı'nın İnternet Açısından Değerlendirilmesi*", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, 2013, Cilt 59, Sayı 1–2, s. 51–153.

Warrick, Patricia S.; The Cybernetic Imagination in Science Fiction, Cambridge 1982.

Yaşar, Osman/Gökcan, Hasan Tahsin/Artuç, Mustafa; Yorumlu - Uygulamalı Türk Ceza Kanunu, Ankara 2014.

Yazıcıoğlu, R. Yılmaz; Bilgisayar Suçları : Kriminolojik, Sosyolojik ve Hukuki Boyutları ile, İstanbul 1997.

Yenidünya, A. Caner; "*Bilişim Sistemine Hukuka Aykırı Erişim Suçu*", Legal Fikri ve Sınai Haklar Dergisi, 2005, Sayı 4, s. 1017–1042.

Yenidünya, A. Caner; "*5846 Sayılı Fikir ve Sanat Eserleri Kanunu'nda düzenlenen manevi ve mali haklara tecavüz suçları*", Erzincan Üniversitesi Hukuk Fakültesi Dergisi, 2006, Cilt 10, Sayı 3–4, s. 237–272.

Yenidünya, A. Caner; Yargıtay Kararları Işığında Hırsızlık Suçu, Ankara 2013.

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

Yenisey, Feridun/Nuhoğlu, Ayşe; Ceza Muhakemesi Hukuku, Ankara 2016.

Yerdelen, Erdal; Müsadere ve Mülkiyetin Kamuya Geçirilmesi, Ankara 2010.

Yerdelen, Erdal; Cezanın Belirlenmesi (Türk - Alman Uygulaması), Ankara 2013.

Yılmaz, Sacit; "*5237 Sayılı TCK'nın 244. Maddesinde Düzenlenen Bilişim Alanındaki Suçlar*", TBB Dergisi, 2011, Sayı 92.

Yılmaz, Sacit; Türk Ceza Hukuku Sisteminde Siber Suçlarla Mücadele, Ankara 2016.

Zafer, Hamide; Ceza Hukuku Genel Hükümler TCK m. 1-75, İstanbul 2015.